第14回　代数的組合せ論研究集会報告集

Proceedings of the 14th Algebraic Combinatorics Symposium

In Honor of Professor Michio Suzuki's 70th Birthday

July 14－17,1997
International Christian University
Mitaka, Tokyo JAPAN
於：国際基督教大学

科学研究補助金（基盤研究A）
（課題番号：08304003）

Proceedings of the 14th Algebraic Combinatorics Symposium

IN HONOR OF PROFESSOR MICHIO SUZUKI'S 70TH BIRTHDAY

July 14 - 17, 1997
International Christian University
Mitaka, Tokyo JAPAN

Contents

Appendix

Preface

This volume contains the proceedings of the 14th Algebraic Combinatorics Conference held at the International Christian University (ICU) in Mitaka, Tokyo from July 14 to July 17, 1997.

This annual domestic conference was extended in size and in scope in honor of the 70th birthday of Professor Michio Suzuki. Over 150 people attended the conference, up from the typical 100 participants. Many distinguished speakers came from over-seas to honor Professor Michio Suzuki at this conference.

Professor Michio Suzuki has had a great influence in group theory during the last 50 years. I believe that his work in the 1950's ignited the work on the classification of finite simple groups, and in the 1960's and 70's he led the developments of the classification. The classification was completed in the early 1980's by Aschbacher, Gorenstein, Thompson and many others. We will see Professor Michio Suzuki's most recent contribution to group theory in this volume.

Although Professor Michio Suzuki has been affiliated with University of Illinois since 1952, he has had a profound influence on the development of group theory (and subsequently of algebraic combinatorics) in Japan. Through him, word of recent developments in group theory often reached Japan, in particular through his regular summer visits. His recommendations gave many of us opportunities to visit abroad for research and to help us land jobs.

I think it is fair to say that much of the respect given to Japanese group theory as a whole derives from that given to Professor Michio Suzuki as one of the top mathematicians in the world.

(Of course, many other Japanese group theorists deserve some of the credit; nonetheless, the influence of Professor Michio Suzuki is extraordinary.)

In the main lecture, Professor Koichiro Harada outlined the mathematical work of Professor Michio Suzuki. Unfortunately the text of this lecture was not available for this proceedings as Professor Harada hopes to expand it to do justice to the breadth and depth of Professor Michio Suzuki's work. We hope that it will be ready for a more formal publication being prepared in honor of Professor Michio Suzuki.

Instead, we include in this proceedings the list of publications of Professor Michio Suzuki and the manuscripts (written in Japanese) of his talks at Summer School of Algebraic Combinatorics, which was held in July in 1994 in Matsuyama, Ehime.

On behalf of the organizing committee, I extend our thanks to many people who helped make this conference a success:

To Professor Michio Suzuki for allowing us to use his birthday for the conference, and thereby attracting many distinguished invited speakers from around the world;

To all the speakers and the participants;

To those who helped make this conference run smoothly, especially to the International Christian University;

In particular to Hiroshi Suzuki for doing all the difficult work in running the conference (including editing this proceedings), to Maki Murata (secretary of the conference) and the students of ICU for their very fine and dedicated work;

To those who contributed financially to this conferences-the conference was financed by several Grants-in-Aid for Scientific Rearch, the Ministry of Education, Science and Culture, Japan (Kaken-hi) with principal investigators H. Yamaki, E. Bannai, H. Suzuki, M. Miyamoto, M. Kitazume, and many others.

Finally we mention that we are hoping to prepare another more formal volume (hopefully in book form) in honor of Professor Michio Suzuki.

Eiichi Bannai,
on behalf of the organizing committee which consists of:
Eiichi Bannai, Hiroshi Suzuki, Hiroyoshi Yamaki and
Tomoyuki Yoshida

Publications of Michio Suzuki

1. On the finite group with a complete partition, *J. Math. Soc. Japan* 2, (1950), 165–185.

2. The lattice of subgroups of a finite group, 数学 [*Mathematics*] 2, (1950), 189–200, Mathematical Society of Japan.

3. On the lattice of subgroups of finite groups, *Trans. Amer. Math. Soc.* 70, (1951), 345–371.

4. On the L-homomorphisms of finite groups, *Trans. Amer. Math. Soc.* 70, (1951), 372–386.

5. A characterization of simple groups $LF(2,p)$, *J. Fac. Sci. Univ. Tokyo. Sect. I.* 6, (1951), 259–293.

6. With Y. Akizuki, 高等代数学 I [*Higher Algebra, I*], 岩波全書 168, Iwanami Shoten, 1952.

7. On finite groups with cyclic Sylow subgroups for all odd primes, *Amer. J. Math.* 77 (1955), 657–691.

8. *Structure of a Group and the Structure of its Lattice of Subgroups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 10, Springer-Verlag, Berlin-Gottingen-Heidelberg, 1956.

9. With Y. Akizuki, 高等代数学 II [*Higher Algebra, II*], 岩波全書 206, Iwanami Shoten, 1957.

10. The nonexistence of a certain type of simple groups of odd order, *Proc. Amer. Math. Soc.* 8 (1957), 686–695.

11. With R. Brauer and G. E. Wall, A characterization of the one-dimensional unimodular projective groups over finite fields, *Illinois J. Math.* 2 (1958), 718–745.

12. Applications of group characters, *Proc. Sympos. Pure Math.*, Vol. 1, 88–99, American Mathematical Society, Providence, R.I., 1959.

13. With R. Brauer, On finite groups of even order whose 2-Sylow group is a quaternion group, *Proc. Nat. Acad. Sci. U.S.A.* 45 (1959), 1757–1759.

14. On characterizations of linear groups, I, II, *Trans. Amer. Math. Soc.* 92 (1959), 191–219.

15. On finite groups containing an element of order four which commutes only with its powers, *Illinois J. Math.* 3 (1959), 255–271.

16. A new type of simple groups of finite order, *Proc. Nat. Acad. Sci. U.S.A.* 46 (1960), 868–870.

17. Investigations on finite groups, *Proc. Nat. Acad. Sci. U.S.A.* 46 (1960), 1611–1614.

18. *Stroenie gruppy i stroenie struktury ee podgrupp*, [*Structure of a group and the structure of its lattice of subgroups*], Translated from the English by L. E. Sadovskii; edited by B. I. Plotkin, Izdat. Inostr. Lit., Moscow, 1960 (in Russian).

19. Finite groups with nilpotent centralizers, *Trans. Amer. Math. Soc.* 99 (1961), 425–470.

20. On a finite group with a partition, *Arch. Math.* 12 (1961), 241–254.

21. On characterizations of linear groups, III, *Nagoya Math. J.* 21 (1962), 159-183.

22. On generalized (ZT)-groups, *Arch. Math.* 13 (1962), 199-202.

23. On a class of doubly transitive groups, *Ann. of Math.* (2) 75 (1962), 105-145.

24. Applications of group characters, *Proc. Sympos. Pure Math.*, Vol. VI, 101-105, American Mathematical Society, Providence, R.I., 1962.

25. Contributions to the theory of finite groups, *Proc. Sympos. Pure Math.*, Vol. VI, 107-109, American Mathematical Society, Providence, R.I., 1962.

26. A class of doubly transitive permutation groups, *Proc. Internat. Congr. Mathematicians* (*Stockholm, 1962*), 285-287, Inst. Mittag-Leffler, Djursholm, 1963.

27. On the existence of a Hall normal subgroup, *J. Math. Soc. Japan* 15 (1963), 387-391.

28. Two characteristic properties of (ZT)-groups, *Osaka Math. J.* 15 (1963), 143-150.

29. Finite groups of even order in which Sylow 2-groups are independent, *Ann. of Math.* (2) 80 (1964), 58-77.

30. On a class of doubly transitive groups, II, *Ann. of Math.* (2) 79 (1964), 514-589.

31. Finite groups in which the centralizer of any element of order 2 is 2-closed, *Ann. of Math.* (2) 82 (1965), 191-212.

32. A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic, *J. Algebra* 2 (1965), 1-14.

33. Transitive extensions of a class of doubly transitive groups, *Nagoya Math. J.* 27 (1966), 159-169.

34. A characterization of the simple groups $PSL(2, q)$, J. Math. Soc. Japan 20 (1968), 342-349.

35. On characterizations of linear groups, IV, *J. Algebra* 8 (1968), 223-247.

36. Characterizations of linear groups, *Bull. Amer. Math. Soc.* 75 (1969), 1043-1091.

37. A simple group of order 448, 345, 497, 600, *Theory of Finite Groups* (*Symposium, Harvard Univ., Cambridge, Mass., 1968*), 113-119, Benjamin, New York, 1969.

38. Characterizations of some finite simple groups, *Actes du Congres International des Mathematiciens* (*Nice, 1970*), Tome 1, 371-373, Gauthier-Villars, Paris, 1970.

39. A characterization of the orthogonal groups over finite fields of characteristic two, *Finite Groups,* (*Sapporo and Kyoto, 1974*), *Proceedings of Taniguchi International Symposium* No. 1, 105-112, N. Iwahori (editor) Japan Society for the Promotion of Science, 1976.

40. 群論 上 [*Group Theory, Vol. 1*], 現代数学 [Modern Mathematics] 18, Iwanami Shoten, Tokyo, 1977.

41. 群論 下 [*Group Theory, Vol. 2*], 現代数学 [Modern Mathematics] 19, Iwanami Shoten, Tokyo, 1978.

42. A transfer theorem, *J. Algebra* 51 (1978), 608-618.

43. 代数 I (改訂) [*Algebra I, Revised Ed.*], 岩波全書 318, Iwanami Shoten, Tokyo, 1980.

44. 代数 II (改訂) [*Algebra II, Revised Ed.*], 岩波全書 322, Iwanami Shoten, Tokyo, 1980.

45. Finite groups with a split BN-pair of rank one, *The Santa Cruz Conference on Finite Groups* (*Univ. California, Santa Cruz, Calif., 1979*), 139-147, Amer. Math. Soc., Providence, R.I., 1980.

46. *Group Theory, I*, Grundlehren der Mathematischen Wissenschaften 247, Springer-Verlag, Berlin-New York, 1982.

47. Classification of finite simple groups, 数学 [*Mathematics*] 34 (1982), 193–210, Mathematical Society of Japan.

48. *Group Theory, II*, Grundlehren der Mathematischen Wissenschaften 248, Springer-Verlag, New York-Berlin, 1986.

49. 有限単純群 [*Finite Simple Groups*], 紀伊国屋数学叢書 28, Kinokuniya Shoten, Tokyo, 1987.

50. Solvable generation of finite groups, *Hokkaido Math. J.* 16 (1987), 109–113.

51. The values of irreducible characters of the symmetric group, *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, 317–319, *Proc. Symposia in Pure Math.* 47 (Part 2) (1987), Amer. Math. Soc., Providence, RI, 1987.

52. A remark on finite groups having a split BN-pair of rank one with characteristic two, *J. Algebra* 112 (1988), 240–249.

53. Elementary proof of the simplicity of sporadic groups, *Group Theory (Singapore, 1987), Proc. of the Singapore Group Theory Conference*, 195–206, de Gruyter, Berlin-New York, 1989.

54. Graphs, geometries, and groups, *Algebraic Combinatorics and Related Topics, Manila 1994, Ateneo de Manila University*, 129–150.

PROGRAM

Plenary Session	Parallel Session	Monday July 14	Tuesday July 15		Wednesday July 16	Thursday July 17	
9:00-9:50		Feit, W.	Shoji		Bender	McKay	
10:10-11:00		Aschbacher	Yoshida		Stellmacher	Miyamoto	
11:20-12:10		Flavell	Stroth		Higman	Timmesfeld	
12:10-13:40		*LUNCH TIME*					
13:40-14:30	13:40-14:05	Ivanov	Usami	Koolen	Solomon	Ziechang	Kitazume
	14:05-14:30		Uno	Hiraki		Yoshiara	Yamada
14:40-15:10	14:40-15:05	Maley	Koshitani	Ito	Aschbacher	Ozeki	Yamazaki
15:10-15:40	15:05-15:30	*BREAK*	Watanabe	Teranishi	*BREAK*	Harada, M.	Hirasaka
15:40-16:30	15:30-16:05	Bannai	*TEA BREAK*		Harada, K.	*TEA BREAK*	
	16:05-16:30		Nomura	Sasaki		Kondo	Munemasa
16:40-17:30	16:40-17:05	Suzuki, H.	Curtin	Kimura	Suzuki, M.	Yamaki	
	17:05-17:30		Sawano				
18:00-20:00					Banquet		

July 14 (Monday)

- 9:00-9:50 Feit, Walter (Yale University)
  Integral Representstions of Weyl Groups and Related Topics

- 10:10-11:00 Aschbacher, Michael (California Institute of Technology)
  Quasithin Groups

- 11:20-12:10 Flavell, P.J. (The University of Birmingham)
  Solubility Criteria for Finite Groups

- 13:40-14:30 Ivanov, Alexandre A. (Imperial College of Science, Technology and Medicine)
  A Cover of the 3-local Geometry of Co_1

- 14:40-15:10 Maley, Miller (Princeton University)
  Hall Polynomials for Classical Groups

- 15:40-16:30 Bannai, Eiichi (Kyushu University)
  Codes on Finite Rings and Finite Abelian Groups (A Survey)

- 16:40-17:30 Suzuki, Hiroshi (International Christian University)
  Problems of Distance-Regular Graphs and Related Topics (A Survey)

July 15 (Tuesday)

- 9:00-9:50 Shoji, Toshiaki (Science University of Tokyo)
  Representations of Finite Chevalley Groups

- 10:10-11:00 Yoshida, Tomoyuki (Hokkaido University)
  Exponential Formulas Related to Finite Groups and Toposes

- 11:20-12:10 Stroth, Gernot
  Small Modules

Room A (Parallel Session)

- 13:40-14:05 Usami, Yoko (Ochanomizu University)
  Principal Blocks with Extra-Special Defect Groups of Order 27

- 14:05-14:30 Uno, Katsuhiro (Osaka University)
  Vertex of Non-Periodic Modules in the Auslander-Reiten Quiver of Finite Groups

- 14:40-15:05 Koshitani, Shigeo (Chiba University)
  Morita Equivalent Blocks of Finite Groups

- 15:05-15:30 Watanabe, Atumi (Kumamoto University)
  Perfect Isometries and Glauberman Correspondences

Room B (Parallel Session)

- 13:40-14:05 Koolen, Jack (Kyushu University)
  Are There Finitely Many Distance-Regular Graphs with a Given Valency?

- 14:05-14:30 Hiraki, Akira (Osaka Kyoiku University)
  An Improvement of a Diameter Bound by Ivanov (Joint work with Jack Koolen)

- 14:40-15:05 Ito, Tatsuro (Kanazawa University)
  Nonthin T-Modules of Endpoint 1

- 15:05-15:30 Teranishi, Yasuo (Nagoya University)
  The Number of Spanning Trees and Laplacian Eigenvalues of a Graph

Room A (Parallel Session)

- 16:05-16:30 Nomura, Kazumasa (Tokyo Medical and Dental University)
  Some Formulas for Spin Models on Distance-Regular Graphs, I

- 16:40-17:05 Curtin, Brian (Kyushu University)
  Some Formulas for Spin Models on Distance-Regular Graphs, II

- 17:05-17:30 Sawano, Mitsuhiro (Kyushu University)
  The Classification of Four-Weight Spin Models with Size 5

Room B (Parallel Session)

- 16:05-16:30 Sasaki, Hiroki (Ehime University)
  The mod 2 Cohomology Algebras of Finite Groups with Wreathed Sylow 2-Subgroups

- 16:40-17:05 Kimura, Hiroshi (Ehime University)
  Construction of Hadamard Matrices Using Dihedral Groups

July 16 (Wednesday)

- 9:00-9:50 Bender, Helmut (Christian-Albrechts-Universität zu Kiel)
  Generalized Fitting π-Subgroups of Finite Groups
- 10:10-11:00 Stellmacher, Bernd (Christian-Albrechts-Universität zu Kiel)
  J-Components in Finite Groups
- 11:20-12:10 Higman, Don G. (University of Michigan)
  Association Schemes and Geometries
- 13:40-14:30 Solomon, Ronald (The Ohio State University)
  The Semisimple Method for the Classification of the Finite Simple Groups
- 14:40-15:10 Aschbacher, Michael (California Institute of Technology)
  Groups Disconnected at the Prime 2
- 15:40-16:30 Harada, Koichiro (The Ohio State University)
  Professor Michio Suzuki's Contribution to the Theory of Finite Groups
- 16:40-17:30 Suzuki, Michio (The University of Illinois Urbana-Champaign)
  On the Prime Graph of Finite Simple Groups
  —An Application of a Method of Feit–Thompson–Bender–Glaubermann

(*Banquet, from 18:00 at ICU Cafeteria West Room*)

July 17 (Thursday)

- 9:00-9:50 McKay, John (Concordia University)
  Moonshine — from Dedekind and Fricke, Klein to the Present Day
- 10:10-11:00 Miyamoto, Masahiko (Tsukuba University)
  The Finite Group Theory on Vertex Operator Algebras
- 11:20-12:10 Timmesfeld, Franz (Justus-Liebig-Universität Giessen)
  Identifications of Lie-type Groups.

Room A (Parallel Session)

- 13:40-14:05 Zieschang, Paul-Hermann (Kyushu University)
  The Classification of the Buildings of Spherical Type in the Light of the Theory of Association Schemes
- 14:05-14:30 Yoshiara, Satoshi (Osaka Kyoiku University)
  Subgroup Complexes for Finite Simple Groups
- 14:40-15:05 Ozeki, Michio (Yamagata University)
  A Polynomial Approach to the Covering Radius Problem for Ternary Self-Ddual Codes

Room B (Parallel Session)

- 13:40-14:05 Kitazume, Masaaki (Chiba University)
  Binary Codes Vertex Operator Algebras and Finite Automorphism Groups
- 14:05-14:30 Yamada, Hiromichi (Hitotsubashi University)
  Ternary Codes Vertex Operator Algebras
- 14:40-15:05 Yamazaki, Norio (Kyushu University)
  On Local Structures of Some Group Association Schemes

- 15:05-15:30 Tomiyama, Masato (Osaka Kyoiku University)
  Characterization of the Group Association Scheme of $PSL(2,7)$

Room A (Parallel Session)

- 15:40-16:05 Harada, Masaaki (Yamagata University)
  New 5-Desings Constructed from the Lifted Golay Code over Z_4
- 16:05-16:30 Kondo, Takeshi (Tokyo Women's Chrisitian University)
  Some Examples of Non-Solvable Unramified Extensions over Quadratic Fields

Room B (Parallel Session)

- 15:40-16:05 Hirasaka, Mitsugu (Kyushu University)
  On Association Schemes with a Nonsymmetric Relation of Valency 4
- 16:05-16:30 Munemasa, Akihiro (Kyushu University)
  Primitive Trinomials and Orthogonal Arrays over $GF(2)$

Room A

- 16:40-17:30 Yamaki, Hiroyoshi (Kumamoto University)
  Prime Graphs (Joint work with N. Chigira and N. Iiyori)

FINITE GROUPS DISCONNECTED AT THE PRIME 2

MICHAEL ASCHBACHER

California Institute of Technology

The study of finite simple groups disconnected at some prime (particularly the prime 2) is one of the most important chapters in finite simple group theory. Since Suzuki, his students, and his postdocs played the leading role in this work, it seems appropriate to give a brief survey of the area at this conference in honor of Professor Suzuki.

Let G be a finite group and p a prime. The *commuting graph* Γ_p for G is the graph whose vertices are the subgroups of G of order p and edges are pairs of commuting subgroups. Define G to be *connected at* p if Γ_p is connected. It is an elementary exercise to see that there are the following equivalent formulations of this condition:

Lemma. *Let G be a finite group, p a prime divisor of the order of G, Δ a connected component of Γ_p and $H = N_G(\Delta)$. Then the following are equivalent:*

(1) Γ_p is disconnected.

(2) H is a strongly p-embedded subgroup of G. That is H is proper of order divisible by p and $|H \cap H^g|$ is prime to p for all $g \in G - H$.

(3) Each nontrivial p-element of H fixes a unique point of the coset space G/H.

(4) $N_G(P) \leq H \geq C_G(X)$ for $P \in Syl_p(H)$ and each X of order p in P.

Depending on the situation, one or another of these points of view may be more valuable. There are also weaker connectedness conditions which are sometimes important. I will mention some of these later.

The theorem determining the groups disconnected at the prime 2 was one of the major steps in the classification of the finite simple groups. This theorem is due to Suzuki and Helmut Bender. Groups disconnected at odd primes are only known as a corollary to the Classification, although treating a very special case of disconnected groups at odd primes was one of the hard steps in the Classification. One also needs to know the disconnected groups in modular representation theory, (Alperin and Dade conjectures) the study of subgroup complexes of finite groups, permutation group theory, etc.

The two major contributors to the determination of the groups disconnected at 2 were Suzuki and Bender. In the early sixties, Suzuki proved:

This work was partially supported by NSF-9622843

Theorem. *(Suzuki, [Su]) Let G be a transitive group of permutations on a set X of odd order such that the stabilizer H of $x \in X$ contains a normal subgroup Q regular on $X - \{x\}$ such that H/Q is of odd order. Then either*

(1) G is solvable and known, or

(2) G is an extension of a rank 1 group L of Lie type and even characteristic and the permutation action is on the Borel subgroups of L.

The rank 1 groups of Lie type and even characteristic are $L_2(q)$, $Sz(q)$, and $U_3(q)$, q even. The groups $Sz(q)$ are the *Suzuki* groups, and were discovered and constructed by Suzuki in the process of proving this theorem. Only later was it discovered that the Suzuki groups are of Lie type.

About 1970, Bender extended Suzuki's result to a classification of groups disconnected at the prime 2 by showing:

Theorem. *(Bender, [B]) Let G be a group with a strongly embedded subgroup H. Then either*

(1) G has cyclic or quaternion Sylow 2-subgroups, or

(2) The representation of G on the cosets of H satisfies the hypotheses of Suzuki's theorem.

In particular G is a simple group with a strongly 2-embedded subgroup if and only if G is a rank 1 group of Lie type and even characteristic. Its also worth noting that it was Brauer and Suzuki [BS] who showed that a group with quaternion Sylow 2-groups is not simple. This follows from an elementary transfer argument when the Sylow 2-groups are cyclic.

Next I want to discuss a connectedness theorem due to Ernie Shult, one of Suzuki's students and an outstanding mathematician in his own right. Given $V \leq H \leq G$, define V to be *strongly closed in H with respect to G* if $v^G \cap H \subseteq V$ for all $v \in V$.

Theorem. *(Shult's Fusion Theorem, [Sh]) Let G be a finite group, V an abelian subgroup of G such that $V = \langle t^G \cap C_G(t) \rangle$ for some involution t, and V is strongly closed in $H = N_G(V)$ with respect to G. Then $G = L_0 \cdots L_m$ where $[L_i, L_j] = 1$ for $i \neq j$, $L_0/O(L_0)$ is an elementary abelian 2-group, and for $i > 0$, L_i is $L_2(2^n)$, $Sz(2^n)$, $U_3(2^n)$, or a covering of $Sz(8)$.*

At first glance this may not look like a connectedness result, but the hypotheses are equivalent to:

G is a finite group, $H \leq G$, t is an involution in H fixing a unique point of the coset space G/H and $V = \langle t^H \rangle$ is abelian and strongly closed in H with respect to G.

Thus the commuting graph on t^G (rather than the set of *all* involutions of G) is disconnected and a connected component of the graph is complete. If t^H is of odd order, one can omit the condition that V is strongly closed in H with respect to G.

Shult's Fusion Theorem was an important tool in the Classification, but even more, it inspired at least three other important tools. First, in [G], David Goldschmidt classified all groups with a strongly closed abelian 2-subgroup. Thus he weakened Shult's hypotheses, but he also appealed to Shult's result in his proof. Goldschmidt's theorem is not strictly speaking a connectedness result.

Shult never published his Fusion Theorem, but one section of his proof is reproduced with slight variations in the next paper. To simplify the statement of the theorem, I assume G is simple, but this is not really necessary if one slightly extends the class of examples.

Theorem. *(Aschbacher* [A1], [A2]*) Let G be a finite simple group, $H < G$, and $z \in H$ an involution in the center of a Sylow 2- subgroup of G. Assume*

(1) z fixes a unique point of the coset space G/H, and

(2) If $z \neq t \in z^G \cap C_G(z)$ then $C_G(tz) \leq H$.

Then H is strongly embedded in G, so $G \cong L_2(2^n)$, $Sz(2^n)$, or $U_3(2^n)$.

I heard Shult speak about his fusion theorem at a seminar at the University of Illinois in 1970 while I was a postdoc at Illinois with Suzuki. Reading Shult's paper and Bender's paper on groups with a strongly embedded subgroup helped me to prove the result above, and that theorem is used in turn to prove the final connectedness result I will mention.

Define Γ_2^2 to be the commuting graph on elementary abelian 2- subgroups of G of rank at least 2 and $\Gamma_2^{2,\circ}$ the subgraph of non-isolated vertices in Γ_2^2.

Theorem. *(Aschbacher* [A1]*) Let G be a finite simple group of 2-rank at least 3 such that $\Gamma_2^{2,\circ}$ is disconnected. Then G is $L_2(2^n)$, $Sz(2^n)$, $U_3(2^n)$ or J_1.*

This last result is used in conjunction with signalizer functor theory to control the groups $O(C_G(t))$, t an involution in G. The problem of determining all such groups (phrased somewhat differently) was posed by Gorenstein and Walter.

In summary, the classification of groups disconnected at the prime 2 and of groups satisfying various weaker properties, is one of the important chapters in the Classification of the finite simple groups. The fact that we have no analogous theory for odd primes causes difficulties at various places in the Classification. Disconnected groups continue to play an important role in representation theory, permutation group theory, and the study of subgroup complexes.

Suzuki began work on the problem by proving the first major result in this area in characterizing the groups of Lie type of even characteristic and Lie rank 1 as the disconnected groups 2-transitive on there connected components. Indeed in the process he discovered and constructed the Suzuki groups, which at that time had not surfaced in the Lie theory. Bender completed the classification, and Suzuki's student Ernie Shult proved the first major result weakening the disconnected hypotheses. I proved the last two results in the area in work that began while I was a postdoc at the University of Illinois with Suzuki and depended heavily on the work of Bender and Shult.

References

M. Aschbacher, *Finite groups with proper 2-generated cores*, Trans. AMS 179 (1974), 87–112.

M. Aschbacher, *On finite groups of component type*, Illionis J. Math. 19 (1975), 78–115.

H. Bender, *Transitive Gruppen gerader Ordung, in denen jede Involution genau einen Punkt festlasst*, J. Alg 17 (1971), 527–554.

R. Brauer and M. Suzuki, *On finite groups of even order whose 2-Sylow subgroup is a quaternion group*, Proc. Nat. Acad. Sci. USA 45 (1959), 1757–1759.

D. Goldshmidt, *2-fusion in finite groups*, Ann. Math. 99 (1974), 70–117.
E. Shult, *On the fusion of an involution in its centralizer*, preprint (1970).
M. Suzuki, *On a class of doubly transitive groups, I*, Ann. Math. 75 (1962), 105–145; *II*, Ann. Math. 79 (1964), 514–589.

Pasadena, California 91125

CODES OVER FINITE RINGS AND FINITE ABELIAN GROUPS (A SURVEY)

Eiichi Bannai

Graduate School of Mathematics
Kyushu University

These notes are basically the transparencies of my talk at the Symposium in honor of Professor Michio Suzuki, which was held at ICU (the International Christian University) in July 1997. In this talk, I gave a survey of recent results on the relations between the weight enumerators of codes, invariant rings of certain finite groups, and modular forms, including several generalizations. The main new point of this talk is that we can define the concept of a Type II code for codes (additive subgroups) over any finite abelian group. (Here we consider codes over any finite abelian group instead of the usual binary field or other fields or rings.) A part of this talk is based on ongoing joint work with Steven Dougherty, Masaaki Harada and Manabu Oura.

§1. Review of codes over F_2.

First, we give a review of the classical results concerning the relations between binary type II (i.e., self-dual doubly even) codes, even unimodular lattices, invariant rings of certain finite groups, and ordinary modular forms.

Let $V = F_2^n$ be the n-dimensional vector space over the binary field $F_2 = \{0, 1\}$. A vector subspace C of V is called a (linear) code. For two elements

$$x = (x_1, x_2, \dots, x_n) \in V$$

and

$$y = (y_1, y_2, \dots, y_n) \in V$$

we define

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \in F_2.$$

The dual code $C^\perp$ is defined by

$$C^\perp = \{y \in V | x \cdot y = 0, \forall u \in C\}.$$

We say that C is self-dual if $C = C^\perp$. We have $k := dimC = n/2$ for a self-dual code C. We call C is doubly-even if

$$4 | wt(u), \forall u \in C.$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Here, for $u = (u_1, u_2, \ldots, u_n) \in C$, we define $wt(u) = |\{j|x_j \neq 0\}|$. We say that a code C is a Type II code (on F_2) if C is self-dual and doubly-even.

Definition (Weight enumerator of a code)
For a code C, the weight enumerator $W_C(x, y)$ of the code C is defined as follows:

$$W_C(x,y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \in \mathbb{C}[x,y].$$

(Note that $W_C(x,y)$ is a homogeneous polynomial of degree n in the indeterminants x and y.)

Now, let G be the finite group of order 192 generated by the two elements $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Here note that the group G is a finite unitary reflection group (No. 9 in the list of Shephard and Todd). It is known that for a binary type II code C, its weight enumerator $W_C(x,y)$ is in the invariant ring $C[x,y]^G$ (by the action of the group G on the polynomial ring $C[x,y]$). Moreover, it is known as Gleason's theorem (1970) that
(1) the vector space spanned by the weight enumerators of Type II codes coincides with the invariant ring $C[x,y]^G$, and that
(2) the invariant ring $C[x,y]^G$ is a polynomial ring $C[f_1, f_2]$ generated by the following two algebraic independent polynomials f_1 and f_2, where

$$f_1 = W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$$

is the weight enumerator of the $[8,4,4]$-Hamming code e_8, and

$$f_2 = W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} = y^{24}$$

is the weight enumerator of the $[24,12,8]$-Golay code g_{24}.

Now, let us recall the procedure (Construction A) of constructing an integral lattice from a binary code. Let φ be the natural homomorphism from Z^n to $(Z/2Z)^n \cong F_2^n$. For a code C in F_2, define

$$L_C = \frac{1}{\sqrt{2}}\varphi^{-1}(C) \subset R^n.$$

It is known that if C is a binary Type II code, then L_C is an even unimodular lattice. The theta function of a lattice L is defined by

$$\Theta_L(\tau) = \sum_{x \in L} q^{\frac{1}{2}x \cdot x}, \quad (q = e^{2\pi i\tau}).$$

(Here τ takes the value in the upper half plane.) Note that if L is an even unimodular lattice, then $\Theta_L(\tau)$ is a modular form of weght $k = n/2$ with respect to the full modular group $SL(2,Z)$. Here we recall that the complex valued function f defined on the upper half plane $\mathcal{H}$ is called a modular form of weight k (with respect to the full modular group $SL(2,Z)$) if the following three conditions are satisfied.
(1) f is a holomorphic function on $\mathcal{H}$.

(2)

$$f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau), \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,Z).$$

(3) $f(\tau)$ has a Fourier expansion

$$f(\tau) = \sum_{r \geq 0} a_r q^r \quad (q = e^{2\pi i r}).$$

Theorem(Broué and Enguehard, 1972)
If C is a Type II code (over F_2), then we have

$$\Theta_{L_C} = W_C(\theta_3(2\tau), \theta_2(2\tau)).$$

(Here note that $\theta_3(2\tau) = A(\tau)$ is the theta series of the 1-dimensional integral lattice $\{\sqrt{2}z | z \in Z\}$ and $\theta_2(2\tau) = B(\tau)$ is the theta series of the translate (by $\frac{1}{\sqrt{2}}$) of the lattice $\{\sqrt{2}z | z \in Z\}$.)

It should be pointed out that by the map

$$x \mapsto \theta_3(2\tau)$$

$$y \mapsto \theta_2(2\tau),$$

we get an isomorphism

$$C[x,y]^G \cong C[E_4, \Delta_{12}]$$

where E_4 is the Eisenstein series of weight 4, and Δ_{12} is the cusp form of weight 12. Note that $C[E_4, \Delta_{12}]$ is a subspace of the space of all the modular forms which is isomorphic to the polynomial ring $C[E_4, E_6]$ generated by E_4 and E_6(the Eisenstein series of weight 6). Here, E_4 and E_6 are algebraically independent.

It is interesting to point out (cf. Ozeki[18] or Runge[19]) that if we take the index 2 subgroup H (of order 96) of G defined by

$$H = < \frac{1+i}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} >,$$

then the above map defines an isomorphism

$$C[x,y]^H \cong C[E_4, E_6].$$

Moreover,$C[x,y]^H = C[f_1, f_3]$, where

$$f_1 = W_{e_8}(x,y)$$

and

$$f_3 = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}.$$

Note that H is another finite unitary reflection group (No.8 in the list of Shephard and Todd.)

The important implication of this fact is that we can understand the space of modular forms completely through the invariant ring of the finite group H.

Interestingly enough, this situation can be generalized in several directions. We list some of them in the following table.

Generalizations.

automorphic forms	codes	invariant rings of finite groups
(ordinary) modular forms	weight enumerator $W_C(x,y)$	H(or G) $\subset GL(2,C)$ $C[x,y]^H$
Siegel modular forms (Runge)	multi-weight enumerator	$H =$ $Z_4 * Z_2^{2n+1} Sp(2g,2)$, $H \subset GL(2^g,C)$
Jacobi forms (Bannai-Ozeki Runge)	certain joint weight enumerator (Jacobi polynomials in the sense of Ozeki)	simultaneous diagonal action of (H (of order 96) $H \subset GL(2r,C)$)
Siegel-Jacobi forms	*	*
......	......	......
Hilbert modular forms (Hirzebruch-van der Geer)	Lee weight enumerator (over F_p)	certain finite group G, $G \subset GL(\frac{p-1}{2},C)$
......	......	......

§2. Type II Codes over Finite Rings and Finite Abelian Groups.

Codes are considered not only over binary field F_2 but also over other finite fields $F_3, F_4, \ldots, F_q$, or over $Z/4Z$ (as was studied by many people, including Hammons-Kumar-Calderbank-Sloane-Sole, and others), over $Z/2kZ$ (by M. Harada et. al.) and so on. Also, recently, there are many interesting works on codes over some finite rings (by Woods, Bachoc, etc. etc.)

The purpose of our study is to study codes over finite rings and arbitrary finite abelian groups. I believe that considering (additive) codes over any finite abelian group is the most natural and most reasonable framework for this kind of study. (A preliminary idea is due to Delsate[8], who considered self-dual codes in this context.) The main purpose of this talk is to define Type II codes in this general setting. I believe that the definition given here is reasonable and gives the correct generalization. (This part of the research is based on joint work with Steven Dougherty, Masaaki Harada and Manabu Oura.)

Before considering codes over finite abelian groups in general, we review some basic concepts on codes over the finite rings $Z/4Z$ and $Z/2kZ$.

On $Z/4Z$, we define the E-$wt(a)$ for $a \in Z/4Z$ as follows. (E-wt stands for Euclidean weight.)

$a \in Z/4Z$	0	1	2	3
E-$wt(a)$	0	1	4	1

Then for $u = (u_1, u_2, \ldots, u_n) \in (Z/4Z)^n$, we define

$$E\text{-}wt(u) = \sum_{i=1}^{n} E\text{-}wt(u_i).$$

We call C is a Type II code over $Z/4Z$ if
(1) C is self-dual, that is $C = C^{\perp}$ with respect to the usual inner product in $(Z/4Z)^n$, namely $C^{\perp} = \{y \in V | x \cdot y = 0, \forall x \in C\}$ with $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n \in Z/4Z$.
(2) $8 | E\text{-}wt(u), \forall u \in C$.

On $Z/2kZ$, we define the $E\text{-}wt(a)$ for $a \in Z/2kZ$ as follows.

$a \in Z/2kZ$	0	1	2	3	$\cdots$	i	$\cdots$	$2k-2$	$2k-1$
$E\text{-}wt(a)$	0	1	4	9	$\cdots$	i^2	$\cdots$	4	1 .

Similarly, we define the code C to be a Type II code, if
(1) C is self-dual with respect to the ordinary inner product in $(Z/2kZ)^n$, and
(2) $4k | E\text{-}wt(u), \forall u \in C$.

In this case, if we define the natural homomorphism from Z^n to $(Z/2kZ)^n$ by φ, then for each code C in $(Z/2kZ)^n$, the set $L_C = \frac{1}{\sqrt{2k}}\varphi^{-1}(C) \subset R^n$ becomes an even unimodular lattice in R^n.

Now let us consider codes on any finite abelian group G. By a code over G, we mean an additive subgroup C of $G^n = G \times G \times \cdots \times G$ (the direct product of n G's).

In order to define the concept of self-dual code, we consider the character table of the abelian group G.

A character table P of the group $G = Z/mZ$ is given as follows.

$$P = \begin{array}{cccccc} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \cdots & \zeta^{m-1} \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \cdots & \zeta^{2(m-1)} \\ 1 & \zeta^3 & \zeta^6 & \zeta^9 & \cdots & \zeta^{3(m-1)} \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{m-1} & \zeta^{2(m-1)} & \zeta^{3(m-1)} & \cdots & \zeta^{(m-1)^2} \end{array}$$

Note that in a character table we can choose, in principle, the orderings of the elements of G and the irreducible characters of G in any order. However, note that here we arranged the character table P in such a way that ${}^tP = P$ holds.

We can take the following matrices P as character tables of the group $Z_2 \times Z_2$.

$$P = \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}$$

or

$$P = \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{array}.$$

Again, we arranged so that ${}^tP = P$ holds. Namely, we have $\chi_a(b) = \chi_b(a), \forall a, b \in G$. This is equivalent to saying (in the terminology of [3]) that we fix a duality

$$a \longleftrightarrow \chi_a$$

where χ_a is the (irreducible) linear character corresponding to the element $a \in G$.

We define the concept of self-dual code by considering the following inner product $< x, y >$ on G^n. Fix a character table P of the abelian group G. It is important that we take P in such a way that ${}^tP = P$ holds. As the above example of the group $G = Z/2Z \times Z/2Z$ shows, the choice of duality, i.e., the choice of the character table P with ${}^tP = P$is not unique in general.

For two elements

$$x = (x_1, x_2, \dots, x_n) \in G^n$$

and

$$y = (y_1, y_2, \dots, y_n) \in G^n$$

we define

$$< x, y >= \prod_{i=1}^{n} \chi_{x_i}(y_i).$$

Then we define

$$C^\perp = \{y \in G^n \mid < x, y >= 1, \forall x \in C\}.$$

A code C is called self-dual if $C^\perp = C$. The problem we want to discuss here is: how to define the concept of Type II code? Here we give an answer to this question. Now, let us recall our notation again.

G is a finite abelian group of order g. Let P be a character table of G with ${}^tP = P$ (so, P is a $g \times g$-matrix.) That is, we fix a duality

$$a \longleftrightarrow \chi_a.$$

We say that a diagonal matrix

$$T = \begin{pmatrix} t_0 & 0 & \cdot & 0 \\ 0 & t_1 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & t_{g-1} \end{pmatrix}$$

has the modular invariance property if

$$(PT)^3 = (scalar) \cdot I.$$

We remark that for each G, the dualities, and the solutions T of the modular invariance property (for each fixed duality) are completely determined. (See Bannai-Bannai-Jaeger[3].)

It is known in [3] that if the order of the group G is even, then the solution T can be expressed in the following way, by using $\eta = e^{2\pi i \frac{1}{2l}}$, where l is the exponent of the abelian group G. (The exponent is the largest order of the elements of the abelian group G.)

$$T = \begin{pmatrix} \eta^{a_0} & 0 & \cdot & 0 \\ 0 & \eta^{a_1} & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \eta^{a_{g-1}} \end{pmatrix}$$

Here the $\alpha(\in G)$th diagonal element is η^{a_α}. (If $|G|$ is odd, we can take $\eta = e^{2\pi i \frac{1}{l}}$ and get a similar expression for T.) Also, here we assume that $a_0 = 0$ holds.

Example.
Note that if $G = Z/2kZ$ then we have a solution

$$T = \begin{pmatrix} \eta^0 & 0 & & & 0 \\ 0 & \eta^1 & & & \\ & & \eta^4 & & \\ \vdots & & & \ddots & 0 \\ 0 & & \cdots & 0 & \eta^{(2k-1)^2} \end{pmatrix}$$

Now, for each solution T of the modular invariance property

$$T = \begin{pmatrix} \eta^{a_0} & 0 & \cdot & 0 \\ 0 & \eta^{a_1} & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \eta^{a_{g-1}} \end{pmatrix},$$

we define for each $\alpha \in G$, $Wt(\alpha) = a_\alpha$. Then for $u = (u_\alpha)_{\alpha \in G}$ we define

$$Wt(u) = \sum_{\alpha \in G} Wt(u_\alpha).$$

Note that in the case of $G = Z/2kZ$, (and for P and T given above), our weight $Wt(u)$ coincides with the Euclidean weight $E\text{-}wt(u)$. So our weight is a generalization of the Euclidean weight.

Definition
We define a code C(over an abelian group G) to be a Type II code (over an abelian group G) if C is self-dual and

$$2l | Wt(u), \forall u \in C.$$

(Note that this definition of Type II codes depends not only on G but also on P and T.)

Complete weight enumerator.
The complete weight enumerator of a code C is defined as follows:

$$W_C(\{x_\alpha | \alpha \in G\}) = \sum_{u \in C} \prod_{\alpha \in G} x_\alpha^{\omega_\alpha(u)},$$

where for $u = (u_1, u_2, \ldots, u_n) \in G^n$, we define

$$\omega_\alpha(u) = |\{j | u_j = \alpha\}|.$$

Then

$$W_C(\{x_\alpha | \alpha \in G\}) \in C[x_\alpha | \alpha \in G]^G$$

where

$$\mathcal{G} := < \frac{1}{\sqrt{g}} P, T > \subset GL(g, C)$$

is a finite group. It can be proved that if $G = Z/2^m Z$, and if P and T are as before, then the group $\mathcal{G}$ is a group of order $192 \cdot 2^{m-1}$. It is very interesting that this group $\mathcal{G}$ is always a finite group for any G, P and T. (This fact will be discussed in a separate paper.) It is an intersting question to know the structure of this group explicitly for any G, P and T.

§3. Concluding Remarks.

First we remark that considering codes over a finite abelian group is more general than considering codes over a finite commutative ring. For a code C over a finite ring R, i.e.,C is an additive subgroup of R^n, the dual code $C^\perp$ is defined by using the multiplication of the ring:

$$C^\perp = \{y \in R^n | x \cdot y = 0, \forall x \in C\}, \tag{1}$$

where $x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$. On the other hand, for a code C over an abelian group G, i.e., an additive subgroup of G^n, the dual code $C^\perp$ is defined by:

$$C^\perp = \{y \in G^n | < x, y >= 1, \forall x \in C\}.$$

Note that (1) corresponds to fixing a duality in the additive abelian group $G = (R, +)$. So codes over a finite ring may be regarded as a special case of codes over a finite abelian group(with a certain choice of duality).

Next we consider how we may construct lattices, in certain general situation, from codes over finite abelian groups. Let K be a finite Galois extensition of the rational number field Q. Let $\mathfrak{o} = \mathfrak{o}_K$ be the ring of the integers of K. Let I be any ideal in $\mathfrak{o}$, and let

$$\mathfrak{o}/I \cong R$$

where R is a finite commutative ring. Let φ be the natural homomorphism from $(\mathfrak{o})^n$ to $(\mathfrak{o}/I)^n$. For a code C in R^n, $\varphi^{-1}(C)$ may be regarded as a lattice in $\mathfrak{o}^n$. Many interesting lattices arise in this way (see for example Bachoc[1], etc.) Finally we emphasize that the following situation is very interesting and worthy of further study.

Example.

$K = Q(i)$ where $i = \sqrt{-1}$. $\mathfrak{o}_K = Z[i]$, $p = 2$, and $I = 2Z[i]$. Then $\mathfrak{o}/I = R$ and $(R, +) \cong Z/2Z \times Z/2Z$. By considering the codes over the ring R or equivalently codes over the abelian group $G = Z/2Z \times Z/2Z$, we can obtain hermitian modular forms. Further details will be treated in a separate paper.

We would like to point out that, in·this way, we can get many automorphic forms, and also get better understandings of automorphic forms. It is very interesting to note that essentially finite objects such as weight enumerators of codes or polynomial invariants of certain finite groups enable us to control essentially infinite objects such as automorphic forms.

References

[1] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Combinatorial Theory (A) 78 (1997), 173-187.

[2] E. Bannai, *Invariant rings of finite groups and automorphic forms (a survey) (in Japanese)*, Algebra Symposium Proceedings (at Yamagata University, July 24-27,1996) 41 (1996), 173-187.

[3] E. Bannai, E. Bannai and F. Jaeger, *On spin models, modular invariance, and duality*, J. Algebraic Combinatorics 6 (1997), 203-228.

[4] E. Bannai and M. Ozeki, *Construction of Jacobi forms from certain combinatorial polynomials*, Proc. Japan Acad (A) 72 (1996), 12-15.

[5] E. Bannai, S. Dougherty, M. Harada and M. Oura, *Thpe II codes, even unimodular lattices and invariant rings, in preparation.*

[6] M. Broué and M. Enguehard, *Polynomes des poids de certains codes et fonctions theta de certains reseaux*, Ann. Sci. Ecole Norm. Sup. 5 (1972), 157-181.

[7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[8] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplments 10 (1973), 125-136.

[9] W. Duke, *On codes and Siegel modular forms*, International Math. Res. Notes (1993), 125-136.

[10] W. Ebeling, *Lattices and Codes, a course partially based on lectures by F. Hirzebruch*, Vieweg, 1994.

[11] M. Eichler and D. Zagier, *The Theory of Jacobi Forms*, Birkhauser, 1985.

[12] E. Freitag, *Siegelsche Modulfunktionen*, Springer, 1983.

[13] P. Gaborit, *Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings*, IEEE Trans. on Inf. Theory 42 (1996), 1222-1228.

[14] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes Congress Intern. Math. 3 (1970), 211-215.

[15] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4-linearlity of Kerdock, Preparata, Goethals and related codes,*, IEEE Trans. on Inf. Theory 40 (1994), 301-319.

[16] S. Nagaoka, *A note on the structure of the ring of symmetric Hermitian modular forms of degree 2 over the Gaussian field*, J. Math. Soc. Japan 48 (1996), 525-549.

[17] M. Oura, *The dimension formula for the ring of code polynomials in genus 4*, Osaka J. Math. 34 (1997), 53-72.

[18] M. Ozeki, *On the notion of Jacobi polynomials for codes*, Math. Proc. Cambridge Phil. Soc. 121 (1997), 15-30.

[19] B. Runge, *On Siegel modular forms, part I*, J. Reine angew. Math. 436 (1993), 57-85.

[20] B. Runge, *Theta functions and Siegel-Jacobi forms*, Acta Mathematica 175 (1995), 165-196.

[21] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. 6 (1954), 274-304.

[22] S. Tsuyumine, *On Siegel modular forms of degree three*, Amer. J. Math. 108 (1986), 755-862.

[23] J. A. Wood, *Duality for modules over finite rings and applications to coding theory (preprint).*

PRIME GRAPHS

NAOKI CHIGIRA, NOBUO IIYORI AND HIROYOSHI YAMAKI†

The purpose of this note is to announce [4]:

Main Theorem. *Every non abelian Sylow subgroup of a finite group of even order contains a non trivial element which commutes with an involution.*

Our main theorem is closely related to the prime graphs of finite groups. Let G be a finite group and $\Gamma(G)$ the prime graph of G. $\Gamma(G)$ is the graph such that the vertex set is the set of prime divisors of $|G|$, and two distinct vertices p and r are joined by an edge if and only if there exists an element of order pr in G. Let $n(\Gamma(G))$ be the number of connected components of $\Gamma(G)$ and $d_G(p,r)$ the distance between two vertices p and r of $\Gamma(G)$. It has been proved that $n(\Gamma(G)) \leq 6$ in [13] [9] [11] and $d_G(p,r) \leq 4$ or $d_G(p,r) = \infty$, that is, there is no path between p and r (See [10]).

Theorem 1. *Let G be a finite group of even order and p be a prime divisor of $|G|$. If $d_G(2,p) \geq 2$, then a Sylow p-subgroup of G is abelian.*

Theorem 1 is a restatement of Main Theorem in terms of the prime graph $\Gamma(G)$.

Corollary 1. Let G be a finite group of even order and p be a prime divisor of $|G|$. If Δ is a connected component of $\Gamma(G) - \{p\}$ not containing 2, then a Sylow r-subgroup of G is abelian for any $r \in \Delta$.

There is a certain relation between a subgraph $\Gamma(G) - \{p\}$ of $\Gamma(G)$ and Brauer characters of p-modular representations of G (See [3]).

Theorem 2. *Let G be a finite non abelian simple group and p be a prime divisor of $|G|$. Then $d_G(2,p) = 1$ or 2 provided $d_G(2,p) < \infty$.*

The significance of the prime graphs of finite groups can be found in [1] [3] [5] [6] [7] [8] [15] [16]. Our spirits of proving theorems can be found in [1] [2] [4] [7] [9] [14].

We will give some examples of case by case analysis for finite simple groups. Theorem 1 holds true for the sporadic simple groups by *Atlas of Finite Groups* although we can find several typos in it. For a positive integer k let $\pi(k)$ be the set of all prime divisors of k. Let $\pi_0 = \{p \in \pi(G) | d_G(2,p) = 1\}$.

†Supported in part by Grant-in-Aid for Scientific Research (No.8304003, No.08640051), Ministry of Education, Science, Sports and Culture, Japan.

Example. Let G be the alternating group on n-letters where $n \geq 7$ and $p \in \pi(G)$. If $p \leq n-4$, then $d_G(2,p) = 1$. If $p \geq n-3$, then Sylow p-subgroups of G are cyclic of order p. Thus Theorem 1 holds true for the alternating groups.

Example. Let $G = PSL(n,q)$, $q \equiv 0(2)$. Then $|G| = q^{n(n-1)/2}\prod_{i=1}^{n-1}(q^{i+1}-1)d^{-1}$, $d = (n, q-1)$. Let I_j be the $j \times j$ identity matrix. Put

$$t_k' = \begin{pmatrix} I_k & 0 & 0 \\ 0 & I_{n-2k} & 0 \\ I_k & 0 & I_k \end{pmatrix}$$

Then $t_k'(1 \leq k \leq r)$ where $r = [n/2]$, are representatives of the conjugacy classes of involutions in $SL(n,q)$. The centralizer of t_k' in $SL(n,q)$ is the set of all matrices of the form

$$\begin{pmatrix} A & 0 & 0 \\ H & B & 0 \\ K & L & A \end{pmatrix}$$

where $(detA)^2 detB = 1$ and A is an $k \times k$ nonsingular matrix. Denote t_k the homomorphic image of t_k' in $PSL(n,q)$. Then t_k $(1 \leq k \leq r)$ are representatives of the conjugacy classes of involutions in $PSL(n,q)$. Let $C_k = C_G(t_k)$. Then

$$\pi(C_k) = \pi(2\prod_{i=1}^{n-2k}(q^i-1)/(q-1)d)$$

and

$$\pi_0 = \pi(\prod_{k=1}^{r}|C_k|) = \pi(2\prod_{i=1}^{n-2}(q^i-1))$$

Suppose that $n \geq 4$. Then the only factors of $|G|$ to be considered is $(q^{n-1}-1)(q^n-1)$. There are maximal tori $T(A_{n-2})$ of order $(q^{n-1}-1)d^{-1}$ and $T(A_{n-1})$ of order $(q^n-1)/(q-1)d$. Let $p \in \pi(T(X)) - \pi_0$ where $X = A_{n-1}$ or A_{n-2}. Let P be a Sylow p-subgroup of $T(X)$. Then $d_G(2,p) = 1$ or P is a Sylow p-subgroup of G. Since P is abelian, Theorem 1 holds true for $G = PSL(n,q)$, $n \geq 4$.

Suppose that $n = 3$. Then $|G| = q^3(q^2-1)(q^3-1)d^{-1}$ and there are three classes of maximal tori of orders

$$(q-1)^2d^{-1}, \quad (q^2-1)d^{-1}, \quad (q^2+q+1)d^{-1}.$$

We note that a torus of order $(q^2+q+1)d^{-1}$ is an isolated subgroup. If $q \geq 4$, then $d_G(2,r) = 2$ for $r \in \pi(q+1)$. Let R be a Sylow r-subgroup of G. Then R is contained in a maximal torus of order $(q^2-1)d^{-1}$. If $q = 4$, then $G = L_3(4)$ and $|G| = 2^6.3^2.5.7$. If $q = 2$, then $G = L_3(2)$ and $|G| = 2^3.3.7$. We have verified Theorem 1 for $n = 3$. It is trivial that Theorem 1 holds true for $PSL(2,q)$.

Theorem 3. *Let G be a simple group of Lie type and T a maximal torus. Let $p \in \pi(T) - \pi_0$. Then T contains a Sylow p-subgroup of G.*

Theorem 3 is a corollary of Theorem 1. Actually we prove Theorem 3 for specified tori when we verify Theorem 1 for the simple groups of Lie type.

Remark. Suzuki[12] determined the structure of (CIT)-groups. A (CIT)-group is a finite group of even order in which the centralizer of every involution is a 2-group. His theorem implies that if p is an odd prime, then a Sylow p-subgroup of a (CIT)-group is always abelian. This means that if a finite group G of even order contains a non abelian Sylow p-subgroup for odd prime p, then G is not a (CIT)-group. Suzuki's theorem, however, appears not to give us any information as to whether any non abelian Sylow p-subgroup of a finite group of even order always contains a non trivial element which commutes with an involution.

References

1. N. Chigira, Finite groups whose abelian subgroups have consecutive orders, To appear in Osaka J. Math.
2. N. Chigira, Number of Sylow subgroups and p-nilpotence of finite groups, To appear in J. Algebra.
3. N. Chigira and N. Iiyori, Prime graphs and Brauer characters, preprint.
4. N. Chigira, N. Iiyori and H. Yamaki, Non abelian Sylow subgroups of finite groups of even order, in preparation.
5. N. Iiyori, Sharp characters and prime graphs of finite groups, J. Algebra 163 (1994) 1–8.
6. N. Iiyori, A conjecture of Frobenius and the simple groups of Lie type IV, J. Algebra 154 (1993) 188–214.
7. N. Iiyori and H. Yamaki, On a conjecture of Frobenius, Bull. Amer. Math. Soc., 25 (1991) 413–416.
8. N. Iiyori and H. Yamaki, A conjecture of Frobenius and the simple groups of Lie type III, J. Algebra 145 (1992) 329–332.
9. N. Iiyori and H. Yamaki, Prime graph components of the simple groups of Lie type over the fields of even characteristic, J. Algebra, 155 (1993) 335–343. Corrigenda, 181 (1996) 659.
10. N. Iiyori and H. Yamaki, A conjecture of Frobenius, Sugaku Expositions, Amer. Math. Soc. 9 (1996) 69–85.
11. A. S. Kondrat'ev, Prime graph components of finite simple groups, Math. USSR Sbornik 67 (1990) 235–247.
12. M. Suzuki, Investigations on finite groups, Proc. Nat. Sci. Acad. Sci. U.S.A. 46 (1960) 1611-1614.
13. J. S. Williams, Prime graph components of finite groups, J. Algebra 69 (1981) 487–513.
14. H. Yamaki, A characterization of the Suzuki simple groups of order 448,345,497,600, J. Algebra 40 (1976) 229–244.
15. H. Yamaki, A conjecture of Frobenius and the sporadic simple groups I, Comm. Algebra 11 (1983) 2513–2518; II. Math. Comp. 46 (1986) 609–611; Supplement. Math. Comp. 46 (1986) S43–S46.
16. H. Yamaki, A conjecture of Frobenius and the simple groups of Lie type I, Arch. Math., 42 (1984) 344–347; II. J. Algebra 96 (1985) 391–396.

Naoki Chigira
Department of Mathematical Sciences,
Muroran Institute of Technology,
Hokkaido 050, Japan
E-mail: chigira@muroran-it.ac.jp

Nobuo Iiyori
Department of Mathematics,
Yamaguchi University,
Yamaguchi 753, Japan
E-mail: iiyori@po.yb.cc.yamaguchi-u.ac.jp

Hiroyoshi Yamaki
Department of Mathematics,
Kumamoto University,
Kumamoto 860, Japan
E-mail: yamaki@gpo.kumamoto-u.ac.jp

Some Formulas for Spin Models on Distance-Regular Graphs

Brian Curtin and Kazumasa Nomura

Abstract. A spin model is a square matrix W satisfying certain conditions which ensure that it yields an invariant of knots and links via a statistical mechanical construction of Jones [11], By a recent result by Jaeger-Matsumoto-Nomura [10], for every spin model W, there corresponds a Bose-Mesner algebra $N(W)$ which contains W. Here we consider the case that $N(W)$ is the Bose-Mesner algebra of a distance-regular graph. Actually we will assume $W \in \mathcal{A} \subseteq N(W)$, where $\mathcal{A}$ is the Bose-Mesner algebra of a distance-regular graph Γ. Under this assumption, we will show that the following numbers can be represented by two parameters: the entries of W, the eigenvalues of the graph Γ, and the intersection numbers of Γ.

Set $X = \{1, \ldots, n\}$ throughout.

1. Preliminaries

1.1. Spin Models

Definition (Jones [11]). A *spin model* is an $n \times n$ matrix W with non-zero complex entries such that (for all a, b, $c \in X$):

$$(1) \qquad \sum_{x \in X} \frac{W(x,a)}{W(x,b)} = 0 \qquad \text{if } a \neq b.$$

$$(2) \qquad \frac{1}{\sqrt{n}} \sum_{x \in X} \frac{W(x,a)W(x,b)}{W(x,c)} = \frac{W(a,b)}{W(a,c)W(c,b)}.$$

Remark. One obtains an invariant of knots (links) from each spin model.

Remark. Equation (2) with $b = c$ implies

$$\frac{1}{\sqrt{n}} \sum_{x \in X} W(x,a) = \frac{1}{W(b,b)}.$$

So $W(b,b) = \alpha$ is a costant, called the *modulus* of W.

Remark. Jones assumed that W is symmetric. The above definition was obtained by Kawagoe-Munemasa-Watatani [12]. A further generalization (called 4-weight spin models) was obtained by Bannai-Bannai [1].

1.2. Association Schemes and Bose-Mesner Algebras

For more precise information about association schemes, the reader is referred to [3].

A *d-class association scheme* on X is a partition

$$X \times X = R_0 \cup R_1 \cup \cdots \cup R_d, \qquad R_i \neq \emptyset$$

such that

(1) $R_0 = \{(x,x) \mid x \in X\}$,

(2) For every $i \in \{0,\ldots,d\}$, there exists $i' \in \{0,\ldots,d\}$ such that $R_{i'} = \{(y,x) \mid (x,y) \in R_i\}$,

(3) There exists integers p_{ij}^{ℓ} $(i,\ j,\ k \in \{0,\ldots,d\})$ such that, for every $(x,y) \in R_\ell$,

$$p_{ij}^{\ell} = \#\{z \in X \mid (x,z) \in R_i, \quad (z,y) \in R_j\},$$

(4) $p_{ij}^{\ell} = p_{ji}^{\ell}$.

p_{ij}^{ℓ} are called the *intersection numbers.*

An association scheme $R_0, \ldots, R_d$ is *symmetric* if every R_i is a symmetric relation (i.e. $i' = i$ for every i).

Let $R_0, R_1, \ldots, R_d$ be an association scheme on X. Let A_i be the adjacency matrix of R_i;

$$A_i(x,y) = \begin{cases} 1 & \text{if } (x,y) \in R_i \\ 0 & \text{otherwise.} \end{cases}$$

Observe that

$$A_iA_j = A_jA_i = \sum_{\ell=0}^{d} p_{ij}^{\ell} A_k.$$

Hence the linear span $\mathcal{A} = \langle A_0, A_1, \ldots, A_d \rangle$ is a commutative subalgebra of $M_n(\mathbb{C})$, with identity $A_0 = I$. $\mathcal{A}$ is called the *Bose-Mesner algebra* of the association scheme.

Let $E_0,\ E_1,\ \ldots,\ E_d$ be the primitive idempotents of $\mathcal{A}$. Then $E_iE_j = \delta_{ij}E_i$ for i, $j = 0,\ldots,d$. We have $J \in \mathcal{A}$ (all one's matrix), since $J = \sum_{i=0}^{d} A_i$. Hence $n^{-1}J$ is a primitive idempotent of $\mathcal{A}$. We always choose notation so that $E_0 = n^{-1}J$.

Now we have two linear basis of $\mathcal{A}$: $A_0 = I,\ A_1,\ \ldots,\ A_d$ (adjacency matrices), $E_0 = n^{-1}J,\ E_1,\ \ldots,\ E_d$ (primitive idempotents).

Write

$$A_i = \sum_{j=0}^{d} P_{ji}E_j, \qquad E_i = n^{-1}\sum_{j=0}^{d} Q_{ji}A_j.$$

The matrices (of size $d+1$) $P = (P_{ji})$ and $Q = (Q_{ji})$ are called the **eigenmatrices** of $\mathcal{A}$.

$V = \mathbf{C}^n$ splits into direct sum

$$V = E_0V \oplus E_1V \oplus \cdots \oplus E_dV,$$

and $E_j : V \longrightarrow E_jV$ is the projection. Observe that P_{ji} is the eigenvalue of A_i on the eigenspace E_jV. Clearly we have $A_iE_j = P_{ji}E_j$ $(i, j = 0, \ldots, d)$.

The entries Q_{ji} of Q are called the *dual eigenvalues.*

$\mathcal{A}$ is closed under Hadamard product $A \circ B$, since $A_i \circ A_j = \delta_{ij}A_i$. Thus $\mathcal{A}$ becomes an algebra under Hadamard product, with identity J.

A *duality* of $\mathcal{A}$ is a linear bijection $\Psi : \mathcal{A} \longrightarrow \mathcal{A}$ which satisfies (for all A, $B \in \mathcal{A}$)

$$\Psi(AB) = \Psi(A) \circ \Psi(B), \quad \Psi(A \circ B) = n^{-1}\Psi(A)\Psi(B), \quad \Psi(\Psi(A)) = n\,{}^tA.$$

When $\mathcal{A}$ has a duality, $\mathcal{A}$ is said to be *self-dual.*

A duality Ψ maps $\{E_i \,|\, i = 0, \ldots, d\}$ onto $\{A_i \,|\, i = 0, \ldots, d\}$. We may choose the ordering of $E_0, \ldots, E_d$ so that $\Psi(E_i) = A_i$ $(i = 0, \ldots, d)$. In this case the eigenmatrices satisfy $P = \overline{Q}$.

1.3. Algebra N(W)

Let W be a spin model on X. For b, c in X, let Y_{bc} be a vector $\in \mathbf{C}^n$ with entries

$$Y_{bc}(x) = \frac{W(x,a)}{W(x,b)} \qquad (x \in X).$$

Let $N(W)$ be the set of matrices $A \in M_n(\mathbf{C})$ such that Y_{bc} is an eigenvector of A for all b, $c \in X$. Define a mapping $\Psi : N(W) \longrightarrow M_n(\mathbf{C})$ by

$$AY_{bc} = \Psi(A)(b,c)Y_{bc} \qquad (A \in N(W),\ b, c \in X).$$

Theorem A (Jaeger-Matsumoto-Nomura [10]).

(i) $N(W)$ *is a Bose-Mesner algebra.*

(ii) $W \in N(W)$.

(iii) $N(W)$ *is self-dual with duality* Ψ.

(iv) $\Psi(A) = \alpha^{-1}W \circ ({}^tW^-({}^tW \circ A))$ *for all* $A \in N(W)$, *where* α *denotes the modulus of* W *and* W^- *is defined by* $W^-(x,y) = W(y,x)^{-1}$.

Let $R_0, \ldots, R_d$ be an association scheme with the corresponding Bose-Mesner algebra $\mathcal{A}$ such that $W \in \mathcal{A} \subseteq N(W)$. Since $W \in \mathcal{A}$, W is a linear combination of the adjacency matrices A_i of $\mathcal{A}$; $W = \sum_{i=0}^{d} t_i A_i$. By the definition of W^-, $W^- = \sum_{i=0}^{d} t_i^{-1} A_i \in \mathcal{A}$.

Lemma B. $\Psi(\mathcal{A}) = \mathcal{A}$. *In particular, $\mathcal{A}$ is self-dual with duality $\Psi|_{\mathcal{A}}$.*

Proof. We have W, $W^- \in \mathcal{A}$. Observe that $\mathcal{A}$ is closed under matrix product, Hadamard product and trasposing operation. Hence, for all $A \in \mathcal{A}$,

$$\Psi(A) = \alpha^{-1} W \circ ({}^tW^-({}^tW \circ A))$$

belongs to $\mathcal{A}$. This shows $\Psi(\mathcal{A}) \subseteq \mathcal{A}$. □

Let $E_0, \ldots, E_d$ be the primitive idempotents of $\mathcal{A}$, where we choose the ordering so that $\Psi(E_h) = A_h$ $(h = 0, \ldots, d)$. Then, for $(b, c) \in R_h$,

$$E_h Y_{bc} = \Psi(E_j)(b,c) Y_{bc} = A_h(b,c) Y_{bc} = Y_{bc}.$$

Lemma C. *For all b, $c \in X$, $A_i Y_{bc} = P_{hi} Y_{bc}$ $(i = 0, \ldots, d)$, where h is the index such that $(b,c) \in R_h$.*

Proof. From the above, we have $E_h Y_{bc} = E_h$. Hence $A_i Y_{bc} = A_i E_h Y_{bc}$. Using $A_i E_h = P_{hi} E_h$, $A_i E_h Y_{bc} = P_{hi} E_h Y_{bc}$. Using $E_h Y_{bc} = Y_{bc}$ again, we obtain the result. □ Status: RO

1.4. Distance-Regular Graph

For more precise information about distance-regular graphs will be found in [4].

Let $\Gamma = (X, E)$ be a connected graph of diameter d (undirected, without loops and multiple edges). Γ is *distance-regular* if the relations

$$R_i = \{(x,y) \mid \partial(x,y) = i\} \qquad (i = 0, \ldots, d)$$

form a (symmetric) association scheme.

It is known that the intersection numbers p^{ℓ}_{ij} are determined by the numbers $c_i = p^i_{1,i-1}$, $a_i = p^i_{1,i}$, and $b_i = p^i_{1,i+1}$. Clearly $b_0 = k$ is the valency and $c_i + a_i + b_i = k$, $c_0 = a_0 = 0$, $c_1 = 1$, $b_d = 0$. The *intersection array* of Γ is

$$\{b_0, b_1, \ldots, b_{d-1};\ c_1, c_2, \ldots, c_d\}.$$

Let Γ be a distance-regular graph of diameter d, and let $\mathcal{A}$ be the corresponding Bose-Mesner algebra. Let A_i be the adjecency matrices, E_i be the primitive idempotents, and P, Q the eigenmatrices. Observe A_i are symmetric, so that all matrices in $\mathcal{A}$ are symmetric. Thus the eigenvalue P_{ji} of A_i on E_jV are real numbers. This implies Q is also a real matrix. The eigenvalues $\theta_j = P_{j1}$ of A_1 on E_jV is called the *eigenvalues of* Γ.

It is known (and not difficult to show) that there exist polynomials $v_i(x)$ $(i = 0, \ldots, d)$ of degree i such that $A_i = v_i(A_1)$. This implies

$$P_{ji} = v_i(\theta_j) \qquad (i, j = 0, \ldots, d).$$

This property is called the *P-polynomiality.*

The *dual eigenvalues* of Γ are defined by

$$\theta_j^* = Q_{j1} \qquad (j = 0, \ldots, d).$$

Γ is *Q-polynomial* if there exist polynomials $v_i^*(x)$ $(i = 0, \ldots, d)$ of degree i such that

$$Q_{ji} = v_i^*(\theta_j^*) \qquad (i, j = 0, \ldots, d).$$

Now suppose that the Bose-Mesner algebra $\mathcal{A}$ of Γ is self-dual. In this case, we have $P = Q$. Hence Γ is necessarily Q-polynomial with $\theta_i = \theta_i^*$.

We will use the well-known reccurence:

$$\theta_1\theta_i = c_i\theta_{i-1} + a_i\theta_i + b_i\theta_{i+1}.$$

Writing $a_i = \theta_0 - b_i - c_i$, this becomes

$$(\theta_1 - \theta_0)\theta_i = c_i(\theta_{i-1} - \theta_i) + b_i(\theta_{i+1} - \theta_i).$$

2. Result and Proof

Theorem 1 *Let $\Gamma = (X, R)$ be a distance-regular graph of diameter $d \geq 2$ with intersection numbers c_i, b_i $(0 \leq i \leq d)$. Let A_0, A_1, $\ldots$, A_d denote the adjacency matrices and let $\mathcal{A}$ denote the Bose-Mesner algebra of Γ. Let W be a spin model such that $W \in \mathcal{A} \subseteq N(W)$. Write $W = \sum_{i=0}^{d} t_i A_i$, and set $x_i = t_i t_{i-1}^{-1}$ $(1 \leq i \leq d)$, $x = x_1$, and $p = x_1^{-1}x_2$.*

(i) $x_i = p^{i-1}x$ $(1 \leq i \leq d)$.

(ii) *Suppose $x^2 \neq 1$. Then the intersection numbers c_i $(0 < i \leq d)$ and b_i $(0 \leq i < d)$ of Γ are given by*

$$\begin{aligned} c_i &= \frac{p^{i-1}(x-1)(px^2-1)(p^{d-i}x+1)(p^{d+i-1}x^2-1)}{(p^{d-1}x+1)(p^dx^2-1)(p^{i-1}x-1)(p^{2i-1}x^2-1)} \begin{bmatrix} i \\ 1 \end{bmatrix}_p, \\ b_i &= \frac{p^i(1-x)(px^2-1)(p^{i-1}x^2-1)(p^{d+i-1}x^3+1)}{x(p^{d-1}x+1)(p^dx^2-1)(p^ix-1)(p^{2i-1}x^2-1)} \begin{bmatrix} d-i \\ 1 \end{bmatrix}_p, \end{aligned}$$

where

$$\begin{bmatrix} i \\ 1 \end{bmatrix}_p = \begin{cases} i & \text{if } p = 1, \\ \frac{p^i-1}{p-1} & \text{otherwise.} \end{cases}$$

Lemma 1 *For all b, $c \in X$*

$$AY_{bc} = \theta_h Y_{bc}, \tag{1}$$

where $h = \partial(b, c)$.

Proof. Observe that Y_{bc} is an eigenvector of each E_j, so $E_j Y_{bc} = \Psi(E_j)(bc)\, Y_{bc} = A_j(bc) Y_{bc} = \delta_{hj} Y_{bc}$. Thus $AY_{bc} = AE_h Y_{bc} = \theta_h Y_{bc}$. □

For all vertices u and v, write

$$\mathrm{D}^i_j(u,v) = \Gamma_i(u) \cap \Gamma_j(v).$$

For any vertex x and any subset $Z \subseteq X$, write

$$e(x,\ Z) = |\Gamma_1(x) \cap Z|.$$

Observe that $e(x,\ Z)$ is just the number of edges from x into Z.

Lemma 2 *Fix u, $v \in X$, and write $h = \partial(u, v)$. For all i, j $(0 \le i, j \le D)$ write $\mathrm{D}^i_j = \mathrm{D}^i_j(u,v)$. Then for all r, s $(0 \le r, s \le D)$ and for all $w \in \mathrm{D}^r_s$,*

$$\sum_{i=r-1}^{r+1} \sum_{j=s-1}^{s+1} e(w, \mathrm{D}^i_j) t_i t_j^{-1} = \theta_h t_r t_s^{-1}, \tag{2}$$

$$\sum_{i=r-1}^{r+1} \sum_{j=s-1}^{s+1} e(w, \mathrm{D}^i_j) t_j t_i^{-1} = \theta_h t_s t_r^{-1}. \tag{3}$$

Proof. We compute the w-entry of each side of (1): $AY_{bc} = \theta_h Y_{bc}$. On one hand,

$$\begin{aligned}
(AY_{uv})(w) &= \sum_{x \in X} A(w,x) Y_{uv}(x) \\
&= \sum_{x \in \Gamma_1(w)} Y_{uv}(x) \\
&= \sum_{i=0}^{D} \sum_{j=0}^{D} \sum_{x \in \mathrm{D}^i_j \cap \Gamma_1(w)} \frac{W(u,x)}{W(v,x)} \\
&= \sum_{i=0}^{D} \sum_{j=0}^{D} \sum_{x \in \mathrm{D}^i_j \cap \Gamma_1(w)} t_i t_j^{-1} \\
&= \sum_{i=0}^{D} \sum_{j=0}^{D} e(w, \mathrm{D}^i_j) t_i t_j^{-1} \\
&= \sum_{i=r-1}^{r+1} \sum_{j=s-1}^{s+1} e(w, \mathrm{D}^i_j) t_i t_j^{-1}.
\end{aligned}$$

On the other hand, the w-entry of the right side of (1) is $\theta_h t_r t_s^{-1}$. Hence (2) holds. Equation (3) is proved similarly using Y_{vu} in place of Y_{uv}. □

Set

$$x_i = t_i t_{i-1}^{-1} \qquad (1 \le i \le D).$$

Lemma 3 *For all r $(1 \le r \le D)$,*

$$\begin{aligned} x_1\theta_r &= c_r x_r^{-1} + a_r + b_r x_{r+1}, & (4)\\ x_1^{-1}\theta_r &= c_r x_r + a_r + b_r x_{r+1}^{-1}, & (5) \end{aligned}$$

where x_{D+1} is an indeterminant.

Proof. Apply Lemma 2 with $w = v$ and simplify. □

Lemma 4 *For all r $(1 \le r \le D)$,*

$$\frac{x_r - x_r^{-1}}{\theta_{r-1} - \theta_r} = \frac{x_1 - x_1^{-1}}{\theta_0 - \theta_1}.$$

Proof. Use Lemma 3 and the 3-term recurrence. □

Corollary 2 *With the above notation*

1. *If $x_r^2 = 1$ for some r $(1 \le r \le D)$, then $x_i^2 = 1$ for all $i \in \{1, \ldots, D\}$.*
2. *If $x_r x_{r+1} = 1$ for some r $(1 \le r \le D-1)$, then $x_i^2 = 1$ for all $i \in \{1, \ldots, D\}$.*

Proof. Use Lemma 4 and the fact that the eigenvalues are distinct. □

Fix r $(1 \le r \le D)$, and pick vertices x, y, z such that $\partial(x,y) = r-1$, $\partial(x,z) = r$, $\partial(y,z) = 1$. Write

$$\gamma = |\Gamma_{r-1}(x) \cap \Gamma_1(y) \cap \Gamma_1(z)|.$$

Fact: γ depends only upon r, not the choice of vertices x, y, z. We will thus sometimes write γ_r for this number.

Lemma 5 *Fix r $(1 \le r \le D)$, and pick vertices x, y, z such that $\partial(x,y) = r-1$, $\partial(x,z) = r$, $\partial(y,z) = 1$. Write*

$$\gamma = |\Gamma_{r-1}(x) \cap \Gamma_1(y) \cap \Gamma_1(z)|.$$

Then

$$\gamma(x_2-1)(x_r-1) = x_1\theta_{r-1} - x_2\theta_r + x_r(x_1x_2-1) + a_1x_r(x_2-1), \qquad (6)$$

$$\gamma x_1(x_2-1)(x_r-1) = x_2x_r\theta_{r-1} - x_1x_r\theta_r + 1 - x_1x_2 + a_1x_1(1-x_2), \qquad (7)$$

$$\gamma x_1(x_2-1)(x_r-1) = x_2\theta_r - x_1\theta_{r-1} + x_r(1-x_1x_2) + a_1x_1(1-x_2), \qquad (8)$$

$$\gamma(x_2-1)(x_r-1) = x_1x_r\theta_r - x_2x_r\theta_{r-1} + x_1x_2 - 1 + a_1x_r(x_2-1), \qquad (9)$$

$$\gamma(x_1+1)(x_2-1)(x_r-1) = a_1(x_2-1)(x_r-x_1), \qquad (10)$$

$$\theta_r(x_2+x_1x_r) - \theta_{r-1}(x_1+x_2x_r) = (x_1x_2-1)(x_r-1). \qquad (11)$$

Proof.

Proof of (6): we apply Lemma 2 with $u = x$, $v = z$, $w = y$, and $h = r$.

$$\begin{aligned}\gamma(x_2-1)(x_r-1) &= x_1\theta_{r-1} - x_2\theta_r \\ &\quad + x_r(x_1x_2-1) + a_1x_r(x_2-1).\end{aligned}$$

Take $u = x$, $v = z$, $w = y$, and $h = r$ in Lemma 2, and set $\mathrm{D}^i_j = \mathrm{D}^i_j(x,z)$, and observe that $y \in \mathrm{D}^{r-1}_1$. Now $e(y, \mathrm{D}^i_j)$ is zero except for

$j\backslash i$	$r-2$	$r-1$	r
2	c_{r-1}	$a_{r-1}-\gamma$	$b_{r-1}-1-(a_1-\gamma)$
1		γ	$a_1-\gamma$
0			1

Therefore (2) implies that

$$\begin{aligned}\theta_r t_{r-1}t_1^{-1} &= c_{r-1}t_{r-2}t_2^{-1} + (a_{r-1}-\gamma)t_{r-1}t_2^{-1} \\ &\quad + (b_{r-1}-1-a_1+\gamma)t_rt_2^{-1} \\ &\quad + (a_1-\gamma)t_rt_1^{-1} + \gamma t_{r-1}t_1^{-1} + t_rt_0^{-1}.\end{aligned}$$

Multiplying both sides by $t_2t_{r-1}^{-1}$, this becomes

$$\begin{aligned}x_2\theta_r &= -\gamma(x_2-1)(x_r-1) \\ &\quad + (c_{r-1}x_{r-1}^{-1} + a_{r-1} + b_{r-1}x_r) \\ &\quad + x_r(x_1x_2-1) + a_1x_r(x_2-1).\end{aligned}$$

By (4) $c_{r-1}x_{r-1}^{-1} + a_{r-1} + b_{r-1}x_r = x_1\theta_{r-1}$. This substitution yields (6).

(7) is obtained in a similar way.

To prove (8) and (9), apply Lemma 2 with $u = x$, $v = y$, $w = z$, $h = r-1$.

(10) is obtained by adding (7) and (8), and (11) is obtained by subtracting (6) from (8). □

* This is enough to treat the case $p^2 = 1$, where $p = x_2/x_1$.

1. If $p = 1$, then $x_i = 1$ for all i.

2. If $p = 1$, $x \neq 1$, then $c_i = i$, $a_i = i(q-2)$, $b_i = (d-i)(q-1)$, where $q = -x^{-1}(x-1)^2$.

3. If $p = -1$, then $x^2 = 1$ and $x_i = (-1)^{i-1}x$.

4. if $p = -1$ and $a_1 = 0$, then $c_i = i$ $(1 \le i \le d)$, $b_i = d - i$ $(0 \le i \le d-1)$, $a_i = 0$ $(0 \le i \le d-1)$.

* This is enough to treat the case $p^2 \neq 1$, $a_1 = 0$.

1. $x_i = p^{i-1}x, \qquad \theta_i = \dfrac{(px^2-1)(p^{2i-1}x^2+1)}{p^{i-1}x^2(p^2-1)}.$

   (intermediate computations)

2. Either $p^{d-1}x^2+1=0$ or $p^dx-1=0$.

3. If $p^{d-1}x^2+1=0$, then

$$\begin{aligned}
\theta_i &= \frac{(p^d+p^2)(p^d-p^{2i})}{p^{d+i}(p^2-1)} \qquad (0 \le i \le d),\\
c_i &= \frac{(p^d+p^2)(p^{2i}-1)}{(p^2-1)(p^{2i}+p^d)} \qquad (0 \le i \le d),\\
b_i &= \frac{(p^d+p^2)(p^{2d}-p^{2i})}{p^d(p^2-1)(p^d+p^{2i})} \qquad (0 \le i \le d).
\end{aligned}$$

4. If $p^dx-1=0$, then

$$\begin{aligned}
\theta_i &= \frac{(1-p^{2d-1})(p^{2i-2d-1}+1)}{p^{i-2}(p^2-1)} \qquad (0 \le i \le d),\\
c_i &= \frac{(p^{2d-1}-1)(p^{2i}-1)}{p^{2d-1}(p^2-1)(p^{2i-2d-1}-1)} \qquad (0 \le i \le d),\\
b_i &= \frac{p^2(p^{2i-4d-2}-1)(1-p^{2d-1})}{(p^2-1)(p^{2i-2d-1}-1)} \qquad (0 \le i < d).
\end{aligned}$$

5. $a_i = 0$ $(0 \le i \le d-1)$.

The numbers γ_r are closely related to the the *kite-numbers* of Terwilliger. Define $e_i(x,y,z)$ $(1 \le i \le d)$ defined for each triple x, y, and z of mutually adjacent vertices by

$$e_i(x,y,z) = |D^i_{i-1}(x,y)|^{-1}|D^i_{i-1}(x,y) \cap \Gamma_{i-1}(z)|.$$

Lemma 6 *For all triples x, y, z of mutually adjacent vertices, $\gamma_i = a_1e_i(x,y,z)$ $(2 \le i \le d)$.*

Proof. Fix two adjacent vertices x ,y, and set $D^i_j = D^i_j(x,y)$. Count the number of pairs (z,u) such that $z \in D^1_1$, $u \in D^i_{i-1}$, and $\partial(u,z) = i-1$ in two ways. □

The following result by Terwilliger is essential.

Theorem 3 *(Terwilliger [18]). Let $\Gamma = (X,R)$ be a Q-polynomial distance-regular graph of diameter d, and let θ^*_0, θ^*_1, $\ldots$, θ^*_d denote the dual eigenvalues of Γ with respect* *to a Q-polynomial ordering of the primitive idempotents. Let x, y, z be mutually adjacent vertices. Then*

$$e_i(x,y,z) = \alpha_i e_2(x,y,z) + \beta_i \qquad (2 \le i \le d),$$

where

$$\begin{aligned} \alpha_i &= \frac{(\theta_1^* - \theta_2^*)(\theta_0^* + \theta_1^* - \theta_{i-1}^* - \theta_i^*)}{(\theta_0^* - \theta_2^*)(\theta_{i-1}^* - \theta_i^*)}, \\ \beta_i &= \frac{(\theta_0^* - \theta_1^*)(\theta_2^* - \theta_i^*) - (\theta_1^* - \theta_2^*)(\theta_1^* - \theta_{i-1}^*)}{(\theta_0^* - \theta_2^*)(\theta_{i-1}^* - \theta_i^*)}. \end{aligned}$$

Fact: The distance-regular graphs such that there is a spin model $W \in \mathcal{A} \subseteq N(W)$ are Q-polynomial, and there is a Q-polynomial ordering of their primitive idempotents such that $\theta_i^* = \theta_i$ $(0 \le i \le D)$.

Lemma 7 *Suppose $p^2 \neq 1$. Then*

$$\gamma_i = \alpha_i \gamma_2 + \beta_i a_1 \qquad (2 \le i \le d).$$

Set

$$\rho_i = x_i - x_i^{-1} \qquad (1 \le i \le d).$$

Lemma 8 *Suppose $p^2 \neq 1$. Then for all i $(2 \le i \le d)$*

$$\begin{aligned} &(\rho_i \gamma_i - \rho_{i-1}\gamma_{i-1})(\rho_1 + \rho_2) \\ &= \rho_2(\rho_i + \rho_{i-1})\gamma_2 + (\rho_1\rho_i - \rho_2\rho_{i-1})a_1. \end{aligned}$$

* This is enough to treat the case $p^2 \neq 1$, $a_1 \neq 1$.

1. $x_i = px^{i-1}$.
2. Compute θ_i $(0 \le i \le d)$ (a long computation): $(px^2-1)\times$
$$\frac{\left((p^{d+i-1}x^3+1)(p^{d-i}-1) + p^{d-i}x(p^{i-1}x+1)(p^i-1)\right)}{x(p^{d-1}x+1)(1-p^dx^2)(p-1)}.$$
3. Compute b_i $(1 \le i < d)$ (now fairly easy):
$$\frac{p^i(1-x)(px^2-1)(p^{i-1}x^2-1)(p^{d+i-1}x^3+1)(p^{d-i}-1)}{x(p^{d-1}x+1)(p^dx^2-1)(p^ix-1)(p^{2i-1}x^2-1)(p-1)}.$$
4. Compute c_i $(1 \le i \le d)$ (now fairly easy):
$$\frac{p^{i-1}(x-1)(px^2-1)(p^{d-i}x+1)(p^{d+i-1}x^2-1)(p^i-1)}{(p^{d-1}x+1)(p^dx^2-1)(p^{i-1}x-1)(p^{2i-1}x^2-1)(p-1)}.$$

References

[1] E. Bannai and Et. Bannai, Generalized generalized spin models (four-weight spin models), *Pacific J. Math.* 170 (1995), 1–16.

[2] E. Bannai, Et. Bannai and F. Jaeger, On spin models, modular invariance, and duality, *J. Algebraic Combin.*, to appear.

[3] E. Bannai and T. Ito, "Algebraic Combinatorics I," Benjamin/Cummings, Menlo Park, 1984.

[4] A.E. Brouwer, A.M. Cohen and A. Neumaier, "Distance-Regular Graphs," Springer, New York, 1989.

[5] B. Curtin, 2-homogeneous bipartite distance-regular graphs, *preprint.*

[6] F. Jaeger, Strongly regular graphs and spin models for the Kauffman polynomial, *Geom. Dedicata* 44 (1992), 23–52.

[7] F. Jaeger, On spin models, triply regular association schemes, and duality, *J. Algebraic Combin.* 4 (1995), 103–144.

[8] F. Jaeger, Towards a classification of spin models in terms of association schemes, *Advanced Studies in Pure Math.* 24 (1996), 197–225.

[9] F. Jaeger, New constructions of models for link invariants, *Pacific J. Math.*, to appear.

[10] F. Jaeger, M. Matsumoto and K. Nomura, Bose-Mesner algebras related to type II matrices and spin models, *J. Alg. Combin.*, to appear.

[11] V. F. R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* 137 (1989), 311–224.

[12] K. Kawagoe, A. Munemasa and Y. Watatani, Generalized spin models, *J. Knot Theory Ramifications* 3 (1995), 465–475.

[13] K. Nomura, Spin models constructed from Hadamard matrices, *J. Combin. Theory Ser. A* 68 (1994), 251-261.

[14] K. Nomura, Spin models on bipartite distance-regular graphs, *J. Combin. Theory Ser. B* 64 (1995), 300–313.

[15] K. Nomura, Spin models on triangle-free connected graphs, *J. Combin. Theory Ser. B* 67 (1996), 284–295.

[16] K. Nomura, Spin models and almost bipartite 2-homogeneous graphs, *Advanced Studies in Pure Math.* 24 (1996), 285–308.

[17] K. Nomura, An algebra associated with a spin model, *J. Alg. Combin.* 6 (1997), 53–58.

[18] P. Terwilliger, Kite-free distance-regular graphs, *Europ. J. Combin.* 16 (1995), 405–414.

ORDERS OF FINITE LINEAR GROUPS

WALTER FEIT

Department of Mathematics
Yale University
New Haven, CT 06520-8283

By using the classification of the finite simple groups, Weisfeiler [W] found bounds for the orders of finite primitive subgroups of PGL$(n, \mathbf{C})$ that are far better than any previously known, and indeed than any bounds which have been achieved without this classification.

As a consequence of his results it is possible to give precise upper bounds for the orders of the finite subgroups of GL$(n, \mathbf{Q})$, and more generally for the finite subgroups of GL(n, K), where K is a cyclotomic field. The object of this paper is to prove Theorems A and B below which describe these bounds.

If ℓ is an even natural number let $\mathbf{Q}(\ell)$ be the cyclotomic field which contains exactly ℓ roots of 1. Hence $\ell = 2$ if and only if $\mathbf{Q}(\ell) = \mathbf{Q}$.

For any field K of characteristic 0 let $M(n, K)$ denote the group of all monomial matrices whose nonzero entries are roots of 1 in K. Let $M(n, \mathbf{Q}(\ell)) = M(n, \ell)$. Thus if K contains exactly ℓ roots of 1 then $M(n, K) = M(n, \ell)$ and $|M(n, \ell)| = n!\ell^n$.

Let ST_i denote the unitary reflection group numbered i in [ST, Table VII]. Then $ST_{31} = Z_4 2^4 \Sigma_6$. John Conway has pointed out that it is the centralizer in $W(E_8)$ of an element of order 4.

$ST_{32} = Sp(4, 3) \times Z_3$ is the centralizer in $W(E_8)$ of an element of order 6.

$ST_{34} = 6PSU(4, 3)2$.

Two finite subgroups G and H of $GL(n, \mathbf{C})$ are *isoclinic over* $\mathbf{C}$ if there is a bijection from G to H which sends each coset of $\mathbf{Z}(G)$ onto a coset of $\mathbf{Z}(H)$ and defines an isomorphism from $G/\mathbf{Z}(G)$ to $H/\mathbf{Z}(H)$ such that every element of H is a scalar multiple of the corresponding element of G.

Two finite groups G and H are *isoclinic* if they can be embedded in a larger group M such that M is generated by G and $\mathbf{Z}(M)$, and also by H and $\mathbf{Z}(M)$. See the ATLAS p. xxiii for a discussion of this concept and the following consequence.

Suppose that G and H are isoclinic. If $g : G \to GL(n, \mathbf{C})$ is a faithful irreducible representation of G, then there exists a faithful irreducible representation
$h : H \to GL(n, \mathbf{C})$ such that $g(G)$ and $h(H)$ are isoclinic over $\mathbf{C}$.

The finite primitive subgroups of GL$(n, \mathbf{C})$ for $n \leq 7$ have been classified up to isoclinism by H.F. Blichfeldt, R. Brauer, J.H. Lindsey II and D. Wales, see e.g. [F1] for the list of groups, (though John Conway has pointed out that unfortunately the group ST_{31} was omitted from the list of 4 dimensional primitive groups). These lists and Weisfeiler's results are essential for the work in this paper.

Theorem A. *A finite subgroup of $GL(n, \mathbb{Q})$ of maximum order is conjugate to $M(n, \mathbb{Q})$, and so has order $n!2^n$, except in the following cases.*

n	G	$\|G\|$
2	$W(G_2)$	$2^2 \cdot 3 = 12$
4	$W(F_4)$	$2^7 \cdot 3^2 = 1152$
6	$W(E_6) \times Z_2$	$2^8 \cdot 3^4 \cdot 5 = 103680$
7	$W(E_7)$	$2^{10} \cdot 3^4 \cdot 5 \cdot 7 = 2903040$
8	$W(E_8)$	$2^{14} \cdot 3^5 \cdot 5^2 \cdot 7 = 696729600$
9	$W(E_8) \times W(A_1)$, *reducible*	$2^{15} \cdot 3^5 \cdot 5^2 \cdot 7 = 1393459200$
10	$W(E_8) \times W(G_2)$, *reducible*	$2^{16} \cdot 3^6 \cdot 5^2 \cdot 7 = 8360755200$

Since $M(n, \mathbb{Q}) = W(B_n) = W(C_n)$, the maximum order is achieved by a Weyl group unless $n = 6$. In any case it is achieved by the automorphism group of a disjoint union of Dynkin diagrams. In all cases the finite subgroup of maximum order in $GL(n, \mathbb{Q})$ is unique up to conjugacy.

It should be noted that while every finite subgroup of $GL(n, \mathbb{Q})$ is conjugate to a subgroup of $GL(n, \mathbb{Z})$, uniqueness up to conjugacy in $GL(n, \mathbb{Z})$ need not hold in Theorem A. For instance, as B_n and C_n are inequivalent roots systems for $n > 2$, the descriptions of $W(B_n)$ and $W(C_n)$ in terms of these root systems lead to non-conjugate subgroups of $GL(n, \mathbb{Z})$.

Theorem B. *Let $\ell > 2$ be an even integer. $M(n, \ell)$ is a finite subgroup of $GL(n, \mathbb{Q}(\ell))$ of maximum order except in the following cases where the maximum order is achieved by the listed group.*

ℓ	n	G	$\|G\|$
4	2	$Z_4SL(2,3)$	$2^4 \cdot 3 = 48$
4	4	ST_{31}	$2^{10} \cdot 3^2 \cdot 5 = 46080$
4	5	$ST_{31} \times Z_4$, *reducible*	$2^{12} \cdot 3^2 \cdot 5 = 184320$
4	8	$ST_{31} wr Z_2$	$2^{21} \cdot 3^4 \cdot 5^2 = 4246732800$
6	4	ST_{32}	$2^7 \cdot 3^5 \cdot 5 = 155520$
6	6	ST_{34}	$2^9 \cdot 3^7 \cdot 5 \cdot 7 = 39191040$
8	2	$Z_8GL(2,3)$,	$2^6 \cdot 3 = 192$
10	2	$Z_5 \times SL(2,5)$	$2^3 \cdot 3 \cdot 5^2 = 600$
10	4	$(Z_5 \times SL(2,5)) wr Z_2$	$2^7 \cdot 3^2 \cdot 5^4 = 720000$
10	6	$(Z_5 \times SL(2,5)) wr \Sigma_3$	$2^{10} \cdot 3^4 \cdot 5^6 = 1296000000$
20	2	$Z_{20}SL(2,5)$	$2^4 \cdot 3 \cdot 5^2 = 1200$

The finite group of maximum order in $GL(n, \mathbb{Q}(\ell))$ is unique up to isoclinism *except in the following cases.*

$\ell = 6, n = 2$: $M(2,6)$ *and* $Z_3 \times SL(2,3)$ *have order* 72,
$\ell = 6, n = 5$: $M(5,6)$ *and* $ST_{32} \times Z_6$ *have order* 933120,
$\ell = 10, n = 3$: $M(3,10)$ *and* $(Z_5 \times SL(2,5)) \times Z_{10}$ *have order* 6000,
$\ell = 30, n = 2$: $M(2,30)$ *and* $Z_{15} \times SL(2,5)$ *have order* 1800.

If $G \subseteq GL(n, \mathbb{Q}(\ell))$ and H is isoclinic to G over $\mathbb{C}$ then in general H need not be isomorphic to a subgroup of $GL(n, \mathbb{Q}(\ell))$. However, if $M(n,\ell)^{\#} \subseteq GL(n, \mathbb{Q}(\ell))$, where $M(n,\ell)^{\#}$ is isoclinic to $M(n,\ell)$ over $\mathbb{C}$ then $M(n,\ell)^{\#} = M(n,\ell)$ is the group of all monomial matrices whose entries are roots of 1 in $\mathbb{Q}(\ell)$.

Hence Theorems A and B and Corollary 2.6 below imply

Corollary C. *If $n > 10$ then $M(n,\ell)$ is a finite subgroup of maximum order in $GL(n, \mathbb{Q}(\ell))$, it is unique up to conjugacy. If $\ell > 2$ this is already the case for $n > 8$.*

It should be pointed out that Corollary C does not imply that any two representations of $M(n,\ell)$ in $GL(n,\ell)$ are equivalent. This phenomenon can be explained by the following observation.

Lemma 1.1. *Let f be a faithful representation of a finite group G over $\mathbb{Q}(\ell)$. Let μ be a linear character of G with values in $\mathbb{Q}(\ell)$ such that μf is also faithful. Assume that the group of scalars Z_ℓ, of order ℓ, is in $f(G)$. Then $f(G) = \mu f(G)$.*

Proof. By definition $\mu(x)f(x) \subseteq Z_\ell f(G)$ for any $x \in G$. Thus

$$\mu f(G) = \{\mu(x)f(x) \mid x \in G\} \subseteq Z_\ell f(G) \subseteq f(G).$$

As $|f(G)| = |\mu f(G)|$ the result follows. □

The notation in this paper is standard in addition to that introduced above.
The details will appear elsewhere.

References

[A] J.H. Conway, R.J. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of finite groups*, Clarendon Press, Oxford (1985).

[F1] W. Feit, *The current situation in the theory of finite groups*, Actes du congrès international des mathématiciens, Nice I (1970), 57–93.

[ST] G.C. Shephard and J.A. Todd, *Finite unitary reflection groups*, Can. J. Math. 6 (1954), 274–304.

[W] B. Weisfeiler, to appear.

Solubility criteria for finite groups

Paul Flavell

The School of Mathematics and Statistics
The University of Birmingham
Birmingham B15 2TT
United Kingdom
e-mail: p.j.flavell@bham.ac.uk

We begin with the following:

Theorem A. A finite group G is soluble if and only if $\langle x, y\rangle$ is soluble for all $x, y \in G$.

This was first proved by John Thompson [4] as a corollary of his classification of the minimal simple groups. A second proof, independent of any classification theorem, has been obtained by the author [2]. Two possible generalizations of Theorem A are:

Conjecture B (A characterisation of the soluble radical). Let x be an element of the finite group G. Then $\langle x^G\rangle$ is soluble if and only if $\langle x, y\rangle$ is soluble for all $y \in G$.

Conjecture C (A soluble Baer-Suzuki Theorem). Let x be an element of order prime to 6 in the finite group G. Then $\langle x^G\rangle$ is soluble if and only if $\langle x, x^y\rangle$ is soluble for all $y \in G$.

This note describes some ideas which are relevant to these problems.

An obvious approach to B and C is to try to generalize the proof of A. Unfortunately, this does not work. To see why, we present part of the proof of A. Firstly recall the

Goldschmidt Lemma. [1, Lemma X.1.6] Let g be a p-element of the soluble group G. Then

$$O_{p'}(C_G(g)) \leq O_{p'}(G).$$

An important part in the proof of A is

Lemma D. Let G be a finite group in which every two elements generate a soluble subgroup. Let g be a p-element of G. Then

$$O_{p'}(C_G(g)) \leq O_{p'}(G).$$

Proof. Let $c \in O_{p'}(C_G(g))$ and let y be a p'-element of G. Set $H = \langle cg, y \rangle$. Since c and g are commuting elements of coprime orders we have $c, g \in H$. Thus

$$c \in H \cap O_{p'}(C_G(g)) \leq O_{p'}(C_H(g)).$$

By hypothesis, H is soluble so the Goldschmidt Lemma implies that $c \in O_{p'}(H)$. Now y is a p'-element of H so then cy is also a p'-element. Since y was an arbitrary p'-element of G, it follows that $\langle c^G \rangle$ is a p'-subgroup. Thus $c \in O_{p'}(G)$. □

Note that the proof does require "two degrees of freedom", hence the difficulty in extending it to cover the situation in B where there is only "one degree of freedom". Some progress is made in [3]. In C, the situation is even worse.

1 Strategy

Conjectures B and C reduce to proving statements of the form

if the group G satisfies ... ... then G is soluble.

A good strategy is to find a method $\mathcal{M}$ such that:

- When $\mathcal{M}$ is applied to a soluble group G then $\mathcal{M}$ returns information regarding the normal subgroups of G.
- $\mathcal{M}$ can be applied to any group G and without any prior knowledge of the normal subgroups of G.

We then apply $\mathcal{M}$ to groups which satisfy the hypothesis of the statement we want to prove in the hope of obtaining information regarding their normal subgroups. Lemma D is a good example of this strategy. The next section describes another.

2 Large 2-generated soluble subgroups

We aim directly for the Fitting subgroup, which is the most important subgroup of a soluble group. For a group G and a subgroup $P \leq G$ define

$$\Sigma_G(P) = \{A \leq G \mid A \text{ is soluble and } A = \langle P, P^a \rangle \text{ for some } a \in A\}.$$

The set $\Sigma_G(P)$ is partially ordered by inclusion and we let

$$\Sigma^*_G(P)$$

denote the set of maximal members of $\Sigma_G(P)$. If q is a prime we let

$$\Sigma^q_G(P)$$

be the set consisting of those members $A \in \Sigma^*_G(P)$ with $|A|_{q'}$ maximal. The elements of $\Sigma^*_G(P)$ have the following property:

Theorem 2.1. *Let G be a group, let P be a subgroup of G with prime order $p > 3$ and let $A \in \Sigma^*_G(P)$. Then*

$$F(A)V$$

is nilpotent for every nilpotent subgroup V of G that is normalized by A.

Recall that $\pi(X)$ is the set of prime divisors of $|X|$ and that if G is soluble then $C_G(F(G)) \leq F(G)$. Then:

Corollary 2.2. *Assume the hypothesis of Theorem 2.1 and that G is soluble. Then*

$$\pi(F(A)) \subseteq \pi(F(G)).$$

Thus, when G is soluble, the members of $\Sigma^*_G(P)$ give us information regarding the Fitting subgroup of G. For the members of $\Sigma^q_G(P)$ we can say a little more:

Corollary 2.3. *Assume the hypotheses of Theorem 2.1, that G is soluble, that q is a prime and that $A \in \Sigma^q_G(P)$. Then*

$$O_q(A) \leq O_q(G).$$

However, this is only useful if we know that $O_q(A) \neq 1$.

Before giving an application of these results, we make some comments about their proof. Most of the effort in proving Theorem 2.1 goes into establishing:

Lemma 2.4. *Let G be a soluble group, let P be a subgroup of G with prime order $p > 3$ such that $G = \langle P^G \rangle$ and let V be a faithful and irreducible G-module. Then*

$$\dim C_V(P) < \frac{1}{2} \dim V.$$

This result seems to be quite deep. The present lengthy proof uses Hall-Higman techniques.

Although the theory developed so far is not strong enough to prove Conjectures B or C, it does easily prove a weak form of C. Thus it seems to be heading in the right direction.

Theorem 2.5. *Let G be a finite group and let x be an element of G with order prime to 6. If every four conjugates of x generate a soluble subgroup then $\langle x^G \rangle$ is soluble.*

Proof. Assume false and let G be a minimal counterexample. Then $\mathrm{sol}(G)$, the largest normal soluble subgroup of G, is trivial. Also, we may suppose that x has prime order $p > 3$. Let $P = \langle x \rangle$.

We claim that there exists a prime q such that $F(A)$ is a q-group for all $A \in \Sigma_G^*(P)$. Let $A, B \in \Sigma_G^*(P)$, choose $q \in \pi(F(B))$, let $g \in G$ and set $H = \langle A^g, B \rangle$. Then $A^g \in \Sigma_H^*(P^g)$ and $B \in \Sigma_H^*(P)$. Theorem 2.1 implies that $F(A^g)F(H)$ and $F(B)F(H)$ are nilpotent, whence

$$O_{q'}(F(A^g)) \leq C_H(O_q(H)) \trianglelefteq H \quad \text{and} \quad O_q(B) \leq C_H(O_{q'}(F(H))) \trianglelefteq H.$$

By hypothesis, H is soluble so $C_H(F(H)) \leq F(H)$. Thus

$$[O_{q'}(F(A^g)), O_q(B)] \leq F(H).$$

Consequently, $O_{q'}(F(A^g))F(H)$ and $O_q(B)F(H)$ are nilpotent subgroups of H that normalize one another. We deduce that $(O_{q'}(F(A)))^g$ centralizes $O_q(B)$ for all $g \in G$. Let

$$K = \langle O_{q'}(F(A))^G \rangle \quad \text{and} \quad N = N(O_q(B)).$$

Then $K \trianglelefteq G$ and $K \leq N \neq G$. Now $P \leq N$ so the minimality of G forces $P \leq \mathrm{sol}(N)$ and hence

$$[K, P] \leq K \cap \mathrm{sol}(N) \leq \mathrm{sol}(K) \leq \mathrm{sol}(G) = 1.$$

Now $G = \langle P^G \rangle$ by the minimality of G, so as $K \trianglelefteq G$ it follows that $K \leq Z(G) = 1$. We deduce that $\mathcal{O}_{q'}(F(A)) = 1$ and then that $F(A)$ is a q-group for all $A \in \Sigma^*_G(P)$.

Now choose $A \in \Sigma^q_G(P)$, let $g \in G$ and set $K = \langle A, A^g \rangle$. Corollary 2.3 implies that $\langle \mathcal{O}_q(A), \mathcal{O}_q(A^g) \rangle \leq \mathcal{O}_q(K)$ so we deduce that $\langle \mathcal{O}_q(A), \mathcal{O}_q(A)^g \rangle$ is a q-group for all $g \in G$. Now A is soluble so the previous paragraph implies that $\mathcal{O}_q(A) \neq 1$. But $\mathcal{O}_q(G) = 1$ so we obtain a final contradiction using the Baer-Suzuki Theorem. □

References

[1] Blackburn, N., Huppert, B.: Finite groups III. Grundlehren der Mathematischen Wissenschaften, vol. 243. Berlin, Heidelberg, New York: Springer 1982.

[2] Flavell, P.J.: Finite groups in which every two elements generate a soluble subgroup. Invent. Math. **121**, 279-285(1995).

[3] Flavell, P.J.: A characterisation of p-soluble groups. Bull. London Math. Soc. **29**, 177-183(1997).

[4] Thompson, J.G.: Non-solvable groups all of whose local subgroups are solvable, I-VI. Bull. Amer. Math. Soc., **74**, 383-437 (1968); Pacific J. Math. **33**, 451-536 (1970); **39**, 483-534 (1971); **48**, 511-592 (1973); **50**, 215-297 (1974); **51**, 573-630 (1974).

New 5-Designs Constructed from the Lifted Golay Code over $\mathbb{Z}_4$

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990, Japan

November 13, 1997

Abstract

It is shown that the lifted Golay code over $\mathbb{Z}_4$ contains several 5-designs. In particular, a 5-$(24, 12, 1584)$ design and a 5-$(24, 12, 1632)$ design are constructed for the first time.

1 Introduction

A t-(v, k, λ) design D is a set of v points with a collection of k-subsets called blocks, so that any t-points are contained in exactly λ blocks. A design with no repeated block is called *simple*. In this paper, we consider only simple designs. The complementary design of D is a design obtained by replacing each block in D by its complement. The incidence matrix of D is the matrix $M = (m_{ij})$ where $m_{ij} = 1$ if the j-th point is contained in the i-th block and $m_{ij} = 0$ otherwise. Two designs are *isomorphic* if the incidence matrix of one design can be obtained from the incidence matrix of the other by permuting its rows and columns.

A fundamental problem in design theory is to determine if there exists a design for a given set of parameters. Coding theory has made a substantial contribution to design theory. For example, the Assmus-Mattson theorem [1] determines whether the codewords of a specified weight in a code over $GF(q)$ form a t-design. In particular, it is well known that the codewords of weight 8 in the binary extended Golay code form the Steiner system $S(5, 8, 24)$, which is the unique 5-$(24, 8, 1)$ design. Moreover, the codewords of weight 12 form a 5-$(24, 12, 48)$ design which is known as the dodecad design. This 5-design is a unique design for the parameters such that every two blocks intersect in an even number of points (cf. [10]).

Recently a number of papers have studied self-dual codes over $\mathbb{Z}_4$ the ring of integers modulo 4 (cf., e.g. [2], [3], [5], [6] and the references given therein). Connections of self-dual codes over $\mathbb{Z}_4$ with unimodular lattices and binary nonlinear codes have been found. In this paper, we present a conncetion with desgins. Type II codes have been introduced by Bonnecaze, Solé, Bachoc and Mourrain [3], as a class of self-dual codes over $\mathbb{Z}_4$. This class includes the octacode O_8 of length 8 and the Hensel lifted Golay code of length 24. In this paper, we demonstrate that certain codewords in the lifted Golay code over $\mathbb{Z}_4$ form 5-designs. In particular, a 5-$(24, 12, 1584)$ design and a 5-$(24, 12, 1632)$ design are constructed. From [8] and Table 3.37 in [4], these two designs are the first designs with these parameters.

2 Self-dual codes and the lifted Golay code

2.1 Self-dual codes

A code C of length n over $\mathbb{Z}_4$ is an additive subgroup of $\mathbb{Z}_4^n$. An element of C is called a codeword. The Hamming weight of a codeword is the number of its non-zero components. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_4^n | \ x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y = x_1 y_1 + \cdots + x_n y_n \pmod 4$, $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. C is *self-dual* if $C = C^\perp$. We say that two codes are *permutation-equivalent* if one can be obtained from the other by permuting the coordinates. The symmetrized weight enumerator (s.w.e.) of a code C over $\mathbb{Z}_4$ is

$$swe_C(X, Y, Z) = \sum_{c \in C} X^{n_0(c)} Y^{n_1(c)} Z^{n_2(c)},$$

where $n_0(c), n_1(c)$ and $n_2(c)$ are the numbers of $0, \pm 1$ and 2 components of c, respectively.

Any code is permutation-equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}, \tag{1}$$

where A and D are matrices over $\mathbb{Z}_2$ and B is a matrix over $\mathbb{Z}_4$. We say that a code with generator matrix (1) is of *type* $4^{k_1} 2^{k_2}$ (cf. [5]). Every code C over $\mathbb{Z}_4$ has two binary codes $C^{(1)}$ and $C^{(2)}$ associated with C:

$$\begin{aligned} C^{(1)} &= \{c \pmod 2) \mid c \in C\} \text{ and} \\ C^{(2)} &= \{\frac{1}{2}c \mid c \in C, \ c \equiv 0 \pmod 2)\}. \end{aligned}$$

If C is of type $4^{k_1} 2^{k_2}$ then $C^{(1)}$ is a binary $[n, k_1]$ code and $C^{(2)}$ is a binary $[n, k_1 + k_2]$ code. Moreover, if C is a self-dual code of length n and type $4^{\frac{n}{2}}$, then $C^{(1)} = C^{(2)}$ and $C^{(1)}$ is a doubly-even self-dual code (cf. [5]). Our terminology for codes over $\mathbb{Z}_4$ follows that in [5].

2.2 The lifted Golay code

The lifted Golay code G_{24} over $\mathbb{Z}_4$ is defined in [2] as the extended Hensel lifted quadratic residue code of length 24. G_{24} is a Type II code constructed from the cyclic code with generator polynomial

$$x^{11}+2x^{10}+3x^9+3x^7+3x^6+3x^5+2x^4+x+3,$$

by appending 3 to the last coordinate of the generator vectors. The s.w.e. of G_{24} is given in [3]:

$$\begin{aligned} W &= X^{24}+Z^{24}+24288Y^{16}Z^8+4096Y^{24}+61824XY^{12}Z^{11} \\ &+12144X^2Y^8Z^{14}+680064X^2Y^{16}Z^6+1133440X^3Y^{12}Z^9+170016X^4Y^8Z^{12} \\ &+1700160X^4Y^{16}Z^4+4080384X^5Y^{12}Z^7+765072X^6Y^8Z^{10}+680064X^6Y^{16}Z^2 \\ &+4080384X^7Y^{12}Z^5+759X^8Z^{16}+1214400X^8Y^8Z^8+24288X^8Y^{16} \\ &+1133440X^9Y^{12}Z^3+765072X^{10}Y^8Z^6+61824X^{11}Y^{12}Z+2576X^{12}Z^{12} \\ &+170016X^{12}Y^8Z^4+12144X^{14}Y^8Z^2+759X^{16}Z^8. \end{aligned}$$

The automorphism group of the binary Golay code is the Mathieu group M_{24}. In [9] Chapman shows that the automorphism group of the lifted Golay code is $SL(2,23)$.

Since G_{24} is of type 4^{12}, $G_{24}^{(1)}=G_{24}^{(2)}$. Moreover $G_{24}^{(1)}$ is the binary Golay code of length 24. Thus the supports of the codewords of Hamming weight 8 form the Steiner system $S(5,8,24)$. Similarly, the supports of the 2576 codewords corresponding to $X^{12}Z^{12}$ in W form a 5-$(24,12,48)$ design and the supports of the 759 codewords corresponding to X^8Z^{16} in W form a complementary design of $S(5,8,24)$. It is shown in [6] that the supports of the codewords of Hamming weight 10 in the lifted Golay code and certain extremal double circulant Type II codes of length 24 form a 5-$(24,10,36)$ design. In this paper, we consider not only the codewords of Hamming weight 12 but also the codewords corresponding to $X^{12}Y^8Z^4$. These are used to construct a 5-$(24,12,1584)$ design and a 5-$(24,12,1632)$ design.

3 5-designs in the lifted Golay code

3.1 A 5-(24, 12, 1584) design and a 5-(24, 12, 1632) design

We first investigate the 170016 codewords corresponding to $X^{12}Y^8Z^4$ in W. Let A be a 170016 by 24 matrix whose rows are the above codewords. If v is a codeword corresponding to $X^{12}Y^8Z^4$ then $3v$ is also a codeword corresponding to $X^{12}Y^8Z^4$, but $2v$ is not. Moreover it is easy to see that

$$A=\begin{pmatrix} B_1 \\ 3B_1 \end{pmatrix},$$

where $B_1=(b_{ij})$ is an 85008 by 24 matrix over $\mathbb{Z}_4$. Now define an 85008 by 24 $(1,0)$-matrix $M_1=(m_{ij})$ where $m_{ij}=1$ if $b_{ij}\neq 0$ and $m_{ij}=0$ otherwise. We have verified by computer that M_1 is an incidence matrix of a (simple) 5-$(24,12,1584)$ design.

As mentioned in Section 2, the supports of the codewords corresponding to $X^{12}Z^{12}$ in W form a simple 5-$(24,12,48)$ design which is isomorphic to the dodecad design. Let M_2

be the incidence matrix of this design. Then it is easy to see that the matrix

$$M_3 = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix},$$

is an incidence matrix for a 5-$(24, 12, 1632)$ design, however this design may contain a repeated block. Let v and w be codewords corresponding to $X^{12}Y^8Z^4$ and $X^{12}Z^{12}$, respectively. Assume that v and w have identical supports in M_3. Then the codeword $v + w$ corresponds to $X^{16}Y^8$, which is a contradiction. Therefore the design is simple.

Kramer, Magliveras and Mesner [8] determined all 5-designs with the Mathieu group M_{24} as the automorphism group. Thus the automorphism groups of our 5-designs are not M_{24}. Information on simple t-designs is given in Table 3.37 of [4, p. 52]. From this table, our designs are the first 5-designs with these parameters. Note that the table in [4] misses some 5-designs in [8].

Since one can easily construct the two 5-designs from the lifted Golay code, to save space the incidence matrices are not listed here. However the incidence matrices are available on the world wide web at `http://kszaohl.kj.yamagata-u.ac.jp/harada`.

3.2 More 5-designs

Our computer search shows that the supports of the codewords of Hamming weight 13 form the complementary design of a 5-$(24, 11, 336)$ design. Let M_4 be the matrix over $\mathbb{Z}_4$ obtained from the codewords of Hamming weight 13. Since the Hamming weight 13 corresponds to $61824X^{11}Y^{12}Z$ in W,

$$M_4 \pmod 2 \equiv \begin{pmatrix} M_2 \\ M_2 \\ \vdots \\ M_2 \end{pmatrix}.$$

Moreover it is not hard to see that the automorphism group of this design is M_{24}. Thus this design must be isomorphic to the design in [8]. In addition, the supports of the 24288 codewords corresponding to X^8Y^{16} in W form a complementary design of the Steiner system $S(5, 8, 24)$.

3.3 Summary

As a summary, we give 5-designs in the lifted Golay code in the following proposition.

Proposition 1 *There exist* 5-$(24, 12, \lambda)$ *designs for* $\lambda = 1584$ *and* 1632. *The lifted Golay code contains* 5-$(24, k, \lambda)$ *designs for* $(k, \lambda) = (8, 1), (10, 36), (11, 336), (12, 48), (12, 1584)$ *and* $(12, 1632)$.

4 Concluding remarks

It is well known that the block intersection numbers of $S(5,8,24)$ are 0, 2 and 4 and the incidence matrix of $S(5,8,24)$ generates the binary Golay code. We have verified that the incidence matrix of any of the above eight designs cannot generate a self-orthogonal code over $\mathbb{Z}_4$, as well as the lifted Golay code.

Since the supports of the codewords of Hamming weight 8 form $S(5,8,24)$, its automorphism group is M_{24}. It is shown in [2] that the supports of the codewords of Hamming weight 10 form a 3-(24, 10, 360) design and $PSL(2,23)$ acts on the design. This design is also a 5-design. Let S be the set of the codewords of Hamming weight 10, then $S \pmod 2$ is the $S(5,8,24)$. Kitazume [7] shows that the automorphism group of the design is $PSL(2,23)$ using properties of the design and $S(5,8,24)$.

Now we give an observation of the extremal Type II codes in [6] such that the supports of the codewords of Hamming weight 10 form 5-(24, 10, 36) designs.

Proposition 2 *Let D be a double circulant code of length 24 such that $D^{(1)} = D^{(2)}$, $D^{(1)}$ is the binary Golay code and D has the same symmetrized weight enumerator as the lifted Golay code. Then the supports of the codewords of Hamming weight 10 in D form a 5-(24, 10, 36) design.*

We conjecture that the above proposition is ture for a code satisfying the condition. In general, we prompt the following question:

Question. Is there a result analogous to the Assmus-Mattson theorem for a code over $\mathbb{Z}_4$?

Acknowledgments. The author would like to thank Dr. Masaaki Kitazume for useful discussions and comments. The author would like to thank Dr. Edward F. Assmus, Jr., Dr. Steven T. Dougherty, Dr. T. Aaron Gulliver, Dr. Patrick Solé and Dr. Vladimir D. Tonchev for reading the manuscript and making helpful comments. The author would like to thank the referees for their useful comments, in particular one of them supplied a useful reference [8]. Thanks are due also to Dr. Akihiro Munemasa for helpful conversations.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., *New 5-designs*, J. Combin. Theory 6 (1969), 122–151.

[2] A. Bonnecaze, P. Solé and A.R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory 41 (1995), 366–377.

[3] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, *Type II codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory 43 (1997), 969–976.

[4] C.J. Colbourn and J.H. Dinitz, *The CRC handbook of combinatorial designs*, CRC Press, Boca Raton, 1996.

[5] J.H. Conway and N.J.A. Sloane, *Self-dual codes over the integers modulo 4*, J. Combin. Theory Ser. A 62 (1993), 30–45.

[6] T.A. Gulliver and M. Harada, *Extremal double circulant Type II codes over $\mathbb{Z}_4$ and construction of 5-$(24, 10, 36)$ designs*, (submitted to Discrete Math.).

[7] M. Kitazume, private communication, October 1996.

[8] E.S. Kramer, S.S. Magliveras and D.M. Mesner, *t-designs from the large Mathieu groups*, Discrete Math. 36 (1981), 171–189.

[9] P. Solé, private communication, October 1996.

[10] V.D. Tonchev, *A characterization of designs related to dodecads in the Witt system* $S(5, 8, 24)$, J. Combin. Theory Ser. A 43 (1986), 219–227.

Some Highly Symmetric Chamber Systems

D. G. Higman

8/26/97

ABSTRACT. After a review of some basics about chamber systems, a list is presented of some chamber systems whose full automorphism groups are transitive on the chambers and have a subgroup acting as the symmetric group on the types.

1. Chamber Systems

We begin by reviewing some basics about these structures which were introduced in [JT]. A *chamber system* $\mathcal{C} = (\Omega, \{E_i \mid i \in I\})$ *over* I, or of *type* I, consists of a set Ω of elements called *chambers*, and a family $\{E_i \mid i \in I\}$ of equivalence relations on Ω, which, in the setup and terminology to be used here, turn out to be the *maximal parabolics* of $\mathcal{C}$. The *type* of $\mathcal{C}$ is I and the *rank* is $|I|$. Write $V_i = \Omega/E_i$ and put $V = \cup_{i \in I} V_i$. The chamber systems considered here are assumed to satisfy the two conditions:

(C1) the sets V_i, $i \in I$, are pairwise disjoint;

(C2) if J is a nonempty subset of I and $\{x_j \mid j \in J\}$ is such that $x_j \in V_j$ and $x_j \cap x_k \neq \emptyset$ for all j, $k \in J$, then $|\cap_{j \in J} x_j| = 1$ or ≥ 2 according as $J = I$ or $J \neq I$.

The *type function* $\tau: V \to I$ is defined by $\tau^{-1}(i) = V_i$. For $J \subseteq I$, a J*–simplex*, or *simplex* of *type* J, is defined to be a set $\{x_j \mid j \in J\}$ such that $x_j \in V_j$, $j \in J$, and $\cap_{j \in J} x_j \neq \emptyset$. Associated with $\mathcal{C}$ is the simplicial complex $\mathcal{K} = (V, \mathcal{S}, \tau, I)$ over I, with vertices V and simplices $\mathcal{S}$, where $\mathcal{S}$ is the set of all J-simplexes, $J \subseteq I$. The elements of V_i are the vertices of type I.

Incidence of x and y in V, written $x * y$, is defined to mean $x \neq y$ and $x \cap y \neq \emptyset$. The geometry over I, or of *type* I, associated with $\mathcal{C}$ is $\mathcal{G} = (V, *, \tau, I)$. In this context the elements of V are called *varieties* and the elements of V_i are the varieties of *type* I.

It is a consequence of (C1) and (C2) that $\mathcal{C}$, $\mathcal{K}$ and $\mathcal{G}$ are equivalent, namely, assuming (C1) and (C2):

(1) The top simplexes of $\mathcal{K}$ are the I-simplexes. An isomorphic copy of $\mathcal{C}$, is recovered from $\mathcal{C}$ by taking as chambers the top simplexes of $\mathcal{K}$ and defining the i-th equivalence relation to consist of the pairs of these with the same vertex of type i;

(2) A *flag* of $\mathcal{G}$ is a set of pairwise incident varieties, and the *type* of a flag (or more generally of any set of chambers) is the set of types of its varieties. The J-simplexes of $\mathcal{K}$ are the flags of type J of $\mathcal{G}$, which means that $\mathcal{K}$ is that flag complex of $\mathcal{G}$. □

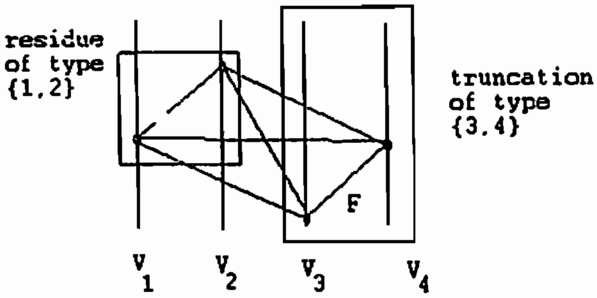


Figure 1:

The geometries over I arising here are characterized by the property that every nonmaximal flag lies in at least two flags of type I. We will pass freely between a chamber system and its interpretations as a simplicial complex or geometry.

A further consequence of (C1) and (C2) is that the mapping $J \mapsto E_J = \cap_{j\in J} Ej$, $J \subseteq I$, is an anti-isomorphism of the lattice of subsets of I onto a sublattice $\mathcal{L}(C)$ of the lattice of equivalence relations on Ω. The equivalence relations E_J will be referred to as the *parabolics* of C, thus the original E_i are the maximal parabolics.

Associated with a chamber system C are additional chamber systems called its *residues* and *truncations.* Given a nonempty, proper subset J of I and a nonempty subset X of $V_J = \Omega/E_J$, there is the chamber system C^X having as its set of chambers the set X and as its maximal parabolics the equivalence relations induced on X by the parabolics $E_{J\cup\{i\}}$, $i \in I - J$. The chamber system C^X, which inherits the conditions (C1) and (C2) and has type $I - J$, will be referred to as a *residue of* C of type $I - J$. Its lattice of parabolics $\mathcal{L}(C^X)$ is isomorphic with the interval $[\emptyset, E_J]$ of the lattice of parabolics of C. In addition we have the chamber system C_J having V_J as its set of chambers and the equivalence relations induced on V_J as its maximal parabolics. Again the conditions (C1) and (C2) are inherited, and this time the type is J and the lattice $\mathcal{L}(C_J)$ of parabolics is isomorphic with the interval $[E_J, \Omega \times \Omega]$ of $\mathcal{L}(C)$; C_J will be referred to as the *truncation* of type J of C.

In the geometry $\mathcal{G}$, $X \in V_J$ can be identified with the set of all maximal flags containing a given flag F of type J. The geometry associated with C^X can be identified with the set of varieties of $\mathcal{G}$ incident with every variety of F, with incidence induced by incidence in $\mathcal{G}$. The truncation of C modulo J can be interpreted as the geometry obtained from $\mathcal{G}$ by deleting the varieties of type not in J.

By a *diagram* Δ *over* I is meant the complete graph on I with each edge $\{i, j\}$ labeled by a class c_{ij} of rank 2 geometries. A geometry over I *satisfies* Δ if, for each

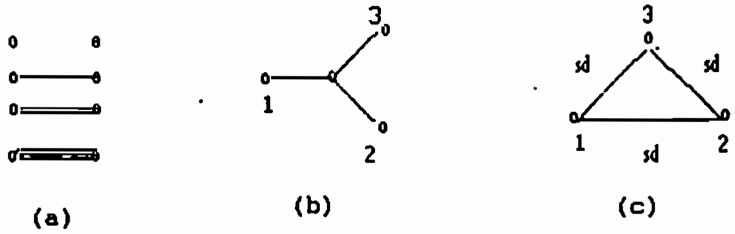


Figure 2:

$i \neq j$, all of its residues of type $\{i, j\}$ belong to the class c_{ij}. Buildings, and more generally SCABS and GABS, satisfy diagrams labeled by generalized digons, triangles, hexagons and octagons, which are rank 2 geometries conventionally represented respectively as in *Figure 1(a)*. Additional labels will arise here, namely *sd (symmetric designs), qsd (quasisymmetric designs), srd1 and srd2 (strongly regular designs of the first and second kind) [DGH]*. For example, the building of type $D_4(q)$, satisfying the diagram of *Figure 2(b)*, has truncation of type $\{1,2,3\}$ satisfying the diagram of *Figure 2(c)*. The rank 2 residues of the truncation are isomorphic with the symmetric $2-(q^3+q^2+q+1, q^2+q+1, q+1)$ design of points and planes of $PG_3(q)$.

2. AUTOMORPHISMS

An *automorphism* of a chamber system $C = (\Omega, \{E_i \,|\, i \in I\})$ is an element (σ, α) of $Sym(\Omega) \times Sym(I)$ such that $\sigma E_i = E_{\alpha(i)}$ for all $i \in I$. An automorphism (σ, α) will be called a *collineation* if $\alpha = 1$, and a *correlation* if it is either the identity or not a collineation. The group $Aut(C)$ of automorphism of C acts on I according to $Aut(C) \rightarrow Sym(I)$, $(\sigma, \alpha) \mapsto \alpha$, and the kernel of this action is the group $Aut_o(C)$ of collineations.

Below we list the examples that we know of chamber systems of rank ≥ 3 for which the sequence

(*) $\qquad 1 \rightarrow Aut_o(C) \rightarrow Aut(C) \rightarrow Sym(I) \rightarrow 1$

is split exact, i.e., for which there is a group S of correlations acting (faithfully) as $Sym(I)$ on I, or equivalently, $Aut(C) = Aut_o(C) : S$, $S \cong Sym(I)$. The condition (*) is inherited by residues and truncations. As geometries, rank 2 examples are simply rank 2 geometries with a polarity, and these are plentiful. Here we are interested in rank 2 examples only in so far as they occur as rank 2 residues of higher rank examples.

Given a subgroup B of a group G there is an isomorphism of the lattice of subgroups H of G containing B onto the lattice of G-invariant equivalence relations on the

transitive G-set $\Omega = G/B$ which maps H onto $E = \{(xB, yB) \in \Omega \cup \Omega \,|\, x^{-1}y \in H\}$. The inverse maps the G-invariant equivalence relation E onto $H = Stab_G(E(B))$. The examples in the list are all instances of the following situation. There is given a group G and a family $\{P_i | i \in I\}$ of subgroups of G, and we put $B = \bigcap_{i \in I} P_i$. The chamber system is C= $(\Omega, \{E_i \,|\, i \in I\})$, where $\Omega = G/B$ and E_i is the G-invariant equivalence relation on Ω corresponding to P_i. The mapping $V_i = \Omega/E_i \rightarrow G/P_i$, $E_i(xB) \mapsto xP_i$, is an isomorphism of G-sets. In each of the examples we have
(**) for each nonempty subset J of I,

(i) if $\{X_j \,|\, j \in J\}$, $X_j \in G/P_j$, is such that $X_j \cap X_k \neq \emptyset$ for all $j \in K$, then $\bigcap_{j \in J} X_j \neq \emptyset$;

and

(ii) if $J \neq I$, then $\bigcap_{i \in J} P_j \neq B$.

Because of the isomorphism of V_i onto G/P_i and (ii) of (**), condition (C1) holds, and because of (**), (C2) holds. The group G acts as a group of collineations of C, transitive on the chambers and hence flag-transitive on the corresponding geometry. In each of the examples there is a subgroup S of $Aut(G)$ which acts faithfully on $\{C_i \,|\, i \in I\}$ as $Sym(I)$ acts on I, where C_i is the conjugacy class in G of P_i. Therefore (*) holds. The subgroups $P_J = \bigcap_{j \in J} P_j$, $J \subseteq I$, which correspond to the parabolics E_J of C, can be called the *parabolic subgroups* of G relative to C, and $B = P_I$ the *Borel subgroup* of G relative to C. We write P_{ij} for $P_i \cap P_j$, and similarly for P_{ijk}, etc. Each row of the list gives the isomorphism class of the group G, of the parabolics $P_i, P_{ij}, ...,$ and of the Borel subgroup B, and finally the class of the rank 2 residues (of course all of the rank 2 residues in each example are isomorphic because of the existence of S).

Examples

(1) $U_3(5)$	A_7	$L_3(2)$	F_{21}	sd	
(2) $O_8^+(2)$	$q^6 : L_4(q)$	$q^{6+3} : L_3(q)$	$q^{6+3+2} : GL_2(q)$	sd	
(3) $O_8^+(2)$	A_9	$L_3(8) : 3$	$D_{14} : 3$	$srd1$	
(4) $2^9 : L_3(4)$	$L_3(4)$	A_6	$3^2 : 2$	$srd1$	
(5) $U_6(2)$	M_{22}	A_7	$(A_4 \times 3) : 2$	$srd2$	
(6) ${}^6E_6(2)$	Fi_{22}	$O_7(2)$	$3^5 : U_4(2) : 2$	$srd2$	
(7) ${}^2E_6(2)$	$F_4(2)$	${}^3D_4(2)$	$7^2 : (3 \times 2A_4)$		
(8) $O_8^+(3)$	$O_8^+(2)$	$2^6 : L_4(2)$	$2^{6+3} : L_3(2)$	$2^{6+3+2}GL_2(2)$	sd

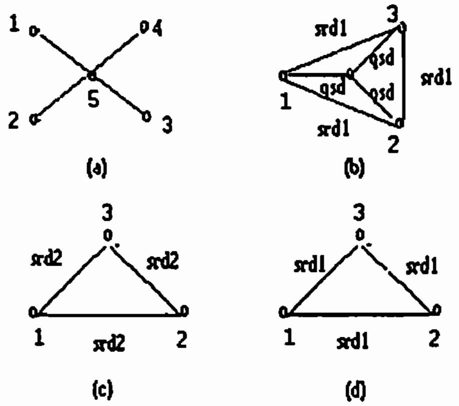


Figure 3:

Examples (1) through (7) have rank 3 and (8) has rank 4. Except for (6) and (7) each of the examples has been constructed explicitly on Magma. Example (2) is classical triality. Example (7) is the case $m = 0$ of a family with $G = {}^2E_2(2)$. Example (8) is the truncation of type $\{1,2,3,4\}$ of the first member of Kantor's family belonging to the diagram of *Figure 3(a)* *[WK]*. Its rank 2 residues are *sd*'s.

Here are some more details about (4) and (5). These are respectively the rank 3 residue of type $\{1,2,3\}$ and the truncation of type $\{1,2,3\}$ of a chamber system D of rank 4 satisfying the diagram of *Figure 3(b)*, with

$G \cong U_6(2)$ *and* $Aut(G) \cong S_3$;
$P_1 \cong P_2 \cong P_3 \cong M_{22}$ *and* $P_4 \cong 2^9 : L_3(3)$;
$P_{12} \cong P_{13} \cong P_{23} \cong A_7$ *and* $P_{14} \cong P_{24} \cong P_{34} \cong L_3(4)$;
$P_{123} \cong (A_4 \times 3) : 2$ *and* $P_{124} \cong P_{134} \cong P_{234} \cong A_6$;
$B \cong 3^2 : 2$
(see *Figure 4*).

For this chamber system the permutation action of G on (the varieties of) D has type $\begin{pmatrix} 8 & 6 & 6 & 4 \\ & 8 & 6 & 4 \\ & & 8 & 4 \\ & & & 4 \end{pmatrix}$. Thus the type of the permutation action of G on the truncation of D of type $\{1,2,3\}$ is $\begin{pmatrix} 8 & 6 & 6 \\ & 8 & 6 \\ & & 8 \end{pmatrix}$. The type of the permutation action of $P_i \cong$

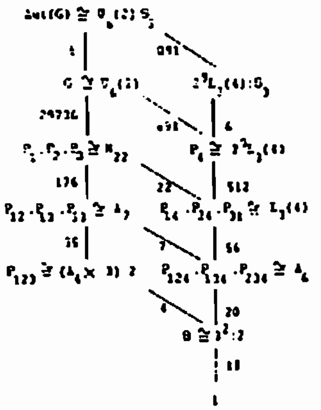


Figure 4:

$M_{22}, i = 1, 2, 3$, on the corresponding rank 2 residue of this truncation is $\begin{pmatrix} 3 & 3 \\ & 3 \end{pmatrix}$, so these rank 2 residues are *srd*2's.

References

[DGH] D. G. Higman, Strongly regular designs and coherent configurations of type $\begin{pmatrix} 3 & 2 \\ & 3 \end{pmatrix}$, European. J. Combin., 9(1988). 411-422; Strongly regular designs of the second kind and coherent configurations of type $\begin{pmatrix} 3 & 3 \\ & 3 \end{pmatrix}$, European J. Combin. 16(1995), 479-490.

[WK] W. Kantor, *Generalized polygons, SCABS and GABS*, Buildings and the geometry of diagrams (Como 1984), 79-158; *Some exceptional 2-adic buildings*, J. Alg. 92(1985), 208-223.

[JT] J. Tits, *A local approach to buildings*, The Geometric Vein, 519-547, Springer, 1981.

An Improvement of the Ivanov Bound

Akira HIRAKI [*] and Jack KOOLEN [†]

1 Introduction

For definitions and information about distance-regular graphs we would like to refer to [1], [2].

Let Γ be a distance-regular graph with valency k, diameter d and define $r := \max\{\, i \mid (c_i, b_i) = (c_1, b_1)\,\}$. A. A. Ivanov [5] showed the diameter bound

$$d \le 4^k r.$$

In this note we will show the following improvement of this bound.

Theorem 1.1 *Let Γ be a distance-regular graph of diameter d, valency k and $r = \max\{\, i \mid (c_i, b_i) = (c_1, b_1)\,\}$. Then*

$$d < \frac{1}{2}k^3 r.$$

2 Proof of Main Result

We introduce only the outline of our proof.

Let Γ be a distance-regular graph. Define

$$\eta_c := |\{\, i \mid c_i = c\,\}| \quad \text{and} \quad \xi_c := \min\{\, i \mid c_i \ge c\,\}.$$

Lemma 2.1 *Let $c > 1$ be an integer. Then $\eta_c \le 2\xi_c - 3$.*

Lemma 2.2 [7] *If $c_t > c_{t-1}$, then $c_t \ge c_i + c_{t-i}$ for all $1 \le i \le t-1$.*

Proposition 2.3 *Let c be a positive integer. If $\eta_c \ne 0$, then $\xi_c \le \frac{c^2}{4}\eta_1 + 1$.*

Proof. We prove our assertion by induction on c. The assertion is true for $c = 2$ as $\xi_2 = \eta_1 + 1$. We assume $c \ge 3$.

[*] Division of Mathematical Sciences, Osaka Kyoiku University, Kashiwara, Osaka 582, JAPAN.

[†] Graduate School of Mathematics, Kyushu University, Fukuoka, 812, JAPAN

Suppose

$$\eta_c \neq 0 \quad \text{and} \quad \xi_c \geq \frac{c^2}{4}\eta_1 + 2$$

to derive a contradiction. Let $\xi := \xi_c$, $t := [\xi/2]$, $\alpha := c_t$ and $s = \xi_\alpha$. Lemma 2.2 implies $c \geq c_s + c_{\xi-s} \geq 2\alpha$. From our inductive assumption,

$$s = \xi_\alpha \leq \frac{\alpha^2}{4}\eta_1 + 1 \leq \frac{c^2}{16}\eta_1 + 1.$$

From Lemma 2.1, we have

$$s + \eta_\alpha \;\leq\; 3s - 3 \;=\; 4(s-1) + 1 - s \;\leq\; \frac{c^2}{4}\eta_1 + 1 - s \;<\; \xi - s.$$

Thus we have $\beta := c_{\xi-s} > \alpha$ and $t + 1 \leq \xi_\beta$. Hence

$$c^2\eta_1 \;\leq\; 4(\xi - 2) \;<\; 8t \;\leq\; 8(\xi_\beta - 1) \;\leq\; 2\beta^2\eta_1$$

from our inductive assumption. This implies $c < \sqrt{2}\beta$.

On the other hand $t \leq s + \eta_\alpha - 1 \leq 3s - 4$ from Lemma 2.1. Hence we have

$$\frac{c^2}{4}\eta_1 \;\leq\; \xi - 2 \;\leq\; 2t - 1 \;<\; 6(s-1) \;\leq\; 6\frac{\alpha^2}{4}\eta_1.$$

This implies $c < \sqrt{6}\alpha$.

By Lemma 2.2 we have

$$c \;=\; c_\xi \;\geq\; c_s + c_{\xi-s} \;=\; \alpha + \beta \;>\; \frac{c}{\sqrt{6}} + \frac{c}{\sqrt{2}} \;>\; c.$$

This is a contradiction. ■

Theorem 2.4 *Let Γ be a distance-regular graph of diameter d, valency $k > 2$ and $\eta_1 := |\{\, i \mid c_i = 1 \,\}|$. Then*

$$d < \frac{1}{2}k^2\eta_1.$$

Proof. Let $c := c_d$. If $2c \leq k$, then Lemma 2.1 and Proposition show that

$$d \;=\; \xi_c + \eta_c - 1 \;<\; 3(\xi_c - 1) \;\leq\; 3\frac{c^2}{4}\eta_1 \;\leq\; \frac{3}{4}(\frac{k}{2})^2\eta_1 \;<\; \frac{1}{2}k^2\eta_1.$$

If $k < 2c$, then $b_\xi \leq k - c_\xi < c_\xi$ which implies

$$d \;<\; 2\xi_c \;\leq\; 2\frac{c^2}{4}\eta_1 \;=\; \frac{1}{2}k^2\eta_1.$$

The assertion follows. ■

Proof of Theorem 1.1. A. V. Ivanov has proved $\eta_1 \leq kr$ (See [2, Theorem 5.9.9]). Using this, Theorem 1.1 is a direct consequence of Theorem 2.4. ■

3 Conclusions

With a much more complicated argument we are able to show the following improvement of Theorem 2.4:
there are constants C and ε with $0.5 > \varepsilon > 0$ such that

$$d \leq Ck^{2-\epsilon}\eta_1.$$

Therefore we conjecture

Conjecture 3.1 *There is a constant* C *such that* $d \leq Ck\eta_1$

A related conjecture is a conjecture by Hiraki.

Conjecture 3.2 (Hiraki [4]) *There is a constant* C *such that* $\eta_1 \leq 2r + C$.

This conjecture is true whenever $r \neq 1$ and ($a_1 \neq 0$ or $r \not\equiv 0 \pmod 3$). [3, 4].
If both previous conjectures are true then this will solve an conjecture by A. V. Ivanov up to a constant.

Conjecture 3.3 (A. V. Ivanov [6]) $d \leq 2(r+1)k$.

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I,* Benjamin-Cummings, California, 1984.

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs,* Springer Verlag, Berlin, Heidelberg, 1989.

[3] A. Boshier and K. Nomura, A remark on the intersection arrays of distance-regular graphs, *J. of Combin. Theory, Ser.* (B) 44 (1988), 147–153.

[4] A. Hiraki, Distance-regular subgraphs in a distance-regular graph, I–II, *Europ. J. Combin.* 16 (1995), 589–602, 603–615.

[5] A. A. Ivanov, Bounding the diameter of a distance-regular graph, *Soviet Math. Doklady* 28 (1983), 149–153.

[6] A. V. Ivanov., *Problem*, pp. 240-241 in *Algebraic, Extremal and Metrics Combinatorics, 1986* London Math. Soc. Lecture Note Ser. 131 (M-M. Deza, P. Frankl & I.G. Rosenberg, eds.) Cambridge Univ. Press, Cambridge, 1988.

[7] J. H. Koolen, On subgraphs in distance-regular graphs, *J. Algebraic Combin.* 1 (1992), 353–362.

On association schemes with a nonsymmetric relation of valency 4

Mitsugu Hirasaka

1997.11.13

Abstract

Let (X,G) be a primittive commutative association scheme with a nonsymmetric relation of valency 4. Then the cardinality of X is a prime to the third.

1 Introduction

Let (X,G) be a primitive commutative association scheme. The following results are obtained until now.

1) $\exists g \in G^{\times}$ s.t. $k_g = 1 \Rightarrow |X| = p$ where p is a prime.
2) $\exists g \in G^{\times}$ s.t. $k_g = 2 \Rightarrow |X| = p$ where p is an odd prime.
3) $\exists g \in G^{\times}$ s.t. $k_g = 3 \Rightarrow |X| = p \equiv 1(3), p^2$ where p is an odd prime more than 3, $|X| = 4, 10, 28, 102$ if $g = g^*$.

Although it is trivial to prove 1), 2), it is rather difficult to prove 3), whose proof is given by N. Yamazaki (See [11]) when $g = g^*$, and by the author (See [9]) when $g \neq g^*$.

In this paper, we treat the case that there exists $g \in G$ such that $k_g = 4$, $g \neq g^*$. The following is the main theorem, which in particular gives a restriction on the X.

Theorem 1.1 *Let (X,G) be a primitive commutative association scheme with a nonsymmetric relation of valency 4, denoted by g. Then the graph (X,g) is isomorphic to the cubical graph, which is described in Example 2.11.*

2 Preliminaries

Definition 2.1 (Association scheme) Let X be a finite set and G be a partition of $X \times X$, not containing the empty set. The pair (X, G) is called *an association scheme* if the following conditions $i), ii), iii)$ hold;

$i)$ $1_X := \{(x,x) | x \in X\} \in G$

$ii)$ $\forall g \in G, \;\; g^* := \{(x,y) | (y,x) \in g\} \in G$

$iii)$ $\forall g, h, l \in G, \forall x, y \in X$ with $(x,y) \in l$,
$|\{z \in X | (x,z) \in g, (z,y) \in h\}|$ depends only on g, h, l. We denote it by p^l_{gh}, which is called *an intersection number*.
(X, G) is said to be *commutative* if it satisfies condition $iv)$;

$iv)$ $\forall g, h, l \in G, p^l_{gh} = p^l_{hg}$.
(X, G) is said to be *symmetric* if it satisfies condition $v)$;

$v)$ $\forall g \in G, g^* = g$.

For each element $g \in G$, we define the adjacency matrix A_g whose entries are indexed by elements of X as follows;

$$(A_g)_{xy} := \begin{cases} 1 & \text{if } (x,y) \in g \\ 0 & \text{otherwise} \end{cases}$$

Note that there exists a one-to-one correspondence between G and $\{A_g\}_{g \in G}$. Using adjacency matrices, we can express the conditions $i), \cdots, v)$ as follows;

$i)'$ $A_{1_X} = I$ where I is the identity matrix.

$ii)'$ $\forall g \in G, \exists g^* \in G$ s.t. $A_g \;= A^t_g$.

$iii)'$ $\forall g, h \in G, A_g A_h = \sum_{l \in G} p^l_{gh} A_l$

$iv)'$ $\forall g, h \in G, A_g A_h = A_h A_g$.

$v)'$ $\forall g \in G, A^t_g = A_g$.

From now on we identify A_g with g for each $g \in G$ for convenience, and denote the ordinary product of matrices A, B by $A \bullet B$ in order to avoid confusions.

Definition 2.2 Let (X, G) be an association scheme. Let $\mathcal{A}$ be a subalgebra spanned by $\{g | g \in G\}$ of the full matrix algebra of order $|X|$ over complex field. We call $\mathcal{A}$ *the Bose-Mesner algebra* of (X, G).

Definition 2.3 We call an element g of G *a relation*, and *a symmetric relation* if $g^* = g$, *a nonsymmetric relation* if $g^* \neq g$.

Definition 2.4 For each subsets E, F of G, we define

$$EF := \{g \in G | \sum_{e \in E} \sum_{f \in F} p_{ef}^{g} \neq 0\}.$$

In particular, for each $e, f \in G$, we denote $\{e\}\{f\}$ by ef.

Definition 2.5 For each $g \in G$ and $x \in X$, we define $xg := \{y | (x, y) \in g\}$.

Remark 2.6 $\{z \in X | (x, z) \in g, (z, y) \in h\} = xg \cap yh^*$

Definition 2.7 For each $g \in G$, we define $k_g := p_{gg}^{1_X}$, which is called *the valency* of g.

Note $k_g = k_g$ and $k_g = |xg|$ for each $x \in X$.

Definition 2.8 Let V be a finite set and $E \subset V \times V$. We call the pair (V, E) *a graph.*

Definition 2.9 A graph (V, E) is *connected* if, for each $u, v \in V$, there exist $v_0 = u, v_1, \cdots, v_t = v \in V$ such that $(v_i, v_{i+1}) \in E$ for all i with $0 \leq i \leq t-1$.

Definition 2.10 Let (X, G) be an association scheme. We say that (X, G) is *primitive* if the graph (X, g) is connected for each $g \in G^\times := G - 1_X$.

Example 2.11 Let F_p be a finite field of order p where p is an odd prime. We define permutations on F_p^3 as follows;

1) Let S_3 be the symmetric group of degree 3. For each $(x_1, x_2, x_3) \in F_p^3$ and $\sigma \in S_3$,

$$(x_1, x_2, x_3)^\sigma := (x_{\sigma^1 (1)}, x_{\sigma^1 (2)}, x_{\sigma^1 (3)}).$$

2) For each $(x_1, x_2, x_3) \in F_p^3$,

$$(x_1, x_2, x_3)^\tau := (-x_1, x_2 - x_1, x_3 - x_1).$$

3) For each $u, v \in F_p^3$,
$$u^v = u + v.$$

Then the permutation group $\Gamma := < S_3, \tau, F_p^3 >$ acts on F_p^3 transitively, and Γ acts on $F_p^3 \times F_p^3$ by $(u,v)^g := (u^g, v^g)$ where $(u,v) \in F_p^3 \times F_p^3, g \in \Gamma$. Let G be the set of orbits of Γ on $F_p^3 \times F_p^3$. Then (F_p^3, G) is an association scheme (See [2, 52]), and it can be verified that (F_p^3, G) is a primitive commutative association scheme with a nonsymmetric relation of valency 4. Indeed, the orbit g containing $((0,0,0),(1,0,0))$ is a nonsymmetric relation of valency 4.

Definition 2.12 Let (X, G) be an association scheme, and $x, y \in X$. We denote the element of G containing (x,y) by $r(x,y)$.

Lemma 2.13 *Let (X,G) be an association scheme. For each $g, h, l \in G$, we have the following;*

(*i*) $k_g k_h = \sum_{l \in G} p_{gh}^l k_l$.

(*ii*) $p_{gh}^l k_l = p_{lh}^g\ k_g = p_{g\ l}^h k_h$.

Proof. See [2, 56].

Definition 2.14 Let (X, G) be an association scheme, and $\mathcal{A}$ be the Bose-Mesner algebra of (X, G). We denote the inner product on $\mathcal{A}$ by $(\ ,\ )$ which has an orthogonal basis $\{g | g \in G\}$ and $(g, g) := k_g$ for each $g \in G$.

Remark 2.15 *Let (X,G) be an association scheme. For each $g, h, l \in G$, we have $(g \bullet h, l) = (g, h^* \bullet l)$ by Lemma 2.13(ii).*

Lemma 2.16 *Let (X,G) be an association scheme. For each $g, h, l \in G$, we have the following;*

(*i*) $\mathrm{lcm}(k_g, k_h) | p_{gh}^l k_l$ *where* $\mathrm{lcm}(k_g, k_h)$ *is the least common multiplier of* k_g *ang* k_h.

(*ii*) $\gcd(k_g, k_h) \geq |gh|$ *where* $\gcd(k_g, k_h)$ *is the greatest common divisor of* k_g *ang* k_h.

Proof. See [3].

3 Outline of the proof

We assume that (X, G) is a primitive commutative association scheme with a nonsymmetric relation of valency 4, and assume

$$\min_{g \in G} k_g = 4. \tag{1}$$

We give some propositions without proof.

Proposition 3.1 *For each $g \in G$ with $k_g = 4$ and $g^* \neq g$, there exist $a, b, f, h, m \in G$ such that*

1) $g \bullet g = 2a + b, k_a = 6, k_b = 4.$

2) $g \bullet g^* = 4 \cdot 1_X + h, k_h = 12.$

3) $a \bullet a^* = 6 \cdot 1_X + 2h + f, k_f = 6.$

4) $a = a^*, g \bullet a = 3g^* + m, k_m = 12.$

5) $ga \cap gb = \{m\}.$

Definition 3.2 A sequence $(x_0, x_1, \cdots, x_n)$ is *a chain* if $(x_i, x_{i+1}) \in g$ for all i with $0 \leq i \leq n-1$ and $(x_i, x_{i+2}) \in b$ for all i with $0 \leq i \leq n-2$.

For all $n \geq 2$, if $(x_0, x_1, \cdots, x_n)$ is a chain then there exists a unique $x_{n+1} \in X$ such that $(x_0, x_1, \cdots, x_n, x_{n+1})$ is also a chain by $p^g_{bg} = p^b_{gg} = 1$. Moreover, we can construct a closed chain $(x_0, x_1, \cdots, x_n = x_0)$ for enough large n since $|X|$ is finite.

Proposition 3.3 *If both $(x_0, x_1, \cdots, x_i)$ and $(y_0, y_1, \cdots, y_i)$ are chains then $r(x_0, x_n) = r(y_0, y_i)$ for each i with $2 \leq i \leq n$.*

Let $o \in X$. We define $og := \{x(1,0,0), x(0,1,0), x(0,0,1)\}$. For fixed pair $(o, x(1,0,0))$, there exists a unique minimal closed chain

$$(o, x(1,0,0), x(2,0,0), \cdots, x(n,0,0) = o).$$

Similarly, there exists a unique minimal closed chain

$$(o, x(0,1,0), x(0,2,0), \cdots, x(0,n,0) = o).$$

By Proposition 3.1, there exist a unique element in $x(1,0,0)g \cap x(0,1,0)g$, and denote it by $x(1,1,0)$. Inductively, we define $x(i+1,1,0)$ to be a unique elment in $x(i,1,0)g \cap x(i+1,0,0)g$. It follows from Proposition 3.3 $x(n,1,0) = x(0,1,0)$. Moreover, we define $x(i+1,2,0)$ to be a unique elment in

$$x(i,2,0)g \cap x(i+1,1,0)g$$

and

$$(x(0,2,0), x(1,2,0), \cdots, x(n,2,0))$$

is also a chain by the same arugment as above. Inductively, we define

$$(x(0,j,0), x(1,j,0), \cdots, x(n,j,0) = x(0,j,0))$$

to be a chain defined $x(i+1,j,0)$ to be a unique elment in $x(i,j,0)g \cap x(i+1,j,0)g$ for all i,j with $0 \leq i,j \leq n-1$. Thus, we can define all elements $x(i,j,0)$ with $0 \leq i,j \leq n-1$. Next, we define $x(i,j,k)$ with $0 \leq i,j,k \leq n-1$ where $x(0,0,0) = o$ by starting to construct a chain

$$(o, x(0,0,1), \cdots, x(0,0,n))$$

and construct all plane, which is the set of $x(i,j,k)$ with $0 \leq i,j \leq n-1$, for each k.

Lemma 3.4 $|\{x(i,j,k) | 0 \leq i,j,k \leq n-1\}| = n^3$.

Proof of the Main Theorem. We may assume that n is an odd prime, if necessarily, because we can construct another closed chain with respect $r(o, x(i,0,0))$ where i is a maximal divisor of n by Proposition 3.1 and 3.3. It follows from Lemma 3.4 that

$$(\{x(i,j,l) | 0 \leq i,j,l \leq n-1\}, g)$$

is isomorphic to the graph given in Example 2.11.

References

[1] Z.Arad, E.Fisman, V.Miloslavsky, M.Muzychuk, On antisymmetric homogeneous integer table algebras, preprint.

[2] E.Bannai and T.Ito, Algebraic Combinatorics I:Association schemes, Benjamin/Cummings, Menlo Park, CA, 1984.

[3] H.I. Blau, Integral Table Algebras, Affine Diagrams, Analysys of Degree Two, J. Algebra 178, 872-918 (1995)

[4] H.I. Blau, On Table Algebras and Applications to Finite Group Theory, J. Algebra 138, 137-185 (1991)

[5] A.E.Brouwer, A.M.Cohen and A.Neumaier, Distance Regular Graphs, Springer-Verlag,1989.

[6] C.D.Godsil, Algebraic Combinatorics, Champman and Hall Mathematics

[7] M.Hall, Jr. Combinatorial Theory, second edition, A Wiley-Interscience Publication.

[8] Akihide Hanaki and Izumi Miyamoto, private communication.

[9] H. Hirasaka, Association schemes with aprime number of points, 1997, preprint.

[10] E.Nomiyama, Classification of association schemes with at most ten vertices, Kyushu J. of Math.49(1995),163-195.

[11] N.Yamazaki, On Symmetric Association Schemes with $k_1 = 3$, 1995, preprint.

A new cover of the 3-local geometry of Co_1

A.A. Ivanov and S. Shpectorov*

Abstract

The 3-local geometry $\bar{\mathcal{G}} = \mathcal{G}(Co_1)$ of the sporadic simple group Co_1 has been known to have a cover $\hat{\mathcal{G}} = \mathcal{G}(2^{24} \cdot Co_1)$ with a flag-transitive automorphism group which is a non-split extension of an elementary abelian 2-group of rank 24 (the Leech lattice modulo 2) by Co_1. It was conjectured that $\hat{\mathcal{G}}$ was simply connected. We disprove this conjecture by constructing a double cover $\mathcal{G}$ of $\hat{\mathcal{G}}$. The automorphism group of $\mathcal{G}$ is of the shape $2_+^{1+24} \cdot Co_1$; however, it is not isomorphic to the involution centralizer of the Monster sporadic simple group.

1 Introduction

We follow the standard terminology concerning diagram geometries and their automorphism groups (cf. [Bue], [Pas]). In [Ron] the problem of finding the universal covers of certain geometries of sporadic groups was considered. The geometry $\bar{\mathcal{G}} = \mathcal{G}(Co_1)$, the 3-local geometry of the Conway group Co_1, is the only geometry from [Ron] for which the universal cover still remains unknown.

First of all, let us describe $\bar{\mathcal{G}}$. Consider the conjugacy class $\bar{\mathcal{C}}$ of subgroups of order 3 in Co_1 generated by the Suzuki 3-elements (class 3A in [Atl]). We say that a set of subgroups from $\bar{\mathcal{C}}$ is *commutative* if the subgroups centralize each other, *i.e.*, if they generate an elementary abelian 3-group. The group Co_1 is transitive on commutative sets of size i, for $i = 1$, 2, 3 and 4. Furthermore, every commutative 4-set is contained in a unique

*This author would like to thank the Martin-Luther-Universität Halle-Wittenberg for the hospitality.

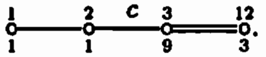
maximal commutative set. The maximal commutative sets are, therefore, all conjugate. They are known to consist of 12 subgroups, and the normalizer of a maximal commutative set induces on it a Mathieu group M_{12} acting naturally.

The geometry $\bar{\mathcal{G}}$ has rank 4 and consists of all the commutative 1-, 2-, 3- and 12-sets. The incidence on $\mathcal{G}$ is defined by inclusion. It easily follows from the above that Co_1 acts on $\bar{\mathcal{G}}$ flag-transitively. The maximal parabolics related to the action of Co_1 on $\mathcal{G}$ are maximal 3-local subgroups of $\bar{G} = Co_1$, having the structure as follows:

$$\bar{G}_1 \cong 3 \cdot Suz.2; \quad \bar{G}_2 \cong 3^2 \cdot U_4(3).D_8;$$

$$\bar{G}_3 \cong 3^{3+4}.2.(S_4 \times S_4); \quad \bar{G}_{12} \cong 3^6 : 2 \cdot M_{12}.$$

The diagram of $\bar{\mathcal{G}}$ is the following:



For various purposes it is convenient to study $\bar{\mathcal{G}}$ in terms of a graph $\bar{\Gamma}$ associated with $\bar{\mathcal{G}}$. The vertex set of $\bar{\Gamma}$ is $\bar{C}$; two vertices-subgroups are adjacent if and only if they commute. Then the elements of $\bar{\mathcal{G}}$ are the vertices, the edges of $\bar{\Gamma}$, as well as all the 3- and 12-cliques of $\bar{\Gamma}$.

Let $\varphi : \Gamma \rightarrow \bar{\Gamma}$ be a covering of graphs such that every 3-cycle from $\bar{\Gamma}$ lifts in Γ to a disjoint union of 3-cycles. Equivalently, φ has the property that it preserves the local structure, that is, for every $x \in \Gamma$, φ establishes an isomorphism between the subgraph of Γ induced on the neighbourhood of x and the subgraph of $\bar{\Gamma}$ induced on the neighbourhood of $\varphi(x)$. Define a geometry $\mathcal{G}$ whose elements are all the vertices, edges, 3- and 12-cliques of Γ. Then, quite clearly, φ induces a covering from $\mathcal{G}$ onto $\bar{\mathcal{G}}$. Reversely, given a covering $\mathcal{G} \longrightarrow \bar{\mathcal{G}}$, one can define a graph Γ using the elements of $\mathcal{G}$ of type 1 as vertices, and the elements of type 2 as edges. Then the covering of geometries induces a covering of graphs $\Gamma \longrightarrow \bar{\Gamma}$ and the latter covering preserves the local structure.

Thus, $\bar{\mathcal{G}}$ (or any its cover $\mathcal{G}$) is simply connected if and only if the fundamental group of $\bar{\Gamma}$ (respectively, Γ) is generated by 3-cycles. It was shown in [Asc] that the fundamental group of $\bar{\Gamma}$ is generated by its 3- and 4-cycles. This is, in a sense, the best possible generation result for $\bar{\Gamma}$ because, in fact, the fundamental group of $\bar{\Gamma}$ is not generated by the 3-cycles alone. The geometry $\bar{\mathcal{G}}$ does have a nontrivial cover; this cover appears as a subgeometry in the 3-local geometry of the Monster (cf. [Ivn]) and can be described as follows. Let $\hat{G}$ be the quotient over its center of the centralizer of a central involution in the Monster. Then $\hat{G} \cong 2^{24} \cdot Co_1$, $O_2(\hat{G})$ is isomorphic to the Leech lattice modulo 2, and $\hat{G}$ does not split over $O_2(\hat{G})$. The definition of the new geometry, $\hat{\mathcal{G}}$, is similar to the definition of $\bar{\mathcal{G}}$ with the only difference that we take $\hat{G}$ in place of $\bar{G}$. Let $\hat{\mathcal{C}}$ be the conjugacy class of subgroups of order 3 in $\hat{G}$ that maps onto $\bar{\mathcal{C}}$ under the natural homomorphism of $\hat{G}$ onto $\bar{G}$. Then the elements of $\hat{\mathcal{G}}$ are all the commutative subsets of $\hat{\mathcal{C}}$ of size 1, 2, 3 and 12, and the incidence is defined by inclusion. Since the Suzuki 3-elements act fixed point freely on the Leech lattice modulo 2 and since $\hat{G}$ does not split over $O_2(\hat{G})$, it is straightforward that $\hat{\mathcal{G}}$ is a 2^{24}-fold cover of $\mathcal{G}$.

It has already been mentioned that $\hat{\mathcal{G}}$ is a subgeometry in the 3-local geometry $\mathcal{H}$ of the Monster. The geometry $\mathcal{H}$ was proved to be simply connected in [IMe]. An important step in the proof was to show that the universal cover of $\mathcal{H}$ also contained a copy of $\hat{\mathcal{G}}$. If an argument existed, showing that $\hat{\mathcal{G}}$ was simply connected, it would lead to a considerable simplification in the proof of [IMe]. In reality, however, $\hat{\mathcal{G}}$ is not simply connected, as our main result demonstrates.

Theorem 1 *The geometry $\hat{\mathcal{G}} = \mathcal{G}(2^{24} \cdot Co_1)$ possesses a flag-transitive double cover $\mathcal{G}$. The automorphism group G of $\mathcal{G}$ is of the form $2_+^{1+24} \cdot Co_1$ and G is not isomorphic to the central involution centralizer of the Monster sporadic simple group.*

What is the universal cover of $\bar{\mathcal{G}}$? We hope for the best and conjecture that the new geometry *is* the universal cover of $\bar{\mathcal{G}}$.

Notice that our argument for Theorem 1 demonstrates also the uniqueness of $\mathcal{G}$ provided that the covering $\mathcal{G} \longrightarrow \hat{\mathcal{G}}$ comes from a group homomorphism $G \longrightarrow \hat{G}$. Using the classification by T. Meixner of the parabolic systems corresponding to the diagram of $\hat{\mathcal{G}}$, one can prove that, in fact, every flag-transitive double cover arrives from a group homomorphism. Thus, indeed, $\mathcal{G}$ is unique.

2 The group G

In order to construct the graph Γ covering $\hat{\Gamma}$, we shall define a group G having a surjective homomorphism φ onto $\hat{G}$, and two subgroups G_1 and G_2 of G, the vertex stabilizer and the edge stabilizer. Certain conditions must be satisfied. First of all, $|G_2 : G_1 \cap G_2| = 2$ must hold. Secondly, since φ should induce a covering from Γ onto $\hat{\Gamma}$, we need that G_1 and G_2 map isomorphically onto the subgroups $\hat{G}_1$ and $\hat{G}_2$, the stabilizers of incident vertex and edge of $\hat{\Gamma}$. In turn, $\hat{G}_1$ and $\hat{G}_2$ map isomorphically onto $\bar{G}_1$ and $\bar{G}_2$, hence

$$G_1 \cong \hat{G}_1 \cong \bar{G}_1 \cong 3 \cdot Suz.2$$

and

$$G_2 \cong \hat{G}_2 \cong \bar{G}_2 \cong 3^2 \cdot U_4(3).D_8.$$

We want φ to be a double cover, so G should be an extension of a normal (hence, central) subgroup of order 2 by $\hat{G} \cong 2^{24} \cdot Co_1$. If G is not perfect, that is, if $G' < G$, then the maximal parabolic $G_{12} \cong 3^6 : 2 \cdot M_{12}$ is fully contained in G'. Furthermore, $G_1 = G_1'(G_1 \cap G_{12})$ is also contained in G'. This clearly contradicts the connectedness of the geometry, since G has to coincide with $\langle G_1, G_{12} \rangle$. Thus, we require that G be perfect—a perfect central extension of $\hat{G}$.

The Schur multiplier of $\hat{G}$ is elementary of order 4 (see [Gri]). The universal central extension $\tilde{G}$ of $\hat{G}$ can be constructed as a subdirect product of the centralizer in the Monster group of its central involution (structure $2^{1+24} \cdot Co_1$) with $Co_0 \cong 2 \cdot Co_1$, the automorphism group of the Leech lattice. Hence $\tilde{G} \cong 2^2.2^{24} \cdot Co_1 \cong 2^{1+24} \cdot Co_0$. In particular, for $O_2(\tilde{G})$ we have the structure $2 \times 2^{1+24}$. Therefore, $Z = Z(\tilde{G}) \cong 2^2$ contains a unique involution z such that $O_2(\tilde{G}/\langle z \rangle)$ is abelian. If y is either of the remaining two involutions, then $\tilde{G}/\langle y \rangle$ has structure $2^{1+24} \cdot Co_1$; and we have our first dilemma: *which of these two quotients should we take as G?*

We follow the terminology of the introduction and call a subgroup of order 3 (in $\tilde{G}$, G, $\hat{G}$, or $\bar{G}$) a *Suzuki 3-subgroup* if its image (the subgroup itself, in case of $\bar{G}$) in $\bar{G} \cong Co_1$ is generated by a Suzuki 3-element. Let $\tilde{X} \leq \tilde{G}$ be the Suzuki 3-subgroup whose image in $\hat{G}$ is the vertex of $\hat{\Gamma}$ stabilized by $\hat{G}_1$. (Notice that since $\tilde{G}$ is a central extension of $\hat{G}$, every Suzuki 3-subgroup from $\hat{G}$ lifts to a unique Suzuki 3-subgroup in $\tilde{G}$. The same applies to G when we define it.) Then $\tilde{N} = N_{\tilde{G}}(\tilde{X})$ is the full preimage of $\hat{G}_1$ in

$\tilde{G}$, *i.e.*, $\tilde{C}$ is an extension of Z by $\hat{G}_1 \cong 3 \cdot Suz.2$. What extension is this? It is well-known that the centralizer of the Suzuki 3-element in Co_0 is the universal perfect extension $6 \cdot Suz$ of the Suzuki sporadic group Suz. This implies that the commutator subgroup $\tilde{N}'$ of $\tilde{N}$ is also isomorphic to $6 \cdot Suz$. Therefore, Z contains a unique involution y (the one in $Z \cap \tilde{N}'$!) such that $\tilde{N}/\langle y \rangle$ contains a subgroup $3 \cdot Suz$ rather than $6 \cdot Suz$. We have that $y \neq z$, because $\tilde{G}/\langle z \rangle \cong 2^{24} \cdot Co_0$ contains $6 \cdot Suz$ since Co_0 does.

Thus, we have established the following

Lemma 2.1 *The group $\tilde{G}$ has a unique quotient $G \cong 2^{1+24} \cdot Co_1$ such that the normalizer in G of a Suzuki 3-subgroup contains a subgroup $3 \cdot Suz$.* □

This quotient is the one that we should take if we want to construct a cover of $\hat{\Gamma}$. Indeed, the subgroup G_1 of G should map isomorphically onto $\hat{G}_1$. Therefore, the full preimage of $\hat{G}_1$ in G must at least contain a subgroup $3 \cdot Suz$.

¿From now on, the group G is as in Lemma 2.1. We mentioned in the introduction that our G is not isomorphic to the involution centralizer in the Monster. Indeed, it is well-known that the centralizer of the central involution in M, though having a similar structure, does contain $6 \cdot Suz$. Hence the centralizer is the remaining—third—quotient of $\tilde{G}$.

3 The vertex stabilizer G_1

The group G is now known and we proceed by defining the vertex stabilizer G_1.

Let X be the Suzuki 3-subgroup of G whose image in $\hat{G}$ is the vertex of $\hat{\Gamma}$ stabilized by $\hat{G}_1$. The subgroup G_1 should map onto $\hat{G}_1$ isomorphically, hence G_1 must be a complement to $Z = Z(G)$ in $N = N_G(X)$, which is the full preimage of $\hat{G}_1$ in G. Our next goal is, therefore, to show that N is the direct product $2 \times 3 \cdot Suz.2$.

We know already that $N' \cong 3 \cdot Suz$; it remains to see that that $N/N' \cong 2^2$, *i.e.*, it is not cyclic. Our goal will be accomplished if we find an involution inverting X. By Lemma 2.1, $C_G(X) \cong 2 \times 3 \cdot Suz$. The second factor of this direct product maps isomorphically onto its image in $\bar{G}$. This gives us control over the orders of some 2-elements of G.

Lemma 3.1 *If a 2-element $g \in G \setminus Z(G)$ centralizes a Suzuki 3-subgroup then the order of g is equal to the order of its image in $\bar{G}$.* □

Let $Y \neq X$ be a Suzuki 3-subgroup commuting with X. Consider the images of X, Y and N in $\bar{G}$.

Lemma 3.2 *There exists an involution $\bar{t} \in \bar{N}$ inverting $\bar{X}$ and centralizing $\bar{Y}$.*

Proof: By symmetry, it suffices to find an involution centralizing $\bar{X}$ and inverting $\bar{Y}$. Let $S = C_{\bar{G}}(\bar{X})/\bar{X} \cong Suz$ and let $U = \bar{X}\bar{Y}/\bar{X}$ be the image of $\bar{Y}$ in S. It is known (cf. [Atl]) that all the order 3 elements in Suz are rational, that is, each element of order 3 is conjugate to its inverse. In particular, $D = N_S(U) \cong 3 \cdot U_4(3).2_3$ contains an element inverting U. This means that every element in D outside D' inverts U. Finally, by checking the page of [Atl] concerning $U_4(3)$, we see that $U_4(3).2_3$ contains involutions (class 2F) outside the commutator subgroup.

This establishes that $C_{\bar{G}}(\bar{X})$ contains an involution $\bar{t}$ normalizing $\bar{X}\bar{Y}$ and acting on it nontrivially. Since $\bar{X}$ and $\bar{Y}$ are the only Suzuki 3-subgroups in $\bar{X}\bar{Y}$ (otherwise, $\bar{G}$ cannot be transitive on triples of commuting Suzuki 3-subgroups!), $\bar{t}$ has to normalize and invert $\bar{Y}$. □

Corollary 3.3 *There is an involution $t \in G$ inverting X and centralizing Y. In particular, $N \cong 2 \times 3 \cdot Suz.2$.*

Proof: Indeed, by Lemma 3.2, there exists $\bar{t} \in \bar{N}$ inverting $\bar{X}$ and centralizing $\bar{Y}$. Let $t \in N$ be in the preimage of $\bar{t}$. Then t inverts X and centralizes Y. Furthermore, by Lemma 3.1, t is an involution. □

We now know that N splits over Z and that, therefore, there are subgroups that map isomorphically onto $\hat{G}_1$. We face, however, a new dilemma: there are two such subgroups. One of them is $C_1 = N'\langle t\rangle$, where t is as in Corollary 3.3, and the other one is $C_2 = N'\langle tz\rangle$, where, of course, z is the involution from Z. (Indeed, N' must be contained in every complement. The elements t and tz represent the two cosets from $N/N' \cong 2^2$ that do not contain z.) *Which of these two complements, C_1 or C_2, must we choose as G_1?*

Without loss of generality we may assume that $\hat{X}$ and $\hat{Y}$, the images of X and Y in $\hat{G}$, make the edge of $\hat{\Gamma}$, stabilized by $\hat{G}_2$. Let K be the full preimage of $\hat{G}_2$ in G. Suppose we have chosen our subgroups G_1 and G_2. Then, first of all, $G_1 \cap K = G_1 \cap G_2$, since $G_1 \cap G_2$ maps onto $\hat{G}_1 \cap \hat{G}_2$ and G_1 does not contain z. Secondly, $G_1 \cap G_2$ is of index 2 in G_2 and hence it is normal in G_2. As $K = \langle z, G_2 \rangle$, we obtain that $G_1 \cap K = G_1 \cap G_2$ is normal in K. This is how we can distinguish C_1 and C_2. Namely, we claim that the following is true.

Lemma 3.4 *The subgroup $C_i \cap K$ is normal in K for one and only one index $i = 1$ or 2.*

Proof: Let K_0 be the index 2 subgroup of K that normalizes both X and Y. Fix $r \in K \setminus K_0$, so that $X^r = Y$ and $Y^r = X$. The subgroup K_0^∞ is isomorphic to $3^2 \cdot U_4(3)$ and hence it has index 8 in K_0. Clearly, K_0^∞ centralizes both X and Y. Since z also centralizes X and Y, t centralizes Y and inverts X, and $s = t^r$ centralizes X and inverts Y, we conclude that $W = \bar{K}_0 = K_0/K_0^\infty$ is generated by the cosets $\bar{z}$, $\bar{t}$ and $\bar{s}$, and hence W is elementary abelian.

Notice that r acts on W as an involution and that $[W, r] = \langle \bar{t}\bar{s} \rangle$ is of order 2. For $i = 1, 2$, the subgroup $C_i \cap K$ is contained in K_0 and has index 2 in it; $C_i \cap K$ is normal in K if and only if the image U_i of $C_i \cap K$ in W is invariant under r. Since U_i is of order 4, it is invariant under r if and only if U_i contains $[W, r]$.

The subgroup $C_1 \cap C_2 = N'$ consists of all those elements of C_i that centralize X. It follows that the image $U = U_1 \cap U_2$ of $C_1 \cap C_2 \cap K$ in W is of order 2 and, if $U = \langle u \rangle$, then u is one of the cosets $\bar{s}$, or $\bar{s}\bar{z}$. (Both s and sz centralize X. Therefore, one of them is contained in N'.) The group $W \cong 2^3$ contains three subgroups of order 4, containing U; one of them is $\langle u, \bar{z} \rangle = \langle \bar{s}, \bar{z} \rangle$, the other two are U_1 and U_2. One and only one of these three subgroups contains $[W, r] = \langle \bar{t}\bar{s} \rangle$ and that is not $\langle \bar{s}, \bar{z} \rangle$. Hence, one and only one U_i is invariant under r, and one and only one $C_i \cap K$ is normal in K. □

In accordance with the discussion before Lemma 3.4, we set $G_1 = C_i$, where C_i is defined by the condition that $C_i \cap K$ is normal in K.

4 The edge stabilizer G_2

We have our graph Γ defined when we specify G_2, the edge stabilizer. The subgroup G_2 should contain $R = G_1 \cap K = G_1 \cap G_2$ and the index of R

in G_2 should be 2. Furthermore, G_2 should isomorphically map onto $\hat{G}_2$, which means that G_2 must complement Z in K. In particular, K/R must be elementary of order 4, rather than cyclic of the same order.

To check that K/R is not cyclic, it suffices to see that $K \setminus K_0$ contains an involution. (Recall that K_0, the joint normalizer of X and Y, is equal to $\langle z \rangle R$.) Clearly, such an involution would interchange X and Y. First we consider the images of X and Y in $\bar{G}$.

Lemma 4.1 *Suppose $\bar{V}$ is a Suzuki 3-subgroup in $\bar{G}$, which centralizes both $\bar{X}$ and $\bar{Y}$. Then there exists an involution $\bar{r}$ that centralizes $\bar{V}$ and interchanges $\bar{X}$ and $\bar{Y}$.*

Proof: Without loss of generality we may assume that $\bar{X}$, $\bar{Y}$ and $\bar{V}$ are contained in the maximal commutative subset Σ normalized by $\bar{G}_{12}$. Notice that the twelve subgroups from Σ generate $O_3(\bar{G}_{12})$, and they are the only Suzuki 3-subgroups contained in $O_3(\bar{G}_{12})$. The group $F = \bar{G}_{12}/O_3(\bar{G}_{12}) \cong 2 \cdot M_{12}$ acts on Σ 5-transitively and $Z(F)$ inverts each subgroup in Σ. This shows that $N_F(\bar{V}) \cong 2 \times M_{11}$ and $C_F(\bar{V}) \cong M_{11}$. Let $\bar{r}$ be an involution in the preimage of $C_F(\bar{V})$ in $\bar{G}_{12}$. Since $F/Z(F) \cong M_{12}$ acts faithfully on Σ, $\bar{r}$ has on Σ at least one orbit of length 2. By the 5-transitivity, we can assume that $\bar{r}$ interchanges $\bar{X}$ and $\bar{Y}$. □

As a corollary, we obtain the following.

Lemma 4.2 *There exists an involution $r \in K$ interchanging X and Y. In particular, $K/R \cong 2^2$ and K splits over Z.*

Proof: Let V be a Suzuki 3-subgroup in G that centralizes both X and Y. Then, by Lemma 4.1, there is an involution $\bar{r}$ in $\bar{G}$ that centralizes $\bar{V}$ and interchanges $\bar{X}$ and $\bar{Y}$. Pick r in the preimage of $\bar{r}$ in K. Then r has to centralize V and hence, by Lemma 3.1, it is an involution. Also, clearly, r interchanges X and Y. □

Since $K/R \cong 2^2$ there are two subgroups, $T_1 = R\langle r \rangle$ and $T_2 = R\langle rz \rangle$, that contain R and complement Z. Thus, we again have a binary choice: *which of the two complements T_i should we take as G_2?*

Notice that, for both our choices of G_2, thus defined graph Γ covers $\hat{\Gamma}$. We claim that one and only one of these two coverings preserves the local structure.

Suppose we have chosen $G_2 = T_i$ for some $i = 1$ or 2. How can we see whether this covering preserves the local structure? We need to check that every 3-cycle from $\hat{\Gamma}$ lifts in Γ to a pair of 3-cycles, rather than a 6-cycle. The group $\hat{G}$ is transitive on the vertices of $\hat{\Gamma}$ and $\hat{G}_1$ acts transitively on (ordered) pairs of ajacent neighbours of the vertex it stabilizes, which is simply $\hat{X}$. By construction, similar properties hold for Γ, G and G_1. This means we only need to check whether one particular 3-cycle from $\hat{\Gamma}$ lifts in Γ to (a pair of) 3-cycles. We choose, as this one particular cycle, the cycle formed by the commutative set $\hat{C} = \{\hat{X}, \hat{Y}, \hat{V}\}$, where $\hat{V}$ is the preimage in $\hat{G}_1$ of $\bar{V}$ from Lemma 4.1.

Let $\hat{Q}$ be the elementwise stabilizer in $\hat{G}$ of $\hat{C}$. Let $\hat{a} \in \hat{G}_1$ be an element that interchanges $\hat{Y}$ and $\hat{V}$. Let also $\hat{b} \in \hat{G}_2$ be an element that stabilizes $\hat{V}$ and interchanges $\hat{X}$ and $\hat{Y}$. For simplicity, we take $\hat{b} = \hat{r}$, where r is as above. Clearly, $\langle \hat{a}, \hat{b} \rangle$ induces S_3 on $\hat{C}$ and $(\hat{a}\hat{b})^3 \in \hat{Q}$. Let Q and a be the preimages in G_1 of $\hat{Q}$ and $\hat{a}$, respectively. Let also b be the preimage in G_2 of $\hat{b}$. (Since $\hat{b} = \hat{r}$, we have $b = r$, or rz depending on whether $i = 1$, or 2.)

Let $x \in \Gamma$ be one of the two liftings of $\hat{X}$ and let y and v be the neighbours of x that map onto Y and V, respectively. Then G_1 is the stabilizer of x and G_2 is the stabilizer of the edge $\{x, y\}$. In particular, both a and b have to stabilize the connected component of the preimage of the cycle $\bar{C}$, that contains x, y and v. If the preimage of C is a pair of 3-cycles then one of them is induced by x, y and v. In this case $(xy)^3$ is in Q which is the joint stabilizer of x, y and v. On the other hand, if the preimage of $\hat{C}$ is a 6-cycle then $\langle a, b \rangle$ induces on it the full group D_{12}. (Indeed, a flips this cycle around x, while b flips it around the edge $\{x, y\}$!) Hence, in the second case $(xy)^3$ is not in Q. We arrive to the following conclusion: the covering from Γ onto $\hat{\Gamma}$ preserves the local structure if and only if $(xy)^3$ is in Q.

Lemma 4.3 *For one and only one choice of $G_2 = T_i$ does the covering $\Gamma \longrightarrow \hat{\Gamma}$ preserve the local structure.*

Proof: The group G_1 is the same for both choices of i, so the meaning of Q and a does not depend on $i = 1$ or 2. On the other hand $b = r$ for $i = 1$, and rz for $i = 2$. Since $(arz)^3 = (ar)^3 z$, in one and only one case is $(ab)^3$ contained in Q. (Indeed, since $(\hat{a}\hat{b})^3 \in \hat{Q}$, we have that $(ab)^3 \in ZQ$, as ZQ is the full preimage of $\hat{Q}$ in G.) □

Clearly, we set $G_2 = T_i$, $i = 1$, or 2, in the unique way, as in Lemma 4.3. Then we obtain a graph Γ and a covering $\Gamma \longrightarrow \hat{\Gamma}$ that preserves local structure. According to the discussion in the introduction, this means we also have a geometry $\mathcal{G}$ covering $\hat{\mathcal{G}}$. Since the action of G_1 on the neighbourgood of x is the same as the action of $\hat{G}_1$ on the neighbourhood of $\hat{X}$, we immediately see that the action of G on $\mathcal{G}$ is flag-transitive. This completes the proof of Theorem 1.

References

[Asc] M. Aschbacher, *Sporadic Groups*, Cambridge Tracts in Mathematics 104, Cambridge University Press, 1994.

[Atl] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[Bue] F. Buekenhout, Diagrams for geometries and groups, *J. Combin. Theory*, **A27** (1979), 121–151.

[Gri] R.L. Griess, The Friendly Giant, *Invent. Math.* **69** (1982), 1–102.

[Ivn] A.A. Ivanov, On the Buekenhout–Fischer geometry of the Monster, In: *Moonshine, the Monster and Related Topics*, C. Dong and G. Mason eds., pp. 149–158, Contemp. Math. **193** AMS, 1996.

[IMe] A.A. Ivanov and U. Meierfrankenfeld, Simple connectedness of the 3-local geometry of the Monster, *J. Algebra* (to appear).

[Pas] A. Pasini, *Diagram Geometries*, Clarendon Press, Oxford, 1994.

[Ron] M.A. Ronan, Coverings of certain finite geometries, In: *Finite Geometries and Designs*, pp. 316–331, Cambridge Univ. Press, Cambridge, 1981.

Department of Mathematics
Imperial College,
London SW7 2BZ, UK
a.ivanov@ic.ac.uk

Department of Mathematics
The Ohio State University,
231 W 18th Avenue,
Columbus, OH 43210, USA
ssh@math.ohio-state.edu

Construction of Hadamard Matrices Using Dihedral Groups

Hiroshi kimura
Ehime University, Matsuyama, Japan
kimura@dpc.ehime-u.ac.jp

Let H be a (± 1)-matrix of oder n. H is a Hadamard Matrix of order n if $HH^t = nI$.

Hadamard's Conjecture:
If n is dividible by 4, then there exists Hadamard matrix of order n

Notation: Let $G =< x, y | x^p = y^2 = 1, yxy = x^{-1} >$ be a dihedral group of order $2p$. Let ZG be a group ring of G over Z. For a subset S of G we use the same symbole S as $\sum_{s \in S} s$

Put $J = \sum_{g \in G} g$, $J_1 = \sum_{g \in < x >} g$
For $A \in ZG$,
$A = A_1 + A_2 y$ with $A_1, A_2 \in < x >$
$\overline{A} = J - A$
$a_1 = |A_1|$ and $a_2 = |A_2|$
Let $j = (1, \cdots, 1)$ be an all 1's vector and put $k = j^t$

Put $D(H) = (H + J)/2$ and we call also $D(H)$ a Hadamard matrix.
We identify elements of G with their matrices of regular representation of G.

When we classified Hadamard matrices of order 28 in [7], we found Hadamard matrices of the following form:

$$D(H)=\begin{bmatrix} 1 & 1 & 1 & 1 & j & j & j & j \\ 1 & 1 & & & j & j & & \\ 1 & & 1 & & j & & j & \\ 1 & & & 1 & & j & j & \\ k & k & k & & A & B & C & D \\ k & k & & k & \overline{B} & A & D & \overline{C} \\ k & & k & k & \overline{C} & \overline{D} & A & B \\ k & & & & D & \overline{C} & B & \overline{A} \end{bmatrix}$$

where A, B, C, D are subsets of a dihedral group G of order 6

Let H be a matrix of order $n = 8p + 4$:

$$H=\begin{bmatrix} 1 & 1 & 1 & 1 & j & j & j & j \\ 1 & 1 & & & j & j & & \\ 1 & & 1 & & j & & j & \\ 1 & & & 1 & & j & j & \\ k & k & k & & A & B & C & D \\ k & k & & k & \overline{B} & A & D & \overline{C} \\ k & & k & k & \overline{C} & \overline{D} & A & B \\ k & & & & D & \overline{C} & B & \overline{A} \end{bmatrix}$$

where A, B, C, D are subsets of G

Proposition 1 *H is H-matrix if and only if the following equations are holded*

$$\begin{aligned} &|A| = p-1,\ |B| = |C| = |D| = p \\ &AA^t + BB^t + CC^t + DD^t = (2p+1)I + 2(p-1)J \\ &A\overline{B}^t + BA^t + CD^t + D\overline{C}^t = (2p-1)J \\ &A\overline{C}^t + B\overline{D}^t + CA^t + DB^t = (2p-1)J \\ &AD^t + B\overline{C}^t + CB^t + D\overline{A}^t = 2pJ \end{aligned}$$

Since $A\overline{B}^t = (p-1)J - AB^t$, the above conditions are equivalent to the followings:

Proposition 2 *H is H-matrix if and only if the following equations are holded*

$$\begin{aligned} &|A| = p-1 \text{ and } |B| = |C| = |D| = p \\ &AA^t + BB^t + CC^t + DD^t = (2p+1)I + 2(p-1)J \\ &AB^t + DC^t = BA^t + CD^t (= (AB^t + DC^t)^t) \\ &AC^t + BD^t = CA^t + DB^t \\ &AD^t + CB^t = BC^t + DA^t \end{aligned}$$

When H is H-matrix, we say (A, B, C, D) H-group array.

Proposition 3 (A, B, C, D) *is a* **H-group array**, *then we have the followings:*

1. (gA, gB, gC, gD) *is* **H-group array**
2. (Ag, Bg, Cg, Dg) *is* **H-group array**
3. $(A^\sigma, B^\sigma, C^\sigma, D^\sigma)$ *is* **H-group array**

where $g \in G$ and σ is an automorphism of G

By signed permutations of rows and columns of H and taking transpose of matrices, we have the following propositions.

Proposition 4 *If* (A, B, C, D) *is* **H-group array**, *then*

1. (A, D, C, B) *is* **H-group array**
2. $(A, B, \overline{C}, \overline{D})$ *is* **H-group array**
3. $(A, \overline{B}, C, \overline{D})$ *is* **H-group array**
4. $(A, C, \overline{B}, \overline{D})$ *is* **H-group array**

By **Proposition** 4 we may assume that

Assumption 1

$a_1 \leq a_2$
b_1 , c_1 and d_1 are odd,
and
b_2 , c_2 and d_2 are even.

By **Proposition** 2 $a_1, \cdots$, and d_2 must satisfy the conditions:

1. $a_1^2 + a_2^2 + b_1^2 + b_2^2 + c_1^2 + c_2^2 + d_1^2 + d_2^2 = 2p^2 + 1$
2. $a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2 = p(p-1)$

Exsample

p	a_1	a_2	b_1	b_2	c_1	c_2	d_1	d_2
3	0	2	1	2	1	2	1	2
5	2	2	1	4	3	2	3	2
7	2	4	5	2	3	4	3	4
9	4	4	3	6	3	6	5	4
11	4	6	7	4	7	4	5	6

Under some assumputions on G we consider the construction of **H-matrices** by dihedral groups

Assumption 2 *Let σ be an element of Aut $< x >$ of order 4. A, B, C, and D are σ-invaliant.*

Under this assumpution there exist H-matrices for p=5,9,17 and 29

Assumption 3 *A, B, C and D are y-invaliant.*

Under this assumpution there exist H-matrices for p=7,17,19,21,23,25 and 27

Assumption 4
$p = 1\ (4)$
$c_1 = d_1 = \frac{p+1}{2},\ c_2 = d_2 = \frac{p-1}{2}$
$C_1 \subset C_2,\ ie. C_1 = C_2 + 1$
$D_1 \subset D_2,\ ie. D_1 = D_2 + 1$
$A_1 + A_2 = J_1 - 1$
$B_1 + B_2 = J_1$

Under this assumpution there exist H-matrices for p=5,13,37,41 and 61

By a computer seach we have H-matrices for the following cases

$$3 \leq p \leq 29 (p \neq 15)$$
$$p = 37, 41, 47, 61$$

Example of H-matrices

$p = 3$

$$\begin{array}{rcccccccc}
A = & 1 & +x & +x^2 & +(& 1 & +x & +x^2)y \\
A = & & & & (& 1 & & +x^2)y \\
B = & 1 & & & +(& & x & +x^2)y \\
C = & & & x^3 & +(& & x & +x^2)y \\
D = & & x & & +(& & x & +x^2)y
\end{array}$$

$p = 5$

$$\begin{array}{rcccccccccc}
A = & & x & & & +x^4 & +(& & x^2 & +x^3 &)y \\
B = & 1 & & & & & +(& x & +x^2 & +x^3 & +x^4)y \\
C = & 1 & & +x^2 & +x^3 & & +(& & x^2 & +x^3 &)y \\
D = & 1 & +x & & +x^4 & & +(& x & & + & x^4)y
\end{array}$$

Remark 1 *Minimal degree of matrix such that we don't know the existence of H-matrix is* $428 (= 53 \cdot 8 + 4)$

Remark 2 *H-matrixecs of Williamson type construct form cyclic groups. Williamson type:*

$$\begin{bmatrix} A & B & C & D \\ \overline{B} & A & \overline{D} & C \\ \overline{C} & D & A & \overline{B} \\ \overline{D} & \overline{C} & B & A \end{bmatrix}$$

where A, B, C and D subsets of cyclic group of order $n/4$

References

[1] M.Hall, Jr., *Combinatotrial Theory*, Ginn(Blaisdell) Boston, 1967.

[2] M.Hall,Jr., *Hadamard matrices of order 16*, J.P.L Reseach Summary,1961.

[3] M.Hall,Jr., *Hadamard matrices of order 20*, J.P.L Technical Report,1965.

[4] N.Ito, J.S.Leon, and J.Q.Longyear, *Classification of 3-(24,12,5) designs and 24-dimensional Hadamard matrices*, J.Combin.Theory(A),1979.

[5] H.Kimura, *New Hadamard matrix of order 24*, Graphs and Combin.,1989.

[6] H.Kimura, *Classification of Hadamard matrices of order 28 with Hall sets*,Discrete Math.,1994.

[7] H.Kimura, *Classification of Hadamard matrices of order* 28 ,Discrete Math.,1994.

[8] H.Kimura,*Hadamard matrices and dihedral groups*, Design,Codes and Cryptography,1996.

Binary code VOA and finite automorphism groups

Masaaki KITAZUME
Department of Mathematics and Informatics
Faculty of Science
Chiba University
Chiba 263, Japan

This report is based on a joint work with Masahiko Miyamoto.

1 Introduction

Vertex operator algebra V is an infinite dimensional Z-graded algebra $V = \oplus_{n=0}^{\infty} V_n$, but it has sometimes a finite full automorphism group. In this paper, we will treat the case where $\dim V_0 = 1$ and $V_1 = 0$. In this case, V_2 is a commutative (nonassociative) algebra with a symmetric invariant bilinear form $\langle *, * \rangle$ given by $\langle v, u \rangle 1 = v_3 u$ for $u, v \in V_2$. This is called a Griess algebra in [M1].

Our purpose in this paper is to study code VOA M_D which are construced from even linear binary codes D in [M2]. If D has no codewords of weight 2, then $\dim(M_D)_0 = 1$ and $(M_D)_1 = 0$ and so $(M_D)_2$ is a Griess algebra. In this case, it is not difficult to see that the full automorphism group of M_D is finite [M3] and the automorphism group of M_D has a normal subgroup which is a 3-transposition group. We will classify such 3-transposition groups G and construct code VOA with automorphism group G.

2 Vertex Operator Algebras and the Griess Algebras

A vertex operator algebra (VOA) is a Z-graded vector space $V = \oplus_{n=0}^{\infty} V_n$ with the specified elements 1 (the vacuum) $\in V_0$, w (the Virasoro element) $\in V_2$ and infinitely many products

$$\times_n : V \times V \to V : (v, u) \mapsto v \times_n u (=: v_n u) \quad (n \in Z)$$

We recall some properties of VOA, but omit the precise definition.
(1) $v_n u \in V_{l+m-n-1}$ for $v \in V_l, u \in V_m$

(2) $\mathbf{1}_{-1}v = v$, $\mathbf{1}_n v = 0$ $(n \neq -1)$
(3) $\mathrm{w}_1 v = nv$ $(v \in V_n)$
(4) $L(i) := \mathrm{w}_{i+1}$ satisfies the Virasoro relations;

$$[L(m), L(n)] = (m-n)L(m+n) + \delta_{m+n,0}\frac{m^3-m}{12}c$$

where c is called the central charge of V.

For the definition of Griess algebras, we assume more properties:
(5) $\dim(V_0) = 1$, that is, $V_0 = \langle \mathbf{1} \rangle$.
(6) $\dim(V_1) = 0$.
We define a binary operation $u \times v$ and a bilinear form $< u, v >$ on V_2 by

$$u \times v := u_1 v, \quad < u, v > \mathbf{1} := u_3 v.$$

Then it can be verified that $u \times v$ and $< u, v >$ are commutative.

3 Idempotents and Automorphisms of order 2

In this section, we will recall the results of [M1] about the relation between idempotents of the Griess algebra V_2 and automorphisms of order 2. Here we further assume that VOAs are over the real field $\mathbb{R}$ and have a positive definite invariant bilinear form $(\,,)$. Rescaling it, we may assume $< u, v >= (u, v)$ on V_2.

Theorem 3.1 *The following two conditions are eqivalent with each other.*
(1) $e \in V_2$ is an idempotent (i.e. $e \times e = e$) and satisfies $< e, e >= \frac{1}{16}$
(2) $2e$ is a conformal vector of central charge $\frac{1}{2}$, that is,

$$[\bar{L}(m), \bar{L}(n)] = (m-n)\bar{L}(m+n) + \delta_{m+n,0}\frac{m^3-m}{12} \cdot \frac{1}{2}$$

for $\bar{L}(m) := (2e)_{m+1}$

Let $\mathrm{Vir}(e)$ be a subVOA generated by e (or $\bar{L}(n)$). Then $\mathrm{Vir}(e)$ is isomorphic to $L(\frac{1}{2}, 0)$. Hence V splits into the direct sum of irreducible $\mathrm{Vir}(e)$-submodules, which is isomorphic to $L(\frac{1}{2}, 0), L(\frac{1}{2}, \frac{1}{2})$ or $L(\frac{1}{2}, \frac{1}{16})$.

Definition 3.2 *An idempotent e is of type 2 if and only if there exist no* $\mathrm{Vir}(e)$*-submodule isomorphic to $L(\frac{1}{2}, \frac{1}{16})$. An idempotent e is of type 1 if and only if there do exist a* $\mathrm{Vir}(e)$*-submodule isomorphic to $L(\frac{1}{2}, \frac{1}{16})$.*

Theorem 3.3 *(1) For an idempotent e of type 1, define an endomorphism τ_e on V by*

$\tau_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$ *or* $L(\frac{1}{2},\frac{1}{2})$
$\tau_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{16})$.

Then τ_e *is a automorphism of the VOA* V, *and* $\tau_e^2 = id_V$
(2) For an idempotent e *of type 2, define an endomorphism* σ_e *on* V *by*

$\sigma_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$
$\sigma_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{2})$.

Then σ_e *is a automorphism of the VOA* V, *and* $\sigma_e^2 = id_V$

Theorem 3.4 *If* $e, f (e \neq f)$ *are idempotents of type 2, then one of the following holds.*
(1) $\langle e, f\rangle = 0$ *and* $(\sigma_e\sigma_f)^2 = 1$
(2) $\langle e, f\rangle = \frac{1}{128}$ *and* $(\sigma_e\sigma_f)^3 = 1$
In particular, The involutions σ_e*'s generate 3-transposition group.*

4 Code Vertex Operator Algebras

Let C be a binary even code of length n. We set $M = L(\frac{1}{2},0) \oplus L(\frac{1}{2},\frac{1}{2})$, and consider the tensor product of n copies of M. For $c = (c_1, c_2, ..., c_n) \in C$, we denote by $(\otimes^{(n)}M)_c$ the set of all linear combinations of the form $u_1 \otimes u_2 \otimes ... \otimes u_n (u_i \in L(\frac{1}{2},\frac{c_i}{2})$, where c_i are regarded as integers $0, 1$. We define

$$M_C := \bigoplus_{c\in C}(\otimes^{(n)}M)_c \otimes e^c,$$

where $\otimes e^c$ is a symbol with $e^c e^{c'} = e^{c+c'}$. M_C has a VOA structure natually. The degree of $u_1 \otimes u_2 \otimes ... \otimes u_n \otimes e^c$ is the sum of the degrees of u_i and $\frac{(c,c)}{2}$ and so the degrees of elements in M_C are integers since C is an even code. It is easy to see that $(M_C)_n = 0$ for $n < 0$ and $\dim(M_C)_0 = 1$.

The element $\hat{1} = 1 \otimes 1 \otimes ... \otimes 1$ is the vacuum of M_C. Set $\hat{w}^i = 1 \otimes 1 \otimes ... \otimes w \otimes ... \otimes 1$ (w is on the i-th component) and define $\hat{w} = \hat{w}^1 + ... \hat{w}^n$. Then $\hat{w}$ is the Virasoro element of M_C.

Moreover M_C satisfies the following properties:

Lemma 4.1 *(1)* M_C *has an invariant bilinear form.*
(2) $\dim(M_C)_0 = 1$
(3) $\frac{1}{2}\hat{w}^i$ *is an idempotent of* $(M_C)_2$ *and satisfies* $< \frac{1}{2}\hat{w}^i, \frac{1}{2}\hat{w}^i >= \frac{1}{16}$.
(4) $\frac{1}{2}\hat{w}^i$ *is of type 2.*

We assume that the minimal weight of C is four. This means that $(M_C)_1 = 0$ and thus $(M_C)_2$ becomes a Griess algebra.

Lemma 4.2 **(M2)** *(1) Let H be a [8,4,4]-Hamming subcode of C with*

$$\mathrm{supp}H = \{i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8\}.$$

Then for any $\alpha \in \mathbf{F}_2^n$,

$$e = e_\alpha := \frac{1}{32}(\hat{\mathrm{w}}^{i_1} + ... + \hat{\mathrm{w}}^{i_8}) + \frac{1}{32} \sum_{\beta \in D,\ |\beta|=4} (-1)^{(\alpha,\beta)} u_\beta$$

is an idempotent of $(M_C)_2$ and satisfies $< e, e >= \frac{1}{16}$.

(2) If $\mathrm{supp}H \subset C^\perp$*, then $e_{\alpha,H}$ is of type 2.*

Remark 4.3 *If α equals to α' modulo $H^\perp$, we have $e_\alpha = e_{\alpha'}$. Hence there exist 2^4 elements $e_{\alpha,H}$ for each H.*

Definition 4.4 *Let D_C be the set of involutions σ_e such that e is an idempotent of type 2 and satisfies $< e, e >= \frac{1}{16}$.*

By the above Lemmas, $\frac{1}{2}\mathrm{w}^i$ and $e_{\alpha,H}$ are elements of D_C.

Theorem 4.5 **(M2)** *Let K_C be the subgroup of* $\mathrm{Aut}(M_C)$ *generated by D_C. Then D_C is a set of 3-transpositions of K_C.*

Let $L = \{\sigma_1, ..., \sigma_n\}$, where $\sigma_i = \sigma_{\hat{\mathrm{w}}^i}$ for $i = 1, ..., n$. The following is a key of this paper.

Lemma 4.6 *Let e be an idempotent of type 2 and assume $\sigma_e \notin L$. Then $|C_L(\sigma_e)| = n - 8$. In particular, L is a maximal subset of mutually commuting elements of D_C.*

Proof. By the equations:

$$\frac{1}{4} =< 2e, 2e >=< \mathrm{w}, 2e >=< \hat{\mathrm{w}}^1 + ... + \hat{\mathrm{w}}^n, 2e >$$

and Theorem 3.4, there are exactly eight $\hat{\mathrm{w}}^i$, say $\hat{\mathrm{w}}^1, ..., \hat{\mathrm{w}}^8$, such that $< \hat{\mathrm{w}}^i, e >= \frac{1}{64}$ for $i = 1, ..., 8$ and $< \hat{\mathrm{w}}^i, e >= 0$ for $i = 9, ..., n$. ∎

Notice that a maximal sebset of mutually commuting elements of D_C is obtained as the intersection of D_C and a Sylow 2-subgroup S of K_C. The number $|L| = |S \cap D_C|$ is called the width of K_C in [Fi].

The 3-transpositions groups satisfying the condition of this Lemma are easily classified by using Fischer's list [Fi] of 3-transposition groups G satisfying $O_2(G) = O_3(G) = 1$.

Let D be the set of 3-transpositions of G. We will describe a 3-transposition group by the graph whose vertices are the elements of D and edges are defined by :

$$\{a,b\} \text{ is an edge} \Longleftrightarrow [a,b] \neq 1$$

We will denote this graph as $\Gamma(G)$ or $\Gamma(D)$. If $O_2(G) \neq 1$, then $\bar{D} = DO_2(G)/O_2(G)$ is a set of 3-transpositions of $\bar{G} = G/O_2(G)$, and the number of the elements of $dO_2(G)$ is a power of 2 for any $d \in D$. If $\Gamma(G)$ is connencted, then this number ($= 2^k$, say) does not depend on the choice of $d \in D$. Then we write $\Gamma(G) = O_2^{(2^k)} \cdot \Gamma(\bar{G})$.

Now we will state the following main theorem.

Theorem 4.7 *Let K_C be the subgroup of* $\mathrm{Aut}(M_C)$ *generated by D_C, and E be a subset of D_C such that $\Gamma(E)$ is a connected component of $\Gamma(D_C)$. Then $\Gamma(E)$ is isomorphic to one of the following.*

	$\Gamma(E)$	$\lvert E\rvert$	ℓ
(i)	$\Gamma(O^+(10,2))$	*496*	*16*
(ii)	$\Gamma(Sp(8,2))$	*255*	*15*
(iii)	$O_2^{(2)} \cdot \Gamma(O^+(8,2))$	*240*	*16*
(iv)	$O_2^{(2)} \cdot \Gamma(Sp(6,2))$	*126*	*14*
(v)	$O_2^{(4)} \cdot \Gamma(S_{2m}) \quad (m > 2)$	*4m(2m-1)*	*4m*
(vi)	$O_2^{(8)} \cdot \Gamma(S_3)$	*24*	*8*

Here ℓ is the maximal number of mutually commuting elements of E.

Remark 4.8 *The main parts of the groups of the cases (iii), (iv) are the Weyl groups $W(E_8), W(E_7)$ respectively. Under such a viewpoint, the main parts of the groups of (v), (vi) are the Weyl groups $W(D_{2m})$ ($m = 2$ for (vi)). (i.e. $O_2^{(4)} \cdot \Gamma(S_{2m}) \cong O_2^{(2)} \cdot \Gamma(W(D_{2m}))$)*

5 Examples

(1) Let C be the 2nd order Reed-Muller code of length 16. Then the case (*i*) of Theorem holds. We will explain this in detail.

Let Ω be the set of all the vectors of the 4-dimensional vector space V over the two element field F_2, that is, a point of Ω is a vector of V. We regard the power set $P(\Omega)$ of Ω (i.e. the set of all the subsets of Ω) as a vector space over F_2 by defining the sum $X + Y$ as their symmetric difference $(X \cup Y) \setminus (X \cap Y)$ for $X, Y \subset \Omega$.

We define the code $C \subset P(\Omega)$ as the subspace spanned by all the 2-dimensional affine subspaces of V. Then C is $[16, 11, 4]$-code and is known as the extended Hamming code of length 16 or the 2nd order Reed-Muller code of length 16.

A codeword of minimal weight of C corresponds with a 2-dimensional affine subspace of V. Hence C contains $140(= \frac{(16-1)(16-2)}{(4-1)(4-2)} \times 4)$ vectors of weight 4, and thus $\dim(M_C)_2 = 156$.

Let W be a 3-dimensional affine subspace of V, and H_W be a subcode of C spanned by all the 2-dimensional affine subspaces of W. Then it is easy to see that H_W is a [8,4,4]-Hamming subcode of C, and supp$H_W \subset C^{\perp}$. Since the number of the 3-dimensional affine subspaces of V is $30(=\frac{(16-1)(16-2)(16-4)}{(8-1)(8-2)(8-4)} \times 2)$, we can obtain $480(= 30 \times 2^4)$ involutions defined by an idempotent e_{a,H_W} for some W. Hence the set D_C contains at least 496 elements. By Theorem 5.8, we have $|D_C| = 496$ and $\Gamma(K_C) \cong \Gamma(O^+(10,2))$.

In the following examples (2)-(4), we use the notation of the previous example (1).

(2) Let 0 be the zero vector of V, and set $\Omega' = \Omega \setminus \{0\}$. We define the code $C' \subset P(\Omega')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $0 \notin W$. Then C' is a $[15,10,4]$-code. By a similar argument as in (1), we have that $\dim(M_{C'})_2 = 120$, $|D_{C'}| = 255$, and $\Gamma(K_{C'}) \cong \Gamma(Sp(8,2))$.

Notice that the code C' is regarded as a subcode of C. Then the structure of $K_{C'}$ is easily deduced by the fact $C_{O^+(10,2)}(d)/\langle d\rangle \cong Sp(8,2)$ for some $d \in D_C$.

(3) Let U be a one-dimensional subspace of V, and set $\Omega'' = \Omega \setminus U$. We define the code $C'' \subset P(\Omega'')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $U \cap W = \emptyset$. Then C'' is a $[14,7,4]$-code, and $\dim(M_{C''})_2 = 91$, $|D_{C''}| = 126$. Moreover we have $\Gamma(K_{C''}) \cong O_2^{(2)} \cdot \Gamma(Sp(6,2))$.

(4) Let r be a integer greater than 1. Let $V_i, \Omega_i, C_i \subset P(\Omega_i)$ be a copy of V, Ω, C of (1) respectively for $i = 1, ..., r$. Set $C^r = C_1 \oplus C_2 \oplus ... \oplus C_r$. We fix a 1-dimensional subspace U_i of V_i for each i, and set $U_{ij} = U_i \cup U_j$ for $i \neq j$. Then the weight of U_{ij} is 4. Let $C(E,r)$ be a code of length $16r$ spanned by C^r and all U_{ij} for $i \neq j$.

Let W_i be a 3-dimensional affine subspace of V_i, and H_{W_i} be a subcode of $C(E,r)$ spanned by all the 2-dimensional affine subspaces of W_i. Then the condition supp$H_{W_i} \subset C(E,r)^{\perp}$ holds if and only if W_i contains $U_i + a$ for any $a \in W_i$. The number of W_i satisfying this condition is $14(=\frac{(16-2)(16-4)}{(8-2)(8-4)} \times 2)$ for each i.

It is easy to see that $|D_{C(E,r)}| = 240r$ and $\Gamma(K_{C(E,r)}) \cong \{O_2^{(2)} \cdot \Gamma(O^+(8,2))\}^r$.

(5) For an integer $m > 1$, we define a $[4m, 3m-2, 4]$-code C_m by the following generating

matrix

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & & & & & & & \dots & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & & & & & & & \dots & & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}$$

Then $\dim(M_{C_m})_2 = 6m^2 - m$, $|D_{C_m}| = 8m^2 - 4m$, and $\Gamma(K_{C_m}) \cong O_2^{(4)} \cdot \Gamma(S_{2m})$

References

[Fi] B. Fischer, Finite group generated by 3-transpositions, preprint.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* 179, (1996) 523-548

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. algebra* 181, (1996) 207-222

[M3] M. Miyamoto, The moonshine VOA and a tensor product of Ising models, *The Monster and Lie algebras (Columbus, OH, 1996)*, Ohio State Univ. Math. Res. Inst. Publ., de Gruyter Berlin, to appear.

Some examples of unramified extensions over quadratic fields

Takeshi KONDO

November 22, 1997

1 Introduction

The purpose of this note is to state the following Theorem 1 and to give some examples of unramified extensions over quadratic fields related to the theorem. For the details of the proof, we refer the readers to [Ko].

Theorem 1 *Let K be an algebraic number field of degree n with the discriminant δ^2 where δ is a square-free odd integer. Let L be the Galois closure of K over $\mathbf{Q}$, the field of rational numbers, and G be the Galois group of $L/\mathbf{Q}$ which is regarded as a permutation group of degree n. If G is primitive as a permutation group, G is one of the following groups:*

(a) A_n, the Alternatin group of degree n,
(b) $n = 8$ and $G \simeq Hol(\mathbf{Z}_2^3)$, the holomorph of an elementary abelian group $\mathbf{Z}_2^3$,
(c) $n = 7$ and $G \simeq PSL(2,7)$,
(d) $n = 6$ and $G \simeq PSL(2,5) (\simeq A_5)$,
(e) $n = 5$ and $G \simeq D_{10}$, the dihedral group of order 10.

This theorem follows from Th.2 and Th.3:

Theorem 2 *Let K, L, G be as above. If p is a prime ramified in $L/\mathbf{Q}$, then the inertia group of p is a group of order 3 generated by a 3-cycle or a group of order 2 generated by a product of two transpositions.*

It is well known (cf.[W]) that a primitive permutation group which contains a 3-cycle is A_n or S_n, from which (a) of Th.1 follows (Note that $G \subseteq A_n$ as the discriminant of K is square). Now Th.1 follows from

Theorem 3 *Assume that a primitive permutation group G of degree n other than A_n or S_n contains a subgroup of order 2 generated by a product of two transpositions. Then G is one of groups listed in (b)$\sim$(e) of Th.1.*

Theorem 4 *Let G be as in (b),(c) or (d) of Th.1. If $\mathbf{Q}(\sqrt{m})$ is a quadratic field with $\delta|m$, then $L(\sqrt{m})/\mathbf{Q}(\sqrt{m})$ is a unramified extension with Galois group $Hol(\mathbf{Z}_2^3)$,$PSL(2,7)$ or $PSL(2,5)$ respectively.*

Some examples of (c) or (d) of Th.4 will be given in §2, In particular, we will note that a family of sextic polynomials constructed by A.Brumer gives many examples of the case (d). The author knows no examples of the case (b).

2 Some examples of Th.4

2.1 The case $PSL(2,7)$

In [Y], K.Yamazaki found several examples of polynomials of degree 7 with the Galois group $PSL(2,7)$, and then, among them, K.Yamamura found the following examples which define number fields satisfying the conditions of Th.1, and noted that they yield unramified extensions of quadratic fields:

$f(x) = x^7 + 2x^6 - 3x^4 - x^3 - x^2 - x + 2$,$d(f) = 105124009 = 10253^2$,
$f(x) = x^7 - x^6 - x^5 + x^4 - x^3 - 3x^2 + 3x + 2$, $d(f) = 157979761 = 12569^2$,
$f(x) = x^7 - x^4 - x^3 - 7x^2 + 4x + 5$, $d(f) = 26536735801 = 162901^2$,
where $d(f)$ is the discriminant of $f(x)$.

Th.1 was suggested by this indication of Yamamura.

2.2 The case $PSL(2,5) \simeq A_5$

The following family of sextic polynomials was constructed by A.Brumer (cf.[O,p765]):

$$\begin{aligned} f(x;b,c,d) = x^6 + 2cx^5 + (c^2 + 2c + 2 - bd)x^4 + (2c^2 + 2c + 2 - 2bd + b - 4d)x^3 \\ + (c^2 + 4c + 5 - bd + 3b)x^2 + (2c + 6 + 3b)x + (b + 1) \end{aligned}$$

In [A] or [Ko], it is proved:

Theorem 5 *If b, c, d is independent variables over $\mathbf{Q}$, then the Galois group of $f(x;b,c,d)$ over $\mathbf{Q}(b,c,d)$ is isomorphic to $PSL(2,5)$ $(\simeq A_5)$.*

Remark. The proof of this theorem was done with the help of "Computer Algebra" due to H.Anai. But, more recently, K.Hasimoto has found a construction of $f(x;b,c,d)$ other than A.Brumer's one, including the proof of Th.5 (cf.[H]).

The discriminant of $f(x;b,c,d)$ is as follows:

$$D(b,c,d) = \delta(b,c,d)^2$$

where

$$\begin{aligned} \delta(b,c,d) = {} & 16bdc^6 + \{(-144d + 16)b - 64d\}c^5 \\ & + \{(-48d^2 - 4d)b^2 + (-16d^2 + 192d - 144)b + (384d - 64)\}c^4 \\ & + \{(288d^2 - 160d - 4)b^2 + (832d^2 + 1008d + 208)b + (64d^2 + 320d + 384)\}c^3 \\ & + \{(48d^3 + 8d^2)b^3 + (32d^3 - 608d^2 + 1336d - 108)b^2 + \\ & \quad (-1280d^2 + 1184d + 896)b + (-2304d^2 - 2752d + 256)\}c^2 \\ & + \{(-144d^3 + 144d^2 + 36d)b^3 + (-768d^3 + 528d^2 - 2880d + 1008)b^2 + \\ & \quad (-576d^3 - 1536d^2 - 10032d + 432)b + (-4032d^2 - 9408d - 2496)\}c \\ & + \{(-16d^4 - 4d^3)b^4 + (-16d^4 + 416d^3 + 24d^2 + 108d + 27)b^3 + \\ & \quad (2112d^3 - 1824d^2 - 264d - 2268)b^2 + (3456d^3 - 6096d^2 - 1936d - 7744)b + \\ & \quad (1728d^3 - 5184d^2 - 2176d - 6592)\} \end{aligned}$$

We note that
(3.1) $\delta(b,c,d) \equiv 27b^3 \quad mod\ 4\mathbf{Z}[b,c,d]$
(3.2) For $b, c, d \in \mathbf{Z}$, $\delta(b,c,d)$ is odd if and only if b is odd.

Furthermore it turns out that there exist (probably infinitely) many $b(odd), c, d \in \mathbf{Z}$ such that $\delta(b, c, d)$ is a square-free odd integer (even a prime number). Thus we have many examples for $PSL(2,5)$-case of Th.4. Numerical examples where $\delta(b, c, d)$ is prime will be given in Table 1 and Table 2 of the end of the present paper.

References

[A] H.Anai, A family of sextic polynomials with Galois group A_5—computation of splitting fields and Galois groups—, preprint

[BM] G.Butler and J.Mckay, The transitive groups of degree up to eleven, Comm.Algebra 11,1983,863-911

[H] K.Hasimoto, On Brumer's family of RM-curves of genus 2, (Preliminary version,1996.11.1)

[Ko] T.Kondo, Some examples of unramified extensions over quadratic fields, Science Reports of Tokyo Woman's Christian University, Nos.121-124(1997),1399-1410

[M] J.F.Mestre, Courbes hyperelliptiques à multiplications réelles, C.R.Acad.Sci.Paris 307(1988),721-724

[O] M.Olivier, Corps sextique primitifs, Ann.Instituts Fourier 40, 1990,757-767

[Y] K.Yamazaki, The computation of Galois group (in Japanese), Report of Symposium at Osaka Univ.(ed. T.Kondo), 1981,57-76

[W] H.Wielandt, Finite Permutation Groups, Academic Press

Table 1. $f(x;b,c,d)$ giving totally real unramified A_5-extension over $\mathbf{Q}(\sqrt{p})$ (p : prime)
$h(p)$ =the class number of $\mathbf{Q}(\sqrt{p})$
± in $h(p)$ denotes the sign of norm of the fundamental unit

p	b	c	d	$h(p)$
8311	−7	−4	0	1
25771	−11	8	−1	1
32611	11	2	2	1
37987	−3	7	−1	1
72707	−27	−6	0	1
83443	3	4	9	3
426427	−11	−5	0	1
515993	−9	−5	0	−1
697441	−9	8	−1	−1
727427	−3	9	−3	1
877867	−19	11	−2	1
944399	31	−1	1	3
1204243	−3	8	−1	1
1207447	−23	−6	0	1
1294723	−3	−5	−1	1
1447811	−3	−5	−3	1
1606763	27	0	1	1
1648379	−3	−5	−2	1
1836811	27	−4	3	1
1924651	−67	−8	0	1
2118163	−11	−6	0	1
2214761	9	0	4	−1
2219807	−15	−6	0	1
2719001	41	−2	1	−1
2828879	15	2	2	1
2956907	−3	−8	0	1
4176239	15	1	2	1
4367879	31	0	1	1
4460909	77	4	1	−1
4748371	−3	9	−2	1
5060053	−5	−8	0	−1
5122259	−3	−9	0	1
6492137	33	0	1	−1
6874397	−29	−7	0	−1
7156883	27	4	2	1
7360273	−25	−7	0	−1
7540529	9	3	4	−5
7912319	−31	10	−1	1
8358299	−3	−10	0	1
8540509	−61	−8	0	−1
8554027	−3	10	−4	1
8573023	15	−1	3	1
8987213	21	−1	2	−3
9072919	39	−6	3	3
11059123	−3	−7	−1	3
11141743	−7	−7	−3	1
11367269	29	8	4	−1
11456923	−3	10	−1	1
11464213	45	−2	1	−11
12143441	−57	−8	0	−1
12542939	19	2	2	25
13957429	−21	−8	−1	−1
14390213	−5	−10	0	−1
15226147	−27	10	−1	1
16013611	−11	−7	−1	1
16102049	41	−1	1	−1
16237597	−5	10	−1	−3
16451047	15	−2	4	13
17110019	−3	10	−2	1
17283269	−21	−8	0	−1
17618281	−17	11	−2	−1
18279497	−25	10	−1	−1
18389779	−3	−7	−2	1
18492841	−9	−7	−1	−1
18616799	−7	−7	−1	1
20265703	−7	−10	0	1
20855221	−37	−8	0	−1
21391471	−7	−8	−5	7
21779123	43	−1	1	1
21787061	21	2	2	−1
23577859	−35	13	−2	1
23732327	79	4	1	3
23786627	−3	−7	−3	1
23881133	13	−1	4	−1
24278819	43	1	1	1
25168387	−3	11	−1	1
26204767	−23	−11	−3	43
27454211	−19	−8	−1	1
29772409	81	−5	1	−1
29961859	−83	−9	0	1

Table 2. $f(x;b,c,d)$ giving unramified A_5-extension over $\mathbf{Q}(\sqrt{p})$
(• shows that $f(x;b,c,d)$ is totally real)
$h(p)$ =the class number of $\mathbf{Q}(\sqrt{p})$

p	b	c	d	$h(p)$
653	3	5	0	−1
2053	−3	−3	0	−1
2083	3	4	0	1
3329	1	4	0	−1
4073	1	7	0	−1
5413	−3	2	0	−1
7433	1	3	0	−1
8311•	1	7	−1	1
10453	11	5	0	−1
10597	3	−1	1	−1
10687	1	7	−2	1
11969	1	2	−1	−1
14321	1	7	2	−1
14323	3	4	1	1
15289	1	−1	0	−1
16193	1	1	0	−1
16529	15	1	1	−1
18049	7	6	0	−1
18329	1	1	−1	−1
19661	3	3	6	−1
21341	−3	0	−2	−1
21757	−3	1	−3	−1
24499	3	2	0	3
25771•	11	8	−1	1
24631	1	7	4	1
26429	1	0	1	−1
26731	21	0	1	1
27947	93	9	0	1
32611•	11	2	2	1
32987	3	2	−1	1
36293	−3	2	−5	−1
37987•	−3	7	−1	1
38767	1	−1	2	1
39139	3	1	0	3
44053	3	5	1	−1
47623	−9	3	0	1
47653	5	5	−1	−1
51461	3	7	0	−1
53923	−5	−1	0	1
54581	3	−2	1	−1
54617	15	4	0	−1
56923	3	−1	0	1
58567	1	−3	3	5
58603	5	−1	1	9
58907	−5	−3	0	3
61211	3	1	−1	3
63149	13	1	1	−1
63929	1	4	1	−1
67231	1	9	0	3
68891	−5	3	−2	1
72707•	−27	−6	0	1
74611	3	−2	0	1
75941	3	1	3	−1
77641	9	2	0	−7
83443•	3	4	9	3
84317	−3	1	2	−1
84871	17	1	1	11
85829	−3	1	−4	−1
87433	7	1	2	−1
94307	−5	3	−3	1
96043	5	4	1	1
100937	1	1	4	−1
101531	3	3	4	3
102587	3	3	5	1
104393	1	2	−2	−1
112459	3	1	1	1
113567	7	4	−1	19
115499	3	1	2	1
115763	−13	4	0	7
119737	7	2	0	−1
121577	1	5	−2	−15
123373	−11	5	0	−1
125777	1	3	−2	−1
127423	−9	−4	0	1
131221	3	6	1	−7
136573	−3	3	−3	−1
137519	9	7	0	1
141761	1	2	5	−3
142217	1	4	−2	−1
144323	−13	2	0	1
149551	9	2	2	1

On a conjecture of Bannai and Ito

Jack Koolen
jackmath.kyushu-u.ac.jp
Graduate School of Mathematics

Kyushu University

October 24, 1997

In this note I will give an outline of the proof of the following result.

Theorem 1 *There are only finitely many distance-regular graphs with valency k, with $3 \leq k \leq 1000$.*

This theorem partially resolves the following 1984 conjecture of Bannai and Ito.

Conjecture 2 *For a fixed $k \geq 3$, there are only finitely many distance-regular graphs with valency k.*

Definitions

In this note all the graphs are simple, undirected and without loops. Let Γ be a graph. For all vertices x of Γ, define $\Gamma_i(x) :=$ $\{y \in \Gamma \mid d(x,y) = i\}$. We will use $\Gamma(x)$ instead of $\Gamma_1(x)$. A graph Γ with diameter D is called *distance-regular* if there exist numbers a_i, b_i, c_i, $i = 0, 1, \ldots, D$ such that if x, y are any two vertices of Γ, say at distance j, then

$$|\Gamma_{j-1}(x) \cap \Gamma(y)| = c_j,$$
$$|\Gamma_j(x) \cap \Gamma(y)| = a_j,$$
$$|\Gamma_{j+1}(x) \cap \Gamma(y)| = b_j.$$

So a distance-regular graph is a regular graph with valency b_0. Furthermore the following hold:

$$b_i \geq b_{i+1},$$
$$c_i \leq c_{i+1}.$$

The (1-skeleton of the) dodecahedron is an example of a distance-regular graph.

Now I will say some words on the history of this conjecture.

History

In a series of papers (1987 -1989), Bannai and Ito showed the following theorem.

Theorem 3
(i) There are only finitely many distance-regular graphs with valency three or four,
(ii) For a fixed $k \geq 3$, there are only finitely many bipartite distance-regular graphs with valency k.

For small valencies the distance-regular graphs are classified.

Theorem 4
(i) [Biggs, Boshier and Shawe-Taylor] There are exactly 13 distance-regular graphs with valency three.
(ii) [Brouwer and Koolen] There are exactly 17 intersection arrays for which a distance-regular graph with valency 4 exists. For two of the intersection arrays there are exactly two examples known, for 14 of the intersection arrays the distance-regular graph is known to be unique, and for the last one there is an example known, but it is not yet known to be unique.

Main Idea

Now I will give the main idea behind the proof. Let θ be an eigenvalue of a distance-regular graph Γ (i.e. of its adjacency matrix) and let θ' be an algebraic conjugate of θ (over the rationals), then the multiplicities of θ and θ' as eigenvalues of Γ are equal.

Some Theorems

In this section I will give some theorems we need for the proof of Theorem 1.

Theorem 5 *Let $k \geq 3$. There are constants $R, \varepsilon > 0$ such that if Γ is a distance-regular graph with valency k, diameter D, $r = l_{1,a_1,b_1}$, $s = l_{b_1,a_1,1}$ satisfying $D - r - s \leq \varepsilon r$, then $r \leq R$.*

This theorem is a generalisation of the following theorem of Bannai and Ito.

Theorem 6 *Let $k \geq 3$ and $C > 0$. There is a constant R such that if Γ is a distance-regular graph with valency k, diameter D, $r = l_{1,a_1,b_1}$, $s = l_{b_1,a_1,1}$ satisfying $D - r - s \leq C$, then $r \leq R$.*

Theorem 7 *Let $k \geq 3$ and $C > 0$. There is a constant R such that if Γ is a distance-regular graph with valency k, diameter D, $r = l_{1,a_1,b_1}$, and satisfying $|\{i \mid a_i - 2\sqrt{b_ic_i} > a_1 + 2 + 2\sqrt{b_1 - 2}\}| < C$, then $r \leq R$.*

This theorem has the following corollary.

Corollary 8 (Bannai and Ito) *For a fixed $k \geq 3$, there are only finitely many bipartite distance-regular graphs with valency k.*

Theorem 9 *Let $k \geq 3$ and $\beta > 0$. Let $a \geq 0$, $b, c > 0$ be such that $a + b + c = k$, and $a + 2\sqrt{bc} > k - \beta - 1 + \sqrt[4]{\beta}(1 + \sqrt{\beta})$. There is a constant R such that if Γ is a distance-regular graph with valency k, $b_1 = \beta$, then $l_{c,a,b} \leq R$.*

Proof of Main Result:

For any k and β with $3 \leq k \leq 1000$ and $1 \leq \beta \leq k - 1$, there are no integers $a \geq 0, b, c > 0$ with $a + b + c = k$,
$a + 2\sqrt{bc} < k - \beta - 1 + \sqrt[4]{\beta}(1 + \sqrt{\beta})$,
and $a - 2\sqrt{bc} > k - \beta + 1 + 2\sqrt{\beta - 2}\}| < C$.
By using Theorems 7 and 9, it follows that there are only finitely many distance-regular graphs with valency at most 1000.
QED.

Remark. In fact it is possible to replace the 1000 of Theorem 1 by 1027.

Open problem.
Let Γ be a distance-regular graph with valency k, $r = l_{(1,a_1,b_1)}$, and diameter D. Assume that
(*) for all $1 \leq i \leq D - 1$ we have $b_i = 1$ or $c_i = 1$.
Show that r is bounded by a function in k.
If we set $\rho := |\{i \mid b_i = 1\}$, then we know that r is bounded by a function of k and ρ. It follows that if Γ is antipodal and satisfying (*), then r is bounded by a function of k.

Morita Equivalent Blocks of Finite Groups

Shigeo KOSHITANI

In modular rèpresentation theory of finite groups, there are several important problems, namely, Brauer conjecture, Alperin-McKay conjecture, Donovan conjecture, Alperin weight conjecture, Dade conjecture and Broué conjecture (see [1], [2], [3], [4], [5], [6], [7], [8], [9], [10, Chap.IV, §5] and [12]). It is considered that they are in the center of modular representation theory of finite groups.

In this short note we discuss on the Broué conjecture. We need several notation in order to state it.

Notation : Let k be an algebraically closed field of prime characteristic p, let G be a finite group which has a Sylow p-subgroup P. We denote by kG the group algebra of G over k. Let $N = N_G(P)$, say, the normalizer of P in G. Moreover, let A and B be the principal block ideals (the principal p-blocks) of kG and kN, respectively. See a book of Nagao and Tsushima [13] for general notion and terminology in representation theory of finite groups.

Broué conjecture (question) : Keep the notation above. If P is abelian, then is it true that the blocks A and B are derived equivalent ? (See [5], [6] and [7] for derived equivalent blocks).

Here we are not going into detail about derived equivalent blocks. What is needed here is that the blocks A and B are derived equivalent if A and B are Morita equivalent (see [7]).

There have been only several known examples where Broué conjecture holds (see [7]). It should be noted that T. Okuyama recently checked it in several other cases which seem very interesting (see [14]).

From now on till the end of this note we assume the following. The groups $\mathrm{PSU}(3, q^2)$ for $2 < q \equiv 2$ or $5 \pmod 9$ are one of the infinite series of finite simple groups whose Sylow 3-subgroups are elementary abelian of order 9. Therefore, it seems natural to investigate if Broué conjecture holds for these groups for $p = 3$.

Assumption : $p = 3$, that is, $\mathrm{char} k = 3$, $G = \mathrm{PSU}(3, q^2)$, $2 < q \equiv 2$ or $5 \pmod 9$, $P \in \mathrm{Syl}_3(G)$, $N = N_G(P)$, $A = B_0(kG)$, $B = kN$ (the principal block ideals of kG and kN). Note that kN is indecomposable as a two-sided ideal. Then it is known that $P \cong C_3 \times C_3$, the elementary abelian group of order 9, and that N is a semi-direct product $P : Q_8$ of P by the quaternion group Q_8 of order 8.

Now, the first observation in this case is the following.

1st Observation : (See [11, (2.2)Lemma]). The group algebra kN has five non-isomorphic simple modules $1_0 = k_N$ (the trivial module), 1_1, 1_2, 1_3, 2, where each 1_i has k-dimension one and 2 has k-dimension two. Then the Loewy and socle series of the projective covers of these five simple modules have the following form.

$$\begin{array}{c} 1_i \\ 2 \\ 1_j \ 1_{k'} \ 1_\ell \\ 2 \\ 1_i \end{array} \qquad\qquad \begin{array}{c} 2 \\ 1_0 \ 1_1 \ 1_2 \ 1_3 \\ 2 \ 2 \ 2 \\ 1_0 \ 1_1 \ 1_2 \ 1_3 \\ 2 \end{array}$$

where $\{i, j, k', \ell\} = \{0, 1, 2, 3\}$.

Then, let's go into the case of the principal block A of kG. Namely,

2nd Observation : The principal block ideal A of the group algebra kG has five non-isomorphic simple modules $S_0 = k_G$ (the trivial module), S_1, S_2, S_3, S_4, where S_1, S_2, S_3 have the same k-dimension $(q-1)(q^2-q+1)/3$, and S_4 has k-dimension $q^2 - q$. Then the Loewy and socle series of the projective covers of these five simple modules have the following form.

$$\begin{array}{c} i \\ 4 \\ j\;k'\;\ell \\ 4 \\ i \end{array} \qquad\qquad \begin{array}{c} 4 \\ 0\;1\;2\;3 \\ 4\;4\;4 \\ 0\;1\;2\;3 \\ 4 \end{array}$$

where $\{i, j, k', \ell\} = \{0, 1, 2, 3\}$ and we write m for S_m for $m = 0, 1, 2, 3, 4$.

Now, let's look at these two diagrams. They surely have the same shape. Thus, it would be natural to ask whether the two blocks A and B are Morita equivalent. Namely,

Question : Are A and B Morita equivalent ?

Answer (by Naoko Kunugi and the author) : YES!

Acknowledgements : The author would like to thank the organizers of this meeting (Alcom 97) for such a beautiful conference celebrating 70th birthday of Professor Michio Suzuki and for giving the author an opportunity to give a talk there. Especially, he would like to express his great thanks to Professors Eiichi Bannai and Hiroshi Suzuki.

References

[1] J.L. Alperin: *The main problem of block theory*, in "Proceedings of the Conference on Finite Groups", edited by W.R. Scott and F. Gross, Academic Press, New York, 1976, pp.341–356.

[2] ——: *Local representation theory*, in "The Santa Cruz Conference on Finite Groups", Proceedings of Symposia in Pure Math. Vol.37, Amer. Math. Soc., Providence, 1980, pp.369–375.

[3] ——: *Weights for finite groups*, in "The Arcata Conference on Representations of Finite Groups", Proceedings of Symposia in Pure Math. Vol.47, Amer. Math. Soc., Providence, 1987, pp.369–379.

[4] —: *A Lie approach to finite groups*, in "Groups-Canberra 1989", edited by L.G. Kovács, Springer Lecture Notes in Math. Vol.1456, Springer, Berlin, pp.1–9.

[5] M. Broué: *Isométries parfaites, types de blocs, catégories dérivées*, Astérisque 181–182 (1990), 61–92.

[6] —: *Isométries de caractéres et equivalences de Morita ou dérivées*, Inst. Hautes Études Sci. Pub. Math. 71 (1990), 45-63.

[7] —: *Equivalences of blocks of group algebras*, in "Finite Dimensional Algebras and Related Topics", edited by V. Dlab and L.L. Scott, Kluwer Acad. Pub., Dordrecht, 1994, pp.1–26.

[8] E.C. Dade: *Counting characters in blocks I*, Invent. math. 109 (1992), 187–210.

[9] —: *Counting characters in blocks II*, J. Reine Angew. Math. 448 (1994), 97–190.

[10] W. Feit: The Representation Theory of Finite Groups, North-Holland, Amsterdam, 1982.

[11] S. Koshitani: *On the Loewy series of the group algebra of a finite p-solvable group with p-length* > 1, Commun. Algebra 13 (1985), 2175–2198.

[12] G.O. Michler: *Contributions to modular representation theory of finite groups*, in "Representation Theory of Finite Groups and Finite-Dimensional Algebras", edited by G.O. Michler and C.M. Ringel, Progress in Math. 95, Birkhäuser, Basel, 1991, pp.99–140.

[13] H. Nagao and Y. Tsushima: Representations of Finite Groups, Academic Press, New York, 1988.

[14] T. Okuyama: *Some examples of derived equivalent blocks of finite groups*, in "Proceedings of the 6th Symposium on Representation Theory of Algebras" (held at Tateyama City, Chiba Prefecture, Japan) edited by S. Koshitani and M. Sato, 1996, pp.108–122 (in Japanese).

Shigeo Koshitani
Department of Mathematics
Faculty of Science
Chiba University
Yayoi-cho, Inage-ku
Chiba City, 263
Japan
E-mail `koshitan@math.s.chiba-u.ac.jp`

The Essentials of Monstrous Moonshine

JOHN M^c^KAY

Centre Interuniversitaire en Calcul Mathématique Algébrique,
Concordia University, Montreal, Canada

This is a fast introduction to Monstrous Moonshine.

All our functions expanded at $\tau = i\infty$ have the form:

$$(*) \qquad f(\tau) = \frac{1}{q} + \sum_{k\geq 0} a_k q^k, \quad q = e^{2i\pi\tau}, \quad \Im(\tau) > 0, \quad a_k \in \mathbb{C}.$$

We further assume that $a_0 = 0$ (standard form) for convenience, and that $a_k \in \mathbb{Q}$ (to ensure trivial Galois action). For replicable functions there is a reasonable conjecture that the a_k are algebraic integers - this, too, we assume. We find that the coefficients of classical modular functions known to Jacobi, Fricke, and Klein, are related to the characters of $\mathbb{M}$, the Monster simple sporadic group, in that, to each conjugacy class of cyclic subgroups $\langle g\rangle$, of $\mathbb{M}$, there is such a function, j_g with coefficient of $q^k = \text{Trace}\big(H_k(g)\big)$ for some representation, H_k, (the k^{th} Head representation) of $\mathbb{M}$.

In November 1978 I wrote to John Thompson that $196884 = 1 + 196883$, relating the coefficient of q in the elliptic modular function, $j(\tau)$, to the degree of the smallest faithful complex representation of $\mathbb{M}$. Little was then known to me of the degrees of irreducible characters of $\mathbb{M}$ but I did have access to those of $E_8(\mathbb{C})$ and related an initial sequence of them to the q-coefficients of the cube root of j. This was quickly disposed of by Victor Kac [Kac], see also [Lep].

There are 194 conjugacy classes of $\mathbb{M}$, 172 classes of cyclic subgroups, and 171 distinct functions j_g. This, and more, is to be found in Conway-Norton [CN]. All these functions are genus zero in that this is the genus of the compactified Riemann surface $\widehat{G_f\backslash\mathcal{H}}$ where G_f is the discrete invariance group of f, acting on the upper half-plane, $\mathcal{H}$.

By axiomatizing the properties of these functions, we arrive at the notion of a replicable function, as one which behaves well under a generalized Hecke operator. These are now under scrutiny. My hope is that their properties will yield an intrinsic description of $\mathbb{M}$.

We study replicable functions, which generalize a degenerate family called by me the "modular fictions", namely $f(\tau) = 1/q + cq$. Cummins [CuN] has proved these are the unique replicable finite Laurent series, $(\forall k \geq k_0,\, a_k = 0)$. A further useful property to impose is that the replication power map (defined later): $f \to f^{(n)}$, is periodic, namely $\forall n \geq 1$, $f^{(\gcd(n,k))} = f^{(n)}$. When this

Research supported by the Natural Sciences and Engineering Research Council (Canada) and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Québec)

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

is so, the modular fictions reduce to three cases, $1/q$, $1/q+q$, $1/q-q$, corresponding to exp, cos, and sin respectively. An amusing consequence of their replicability is that $\sin(2kt)$ is not a polynomial in $\sin(t)$, whereas $\cos(2kt)$ is a polynomial in $\cos(t)$. This follows from a study of the modular equation [Sil], [Mar] for f, with formal coefficients [McK]. The modular fictions play no further part in what follows.

Replicable functions are generalizations of the prototype, $j(\tau)$, the elliptic modular function which is characterized by its form and the property under the action of Hecke operators [Serre]:

$$\forall n \geq 1,\ nT_n(j(\tau)) = \sum_{\substack{ad=n \\ 0\leq b<d}} j\Big(\frac{a\tau+b}{d}\Big) = P_{n,j}(j(\tau)),$$

where T_n denotes the standard Hecke operator, and $P_{n,j} = P_n$ is the Faber [Fab, Cur] polynomial of degree n. The notation is to remind one that the coefficients of the Faber polynomial come from its argument.

One characterization of these polynomials is that

$$P_{n,f}(f) - \frac{1}{q^n} \in q\,\mathbb{C}[[q]].$$

We find

$$\begin{aligned} P_1(f) &= f, \\ P_2(f) &= f^2 - 2a_1, \\ P_3(f) &= f^3 - 3a_1 f - 3a_2, \\ P_4(f) &= f^4 - 4a_1 f^2 - 4a_2 f + 2a_1^2 - 4a_3. \end{aligned}$$

More generally:

$$P_n(f) = \det(A_n + fI)$$

where

$$A_n = \begin{pmatrix} e_1 & 1 & & & & \\ 2e_2 & e_1 & 1 & & 0 & \\ \vdots & \vdots & \vdots & & & \\ (n-2)e_{n-2} & e_{n-3} & e_{n-4} & \cdots & 1 & \\ (n-1)e_{n-1} & e_{n-2} & e_{n-3} & \cdots & e_1 & 1 \\ ne_n & e_{n-1} & e_{n-2} & \cdots & e_2 & e_1 \end{pmatrix}$$

with e_k replaced by $(-1)^k a_{k-1}$.

This is related to expressing the power sums in terms of elementary symmetric functions. Truncating f and replacing q by $1/x$, we derive: $F(x) = x^n + a_0 x^{n-1} + \cdots + a_{n-1}$ and we may identify the $\{e_k\}$ with the elementary symmetric functions of the roots of $F(x)$. Note that the power sum $s_k \in \mathbb{Z}[a_0, \ldots, a_{k-1}]$.

Expanding $P_{n,f}(f(\tau))$ in powers of q, the Grunsky [G] coefficients, $h_{m,n}$, are defined by

$$P_n(f(\tau)) = \frac{1}{q^n} + n \sum_{m\geq 1} h_{m,n} q^m,$$

We generalize j to a family of replicable functions (of standard form), $f^{(k)}$, $k \geq 1$, for which

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\Big(\frac{a\tau+b}{d}\Big) = P_{n,f}(f(\tau)).$$

This yields a new Hecke operator, $\hat{T}_n$ with $h_{m,n}$ as the coefficient of q^m in $\hat{T}_n(f)$. It is Grunsky's law of symmetry that $h_{m,n} = h_{n,m}$.

We now have an inductive definition of the important "replication power map" taking f to $f^{(n)}$, since $f^{(n)}(n\tau) = P_n(f) - \sum'$ where $\sum'$ omits the single term with $a = n$. This imposes the condition that the right side is a series in q^n. We take the principal branch to define $f^{(n)}(\tau)$. The replication power map f to $f^{(n)}$, f replicable, restricts on Monstrous Moonshine functions to the map induced on them by taking $g \in \mathbb{M}$ to g^n. Norton [N], in a important paper, defines the generating functions for the Faber polynomials and the $h_{m,n}$, unaware of the work of Faber [Fab] and Grunsky [G] preceding him. He gives an definition of replicability equivalent to the above, [ACMS], namely (paraphrased):

Definition. A function is replicable if $\gcd(m,n) = \gcd(r,s)$ and $\mathrm{lcm}(m,n) = \mathrm{lcm}(r,s)$ implies $h_{m,n} = h_{r,s}$.

[This suggests seeking an interpretation of the $\{h_{m,n}\}$ in terms of double coset representatives.]

Norton also proves his basis theorem:

Theorem. *The twelve coefficients a_k, $k \in \{1, 2, 3, 4, 5, 7, 8, 9, 11, 17, 19, 23\}$, determine a replicable function.*

This remarkable result is useful for computing with replicable functions.

Newton's relations, which derive from the form of f, between the a_k and the Faber polynomials, together with Norton's defining properties of the $\{h_{m,n}\}$, show that replicable functions correspond to K-points on a variety. Norton has proved that K lies in a composite of quadratic extensions of $\mathbb{Q}$.

The Newton relations are equivalent to the generating function identity:

$$q(f(q) - f(p)) = \exp\Big(-\sum_{n\geq 1} P_n(f(p))q^n\Big),$$

with $p = \exp(2\pi i\sigma)$ etc., where we abuse notation using $f(p)$ and $f(q)$ instead of $f(\sigma), f(\tau)$.

There is an outstanding conjecture of Norton [CuG], [CuN]:

Conjecture 1.2.. *A function $f = q^{-1} + \sum_{i\geq 1} a_i q^i$ with rational integer coefficients is replicable if and only if either f is a modular fiction or it is the Hauptmodul for a group $G \subset PGL_2(\mathbb{Q})^{>0}$ satisfying*

1. G has genus zero,
2. G contains a finite index $\Gamma_0(N)$,
3. G contains $z \mapsto z + k$ if and only if $k \in \mathbb{Z}$.

Our model is Dedekind's (1877) [Ded] construction of $j(\tau)$ in terms of its Schwarz differential equation.

We define the Schwarz derivative $\{f,\tau\}$ to be $2(f''/f')' - (f''/f')^2$, where differentiation is with respect to τ. When f is a modular form, $\{f,\tau\}$ increases the weight by 4 and preserves the invariance properties, thus when f is a Hauptmodul, we have $\{f,\tau\} + R(f)f'^2 = 0$ with $R(f) = N(f)/[D(f)]^2$, the differential resolvent, and $f' = df/d\tau$ of weight 2. When expressed in partial fractions, we see $R(f)$ gives ramification data (in N) and also the critical points of f (namely those values of f for which $f'(\tau) = 0$).

¿From Dedekind (with normalization $1728j(\tau) = 1/q + 744 + 196884q + \cdots$) we find

$$R(j) = \frac{1-\frac{1}{2^2}}{(j-1)^2} + \frac{1-\frac{1}{3^2}}{j^2} - \frac{1-\frac{1}{2^2}-\frac{1}{3^2}}{j(j-1)},$$

with ramification multiplicity 2 at $j\big(\exp(\pi i/2)\big) = 1$, and 3 at $j\big(\exp(\pi i/3)\big) = 0$.

To each f, there is a corresponding conformal invariance group, G_f acting on $\mathcal{H}$. From $R(f)$ we can find the critical points in $\mathcal{H}$, and the ramification gives the angles between bounding circular arcs intersecting at a critical point. A fundamental domain can be constructed and, once edges are identified, a presentation found for the group generated by hyperbolic reflections in the bounding circular arcs in $\mathcal{H}$. The Schwarz derivative takes us from f to G_f.

Over 600 Hauptmodules, f, as above, are now known, some of which appear in [FMN]. For each, $R(f)$ has been computed. The Galois group of D is of "dihedral type", in that it has a unique cyclic subgroup of index 2. This provides an ordering of the critical points for Ohyama's construction of dynamical systems [Ohy1]. With a little more work, we should obtain a dynamical system of differential equations for each f, as shown by Ohyama [Ohyl] and exemplified by the Halphen system. This system was first studied in 1881 [Hal], and is a reduction of the self-dual Yang-Mills equations. For us, it is derived from the $\Gamma(4)$-Hauptmodule, namely $f = \big(\eta(\tau)/\eta(4\tau)\big)^8$. This has a triangular fundamental domain with angles $(0,0,0)$ at cusps $(0,1,\infty)$. It is remarkable that we have $\{f,\tau\} + E_4(2\tau) = 0$, where $E_4(\tau)$ is the Eisenstein series of weight 4:

$$E_4(\tau) = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n.$$

In a further paper [Ohy2] the function $f = \big(\eta(\tau)/\eta(9\tau)\big)^3$ appears and we find it satisfies the Schwarz equation above with $E_4(2\tau)$ replaced by $E_4(3\tau)$.

Any function of the form (*) satisfies

$$\frac{df}{dq} + \frac{1}{q^2}\exp(-v^t H v) = 0,$$

where $v^t = (q, q^2, q^3, \dots)$, and H is the semi-infinite matrix of Grunsky coefficients.

To each Hauptmodul there are two differential objects:

(1) A Schwarz equation, and
(2) a dynamical system.

There is also a pseudo-differential operator (roughly-treating the functions as Laplace transforms) which has not yet been studied.

A purpose of this approach is to learn more about analytic aspects associated with the Monster in the hope of better understanding the relation between the simple Lie groups and the sporadic simple groups.

Witten's ideas suggest there may be a finite-dimensional spin manifold with M acting on its loop space. A discussion of this is found in the book [Hirz].

Acknowledgements: I thank the organizers of the Suzuki conference for inviting me, and especially, Professor Miyamoto for his hospitality in making it possible.

References

[ACMS] Alexander, D., Cummins, C., McKay, J., and Simons, C., *Completely replicable functions*, Lond. Math. Soc. Lecture Notes 165, edited by Liebeck and Saxl (1992), 87–98.

[CN] Conway, J.H., and Norton, S.P., *Monstrous moonshine*, Bull. Lond. Math. Soc. 11 (1979), 308–339.

[CuG] Cummins, C. J., Gannon, T., *Modular equations and the genus zero property of Moonshine functions*, Inv. Math. 129 (1997), 413–443.

[CuN] Cummins, C. J., Norton, S.P., *Rational Hauptmoduls are replicable*, Can. J. Math. 47 (1995), 1201–1218.

[Cur] Curtiss, J., H., *Faber polynomials and the Faber series*, Amer. Math. Monthly 78 and 79 (1974), 577–596 and 363.

[Ded] Dedekind, R., *Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen*, Crelle, 83, 265–292.

[Fab] Faber, G., *Über polynomische Entwicklungen*, Math. Annalen, 57 (1903), 389–408..

[FMN] Ford, D.J., McKay, J., and Norton, S.P., *More on replicable functions*, Comm. in Alg., 22 (1994), 5175–5193.

[G] Grunsky, H., *Koeffizientenbedingungen für schlicht abbildende meromorphe Funktionen*, Math. Zeit., 45 (1939), 29–61.

[Hir] Hirzebruch F., Berger T., Jung R., *Manifolds and Modular Forms (Vieweg)*, 1992.

[Kac] Kac V., *An elucidation of: "Infinite-dimensional algebras, Dedekind's η-function, classical Möbius function and the very strange formula". $E_8^{(1)}$ and the cube root of the modular invariant j*, Adv. in Math. 35 (1980), 264–273.

[Lep] Lepowsky, J., *Proc. Symp. Pure Math., 37, Amer. Math. Soc.*, 1980, pp. 567–570.

[Mar] Martin, Y., *On modular invariance of completely replicable functions*, Contemp. Math. 193 (1996), 263–286.

[McK] McKay, J., *The formal modular equation*, (unpublished).

[N] Norton, S.P., *Computational group theory, edited by M.D. Atkinson, Academic*, 1984, pp. 185–193.

[Ohy1] Ohyama, Y., *Systems of nonlinear differential equations related to second order linear equations*, Osaka J. Math. 33 (1996), 927–949.

[Ohy2] Ohyama, Y., *Differential equations for modular forms with level three*, To appear.

[Ser] Serre, J-P., *A course in arithmetic, Springer-Verlag*, 1973.

[Sil] Silverman, J.H., *Advanced topics in the arithmetic of elliptic curves, Springer-Verlag*, 1994, pp. 181.

E-mail address: mckay@cs.concordia.ca

The finite group theory on vertex operator algebras

Masahiko Miyamoto

Institute of Mathematics
University of Tsukuba
Tsukuba 305, Japan

0 Introduction

I put a large title, but I believe this is true. I was trying to use the group theoretic arguments for the theory of vertex operator algebras (shortly VOA) and I can now say that many techniques of the finite group theory are useful for the study of VOAs and there is a large area in the research of VOA for finite group theorists. "A vertex operator algebra", is a conformal field theory (in the physics) itself with a mathematically rigorous axioms, but it comes from a famous moonshine conjecture of the largest sporadic simple finite group "Monster". Recently, a vertex operator algebra is getting very popular in many subjects of mathematics. Compare to the finite group theory, it has an "infinite dimensional" vector space V with "infinitely many products" $\times_n : n \in \mathbb{Z}$ and complicated relations called Jacobi identity (or Borcherds identity). Also all calculations are done by formal power series, "distributions". In spite of these stuffs, it has many properties of the finiteness. The most important thing is that if a vertex operator algebra has a finite automorphism group, the study of the vertex operator algebra becomes very interesting and it is an area for the finite group theorists.

The groups appear in the study of VOAs are not only the monster simple group, but also other simple groups. Actually, I will show you one example of VOA whose the full automorphism group is $E_7(2)$ later. This is the second of an infinite series of VOAs in my constructions with the finite automorphism groups and the monster is the first one. My construction is not difficult. It is true that it is a very hard and complicated job if we construct a VOA from the beginning. But, we now have a lot of the known results about the conformal field theory done by many pioneers, for example, Feigin-Fuchs, Tsuchiya-Kanie, etc. As finite group theorists, we should aim the next steps. Every vertex operator algebra V contains a sub VOA called Virasoro algebra Vir, it is an axiom. My point is to factorize V by the action of Vir(or a suitable sub VOA W). Then some VOAs satisfies that "the set of intertwining operators V/W" looks like a finite object D, like a code, a lattice, and a finite group. For such a VOA, we can use the finite group theoretic methods. Conversely, we can expect to construct a VOA from the known and easy VOAs W and a finite object D.

The advantage of studying a vertex operator algebra with a finite group does not only offers a problems of the finite group theory, but also offers a relation between a finite group and a modular form. For example, we have many identities as Kitazume's talk in the conference.

I will summarize my results and separate my talk into five parts.

(1) A brief explanation of vertex operator algebras.

(2) Merits of automorphism group of vertex operator algebra

(2.i) Examples,

(2.ii) Determination of automorphism groups,

(3) $2A$-involution and Z_2-codes (Z_4-codes),

(4) $3A$-triality and Z_3-codes,

(5) Characters of automorphism groups

(5.i) Application to vertex operator algebra

(5.ii) Application to character theory

1 A brief introduction to VOA

In this section, we recall the definition of VOA and intertwining operators from [FLM] and [FHL].

Definition 1 *A vertex operator algebra is a Z-graded vector space* $V = \sum_{n=0}^{\infty} V_n$ *with finite dimensional homogeneous spaces* V_n*; equipped with a formal power series*

$$Y(v,z) = \sum_{n\in Z} v_n z^{-n-1} \in \mathrm{End}(V)[[z,z^{-1}]]$$

called the vertex operator of v for each $v \in V$ *satisfying the following* (1) $\sim$ (3).

(1) There is a specific element $\mathbf{1} \in V_0$ *called the vacuum such that*

(1.a) $Y(\mathbf{1},z) = 1_V$ *and*

(1.b) $v_{-1}\mathbf{1} = v$ *and* $v_n\mathbf{1} = 0$ *for all* $n \geq 0$.

(2) There is an specific element $\mathrm{w} \in V_2$ *called the Virasoro element such that*

(2.a) $\{L(n) := \mathrm{w}_{n+1}\}$ *is a Virasoro algebra generator, that is, they satisfy*

$$[L(m),L(n)] = (m-n)L(m+n) + \delta_{m+n,0}\frac{m^3-m}{12}c,$$

where $c \in \mathbb{C}$ is called the rank (or the central charge) of V,
(2.b) the $L(-1)$-derivative property:

$$[L(-1), Y(v,z)] = \frac{d}{dz}Y(v,z)$$

(2.c) $L(0)v_n = n1v_n$.
(3) Commutativity: for any $u, v \in V$

$$Y(v,z)Y(u,w) \sim Y(u,w)Y(v,z).$$

Here $A(z_1,z_2) \sim B(z_1,z_2)$ means that there is an integer N such that $(z_1-z_2)^N\{A(z_1,z_2)-B(z_1,z_2)\} = 0$.

Since VOA is a kind of algebra, we can think of its modules, irreducible modules, factor modules, completely reducible.

Definition 2 *A module for $(V, Y, 1, \mathrm{w})$ is a $\mathbb{Z}$-graded vector space $M = \oplus_{n\geq 0}M_n$ with finite dimensional homogeneous spaces M_n; equipped with a formal power series*

$$Y^M(v,z) = \sum_{n\in\mathbb{Z}} v_n^M z^{-n-1} \in (\mathrm{End}(M))[[z,z^{-1}]]$$

called the module vertex operator of v for $v \in V$ satisfying:
(1) $Y^M(1,z) = 1_M$;
(2) $Y^M(\mathrm{w},z) = \sum L^M(n)z^{-n-1}$ satisfies:
(2.a) the Virasoro algebra relations,
(2.b) the $L(-1)$-derivative property:

$$Y^M(L(-1)v,z) = \frac{d}{dz}Y^M(v,z), and$$

(2.c) $L^M(0)_{M_n} = (k_n)1_{M_n}$ for some $k_n \in \mathbb{C}$.
(3) Commutativity.

$$Y^M(v,z)Y^M(u,w) \sim Y^M(u,w)Y^M(u,z)$$

(4) Associativity:

$$Y(u_nv,z) = Y^M(u,z)_nY^M(v,z).$$

for $u, v \in V$ and $Y(u,z) = \sum u_nz^{-n-1}$.

Definition 3 *Let $(V, Y, 1, \mathrm{w})$ be a VOA and let (W^1, Y^1), (W^2, Y^2) and (W^3, Y^3) be three V-modules. An intertwining operator of type $\left(\begin{array}{ccc} & W^1 & \\ W^2 & & W^3 \end{array}\right)$ is a linear map*

$$\begin{array}{rccl} I(*, z): & W^2 & \to & (\mathrm{Hom}(W^3, W^1))\{z\} \\ & u & \to & I(u, z) = \sum_{n \in \mathbf{Q}} u_n z^{-n-1} \end{array}$$

satisfying:
(1) $L^1(-1)$-derivative property:

$$I(L^1(-1)u, z) = \frac{d}{dz} I(u, z).$$

(2) Commutativity: for $v \in V, u \in W^2$,

$$Y^1(v, z) I(u, z_1) \sim I(u, z_1) Y^3(v, z)$$

(3) Associativity:

$$I(v^1_n u, z) = Y(v, z)_n I(u, z).$$

Here the n-th normal product $Y(v, z)_n I(u, z)$ for intertwining operator is given by

$$\mathrm{Res}_{z_1} \{(z_1 - z)^n Y^1(v, z_1) I(u, z) - (-z + z_1)^n I(u, z) Y^3(v, z_1)\}$$

and $Y^i(\mathrm{w}, z) = \sum_{n \in \mathbf{Z}} L^i(n) z^{-n-2}$.

Definition 4 *$I_V \left(\begin{array}{ccc} & W^1 & \\ W^2 & & W^3 \end{array}\right)$ denotes the set of intertwining operators of type $\left(\begin{array}{ccc} & W^1 & \\ W^2 & & W^3 \end{array}\right)$. It is a vector space and its dimension is denoted by $N^{W^1}_{W^2, W^3}$. In order to denote the dimensions, we use an expression*

$$W^2 \times W^3 = \sum_W N^W_{W^2, W^3} W,$$

called "fusion rule", where W runs over all irreducible V-modules. We note that $N^W_{W^2, W^3}$ might be infinite, but we will deal only the case where $\sum_W N^W_{W^2, W^3}$ is finite.

Definition 5 *To simplify the notation, we sometimes omit V in $I_V \left(\begin{array}{ccc} & W^1 & \\ W^2 & & W^3 \end{array}\right)$.*

Remark 1 *Since $L(-1)$ satisfies the property of the derivation, it offers us a relation between a differential equation and a VOA.*

If a VOA has only a finitely many irreducible module and all modules are completely reducible, then such a VOA is called "rational". For a finite group theory, we will treat a "rational VOA". Since each irreducible module denotes a particle in Physics and a number of kind of particles should be finite, it is natural to study this kind of VOA. Especially, a vertex operator algebra with only one irreducible module is called "holomorphic". This is one of most important VOAs for the finite group theory.

2 Automorphism

An automorphism $\tau of V$ is one-to-one endomorphism of V satisfying $\tau(v \times_n u) = \tau(v) \times_n \tau(u)$ and keeping the grade. Let G be an automorphism group of V, then each V_n is a G-module and so we can get a character $tr(g)|_{V_n}$ like a finite group theory. The advantage of VOA is that since we have many V_ns and so we have a formal power series

$$ch(g,z) = \sum tr(g)|_{V_n} q^n, \qquad q = e^{2\pi i z}.$$

So the set of characters of a finite group plays an interesting role as a set. For example, [Zhu], [Dong, Li, Mason] have showed that if V is holomorphic, then

$$q^{-t/24} ch(g,z)$$

has a modular function with some congruent groups. Also, as I told you the Virasoro element has a property of the derivation and we can get many differential equations related to the characters of finite groups.

For example, the following is a joint work with M.Kitazume and H.Yamada. In 1991 Borwein showed

$$a(q)^3 - b(q)^3 = c(q)^3$$

for

$$\begin{aligned} a(q) &= \textstyle\sum_{(n,m)\in Z^2} q^{n^2+mn+m^2} \\ b(q) &= \textstyle\sum_{(n,m)\in Z^2} q^{(n+\frac{1}{3})^2+(m+\frac{1}{3})(n+\frac{1}{3})+(m+\frac{1}{3})^2} \\ c(q) &= \textstyle\sum_{(n,m)\in Z^2} w^{m-n} q^{n^2+mn+m^2} \end{aligned}$$

by using the modular forms, where $q = e^{2\pi i z}$. After him, several proofs are given by using a certain identities of Ramanjan [Bernat], infinite products [BBG], and codes and lattice [Sole'].

We can explain the explicit meaning of the both sides of this equality in terms of vertex operator algebras. The both terms are $\Delta(z)^6$ times of characters of conjugate two automorphisms of the vertex operator algebras of E_6-type. We can apply these arguments to many vertex operator algebras. Namely, a vertex operator algebra $V = \sum V_n$ and a pair of conjugate two automorphisms τ and σ of V are given, then we have an identity:

$$\sum tr(\tau)|_{V_n} q^n = \sum tr(\sigma)|_{V_n} q^n.$$

So the characters of finite group play an interesting role as a set. For example, if V is holomorphic, then

$$\sum tr(\tau)|_{V_n} q^n = \sum tr(\sigma)|_{V_n} q^n.$$

For this result and related topics, see the paper by Kitazume in this book.

3 $2A$ involution and Z_2-code (Z_4-code)

The important relation between a vertex operator algebra and a finite group is that some structure of sub VOA offers an automorphism of VOA.

For example, there is a classical conformal field theory called Ising model $L(\frac{1}{2}, 0)$. This has been studies well. I have proved that if VOA V contains an Ising model $L(\frac{1}{2}, 0)$, then it defines an automorphism τ of order at most 2. [M1996(1)]. Actually, on the moonshine VOA $V^\natural$, it defines a $2A$-element of the monster simple group. Use this property, we can easily prove the finiteness of the full automorphism group of the moonshine VOA. Also we can expect the phenomenon on $2A$-elements would be explained by this definition. If VOA V contains $L(\frac{1}{2}, 0)$ and τ is trivial, then we can define another automorphism σ of order at most 2. This automorphism satisfies a nice property. It is truly a generalization of the reflection. Such automorphisms satisfy the property of 3-transpositions.

As an application of binary codes, I prove the following: If we have an even linear binary code D, then we can construct a new VOA M_D called a code VOA [M1996(2)]. The construction is very simple, but they have interesting properties for the finite group theory. For an example, its representation has a deep relation with the representation of an extra special 2-group [M1997(1)]. Also, as in the paper of Kitazume in this book, many VOAs of this kind have a 3-transposition group as the full automorphism group. Using the representation theory of code VOAs and a Z_4-code, we find a new construction of the moonshine VOA [M1997(2)] and [M1997(3)].

The main result in our construction is:

Hypotheses II

(1) D and S are both even linear codes of length $8k$ and $S \subseteq D \cap D^{\perp}$.

(2) For any $\alpha, \beta \in S$, $(\alpha \neq \beta)$, there is subcode $E_\alpha \oplus E_{\alpha^c}$ of D and maximal self-orthogonal

subcodes H_β and $H_{\alpha+\beta}$ of K_β and $K_{\alpha+\beta}$, respectively, such that

(2.1) E_α and E_{α^c} are direct sums of $[8,4,4]$-Hamming codes

(2.2) $Supp(E_\alpha) = \alpha$ and $Supp(E_{\alpha^c}) = \alpha^c$,

(2.3) $H_\beta + E_\alpha + E_{\alpha^c} = H_{\alpha+\beta} + E_\alpha + E_{\alpha^c}$,

where $K_\alpha = \{\gamma \in D : Supp(\gamma) \subseteq Supp(\alpha)\}$ and $\alpha^c = (1^{8k}) - \alpha$ is the complement of α.

(3) There is an S-graded M_D-module $V = \oplus_{\alpha\in S} V^\alpha$ such that each V^α is an M_D-submodule with $\tilde{h}(V^\alpha) = \alpha$. In particular, $V^{(0^{8k})} \cong M_D$ as M_D-modules.

(4) For $\alpha, \beta \in S - \{(0^n)\}$ and $\alpha \neq \beta$,

$$M_D \oplus V^\alpha \oplus V^\beta \oplus V^{\alpha+\beta}$$

has a simple VOA structure containing M_D as a sub VOA.

Here $\tilde{h}(V^\alpha)$ denotes a binary word of length n satisfying that if a T-submodule is isomorphic to $\otimes L(\frac{1}{2}, h_i)$ then $h_i = \frac{1}{16}$ if and only if $i \in Supp(\tilde{h}(V^\alpha))$. We call $\tilde{h}(V^\alpha)$ "a $\frac{1}{16}$-word of V^α."

Our main aim in this paper is to prove the following theorem:

Theorem *Under the above assumptions (1)~(4) of Hypotheses II,*

$$V = \oplus_{\alpha\in S} V^\alpha$$

has a structure of simple VOA with M_D as a sub VOA. The structure of vertex operator algebra is uniquely determined up to M_D-isomorphisms.

Remark 2 Let's explain the above assumptions. (1) and (2) are conditions for the codes D and S. (3) is just a setting. Hence, the important condition is (4), but it is still a local condition. Among the conditions on the codes, (2) looks complicated. By (2.1) and (2.2), there is a tensor product of Hamming code VOAs such that each V^α decomposes into the direct sum of irreducible modules satisfying the condition (A). We use the assumption (2.3) in order to make the calculation easier. We are expecting that the similar result holds without the condition (2.3).

By this construction, if $D = S^\perp$, then we can construct a holomorphic VOA. Generally, from any above D and S, we can get a holomorphic VOA corresponding to $S^\perp$ and S. Actually, I constructed many holomorphic VOAs with the finite full automorphism groups. I want to characterize their full automorphism groups, but it is not an easy job for the researcher for VOAs. We need a lot of knowledge of the finite group theory to characterize them.

For example, I recently succeeded to characterize one of them. It is a VOA with rank 48 and the full automorphism group is $E_7(2)$.

4 $3A$-triality and Z_3-codes

The important finite objects for VOA are not only the binary code and an involution. We can also expect to get a similar result for other number. For example, we can expect an automorphism of order 3 from the Pott model $L(\frac{4}{5},0)$. This should correspond to 3A-triality of the monster simple group. In this case, the ternary codes will be also important. The paper of Yamada in this book is the initial work for this part. We can also construct a new VOA by using ternary codes. For an automorphism of order greater than or equal to 5, we don't know anything now, but we can expect a similar arguments.

5 Characters

Let G is a finite automorphism group of V and H a subgroup of G. Assume that χ is an irreducible character of G. In their paper [DM], they studied the sub VOA $V^H = \{v \in V : h(v) = v \forall h \in H\}$ of H-invariants and the subspace V^χ on which G acts according to the character χ and they conjectured the following Galois correspondence between sub VOAs of V and.subgroups of G and proved it for an Abelian or dihedral group G [DM, Theorem 1].

Conjecture 1 (Quantum Galois Theory) *Let V be a simple VOA and G a finite and faithful group of automorphisms of V. Then there is a bijection between the subgroups of G and the sub VOAs of V which contains V^G defined by the map $H \to V^H$.*

The following is a joint work with Akihide Hanaki. We translated the above conjecture into a problem of finite group. The following is equivalent to the quantum Galois theory for the solvable group G.

Conjecture 2 *Let G be a finite group and $\{M_\chi : \chi \in Irr(G)\}$ be the set of all simple modules of G. Assume M_{1_G} is a trivial module. Let R be a subspace of $M = \oplus_{\chi \in Irr(G)} M_\chi$ containing M_{1_G}. Assume that R satisfies the following condition: for any G-homomorphism $\pi : M \otimes M \to M$, $\pi(R \otimes R) \subseteq R$. Then there is a subgroup H of G such that $R = M^H$.*

For example, we can check that this conjecture is true for A_4.

6 After the conference

After the talk at the conference, D. Tambara has proved the above conjecture. So now my conjecture becomes a theorem and we have the quantum Galois theorem for solvable groups.

Namely, we prove the following theorems:

Theorem 6.1 *(D.Tambara) Let G be a finite group and $\{M_\chi : \chi \in Irr(G)\}$ be the set of all simple modules of G. Assume M_{1_G} is a trivial module. Let R be a subspace of $M = \oplus_{\chi\in Irr(G)} M_\chi$ containing M_{1_G}. Assume that R satisfies the following condition: for any G-homomorphism $\pi : M \otimes M \to M$, $\pi(R \otimes R) \subseteq R$. Then there is a subgroup H of G such that $R = M^H$.*

Theorem 6.2 *(A.Hanaki, M.Miyamoto, D.Tambara) Let V be a simple VOA and G a finite and faithful solvable group of automorphisms of V. Then there is a bijection between the subgroups of G and the sub VOAs of V which contains V^G defined by the map $H \to V^H$.*

References

[B] R.E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, Proc. Natl. Acad. Sci. USA 83 *(1986), 3068-3071*

[DM] C. Dong and G. Mason, On quantum Galois theory, Duke Math. J. 86 *(1997), no.2, 305-321.*

[DMZ] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math., American Math. Soc. 56 *II (1994), 295-316.*

[FHL] I. Frenkel, Y.-Z. Huang and J. Lepowsky, "On axiomatic approaches to vertex operator algebras and modules", Memoirs Amer. Math. Soc. 104, 1993.

[FLM] I.B. Frenkel, J. Lepowsky, and A. Meurman, Vertex Operator Algebras and the Monster, Pure and Applied Math., Vol. 134, Academic Press, 1988.

[M1] M. Miyamoto, *Griess algebras and conformal vectors in vertex operator algebras, J. Algebra* **179**, *(1996) 523-548*

[M2] M. Miyamoto, *Binary codes and vertex operator (super)algebras, J. Algebra* **181**, *(1996) 207-222*

[M3] M. Miyamoto, *Representation theory of code VOA, J. Algebra, to appear.*

[M4] M. Miyamoto, *Hamming code VOA and construction of VOAs, preprint.*

[M5] M. Miyamoto, *A construction of vertex operator algebra. I (The moonshine VOA), preprint.*

Primitive Trinomials and Orthogonal Arrays over GF(2)

Akihiro Munemasa
Graduate School of Mathematics
Kyushu University
Fukuoka, 812-81
Japan

The maximum-length shift-register sequences are widely used in generating pseudorandom numbers. The generation of shift-register sequences is particularly fast when the characteristic polynomial is a trinomial, that is, a polynomial with three terms. However, several authors pointed out that there are statistical biases in shift-resister sequences whose characteristic polynomials are trinomials. The purpose of this paper is to investigate such shift-register sequences from the viewpoint of orthogonal arrays.

Let GF(2) denote the field of two elements. Given a vector $v = (v_1, \ldots, v_n) \in \mathrm{GF}(2)^n$, we define

$$\begin{aligned} \mathrm{Supp}(v) &= \{i | v_i = 1,\ 1 \le i \le n\}, \\ \mathrm{wt}(v) &= |\,\mathrm{Supp}(v)|. \end{aligned}$$

A vector subspace C of $\mathrm{GF}(2)^n$ is called a linear code. The minimum weight of C is defined by

$$\min\{\mathrm{wt}(v) | 0 \ne v \in C\}.$$

The dual code of C is defined by

$$C^\perp = \{w \in \mathrm{GF}(2)^n | v \cdot w = 0 \text{ for all } v \in C\},$$

where $v \cdot w = \sum_{i=1}^n v_i w_i$. For a subset $T = \{i_1, i_2, \ldots, i_t\}$ of $\{1, 2, \ldots, n\}$, we denote by $v|T$ the restriction of the vector to the coodinate positions T, that is,

$$v|T = (v_{i_1}, \ldots, v_{i_t}) \in \mathrm{GF}(2)^t.$$

For a subset C of $\mathrm{GF}(2)^n$ and a vector $b \in \mathrm{GF}(2)^t$ with $1 \le t \le n$, we define

$$\lambda_b^T(C) = |\{v \in C |\, v|T = b\}|.$$

This means that we count the number of vectors $v \in C$ whose restriction to T coincides with a given vector b of a shorter length. A subset C of $\mathrm{GF}(2)^n$ is called an orthogonal array of strength t if $\lambda_b^T(C) = |C|/2^t$ holds for all t-subset T of $\{1, 2, \ldots, n\}$ and for all vector $b \in \mathrm{GF}(2)^t$. Let me illustrate the situation. Regarding C as a matrix, because C is a set of vectors, we may arrange its elements as row vectors of a matrix. Now T is a set of columns. $\lambda_b^T(C)$ is the number of occurences of the vector b in the submatrix of C consisting of columns corresponding to the set T. Note that there are 2^t choices for b so the number $|C|/2^t$ makes sense.

If one takes $C = GF(2)^n$, then C is an orthogonal array of strength t for all t. Another remark is that an orthogonal array of strength t is automatically an orthogonal array of strength s for any $s \leq t$. The strength t measures uniformity of distribution of C in $GF(2)^n$.

Minimum weight of codes and strength of orthogonal arrays are related by duality, according to the Theorem of Delsarte. In general, an orthogonal array does not have to be a subspace, but when it is a subspace, then the following theorem holds.

Theorem 1 (Delsarte). *Let C be a linear code over* $\mathrm{GF}(q)$. *Then C is an orthogonal array of maximal strength t if and only if $C^\perp$ has minimum weight $t+1$.*

Here 'maximum' means that t is the largest integer such that C is an orthogonal array of strength t.

In other words, if one has a linear code with large minimum weight, then its dual is an orthogonal array with large strength.

The next theorem describes the behaviour of an orthogonal array of strength $t-1$ when we take a set of t columns (or coodinate positions). When one takes T to be a t-element set, then $\lambda_b^T(C)$ may no longer be $\frac{|C|}{2^t}$ which is the average, but indeed, $\lambda_b^T(C)$ is equal to $\frac{|C|}{2^t}$ unless you are in the exceptional cases here. In the example we will discuss later, the exceptional case is indeed minority.

Theorem 2. *Let C be a linear code of length n over* $\mathrm{GF}(q)$ *and assume that C is an orthogonal array of strength $t-1$. Then for any t-subset T of $\{1, \ldots, n\}$ and for any t-tuple $b \in \mathrm{GF}(q)^t$, we have*

$$\lambda_b^T(C) = \begin{cases} \delta_{(u|_T, b), 0} \frac{|C|}{q^{t-1}} & \textit{if } T = \mathrm{Supp}(u) \textit{ for some } u \in C^\perp, \\ \frac{|C|}{q^t} & \textit{otherwise.} \end{cases}$$

Next we want to define primitive polynomials. Let $f(x)$ be an irreducible polynomial of degree m over GF(2). The polynomial $f(x)$ is called primitive if a root of $f(x)$ in $\mathrm{GF}(2^m)$ has order $2^m - 1$. If a root of $f(x)$ has this property, then so does any other root. This means a root of $f(x)$ is a generator of the multiplicative group of the splitting field. If we write $f(x)$ as the leading term plus the sum of the rest

$$f(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$$

then we can define a shift-register sequence to be a sequence satisfying the reccurrence relation determined by $f(x)$ with a nonzero initial value:

$$a_{k+m} = \sum_{i=0}^{m-1} c_i a_{k+i}, \quad (a_0, a_1, \ldots, a_{m-1}) \neq (0, \ldots, 0).$$

Of course you can define shift-register sequence for any polynomial, but when $f(x)$ is primitive, then the sequence has least period $2^m - 1$. Since any segment of length m determines the rest of the sequence by the recurrence relation, this means that all nonzero vectors of dimension m appear in $\{a_k\}_{k=0}^{\infty}$.

As we wrote earlier, the strength t of an orthogonal array is a measure for uniformity. We want to apply this measure to determine uniformity of shift-register sequences. In order to do this, we need to convert shift-register sequence to a subspace of GF(2)^n. An obvious way to do this is to take all segments of length n, $m \leq n \leq 2^m - 1$. To avoid triviality we will assume $m \leq n \leq 2^m - 1$. A little bit artificial, but we want to add the zero vector which can not appear as a segment of the sequence. So we denote by C_n the set of all subsequences of length n, together with the zero vector of length n. Then C_n is a GF(2)-vector subspace of the vector space GF(2)^n. If $n < m$, then $C_n = GF(2)^n$. If $n > 2^m - 1$, then the periodicity of the sequence implies that there exist two coordinate positions such that any vectors in C_n has the same entries in these positions. So it is a sort of duplicates.

An important property of C_n is that it is an orthogonal array of strength 2. This can be proved directly, or if you notice that $C_{2^m-1}^{\perp}$ is the so-called Hamming code. By Delsarte's theorem, C_{2^m-1} is an orthogonal array of strength 2. But when you make n smaller, then the property of being an orthogonal array is preserved. Let us apply the previous theorem with $t = 3$. In order to know when these irreugularities occur, we need to determine $C_n^{\perp}$, and the elements of $C_n^{\perp}$ of weight 3. $C_n^{\perp}$ is easy to determine but in general, it is difficult to determine the set of elements of weight 3 in $C_n^{\perp}$.

We are interested in elements of weight 3 in $C_n^{\perp}$ which may be regarded as polynomials of degree less than n with only three terms. A polynomial with three terms is called a trinomial. Note that $C_n^{\perp}$ depends on the choice of $f(x)$, and there are many primitive polynomial of given degree m, so it is very difficult to say anything exact about the set of trinomials of degree less than n divisible by $f(x)$. But when $f(x)$ itself is a trinomial, then we can actually determine all trinomials of degree at most $2 \deg f$ divisible by $f(x)$.

Maybe we should say a few words about why we assume $f(x)$ to be a trinomial. In the early days of pseudorandom number generation, shift-register sequences were used to generate pseudorandom numbers. Shift-register sequences are extremely easy to generate, yet it has very long period. Furthermore, if $f(x)$ has very few terms like 3, then the generation of shift-register sequences is very fast, because the recurrence is very simple. This is why people were interested in primitive trinomials. So we want to investigate trinomials divisible by a given trinomial.

The next theorem determines trinomials divisible by a given trinomial. The trinomial $f(x)$ doesn't have to be primitive, or even irreducible. The proof of this theorem is purely combinatorial.

Theorem 3. *Let $f(x) = x^m + x^l + 1$ be a trinomial such that $m > 2l$, $m \geq 4$, and assume that either m is not divisible by l, or $l = 1$. If $g(x)$ is a trinomial of degree at most $2m$ divisible by $f(x)$, then $g(x) = x^{\deg g - m} f(x)$ or $g(x) = f(x)^2$.*

From this we obtain our main result.

Main Theorem. *Let $f(x) = x^m + x^l + 1$ be a primitive trinomial of degree m over*

GF(2), *and let* $a = (a_0, a_1, a_2, \dots)$ *be the sequence defined by*

$$a_{k+m} = a_{k+l} + a_k \qquad (k = 0, 1, 2, \dots) \tag{1}$$

with $(a_0, \dots, a_{m-1}) \neq (0, \dots, 0)$. *Let* n *be a positive integer satisfying* $m < n \leq 2m + 1$, *and let* C_n *be the set of all subsequences of* a *of length* n, *together with the zero vector of length* n:

$$C_n = \{(a_k, \dots, a_{k+n-1}) | k = 0, 1, 2, \dots\} \cup \{(0, \dots, 0)\}. \tag{2}$$

Define

$$T_n = \begin{cases} \{\{i, i+l, i+m\} | 1 \leq i \leq n - m\} & \text{if } n \leq 2m, \\ \{\{i, i+l, i+m\} | 1 \leq i \leq n - m\} \cup \{\{1, 2l+1, 2m+1\}\} & \text{if } n = 2m + 1. \end{cases}$$

Then for any 3-subset $\{i_1, i_2, i_3\}$ *of* $\{1, \dots, n\}$ *and for any triple* $b = (b_1, b_2, b_3) \in \mathrm{GF}(2)^3$, *the number of elements* $v \in C_n$ *satisfying* $v_{i_1} = b_1$, $v_{i_2} = b_2$, $v_{i_3} = b_3$ *is* $\delta_{b_1+b_2+b_3,0}2^{m-2}$ *if* $\{i_1, i_2, i_3\} \in T_n$, 2^{m-3} *otherwise.*

The point is that the number of exceptional cases is rather small compared with the set of all 3-elements subsets of $\{1, 2, \dots, n\}$.

Remark 4. One might wonder how much Theorem 3 can be improved. The weight enumerator of the Hamming code $C^{\perp}_{2^m-1}$ is known [6]. In particular, there are $(2^m - 1)(2^{m-1} - 1)/3$ trinomials of degree less than $2^m - 1$ divisible by a primitive polynomial. Thus we can not expect to find a small set of exceptions like T_n consisting of the set of supports of elements of weight 3. It may be interesting to determine trinomials of small degree divisible by a primitive polynomial $f(x)$, when $f(x)$ has more than three terms. A particular case of this question was raised by Takashima [8]. It would be very interesting if we could find primitive polynomials which maximize the integer n such that C_n is an orthogonal array of strength 3. For a primitive polynomial f with more than three terms, C_n can become an orthogonal array of strength 4, but such an integer n can not be very large due to Rao's bound

$$1 + n + \binom{n}{2} \leq |C_n| = 2^m.$$

Acknowledgments

The author would like to thank Keizo Takashima for helpful discussions, and showing him computational evidence which lead him to prove Theorem 3. Thanks are due also to Jürgen Bierbrauer for greatly simplifying the proof of Theorem 2.

References

[1] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. Control, 23 (1973), 407–438.

[2] H. F. Jordan and D. C. M. Wood, On the distribution of sums of successive bits of shift-register sequences, IEEE Trans. Comp., C-22 (1973), 400–408.

[3] Lidl and H. Niederreiter, "Finite Fields", Cambridge Univ. Press.

[4] J. H. Lindholm, An analysis of the pseudo-randomness properties of subsequences of long m-sequences, IEEE Trans. Inform. Theory, IT-14 (1968), 569–576.

[5] A. Munemasa, Orthogonal arrays, primitive trinomials, and shift-register sequences, submitted.

[6] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam 1977.

[7] C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, J. Royal Stat. Soc., 9 (1947), 128–139.

[8] K. Takashima, On the number of multiples of certain primitive polynomials over GF(2), preprint.

On the covering radius problem for ternary self-dual codes.

Michio Ozeki
Department of Mathematical Sciences
Faculty of Science
Yamagata University
1-4-12, Koshirakawa-chou, Yamagata
Japan
email address : ozeki@kszaoh3.kj.yamagata-u.ac.jp

1 Introduction

1.1 Basic notions

Let $\mathbf{F}_3 = GF(3)$ be the Galois field of three elements. Let $V = \mathbf{F}_3^n$ be the vector space of dimension n over $\mathbf{F}_3$, equipped with the usual inner product which is denoted by

$$(\mathrm{x},\mathrm{y}) = x_1y_1 + x_2y_2 + \cdots + x_ny_n,$$

where

$$\mathrm{x} = (x_1, x_2, \ldots, x_n), \quad \mathrm{y} = (y_1, y_2, \ldots, y_n) \in V.$$

The Hamming distance $d(\mathrm{x},\mathrm{y})$ between two vectors x and y in V is defined to be the number of indeces i with $1 \leq i \leq n$ such that $x_i \neq y_i$. The Hamming sphere $S_r(\mathrm{u})$ of radius r with center $\mathrm{u} \in V$ is the subset of V defined by

$$S_r(\mathrm{u}) = \{\mathrm{x} \mid d(\mathrm{u},\mathrm{x}) \leq r\} .$$

A ternary linear code C is a vector subspace of V. The dual code $C^{\perp}$ of C is a subspace of V defined by

$$C^{\perp} = \{x \in V \mid (x, u) = 0 \ \forall u \in C\}$$

A self-dual code is a code C which satisfies $C = C^{\perp}$.

When bfC is a ternary self-dual code, it is known that

$$d(C) \leq 3\left[\frac{n}{12}\right] + 3.$$

A self-dual code C satisfying $d(C) = 3\left[\frac{n}{12}\right] + 3$ is called an extremal ternary self-dual code.

1.2 Statement of the Problem

The covering radius problem is to determine the least value r for which the condition

$$V = \bigcup_{u \in C} S_r(u)$$

holds for a given code C.

Notation : The least such r is denoted by $\rho(C)$.
It is known that $\rho(C)$ is bounded by

$$\lfloor \frac{d-1}{2} \rfloor \leq \rho(C) \leq s(C^{\perp}),$$

where $d = d(C)$ is the minimal distance of C and $s(C^{\perp})$ the number of nonzero distances in $C^{\perp}$.

Another formulation of $\rho(C)$ is

$$\begin{aligned} \rho(C) &= \max_{v \in F_3^n}\left(\min_{z \in -v+C} wt(z)\right) \\ &= \max_{v \in F_3^n}\left(\min_{z \in v+C} wt(z)\right) \end{aligned}$$

Here $\min_{z \in v+C} wt(z)$ is the minimal value of the weights in the coset $v + C$ (an element of the coset space F_3^n/C). This value is called the weight of the coset v + C. Thus $\rho(C)$ is the maximal value of the weights of the cosets v+C (for $v \in F_3^n$). The following table gives the values of $\lfloor\frac{d-1}{2}\rfloor, s(C^\perp), \rho(C)$ for the first few ternary self-dual extremal codes.

code	$\lfloor\frac{d-1}{2}\rfloor$	$s(C^\perp)$	$\rho(C)$
[4,2,3]	1	1	1
[8,4,3]	1	2	2
[12,6,6]	2	3	3
[16,8,6]	2	4	4 *
[20,10,6]	2	5	5 *
[24,12,9]	4	6	? (possible to determine)
[28,14,9]	4	7	?
[32,16,9]	4	8	?
[36,18,12]	5	9	?
[40,20,12]	5	10	?
[44,22,12]	5	11	?

The numbers marked * will be determined by our present paper.
In earlier papers ([1],[9],[10],[11]) we developed a method to determine the covering radius of binary self-dual binary codes. In this paper we show how to modify the method so as to apply to ternary self-dual codes.

2 An algebraic method to treat the problem

We treat the problem algebraically.
We aim not only the weights of the cosets but all the weights in each coset. These informations are important for analyzing the effectiveness of the code C.

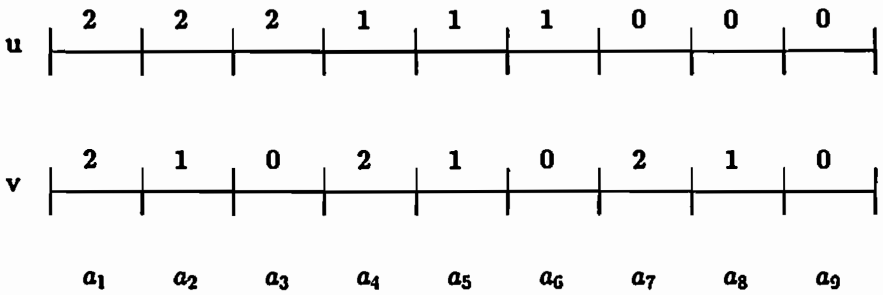
To describe the various weights in a coset v + C, one may consider the coset weight enumerator

$$W_{v+C}(X) = \sum_{u \in C} X^{wt(u+v)}$$

or in a homogeneous form

$$W_{v+C}(X,Y) = \sum_{u \in C} X^{n-wt(u+v)} Y^{wt(u+v)}$$

To capture a property of the weight function wt, one may consider the following picture:



The symbol a_1 implies the cardinality

$$a_1 = |\{i \mid u_i = v_i = 2 \ 1 \leq i \leq n\}|$$

Similarly $a_2, \cdots, a_9$ are defined.
On this notations we introduce some functions:

$$\begin{aligned} \mathrm{u} * \mathrm{v} &= |\{i \mid u_i \neq 0, v_i \neq 0 \ 1 \leq i \leq n\}| \\ \mathrm{u} \sharp \mathrm{v} &= |\{i \mid u_i = v_i \neq 0 \ 1 \leq i \leq n\}| \\ \mathrm{u} \natural \mathrm{v} &= |\{i \mid u_i \neq 0, v_i \neq 0, u_i \neq v_i \ 1 \leq i \leq n\}| \end{aligned}$$

By definition we have

$$\begin{aligned} \mathrm{u} * \mathrm{v} &= a_1 + a_2 + a_4 + a_5 \\ \mathrm{u} \sharp \mathrm{v} &= a_1 + a_5 \\ \mathrm{u} \natural \mathrm{v} &= a_2 + a_4, \end{aligned}$$

and consequently

$$\begin{aligned} wt(\mathrm{u} + \mathrm{v}) &= wt(\mathrm{u}) + wt(\mathrm{u}) - 2\mathrm{u} * \mathrm{v} + \mathrm{u} \sharp \mathrm{v} \\ &= wt(\mathrm{u}) + wt(\mathrm{u}) - 2\mathrm{u} \natural \mathrm{v} - \mathrm{u} \sharp \mathrm{v} \end{aligned}$$

Thus the coset weight enumerater $W_{\mathbf{v}+\mathbf{C}}(X)$ is rewritten as

$$W_{\mathbf{v}+\mathbf{C}}(X) = X^{wt(\mathbf{v})} \sum_{\mathbf{u}} X^{wt(\mathbf{u})-2\mathbf{u}\bullet\mathbf{v}+\mathbf{u}|\mathbf{v}}$$

Our starting point is to consider a polynomial in three variables (we call it a modified Jacobi polynomial):

$$M\text{-}Jac(\mathrm{C}, \mathrm{v}; X, Y, Z) = \sum_{\mathbf{u}\in\mathbf{C}} X^{wt(\mathbf{u})} Y^{\mathbf{u}|\mathbf{v}} Z^{\mathbf{u}\natural\mathbf{v}}.$$

From this polynomial one may easily obtain

$$\begin{aligned}
& X^{wt(\mathbf{u})} M\text{-}Jac(\mathrm{C}, \mathrm{v}; X, X^{-1}, X^{-2}) \\
&= \sum_{\mathbf{u}} X^{wt(\mathbf{u})+wt(\mathbf{v})} X^{-\mathbf{u}|\mathbf{v}} X^{-2\mathbf{v}\natural\mathbf{u}} \\
&= \sum_{\mathbf{u}\in\mathbf{C}} X^{wt(\mathbf{u})+wt(\mathbf{v})-\mathbf{u}|\mathbf{v}-2\mathbf{v}\natural\mathbf{u}} \\
&= \sum_{\mathbf{u}\in\mathbf{C}} X^{wt(\mathbf{u}+\mathbf{v})} \\
&= W_{\mathbf{v}+\mathbf{C}}(X)
\end{aligned}$$

The polynomial $M\text{-}Jac(\mathrm{C}, \mathrm{v}; X, Y, Z)$ has a transformation formula :

$$\begin{aligned}
& M\text{-}Jac(\mathrm{C}^{\perp}, \mathrm{v}; X, Y, Z) \\
&= \frac{1}{|\mathrm{C}|}(1+2X)^{n}\left[\frac{1+XY+XZ}{1+2X}\right]^{wt(\mathbf{v})} \times \\
&\quad M\text{-}Jac(\mathrm{C}, \mathrm{v}; \frac{1-x}{1+2X}, \frac{(1+\omega XY+\omega^2 XZ)(1+2X)}{(1-X)(1+XY+XZ)}, \frac{(1+2X)(1+\omega^2 XY+\omega XZ)}{(1-X)(1+XY+XZ)}),
\end{aligned}$$

where $|\mathrm{C}| = 3^{\frac{n}{2}}$ and ω is the cubic root of 1 :$\omega = e^{\frac{2\pi i}{3}}$.
The polynomial $M\text{-}Jac(\mathrm{C}, \mathrm{v}; X, Y, Z)$ is better understood by homogenizing it :

$$HM\text{-}Jac(\mathrm{C}, \mathrm{v}; x, y, u, v, w) = \sum_{\mathbf{u}\in\mathbf{C}} x^{n-wt(\mathbf{u})-wt(\mathbf{v})+\mathbf{u}\bullet\mathbf{v}} y^{wt(\mathbf{u})-\mathbf{u}\bullet\mathbf{v}} u^{wt(\mathbf{v})-\mathbf{u}\bullet\mathbf{v}} v^{\mathbf{u}|\mathbf{v}} w^{\mathbf{v}\natural\mathbf{u}}.$$

The homogenized modified Jacobi polynomial satisfies the identity :

$$HM\text{-}Jac(\mathrm{C}^{\perp},\mathrm{v};x,y,u,v,w) =$$
$$\frac{1}{|\mathrm{C}|}HM\text{-}Jac(\mathrm{C},\mathrm{v};x+2y,x-y,u+v+w,u+\omega v+\omega^2 w,u+\omega^2 v+\omega w).$$

Here we give the homogenization process and the dehomogenization process. homogenization:

$$x^n\left(\frac{u}{x}\right)^{wt(\mathrm{v})} M\text{-}Jac(\mathrm{C},\mathrm{v};\frac{y}{x}(\frac{xv}{yu}),(\frac{xw}{yu})) =$$
$$\sum_{\mathrm{u}\in\mathrm{C}} x^{n-wt(\mathrm{u})-wt(\mathrm{v})+\mathrm{u}\cdot\mathrm{v}}y^{wt(\mathrm{u})-\mathrm{u}\cdot\mathrm{v}}u^{wt(\mathrm{v})-\mathrm{u}\cdot\mathrm{v}}v^{\mathrm{u}\|\mathrm{v}}w^{\mathrm{v}|\mathrm{u}}.$$

dehomogenization :

$$HM\text{-}Jac(\mathrm{C},\mathrm{v},1,X,1,XY,XZ) = M\text{-}Jac(\mathrm{C},\mathrm{v};X,Y,Z)$$

3 Connection with the theory of invariants for finite transformation groups

3.1 Group of invariance for modified Jacobi polynomials

If C is self-dual, it is known that 4 divides n. In this case $HM\text{-}Jac(\mathrm{C},\mathrm{v};x,y,u,v,w)$ satisfies

$$HM\text{-}Jac(\mathrm{C}^{\perp},\mathrm{v};x,y,u,v,w) = HM\text{-}Jac(\mathrm{C},\mathrm{v};x',y',u',v',w'),$$

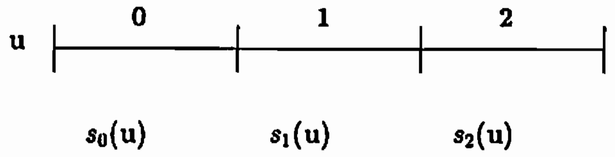
where

$$\begin{pmatrix} x' \\ y' \\ u' \\ v' \\ w' \end{pmatrix} = \frac{1}{\sqrt{3}}\left(\begin{array}{cc|ccc} 1 & 2 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & \omega^2 & \omega \end{array}\right)\begin{pmatrix} x \\ y \\ u \\ v \\ w \end{pmatrix},$$

where ω is a cube root of unity.

For further algebraic investigation it is convenient to assume that

The code C contains 1 (all one vector).
This assumption will eliminate the important class of codes (code of length's not divisible by 12). We consider the picture :



The condition $(\mathrm{u},\mathrm{u}) = 0$ implies $s_1(\mathrm{u}) + s_2(\mathrm{u}) \equiv 0 \bmod 3$.
The condition $(\mathbf{1},\mathrm{u}) = 0$ implies $s_1(\mathrm{u}) \equiv s_2(\mathrm{u}) \bmod 3$,
therefore we have

$$s_1(\mathrm{u}) \equiv 0 \bmod 3 \text{ and } s_2(\mathrm{u}) \equiv 0 \bmod 3$$

The condition $(\mathbf{1},\mathbf{1}) = 0$ implies that $n \equiv 0 \bmod 3$. If we remark that

$$s_0(\mathrm{u}) + s_1(\mathrm{u}) + s_2(\mathrm{u}) = 0,$$

we have $s_0(\mathrm{u}) \equiv 0 \bmod 3$.
Consider the substitutions

$$x \mapsto \omega x,\quad y \mapsto y,\quad u \mapsto \omega u,\quad v \mapsto v,\quad w \mapsto w$$

then each term of $HM\text{-}Jac(\mathrm{C},\mathrm{v};x,y,u,v,w)$ is multiplied by ω to the exponent

$$n - wt(\mathrm{u}) - wt(\mathrm{v}) + \mathrm{u} * \mathrm{v} + wt(\mathrm{v}) - \mathrm{u} * \mathrm{v} = s_0(\mathrm{u}) \equiv 0 \bmod 3,$$

Therefore we have

$$HM\text{-}Jac(\mathrm{C},\mathrm{v};\omega x,y,\omega u,v,w) = HM\text{-}Jac(\mathrm{C},\mathrm{v};x,y,u,v,w).$$

If we denote the group of linear transformations, which leaves $HM\text{-}Jac$ invariant by $Inv(HM\text{-}Jac)$, then we have

$$Inv(HM\text{-}Jac) \ni L_2 = diag(\omega,1,\omega,1,1)$$

Likewise we have

$$Inv(HM\text{-}Jac) \ni diag(1,\omega,1,\omega,\omega)$$

and

$$Inv(HM\text{-}Jac) \ni L_3 = diag(\zeta_{12},\zeta_{12},\zeta_{12},\zeta_{12},\zeta_{12}),$$

where ζ_{12} is the 12-th root of unity.
One may remark that as the size of the code C (i.e n) increases the group of invariance $Inv(HM\text{-}Jac(\mathrm{C})$ will become larger. For instance if C has length 24. then $Inv(HM\text{-}Jac(\mathrm{C})$ contains $diag(\zeta_{24},\zeta_{24},\zeta_{24},\zeta_{24},\zeta_{24})$, the diagonal matrix with diagonal entries all ζ_{24} the 24-th root of unity .
Let $G_3 =< L_1, L_2, L_3 >$ be the group generated by L_1, L_2 and L_3.
Our main strategy is first to study $\mathbb{C}[x,y,u,v,w]^{G_3}$, the ring of polynomials in the variables x,y,u,v,w that are invariant under the natural action of G_3.
One major clue for this is the Molien series $\Phi_{G_3}(\lambda)$ for G_3 . One has

$$\begin{aligned} &\Phi_{G_3}(\lambda) \\ = &\ \frac{1+91\lambda^{12}+474\lambda^{24}+287\lambda^{36}+11\lambda^{48}}{(1-\lambda^{12})^5} \\ = &\ 1+96\lambda^{12}+944\lambda^{24}+4057\lambda^{36}+11811\lambda^{48}+27441\lambda^{60}+\cdots \end{aligned}$$

3.2 Other groups of linear transformations

Let $CW(\mathrm{C},x,y,z)$ be the complete weight enumerator for ternary code C:

$$CW(\mathrm{C},x,y,z) = \sum_{\mathbf{u}\in\mathrm{C}} x^{s_0(\mathbf{u})}y^{s_1(\mathbf{u})}z^{s_2(\mathbf{u})},$$

where the exponents $s_0(\mathrm{u}), s_1(\mathrm{u}), s_2(\mathrm{u})$ are already explained.
As before we assume that C is self-dual and contains 1. Then we can show that the group of invariance for $CW(\mathrm{C},x,y,z)$ contains

$$\begin{aligned} M_1 &= \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \\ M_2 &= \begin{pmatrix} \zeta_{12} & 0 & 0 \\ 0 & \zeta_{12} & 0 \\ 0 & 0 & \zeta_{12} \end{pmatrix} \end{aligned}$$

$$\begin{aligned} M_3 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ M_4 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix} \end{aligned}$$

We put

$$G_1 = < M_1, M_2, M_3, M_4 >,$$

the group generated by M_i's. The order of G_1 is 2592. One also has the Molien series $\Phi_{G_1}(\lambda)$ for G_1 :

$$\Phi_{G_1}(\lambda) = \frac{1+\lambda^{24}}{(1-\lambda^{12})^2(1-\lambda^{36})}$$

basic polynomials corresponding to the denominator of $\Phi_{G_1}(\lambda)$

(0) Preliminary polynomials.

$$\begin{aligned} \alpha_1 &= x^3 + y^3 + z^3 \\ \alpha_2 &= 3xyz \\ \alpha_3 &= x^3y^3 + x^3z^3 + y^3z^3 \\ \alpha_4 &= \alpha_1(\alpha_1^3 + 8\alpha_2^3) \\ \alpha_5 &= \alpha_1^2 - 12\alpha_3 \\ \alpha_6 &= \alpha_1^6 - 20\alpha_1^3 - 8\alpha_2^6 \\ \alpha_7 &= \alpha_2^3(\alpha_1^3 - \alpha_2^3)^3 \end{aligned}$$

the denominator polynomials for $\psi_{G_1}(\lambda)$ are given by α_4, and α_5^2.
The numerator polynomial for $\psi_{G_1}(\lambda)$ is given by $\alpha_5\alpha_6$. The group G_1 has a subgroup H_1. H_1 consists of elements which leave the polynomial

$$(x^3 + y^3 + z^3)^2 - 12(x^3y^3 + x^3z^3 + y^3z^3)$$

invariant. The order of H_1 is 1296, and $[G_1 : H_1] = 2$.
Molien series for H_1 is well known :

$$\Phi_{H_1}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^{12})(1-\lambda^{18})}.$$

λ^6 corresponds to the above polynomial of degree 6, λ^{12} corresponds to complete weight enumerator of ternary Golay [12,6,6] code, and λ^{18} corresponds to α_6 before given.

3.3 Ring of simultaneous invariants for G and its Molien series.

The polarization of the complete weight enumerator of ternary self-dual code is invariant under the natural action of

$$\begin{aligned} G_2 &= diag(G_1, G_1) \\ &= < diag(M_1, M_1), diag(M_2, M_2), diag(M_3, M_3), diag(M_4, M_4) > \end{aligned}$$

Molien series for G_2 is

$$\begin{aligned} &\Phi_{G_2}(\lambda) \\ &= \frac{1}{(1-\lambda^{12})^4(1-\lambda^{36})^2} \times \\ &\quad \{1 + 44\lambda^{12} + 467\lambda^{24} + 1446\lambda^{36} + 2487\lambda^{48} + 2836\lambda^{60} + 1992\lambda^{72} + 913\lambda^{84} \\ &\quad +177\lambda^{96} + 5\lambda^{108}\} \\ &= 1 + 48\lambda^{12} + 653\lambda^{24} + 3776\lambda^{36} + 13952\lambda^{48} + 39486\lambda^{60} + 93570\lambda^{72} \\ &\quad +195411\lambda^{84} + 371290\lambda^{96} + 653949\lambda^{108} + \cdots \end{aligned}$$

The group G_2 has a subgroup H_2 of index 2 : $H_2 = diag(H_1, H_1)$. Molien series $\Phi_{H_2}(\lambda)$ for H_2 is calculated by using computer algebra system. The result is

$$\begin{aligned} &\Phi_{H_2}(\lambda) \\ &= \frac{1}{(1-\lambda^{6})^3(1-\lambda^{12})(1-\lambda^{18})^2} \cdot \\ &\quad \{1 + 4\lambda^{6} + 29\lambda^{12} + 78\lambda^{18} + 128\lambda^{24} + 163\lambda^{30} + 138\lambda^{36} + 72\lambda^{42} \\ &\quad +30\lambda^{48} + 5\lambda^{54}\} \\ &= 1 + 7\lambda^{6} + 48\lambda^{12} + 653\lambda^{24} + 208\lambda^{18} + 1688\lambda^{30} + 3776\lambda^{36} + 7562\lambda^{42} \\ &\quad +13952\lambda^{48} + 24110\lambda^{54} + 39486\lambda^{60} + 61909\lambda^{66} + \cdots. \end{aligned}$$

At present we have not determined explicit polynomials (the first and the second invariants) for the rings of invariants $\mathbb{C}[x,y,z,u,v,w]^{G_2}$,$\mathbb{C}[x,y,z,u,v,w]^{H_2}$, and $\mathbb{C}[x,y,u,v,w]^{G_3}$, although we know relations between them.

4 Explicit results.

4.1 Reformulation of the covering radius problem by means of the invariants for G_3

Let $HM\text{-}Jac(\mathrm{C},\mathrm{v},x,y,u,v,w)$ be a homogeneous modified Jacobi polynomial for ternary code C of length n, we can show that

$$X^{-n}HM\text{-}Jac(\mathrm{C},\mathrm{v},X,X^2,X^2,X^2,X)=W_{\mathrm{v+C}}(X)$$

Basically, we can determine $W_{\mathrm{v+C}}(X)$, if we could know the values $\mathrm{u}\sharp\mathrm{v}$ and $\mathrm{u}\natural\mathrm{v}$ for all $\mathrm{u}\in\mathrm{C}$. Of many HM-Jac's it is important to enumerate all HM-Jac's such that v's is a coset leader of the coset $\mathrm{v}+\mathrm{C}$. Note that

$$\begin{aligned}\text{v is a coset leader} &\iff wt(\mathrm{v})\le wt(\mathrm{u}+\mathrm{u}) \quad \forall\ \mathrm{u}\in\mathrm{C}\\ &\iff 0\le wt(\mathrm{u})-2\mathrm{u}*\mathrm{v}+\mathrm{u}\sharp\mathrm{v} \quad \forall\ \mathrm{u}\in\mathrm{C}\\ &\iff wt(\mathrm{u})\ge 2\mathrm{u}*\mathrm{v}-\mathrm{u}\sharp\mathrm{v} \quad \forall\ \mathrm{u}\in\mathrm{C}\end{aligned}$$

With this remark in mind we can determine the complete coset weight distributions of ternary self dual extremal codes of lengths of small size (e.g. 12,16,20,24). As to bigger sizes of codes one must know algebraic structure of the ring $\mathbb{C}[x,y,u,v,w]^{G_3}$. This knowledge will eliminate longer (in size and in time) computations. Also the knowledge will contribute to giving the good lower bounds for $\rho(\mathrm{C})$.

4.2 Ternary Golay code

Let $\mathcal{G}_{12}$ be the ternary Golay code of length 12. The complete weight enumerator $CW_{\mathcal{G}_{12}}$ is known to be

$$CW_{\mathcal{G}_{12}}=x^{12}+y^{12}+z^{12}+22(x^6y^6+y^6z^6+z^6x^6)+220(x^6y^3z^3+x^3y^6z^3+x^3y^3z^6)$$

We give homogeneous modified Jacobi polynomials.

First we remark that upto weight 2 each coset has unique coset leaders. Otherwise we could show the existence of codeword of weight less than 6, that is absurd. In the coset of weight 3 there are 4 coset leaders in each coset of weight 3.
(i) There are 24 coset leaders of weight 1, and each such vector induces unique homogeneous modified Jacobi polynomial :

$$\begin{aligned} &HM\text{-}Jac(\mathrm{C}, \mathrm{v}_1; x, y, u, v, w) = \\ &\quad ux^{11} + 12y^{11}(v+w) + 66x^6y^5(v+w) + 110x^2y^9u \\ &\quad +132x^5y^6u + 165x^3y^8(v+w) \end{aligned}$$

(ii) There 264 coset leaders of weight 2, and each such vector induces unique homogeneous modified Jacobi polynomial :

$$\begin{aligned} &HM\text{-}Jac(\mathrm{C}, \mathrm{v}_2; x, y, u, v, w) = \\ &\quad x^{10}u^2 + 15(v+w)^2x^6y^4 + 72x^5y^5u(v+w) + 60x^4y^6u^2 \\ &\quad 60x^3y^7(v+w)^2 + 90x^2y^8u(v+w) + 6y^{10}(v+w)^2 + 20xy^9u^2 \end{aligned}$$

(iii) There 1760 coset leaders of weight 3, and in each coset there are 4 coset leaders of weight 3. But they all produce the unique homogeneous modified Jacobi polynomial :

$$\begin{aligned} &HM\text{-}Jac(\mathrm{C}, \mathrm{v}_3; x, y, u, v, w) = \\ &\quad x^9u^3 + 3x^6y^3(v+w)^3 + 27x^5y^4u(v+w)^2 + 54x^4y^5u^2(v+w) \\ &\quad +21x^3y^6(v+w)^3 + 54x^2y^7u(v+w)^2 + 27xy^8u^2(v+w) \\ &\quad +3y^9(v+w)^3 + 24x^3y^6u^3 + 2y^9u^3 \end{aligned}$$

By the process described before (see 4.1) we get all the coset weight distributions for this code.

Table of coset weight distributions of ternary Golay code of Length 12

coset weight	0	1	2	3	4	5	6	7	8	9	10	11	12	num. of diff. cosets
0	1						264			440			24	
1		1				66	66	132	165	165	110	12	12	24
2			1		15	30	87	132	180	150	96	32	6	264
3				4	9	36	78	144	171	156	90	36	5	440

$$1 + 24 + 264 + 440 = 729 = 3^6 =| \mathbf{F}_3^{12}/G_{12} |$$

4.3 Ternary Extremal Codes of length 16

There is unique ternary self-dual extremal code of length 16 ([3]). The weight enumerator of ternary self-dual extremal [16,8,6] code is given by

$$x^{16} + 224x^{10}y^6 + 2720x^7y^9 + 3360x^4y^{12} + 256xy^{15}$$

As before we can determine the homogeneous modified Jacobi polynomials of various indeces, and as a consequence we obtain complete list of coset weight distributions of such code. For the limitation of the space we only give the table of coset weight distributions of this code.

coset weght	0	1	2	3	4	5	6	7	8	num. of diff. cosets
0	1						224			1
1		1				42	42	140	765	32
2			1		7	14	63	260	492	480
3				1	4	21	80	221	504	1792
3				2	3	18	82	222	513	896
3				4	1	12	86	224	531	224
4					5	24	78	220	495	3136

coset weight	9	10	11	12	13	14	15	16	num. of diff. cosets
0	2720			3360			256		1
1	765	1190	1260	1260	840	120	120	16	32
2	918	1176	1400	1134	728	280	72	16	480
3	888	1257	957	359	293	705	859	412	1792
3	876	1260	954	361	294	702	866	308	896
3	852	1266	948	365	296	696	880	400	224
4	900	1254	1368	1125	700	300	84	8	3136

References

[1] E. Bannai, E. Bannai, M. Ozeki and S. Teranishi, Rings of simultaneous invariants for the MacWilliams-Gleason group , (in preparation)

[2] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag 1988.

[3] J.H.Conway, V.Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$and $GF(4)$ of length not exceeding 16, IEEE Trans. Inform. Theory, IT-25 (1979), 312-322

[4] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Information and Control Vol.23, (1973) 407-438

[5] W.C. Huffman, On extremal Self-Dual Ternary Codes of Lengths 28 to 40, IEEE Trans. Inform. Theory, Vol.38 (1992), 1395-1400

[6] J.S. Leon, V. Pless and N.J.A. Sloane, On ternary self-dual codes of length 24, IEEE Trans. Inform. Theory, IT-27 (1981), 176-180

[7] F.J. MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes",North-Holl and, Amsterdam, 1977.

[8] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, SIAM J. Appl. Math. Vol. 31, 649-666

[9] M. Ozeki, Determination of the ring of simultaneous invariants for a group associated with MacWilliams identity (an intermediate report of a joint work with E. Bannai), in Meeting on algebraic combinatorics, Suuri Kaiseki Kenkyuusho Koukyuuroku No. ??? (yet unpublished), (1995) Research Institute of Mathematical Sciences in Kyouto Univ.

[10] M. Ozeki, On the notion of Jacobi polynomilas for codes, Math. Proc. Cambridge Philos. Soc. Vol. 121 (1997) 15-30

[11] M. Ozeki, On covering radii and coset weight distributions of extremal binary self-dual codes of length 40, to appear in Theoretical Computer Science

[12] M. Ozeki, On the covering radius problem for Ternary self-dual Codes, preprint 1997

[13] V. Pless, N.J.A. Sloane and H.N. Ward, Ternary codes of minimum weight 6, and the classification of length 20, IEEE Trans. Inform. Theory, IT-26 (1980), 305-316

[14] N.J.A. Sloane, Error-correcting codes and invariant theory: new applications of a nineteenth-century technique, Amer. Math. Month. 84 (1977) 82-107.

[15] N.J.A.Sloane, Self-dual codes and lattices, in "Relations between Combinatorics and Other Parts of Mathematics", Proc. Symp. in Pure Math., no.34 (1979) 273-308.

THE MOD 2 COHOMOLOGY ALGEBRAS OF FINITE GROUPS WITH WREATHED SYLOW 2-SUBGROUPS

HIROKI SASAKI

1. INTRODUCTION

The simple groups of 2-rank 2 were classified about 1970 by Alperin, Brauer, Gorenstein, Walter, Lyons. See for example Alperin-Brauer-Gorenstein [5]. The 2-groups of rank 2 which can be Sylow 2-subgroups of finite simple groups are

(1) dihedral 2-groups (including four-groups);
(2) semidihedral 2-groups;
(3) wreathed 2-groups;
(4) special 2-group which is a Sylow 2-subgroup of $SU(3,4)$.

We note that in those works all finite groups with these Sylow 2-subgroups above were determined.

The cohomology algebras of finite simple groups of 2-rank 2 have been known, depending on the classification theorems and on the fact that the cohomology algebras of some classical groups were calculated. A nice overview of these results is in the work by Adem-Milgram [3].

TABLE 1. Finite simple groups of 2-rank 2 and cohomology algebras

Sylow 2-subgroup (non-abelian)	Simple Groups	Cohomology Algebras
dihedral	$PSL(2,q)$, q odd A_7	$k[\varepsilon_2,\zeta_3,\theta_3]/(\zeta\theta)$
semidihedral	$PSL(3,q)$, $q\equiv 3 \pmod 4$ $PSU(3,q)$, $q \equiv 1 \pmod 4$ M_{11}	$k[\beta_3,\gamma_4,\delta_5]/(\beta^2\gamma-\delta^2)$
wreathed	$PSL(3,q)$, $q\equiv 1 \pmod 4$ $PSU(3,q)$, $q \equiv 3 \pmod 4$	$k[\theta_3,\rho_4,\theta_5,\sigma_6]/(\theta_3^2,\theta_5^2)$
special of order 64	$SU(3,4)$	

Remark. In Table 1 and in the rest of this report the subscript of a cohomology class indicates the degree. For example ρ_4 is of degree 4, σ_6 is of degree 6, and so on.

From the late 1980's the mod 2 cohomology algebras of those finite groups with dihedral, semidihedral , and quaternion Sylow 2-subgroups have been calculated:

(1) dihedral and quaternion case by Martino-Priddy [20], 1991; by Asai-Sasaki [7], 1993;

(2) semidihedral case by Martino [19], 1988; by Sasaki [23], 1994.

The works by Martino and Priddy dealt with the classifying spaces, and, as a consequence, obtained the cohomology algebras. On the other hand, the works by Asai and Sasaki depend on the theory of cohomology varieties of modules and on the modular representation theory of finite groups. Especially the theory of relative projectivity of modules played a crucial role.

The purpose of this report is to show a calculation of the mod 2 cohomology algebras of finite groups with wreathed Sylow 2-subgroups. Our method is again module theoretic. This work was done with T. Okuyama.

Let S be a wreathed 2-group

$$S = \langle a, b, t \mid a^{2^n} = b^{2^n} = t^2 = 1,\ ab = ba,\ tat = b \rangle, \quad n \geq 2.$$

Let G be a finite group which has S as a Sylow 2-subgroup. Structure of these groups was deeply investigated in Brauer-Wong [11], Brauer [10], and Alperin-Brauer-Gorenstein [4]. As a continuation of [4] the classification of these finite groups was completed in the paper [5].

The fusion of 2-elements can be described by behavior of several involutions and subgroups. Among them we use four-groups and their normalizers. The reason is that Theorem 2.1 by Carlson shows that we can choose a system of parameters whose elements are sums of corestrictions from the centralizers of elementary abelian subgroups; and Corollary 2.2 due to Okuyama shows that a tensor product of some Carlson modules of parameters taken as in Theorem 2.1 is projective relative to the centralizers of elementary abelian subgroups. These results are of great help to our calculation. Let

$$x = a^{2^{n-1}},\ y = b^{2^{n-1}},\ z = xy$$

and let

$$E = \langle x, y \rangle, \quad F = \langle z, t \rangle.$$

Then $\{E, F\}$ is a complete set of representatives of the conjugacy classes of four-groups in S. The fusion of 2-elements in G is indicated in Table 2.

TABLE 2. Fusion of 2-elements

	a: $N_G(E)/C_G(E) \simeq Z_2$ $(x \not\sim z)$	b: $N_G(E)/C_G(E) \simeq S_3$ $(x \sim z)$
1: $E \not\sim F$ $(x \not\sim t)$	$S \cap G' = S' = \langle ab^{-1} \rangle$	$S \cap G' = \langle a, b \rangle$
2: $E \sim F$ $(x \sim t)$	$S \cap G' = \langle ab^{-1}, xt \rangle$	$S \cap G' = S$

Following Alperin-Brauer-Gorenstein [4], we call a group of type 1b a "D-group"; a group of type 2a a "Q-group"; a group of type 2b a "QD-group". However, our calculation does not depend on the structural results such as, for example, a Q-group G has $O^2(G)$ of index 2^n with generalized quaternion Sylow 2-subgroup $S \cap G' = \langle ab^{-1}, xt \rangle$.

The cohomology algebra of the wreathed 2-group is calculated by Nakaoka's theorem. In the main theorem below the cohomology algebras of other types of groups are stated as subalgebras of that of the wreathed Sylow 2-subgroup S.

Main Theorem. *Let k be a field of characteristic 2.*

(1) *If G is of type 1a, then*

$$\begin{aligned} H^\bullet(G,k) &\simeq H^\bullet(S,k) \\ &= k[\zeta_1,\tau_1,\zeta_2,\nu_2,\zeta_3,\nu_4]/(\zeta_1^2,\nu_2^2,\zeta_3^2,\tau\zeta_1,\tau\zeta_2,\tau\zeta_3,\nu_2\zeta_1,\nu_2\zeta_3,\zeta_1\zeta_3-\zeta_2\nu_2). \end{aligned}$$

(2) *If G is a D-group, then*

$$H^\bullet(G,k) = k[\tau_1,\nu_2,\theta_3,\rho_4,\theta_5,\sigma_6],$$

where

$$\theta_3 = \tau_1\nu_2 + \zeta_1\zeta_2 + \zeta_3,\ \rho_4 = \tau_1^4 + \zeta_2^2 + \nu_4,\ \theta_5 = \tau^3\nu_2 + \zeta_1\rho_4 + \zeta_2\zeta_3,\ \sigma_6 = (\tau_1^2 + \zeta_2)\nu_4.$$

(3) *If G is a Q-group, then*

$$H^\bullet(G,k) = k[\zeta_1,\sigma_2,\theta_3,\rho_4],$$

where

$$\sigma_2 = \tau_1^2 + \zeta_2.$$

(4) *If G is a QD-group, then*

$$H^\bullet(G,k) = k[\theta_3,\rho_4,\theta_5,\sigma_6].$$

Our plan to calculate the cohomology algebras is as follows:

(I) To get a homogeneous system of parameters $\{\rho,\sigma\}$ for $H^\bullet(S,k)$ which is universally stable.

(II) To obtain dimension formulae $\dim H^n(G,k) =?$.

(III) To investigate generators of $H^\bullet(G,k)$ over $k[\rho,\sigma]$.

Finally we note that the work of Adem [1] gives us good knowledge on recent development of the cohomology theory of finite groups, especially cohomology algebras some sporadic finite simple groups.

2. System of Parameters

Let G be a finite group of p-rank r and let P be a Sylow p-subgroup of G, where p is a prime number. For $i = 1,\ldots,r$, let

$$\mathcal{H}_i(G) = \{\, C_G(E) \mid P \geq E \text{ is elementary abelian of rank } i \,\}.$$

Let k be a field of characteristic p. The following theorem by Carlson and its corollary due to Okuyama made our argument clear and simple.

and let

$$\rho_4 = \tau_1^4 + \zeta_2^2 + \nu_4$$
$$\sigma_6 = (\tau_1^2 + \zeta_2)\nu_4.$$

Then we have

Theorem 2.3. (1) *The set* $\{\rho_4, \ \sigma_6\}$ *is a homogeneous system of parameters of* $H^\bullet(S, k)$.

(2) $\sigma_6 \in \mathrm{cor}_U^S H^6(U, k) + \mathrm{cor}_V^S H^6(V, k)$;

(3) *The Carlson module* L_{ρ_4} *is* $\{U, \ V\}$*-projective. In fact*

$$L_{\rho_4} = L_{\alpha_2+\omega\beta_2}{}^S \oplus L_{\chi_2+\omega\psi_2}{}^S,$$

where $\omega = \sqrt[3]{1} \in k$.

(4) *The element* ρ_4 *is regular in* $H^\bullet(S, k)$.

Using the structure of the Carlson module L_ρ above, we can determine an L_ρ-injective hull of the trivial module k. For the notion of projectivity of modules relative to "modules", which is a generalization of that of projectivity relative to subgroups, see Okuyama [21], Carlson [12], or Sasaki [22].

Theorem 2.4. *The extension induced by the element* $\rho_4 \in H^4(S, k)$

$$0 \longrightarrow k \longrightarrow \Omega^{-1}L_\rho \longrightarrow \Omega^3 k \longrightarrow 0$$

is an L_ρ*-injective hull of the trivial module* k. *Namely tensor product of* L_ρ *with the exact sequence above splits.*

The exact sequence above can be lifted up to G:

Theorem 2.5. *There exists a* kG*-module* X *such that*

(1)

$$X_{|S} = L_\rho \oplus (\text{projective})\ ;$$

(2) *an* X*-injective hull of* k_G *is of the form*

$$0 \longrightarrow k_G \longrightarrow \Omega^{-1}X \longrightarrow \Omega^3 k_G \longrightarrow 0.$$

Let

$$\widetilde{\rho}_4 \in H^4(G, k)$$

be the cohomology element defined by the extension above. Then we obtain an $L_{\widetilde{\rho}}$-injective hull of the trivial module k_G

$$0 \longrightarrow k_G \longrightarrow \Omega^{-1}L_{\widetilde{\rho}} \longrightarrow \Omega^3 k_G \longrightarrow 0$$

and we see that

$$\mathrm{res}_S\, \widetilde{\rho}_4 = \rho_4.$$

Namely ρ_4 is universally stable.

The $L_{\widetilde{\rho}}$-injective hull above gives us much information about the cohomology algebra. First we can deduce the following theorem.

Theorem 2.1 (Carlson [11]). *The cohomology algebra $H^{\bullet}(G,k)$ has a homogeneous system of parameters $\{\zeta_1,\ldots,\zeta_r\}$ such that*

$$\zeta_i \in \sum_{H\in\mathcal{H}_i(G)} \operatorname{cor}_H^G H^{\bullet}(H,k), \quad i=1,\ldots,r.$$

Corollary 2.2 (Okuyama). *If a homogeneous system of parameters $\{\zeta_1,\ldots,\zeta_r\}$ is taken as in the theorem above, then the tensor product $L_{\zeta_1}\otimes\ldots\otimes L_{\zeta_{r-1}}$ is $\mathcal{H}_r(G)$-projective, where L_{ζ_i} is the Carlson module of the element ζ_i, $i=1,\ldots,r$.*

In particular, if $r=2$, then L_{ζ_1} is $\mathcal{H}_2(G)$-projective and the element ζ_1 is regular in $H^{\bullet}(G,k)$.

We apply these results to the wreathed 2-group

$$S=\langle a,b,t \mid a^{2^n}=b^{2^n}=t^2=1,\ ab=ba,\ tat=b\rangle, \quad n\geq 2$$

and the finite group G, which has S as a Sylow 2-subgroup.

Let

$$c=ab,\ x=a^{2^{n-1}},\ y=b^{2^{n-1}},\ z=xy=c^{2^{n-1}}$$

and let

$$E=\langle x,y\rangle, \quad F=\langle z,t\rangle.$$

Then $\{E,F\}$ is a complete set of representatives of the conjugacy classes of four-groups in S. Their centralizers are

$$C_S(E)=\langle a\rangle\times\langle b\rangle, \quad C_S(F)=\langle c\rangle\times\langle t\rangle.$$

We set

$$\langle a\rangle\times\langle b\rangle=U, \quad \langle c\rangle\times\langle t\rangle=V.$$

Then we have

$$\mathcal{H}_2(S)=\{U,\ V\}.$$

By Theorem 2.1 and Corollary 2.2, the cohomology algebra $H^{\bullet}(S,k)$ has a homogeneous system of parameters $\{\xi_1,\xi_2\}$ such that

(1) $\xi_2\in\operatorname{cor}_U^S H^{\bullet}(U,k)+\operatorname{cor}_V^S H^{\bullet}(V,k)$;
(2) L_{ξ_1} is $\{U,\ V\}$-projective;
(3) ξ_1 is regular in $H^{\bullet}(S,k)$.

To obtain such parameters we let

$$\alpha_2\in\inf^U H^2(U/\langle b\rangle,k),\ \beta_2\in\inf^U H^2(U/\langle a\rangle,k)$$
$$\chi_2\in\inf^V H^2(V/\langle t\rangle,k),\ \psi_2\in\inf^V H^2(V/\langle c\rangle,k).$$

Let

$$\tau_1\in\inf^S H^1(S/U,k)$$
$$\zeta_2=\operatorname{cor}_U^S\alpha_2\in H^2(S,k)$$
$$\nu_4=\operatorname{norm}_U^S\alpha_2\in H^4(S,k)$$

Theorem 2.6. *The element σ_6 is universally stable. Namely there exists an element $\tilde{\sigma}_6 \in H^6(G,k)$ such that*

$$\operatorname{res}_S \tilde{\sigma}_6 = \sigma_6.$$

Thus the set

$$\{\rho_4, \sigma_6\}$$

is a homogeneous system of parameters for $H^*(G,k)$ for every G.

Second we can deduce dimension formulae for the cohomology groups $H^*(G,k)$. The cohomology long exact sequence induced from the extension

$$0 \longrightarrow k_G \longrightarrow \Omega^{-1}L_{\bar{\rho}} \longrightarrow \Omega^3 k_G \longrightarrow 0$$

gives rise to short exact sequences

$$0 \longrightarrow \operatorname{Hom}_{kG}(\Omega^3 k, k) \longrightarrow \operatorname{Hom}_{kG}(\Omega^{-1} L_{\bar{\rho}_4}, k) \longrightarrow 0,$$

$$0 \longrightarrow \operatorname{Ext}^n_{kG}(k,k) \longrightarrow \operatorname{Ext}^{n+1}_{kG}(\Omega^3 k, k) \longrightarrow \operatorname{Ext}^{n+1}_{kG}(\Omega^{-1}L_{\bar{\rho}_4}, k) \longrightarrow 0, \quad n \geq 0.$$

In particular we have a formula

$$\dim \operatorname{Ext}^{n+4}_{kG}(k,k) = \dim \operatorname{Ext}^n_{kG}(k,k) + \dim \operatorname{Ext}^n_{kG}(L_{\bar{\rho}_4}, k)$$

and we can compute $\dim \operatorname{Ext}^n_{kG}(L_{\bar{\rho}_4}, k)$. For example, if G is a QD-group, then

$$\dim \operatorname{Ext}^n_{kG}(L_{\bar{\rho}_4}, k) = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 3 \\ 1 & \text{if } n \equiv 1 \pmod 3 \\ 1 & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

We can also calculate $\dim \operatorname{Ext}^n_{kG}(k,k)$, $n = 1,2,3.$ so that we obtain dimension formulae for $H^*(G,k)$.

3. Generators of Cohomology Algebras

We have obtained a system of parameters $\{\tilde{\rho}_4, \tilde{\sigma}_6\}$ and established dimension formulae for the cohomology groups $H^*(G,k)$. We have to get generators of the cohomology algebras over the subalgebra $k[\tilde{\rho}_4, \tilde{\sigma}_6]$.

First let us state generators of the cohomology algebra of the wreathed 2-group S. The cohomology algebra $H^*(S,k)$ has $\{\sigma_2(=\tau_1^2+\zeta_2), \rho_4\}$ as a system of parameters. Hence we can take generators of degree up to 4. In fact, $H^*(S,k)$ is generated over the subalgebra $k[\sigma_2, \rho_4]$ by τ_1, which was defined in Section 2, and the elements $\zeta_1, \nu_2, \zeta_3 \in H^*(S,k)$. To state these elements, let $\alpha_1 \in \inf^U H^1(U/\langle b \rangle, k)$. Let us define

$$\zeta_1 = \operatorname{cor}^S_U \alpha_1 \in H^1(S,k)$$

$$\nu_2 = \operatorname{norm}^S_U \alpha_1 \in H^2(S,k)$$

$$\zeta_3 = \operatorname{cor}^S_U(\alpha_1\alpha_2) \in H^3(S,k).$$

It is easily seen that the cohomology algebras of the groups G in which E and F are not conjugate are isomorphic with those of the normalizer $N_G(E)$, by comparing the dimensions of the cohomology groups. On the other hand, when E and F are conjugate, one can take an element $g_0 \in C_G(c)$ such that $E^{g_0} = F$ and $U^{g_0} \cap S = V$. Then we can determine the stable elements considering the subspaces

$$\{\xi \in H^n(S,k) \mid \xi^{g_0}{}_V = \xi_V\}, \quad n \leq 4.$$

Remark. Of course the element g_0 above plays an important role throughout in our investigation for those groups in which E and F are conjugate.

References

1. A. Adem, *Recent developments in the cohomology of finite groups*, Notices Amer. Math. Soc. **44** (1997), 806–812.
2. A. Adem and R. Milgram, *Cohomology of finite groups*, Grundlehren der math. Wissenshaften, vol. 309, Springer-Verlag, Berlin/New York/London, 1994.
3. ______, *The mod 2 cohomology rings of rank 3 simple groups are Cohen-Macaulay*, Prospects in topology (Princeton) (F. Quinn, ed.), Ann. Math. Studies, vol. 138, Princeton Univ. Press, 1995, pp. 3–12.
4. J. L. Alperin, R. Brauer, and D. Gorenstein, *Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups*, Trans. Amer. Math. Soc. **151** (1970), 1–261.
5. ______, *Finite simple groups of 2-rank two*, Scripta Math. **29** (1973), 191–214.
6. T. Asai and H. Sasaki, *The mod 2 cohomology algebras of finite groups with dihedral Sylow 2-subgroups*, Comm. Algebra **21** (1993), 2771–2790.
7. D. J. Benson, *Representations and cohomology II: Cohomology of groups and modules*, Cambridge studies in advanced mathematics, vol. 31, Cambridge University Press, Cambridge, 1991.
8. D. J. Benson and J. F. Carlson, *Diagrammatic methods for the modular representations and cohomology*, Comm. Algebra **15** (1987), 53–121.
9. R. Brauer, *Character theory of finite groups with wreathed Sylow 2-subgroups*, J. Algebra **19** (1971), 547–592.
10. R. Brauer and W. J. Wong, *Some properties of finite groups with wreathed Sylow 2-subgroups*, J. Algebra **19** (1971), 263–273.
11. J. F. Carlson, *Depth and transfer maps in the cohomology of groups*, Math. Z. **218** (1995), 461–468.
12. ______, *Modules and group algebras*, Lectures in Mathematics, ETH Zürich, Birkhäuser, Basel/Boston/Berlin, 1996.
13. L. Evens, *The cohomology of groups*, Oxford Mathematics Monograph, Oxford University Press, New York, 1991.
14. L. Evens and S. Priddy, *The ring of universally stable elements*, Quart. J. Math. Oxford (2) **40** (1989), 399–407.
15. D. Gorenstein, *Finite groups*, Harper & Row, Publishers, New York, 1968.
16. D. Gorenstein and J. H. Walter, *The characterization of finite groups with dihedral sylow 2-subgroups, I, II, III*, J. Algebra **2** (1965), 85–151, 218–270, 334–393.
17. R. Lyons, *A characterization of $U_3(4)$*, Trans. Amer. Math. Soc. **164** (1972), 371–387.
18. J. Martino, *Stable splittings of the Sylow 2-subgroups of* $\mathrm{SL}_3(\mathrm{F}_q)$, *$q$ odd*, Ph.D. thesis, Northwestern University, 1988.
19. J. Martino and S. Priddy, *Classification of BG for groups with dihedral or quaternion Sylow 2-subgroups*, J. Pure Appl. Algebra **73** (1991), 13–21.
20. H. Nagao and Y. Tsushima, *Representations of finite groups*, Academic Press, New York, London, 1989.
21. T. Okuyama, *A generalization of projective covers of modules over group algebras*, preprint.
22. H. Sasaki, *The mod 2 cohomology algebras of finite groups with semidihedral Sylow 2-subgroups*, Comm. Algebra **55** (1994), 243–275.

Department of Mathematical Sciences, Faculty of Science, Ehime University, Matsuyama 790-77, Japan

The Classification of Four-weight Spin Models with Size Five

Mitsuhiro Sawano
Kyusyu University

1.

This is a joint work with Etsuko Bannai.

The concept of the spin model was introduced by V.F.R.Jones to construct invariants of knots and links. It was generalized by Kawagoe, Munemasa and Watatani. Finally, Bannai and Bannai introduced the much more general four-weight spin models [1].

First we give the definition of four-weight spin model.

Let X be a finite set with $|X| = n$ and $M_C(X)$ be the set of all the matrices over complex number field C with rows and columns indexed by X.

Definition (Bannai and Bannai)

(W_1, W_2, W_3, W_4, D) is a four-weight spin model on a finite non-empty set X, where $D^2 = |X|$, W_1, W_2, W_3, W_4 are complex matrices in $M_C(X)$ satisfying the following conditions.

For all a, b, c in X

i) $W_1(a, b)W_3(b, a) = 1 \qquad W_2(a, b)W_4(b, a) = 1$

ii) $\Sigma_{x \in X} W_1(a, x)/W_1(b, x) = |X|\ \delta_{a, b}, \ \Sigma_{x \in X} W_2(a, x)/W_2(b, x) = |X|\ \delta_{a, b}$

iii) $\Sigma_{x \in X} W_2(a, x)W_2(b, x)/W_2(c, x) = DW_1(b, a)/W_1(c, a)W_1(b, c)$

$\Sigma_{x \in X} W_2(x, a)W_2(x, b)/W_2(x, c) = DW_1(a, b)/W_1(a, c)W_1(c, b).$

The equation i) shows that four-weight spin models are determined by two matrices W_1 and W_2. If you have a two-weight spin model (W_+, W_-, D), then it is easy to see that (W_+, W_+, W_-, W_-, D) is a four-weight spin model.

Recently Guo constructed examples of four-weight spin model using symmetric design [2]. Guo's examples are the first ones, which are not constructed from two-weight spin models using the method mentioned above. Next definition corresponds to the condition ii) of the definition above.

Definition

A matrix W in $M_C(X)$ is a Type II matrix

, if $\Sigma_{x \in X} W(a, x)/W(b, x) = \delta_{a,b}$ holds for any a, b $\in$ X.

If W is a Type II matrix then it is easy to see that $W' = P \Delta W \Delta' P'$ is also a Type II matrix for any permutation matrices P, P′ and for any invertible diagonal matrices Δ, Δ'. For Type II matrices W and W′, we say W′ is equivalent to W if and only if there exist permutation matrices P, P′ and invertible diagonal matrices Δ, Δ' such that W′ is equal to $P \Delta W \Delta' P'$. Then this defines an equivalence relation.

We note that if (W_1, W_2, W_3, W_4, D) and $(W_1', W_2', W_3', W_4', D)$ are gauge equivalent this W_i and W_i' are equivalent as Type II matrices.

To investigate four-weight spin models we need more examples. We study the four-weight spin models in two directions. One direction is to classify them for small sizes of X. Another is to seek for four-weight spin models in the equivalence classes (as Type II matrices) of known two-weight spin models.

Examples 1

We can easily check that the following matrices are Type II matrices.

(i) W $\in$ $M_C(X)$ defined by

$$W(x, y) = \alpha \quad (x = y)$$
$$= 1 \quad (x \neq y) \qquad ,\text{where } \alpha + \alpha^{-1} + n - 2 = 0$$

(ii) W $\in$ $M_C(X)$ defined by

$$W(x, y) = \eta^{(x-y)2} \quad \text{for any } x, y \in X$$

,where η is a primitive n-th root of unity.

In this example we take X={0, 1, ..., n}.

Note : The two matrices defined in (i) according to the two solutions of $\alpha + \alpha^{-1} + n - 2 = 0$ are not equivalent as Type II matrices except for n<5. The matrices defined in (ii) according to primitive n-th root of unity are equivalent to each other as Type II matrices. For n is equal to or less than four, there are some matrices that are potts type and cyclic type at the time.

In this paper we say $M \in M_C(X)$ is potts type if M is equivalent (as Type II matrix) to one of the matrices given in Example 1 (i), and cyclic type if M is equivalent (as Type II matrix) to one of the matrices given in Example 1 (ii).

Example 2

Four-weight spin models of size $|X| = n$.

i) Cyclic model

$W_1(x, y) = \eta^{(x-y)^2}$ $\qquad$ $W_2(x, y) = \eta^{(x-y)^2}$

,where η^2 is the primitive n-th root of unity.

ii) Potts model

$W_1(x, y) = \alpha \ (x = y)$ $\qquad$ $W_2(x, y) = W_1$

$= 1 \ (x \neq y)$

,where $\alpha + \alpha^{-1} + (n-2) = 0$.

We will call a four-weight spin model of i) cyclic model. The (x, y)-entry of W_1 is $\eta^{(x-y)2}$ and W_2 is equal to W_1. η^2 is a primitive n-th root of unity. We will call a four-weight spin model of ii) potts model.

Type II matrices of size five was classified by Nomura[3].

Theorem 1 (Nomura)

Every type II matrix of size five is equivalent to either potts type or cyclic type in Example 1.

,where η is a primitive 5-th root of unity and $\alpha + \alpha^{-1} + 3 = 0$.

For i) the equivalence class does not depend on the choice of primitive 5-th roots of unity. In case ii) there are two matrices corresponding to the two solutions of $\alpha + \alpha^{-1} + 3 = 0$ and these two matrices are not equivalent to each other. If size is more than or equal to 6 then there may exist infinitely many families of Type II matrices.

F.jaeger developed the concept of gauge transformations among four-weight spin models [4]. He defined odd and even gauge transformations of spin models supported by the following two theorems respectively.

Theorem 2 (Jaeger)

Let (W_1, W_2, W_3, W_4, D) be a four-weight spin model. Then $(W_1', W_2, W_3', W_4, D)$ is a four-weight spin model if and only if there exists a invertible diagonal matrix in $M_C(X)$ satisfying $W_1' = \Delta W_1 \Delta^{-1}$, $W_3' = \Delta W_3 \Delta^{-1}$. Moreover if $(W_1', W_2, W_3', W_4, D)$ is a four-weight spin model then the associated link invariant is the same as the one associated to (W_1, W_2, W_3, W_4, D).

Theorem 3 (Jaeger)

Let (W_1, W_2, W_3, W_4, D) be a four-weight spin model. Then $(W_1, W_2', W_3, W_4', D)$ is a four-weight spin model if and only if there exists a permutation matrix P in $M_C(X)$ satisfying the following conditions.

(i) $W_2^{-1}PW_2$ is also a permutation matrix.

(ii) $W_2' = PW_2$, $W_4' = W_4{}^tP$.

Moreover if $(W_1, W_2', W_3, W_4', D)$ is a four-weight spin model then the associated link invariants are the same as the one associated to (W_1, W_2, W_3, W_4, D).

We can obtain the following Theorem 4 easily from Theorem 2 and Theorem 3.

Theorem 4 (Jaeger)

Let (W_1, W_2, W_3, W_4, D) be a four-weight spin model. Let P be a permutation matrix in $M_C(X)$ such that $W_2^{-1}PW_2$ is also a permutation matrix, Δ be an invertible diagonal matrix in $M_C(X)$, and λ be a non-zero complex number.

Then $(\lambda\, \Delta W_1 \Delta^{-1}, \lambda^{-1}\, PW_2,\ \lambda^{-1} \Delta W_3 \Delta^{-1}, \lambda\, W_4{}^tP, D)$ is a four-weight spin model, and gives the same link invariant as the one associated to(W_1, W_2, W_3, W_4, D).

These spin models, which are obtained from a given spin model by gauge transformations, have the same link invariant. In this paper, we say $(W_1', W_2', W_3', W_4', D)$ is gauge equivalent to (W_1, W_2, W_3, W_4, D) when $(W_1', W_2', W_3', W_4', D)$is expressed as $(\lambda\, \Delta W_1 \Delta^{-1}, \lambda^{-1}\, PW_2,\ \lambda^{-1} \Delta W_3 \Delta^{-1}, \lambda\, W_4{}^tP, D)$.

It is natural to consider the following question. Take two four-weight spin models (W_1, W_2, W_3, W_4, D) and $(W_1', W_2', W_3', W_4', D)$. Assume W_i and W_i' are equivalent as Type II matrices. Then are they gauge equivalent?

We studied this problem for the spin models whose matrices are equivalent (as Type II matrix) to the matrices of potts type and cyclic type given in Example 1.

For the potts type we obtained the following theorem.

Theorem 5

Let (W_1, W_2, W_3, W_4, D) be a four-weight spin model. If there exists $1 \leqq i \leqq 4$ such that W_i is equivalent (as Type II matrix) to one of the matrices given in Example 1 (i) then (W_1, W_2, W_3, W_4, D) is gauge equivalent to a potts model.

When n is at most four, this theorem does not hold. There are counter examples. Four-weight spin models of size at most four are classified by Guo – Huang[5].

Every four-weight spin model of size at most four is gauge equivalent to one of the followings.

i) $n = 2$.

$$W_1 = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \qquad W_2 = \frac{D(1-i)}{2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

ii) $n = 3$.

$$W_1 = \begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix} \qquad W_2 = \frac{D}{\alpha - 1}\begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix}$$

, where $\alpha + \alpha^{-1} + 1 = 0$

iii) $n = 4$.

$$W_1 = \begin{pmatrix} 1 & 1 & b & -b \\ 1 & 1 & -b & b \\ b & -b & 1 & 1 \\ -b & b & 1 & 1 \end{pmatrix} \qquad W_2 = \frac{D}{2}\begin{pmatrix} 1 & 1 & b^{-1} & -b^{-1} \\ 1 & 1 & -b^{-1} & b^{-1} \\ b^{-1} & -b^{-1} & 1 & 1 \\ -b^{-1} & b^{-1} & 1 & 1 \end{pmatrix}$$

, where b is non-zero complex number.

Note : In case iii) two of these spin models are not gauge equivalent to each other, when they do not have the same $|b|$.

If n is equal to five then by Theorem 1 and Theorem 5 W_1 and W_2 are equivalent to potts matrix at the same time or cyclic matrix at the same time. So we obtain the following theorem.

Theorem6

Every four-weight spin model of size five is gauge equivalent to one of the following four weight spin models.

i) Cyclic model (W, ±W, D^2W^{-1}, $\pm D^2W^{-1}$, D)

W is the matrix of i) in Theorem 1.

ii) Potts model (W, DW/(α-1), D^2W^{-1}, D(α-1)W^{-1}, D)

W is the matrix of ii) in Theorem 1

For Theorem 5, we can do similar argument for cyclic models and I believe that we can obtain a similar result. Now we are working on it.

References

[1] E.Bannai and E.Bannai, Generalized generalized spin models (four-weight spin models), Pacific Journal of Mathematics Vol. 170 (1995) 1-16.

[2] H.Guo, On Four-Weight Spin Models, PhD Thesis, Kyushu University.

[3] K.Nomura, Type II matrices of size five, to appear in Graphs and Combinatorics.

[4] F.Jaeger, On four-weight spin models and their gauge transformation, preprint.

[5] H.Guo and T.Huang, Some Classes of Four-weight Spin Models, preprint.

REPRESENTATIONS OF FINITE CHEVALLEY GROUPS

TOSHIAKI SHOJI

Department of Mathematics
Science University of Tokyo
Noda, Chiba 278 Japan

1. Introduction

This note is an exposition of the representation theory of finite Chevalley groups, developed mainly by G. Lusztig since 1970's. The main problem which we are concerned here is the classification of irreducible ordinary representations of such groups, and the determination of their character values, namely, to give a complete algorithm of computing character tables. In 1976, Deligne and Lusztig ([DL]) constructed, in a general framework of finite reductive groups, a family of representations endowed with some nice properties by using l-adic cohomology theory. By extending their results, based on the powerful tool of l-adic cohomology theory combined with the theory of perverse sheaves on reductive algebraic groups G, Lusztig succeeded in 1980's in classifying all the irreducible representations of finite reductive groups $G(\mathbf{F}_q)$ and in determining their degrees ([L1]).

So the remaining problem is the determination of character values. In order to approach to this problem in a general point of view, Lusztig founded the theory of character sheaves ([L2]), which makes it possible to produce certain type of class functions of $G(\mathbf{F}_q)$ (but not necessarily characters) in a systematic way. He showed that such class functions are actually computable, and form a basis of the space of class functions of $G(\mathbf{F}_q)$. Under these circumstances he proposed a conjecture connecting such class functions with irreducible characters of $G(\mathbf{F}_q)$. Lusztig's conjecture offers a way to a general algorithm of computing irreducible characters. In the case where the center of G is connected, Lusztig's conjecture was solved by the author, by using the theory of Shintani descent developed by Shintani, Kawanaka and Asai, (see e.g., [K]).

In this note, we first review Lusztig's classification of irreducible characters, and then its relations with the theory of Shintani descent. After formulating Lusztig's conjecture, we summarize related results on the computation of irreducible characters in the case where the center is connected. In the case of disconnected center, Lusztig's conjecture is not yet established. We.discuss this case, in connection with recent results on Shintani descent, the Mackey formula and generalized Gelfand-Graev representations.

2. The classification of irreducible representations

Let G be a connected reductive algebraic group defined over $\mathbf{F}_q$, a finite field of q elements with $ch\mathbf{F}_q = p$. We denote by $F : G \to G$ the corresponding Frobenius map on G. Then the group $G(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points in G coincides with the subgroup G^F of fixed points by F in G. Let $\bar{\mathbf{Q}}_l$ be the algebraic closure of the l-adic number field $\mathbf{Q}_l$, for $l \neq p$. Then $\bar{\mathbf{Q}}_l \simeq \mathbf{C}$, and in what follows we consider the representations of G^F over $\bar{\mathbf{Q}}_l$ so that l-adic cohomology theory can be applied. We are interested in the following problem.

Problem. Classify all the irreducible representations of a finite reductive group G^F, and determine the values of irreducible characters, i.e., complete the character table of G^F

The fundamental tool for the classification is the virtual G^F-module $R_T^G(\theta)$ introduced by Deligne and Lusztig in 1976. Let T be an F-stable maximal torus of G and take $\theta \in \widehat{T}^F = \mathrm{Hom}(T^F, \bar{\mathbf{Q}}_l^*)$, a linear character of T^F. For such a pair (T, θ), a virtual G^F-module $R_T^G(\theta)$ is constructed as an alternating sum of certain l-adic cohomology groups on which G^F acts naturally.

Let G_{uni} be the unipotent variety of G, and G_{uni}^F the set of unipotent elements in G^F. We define a G^F-invariant function $Q_T^G : G_{\mathrm{uni}}^F \to \bar{\mathbf{Q}}_l$ by

$$Q_T^G(u) = \mathrm{Tr}\,(u, R_T^G(\theta)), \qquad (u \in G_{\mathrm{uni}}^F).$$

The function Q_T^G does not depend on the choice of θ, and is called the **Green function of G^F**. As the following formula shows, the computation of character values of $R_T^G(\theta)$ is reduced to the determination of Green functions of various reductive subgroups of G.

(Character formula.) Let $g = su = us \in G^F$ with s : semisimple and u : unipotent. Then we have

$$\mathrm{Tr}\,(g, R_T^G(\theta)) = |Z_G^0(s)^F|^{-1} \sum_{\substack{x \in G^F \\ x^{-1}sx \in T^F}} Q_{xTx^{-1}}^{Z_G^0(s)}(u)\theta(x^{-1}sx).$$

Another important property of $R_T^G(\theta)$ is the following orthogonality relations.

(Orthogonality relations.)

$$\langle R_T^G(\theta), R_{T'}^G(\theta')\rangle_{G^F} = \sharp\{w \in W(T, T')^F \mid {}^w\theta = \theta'\},$$

where $\langle\ ,\ \rangle_{G^F}$ means the usual inner product, and $W(T, T') = N(T, T')/T'$ with $N(T, T') = \{n \in G \mid n^{-1}Tn = T'\}$.

It follows from the above formula that $\pm R_T^G(\theta)$ turns out to be irreducible if θ is enough generic. In this way, almost all irreducible characters of G^F are obtained from some pairs (T, θ). In what follows, we denote by $\widehat{G}^F$ the set of irreducible characters of G^F. The first task for the classification is the partition of $\widehat{G}^F$ into certain subsets as follows. Let G^* be the dual group of G, i.e., G^* is a connected reductive group over $\mathbf{F}_q$, with Frobenius map F, and its root system is dual to the original one. For each F-stable maximal torus T in G, there corresponds an F-stable maximal torus T^* in G^* which is dual to T, (unique up to G^{*F}-conjugate). Then the set of pairs (T,θ) (up to G^F-conjugate) is in bijection with the set of pairs (T^*,s) for $s \in T^{*F}$ (up to G^{*F}-conjugate). For each F-stable semisimple class $\{s\}$ in G^*, we define a subset of $\widehat{G}^F$ by

$$\mathcal{E}(G^F,\{s\}) = \bigcup_{(T_1,\theta_1)} \{\rho \in \widehat{G}^F \mid \langle \rho, R^G_{T_1}(\theta_1)\rangle_{G^F} \neq 0\},$$

where $(T_1;\theta_1)$ runs over all the pairs such that (T_1,θ_1) corresponds to (T_1^*,s_1) with $s_1 \in T_1^{*F} \cap \{s\}$ under the above correspondence. In the case where the center of G is connected, the set $\{s\}^F$ consists of a single G^{*F}-class, and we may choose $s_1 = s$. Moreover in this case, the centralizer $Z_{G^*}(s)$ of s is connected.

Lusztig has proved the following result.

Theorem 2.1 (Lusztig [L1]). *Assume that the center of G is connected. Then*

(i) *$\widehat{G}^F$ is partitioned as*

$$\widehat{G}^F = \coprod_{\{s\}} \mathcal{E}(G^F,\{s\}),$$

where $\{s\}$ runs over all semisimple classes in G^{*F}.

(ii) *There exists a natural bijection*

$$\mathcal{E}(G^F,\{s\}) \simeq \mathcal{E}(Z_{G^*}(s)^*,\{1\}).$$

An irreducible character ρ on G^F is called a unipotent character if ρ belongs to the set $\mathcal{E}(G^F,\{1\})$. This is equivalent to saying that $\langle \rho, R^G_T(1)\rangle_{G^F} \neq 0$ for some T. In view of (ii) in the theorem, the classification of irreducible characters of G^F is reduced to that of unipotent characters.

2.2. The classification of unipotent characters.

In order to explain the parametrization of unipotent characters due to Lusztig, we prepare some notation. Let T_0 be an F-stable maximal torus contained in an F-stable Borel subgroup B of G. Then a pair (B,T_0) is unique up to G^F-conjugate. Let $W = N_G(T_0)/T_0$ be the Weyl group of G. Then F acts naturally on W. We assume, for simplicity, that F acts trivially on W, i.e., G^F is of split type (or G^F is a finite Chevalley group). Then G^F-conjugacy classes of F-stable maximal tori in G are in one to one correspondence with the conjugacy classes in W. We denote by T_w an F-stable maximal torus corresponding to $w \in W$. If $T = T_w$ with $w = 1$, T coincides with T_0, and in this case we have $R^G_T(1) = \mathrm{Ind}^{G^F}_{B^F} 1$. It is known that

$$\mathrm{End}_{G^F}(\mathrm{Ind}^{G^F}_{B^F} 1) \simeq H_q(W) \simeq \bar{\mathbb{Q}}_l[W],$$

where $H_q(W)$ is the Iwahori-Hecke algebra of W with parameter q. Hence $\mathrm{Ind}_{B^F}^{G^F} 1$ is decomposed, as $H_q(W) \times G^F$-module,

$$\mathrm{Ind}_{B^F}^{G^F} 1 \simeq \bigoplus_{E \in W^\wedge} V_E \otimes \rho_E,$$

where V_E is an irreducible representation of $H_q(W)$ and ρ_E is the corresponding irreducible representation (or irreducible character) of G^F. In particular, we obtain (a part of) unipotent characters $\{\rho_E \mid E \in W^\wedge\}$ parametrized by the set of irreducible characters of W. We now define, for $E \in W^\wedge$,

$$R_E = |W|^{-1} \sum_{w \in W} E(w) R_{T_w}^G(1) \in C(G^F/\sim),$$

where $C(G^F/\sim)$ denotes the $\bar{\mathbb{Q}}_l$-space of class functions of G^F. The following formula is an immediate consequence of orthogonality relations of $R_T^G(\theta)$.

$$\langle R_E, R_{E'} \rangle_{G^F} = \begin{cases} 1 & \text{if } E = E' \\ 0 & \text{if } E \neq E'. \end{cases}$$

According to Lusztig, the set $\mathcal{E}(G^F, \{1\})$ of unipotent characters is parametrized by a set $X(W)$, which is completely described in terms of the data coming from two sided cells of $H_q(W)$. In particular, the parametrization depends only on the Coxeter diagram of W, and independent of p. He also showed the existence of a certain non-degenerate pairing $\{\ ,\ \} : X(W) \times X(W) \to \bar{\mathbb{Q}}_l$. We express the unipotent character corresponding to $x \in X(W)$ by ρ_x. By the previous remark, there exists an injection $W^\wedge \hookrightarrow X(W)$ via $E \mapsto x_E$ with $\rho_{x_E} = \rho_E$. The following formula gives the decomposition of R_E into irreducible characters of G^F.

(2.2.1)
$$R_E = \sum_{y \in X(W)} \{y, x_E\} \rho_y.$$

Note that in certain $E \in W^\wedge$ for type E_7 or E_8 (exceptional characters of W), some modification is needed for the above formula. We also note that except the above case, unipotent characters are characterized by the multiplicities for various R_E. This is the leading principle of the parametrization by Lusztig.

Now the decomposition of R_E in (2.2.1) suggests to define formally a class function R_x on G^F for any $x \in X(W)$ by

$$R_x = \sum_{y \in X(W)} \{y, x\} \rho_y.$$

Then the orthogonality property holds also for such R_x, and we see that $\{R_x \mid x \in X(W)\}$ gives rise to an orthonormal basis of the subspace of $C(G^F/\sim)$ generated by unipotent characters.

Remarks. (i) More generally, the set $\mathcal{E}(G^F, \{s\})$ is also described in a similar way (cf. (ii) of Theorem 2.1), and we get the total parameter set $X(G^F)$ for G^F. Then one can define functions R_x for $x \in X(G^F)$ similar to the previous case. The set $\{R_x \mid x \in X(G^F)\}$ gives rise to an orthonormal basis of $C(G^F/\sim)$, and R_x's are called **almost characters** of G^F.

(ii) In the case where the center of G is disconnected, the classification of $\widehat{G}^F$ is done by reducing it to the case of connected center. However, the construction of almost characters in this case is not so clear.

3. Shintani descent for reductive groups

Although we keep the assumption in section 2, we note that the theory of Shintani descent itself makes sense for (not necessarily reductive) all connected algebraic groups. We consider a finite group $G^{F^m} = G(\mathbf{F}_{q^m})$ for a positive integer m. Then F leaves G^{F^m} invariant, and one can define the set $G^{F^m}/\sim_F$ of F-twisted conjugacy classes in G^{F^m}. (Here $x, y \in G^{F^m}$ are said to be F-twisted conjugate if there exists $z \in G^{F^m}$ such that $y = z^{-1}xF(z)$). There exists a natural bijection $N_{F^m/F}$, called a norm map,

$$N_{F^m/F} : G^{F^m}/\sim_F \to G^F/\sim,$$

induced from the assignment $x \in G^{F^m} \mapsto x' \in G^F$ where x is written as $x = \alpha^{-1}F(\alpha)$ for some $\alpha \in G$ (by Lang's theorem) and x' is given by $x' = F^m(\alpha)\alpha^{-1}$. We define a Shintani descent map $Sh_{F^m/F}$ by its transposed inverse,

$$Sh_{F^m/F} = N^{*-1}_{F^m/F} : C(G^{F^m}/\sim_F) \to C(G^F/\sim),$$

where $C(G^{F^m}/\sim_F)$ denotes the space of functions on G^{F^m} which are constant on each F-twisted classes. Now for each F-stable irreducible character ρ of G^{F^m}, one can associate an element $[\rho] \in C(G^{F^m}/\sim)$, unique up to an m-th root of unity multiple. We denote by $(\widehat{G}^{F^m})^F$ the set of F-stable irreducible characters of G^{F^m}. Then the set $\{[\rho] \mid \rho \in (\widehat{G}^{F^m})^F\}$ form an orthonormal basis of $C(G^{F^m}/\sim)$ under a suitable inner product on it. Hence the above discussion implies that the cardinality of the set $(\widehat{G}^{F^m})^F$ is equal to the cardinality of the set $\widehat{G}^F$.

The fundamental problem in the theory of Shintani descent is the description of $Sh_{F^m/F}([\rho])$ for each $\rho \in (\widehat{G}^{F^m})^F$, and was studied extensively by Shintani and Kawanaka from the view point of the character correspondence. The connection of the theory of Shintani descent and Deligne-Lusztig theory was first noticed by Asai. It is summarized in the following theorem, (see e.g., [S1]) .

Theorem 3.1 (S). *Assume that the center of G is connected. Assume further that m is sufficiently divisible. Then for each $\rho \in (\widehat{G}^{F^m})^F$, $Sh_{F^m/F}([\rho])$ coincides with an almost character of G^F up to scalar. Hence the map $Sh_{F^m/F}$ gives a natural bijection*

$$(\widehat{G}^{F^m})^F \simeq \{R_x \mid x \in X(G^F)\}.$$

Remark. We shall illustrate by a simple example why the Shintani descent gives a connection between these two objects. We consider the following two kinds of decompositions.

$$\mathrm{Ind}_{B^{F^m}}^{G^{F^m}} 1 = \bigoplus_{E \in W^\wedge} V_E \otimes \rho_E^{(m)}$$

$$R_{T_w}^G(1) = \sum_{E \in W^\wedge} E(w) R_E,$$

where V_E is an irreducible $H_{q^m}(W)$-module as before, and $\rho_E^{(m)}$ is the corresponding G^{F^m}-module. Let V be the representation space of $\mathrm{Ind}_{B^{F^m}}^{G^{F^m}} 1$. Then we have an action of F on V besides the action of $H_{q^m}(W)$ and G^{F^m}. On the other hand, $R_{T_w}^G(1)$ is defined as an alternating sum of cohomology, and we have an action of F^m for each cohomology group. Then it is known (Shintani descent identity) that the trace of $F \cdot T_w \cdot x$ on V coincides with the trace of $F^m x'$ on $R_{T_w}^G(1)$, where T_w is a standard basis of $H_{q^m}(W)$ corresponding to $w \in W$, and $x \in G^{F^m}, x' \in G^F$ are related by $N_{F^m/F}(x) = x'$. Hence by specializing $q^m \to 1$, $Sh_{F^m/F}$ gives a connection between $\rho_E^{(m)}$ and R_E.

We define a linear map

$$R_T^G : C(T^F/\sim) \to C(G^F/\sim)$$

by assigning $R_T^G(\theta)$ to $\theta \in \widehat{T}^F$, and extending it linearly. Generalizing the construction of $R_T^G(\theta)$, Lusztig defined, for an F-stable Levi subgroup of a not necessarily F-stable parabolic subgroup P of G, a linear map

$$R_{L \subset P}^G : C(L^F/\sim) \to C(G^F/\sim),$$

which is called the Lusztig induction (or twisted induction) from L^F to G^F. It is expected that Lusztig induction depends only on L and not on P, but it is not yet known in the full generality. The Shintani descent identity formula can be extended to this more general situation. Then using a similar argument as in the remark, one can describe the decomposition of $R_{L \subset P}^G(\pi)$ for $\pi \in \widehat{L}^F$. More precisely, we have

Corollary 3.2. *Assume that the center of G is connected. Then the decomposition of the Lusztig induction into almost characters is completely described by means of the Harish-Chandra induction $\mathrm{Ind}_{P^{F^m}}^{G^{F^m}}$ on G^{F^m} via the Shintani descent.*

4. Character sheaves and Lusztig's conjecture

First we briefly recall the theory of character sheaves developed by Lusztig. Let $\mathcal{D}G$ be the (bounded) derived category of $\bar{\mathbb{Q}}_l$-sheaves on G, and $\mathcal{M}G$ the full subcategory of $\mathcal{D}G$ consisting of perverse sheaves. $\mathcal{M}G$ is an abelian category admitting composition series of finite length. A notion of G-equivariance is introduced in $\mathcal{M}G$. We denote by $\mathcal{M}_G G$ the subcategory of $\mathcal{M}G$ consisting of G-equivariant perverse sheaves with respect to the adjoint action of G on G.

A complex $K \in \mathcal{D}G$ is called F-stable if $F^*K \simeq K$, where F^*K is the pull back of K under the Frobenius map F. For an F-stable K, we fix an isomorphism $\varphi : F^*K \xrightarrow{\sim} K$. It induces a linear isomorphism $\varphi_x : \mathcal{H}^i_x K \xrightarrow{\sim} \mathcal{H}^i_x K$ for $x \in G^F$. (Here for each $x \in G$, $\mathcal{H}^i_x K$ denotes the stalk at x of i-th cohomology sheaf $\mathcal{H}^i K$ of K). We define, for a given (K, φ) as above, a function $\chi_{K,\varphi} : G^F \to \bar{\mathbf{Q}}_l$ by

$$\chi_{K,\varphi}(x) = \sum_i (-1)^i \operatorname{Tr}(\varphi_x, \mathcal{H}^i_x K) \qquad (x \in G^F),$$

which is called the **characteristic function** of K with respect to φ. Note that perverse sheaves are purely geometric objects associated to G (but not to G^F). However, if K is a G-equivariant perverse sheaf, then $\chi_{K,\varphi}$ turns out to be a class function of G^F. Hence $\mathcal{M}_G G$ provides a machinery of producing class functions of G^F, and this gives a bridge connecting perverse sheaves on G with the character theory of G^F. It is of course essential to consider simple perverse sheaves. The.set of character sheaves defined by Lusztig is a certain set ($\subset \mathcal{M}_G G$) of G-equivariant simple perverse sheaves on G. We denote by $\widehat{G}$ the set of character sheaves on G. The scheme of the theory of character sheaves is quite analogous to that of Harish-Chandra theory for finite reductive groups in the following sense; there exists a notion of cuspidal character sheaves, and for each Levi subgroup L of a parabolic subgroup P of G, there exists an induction functor $\operatorname{ind}_P^G : \mathcal{M}_L L \to \mathcal{D}G$ satisfying the following property.

- For each cuspidal character sheaf $A_0 \in \widehat{L}$, $\operatorname{ind}_P^G A_0$ is a semisimple object in $\mathcal{M}_G G$, and each direct summand belongs to $\widehat{G}$.
- Any $A \in \widehat{G}$ is obtained as a direct summand of $\operatorname{ind}_P^G A_0$ for some $A_0 \in \widehat{L}$, cuspidal.

Before stating Lusztig's results on character sheaves, we prepare some notation. A prime $p = ch\mathbf{F}_q$ is called almost good for G if p satisfies the following conditions;

$$\begin{cases} p \neq 2, 3 & \text{if } G \text{ has factors of type } E_7, F_4, G_2, \\ p \neq 3 & \text{if } G \text{ has a factor of type } E_6, \\ p \neq 2, 3, 5 & \text{if } G \text{ has a factor of type } E_8, \end{cases}$$

and no conditions for factors of classical type. We denote by $(\widehat{G})^F$ the set of F-stable character sheaves on G. (Do not confuse this with $\widehat{G^F}$). For each $A \in (\widehat{G})^F$, we choose $\varphi_A : F^*A \xrightarrow{\sim} A$. Note that since A is simple, φ_A is unique up to scalar multiple.

Theorem 4.1 (Lusztig [L2]). *Assume that p is almost good for G. Then*

(i) *Under a certain normalization, $\{\chi_{A,\varphi_A} \mid A \in (\widehat{G})^F\}$ gives rise to an orthonormal basis of $C(G^F/\sim)$.*

(ii) *There exists a general algorithm of computing characteristic functions χ_{A,φ_A}.*

Based on his results, Lusztig proposed the following conjecture.

Conjecture 4.2 (Lusztig). There exists a natural parametrization $X(G^F) \simeq (\widehat{G})^F$, (which we denote by $x \leftrightarrow A_x$, and write as $\varphi_{A_x} = \varphi_x : F^*A_x \xrightarrow{\sim} A_x$), such that

$$\chi_{A_x,\varphi_x} = c_x R_x \qquad (c_x \in \bar{\mathbf{Q}}_l^*).$$

Lusztig's conjecture asserts that characteristic functions χ_{A,φ_A} coincide with almost characters up to scalar. Since we know the decomposition of almost characters into irreducible characters (especially in the case of connected center), Lusztig's conjecture provides us an algorithm of computing irreducible characters whenever we know the scalar constants c_x.

The following result by the author gives a partial answer to Lusztig's conjecture. Its proof is done by appealing to the theory of Shintani descent based on the Shintani descent identity for character sheaves, which is an analogy of the formula discussed in section 3.

Theorem 4.3 ([S2]). *Assume that the center of G is connected, and assume that p is almost good. Then Lusztig's conjecture holds for G^F.*

On the other hand, under some restrictions on p and q, Lusztig has proved the following result for arbitrary G.

Theorem 4.4 (Lusztig [L5]). *Let G be an arbitrary reductive group. Assume that p and q are large enough. Then for each cuspidal character sheaf A_x, the formula in the conjecture holds.*

Note that if the decomposition of the Lusztig induction $R^G_{L\subset P}$ is known, the above result implies the conjecture (for $p \gg 0, q \gg 0$). However such a decomposition is known, at present, only for the case of connected center (cf. Corollary 3.2).

Once Lusztig's conjecture is established (for example, in the case of connected center), the next step towards the computation of irreducible characters is the determination of scalars c_x appearing in the conjecture. In this direction, Lusztig has proved the following.

Theorem 4.5 (Lusztig [L3]). *Assume that G^F is an adjoint Chevalley group. Assume further that $p \equiv 1 \pmod N$ for some N, (for example, $N = 2$ for type B_n, $N = 4$ for type D_n and $N = 60$ for type E_8). Then for almost characters R_x whose supports are contained in G^F_{uni}, the scalars c_x are determined.*

We can also determine the scalar c_x in the following special cases. In the following, an almost character R_x is called a unipotent almost character if R_x is a linear combination of unipotent characters.

Theorem 4.6 ([S3]). *Assume that G^F is a Chevalley group of classical type with connected center. Assume further that p is odd. Then the scalar c_x is determined for a unipotent almost character R_x.*

This can be generalized to the case of exceptional groups.

Theorem 4.7 (Lübeck, Shinoda, S). *Assume that G^F is an exceptional group of adjoint type. Assume further that p is good. Then the scalar c_x is determined for a unipotent almost character R_x.*

Here we give the number of unipotent characters in the case of exceptional groups.

G_2	F_4	E_6	E_7	E_8
10	37	30	76	112

Remark. The above results provide an algorithm of computing unipotent characters. In fact, Lübeck "computed" all the character values of unipotent characters for F_4 and E_6 by making use of the computer algebra system CHEVIE ([GPHLM]). His program will work also for E_7 and E_8. However in applying Lusztig's algorithm in practice, still there remains a problem in choosing rational unipotent classes in a given geometric unipotent class. So in order to justify Lübeck's computation, we need to determine some parameters related to the choice of representatives (see the next section).

5. The computation of χ_{A,φ_A}

We shall explain briefly Lusztig's algorithm of computing characteristic functions x_{A,φ_A} for $A \in (\widehat{G})^F$. Here we consider an arbitrary reductive group G. Let $A_0 \in \widehat{L}$ be cuspidal, and put $K = \operatorname{ind}_P^G A_0$. We assume that L is an F-stable Levi subgroup of an F-stable parabolic subgroup P of G. We also assume that A_0 is F-stable, and fix an isomorphism $\varphi_0 : F^*A_0 \xrightarrow{\sim} A_0$. As in the case of maximal tori, any F-stable Levi subgroups conjugate to L are parametrized (up to G^F-conjugate) by the conjugacy classes of $\mathcal{W} = N_G(L)/L$. We denote by L_w an F-stable Levi subgroup corresponding to $w \in \mathcal{W}$. It is known that $\operatorname{End} K \simeq \bar{\mathbb{Q}}_l[\mathcal{W}_0]_t$ (a twisted group algebra of a subgroup $\mathcal{W}_0$ of $\mathcal{W}$). In the case of connected center, it is actually the group algebra of a reflection subgroup $\mathcal{W}_0$. Now $\varphi_0 : F^*A_0 \xrightarrow{\sim} A_0$ on L gives rise to an isomorphism $\varphi_w : F^*A_0 \xrightarrow{\sim} A_0$ on L_w for $w \in \mathcal{W}_0$. This induces an isomorphism $F^*K \xrightarrow{\sim} K$ which is denoted also by φ_w. We consider the characteristic function χ_{K,φ_w} of K. Then by using the orthogonality relations of the characters of $\mathcal{W}_0$, it is shown that the determination of χ_{A,φ_A} for various direct summand A in K is equivalent to the determination of χ_{K,φ_w} for various $w \in \mathcal{W}_0$. The class functions χ_{K,φ_w} have similar properties as $R_T^G(\theta)$. In fact, if $L_w = T_w$ and $A_0 \in (\widehat{L})^F$ is obtained from $\theta \in \widehat{T}_w^F$, then χ_{K,φ_w} coincides with $R_{T_w}^G(\theta)$. Lusztig proved that χ_{K,φ_w} also has the character formula analogous to the character formula in section 2, where the role of Green functions are replaced by generalized Green functions Q_{L_w,φ_0}^G ($w \in \mathcal{W}$), which are G^F-invariant functions on G_{uni}^F. Put, for $E \in \mathcal{W}^\wedge$,

$$Q_{L,E}^G = |\mathcal{W}|^{-1} \sum_{w \in \mathcal{W}} E(w) Q_{L_w,\varphi_0}^G.$$

Then the determination of Q_{L_w,φ_0}^G is equivalent to that of $Q_{L,E}^G$ for various $E \in \mathcal{W}^\wedge$.

We consider a pair (C, ξ), where C is a unipotent class in G, and ξ is an irreducible character of $A_G(u) = Z_G(u)/Z_G^0(u)$ for some $u \in C^F$. Now the set of G^F-conjugacy classes in C^F is in bijection with the set $A_G(u)/\sim_F$. We denote by u_a a representative in C^F corresponding to $a \in A_G(u)$. Let us define a G^F-invariant function f_ξ on G^F_{uni} by

$$f_\xi(x) = \begin{cases} \xi(a) & \text{if } x \text{ is } G^F\text{-conjugate to } u_a, \\ 0 & \text{if } x \notin C^F. \end{cases}$$

Then by the generalized Springer correspondence, for each $Q^G_{L,E}$ there corresponds a pair (C, ξ) satisfying the following. $Q^G_{L,E}$ has support in $\bar{C}^F$ ($\bar{C}$ denotes the closure of C in G), and the restriction $Q^G_{L,E}|_{C^F}$ of $Q^G_{L,E}$ to C^F coincides with $\lambda_\xi f_\xi$ for some $\lambda_\xi \in \bar{\mathbf{Q}}_l^*$.

Lusztig showed, by modifying and generalizing the author's method of computing Green functions, that there exists an algorithm of expressing $Q^G_{L,E}$ in terms of various $\lambda_\xi f_\xi$. Hence in order to obtain a complete algorithm of computing χ_{A,φ_A}, we need to determine the constants λ_ξ for each $\xi \in A_G(u)^\wedge$. This problem is also related to the choice of a "good representative" $u \in C^F$. It has been established in the case of Green functions, i.e., in the case where $L = T$, but it is not yet solved for generalized Green functions in general.

6. The case of disconnected center

In the case where the center of G is disconnected, the main problem is the proof of Lusztig's conjecture. For this we need to know the decomposition of the Lusztig induction $R^G_{L\subset P}$. As in the case of connected center, one possible approach for this would be the theory of Shintani descent. Hence it is important to determine the Shintani descent. The typical example for such a group is $G^F = SL_n(\mathrm{F}_q)$. In this case we have the following result.

Theorem 6.1 ([S4]). *Let $G^F = SL_n(\mathrm{F}_q)$. Assume that m is sufficiently divisible. Then the Shintani descent $Sh_{F^m/F}$ can be described. In particular, almost characters of G^F are explicitly given.*

Note that however, this result is not enough to give a complete description of the Lusztig induction. In the remainder of this section we assume that G is an arbitrary reductive group.

- **The Mackey formula**

Another approach for getting the information on the Lusztig induction is the following Mackey formula for Lusztig induction which is an analogue of the usual Mackey formula of finite groups. We define a linear map ${}^*R^G_{L\subset P}$, called the Lusztig restriction,

$${}^*R^G_{L\subset P} : C(G^F/\!\sim) \to C(L^F/\!\sim)$$

as the adjoint functor of the Lusztig induction $R^G_{L\subset P}$. Let M be an F-stable Levi subgroup of another parabolic subgroup Q of G. Put

$$\mathcal{E}(L, M) = \{x \in G \mid L \cap {}^xM \text{ contains a maximal torus of } G\}.$$

We shall formulate the Mackey formula as follows.

(The Mackey formula.)

$$ {}^*R^G_{L\subset P} \circ R^G_{M\subset Q} = \sum_{x\in L^F\backslash\mathcal{E}(L,M)^F/M^F} R^L_{L\cap {}^xM\subset L\cap {}^xQ} \circ {}^*R^{{}^xM}_{L\cap {}^xM\subset P\cap {}^xM}. $$

It is not yet known whether the Mackey formula holds in a full generality. It has been verified in the following special cases, (a) P and Q are F-stable parabolic subgroups, i.e., the case of Harish-Chandra inductions and Harish-Chandra restrictions, (b) L and M are maximal tori of G. We note here that the Mackey formula implies the fact that the Lusztig induction $R^G_{L\subset P}$ depends only on L and not on P.

Recently C. Bonnafé proved the following result.

Theorem 6.2 (Bonnafé [B]). *Assume that q is large enough, (but no assumption on p). Then the Mackey formula holds for any F-stable Levi subgroups L and M.*

- **Generalized Gelfand-Graev representations.**

Generalized Gelfand-Graev representations have been introduced by Kawanaka, by generalizing the usual Gelfand-Graev representations. In the case of disconnected center, a similar approach as in the case of connected center, such as Deligne-Lusztig theory, does not give enough information for irreducible characters. It is expected that generalized Gelfand-Graev representations provide us necessary informations in such a case. In fact, in the case of $SL_n(\mathbf{F}_q)$, generalized Gelfand-Graev characters are used to parametrize irreducible characters in a more precise way than Lusztig's parametrization. Now for each unipotent element $u \in G^F$, there corresponds an F-stable parabolic subgroup P with unipotent radical U_P, i.e., the parabolic subgroup associated to the unipotent class of u in G^F. Also one can construct an irreducible representation Λ_u of U_P^F. Then $\Gamma_u = \mathrm{Ind}_{U_P^F}^{G^F} \Lambda_u$ depends only on the G^F-conjugacy class of u, and is called the **generalized Gelfand-Graev representation** of G^F associated to the class of u. Note that if u is a regular unipotent element, then Γ_u coincides with the usual Gelfand-Graev representations.

Kawanaka decomposed Γ_u into irreducible characters in the case of GL_n for arbitrary p and q, and also treated the exceptional groups of adjoint type, (see, e.g., [K]). On the other hand, under the assumption that p and q are large enough, Lusztig described the decomposition of Γ_u in terms of the characteristic functions of character sheaves. Using this, he showed the following result.

Theorem 6.3 (Lusztig [L4]). *Assume that p and q are large enough. Then for any $\rho \in \widehat{G}^F$, there exists a unique unipotent class C in G such that $\sum_{g\in C^F} \rho(g) \neq 0$, and having maximal dimension among the classes with this property.*

The class C attached to ρ is called the **unipotent support** of ρ. Recently, M. Geck succeeded in removing the assumption on p, q of Lusztig's result in the case where p is good, and then extended it with G. Malle to the case where p is bad.

Theorem 6.4 (Geck [G], Geck-Malle [GM]). *The statement of Theorem 6.3 holds for any G with no restrictions on p and q.*

We close this note by stating the following result, which discusses the Lusztig restriction of Gelfand-Graev characters.

Theorem 6.5 (Digne-Lehrer-Michel [DLM]). *Assume that p is good and that q is large enough. Let Γ_u be the Gelfand-Graev character of G^F associated to a regular unipotent element $u \in G^F$. Let L be an F-stable Levi subgroup of a (not necessarily F-stable) parabolic subgroup P of G. Then there exists a regular unipotent element $v \in L^F$ such that*

$$^*R^G_{L\subset P}(\Gamma_u) = \varepsilon_G \varepsilon_L \Gamma_{L,v},$$

where $\Gamma_{L,v}$ is the Gelfand -Graev character of L^F associated to v, and ε_G (resp. ε_L) is the split rank of G (resp. L), respectively.

Note that in the case of disconnected center, it follows from the theorem that a rational regular unipotent class in G^F determines a rational regular unipotent class in each F-stable Levi subgroup L. However, the correspondence is not explicitly known.

References

[B] C. Bonnafé, Formule de Mackey, to appear in J. of Algebra.

[DL] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, Ann. of Math. 103 (1976), 103–161.

[DLM] F. Digne, G. I. Lehrer and J. Michel, On Gelfand-Graev characters of reductive groups with disconnected center, to appear in Crelles J.

[G] M. Geck, On the average values of the irreducible characters of finite groups of Lie type on geometric unipotent classes, preprint (1996).

[GM] M. Geck and G. Malle, On the existence of a unipotent support for the irreducible characters of a finite group of Lie type, preprint (1996).

[GPHLM] M. Geck, G. Pfeiffer, G. Hiss, F. Lubeck and G. Malle, CHEVIE— Generic character tables of finite groups of Lie type, Hecke algebras and Weyl groups, preprint Heidelberg, 1993.

[K] N. Kawanaka, Shintani lifting and Gelfand-Graev representations, in "The Arcata conference on Representations of finite groups," Proceedings of Symposia in Pure Math., Vol. 47–1, pp. 147–163. Amer. Math. Soc. Providence, RI, 1987.

[L1] G. Lusztig, "Characters of Reductive groups over a Finite field," Ann. of Math. Studies, Vol. 107, Princeton Univ. Press, Princeton, 1984.

[L2] G. Lusztig, Character sheaves, I, Adv. in Math. 56 (1985), 193–237, II, Adv. in Math. 57 (1985), 226–265, III, Adv. in Math. 57 (1985), 266–315, IV, Adv. in Math. 59 (1986), 1–63, V, Adv. in Math. 61 (1986), 103–155.

[L3] G. Lusztig, On the character values of finite Chevalley groups at unipotent elements, J. of Algebra, 104 (1986), 146–194.

[L4] G. Lusztig, Unipotent support for irreducible representations, Adv. in Math. 94 (1992), 139–179.

[L5] G. Lusztig, Remarks on computing irreducible characters, J. Amer. Math. Soc. 5 (1992), 971–986.

[S1] T. Shoji, Shintani descent for exceptional groups over a finite field, J. Fac. Sci. Univ. Tokyo Sect. IA 34 (1987), 599–653.

[S2] T. Shoji, Character sheaves and almost characters of reductive groups, Adv. in Math. 111 (1995), 244 - 313, II, Adv. in Math. 111 (1995), 314 - 354.

[S3] T. Shoji, Unipotent characters of finite classical groups, in " finite reductive groups: related structures and representations." Proceedings of an international conference held in Luminy, Progress in Math. Vol 141 (1997), 373 - 413.

[S4] T. Shoji, Shintani descent for special linear groups, to appear in J. of Algebra.

THE SEMISIMPLE APPROACH TO THE CLASSIFICATION OF THE FINITE SIMPLE GROUPS

RONALD SOLOMON

The Ohio State University

To date there have been two successful approaches to the proof of the classification of the finite simple groups, which I shall call the "semisimple approach" and the "parabolic approach". Neither is sufficient by itself to yield a complete classification theorem, but in unison they have led to the existing classification proof. Although other approaches have been envisioned, the most active line of inquiry at present relates to the appropriate demarcation lines between these two approaches. I shall describe approximate definitions for these two approaches and discuss various possibilities for these demarcation lines.

Much of the early work in the modern era of the classification proof centered around Brauer's philosophy of identifying a finite simple group via the centralizer of one of its involutions. This approach was articulated by Brauer in his International Congress address in 1954 and gained further credibility when Feit and Thompson proved that every non-abelian finite simple group does indeed contain an involution.

Much of the work of Brauer and his students Fong and W.J.Wong focussed on the characterization of classical linear groups over fields of odd characteristic in which elements of order 2 are semisimple (diagonalizable). The work of Gorenstein and Walter directed towards "killing the cores" of involution centralizers continued this pattern of focussing attention on target groups in which involutions were semisimple elements (in the natural linear representations of the groups).

In the early 1970's as this phase of the classification effort neared its completion, Gorenstein and Lyons directed their attention towards the remaining problem of characterizing the finite simple groups of Lie type in characteristic 2, in which involutions were unipotent elements. At this point they conceived the idea of shifting attention from the prime 2 to a different prime p such that elements of order p would again be semisimple elements in the target group G.

This indeed became the ultimately successful strategy for the original classification proof and it may be formulated in the following way. All approaches rest on the fundamental concept of the Fitting and generalized Fitting subgroups, first fully defined by Helmut Bender.

Definition. *A finite group is semisimple if it is the product of commuting quasisimple groups. If H is a finite group, then $E(H)$ is the maximal normal semisimple subgroup of H, $F(H)$ is the maximal normal nilpotent subgroup of H and*

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

$F^*(H) = E(H)F(H)$. Moreover if p is a prime, then $O_p(H)$ is the maximal normal p-subgroup of H (which is contained in the Fitting subgroup $F(H)$).

First Semisimple Approach to the Classification.

Definition. *Let p be a prime and let g be an element of the finite group G of prime order p. We say that g is a semisimple element of G of order p if $E(C_G(g)) \neq 1$. We say that g is a unipotent element of G of order p if $F^*(C_G(g)) = O_p(C_G(g))$.*

***B*-Theorem.** *Let p be a prime such that G has p- rank at least 3. Then either G contains a semisimple element of order p or every element of order p is unipotent. (In the latter case we say that G is of characteristic p type.)*

Step 1: The Semisimple Case. *If possible find a prime p such that G contains a semisimple element of order p. Choose $p = 2$, if possible. Implement Brauer's strategy to characterize G via the centralizer of a semisimple element of order p.*

For the prime $p = 2$, Aschbacher's Component Theorem gives fundamental information about the structure of the centralizer of a suitable semisimple element of order 2. In an inductive context Aschbacher's result can be extended to all primes p. Then induction reduces Step 1 to a "finite" problem of Brauer type.

Step 2: The Parabolic Case. *If no semisimple element can be found in G, then by the B-Theorem, this has one of three possible implications:*

(1) *G has 2-rank at most 2; or*
(2) *G is of characteristic 2-type and G has 2-local p-rank at most 2 for all odd primes p; or*
(3) *G is of both characteristic 2-type and characteristic p-type for some odd prime p such that G has 2-local p-rank at least 3.*

The first case was historically treated first and includes the Odd Order Theorem of Feit and Thompson, the Brauer-Suzuki Theorem, the Dihedral Theorem of Gorenstein and Walter and the 2-Rank 2 Theorem of Alperin, Brauer and Gorenstein. (Operationally much of the analysis of the Dihedral and 2-Rank 2 Theorems fall within the Semisimple Methodology, although the final identifications of the target groups are as BN pairs of rank 1 or 2.)

The second case is the Quasi-Thin Theorem, currently being given a final treatment by Aschbacher, S.D.Smith and Meierfrankenfeld.

The third case was handled by Klinger and G. Mason extending results of J.G.Thompson.

In this original proof of the Classification Theorem, the Semisimple Method is used whenever possible, i.e. whenever G contains a semisimple element of prime order. Only in extremis does one resort to the parabolic method – primarily for the Odd Order Theorem and the Quasi-Thin Theorem, though also for certain Uniqueness Theorems.

Second Semisimple Approach to the Classification.

In the "second generation" proof of the Classification Theorem, the strategy remains the same with one significant modification. It is difficult to detect from internal evidence the fact that extensions of a group of Lie type in characteristic 2 by a field automorphism of order 2 are not simple groups. For this reason in the original proof of the Classification Theorem, these simple groups are identified twice – in the Semisimple Case starting from the centralizer of a field automorphism of order 2 and in the Parabolic Case starting from the centralizer of a semisimple element of odd order or from a pair of maximal parabolic subgroups. To avoid this redundancy, the second generation strategy modifies the definition of semisimple. The price we pay is a more complicated definition and a definition which rests on the inductive nature of the proof. In fact I will not give the precise definition but only a reasonable approximation.

Definition. *If H is a p-local subgroup of the finite simple group G and if L is a quasi-simple normal subgroup of $E(H)$ of order divisible by p, then we call L a p-component of H.*

Definition. *Let G be a finite simple group and let g be an element of G of prime order p. We say that g is strongly semisimple if $E(C_G(g))$ has a p-component L which is neither a sporadic group nor a group of Lie type in characteristic p.*

As suggested above the principal purpose of the definition is to distinguish the "truly" semisimple elements from the field automorphisms of order equal to the characteristic of the field. The domain of the parabolic method is now expanded slightly as follows.

Definition. *Let G be a finite simple group. We say that G is of even type if G has 2-rank at least 3 and G contains no strongly semisimple involutions. Analogously G is of p-type (for the odd prime p) if G has p-rank at least 3 and contains no strongly semisimple elements of order p.*

We remark that insofar as the actual target simple groups are concerned, the effect is to shift the border only slightly, namely most of the sporadic simple groups move from being of semisimple type to being of even type. In point of fact however, most of the sporadic simple groups were identified in the original approach at least once by parabolic methods – either as quasi-thin groups or as groups in which some involution centralizer is of symplectic type.

New Step 1: The New Semisimple Case. *If possible find a strongly semisimple element in G of prime order. Again choose an involution if possible. In any case implement Brauer's approach to identify G.*

New Step 2: The New Parabolic Case. *Again if Step 1 fails, we are in one of three possible cases:*

(1) *G has 2-rank at most 2; or*
(2) *G is of even type and the 2-local p-rank of G is at most 2 for all odd primes p; or*
(3) *G is both of even type and of p-type for some odd prime p such that the 2-local p-rank of G is at least 3.*

The third case was handled by Gorenstein and Lyons extending the work of Klinger and Mason. It leads to the largest sporadic simple groups as well as a few classical groups. The second case is the extended Quasi-Thin Theorem, currently being treated by Aschbacher, Smith and Meierfrankenfeld.

A Third Approach.

One serious objection to the first and second approaches to the Classification proof is that the Semisimple Case rests eventually on quite difficult Uniqueness Theorems, which in the even type case rely on elaborate parabolic analysis. Thus the parabolic methodology is invoked on an emergency basis in two principal contexts – the Quasi-Thin Case and the Uniqueness Case.

It has been suggested by Bernd Stellmacher and Ulrich Meierfrankenfeld that it would be more natural and conceptually unified to treat the entire characteristic p-type case (at least for $p = 2$) via parabolic analysis, relegating the semisimple approach to the traditional Brauer context of semisimple involutions. I believe that it would even more natural in this spirit to treat the entire even type case by parabolic methods. Thus a potential third approach to the Classification proof might be subdivided as follows.

Potential Step 1: The Parabolic Approach. *If possible, find a prime p such that G is of p-type. Identify G via p-parabolic methods.*

It should be noted that the "amalgam method "implemented by Stellmacher and Meierfrankenfeld presupposes that G is generated by the parabolic overgroups of a fixed Sylow p-subgroup of G. When this fails, one is again in a Uniqueness Case. For $p = 2$, this uniqueness problem was handled by Aschbacher relying eventually on the fundamental Strongly Embedded Subgroup Theorem of Suzuki and Bender. For odd p there is at present no good strategy for treating the resulting uniqueness problem and so for the present this Step 1 is best regarded as an alternate approach to the Even Type Case. Indeed it is precisely by this subdivision of the problem that the uniqueness theorems for odd primes can be completely circumvented, except of course for the Odd Order Theorem.

Potential Step 2: The Semisimple Approach. *If Step 1 fails, then in particular, some involution in G is strongly semisimple. Identify G via Brauer's approach in this case.*

Indeed even if Step 1 fails only in the weak sense that G is not of even type, then some involution in G is strongly semisimple and the classical approach will complete the Classification proof. Step 2 of this method is not "potential ". What remains to be accomplished is the resolution of the full even type case (or even the characteristic 2-type case) by amalgam methods.

COLUMBUS, OHIO 43210 USA

J-Components in finite groups

Bernd Stellmacher

Christian-Albrechts-Universität zu Kiel

1. Introduction. This talk is a survey of my joint work with U. Meierfrankenfeld on the embedding of J-components in finite groups.

The proof of the classification theorem for the finite simple groups, very roughly, falls into two major parts according to the following two cases:

(I) There exists a 2-local subgroup M such that $F^*(M)$ is not a 2-group.

(II) All 2-local subgroups M satisfy $F^*(M) = O_2(M)$ (or equivalently $C_M(O_2(M)) \leq O_2(M)$).

For the first case the fundamental work of Aschbacher on components gives the frame work. Our work is related to the second case, and our arguments allow to substitute 2 in (II) by an arbitrary prime. Such a group all of whose p-local subgroups satisfy (II) is call a group of characteristic p type. In fact, we can furhter relax condition (II) by demanding this property only for certain of the p-local subgroups of G, but I will omit these technical details.

¿From now on G is a finite group of characteristic p type. We will need two further hypotheses on the p-local subgroups M of G:

i) Schreier's conjecture holds for every simple section of M.

ii) The simple sections of M are known simple groups.

Both conditions hold for a minimal counterexample in the proof of the classification theorem, and condition i) follows from ii). I have stated them seperately since the first one is basic for our investigation while the second one is only used in a particular case to give a "round" result. I will comment on that later.

2. p-Components. Let M be a p-local subgroup of G. There do not exist components[1] of M since $O_p(M)$ contains its centralizer. But there is an obvious way of generalizing the concept of a component so that it fits p-local subgroups satisfying (II):

Let X be a subgroup of G and K a subgroup of X. Then K is a p-component of X, if

[1] A component of M is a quasisimple subnormal subgroup of M.

(a) K is subnormal in X, and

(b) $K = O^p(K)$, and $K/O_p(K)$ is quasisimple.

In particular, if $X = M$ as in (II), then $KO_p(M)/O_p(M)$ is a component in $M/O_p(M)$. Of course, in genereal, there might be no components in $M/O_p(M)$. We will introduce further below the notion of a solvable J-component to cover this situation.

Because of (II) p-components K of M satisfy

$$(*) \quad C_K(O_p(K)) \leq O_p(K).$$

Let C be the set of all $K \leq G$ such that K is a p-component in some p-local subgroup of G. We are interested in the following questions:

What can be said about the embedding of elements of C in p-local subgroups? Are there elements in C which are contained in a unique maximal p-local subgroup?

In the investigation of components "cross characteristic" properties are used. In the case of p-components this is not possible. The non-central chief factors of K in $O_p(K)$ ($K \in C$) are obstructions for nice inheritance properties of centralizers of p-elements in K and $K/O_p(K)$, respectively. On the other hand, the action of K on non-central p-chief factors might give additional information; at least, if the p-components are chosen appropriate. This leads to the definition of a (solvable) J-component. First we fix the following notation[2]:

$$S \in Syl_p(G), Z = Z(S), C = C_G(Z), J = J(S).$$

An arbitrary subgroup K is a J-component of G, if

(1) K is a p-component of $[K, J]$ and

(2) $O_p(K) \not\leq Z(K)$;

and K is a solvable J-component of G, if

(1′) $K/O_p(K)$ is a q-group (q a prime), and

(2′) $K = [K, J] = O^p(K)$ and $O_p(K) \not\leq Z(K)$.

There are two basic properties of J-components K which are essential for the entire investigation :

[2] $J(S)$ denotes the Thompson subgroup of S.

Lemma 1. Let K be a J-component and R a p-subgroup of G. Suppose that $\langle K, J\rangle \leq N_G(R)$. Then $R \leq N_G(K)$.

Proof. Note first that R normalizes $\langle J^K\rangle$ since $J = J(RJ)$ and $KR = RK$. Note further that

$$K \leq [K, J] \leq \langle J^K\rangle \leq \langle K, J\rangle R.$$

K is subnormal in $[K, J]$ and thus in $\langle K, J\rangle R$; in particukar, K is subnormal in KR. Now $O^p(K) = K$ implies that $K = O^p(KR)$.

The second property is not elementary. For $p = 2$ it is a result of Aschbacher and Timmesfeld (see [Ti]); for arbitrary p recently Chermak [Ch] gave a short and self-contained proof.

Lemma 2. Let K be a J-component of G. Suppose that $[Z(O_p(K)), K] \neq 1$. Then $J \leq N_G(K)$.

Suppose that K is a J-component of G and $\langle K, J\rangle \leq L$ for some p-local subgroup L of G. The first lemma shows that $O_p(L) \leq N_G(K)$. The second lemma together with Schreier's conjecture allows to handle the embedding of $\overline{K}$ in $F^*(\overline{L})$, where $\overline{L} := L/C_L(Z(O_p(L)))$; of course with some care, since Lemma 2 does not apply to J-components satisfying

$$[K, Z(O_p(K))] = 1.$$

Since one cannot exclude such "central" J-components the strategy is to deal with them from the very beginning. More precisely, we start with J-components which are p-components in C ($= C_G(Z)$) and investigate their embedding in other p-local subgroups.

3. Results. We use the following notation:

$\mathcal{C}_J$: the set of J-components of G,

$\mathcal{S}_J$: the set of solvable J-components of G, and

$\mathcal{SC}_J := \mathcal{C}_J \cup \mathcal{S}_J$.

An element $K \in \mathcal{SC}_J$ is said to be a **uniqueness subgroup for** J, if

(U_1) $\langle K, J\rangle$ is contained in a unique maximal p-local subgroup M of G, and

(U_2) K is subnormal in M.

And K is weak uniqueness subgroup for J, if (U_2) holds for every p-local subgroup M containing $\langle K, J\rangle$.

Theorem 1. One of the following holds:

(a) $\mathcal{SC}_J = \emptyset$, and $N_G(J)$ is the unique maximal p-local subgroup containing J.

(b) $\mathcal{C}_J = \emptyset$, and every element in $\mathcal{S}_J$ is a weak uniqueness subgroup for J.

(c) There exists a uniqueness subgroup for J in $\mathcal{C}_J$.

In case (c) of Theorem 1 an explicit "algorithm" can be given to find uniqueness subgroups. This is described in the next theorem. We use the following further notation:

$\mathcal{C}_J^+ := \{K \in \mathcal{C}_J \mid [Z(O_p(K)), K] \neq 1\}$.

$\mathcal{C}_J^- := \{K \in \mathcal{C}_J \mid [Z(O_p(K)), K] = 1\}$.

$\mathcal{K}_J(X) := \{K \in \mathcal{C}_J^+ \mid \langle X, J\rangle \leq N_G(K)\}$.

$\mathcal{C}_J(X)$: the set of $K \in \mathcal{C}$ which are subnormal in the subgroup X;

similarly $\mathcal{C}_J^+(X)$ and $\mathcal{C}_J^-(X)$ are defined.

Theorem 2. Suppose that $\mathcal{C}_J \neq \emptyset$. Then one of the following holds:

(a) $\mathcal{SC}_J(C) = \emptyset$. Every maximal element in $\mathcal{C}_J$ is a uniqueness subgroup for J.

(b) $\mathcal{C}_J^+(C) \neq \emptyset$. For every maximal element

$$K \in \cup_{g \in N_G(J)} C^g$$

the maximal elements of $\mathcal{C}_J$ containing K are uniqueness subgroups for J.

(c*) $\mathcal{C}_J(C) \neq \mathcal{C}_J^+(C) = I_J(K) = \emptyset$ for every $K \in \mathcal{SC}_J(C)$, and every element of $\mathcal{C}_J(C)$ is a uniqueness subgroup for J.

(d) $\mathcal{C}_J(C) \neq \mathcal{C}_J^+(C) = \emptyset$ and $\mathcal{K}_J(K) \neq \emptyset$ for some $K \in \mathcal{SC}_J(C)$. For every such K and $E \in \mathcal{K}_J(K)$ the maximal elements of $\mathcal{C}_J$ containing E are uniqueness subgroups for J.

It is in case (c) where condition ii) is used to solve a certain pushing up problem, which allows to conclude that a weak uniqueness subgroup for J is already a uniqueness subgroup.

References. [Ch] Chermak, A.: Quadratic action, and the $\mathcal{P}(G,V)$-theorem in arbitrary characteristic, Preprint (1996).

[Ti] Timmesfeld, F.: A remark on Thompson's replacement theorem and a consequence, Arch. Math. 38 (1982), 491 - 499.

Small modules

Gernot Stroth[1]
Fachbereich Mathematik und Informatik
Institut für Algebra und Geometrie
Martin-Luther-Universität Halle Wittenberg
06099 Halle, Germany

There is no well defined concept of small modules. First of all we will give some motivation why a certain class of modules, which we will call small lateron, is of interest.

a) Failure of factorization:

Let G be a group with

$$F^*(G) = O_p(G), \text{ and } S \in \mathrm{Syl}_p(G)$$

A classical result due to G. Glauberman [Go, 8.2.11] is:

If p is odd and G is p-stable, then $\Omega_1(Z(J(S))) \trianglelefteq G$.

Here p-stable means that $p^2SL_2(p)$ is not involved. A certain extension of this result for $p = 2$ was recently established by B. Stellmacher [Stell]. The result tells us that the structure of G is determined by the normalizer of a well defined characteristic subgroup of the Sylow p-subgroup S.

Now we look at a more general situation. Set $Z = \langle \Omega_1(Z(S))^G \rangle$, then $Z \leq \Omega_1(Z(O_p(G)))$. If $J(S) \leq C_G(Z)$ then we get

$$G = C_G(\Omega_1(Z(S)))N_G(Z(J(S))).$$

In that case the structure of G is determined by the structure of two normalizers of well defined characteristic subgroups of S.

So assume that $J(S) \not\leq C_G(Z)$. Then there is some

$$A \in \mathcal{A}(S) = \{B | B \leq S, \text{elementary abelian of maximal rank}\}$$

such that $A \not\leq C_G(Z)$. Now $ZC_A(Z)$ is also elementary abelian, hence

$$|ZC_A(Z)| \leq |A|$$

$$|Z/C_Z(A)| \leq |Z/Z \cap A| \leq |A/C_A(Z)|.$$

So what we get is a so called F-module (failure of factorization).

[1] Email:stroth@coxeter.mathematik.uni-halle.de

Definition Let G be a group and V be a faithful $GF(p)G$–module. Then V is called a F–module for G if there is some elementary abelian p–subgroup A in G, $1 \neq A$ such that

$$|V : C_V(A)| \leq |A|.$$

Any group A with this property is called an offending subgroup.

b) Amalgam method :

Here the situation is as follows. There are two groups P_1 and P_2 with $O_p(P_i) = F^*(P_i)$, sharing a Sylow p–subgroup S. We introduce the coset graph $\Gamma = P_1g \cup P_2h$, whose vertices are the cosets of P_1 and P_2 and edges are the pairs $\{P_1g, P_2h\}$ with $P_1g \cap P_2h \neq \emptyset$. We denote the vertices P_1 and P_2 of Γ with 1 and 2, respectively. Let $\beta \in \Gamma$ then the stabilizer P_β of β is conjugate to P_1 or P_2. Set $Z_i = \langle \Omega_1(Z(S))^{P_i} \rangle$, $i = 1, 2$. Let

$$b_i = \min(d(\alpha, i) \mid \alpha \in \Gamma : Z_i \not\leq P_\beta \text{ for some } \beta \in \Delta(\alpha))$$

and

$$b = \min(b_1, b_2).$$

One case which arises quite often is

$$d(1, \alpha) = b, Z_1 \leq P_\alpha, Z_\alpha \leq P_1 \text{ and } [Z_1, Z_\alpha] \neq 1.$$

Then by symmetry we may assume that

$$|Z_1 : C_{Z_1}(Z_\alpha)| \leq |Z_\alpha : C_{Z_\alpha}(Z_1)|$$

and again we have an F–module Z_1. In fact we see a little bit more

$$[Z_1, Z_\alpha, Z_\alpha] \leq [Z_1 \cap Z_\alpha, Z_\alpha] = 1$$

So Z_1 is a quadratic module. But this is for F–modules always the case, as can be seen by Thompson replacement [Go].

So we can see that F-modules do play an important role. There is a classification of F–modules in characteristic two due to M. Aschbacher [Asch] for alternating , sporadic and Lie type groups in odd characteristic and B. Cooperstein [Coop] for Lie type groups in characteristic two. Unfortunately the latter depends on unpublished results of B. Cooperstein and G. Mason [CoMa].

Suppose now $p = 2$ and $P_2/O_2(P_2) \cong \Sigma_3$. Suppose further $\Omega_1(Z(S)) \trianglelefteq P_2$ and $\alpha \sim 2$. We have $[Z_1, Z_\alpha] = 1$ and further

$$|Z_1 : Z_1 \cap P_\beta| = 2 \text{ and } [Z_1 \cap P_\beta, Z_\beta] \leq Z_\beta.$$

Let us assume that we have symmetry , i.e. $|Z_\beta : Z_\beta \cap P_1| \leq 2$. Then we may assume

$$|Z_1 : C_{Z_1}(Z_\beta \cap P_1)| \leq |Z_\beta : C_{Z_\beta}(Z_1 \cap P_\beta)|.$$

Now as the index was 2 we get

$$|Z_1 : C_{Z_1}(Z_\beta \cap P_1)| \leq 2|Z_\beta \cap P_1/C_{Z_\beta \cap P_1}(Z_1)|.$$

So if $Z_\beta \cap P_1$ acts notrivially on Z_1 we get what is called an $F+1$–module

Definition Let G be a group and V be a faithful $GF(p)G$–module. Then V is called a $F+1$–module for G if there is some elementary abelian p–subgroup A in G, $1 \neq A$ such that

$$|V : C_V(A)| \leq p|A|.$$

Any group A with this property is called an offending subgroup.

Again there is a classification of $F+1$–modules in characteristic two due to M. Aschbacher [Asch] for alternating, sporadic and Lie type groups in odd characteristic and P. McClurg [McC] for Lie type groups in characteristic two. Unfortunately the latter is not published and also depends on the unpublished work mentioned before.

All these arguments leading to F- or $F+1$-modules in the amalgam method work very well if b is large. For small b one needs more information.

Let $b = 2$, $P_1/O_2(P_1) \cong \Sigma_3$ and $\langle z \rangle = \Omega_1(Z(S)) \trianglelefteq P_2$. Then $Z_1 = \langle z, t \rangle$ is of order 4. Set $E = \langle Z_1^{P_2} \rangle$. Then $E' = \langle z \rangle$. So this situation is very similar to the extraspecial situation in the classification of the finite simple groups. So assume for the moment that $P_2 = C_G(z)$ and $O_2(C_G(z))$ is extraspecial, $Z_1 \leq O_2(C_G(z))$. Then $O_2(C_G(t)) \cap P_2$ is of index two in $O_2(C_G(t))$. Furthermore $O_2(C_G(t)) \cap O_2(C_G(z))$ is elementary abelian. Let now $|O_2(C_G(z))| = 2^{2n+1}$. Then $|O_2(C_G(z)) \cap O_2(C_G(t))| \leq 2^{n+1}$ and so

$$|A| = |O_2(C_G(t)) \cap P_2/O_2(C_G(z))| \geq 2^{n-1}.$$

The usual action of A on $O_2(C_G(z))/\langle z \rangle$ is that it centralizes exactly $\langle t \rangle$ so we get that

$$|O_2(C_G(z))/\langle z \rangle : C_{O_2(C_G(z))/\langle z \rangle}(A)| \leq 2|A|^2.$$

This leads to the following definition

Definition Let G be a group and V be a faithful $GF(p)G$–module. Then V is called a $2F+1$–module for G if there is some elementary abelian p–subgroup A in G, $1 \neq A$ such that

$$|V : C_V(A)| \leq p|A|^2.$$

Any group A with this property is called an offending subgroup.

Now we can say what we will mean by a small module. These are quadratic modules, F–modules, $F+1$–modules and $2F+1$–modules.

Definition Let G be a group and V be a faithful $GF(p)G$-module. Then V is called quadratic if one of the following holds

(1) p is odd and there is some element $g \in G$ with $[V, g, g] = 1$.

(2) $p = 2$ and there is some fours group $A \leq G$ with $[V, A, A] = 1$.

For the remainder we will restrict ourself to the case $p = 2$. The following is joint work with U. Meierfrankenfeld. In the classification results for the F-modules quoted before the usual approach is to obtain lower bounds for the codimensions of centralizers of involutions in modules for G. Then using this information one either see that there are no F-modules or just a small list of possible modules. In contrast our approach uses the fact that F-modules are quadratic.

Theorem A [MeiStr1][MeiStr2] *Let V be an irreducible faithful GF(2)G -module, where $E(G)$ is sporadic, alternating or a Lie type group in odd characteristic which is not in even characteristic too. If V is quadratic then $E(G)$ is one of the following :*

1. $M_{12}, M_{22}, 3 \cdot M_{22}, M_{24}, J_2, Co_1, Co_2, 3 \cdot Suz$, the modules are known.

2. A_n and the module is the natural one or the spin module

3. $3 \cdot U_4(3)$ and $|V| = 2^{12}$.

This now can be used to classify the F–modules

Theorem B *Let V be an irreducible faithful GF(2)G -module, where $E(G)$ is sporadic, alternating or a Lie type group in odd characteristic which is not in even characteristic too. If V is an F–module, then $E(G) \cong A_n$ and V is the natural module or $n \leq 8$ and $|V| = 16$, or $E(G) \cong 3A_6$ and $|V| = 64$.*

So for quadratic and F–modules we are left with groups of Lie type over $GF(q)$, $q = 2^m$. Unfortunately there is no classification of quadratic modules. We have the following

Definition Let $G = G(q)$, $q = 2^m$, be a group of Lie type and V be a faithful module over $GF(2)$. Then V is called strong quadratic if there is a quadratic fours group which is not contained in any root subgroup but intersects a root subgroup nontrivially.

Theorem C [Str] *Let V be an irreducible faithful GF(2)G -module, where $G = G(q)$ is a group of Lie type, $q = 2^m$. If V is strong quadratic, then one of the following holds*

1. $G \cong (S)L(n,q), (S)U(n,q), Sp(2n,q), F_4(q)$ and $V \cong V(\lambda)$ for some fundamental weight λ.

2. $G \cong \Omega^{\pm}(2n, q)$ and V is the natural or a half spin module.

3. $G \cong E_6(q)$ and $V \cong V(\lambda_1)$ or $V(\lambda_6)$

4. $G \cong E_7(q)$ and $V \cong V(\lambda_7)$

5. $G \cong {}^2E_6(q)$ and $V \cong V(\lambda_4)$

6. $G \cong G_2(q)$ or ${}^3D_4(q)$ and V is the natural module.

Theorem D *Let V be an irreducible faithful $GF(2)G$ -module, where $E(G)/Z(E(G)) = G(q)$ is a group of Lie type, $q = 2^m$. If V is a F-module then one of the following holds*

1. $G(q) \cong L_n(q), Sp(2n,q), \Omega^{\pm}(2n,q)$ or $U_n(q)$ and V is the natural module or its dual.

2. $G(q) \cong L_n(q)$ and V is the exterior square of the natural or dual module

3. $G(q) \cong Sp(6,q)$ and V is the spin module

4. $G(q) \cong \Omega^+(8,q)$ or $\Omega^+(10,q)$ and V is a half spin module

5. $G(q) \cong G_2(q)$ and V is the natural module

The problem in the proof is that we do not know that F-modules are strong quadratic. We just know that they are quadratic. In what follows we will sketch the proof using the group $E_6(q)$ as an example.

We first collect some facts about modules about modules for our groups of Lie type, which are helpful for the classification of F-, $F+1$- and $2F+1$-modules.

(1) Let $1 \neq V$ be an irreducible module for $G(q)$ and P be a parabolic. Then $V_P = C_V(O_p(P))$ is an irreducible P-module. Further V is determined by the V_P.

(2) (Steinberg tensor product theorem) Let $G = G(q)$ be a group of Lie type and V be an irreducible module over $GF(q)$. Then

$$V = V_1^{\sigma_1} \otimes \cdots \otimes V_l^{\sigma_l}$$

where the V_i are basic irreducible $GF(q)G$–modules. Further distinct l–tuples $(M_1, \ldots M_l)$ and $(M_1', \ldots, M_l')$ give nonisomorphic $GF(q)G$–modules.

(3) If $V = X \otimes W$ is a $GF(q)$-module for G, an A acts quadratically on V, then $|A| \leq q$.

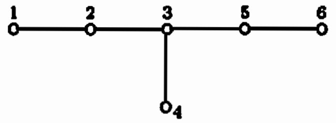
(4) If V is a F–module for $G(q)$ with offending subgroup A with $|A| \leq q$, then V is strong quadratic

(5) If A is a maximal α-offender, i.e. $|C_V(A)||A|^\alpha$ maximal, then also $\langle A, A^g \rangle$, $g \in G$ is a, maybe nonabelian, maximal α-offender.

(6) (Timmesfeld replacement) If there is a normal offender A, there is a normal offender B contained in A which acts quadratically.

(7) Let V be an F-module for G and V_1 be an invariant subspace. Then V_1 is a trivial subspace or V_1 is an F-module too.

Let now $G = E_6(q)$ and V be an irreducible F-module. The whole proof goes by induction on the Lie rank. So we will assume that the theorem holds for all groups of rank smaller then 6. First of all we may assume that V is defined over $GF(q)$. Next we will assume that V is not strong quadratic. Then by the facts (3) and (4) V is not a tensor product. So by fact (2) $V = V(\lambda)$, λ some weight. We will choose numbering of weights such that



We look at the maximal parabolic G_4 which is an extension of q^{1+20} by $GL_6(q)$.

By fact (4) we have $|A| > q$. If $A \leq O_2(G_4)$, then we have that $A \cap Z(O_2(G_4)) = 1$. Choose $a \in A^\sharp$. Set $C = C_{O_2(G_4)}(a)$. Then $|O_2(G_4) : C| = q$. Let $x \in O_2(G_4) \setminus C$, then there is $1 \neq b \in C_A(x)$. So

$$\langle a, b\rangle^x = \langle az, b\rangle, \text{ for some } 1 \neq z \in Z(O_2(G_4))$$

acts quadratically on V. But then $\langle z, b\rangle$ acts quadratically and so V is strong quadratic. So we have that there is no quadratic A in $O_2(G_4)$. Set $V_4 = C_V(O_2(G_4))$. By fact (7) V_4 is a F–module for $G_4/O_2(G_4)$. Hence by induction V_4 is either trivial of some $V(\lambda)$ for some fundamental weight λ. Now we may assume that $V_6 = C_V(O_2(G_6))$ is a nontrivial module. If $A \leq O_2(G_6))$ then $\langle A^{G_6}\rangle = O_2(G_6)$ is an offender. And so we get that $O_2(G_6)$ acts quadratically, and V is strong quadratic.
So we have that V_6 is an F–module. If $V_1 = C_V(O_2(G_1))$ is trivial, we get $V \cong V(\lambda_1)$ and we are done. So we may assume it is nontrivial. Again $A \not\leq O_2(G_1)$ and so it is an F–module and we see that $V \cong V(\lambda_6)$ or $V(\lambda_4)$.
Let $V = V(\lambda_4)$. Then V is the adjoint module and so $|V| = q^{78}$. Now by fact (5) $G = \langle A^g \mid g \in G\rangle$ is an offender too, and so $|V| > |G|$, a contradiction.
In case of $V(\lambda_1)$ and $V(\lambda_6)$ one has to investigate both modules very carefully, as they are $F + 1$-modules.

Next we turn to the $F + 1$- and $2F + 1$-modules. For this we change the definition of $F + 1$- and $2F + 1$–modules a little bit just for the case of $G(q)$.

Definition Let $G = G(q)$ and V be a faithful $GF(2)G$–module. Then V is called a $F + 1$- or $2F + 1$- for G if there is some elementary abelian p–subgroup A in G, $1 \neq A$ such that $|V : C_V(A)| \leq q|A|$ or $q|A|^2$, respectively. Any group A with this property is called an offending subgroup.

Theorem E *Let V be an irreducible faithful $GF(2)G$ -module, where G is a quasisimple group $G(q)$, $q = 2^m$. Suppose V is an $F + 1$-module but not an F–module. Then one of the following holds*

1. *$G(q) \cong Sp(8,q)$ and V is the spin module*
2. *$G(q) \cong U(3,q)$ and V is the natural module*
3. *$G(q) \cong Sz(q)$ and V is the natural module*
4. *$G(q) \cong E_6(q)$ and $V \cong V(\lambda_1)$ or $V(\lambda_6)$*
5. *$G(q) \cong G_2(q)$ and $V \cong V(\lambda_2)$*
6. *$G(q) \cong L_n(q^2)$ and $V \cong V(\lambda_1) \otimes V(\lambda_1)^\sigma$*

Theorem F *Let V be an irreducible faithful GF(2)G -module, where G is a quasisimple group $G(q)$, $q = 2^m$. Suppose V is an $2F+1$-module but not an $F+1$-module. Then one of the following holds*

1. *$G(q) \cong L_6(q)$ or $U_6(q)$ and $V \cong V(\lambda_3)$*
2. *$G(q) \cong Sp(2n,q)$ and $V \cong V(\lambda_2)$*
3. *$G(q) \cong Sp(10,q)$ and V is the spin module*
4. *$G(q) \cong \Omega^-(8,q)$, $\Omega^-(10,q)$ or $\Omega^+(12,q)$ and V is a half spin module*
5. *$G(q) \cong F_4(q)$ and $V \cong V(\lambda_1)$ or $V(\lambda_4)$*
6. *$G(q) \cong E_7(q)$ and $V \cong V(\lambda_7)$*
7. *$G(q) \cong Sp(4,q^2)$ and $V \cong V(\lambda_1) \otimes V(\lambda_1)^\sigma$*
8. *$G(q) \cong L_2(q^3)$ and $V \cong V(\lambda_1) \otimes V(\lambda_1)^\sigma \otimes V(\lambda_1)^{\sigma^2}$.*

There is a little but important difference between Theorem B and Theorem E or Theorem F. In the first case the offending subgroup is contained in AutG(q), while in the latter two cases it has to be contained in $G(q)$ itself. The extension of these results to Aut$G(q)$ is in progress.

As can be seen from the examples $F+1$-modules do not have to be quadratic. So we have to change our approach. For this we define a new class of modules

Definition Let $G = G(q)$, $q = 2^m$ be a group of Lie type and $P_1, \ldots, P_n$ the set of minimal parabolics containing a Sylow 2-subgroup. Let i be some natural number. A faithful $GF(2)G$-module is called an iC-module if there is some parabolic P_j such that $O'(P_j)$ has at most i nontrivial chief factors on V.

The relation between the iC-modules and our $F+1$- or $2F+1$-modules is as follows. Let V be an $F+1$- or $2F+1$-module and A be an offending subgroup. Let $x \in A^\sharp$. Then $|V : C_V(x)| \leq q|A|$ or $q|A|^2$. There is some P_j and some conjugate y of x with

$y \in P_j \setminus O_2(P_j)$. So on any nontrivial $O'(P_j)$ chief factor W, we have $|W : C_W(y)| \geq q$. Hence we see that $O'(P_j)$ has at most

$$\log_q(|A|) + 1 \text{ or } 2\log_q(|A|) + 1$$

nontrivial chief factors. So we have a iC-module for $i = \log_q(|A|) + 1$ or $2\log_q(|A|) + 1$.

If m is the q-rank of G then we would like to have a list of $(m+1)C-$ and $(2m+1)C-$ modules. So the first step of the proof is to get an overview over these modules.

Let $V = V(\lambda)$, $\lambda = \sum_{i \notin J} \lambda_i$, λ some dominant weight. Then W_J is the stabilizer of λ in the Weyl group W. Let

$$\Omega = \{v_\lambda^w \mid w \in W\}.$$

Then one can show that the number of nontrivial chief factors of P_i on $V(\lambda)$ is exactly the number of nontrivial orbits of w_i on Ω and so on W/W_J.

I just will give the formula if all roots are of the same length. Let Φ be the rootsystem and Φ_J be the roots just using the fundamental roots in J.

$$o_J = \frac{1}{2}|W/W_J|\left(1 - \frac{|\Phi_J|}{|\Phi|}\right)$$

Further if $J \subset J' \subseteq I = \{1, 2, \ldots, n\}$ we get

$$o_J \geq |W_{J'}/W_J| o_{J'}$$

Now we get for example

Proposition *Let W be of type A_l. Put $n = l + 1$ and $m = \frac{n^2}{4}$ if n is even and $m = \frac{n^2-1}{4}$ if n is odd. Suppose that $J \subset I$ with $o_J \leq 2m + 1$. Then J and o_J are as follows, where the last three column state for which values of n, $o_J \leq m, m+1$ and $2m+1$ respectively.*

weight	o_J	$o_J \leq m$	$o_J \leq m+1$	$o_J \leq 2m+1$
λ_1, λ_{n-1}	1	*all*	*all*	*all*
λ_2, λ_{n-2}	$n-2$	$4 \leq n$	$4 \leq n$	$4 \leq n$
λ_3, λ_{n-3}	$\binom{n-2}{2}$	$6 \leq n \leq 8$	$6 \leq n \leq 9$	$6 \leq n$
λ_4, λ_{n-4}	$\binom{n-2}{3}$	*never*	*never*	$8 \leq n \leq 9$
$\lambda_1 + \lambda_{n-1}$	$2n-3$	$4 \leq n$	$3 \leq n$	$3 \leq n$
$\lambda_1 + \lambda_2, \lambda_{n-2} + \lambda_{n-1}$	$2n-3$	$4 \leq n$	$3 \leq n$	$3 \leq n$
$\lambda_1 + \lambda_{n-2}, \lambda_2 + \lambda_{n-1}$	$\frac{(n-2)(3n-7)}{2}$	*never*	*never*	$n = 5$

For our example $E(q)$ we get

Proposition *Let W be of type E_6 and put $m = 16$. Suppose that $J \subset I$ with $o_J \leq 2m+1$. Then J, and o_J are as follows, where the last three column state whether $o_J \leq m, m+1$ and $2m+1$, respectively.*

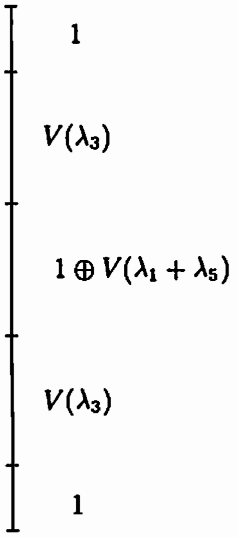
weight	o_J	$o_J \leq m$	$o_J \leq m+1$	$o_J \leq 2m+1$
$\lambda_1, \lambda_6,$	6	*Yes*	*Yes*	*Yes*
λ_4	21	*No*	*No*	*Yes*

Proof. We have $|W| = |O_6^-(2)| = 2^7 \cdot 3^4 \cdot 5$ and $|\Phi| = 72$.

Suppose first that $J = I \setminus \{k\}$ for some $k \in I$. If $k = 1$ or 6, then $|W_J| = |2^4 Sym(5)| = 2^7 \cdot 3 \cdot 5$ and $|\Phi_J| = 40$. Thus $o_J = 6$. If $k = 4$ then $|W_J| = |Sym(6)| = 2^4 \cdot 3^2 \cdot 5$ and $|\Phi_J| = 30$. Thus $o_J = 21$.

If $k = 2, 5$, then $|W_J| = |2\text{Sym}(5)|$ and $|\Phi_J| = 22$. This gives $o_J = 75$. If $k = 3$, then $|W_J| = |2\text{Sym}(3) \times \text{Sym}(3)|$ and $|\Phi_J| = 14$, so we get $o_J > 100$. Moreover clearly no case with $|I \setminus J| \geq 2$ is possible, besides maybe $V(\lambda_1 + \lambda_6)$. But there $|W_J / W_J'| \geq 5$, a contradiction.

So for $E_6(q)$ we just have to show that $V(\lambda_4)$ is not $2F+1$. This is the adjoint module and we easily get the structure as $G_4/O_2(G_4)$-module



Let $A \not\leq O_2(G_4)$. As $V(\lambda_1 + \lambda_5)$ is not $2F+1$ for $L_6(q)$, we get that the index of the centralizer of $A/A \cap O_2(G_4)$ in this module is at least $|A/A \cap O_2(G_4)|^2 q^2$.

As $V(\lambda_3)$ is not $F+1$, we get that the centralizer of $A/A \cap O_2(G_4)$ is at least $|A/A \cap O_2(G_4)|q^2$. Now we get that the index of the centralizer of A is at least

$$|A/A \cap O_2(G_4)|^3 q^4 |A \cap O_2(G_4)| q \leq q|A|^2$$

Hence we get

$$q|A|^2 \leq |A \cap O_2(G_1)|^{3.5}$$

So also in the case of $A \leq O_2(G_4)$ we get

$$|V : C_V(A \cap O_2(G_4))| \leq |A \cap O_2(G_4)|^{3.5}.$$

Now we can apply fact (5) with $\alpha = 3.5$. We get that $\langle (A \cap O_2(G_4))^{G_4} \rangle = O_2(G_4)$ is a 3.5-offender. So we have

$$q^{77} = |V : C_V(O_2(G_4))| \leq |O_2(G_4)|^{3.5} = q^{21 \cdot 3.5} \leq q^{74}$$

This contradiction proves the theorem in case of $G = E_6(q)$ and $V = V(\lambda)$.

Just tensor products are left. Here is the corresponding formula for tensor products.
Let $V_1 \otimes V_2$ be a tensor product of two G-modules V_1 and V_2 over $GF(q)$ and P_J be a parabolic with $L_J = O^{p'}(P_J)$. Suppose that L_J possesses on V_i l_i noncentral and k_i central chieffactors, $i = 1, 2$. Then L_J possesses on $V_1 \otimes V_2$ at least $l_1 l_2 + l_1 k_2 + l_2 k_1$ noncentral chieffactors.

Using this formula it is easy to see that in case of $G = E_6(q)$ no tensor products occur.

What is left is to investigate $F+1$- and $2F+1$-modules for alternating, sporadic and groups of Lie type in odd characteristic. Furthernore results on all this modules for p odd are also of interest.

References

[Asch] M. Aschbacher, $GF(2)$-representations of finite groups, Amer. J. Math. 104, 1982, 683 - 771

[Coop] B.Cooperstein, An enemies list for factorization theorems, Comm. Alg. 6, 1978, 1239 - 1288

[CoMa] B. Cooperstein, G. Mason, Some questions concerning the representations of Chevalley groups in characteristic two, preprint 1977

[Go] D. Gorenstein, Finite Groups, Harper & Row 1968

[McC] P. McClurg, The classification of F_1-pairs, PhD thesis, University of California at Santa Cruz, 1980

[MeiStrl] U. Meierfrankenfeld, G. Stroth, Quadratic $GF(2)$ - modules for sporadic simple groups and alternating groups, Comm. Algebra 18, 1990, 2099 - 2139

[MeiStr2] U. Meierfrankenfeld, G. Stroth, On quadratic $GF(2)$-modules for chevalley groups over fields of odd order, Arch. Math. 55, 1990, 105 - 110

[Stell] B. Stellmacher, A characteristic subgroup of Σ_4-free groups, Israel J. Math. 94, 1996, 367 - 379

[Str] G. Stroth, Srong quadratic modules, Israel J. Math. 79, 1992, 257 -279

A Problem of Distance-Regular Graphs and Related Topics (A Survey)

Hiroshi SUZUKI
Department of Mathematics
International Christian University
10-2, Osawa 3-chome, Mitaka-shi Tokyo 181, JAPAN

July 14, 1997

Abstract

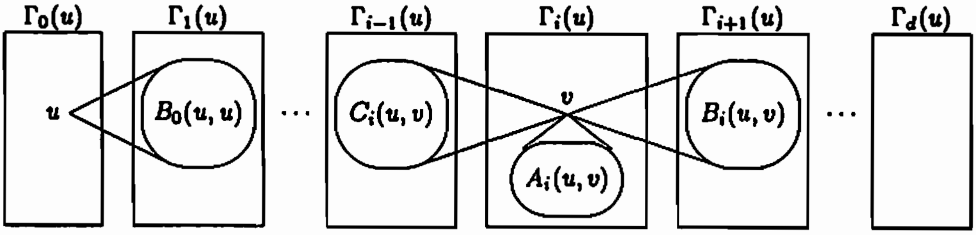
In this short survey we focus on the *absolute constant bound conjecture* on the geometric girths of distance-regular graphs and some related problems.

1 Introduction

We use the following notation throughout this survey. Most of them are standard, for the general theory closely related to this article, we refer the readers to two excellent monographs [1, 8].

- $\Gamma = (V\Gamma, E\Gamma)$: a connected graph with vertex set $V\Gamma$ and edge set $E\Gamma$.
- $\partial_\Gamma(\alpha, \beta)$: the distance between α and β.
- $\Gamma_i(\alpha) = \{\beta \in V\Gamma | \partial_\Gamma(\alpha, \beta) = i\}$, $\Gamma(\alpha) = \Gamma_1(\alpha)$.
- $k_\Gamma(\alpha) = k(\alpha) := |\Gamma(\alpha)|$: the valency at α.
- $d_\Gamma(\alpha) = d(\alpha) = \max\{\partial_\Gamma(\alpha, \beta) | \beta \in V\Gamma\}$: the local diameter at α.
- For α, $\beta \in V\Gamma$ with $\partial(\alpha, \beta) = i$, let

$$\begin{aligned} C(\alpha,\beta) &= C_i(\alpha,\beta) = \Gamma_{i-1}(\alpha) \cap \Gamma(\beta) \\ A(\alpha,\beta) &= A_i(\alpha,\beta) = \Gamma_i(\alpha) \cap \Gamma(\beta) \\ B(\alpha,\beta) &= B_i(\alpha,\beta) = \Gamma_{i+1}(\alpha) \cap \Gamma(\beta). \end{aligned}$$



We use lower case letters for the cardinalities of these sets.

$$c_i(\alpha,\beta) = |C_i(\alpha,\beta)|, \; b_i(\alpha,\beta) = |B_i(\alpha,\beta)|, \; a_i(\alpha,\beta) = |A_i(\alpha,\beta)|.$$

Definition 1.1 A connected graph $\Gamma = (V\Gamma, E\Gamma)$ is a *distance-regular graph* (DRG) if the numbers $c_i = c_i(\alpha,\beta)$, and $b_i = b_i(\alpha,\beta)$ depend only on i for each i.

Example 1 1. *n-gons.* A DRG of valency 2 is nothing but an ordinary polygon. We always assume the valency is at least 3 in the following.

2. *Strongly regular graphs.* A strongly regular graph is a DRG of diameter 2.

3. $J(v,d)$, *the Johnson graphs.* Let X be a set with $|X| = v$.

$$V\Gamma = \binom{X}{d}, \quad (\alpha,\beta) \in E\Gamma \Leftrightarrow |\alpha \cap \beta| = d - 1.$$

4. $H(d,q)$, *the Hamming graphs.* Let Q be a set with $|Q| = q$.

$$V\Gamma = Q^d, \quad (\alpha,\beta) \in E\Gamma \Leftrightarrow |\{i|\alpha_i \neq \beta_i\}| = 1.$$

5. *Dual polar graphs.* Let V be a vector space over a finite field with a non-degenerate (quadratic, simplectic or hermitian) form. Let $V\Gamma$ be the set of maximal totally isotropic subspaces of V. Let d be the dimension of the maximal totally isotropic subspaces of V in $V\Gamma$. For $\alpha, \beta \in V\Gamma$, define the adjacency by the condition $\dim(\alpha \cap \beta) = d - 1$. Then this graph becomes a DRG with diameter d.

6. $Her_q(r)$, *the Hermitian forms graphs.* Let $V = V(d, r^2)$ be a d-dimensional vector space over a finite field $GF(r^2)$ with r^2 elements. Let $V\Gamma$ be the set of all Hermitian forms on V. Then $V\Gamma$ can be regarded as the set of Hermitian matrices over $GF(r^2)$ (i.e., $\alpha^T = \bar{\alpha}$, where the bar denotes the image of the involutive Frobenius automorphism). Two forms f, $g \in V\Gamma$ are defined to be adjacent if $\operatorname{rank}(f - g) = 1$. Then this graph is a DRG and is called a Hermitian forms graph.

2 Absolute Constant Bound Conjecture

2.1 Bannai-Ito Conjecture and Related Problems

Conjecture 2.1 (Bannai-Ito [1]) *There are only finitely many DRGs with fixed valency k.*

For a connected regular graph $\Gamma = (V\Gamma, E\Gamma)$ of valency k and diameter d, it is easy to see that the size of Γ, i.e., the cardinality of $V\Gamma$, is bounded by a function of k and d, say $|V\Gamma| \leq 3(k-1)^d$. Hence the conjecture above says that the diameter of a DRG can be bounded if the valency is fixed.

The following lemma is easily verified.

Lemma 2.1 *Let Γ be a DRG.*

(1) *For α, $\beta \in V\Gamma$ with $\partial(\alpha,\beta) = i$, the numbers $p^i_{j,l} = |\Gamma_j(\alpha) \cap \Gamma_l(\beta)|$ do not depend on the choices of α and β. In particular, $k_i := p^0_{i,i} = |\Gamma_i(\alpha)|$, $k = k_1 = k(\alpha)$, and $d = d(\Gamma) := d(\alpha)$ do not depend on the choice of α.*

(2) $1 = c_1 \leq c_2 \leq \cdots \leq c_d \leq k$, $k = b_0 > b_1 \geq \cdots \geq b_{d-1} \geq 1$ *and* $k = c_i + a_i + b_i$. *In particular,*

$$k - 2 \geq b_1 - c_1 \geq b_2 - c_2 \geq \cdots \geq b_{d-1} - c_{d-1} \geq -(k-2).$$

The following is called the intersection array of Γ and denoted by $\iota(\Gamma)$.

$$\left\{\begin{array}{c} c_i \\ a_i \\ b_i \end{array}\right\} = \left\{\begin{array}{cccccccccccccc} * & 1 & \cdots & 1 & c' & \cdots & c' & \cdots & c'' & \cdots & c'' & \cdots & c_d \\ 0 & a & \cdots & a & a' & \cdots & a' & \cdots & a'' & \cdots & a'' & \cdots & a_d \\ k & b & \cdots & b & b' & \cdots & b' & \cdots & b'' & \cdots & b'' & \cdots & * \end{array}\right\}$$

$$l(c,a,b) = |\{i|(c_i,a_i,b_i) = (c,a,b)\}|,\ r = r(\Gamma) = l(c_1,a_1,b_1).$$

The number $r(\Gamma)$ is a key, which is about the half of the geometric girth. (We will define the geometric girth later.)

Apart from the first and the last columns there are at most $2k-3$ different columns in $\iota(\Gamma)$ by Lemma 2.1 (2). The following theorem gives a start point of what it follows.

Theorem 2.2 (A.A.Ivanov [25]) *Let Γ be a DRG. Then the following hold.*

$$(c_s,a_s,b_s) \neq (c_{s+1},a_{s+1},b_{s+1}) \Longrightarrow l(c_{s+1},a_{s+1},b_{s+1}) \leq s+1.$$

Moreover, $d(\Gamma) \leq 2^{2k-4}(r(\Gamma)+1)$.

The theorem above asserts that the size is bounded by a function of k and $r(\Gamma)$ if Γ is a DRG. In other words, there are only finitely many DRGs with fixed valency k and fixed $r(\Gamma)$.

Using the results above, E. Bannai and T. Ito obtained many results concerning Conjecture 2.1 in 80's, using so-called eigenvalue techniques which uses the integrality condition of multiplicities of eigenvalues of graphs. See [2, 3, 4, 5].

Conjecture 2.2 (A.V.Ivanov [26]) (1) $l(c,a,b) \leq r(\Gamma)+1$.

(2) $d(\Gamma) \leq 2(k-2)(r+1)$.

It is easy to see that (2) follows from (1). A.V.Ivanov proved (1) in various cases. The following result is essentially due to P. Terwilliger [31].

Theorem 2.3 *Let Γ be a DRG with $r = r(\Gamma) \geq 2$. If $c_{r+1} > 1$, then $b_i > b_{i+r}$, and $c_i < c_{i+r}$ for any $i = 0,1,\ldots,d-r$. In particular, $l(c,a,b) \leq r(\Gamma)$.*

A. Hiraki and J. Koolen proved that $d(\Gamma)$ is bounded by $C \cdot k^4 \cdot r$. See an article of Hiraki in this proceedings. Combining other deep results of Hiraki, it is easy to see that $d(\Gamma)$ can now be bounded by $C \cdot k^2 \cdot r$ with one very special remaining case. But there seems to be some gap to have a linear bound yet.

2.2 Absolute Constant Bound Conjecture

In view of Theorem 2.2, or the result of Hiraki and Koolen above, it suffices to give an upper bound of $r(\Gamma)$ by a function of the valency k in order to prove Conjecture 2.1. However, for all known examples $r(\Gamma) \leq 5$. If Γ is primitive and $d(\Gamma) > r(\Gamma)+1$ then $r(\Gamma) \leq 2$ with only one exception, i.e., the Biggs-Smith Graph of valency 3. Note that the colinearity graph of a generalized polygon satisfies $d(\Gamma) = r(\Gamma)+1$. So it is natural to expect much stronger bound for this $r(\Gamma)$, the absolute constant bound of the geometric girth of Γ.

Conjecture 2.3 *There is a constant R such that $r(\Gamma) \leq R$ for all DRGs Γ.*

We strongly believe that this is the right conjecture to investigate. If we could have a reasonably small bound R, we may be able to proceed to the classification of DRGs.

To close this section, we make two remarks. It is now a classical result that there are only finitely many *distance-transitive graphs* with a fixed valency, i.e., Bannai-Ito conjecture holds if Γ is distance-transitive [33]. But even we assume the distance-transitivity, the absolute constant bound conjecture above is still open. Distance-regular graphs with Q-polynomial property are well studied by P. Terwilliger and his students. These graphs satisfy $r(\Gamma) \leq 2$, and the only such graphs with $c_2 = 1$ of diameter at least 3 are either bipartite or generalized Hexagons of order (q, q^3).

3 Incidence Graphs

3.1 Distance-Regular Graphs of Order (s,t) and its Incidence Graph

If $r(\Gamma) \geq 2$, $c_2 = 1$ and there is no induced subgraph isomorphic to $K_{2,1,1}$. So every edge is contained in a unique maximal clique of size $a_1 + 2$. Thus $\Gamma(\alpha) \simeq (t+1)\cdot K_s$, where $s = a_1 + 1$ and $t + 1 = k/s$. In this case, we can define geometric girth $gg(\Gamma)$, which is the length of a shortest circuit without any triangles. Let $r = r(\Gamma)$. Then $gg(\Gamma) = 2r + 2$ if $c_{r+1} > 1$ and $gg(\Gamma) = 2r + 3$ if $c_{r+1} = 1$. This is actually the girth of the collinearity graph of the partial linear space with the point set $V\Gamma$ and the set of all maximal cliques as the set of (singular) lines. Taking this connection to a geometric structure in mind, we define the following terminologies.

Definition 3.1 A DRG Γ is said to be of *order* (s,t), if $\Gamma(\alpha) \simeq (t+1)\cdot K_s$ for every vertex $\alpha \in V\Gamma$. The *incidence graph* $\tilde{\Gamma}$ of a DRG Γ of order (s,t) is a bipartite graph with a bipartition $V\tilde{\Gamma} = P \cup L$ with $P = V\Gamma$, $L = L\Gamma :=$ the set of maximal cliques (of size $s+1$), where the adjacency $\alpha \sim x$ is defined by $\alpha \in x$ when $\alpha \in P$, $x \in L$.

A triangle-free DRG, i.e., a DRG with $a_1 = 0$ is of order $(1, k-1)$. The Hamming graph $H(d,q)$ is a DRG of order $(s,t) = (q-1, d-1)$. The dual polar graphs are of order $(s,t) = (q^e, \binom{d}{1}_q - 1)$ for suitable e depending on each underlying space. So in these cases t is closely related to the dimension of the underlying space. Hence the first subproblem to consider the absolute bound conjecture is the following.

Problem 1 Is there a constant $R(t)$ depending only on t such that $r(\Gamma) \leq R(t)$ for all DRGs Γ of order (s,t)? Are there only finitely many DRGs Γ of order (s,t) for a fixed t?

3.2 Distance-Regular Graphs of Order (s,t) with small t

When $a_1 = s - 1 = 0$, $t = k - 1$. As for Problem 1, $R(1)$ is known to be 5 ([8, Theorem 4.2.16, Proposition 4.3.4]), and $R(2)$ is as follows. Note that DRGs of order $(1,2)$ are nothing but cubic DRGs. For the references see [24, 6, 3, 23, 35], also [29].

Theorem 3.1 *Let Γ be a DRG of order $(s,2)$. Then one of the following holds.*

(1) *$s = 1$ and Γ is isomorphic to one of the 13 cubic DRGs.*

(2) *$s = 2$ and Γ is isomorphic to one of the 5 DRGs.*

(3) *$s > 2$ and $d(\Gamma) \leq r + 2$ (≤ 41).*

(4) *$s > 2$ and the incidence graph $\tilde{\Gamma}$ is DBR.*

Hence except the case (4), $R(2)$ is bounded.

As for the case $t = 3$, not much is known. The DRGs of order $(1,3)$ is the one with valency 4. In late 80's Bannai and Ito proved that the diameter of DRGs of valency 4 is bounded, but the complete classification was not finished at that time.

Recently, A.E.Brouwer and J. Koolen have succeeded in completing the classification of DRGs of valency 4 by use of computer by showing that all these graphs are among 17 known DRGs. They also used some improvements of the arguments of Bannai and Ito. J. Koolen is now improving Bannai-Ito's arguments on the multiplicities of eigenvalues of DRGs with fixed valency and obtained several good results. See the article of J. Koolen in this proceedings.

From the experience of the study above, we make the following remarks.

- There are four different cases.

  1. $s = 1$, i.e., $a_1 = 0$. (The case that singular lines are thin.) Many exceptional cases.
  2. $s < t$, difficult but much easier than the case $s = 1$.
  3. $s = t$, the bipartite half of bipartite DRGs appear.
  4. $s > t$, the induced graphs $C(x,y), A(x,y)$ and $B(x,y)$ have extra regularity.

- Technical matter.

  1. 'Circuit Chasing' argument, which is similar to the 'fusion argument' in finite group theory is very useful. (But it is still an argument or technique.)
  2. The study of the structure of incidence graph and its regularity is essential.
  3. If the diameter $d(\Gamma)$ is not large relative to $r(\Gamma)$, the bound we obtain by eigenvalue technique becomes very small.

3.3 WDSRGs, DSRGs, DBRGs and RNPs

We first discuss the regularity of incidence graphs. For the references of the results in this subsection, see [29].

Definition 3.2 A connected bipartite graph $\tilde{\Gamma}$ with a bipartition $P \cup L$ is said to be *distance-semiregular* (DSR) (on P) if $\tilde{c}_i = c_i(\alpha,\beta)$ and $\tilde{b}_i = b_i(\alpha,\beta)$ do not depend on α and β provided $\alpha \in P$ and $\beta \in V\tilde{\Gamma} = P \cup L$, and it is *distance-biregular* (DBR), if it is DSR on both P and L.

Definition 3.3 A connected bipartite graph $\tilde{\Gamma}$ with a bipartition $P \cup L$ is said to be *weakly distance-semiregular* (WDSR) (on P), if the following condition is satisfied:

(1) It is biregular, i.e., $b_0(\alpha,\alpha)$ depends only on the part α belongs to.

(2) $\tilde{c}_i = c_i(\alpha,\beta)$ does not depend on α and β provided $\alpha \in P$ and either $\beta \in P$ or $b_i(\alpha,\beta) \neq 0$.

$$\begin{matrix}\text{RNP}\\ \text{DBR}\end{matrix} \Rightarrow \text{DSR} \Rightarrow \text{WDSR}.$$

The incidence graph of a regular near polygon (RNP) is nothing but a DSRG with $\tilde{c}_{2i-1} = 1$ for every i. The incidence graph of a RNP is DBR only if it is bipartite distance-regular.

Lemma 3.2 *Let Γ be a DRG of order (s,t) and let $\tilde{\Gamma}$ be its incidence graph. Let α, β be vertices of Γ at distance i. Let $\tilde{c}_j$'s be the parameters of $\tilde{\Gamma}$.*

(1) *$\tilde{\Gamma}$ is WDSR if and only if $C_i(\alpha,\beta)$ is a disjoint union of $\tilde{c}_{2i}$ cliques of equal size for every i.*

(2) *$\tilde{\Gamma}$ is DSR if and only if $\tilde{\Gamma}$ is WDSR and there is no maximal clique that is completely contained in $\Gamma_i(\alpha)$ for some α and i.*

(3) *$\tilde{\Gamma}$ is the incidence graph of a RNP if and only if $\tilde{\Gamma}$ is WDSR and that $C_i(\alpha,\beta)$ is a clique (i.e., the induced graph has no edge) for every i.*

Example 2 $H(d,q)$ is a DRG of order $(q-1,d-1)$ and the parameters of the incidence graph can be given as follows. Here α, $\beta \in V\Gamma$ and x, $\in L\Gamma$.

$$\begin{bmatrix} \tilde{c}_{2i-1}(\alpha,x) & \tilde{c}_{2i}(\alpha,\beta) \\ \tilde{b}_{2i-1}(\alpha,x) & \tilde{b}_{2i}(\alpha,\beta) \end{bmatrix} = \begin{bmatrix} 1 & i \\ q-1 & d-i \end{bmatrix}, \begin{bmatrix} \tilde{c}_{2i-1}(x,\alpha) & \tilde{c}_{2i}(x,y) \\ \tilde{b}_{2i-1}(x,\alpha) & \tilde{b}_{2i}(x,y) \end{bmatrix} = \begin{bmatrix} i-1 & 1,q \\ d-i+1 & q-1,0 \end{bmatrix}$$

Hence the incidence graph is DSR and the incidence graph of a RNP on $V\Gamma$ but it is not DSR on $L\Gamma$.

Problem 2 Find the condition for the vertex-clique incidence graph $\tilde{\Gamma}$ of a DRG Γ of order (s,t) to be DBR, DSR, or WDSR. Is the incidence graph of a DRG of order (s,t) always WDSR?

In most known examples with $s > 1$, $\tilde{\Gamma}$ is either DBR or the incidence graph of a RNP, in particular, it is DSR. The hermitian forms graphs are the only examples with unbounded diameter such that $\tilde{\Gamma}$ is not DSR, but it is WDSR. Note that if $s = 1$, $\tilde{\Gamma}$ is always WDSR but it is DSR only if $a_1 = \cdots = a_{d-1} = 0$.

Theorem 3.3 *Let Γ be a DRG of order (s,t) and let $\tilde{\Gamma}$ be its incidence graph. Then every eigenvalue of Γ is at least $-t-1$. If Γ has an eigenvalue $-t-1$, then $\tilde{\Gamma}$ is a DSRG with $d_{\tilde{\Gamma}}(\alpha)$ even for every $\alpha \in P$. Moreover, if $s > t$, Γ always has an eigenvalue $-t-1$.*

The following theorem is obtained by an application of a result of Haemers.

Theorem 3.4 *Let Γ be a DRG of order (s,t) of diameter $d = d(\Gamma) > 1$, and $\tilde{\Gamma}$ be the incidence graph of Γ. For each vertex $\alpha \in V\Gamma$, let*

$$\bar{c}_j(\alpha) = \frac{1}{|\bar{\Gamma}_j(\alpha)|} \sum_{\beta \in \bar{\Gamma}_j(\alpha)} c_j(\alpha,\beta),\ \bar{b}_j(\alpha) = \frac{1}{|\bar{\Gamma}_j(\alpha)|} \sum_{\beta \in \bar{\Gamma}_j(\alpha)} b_j(\alpha,\beta).$$

If, for each vertex $\alpha \in V\Gamma$ and $1 \le i \le d$, $c_i = \tilde{c}_{2i-1}(\alpha)\bar{c}_{2i}(\alpha)$, and $b_{i-1} = \bar{b}_{2i-2}(\alpha)\bar{b}_{2i-1}(\alpha)$, then $\tilde{\Gamma}$ is DSR.

Problem 3 Consider conjectures and problems when the vertex-clique incidence graph $\tilde{\Gamma}$ is DSR, DBR or the incidence graph of a RNP.

Proposition 3.5 *Let Γ be a DRG of order (s,t). Suppose that the incidence graph $\tilde{\Gamma}$ of Γ is DSR, then*

$$l(c,a,b) \le r+1, \text{ and } d(\Gamma) \le t(r+1).$$

Compare with Theorem 2.2.

4 Subgraph Theorems and Circuit Chasing Technique

4.1 Strongly Closed Subgraphs and Geodetically Closed Subgraphs

Let $S(x,y) = \{y\} \cup C(x,y) \cup A(x,y)$.

Definition 4.1 Let Y be a subset of $V\Gamma$.

1. Y is said to be *geodetically closed* if Y satisfies one of the following equivalent conditions.
   (a) $C(x,y) \subset Y$ for all $x,y \in Y$.
   (b) $\{z \mid \partial(x,z) + \partial(z,y) = \partial(x,y)\} \subset Y$ for all $x,y \in Y$.
2. Y is said to be *strongly closed* if Y satisfies one of the following equivalent conditions.
   (a) $S(x,y) = \{y\} \cup C(x,y) \cup A(x,y) \subset Y$ for all $x,y \in Y$.
   (b) $\{z \mid \partial(x,z) + \partial(z,y) \leq \partial(x,y) + 1\} \subset Y$ for all $x,y \in Y$.
3. The (vertex) induced subgraph on Y is said to be a geodetically closed subgraph [or strongly closed subgraph] if Y is geodetically closed [or strongly closed respectively].

Clearly, a strongly closed subgraph is geodetically closed. Most of the known DRGs have geodetically closed subgraphs and many have strongly closed subgraphs. For example in the case of dual polar graphs, strongly closed subgraphs correspond to the subspaces. So if we can show the existence of these subgraphs, the structure is very much restricted. Moreover, if it has a sequence of subgraphs, we have chance to construct geometry. Most of the strongly closed subgraphs in DRGs are distance-regular, but there are some exceptions [28].

Recently, C-W Weng [34], A. Hiraki [19] and the author [30] constructed a sequence of subgraphs if $r(\Gamma) = 1$ and Γ does not have a certain configuration called parallelogram. But there is still a gap to construct geometry for classification.

In the next subsection we focus on the construction of a subgraph to bound $r(\Gamma)$.

4.2 Hiraki's Results on the Existence of Subgraphs

A DRG Γ with $d(\Gamma) = r(\Gamma) + 1$ is said to be a generalized Moore graph. It is known that the diameter of a generalized Moore graph is at most 13 by the results of Fuglister and others [8, 10, 11]. So if we can construct a subgraph isomorphic to a generalized Moore graph, then we have a bound of $r(\Gamma)$. The following results of A. Hiraki are in this direction. See also [27].

Definition 4.2 Let Γ be a DRG with $r = r(\Gamma)$.

1. A four vertex configuration $(x,z;x',z')$ is said to be a *root* if
$$\partial(x,z) = \partial(x',z') = r+1,\ x' \in S(z,x),\ z' \in S(x,z).$$
2. A three vertex configuration $(x,y;z)$ is said to be a *conron* if there are sequences of vertices $(x_0,x_1,\ldots,x_t)$, $(y_0,y_1,\ldots,y_t)$ and $(z_0,z_1,\ldots,z_t)$ satisfying the following:
   (a) $x = x_0, y = y_0, z = z_0$ and $\partial(x_t,y_t) \leq 1$.
   (b) $(x_i,z_i;x_{i+1},z_{i+1})$ and $(y_i,z_i;y_{i+1},y_{i+1})$ are roots for $i = 0,1,\ldots,t-1$.
3. Γ is said to satisfy *CR condition* if for every conron $(x,y;z)$, we have $S(x,z) = S(y,z)$.

Observe that if $\ll x,z \gg$ denotes the smallest strongly closed subgraph containing the vertices x,z, then $\ll x,z \gg = \ll x',z' \gg$ for every root $(x,z;x',z')$. Hence by induction, it is easy to see that $\ll x,z \gg = \ll x,y \gg$ for every conron $(x,y;z)$. In particular, if the diameter of $\ll x,z \gg$ is $r+1$, then CR condition $S(x,z) = S(y,z)$ must be satisfied. The first interesting result of A. Hiraki states that this CR condition is also sufficient.

Theorem 4.1 ([21]) *Let Γ be a DRG of order (s,t) with $r = r(\Gamma)$. Then the following are equivalent.*

(*i*) *Γ satisfies CR condition.*

(*ii*) *For vertices $x,y \in V\Gamma$ with $\partial(x,y) = r+1$, there is a strongly closed subgraph Δ containing x,y of diameter $r+1$, and Δ is DR.*

This theorem is very helpful when we define a candidate of a strongly closed subgraph containing the vertices x,z of distance $r+1$. It is not difficult to see that the strongly closed subgraph Δ containing x,z has the following shape.

$$V\Delta = \{u \mid \partial(x,u) + \partial(u,y) = r+1,\ y \in \Phi\},$$

where Φ is a union of some connected components of $\Gamma_{r+1}(x)$. If Γ satisfies the CR condition, we see by investigation that

$$\Phi = \{y \mid (y,z;x) \text{ is a conron}\}.$$

Hence in order to construct a strongly closed subgraph, the step is to show the CR condition. Hiraki showed this condition in various cases by circuit chasing technique, assuming the parametrical conditions for c_i's and b_i's for i's up to $2r+1$ or $2r+2$. The following are the some of his results.

Corollary 4.2 ([17, 18, 21]) *Let Γ be a DRG with $r = r(\Gamma)$. If $c_{2r+1} = 1$, then there exists a collinearity graph of a Moore geometry of valency $a_{r+1}+1$ and diameter $r+1$ as a subgraph of Γ. In particular, either $r = 1$ or $a_1 = a_{r+1} - 1 = 0$.*

Corollary 4.3 ([20, 21]) *Let Γ be a point graph of a RNP with $r = r(\Gamma)$. If $d \geq 2 \cdot r + 1$ and $a_1 > 0$, then there exists a strongly closed subgraph, which is a generalized polygon of diameter $r+1$. In particular, $r \leq 3$.*

Thus the above corollary show that if Γ is a point graph of a RNP with $r = r(\Gamma)$ of order (s,t), then one of the following holds.

1. $r \leq 3$.
2. $s = 1$, i.e., $a_1 = 0$.
3. $d \leq 2 \cdot r(\Gamma)$.

Hence if we restrict our attention to RNPs with $s > 1$, then we may assume $d \leq 2 \cdot r(\Gamma)$ to prove the absolute constant bound conjecture.

A. Hiraki also treated the case when the diameter of the subgraph is larger than $r+1$ in [22].

Can we generalize Hiraki's result to geodetically closed subgraphs containing $A(x,y)$ for all edge $x \sim y$?

Interpret Hiraki's result to subgraphs in the incidence graph to apply to wider class such as DSRGs.

Problem 4 Study the existence conditions of geodetically closed subgraphs of DRGs of order (s,t). In particular, is it possible to construct such a subgraph by assuming the diameter is large in compared with $r(G)$, when the incidence graph of Δ is DSRG or WDSRG?

5 Algebraic Arguments

The following is a result of Feit–Higman, Bannai-Ito, Damerell, Fuglister and others. This class contains, generalized polygons, the incidence graphs of Moore geometries. See [8].

Let Γ be a DRG of order (s,t).

$$d(\Gamma) \leq r(\Gamma) + 1 \Rightarrow r(\Gamma) \leq 12.$$

Problem 5 Find a combinatorial proof of the above result.

It is possible to give a constant bound of $r(\Gamma)$ when $d(\Gamma) \leq r(\Gamma) + 3$. There is still some gap, but the author believes that it is possible to prove the following:

If $d(\Gamma) \leq r(\Gamma) + C$, then $r(\Gamma)$ is bounded by a function of C.

Problem 6 Let Γ be a DRG with $d(\Gamma) \leq C \cdot r(\Gamma)$. Give a bound of $r(G)$ as a function of C.

For example if Γ is a point graph of a RNP with $s > 1$, we need to consider the case $C = 2$. So start with the case $C = 2$.

Problem 7 Let Γ be a DRG with $d(\Gamma) \leq 2 \cdot r(\Gamma)$. Give an absolute bound of $r(\Gamma)$.

In the following we propose some typical array to consider.

$$\left\{\begin{array}{cccccccccc} * & 1 & \cdots & 1 & 1 & 4 & \cdots & 4 & 4 & c_d \\ 0 & s-1 & \cdots & s-1 & s+1 & 2s-3 & \cdots & 2s-3 & a & a_d \\ 3s & 2s & \cdots & 2s & 2(s-1) & s-1 & \cdots & s-1 & b & * \end{array}\right\},$$

where $(b, c_d) = (s-1, 6)$, or $(s-2, 9)$. These are the remaining cases of DRGs of order $(s,2)$ such that no bound of $r(\Gamma)$ is known.

$$\left\{\begin{array}{cccccccc} * & 1 & \cdots & 1 & c & \cdots & c & k \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ k & k-1 & \cdots & k-1 & k-c & \cdots & k-c & * \end{array}\right\}$$

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin-Cummings, California, 1984.

[2] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, Graphs and Combin. 3 (1987), 95-109.

[3] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, II, Graphs and Combin. 4 (1988), 219-228.

[4] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, III, J. Algebra 107 (1987), 43-52.

[5] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, IV, Europ. J. Combin. 10 (1989), 137-148.

[6] N. L. Biggs, A. G. Boshier, and J. Shawe-Taylor, Cubic distance-regular graphs, J. London Math. Soc. (2) 33 (1986), 385–394.

[7] A. Boshier and K. Nomura, A remark on the intersection arrays of distance-regular graphs, J. Combin. Th. (B) 44 (1988), 147-153.

[8] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer Verlag, Berlin, Heidelberg, 1989.

[9] B. V. C. Collins, The girth of a thin distance-regular graph, preprint.

[10] F. Fuglister, On generalized Moore geometries, I, Discrete Math. 67 (1987), 249-258.

[11] F. Fuglister, On generalized Moore geometries, II, Discrete Math. 67 (1987), 259-269.

[12] W. H. Haemers, Distance regularity and the spectrum of graphs, Report FEW 582 Dept. of Economics, Univ. of Tilburg (1992).

[13] A. Hiraki, An improvement of the Boshier-Nomura bound, J. Combin. Th. (B) 61 (1994), 1–4.

[14] A. Hiraki, A circuit chasing technique in distance-regular graphs with triangles, Europ. J. Combin 14 (1993), 413–420.

[15] A. Hiraki, A constant bound for the number of columns $(1, k-2, 1)$ in the intersection array of distance-regular graph, preprint.

[16] A. Hiraki, Circuit chasing technique for a distance-regular graph with $c_{2r+1} = 1$, Kyushu J. Math. 49 (1995), 197–219.

[17] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, I, Europ. J. Combin 16 (1995), 589–602.

[18] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, II, Europ. J. Combin 16 (1995), 603–615.

[19] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, III, Europ. J. Combin 17 (1996), 629–636.

[20] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, IV, to appear in Europ. J. Combin.

[21] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, V, to appear in Europ. J. Combin.

[22] A. Hiraki, Distance-Regular Subgraphs of a Distance-Regular Graph, VI, preprint.

[23] A. Hiraki, K. Nomura and H. Suzuki, Distance-regular graphs of valency 6 and $a_1 = 1$, preprint.

[24] T. Ito, Bipartite distance-regular graphs of valency 3, Linear Algebra Appl. 46 (1982), 195-213.

[25] A. A. Ivanov, Bounding the diameter of a distance regular graph, Soviet Math. Dokl. 28 (1983), 149–152.

[26] A. V. Ivanov, Problem, ***Algebraic, Extremal and Metric Combinatorics, 1986***, Cambridge Univ. Press, Cambridge, 1988, 240–241.

[27] J. H. Koolen, On subgraphs in distance-regular graphs, J. Alg. Combin. 1 (1992), 353–362.

[28] H. Suzuki, On strongly closed subgraphs of highly regular graphs, Europ. J. Combin. 16 (1995), 197–220.

[29] H. Suzuki, Distance Semi-Regular Graphs, Algebraic Colloquium, 2 (1995), 315–328.

[30] H. Suzuki, Strongly closed subgraphs of a distance-regular graph with geometric girth five, Kyushu J. Math. 50 (1996), 371–384.

[31] P. Terwilliger, Distance-regular graphs and (s, c, a, k)-graphs, J. of Combin. Th. (B) 34 (1983), 151–164.

[32] P. Terwilliger, Distance-regular graphs with girth 3 or 4:I, J. of Combin. Th. (B) 39 (1985), 265–281.

[33] R. Weiss, Distance-transitive graphs and generalized polygons, Arch. Math. 45 (1985), 186–192.

[34] C-W. Weng, Weal-geodetically closed subgraphs in distance-regular graphs, preprint.

[35] N. Yamazaki, Distance-regular graphs with $\Gamma(x) \simeq 3 \cdot K_{a+1}$, European J. Combin. 16 (1995), 525–535.

ON THE PRIME GRAPH OF A FINITE SIMPLE GROUPS AN APPLICATION OF THE METHOD OF FEIT-THOMPSON-BENDER-GLAUBERMAN

MICHIO SUZUKI

Department of Mathematics
University of Illinois at Urbana-Champaign

Introduction The theorem alluded in the subtitle is the Odd Order Theorem of Feit-Thompson [FT] which states that all finite groups of odd order are solvable. For the remarkable proof, they invented a revolutionary new method which was influential to the development of finite group theory in the last 30 odd years. Recently, Bender and Glauberman [BG] has published a highly polished proof covering the group theoretical portion of the proof of the Odd Order Theorem.

By design, their proof is by contradiction. From the start they work on the hypothetical minimal simple group of odd order and study its properties. Thus, all the wonderful intermediate results are properties of the hypothetical group and hence they may be vacuous. One of the goals of this note is to show that this is not so; their method do give positive results and all the intermediate results are properties of some real groups.

We consider the prime graph $\Gamma(G)$ of a finite group G. This is the graph defined as follows. The set of vertices of $\Gamma(G)$ is the set $\pi(G)$ of the primes dividing the order $|G|$ of G. If $p, q \in \pi(G)$, we join p and q by an edge in $\Gamma(G)$ if and only if $p \neq q$ and G has an element of order pq.

The classification of finite simple groups has several interesting consequences on the prime graph of a finite group. The following is one of them.

Theorem A. *Let Δ be a connected component of the prime graph $\Gamma(G)$ of a finite group G and let ϖ be the set of primes in Δ. Assume that $\Delta \neq \Gamma(G)$ and $2 \notin \varpi$. Then, Δ is a clique.*

Usually, we identify Δ with ϖ and abuse the terms saying ϖ is a connected component of the graph $\Gamma(G)$. Theorem A has not been stated in literature in this form. But, the works of Gruenberg and Kegel [GK] and Williams [W] together with properties of Frobenius groups yield Theorem A. The classification of finite simple groups is used in two separate places of its proof. The first is in the proof of the following theorem.

Theorem B. *Theorem A holds for a finite simple group.*

The second use of the classification is to prove the following lemma.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Lemma. *Let G be a finite simple group. Then, $\pi(\operatorname{Out} G)$ is contained in the connected component of the prime graph $\Gamma(G)$ that includes the prime 2.*

This is fairly easy to check because $\operatorname{Out} G$ for a simple group G is not too complicated. The checking of Theorem B is more complex.

The purpose of this work is to show that the method of Feit, Thompson, Bender, and Glauberman can be adapted to give a proof of Theorem B without using the classification of finite simple groups.

Actually, Williams [W] has checked the following result for a finite simple group.

Theorem C. *Let Δ be a connected component of the prime graph $\Gamma(G)$ of a finite simple group G. Let ϖ be the set of primes in Δ. Assume that $\Delta \neq \Gamma(G)$ and $2 \notin \varpi$. Then, G contains a nilpotent Hall ϖ-subgroup H that is isolated in G.*

A subgroup H of any group G is called *isolated* in G if $1 \neq H \neq G$ and for every element $x \in H^\sharp$, we have

$$C_G(x) \subseteq H.$$

Theorem B is weaker than Theorem C which may be considered a local version of the Odd Order Theorem. It would be nice if our method would be able to prove Theorem C.

Originally, Gruenberg and Roggenkamp [GR] are led to study the prime graph, in particular its connectivity, through their work on the decomposition of the augmentation ideal of the integral group ring of a finite group. Specifically they considered the following three conditions on a finite group G.

(1) G has an isolated subgroup.
(2) The augmentation ideal decomposes as a right $\mathbb{Z}G$-module.
(3) The prime graph $\Gamma(G)$ is not connected.

Gruenberg and Roggenkamp [GR] proved that (1) ⇒ (2) ⇒ (3). Using Theorem C, Williams [W] was able to prove that (3) ⇒ (1). If ϖ is a connected component of the prime graph $\Gamma(G)$ such that $2 \notin \varpi$ and $\varpi \neq \Gamma(G)$, it is not necessarily true that G has a Hall ϖ-subgroup that is isolated.

1. The Beginning of the Proof Let G be a finite group and let $\varpi \subseteq \pi(G)$ be the set of primes of a connected component Δ of the prime graph $\Gamma(G)$. Assume that

$$\varpi \neq \pi(G) \quad \text{and} \quad 2 \notin \varpi.$$

These conditions and notation are used throughout this note. The starting point of the proof is the following proposition.

Proposition 1. *Let P be a nonidentity ϖ-subgroup of G. If $N_G(P)$ is of even order, then G has an abelian Hall ϖ-subgroup that is isolated in G.*

Proof. Since $2 \notin \varpi$, P is of odd order. By assumption, there is an element t of order 2 that normalizes P. Since ϖ is a connected component and $2 \notin \varpi$, the element t acts regularly on P. This yields that

$$x^t = x^{-1} \quad \text{for} \quad x \in P.$$

Thus, P is abelian. If $x \in P^\sharp$, $C_G(x)$ is a ϖ-group and normalized by t. It follows that $A = C_G(x)$ is abelian and the element t inverts every element of A. If $y \in A^\sharp$, the same argument proves that $C_G(y)$ is abelian. Since $A = C_G(x) \subseteq C_G(y)$, we have $C_G(y) = A$. Therefore, A is an abelian subgroup that is isolated in G. It is known that every isolated subgroup is a Hall subgroup. □

Therefore, to prove Theorem B, we may assume that every ϖ-local subgroup is of odd order. From now on we use the following notation and assumptions in addition to the ones already stated.

Let G be a finite simple group. Let

$$\mathcal{M} = \{\, M \mid M \text{ is a maximal } \varpi\text{-local subgroup of } G\},$$

define

$$\mathcal{M}(H) = \{M \in \mathcal{M} \mid H \subseteq M\}$$

for any subgroup H of G, and assume that *every subgroup $M \in \mathcal{M}$ is of odd order.*

The set of subgroups $\mathcal{M}$ satisfies properties which are similar to the properties of the set of all maximal subgroups of the hypothetical minimal simple group of odd order studied by [FT] and [BG]. We remark that the situation considered here does occur in real groups. For example, if p is a prime such that $p \equiv 3 \pmod 4$, the alternating group A_p satisfies the condition for $\varpi = \{p\}$.

2. The Local Analysis of $\mathcal{M}$ We can apply the method of Bender and Glauberman to study the subgroups in $\mathcal{M}$. The subgroups in $\mathcal{M}$ are of odd order; hence, they are solvable by the Odd Order Theorem. By definition, $M \in \mathcal{M}$ is a ϖ-local subgroup. It follows that $F(M)$, the Fitting subgroup of M, is a ϖ-subgroup. Let $p \in \pi(G)$ and let $P \in \mathrm{Syl}_p(M)$. If P is not cyclic, P contains an elementary abelian p-subgroup A of order p^2. Then, A normalizes $N = O_\varpi(M)$ which is not 1. By a well-known proposition (Proposition 1.16 [BG]),

$$N = \langle C_N(x) \mid x \in A^\natural \rangle.$$

It follows that $p \in \varpi$. Thus, if M is not a ϖ-group, M has a cyclic Sylow p-subgroup for every $p \in \pi(M) \setminus \varpi$, Thus, $M \in \mathcal{M}$ is almost a ϖ-subgroup. However, I call attention to the following point. For $M \in \mathcal{M}$, the set $\sigma(M)$ of primes is defined in [BG] as

$$\sigma(M) = \{\, p \in \pi(M) \mid N_G(P) \subseteq M \text{ for some } P \in \mathrm{Syl}_p(M)\,\}$$

(p.70 [BG]). The important set in our case is

$$\sigma_0(M) = \sigma(M) \cap \varpi$$

and the subgroup we should study is

$$M_{\sigma_0} = O_{\sigma_0(M)}.$$

It is proved that M_{σ_0} is a Hall $\sigma_0(M)$-subgroup of M.

Proposition 2. *All the statements of the sections 7–15 of* [BG] *holds with proper changes in hypothesis and the conclusions.*

The *types* of subgroups in $\mathcal{M}$ are defined as in pp.128–129 [BG] with the following three changes.

(IIiv) should read: $V \neq 1$ and if V is a ϖ-group, then

$$N_G(V) \not\subseteq M.$$

(IIv) should read: $N_G(A) \subseteq M$ for every nonidentity subgroup A of M' such that $C_H(A) \neq 1$.

(IIIiii) should read: V is an abelian ϖ-group and $N_G(V) \subseteq M$.

Then, $M \in \mathcal{M}$ is of type I, II, III, IV, or V. We have the following two theorems which are the goal of the local analysis.

Theorem I. *Either every subgroup in $\mathcal{M}$ is of type I or all the following conditions are true.*

(1) *G contains a cyclic subgroup $W = W_1 \times W_2$ with the property that $N_G(W_0) = W$ for every nonempty subset W_0 of $W - \{W_1, W_2\}$. Also, $W_i \neq 1$ for $i = 1, 2$.*

(2) *There are two subgroups S and T in $\mathcal{M}$ such that S and T are of type II, III, IV, or V, $S \cap T = W$, S is not conjugate to T in G, and either S or T (may be both) is of type II.*

(3) *Every $M \in \mathcal{M}$ is either of type I or conjugate to S or T in G.*

There are other conditions which S and T must satisfy. For each $M \in \mathcal{M}$, two particular subsets $A(M)$ and $A_0(M)$ of M are defined (cf. p.124 and p.131 [BG]). The notation M_F for each $M \in \mathcal{M}$ denotes the normal nilpotent Hall subgroup of maximal order of M.

Theorem II. *For a subgroup $M \in \mathcal{M}$, let $X = A(M)$ or $A_0(M)$, and let*

$$D = \{\, x \in X^{\sharp} \mid C_G(x) \not\subseteq M \}.$$

Then, $D \subseteq M_{\sigma_0}$, $|\mathcal{M}(C_G(x)| = 1$ for all $x \in D$, and the following conditions are satisfied.

(Ti) *Whenever two elements of X are conjugate in G, they are conjugate in M.*

(Tii) *If D is not empty, there are ϖ-subgroups $M_1, \dots, M_n$ in $\mathcal{M}$ of type I or II such that with $H_i = (M_i)_F$,*

(a) $(\,|H_i|, |H_j|\,) = 1$ *for* $i \neq j$,

(b) $M_i = H_i(M \cap M_i)$ *and* $M \cap H_i = 1$,

(c) $(\,|H_i|, |C_M(x)|\,) = 1$ *for all* $x \in X^{\sharp}$,

(d) *$A_0(M_i) - H_i$ is a nonempty TI-set in G with normalizer M_i, and*

(e) *if $x \in D$, then there is a conjugate y of x in D and an index i such that*

$$C_G(y) = C_{H_i}(y) C_M(y) \subseteq M_i.$$

If $y \in D$ with $C_G(y) \subseteq M_i$, then $y \in A(M_i)$.

(Tiii) *If some M_i in (Tii) has type II, then M is a ϖ-group and is a Frobenious group with cyclic Frobenius complement, and M_F is not a TI-set in G.*

3. Application of Character Theory We can study subgroups of $\mathcal{M}$ using character theory as in [FT]. The following are the major steps.

Proposition 3. *There is no subgroup $M \in \mathcal{M}$ of type V.*

Proposition 4. *Every subgroup $M \in \mathcal{M}$ of type I is a Frobenius group.*

This is very powerful. Suppose that $M \in \mathcal{M}$ is not a Frobenius group. Then, any supporting subgroup M_i for M in Theorem II is of type I by $(Tiii)$. Then, Proposition 4 yields that M_i is a Frobenius group. However, it is easy to see that $A_0(M_i) = H_i$ for a Frobenius group. This contradicts $(Tii)(d)$. Therefore, there is no supporting subgroup. It follows that X is a TI-set in G. This gives a very tight control on the imbedding of M that is not a Frobenius group. In particular, we can study the subgroups in $\mathcal{M}$ which are of type II, III, or IV. Final result is the following.

Theorem III. *Let G be a finite simple group with disconnected prime graph $\Gamma(G)$. Let ϖ be a connected component such that $2 \notin \varpi$. Then, one of the following two cases occurs.*

(1) *G contains a nilpotent Hall ϖ-subgroup that is isolated in G.*

(2) *We have $\varpi = \{p, q\}$ for some primes p and q, and G has a self-normalizing cyclic subgroup of order pq.*

If the second case occurs, there are many more conditions the primes p and q must satisfy. It may be possible to eliminate the case (2) without referring to the classification of finite simple groups. In any case, Theorem III implies Theorem B.

Theorem IV. *Let G be a finite simple group with disconnected prime graph $\Gamma(G)$. Let Δ be a connected component consisting of odd primes. Then, Δ is a clique.*

References

[BG] H. Bender and G. Glauberman, *Local Analysis for the Odd Order Theorem, London Math. Soc. Lecture Note Series 188*, Cambridge University Press, 1995, pp. 1–174.

[FT] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775–1029.

[GK] K. W. Gruenberg and O. Kegel, *Unpublished manuscript* (1975).

[GR] K. W. Gruenberg and K. W. Roggenkamp, *Decomposition of the augmentation ideal and of relation modules of a finite group*, Proc. London Math. Soc. (3)31 (1975), 149–166.

[W] J. S. Williams, *Prime Graph Components of Finite Groups*, J. Algebra 69 (1981), 487–513.

1409 West Green Street, Urbana, IL 61801
E-mail address: suzuki@math.uiuc.edu

LAPLACIAN SPECTRUM,TREE NUMBERS AND COMPLETELY REGULAR CODES OF GRAPHS

Yasuo Teranishi
Graduate School of Polymathematics
Nagoya University
Nagoya, 464-01, Japan

This article attempts to give an account of the recent work of the author on the study of Laplacian spectrum of graphs. A paper on the details of the results announced in this article is in preparation.

Let G be an undirected simple graph. The Laplacian matrix is $L(G) = D(G) - A(G)$, where $D(G)$ is the diagonal matrix of vertex degrees and $A(G)$ is the adjacency matrix of G. An eigenvalue of $L(G)$ is called a Laplacian eigenvalue of G. We denote by $t(G)$ the number of spanning trees of G and call it the tree number of G.

For a Laplacian eigenvalue λ, $\lambda \neq 0$, let $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(s)}$ be its algebraic conjugate over the rational number field Q. Then the norm $N(\lambda) = \lambda^{(1)}\lambda^{(2)}\cdots\lambda^{(s)}$ is a positive integer.

Theorem 1. *Let λ be a Laplacian eigenvalue of a connected graph G. If the multiplicity $m(\lambda)$ of λ is greater than 1, then $N(\lambda)$ divides the tree number $t(G)$.*

For example, if λ is a Laplacian eigenvalue of a tree

T with $m(\lambda) \geq 2$, then λ ia a unit of the ring of algebraic integers in the algebraic number field $Q(\lambda)$.

In partiqular if $\lambda > 1$ is an integer Laplacian eigenvalue of T, then $m(\lambda) = 1$ ([2] Theorem 2.1).

Proposition 1. *Let T be a tree with $n \geq 2$ vertices. Then T has at least one positive Laplacian eigenvalue with multiplicity 1. Moreover if T has only one positive Laplacian eigenvalue with multiplicity 1 then T is the star $K_{1,n-1}$.*

For two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ on disjoint sets of vertices, their disjoint union is $G_1 + G_2 = (V_1 \cup V_2, E_1 \cup E_2)$. A coalescence of G_1 and G_2 is a graph $G_1 \cdot G_2$ obtained from $G_1 + G_2$ by identifying a vertex of G_1 with a vertex of G_2.

Proposition 2. *Let G_1 and G_2 be graphs. If λ is a Laplacian eigenvalue of G_1 with multiplicity $m_{G_1}(\lambda) > 1$, then λ is a Laplacian eigenvalue of $G_1 \cdot G_2$ with multiplicity at least $m_{G_1}(\lambda) - 1$. Moreover $m_{G_1}(\lambda) > 1$ and $m_{G_2}(\lambda) > 1$ then $m_{G_1 \cdot G_2}(\lambda) \geq m_{G_1}(\lambda) + m_{G_2}(\lambda) - 2$.*

A graph G is called Laplacian integral if the spectrum consists entirely of integers. It follows from Proposition 2 that if a coalescence $G_1 \cdot G_2$ of G_1 and G_2 is Laplacian integral then non-simple Laplacian eigenvalues are all integers. In [1] Cvetkovic showed that the set of connected adjacency integral regular graphs with fixed valency is finite. This can be generalized as follows:

Theorem 2. *If a connected Laplacian integral graph with n vertices has the largest Laplacian eigenvalue m then we have $n | m!$.*

For two graphs G_1 and G_2, the join $G_1 * G_2$ is the graph obtained from the disjoint union of G_1 and G_2 by adding all edges $v_1 v_2$, $v_1 \in V(G_1)$ and $v_2 \in V(G_2)$. Let $G = G_1 * G_2$. Then G is Laplacian integral if and only if G_1 and G_2 are Laplacian integral. A connected graph G is saied to be primitive or imprimitive according as the complement G^c is connected or not. In other words, G is imprimitive if and only if G is the join of some graphs G_1 and G_2.

Propositon 3. *If the number of vertices of a connected Laplacian integral graph G is a prime number then G is imprimitive.*

Proposition 4. *Let G be a connected Laplacian integral graph. Then the second largest Laplacian eigenvalue l_2 satisfies*

$$l_2 < 2\iota(G).$$

Corollary ([2]). *A tree T on n vertices is Laplacian integral if and only if $T = K_{1,n-1}$.*

Proof. The distinct Laplacian eigenvalues of $K_{1,n-1}$ is 0,1 and n, and hence it is Laplacian integral. If T is Laplacian integral tree then it follows from the proposition that $l_2 \leq 1$. Then we see that the diameter of T is at most 2, and hence T is a star.

By Corollary of Proposition 4, we know that if $\iota(G) = 1$, then G is imprimitive.

Theorem 3. *There are only finitely many primitive Laplacian integral graphs with fixed tree number.*

Two graphs G_1 and G_2 are called Laplacian cospectral if they have the same spectrum. For a non-empty proper subset V of the vertex set $V(G)$ of a graph G, let G' be the Seidel switching of G with respect to V.

Proposition 5. *Let G be a connected graph. If G and G' have the same degree matrix, then G and G' are Laplacian cospectral* graphs.

A vertex partition $\iota = (C_1, \ldots, C_t)$ of a graph G is called an equitable partition if, for each i, the number c_{ij} of edges between any vertex in C_i and vertecies in C_j does not depend on the choice of vertex in C_i. The quotient graph G/π is the digraph with vertices $C_1,\ldots,C_t$ and c_{ij} arcs from C_i to C_j. The Laplacian matrix $L(G/\pi) = (a_{ij})$ of G/π is defined by

$$a_{ij} = \begin{cases} -c_{ij}, & \text{if } i \neq j \\ \left(\sum\limits_{1 \leq r \leq t} c_{ir}\right) - c_{ii}, & \text{if } i = j. \end{cases}$$

Theorem 4. *Let $\pi = (C_1,\ldots,C_t)$ be an equitable partition of a connected graph G with n vertices. Let $\lambda_1,\ldots,\lambda_s$ be the distinct positive eigenvalues of $L(G/\pi)$. Then for each i, $\lambda_1 \cdots \lambda_s |C_i|$ is an integer divisible by n.*

A non-empty subset C of $V(G)$ is called a code. For a code C, let C_i denote the set of vertices in G at distance i from C. If $\pi = (C_0,\ldots,C_t)$ is an equitable partition then C is called a completely regular code with covering radius t. For basic theory of completely regular codes see [4].

Theorem 5. *Let G be a connected graph with n vertices and let C be a completely regular code of G with intersection array*

$$i(C) = (b_0,\ldots,b_{t-1};c_1,\ldots,c_t).$$

Let $\lambda_1,\ldots,\lambda_t$ be the positive Laplacian eigenvalues of the quotie graph G/π, where π is the distance partition of $V(G)$ with respect to C. Then

$$|C|\lambda_1 \cdots \lambda_t = nc_1 \cdots c_t.$$

As an apllication we obtain the following result:

Proposition 6. *If C is a completely regular code with covering radius t, then*

$$(\Sigma_{i=0}^{t}(b_i + c_i))/t)^t \geq nc_1\cdots c_t/|C|, \text{ with } c_0 = b_t = 0.$$

In partiqular,

$$(d_{max})^t|C| \geq nc_1\cdots c_t/e.$$

where d_{max} *denotes the maximal degree of vertices and* $e = \lim (1+1/m)^m$.

References

[1] D.Cvetkovic, *Cubic integral graphs, Univ.Beograd Publ. Electrotehn. Fac. Ser. Math. Fiz. 498-541, 107-113 (1975).*

[2] M.Fiedler, *Algebraic connectivity of graphs, Czechoslovak Math. J.23, 298-305 (1973).*

[3] R.Grone, R.Merris and V.S.Sunder, *The Laplacian spectrum of a graph, SIAM J. Matrix Analysis and Appl.11, 218-238 (1990).*

[4] A.Neumair, *Completely regular codes, Discrete Math.106/107, 353-360 (1992).*

[5] Y.Teranish, *The Hoffman number of graphs (preprint).*

Subgroups of Lie-type groups, spherical Tits chambersystems and Presentations of Chevalley-groups.

F.G.Timmesfeld
Mathematisches Institut
Arndtstrasse 2
35392 Giessen, FRG

November 13, 1997

§1. Statement of the Theorems

In [Sei], G. Seitz determined the "chambertransitive" subgroups of the finite Lie-type groups. This theorem was the basis of the (local) classification of the locally finite, chamber transitive Tits-geometries and corresponding parabolic systems. (See [Mei], [St,Ti].)

In [Ti1] we gave certain presentations for Chevalley-groups of type A_n, D_n and E_n. Except in case A_n, the proof succeeded by constructing from the given presentation a parabolic system of type D_n or E_n and then using the universal covering theorem of Tits [Tits2]. As a final step in the proof it then remains to show that a certain chamber transitive subgroup of the Chevalley-group is indeed the full Chevalley-group.

This shows that it would be desirable to extend Seitz's theorem to arbitrary "Lie-type" groups. Unfortunately such a complete determination of chamber transitive subgroups does not seem to be possible, because of examples of type:

$$SL_n(\mathbb{R}) = B \cdot SO_n(\mathbb{R}),\ SL_n(\mathbb{C}) = B \cdot SU_n(\mathbb{C}),\ SL_n(\mathbb{Q}) = B \cdot SL_n(\mathbb{Z}),$$

where B is always a group of triangle matrices. But for the purpose of parabolic systems and presentations of Chevalley-groups a more technical version of Seitz' theorem, see theorem 1 below, suffices. To be able to express this we need some notation:
A classical Moufang-polygon is the Moufang-polygon of some classical group of Witt-index 2 or of some simple algebraic group of rank 2. (The facts we need are probably true for all Moufang polygons. But we wish to avoid the "classification" of these!)

If now $\mathcal{B}$ is an irreducible spherical building of rank ≥ 3 or a classical Moufang polygon and $\widehat{G} = \mathrm{Aut}(\mathcal{B})$ (group of type preserving automorphisms) then there are certain "unipotent" subgroups of $\widehat{G}$. These can be defined completely in the terminology of buildings. Namely if Φ is a root-system connected with $\mathcal{B}, \Pi = \{r_1, \cdots, r_\ell\}$ a fundamental system of Φ with corresponding positive system Φ^+, then the (full) unipotent subgroups of $\widehat{G}$ are the conjugates of

$$U := \langle U_r \mid r \in \Phi^+ \rangle,$$

where U_r is the root-group on $\mathcal{B}$ corresponding to the root r. (See Ronan [Ro].) It follows from the classification of irreducible spherical buildings of rank ≥ 3 [Tits1] or from the Tits commutator relations [Tits3] that U is a nilpotent subgroup of $\widehat{G}$. We call

$$G := \langle U^{\widehat{G}} \rangle \text{ - the Lie-type group of type } \mathcal{B}.$$

Except in certain well-known cases over $GF(2)(Sp(4,2), G_2(2), {}^2F_4(2)!)$ G is the uniquely determined simple normal subgroup of $\widehat{G}$. U is contained in the stabilizer $\widehat{B}$ of a chamber c of $\mathcal{B}$ inside $\widehat{G}$. (This follows from the definition of the U_r! We consider $\mathcal{B}$ as a chambersystem, see [Tits2].) Let $P_1, \cdots, P_\ell$ be the minimal parabolic subgroups of $\widehat{G}$ containing B, i. e. the stabilizers of the rank 1 residues (cells) of $\mathcal{B}$ containing c and

$$\begin{array}{rcll} R_i & := & \langle U^{P_i} \rangle & i = 1, \cdots, \ell \\ U_i & := & \bigcap U^g, \quad g \in P_i, & i = 1, \cdots, \ell \\ K_i & := & \bigcap \widehat{B}^g, \quad g \in P_i, & i = 1, \cdots, \ell. \end{array}$$

Then we have in this terminology:

Theorem 1.

Let $\mathcal{B}$ be an irreducible spherical building of rank ≥ 3 or a classical Moufang-polygon. Suppose there exists a subgroup L of $\widehat{G}$ satisfying:

$$(*) \qquad R_i \subseteq K_i(L \cap P_i) \text{ for } i = 1, \cdots, \ell.$$

Then one of the following holds:

(1) $G \subseteq L$

(2) $G = Sp(4,2), G_2(2)$ or ${}^2F_4(2)$ and $L = A_6, G_2(2)'$ or ${}^2F_4(2)'$

(3) $G = L_4(2) \simeq A_8$ and $L \simeq A_7$.

Remark: Condition $(*)$ implies that L is chamber-transitive on $\mathcal{B}$. This follows from the connectivity of the chambergraph and the fact that each R_i is transitive on the rank 1 residue of type i containing c.

From Theorem 1 we obtain a classification of certain spherical Tits-chambersystems, i. e. chambersystems of type M, M a spherical Coxeter-matrix in the notation of [Tits2]. Such a chambersystem is called classical if all rank 2 residues are classical Moufang-polygons of generalized digons. We have:

Theorem 2.

Let $\mathcal{B}$ be a classical Tits-chambersystem of spherical irreducible type Δ and rank ≥ 3. Fix a chamber c of $\mathcal{B}$ and let $G = \mathrm{Aut}(\mathcal{B})$. Assume:

(+) If $\mathcal{B}_{ij}$ is a rank 2 residue of $\mathcal{B}$ containing c, which is a Moufang polygon and $L_{ij} = G^{\mathcal{B}_{ij}}$ (i.e. the group induced by G on $\mathcal{B}_{ij}$) then L_{ij} satisfies as a subgroup of $\mathrm{Aut}(\mathcal{B}_{ij})$ condition $(*)$ of Theorem 1.

Then either $\mathcal{B}$ is a building of type Δ or $\Delta = C_3$ and $\mathcal{B}$ is the A_7 geometry.

Theorem 1 shows that either L_{ij} contains the Lie-type group of type $\mathcal{B}_{ij}$ or $L_{ij} = A_6$ and $\mathcal{B}_{ij}$ is the $Sp(4,2)$-quadrangle. (Since by hypothesis residues which are hexagons or octogons do not occur!)

As in Theorem 1 it is easy to see that (+) implies that L is chamber transitive on $\mathcal{B}$. (We assume that Tits chambersystems are connected.) So in some sense Theorem 2 is a generalization of Theorem 3 of [Asch] resp. Theorem 3.1 of [Ti2] to the infinite case.

Although condition (+) (and (*)) look artificial, these are exactly the conditions one obtains in context of parabolic systems. Here the system of subgroups $\mathcal{P} = \{P_i \mid i \in I\}$, $I = \{1, \cdots, \ell\}$ of a group G is called a parabolic system (with respect to G and B) if the following conditions hold:

(1) $B := \bigcap_{i \in I} P_i = P_j \cap P_k$ for all $j \neq k \in I$.

(2) $G = \langle P_i \mid i \in I \rangle$ and $B_G = \bigcap_{g \in G} B^g = 1$.

(3) Either

  (i) $P_{ij} := \langle P_i, P_j \rangle = P_i P_j = P_j P_i$, or

  (ii) $\mathcal{B}_{ij} = \mathcal{C}(P_{ij}, B, P_i, P_i)$ is a classical Moufang polygon and $P^{ij} = P_{ij}/B_{ij}$, $B_{ij} = \bigcap B^h, h \in P_{ij}$, is a Lie-type group of type $\mathcal{B}_{ij}$ or $A_6, G_2(2)'$ or ${}^2F_4(2)$.

(For definition of $\mathcal{C}(\quad)$ see [Tits2].)

If now $\mathcal{P} = \{P_i \mid i \in I\}$ is such a parabolic system one can define the diagram $\Delta(I)$ in the obvious way. Namely if $i \neq j \in I$, then i and j are not connected in $\Delta(I)$ if (3)(i) holds, while if $\mathcal{B}_{ij}$ is a m_{ij}-gon then i and j are connected by a bond of strength $m_{ij} - 2$. We have:

Corollary 3.

Let $\mathcal{P} = \{P_i \mid i \in I\}$, $|I| \geq 3$ be a parabolic system of G with irreducible spherical diagram $\Delta(I)$. Then one of the following holds:

(1) $\mathcal{C} = \mathcal{C}(G, B, (P_i)_{i \in I})$ is a building of type $\Delta(I)$ and G is an extension of a Lie-type group of type $\mathcal{C}$ by diagonal automorphisms or $\Delta(I) = A_3$ and $G = A_7$.

(2) $\mathcal{C} = \mathcal{C}(G, B, (P_i)_{i \in I})$ is the A_7 chambersystem of type C_3 and $G = A_7$.

Finally, using theorem 1 and 2, we obtain a uniform presentation for all Chevalley-groups:

Theorem 4.

Let $G = \langle X_i \mid i \in I \rangle, I = \{1, \cdots, \ell\}, \ell \geq 2$, satisfying:

(1) Each X_i is a perfect central extension of $PSL_2(K)$, K a divisionring.

(2) In each X_i there exists a full extension diagonal subgroup $H_i \neq 1$ normalizing all $X_j, j \in I$.

(3) For $X_{ij} = \langle X_i, X_j \rangle, i \neq j$, one of the following holds:

   (a) $[X_i, X_j] = 1$ or

   (b) X_{ij} is a perfect central extension of $PSL_3(K)$, $\mathrm{PSp}(4, K)$ or $P\Omega(5, K)$. Further the unipotent subgroups of X_i and X_j are mapped onto root subgroups of X_{ij}, such that at least one root-subgroup corresponds to a long root of the underlying root-system.

(4) The naturally defined diagram $\Delta = \Delta(I)$ is spherical.

(5) If $|K| = 4$ then there exists a connected pair of nodes $i, j \in I$ with $X_{ij}/Z(X_{ij}) \simeq PSL_3(4)$ and $|Z(X_{ij})| < 12$.

Then the following hold:

(I) Either G is a perfect central extension of $PSL_{\ell+1}(K)$, K a divisionring or K is a field and G is a perfect central extension of the adjoint Chevalley-group of type Δ over K.

(II) If K is commutative and X_1 and X_ℓ are already factor groups of $SL_2(K)$ for end nodes 1 and ℓ of $\Delta(I)$, then G is already a factor-group of the universal Chevalley group of type Δ over K.

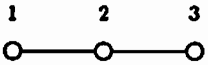
Here a diagonal subgroup H_i of X_i is the coimage of a diagonal subgroup of $PSL_2(K)$. If $\widehat{A}_i$ is an H_i-invariant coimage of a unipotent subgroup of $PSL_2(K)$, then $A_i = [\widehat{A}_i, H_i]$ is called a unipotent subgroup of X_i. By the comments in the introduction of [Til] A_i is in any case an abelian H_i-invariant complement to $Z(X_i)$ in $\widehat{A}_i$.

The diagram $\Delta = \Delta(I)$ is defined as follows: Two nodes $i, j \in I$ are not connected iff $[X_i, X_j] = 1$. They are connected by a bond of strength 1 iff $X_{ij}/Z(X_{ij}) \simeq PSL_3(K)$ and by a bond of strength 2 iff $X_{ij}/Z(X_{ij}) \simeq \mathrm{PSp}(4, K)$ or $P\Omega(5, K)$.

A perfect central extension does not need to be perfect itself. It just means that the centre is in the commutator subgroup. (I. e. $SL_2(3)$!). So condition (1) also makes sense in case $|K| \leq 3$. On the other hand by condition (2) $(H_i \neq 1)$ $|K| \neq 2$.

Of course the groups $\mathrm{PSp}(4, K)$ and $P\Omega(5, K)$ are only defined over fields. Thus if K is non-commutative we have $\Delta = A_n, D_n$ or E_n and the hypothesis of Theorem 1 of [Til] is satisfied. So for the proof of Theorem 4 one may assume that K is a field.

I do not know if the extra condition in case $|K| = 4$ is really necessary. But if $X_{ij}/Z(X_{ij}) \simeq PSL_3(4)$ and $3 \nmid |Z(X_{ij})|$, then $H_i = H_j$, a situation which does not occur, since for example if we have a subdiagram



of type A_3, this would imply $H_1 = H_2 = H_3$, contradicting $[X_1, H_3] \leq [X_1, X_3] = 1$. So 3 divides $|Z(X_{12})|$ and $|Z(X_{23})|$. If now $|Z(X_{12})| = 12 = |Z(X_{23})|$ I come to a very tight situation, which in my opinion is likely to occur, although I am not able to construct an example.

The problem in the proof of theorem 4 is to construct a "universal" group satisfying the conditions of theorem 4. To do this, we construct a parabolic system of type $\Delta(I)$. Then the universal group is given by the universal covering of the corresponding Tits-chambersystem, see Corollary 3 and Theorem 2.

One could also think of taking for this universal group the "amalgamated product of the X_{ij} amalgamated along the X_i ". But I do not know how to make this notion precise.

Moreover, I believe that the existence of this universal group depends on the fact that $\Delta(I)$ is spherical. (Which in my proof comes in via Weyl-groups and root-systems.)
Namely if $\Delta(I)$ is affine of type $\widetilde{A}_n, \widetilde{D}_n$ or $\widetilde{E}_n$ it was shown in [Ti1] that Chevalley-groups of type A_n, D_n or E_n over the ring $K[t, t^{-1}]$ of Laurent-polynomials provide examples of type $\Delta(I)$ over K. Moreover it can be shown that Kac-Moody groups of type $\Delta(I)$ over K provide further examples. And I do not believe that all these examples come from the same universal group.

One final comment on theorem 4. Theorem 1 and 2 and Corollary 3 suggest the possibility of a more general theorem, which gives a uniform presentation of all "Lie-type groups" of rank ≥ 3. And indeed over finite fields I do know what the formulation of this theorem and (hopefully) the proof should look like. But in general there are certain fundamental questions which have to be answered:

(1) What is the definition of the X_i ?
(All classical groups of Witt-index 1 over some division-ring are canditates.)

(2) How can the commutator relations on the root subgroups of $\overline{X}_{ij} = X_{ij}/Z(X_{ij})$ be lifted to X_{ij}. ($\overline{X}_{ij}$ is a rank 2 Lie-type group.)
If $\overline{X}_{ij}$ is a Chevalley-group one uses for this, as in Steinberg's work on central extensions of Chevalley-groups, the action of H_i and H_j on the root subgroups.

(3) How to construct the Moufang-polygon of $\overline{X}_{ij}$ from the fact that the "unipotent subgroups " of X_i and X_j are mapped onto root-subgroups of $\overline{X}_{ij}$?

§2. Some comments on Proofs

The proof of theorem 1 depends on the following proposition, which states some properties of all Lie-type groups, which are not defined over $GF(2)$.

(2.1) Proposition.

Let G be a Lie-type group in the sense of theorem 1 of rank ≥ 2, which is not defined over $GF(2)$. (I. e. there is some root-subgroup U_r with $|U_r| > 2$!) Let Φ be a root system of G with fundamental system $\Pi = \{r_1, \cdots, r_\ell\}$ and positive system Φ^+. Then in the notation of theorem 1 the following hold:

(1) $U = \langle U_{r_1}, \cdots, U_{r_\ell} \rangle$. Further all root-subgroups corresponding to compound root of Φ^+ are contained in U'.

(2) For $r \in \Phi^+$ let $X_r = \langle U_r, U_{-r} \rangle, H_r = N_{X_r}(U_r) \cap N_{X_r}(U_{-r})$ and $H = \langle H_r \mid r \in \Phi^+ \rangle$. Then for appropriate end nodes r_1 and r_ℓ of Π, there exists a subgroup H^0 of H with $[U_{r_1}, H^0] = 1$ and $[U_{r_\ell}, H^0] = U_{r_\ell}$.

It is obvious that both properties are false over GF (2). (2) holds for appropriate enumeration of Π. The proof of (2.1) is by induction on $\ell = \operatorname{rank} G$, where only the rank 2 case is difficult. Condition (1) depends on (elementwise) commutator relations of the root elements corresponding to roots $r \in \Phi^+$. For Moufang planes such relations are wellknown. For Moufang quadrangles corresponding to classical groups they are contained in Van Maldeghem's forthcomming book on generalized polygons. For Moufang hexagons they can be obtained from my (yet unpublished) work on Moufang hexagons.

For Moufang quadrangles corresponding to exceptional algebraic groups (1) follows from commutator relations given by Tits, for which I do not know any proof. But on the other hand theorem 2 and 4 and Corollary 3 are about groups of rank ≥ 3 and all parabolic subgroups of rank 2 in these correspond either to Moufang planes or to Moufang quadrangles corresponding to classical groups of Witt-index 2. So if one wants to restrict oneself on the rank ≥ 3 case, one does not need proposition (2.1) for Moufang hexagons and Moufang quadrangles of exceptional algebraic groups.

(2.1) (1) is used heavily in Seitz's paper. (See (1.4) of [Sei].) But strangely he only states it for Chevalley groups not of type $B_n(2^k)$, $F_4(2^k)$, $G_2(q)$, ${}^3D_4(q)$ or ${}^2F_4(q)$, which then is responsible for (unnecessary) complications in the proof.

Now for the proof of theorem 1 one quotes [Sei] for the $GF(2)$-case. In the other case one shows, using (2.1), induction on $\ell = \operatorname{rank} G$ and some commutator arguments, that $U \subseteq L$. If now $g \in G$, then $g = b{\cdot}l, b \in \hat{B}, l \in L$ by flag-transitivity of L. Hence

$$U^g = U^{b \cdot l} = U^l \leq L$$

and thus $G = \langle U^g \mid g \in \hat{G} \rangle \leq L$.

(2.2) Theorem 2.

The proof of theorem 2 and Corollary 3 depends on the universal covering theorem of [Tits2], which says that the universal 2-cover $\pi : \tilde{C} \to C$ of a Tits-chambersystem C is a building, iff all rank 3 residues of C are covered by buildings.

Let now C be as in theorem 2 or, under the hypothesis of Corollary 3 let $C = C(G, B, (P_i)_{i \in I})$ in the notation of [Tits2] and assume that all rank 3 residues of C are covered by buildings. Then our group G is lifted to some $\tilde{G} \subseteq \mathrm{Aut}(\tilde{C})$, i. e. there is a surjective homomorphism

$$\sigma : \tilde{G} \to G.$$

Now one can show that condition (+) of theorem 2 is also lifted to $\tilde{G}$, that is $\tilde{G}$ satisfies as a subgroup of the automorphism group of the spherical building $\tilde{C}$ condition $(*)$ of theorem 1. Hence by theorem 1 $F^*(\tilde{G})$ is simple. Thus $\mathrm{Kern}\, \sigma = \{1\}$ and σ and whence π are isomorphisms, which proves theorem 2.

So the proof of theorem 2 reduces to showing that all rank 3 residues of C are covered by buildings. To do this one may assume $\mathrm{rank} C = 3$ and C is of type A_3 or C_3. Now there is some real work to do, since there is the additional example of the A_7-geometry. First we show as in (3.1) of [Ti2] that the geometry $\Gamma(C)$ is also of type A_3 or C_3. If now $\Gamma(C)$ is of type A_3, then $\Gamma(C)$ is a projective 3-space. So we may assume $\Gamma(C)$ is of type C_3.

Now we argue similar as in [Asch], that is we try to show that either $\Gamma(C)$ is the A_7-geometry or $\Gamma(C)$ is a partial linear space. In the latter case it follows from (6.2.4.2) in [Tits2] that then $\Gamma(C)$ is a rank 3 polar space.

The arguments in detail are similar as in [Asch]. We use theorem 1 to obtain that on the rank 2 residues of $\Gamma(C)$ of type A_2 and C_2 rank 2 Lie-type groups are induced. Here the hypothesis that C is classical is essential. Now one uses detailed properties of these rank 2 Lie-type groups and of their action on the projective plane resp. generalized quadrangle to show that either $\Gamma(C)$ is a partial linear space or $\Gamma(C)$ is defined over $GF(2)$. (I. e. the residues of $\Gamma(C)$ are of type $L_3(2)$ resp. $\mathrm{Sp}(4,2)$.) For the $GF(2)$-case we quote theorem 1 of [Asch].

The crucial lemma for the proof of theorem 4 is:

(2.3) **Lemma.** Suppose that for $\overline{X}_{ij} = X_{ij}/Z_{ij}, Z_{ij} = Z(X_{ij})$ case (3)(b) of theorem 4 holds. Let $H_{ij} = \langle H_i, H_j \rangle$. Then the following hold:

(1) There exists a system $\{A_r \mid r \in \Phi\}, \Phi$ a root-system of type A_2 or B_2, of H_{ij}-invariant conjugates of A_i und A_j satisfying:

(a) $X_r = \langle A_r, A_{-r} \rangle$ is a perfect central extension of $PSL_2(K)$ and A_r, A_{-r} are H_{ij}-invariant unipotent subgroups of X_r.

(b) If $r, s \in \Phi$, $s \neq \pm r$ and $r + s \notin \Phi$, then $[A_r, A_s] = 1$.

(c) If Φ is of type $A_2, r, s \in \Phi$ with $r + s \in \Phi$, then $[A_r, A_s] = A_{r+s}$

(d) If Φ is of type B_2, r, s both short with $r + s \in \Phi$, then $[A_r, A_s] \leq A_{r+s}$. Further $[A_r, A_s] = A_{r+s}$ if Char$K \neq 2$.

(e) If r is short, s is long and $r + s, 2r + s \in \Phi$, then $[A_r, A_s] = A_{r+s}A_{2r+s}$.

(2) Let $w_\ell \in N_{X_\ell}(H_{ij})$ interchanging A_ℓ and $A_{-\ell}$ with $w_\ell^2 \in H_{ij}; \ell = i$ or j. Then $W_{ij} = \langle w_i, w_j \rangle H_{ij}/H_{ij}$ is dihedral of order 6 or 8 and acts as $W(A_2)$ or $W(B_2)$ on $\{A_r \mid r \in \Phi\}$.

In the proof of (2.3) one first shows that (2.3) holds for $\overline{X}_{ij}$. That is, there exists an $\overline{H}_{ij}$-invariant set $\{\overline{A}_r \mid r \in \Phi\}$ of conjugates of $\overline{A}_i, \overline{A}_j$ satisfying all the conditions of (2.3). This follows from the condition that $\overline{A}_i$ and $\overline{A}_j$ are both root-subgroups of $\overline{X}_{ij}$, which do not both correspond to short roots. After that one lifts all these commutator relations to X_{ij}, using the action of H_{ij} on the root-subgroups. This type of argument is similar to Steinberg's argument in his wellknown work on central extensions of Chevalley groups.

Now this generic argument only works in case $|K| \neq 4$, since if $|K| = 4$ one has $\overline{H}_i = \overline{H}_j \simeq \mathbb{Z}_3$. Thus in case $|K| = 4$ one needs to embed X_{ij} into a larger group (of type A_3 or B_3) and show that, thanks to the extra condition in case $|K| = 4$ in theorem 4, PGL_3 (4) is induced on $\overline{X}_{ij}$ in this larger group.

Now let $H = \langle H_i \mid i \in I \rangle, N = \langle w_i \mid i \in I \rangle H$ and $W = N/H$. Then one shows next:

(2.4) The following hold:

(1) $W \simeq W(\Delta(I))$

(2) The permutation action of W on the conjugates of the $w_i, i \in I$ is equivalent to the permutation action of W on the conjugates of the $X_i, i \in I$ under W.

From (2.3) (2) it is clear that the w_i satisfy the relations of the fundamental reflections of $W(\Delta(I))$. So the proof of (1) essentially reduces to showing that W is no center factor group of $W(\Delta(I))$. Here it is necessary to discuss the different types of $\Delta(I)$.

For example if $\Delta(I) = D_4$ and $W \simeq W^*(D_4)$, the center factor group of $W(D_4)$, then a product of four commuting reflections of W is 1. But on the other hand one can show that these reflections come from the reflections of a product of four commuting X_r's. Since such a product is mod the center a direct product of four $PSL_2(K)$'s, the product of the four reflections can not be 1.
This type or argument succeeds in all cases and proves (1).

Now one takes the natural action of W on a root-system Φ of type $\Delta(I)$ (here a careful distinction between B_ℓ and C_ℓ, which both correspond to the same $\Delta(I)$ is necessary !) and extends this action on $\{A_r \mid r \in \Phi\}$ using (2.3)(1) and (2.4)(2). Then one shows that for all pairs $r, s \in \Phi$ the same type of commutator relations as in (2.3)(1) are satisfied. Now let $U = \langle A_r \mid r \in \Phi^+ \rangle$. Then it follows from the commutator-relations that U is nilpotent. (The proof is the same as for Chevalley-groups!)

Let $B = UH$ (H normalizes all $A_r, r \in \Phi$ by definition.) and $P_i = \langle B, X_i \rangle, i \in I = \{1, \cdots, \ell\}$. Then the final aim is to show:

(2.5) $\{P_i \mid i \in I\}$ is a parabolic system of type $\Delta(I)$ of G.

Now with (2.5) theorem 4 is a consequence of Corollary 3.

References

[Asch] Aschbacher, M.: Finite geometries of type C_3 with flag transitive groups, Geom. Dedicata 16 (1984), 195-200

[Mei] Meixner, Th.: Groups acting transitively on locally finite classical Tits chamber systems, in "Finite Geometries, Buildings and Related Topics", Clarendon Press, Oxford, 45-65.

[Ro] Ronan, M.: Lectures on Buildings, Academic Press (1989)

[Sei] Seitz, G.: Flag-transitive subgroups of Chevalley groups, Ann. of Math. (2), 97, 27-56, 1973

[St,Ti] Stellmacher, B., Timmesfeld, F. G.: Rank 3 Amalgam, To appear in Mem. of the AMS.

[Tits1] Tits, J.: Buildings of spherical Type and finite BN-Pairs, Lect. Notes in Math. 386, Springer Verlag

[Tits2] Tits, J.: A local approach to Buildings, In The geometric Vein, pp. 519-547, Springer Verlag

[Tits3] Tits, J.: Moufang Polygons I, Root data, Bull. Belg. Math. Soc. 3, (1994), 455-468

[Ti1] Timmesfeld, F. G.: Presentations for certain Chevalley-groups, submitted

[Ti2] Timmesfeld, F. G.: Tits geometries and Revisionism of the classification of finite simple groups of char 2-type, Proc. of the Rutgers Group Theory Year, 1983-1984, Cambridge Univ. Press 1984

Group association scheme of $PSL(2,7)$

Masato TOMIYAMA [*]
Division of Mathematical Sciences
Osaka Kyoiku University
Kashiwara, Osaka 582, JAPAN

1 Introduction

An association scheme can be thought of as a combinatorial interpretation of transitive permutation groups. It is one of the central concepts for those who attempt to study combinatorial structure with high regularity, not relying on group theory. Since the regularity of an association scheme is measured by its parameters (intersection numbers), it is a natural problem to characterize (or classify) association schemes with a given set of parameters. There are many contributions to this problem (e.g., [4] for the Hamming schemes, [8],[13] for the Johnson schemes, [12] for the q-analogue Johnson schemes, [6] for the dual polar schemes, [7], [5] for the forms schemes and so on), but almost all of them concern P- (and Q-) polynomial schemes.

A standard example of non-P- nor Q- polynomial association schemes can be constructed from each group G, which is called the *group association scheme* $\mathcal{X}(G)$ *of* G. It is well known that $\mathcal{X}(G)$ is primitive if and only if G is simple, and that primitive association schemes play an important role in commutative association schemes, similar to the role simple groups play in finite groups. (See [2, section II.9], [9],[10].) So in order to study finite simple groups from the viewpoint of algebraic combinatorics, it would be interesting and necessary to determine whether the group association scheme $\mathcal{X}(G)$ of a given simple group G is characterized by its intersection numbers: however, this problem has been open even for the smallest non-abelian simple group A_5, the alternating group of degree 5. (See [1].) In [14] the author showed that $\mathcal{X}(A_5)$ is characterized by its intersection numbers. In this note, we treat G is the second smallest non-abelian simple group $PSL(2,7)$, the 2-dimensional projective special linear group over the field of oreder 7. We show that $\mathcal{X}(PSL(2,7))$ is characterized by its intersection numbers. For the other finite simple groups G, characterization problems of $\mathcal{X}(G)$ are still open.

[*] e-mail address: tomiyama@cc.osaka-kyoiku.ac.jp

We note that the character table of G determines the intersection numbers of $\mathcal{X}(G)$, and vice versa. (See [2, Section II.7].) Thus for group association schemes, the characterization problem by their intersection numbers is reduced to a classical problem of characterizing groups by their character tables (though the association schemes of two non-isomorphic groups may be isomorphic). Here we can rely on many results in structure and representation theory of groups.

However, difficulties arises when we attempt to classify all association schemes (not necessarily group association schemes) with the intersection numbers to those of a given group association scheme. Because, the problem is now completely different in nature: we are not allowed to rely on group theory, but are required purely combinatorial methods. Further, the result is not always simple: there are exactly three non-isomorphic association schemes with the intersection numbers identical to those of $\mathcal{X}(S_4)$ of the symmetric group S_4 of degree 4, among them $\mathcal{X}(S_4)$ is the unique group association scheme. (See [14].)

Because of these difficulties, not so many results appeared about the classification of association schemes with the parameters identical to those of the group association scheme $\mathcal{X}(G)$ for a give group G: [14] for $G = A_5$, S_4 and $SL(2,5)$, and [15] for $G = PSL(2,7)$. They are individual groups, and the arguments heavily depend on each group.

In [16] and [17], N. Yamazaki and the author consider the above problem for an infinite family of groups $G = S_n$, the symmetric group of degree n, for every n. They characterize $\mathcal{X}(S_n)$ by its parameters when $n \neq 4$.

2 Definitions and Main Theorem

Let X be a finite set and $R_0, R_1, \dots, R_d$ the relations on X, i.e., subsets of $X \times X$. Then $\mathcal{X} = (X, \{R_i\}_{0\leq i\leq d})$ is a *commutative association scheme of d classes on X* if the following conditions hold.

(1) $R_0 = \{(x,x)|x \ \in X\}$.

(2) $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$, and $R_i \cap R_j = \emptyset$ if $i \neq j$.

(3) For all $i \in \{0,1,\dots,d\}$, there exists $i' \in \{0,1,\dots,d\}$ such that ${}^tR_i = R_{i'}$, where ${}^tR_i = \{(x,y)|(y,x) \in R_i\}$.

(4) For all $i,j,k \in \{0,1,\dots,d\}$, the number of $z \in X$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$ is a constant, p_{ij}^k, whenever $(x,y) \in R_k$.

(5) $p_{ij}^k = p_{ji}^k$ for all $i,j,k \in \{0,1,\dots,d\}$.

The non-negative integers $\{p_{ij}^k\}_{0\leq i,j,k\leq d}$ are called the *intersection numbers* of $\mathcal{X}$.

The reader is referred to [2] and [3] for the general theory of association schemes and related terminology.

Take any finite group G. Let $C_0 = \{1\}, C_1, \ldots, C_d$ be the conjugacy classes of G. Define the relations R_i on G by $R_i = \{(x,y) | yx^{-1} \in C_i\}$ for $i = 0, 1, \ldots, d$. Then $\mathcal{X}(G) = (G, \{R_i\}_{0 \leq i \leq d})$ is a commutative association scheme of d classes on G called the *group association scheme* of G. (See [2, Example II.2.1(2)].)

The main theorem in this note is the following:

Theorem 2.1 *The group association scheme $\mathcal{X}(PSL(2,7))$ is characterized by its intersection numbers, where $PSL(2,7)$ is the 2-dimensional projective special linear group over the field of order* 7.

The i^{th} *adjacency matrix* A_i of $\mathcal{X}$ is defined to be the matrix of degree $|X|$ whose rows and columns are indexed by the elements of X and whose (x,y) entries are

$$(A_i)_{x,y} = \begin{cases} 1 & \text{if} \quad (x,y) \in R_i, \\ 0 & \text{otherwise.} \end{cases}$$

The i^{th} *intersection matrix* B_i of $\mathcal{X}$ is defined to be the matrix of degree $d+1$ whose (j,k) entries are

$$(B_i)_{j,k} = p_{ij}^k.$$

The intersection numbers of the group association scheme $\mathcal{X}(G)$ can be obtained from the following formula:

$$p_{ij}^k = \frac{|C_i||C_j|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(u_i)\chi(u_j)\overline{\chi(u_k)}}{\chi(1)},$$

where $Irr(G)$ is the set of all irreducible characters of G, and u_l is the representative of C_l. (See [2, Section II.7].)

To calculate the intersection numbers of $\mathcal{X}(PSL(2,7))$, we order the conjugacy classes of $PSL(2,7)$ as follows:

	C_0	C_1	C_2
representative :	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} Z$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Z$	$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} Z$
order of representative :	1	7	7
$\lvert C_i \rvert$:	1	24	24

	C_3	C_4	C_5
representative :	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Z$	$\begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix} Z$	$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} Z$
order of representative :	2	4	3
$\lvert C_i \rvert$:	21	42	56

where $Z = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$.

Then the intersection matrices of $\mathcal{X}(PSL(2,7))$ are as follows:

$$B_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 9 & 8 & 0 & 3 \\ 24 & 1 & 1 & 0 & 8 & 3 \\ 0 & 0 & 7 & 0 & 4 & 3 \\ 0 & 14 & 0 & 8 & 4 & 6 \\ 0 & 7 & 7 & 8 & 8 & 9 \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 24 & 1 & 1 & 0 & 8 & 3 \\ 0 & 9 & 1 & 8 & 0 & 3 \\ 0 & 7 & 0 & 0 & 4 & 3 \\ 0 & 0 & 14 & 8 & 4 & 6 \\ 0 & 7 & 7 & 8 & 8 & 9 \end{pmatrix}, \qquad B_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & 0 & 4 & 3 \\ 0 & 7 & 0 & 0 & 4 & 3 \\ 21 & 0 & 0 & 4 & 4 & 3 \\ 0 & 7 & 7 & 8 & 1 & 6 \\ 0 & 7 & 7 & 8 & 8 & 6 \end{pmatrix},$$

$$B_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 14 & 0 & 8 & 4 & 6 \\ 0 & 0 & 14 & 8 & 4 & 6 \\ 0 & 7 & 7 & 8 & 1 & 6 \\ 42 & 7 & 7 & 2 & 16 & 12 \\ 0 & 14 & 14 & 16 & 16 & 12 \end{pmatrix}, \quad B_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 7 & 7 & 8 & 8 & 9 \\ 0 & 7 & 7 & 8 & 8 & 9 \\ 0 & 7 & 7 & 8 & 8 & 6 \\ 0 & 14 & 14 & 16 & 16 & 12 \\ 56 & 21 & 21 & 16 & 16 & 19 \end{pmatrix}.$$

In the following, we assume $\mathcal{X} = (X, \{R_i\}_{0 \le i \le 5})$ is an association scheme having the same intersection matrices as those of $\mathcal{X}(PSL(2,7))$.

In general, it is well known that $p_{ij}^0 \neq 0$ if and only if $j = i'$. Hence, in our case, $1' = 2$, $2' = 1$ and $i' = i$ hold for $i = 0,3,4,5$. Also ${}^tR_1 = R_2$, ${}^tR_2 = R_1$ and ${}^tR_i = R_i$ hold for $i = 0,3,4,5$.

For any subset E of X, we define the graph (E, R_i) as the graph with vertex set E and edge set $(E \times E) \cap R_i$. The graph (E, R_i) is directed if $i \in \{1,2\}$ and undirected if $i \in \{0,3,4,5\}$.

To prove Theorem 2.1, we have to show that all relations $R_1, R_2, \ldots, R_5$ of $\mathcal{X}$ are uniquely determined by the intersection numbers. But it is enough to show the following:

Proposition 2.2 *The directed graph (X, R_1) is uniquely determined by the intersection numbers.*

First we prove our main theorem.

Proof of Theorem 2.1: By Proposition 2.2, the graph $\Gamma = (X, R_1)$ is uniquely determined. So the relation R_1 is unique and so is the first adjacency matrix A_1. Then we have the other adjacency matrices of $\mathcal{X}$ by using the equation

$$A_1{}^2 = \sum_{k=0}^{5} p_{11}^k A_k = 0A_0 + 1A_1 + 9A_2 + 8A_3 + 0A_4 + 3A_5.$$

Namely, we determine them as follows:

$$\begin{aligned} R_2 &= \{(x,y)|(A_1{}^2)_{x,y} = 9\} = {}^tR_1, \\ R_3 &= \{(x,y)|(A_1{}^2)_{x,y} = 8\}, \\ R_4 &= \{(x,y)|(A_1{}^2)_{x,y} = 0, x \neq y\}, \\ R_5 &= \{(x,y)|(A_1{}^2)_{x,y} = 3\}. \end{aligned}$$

Thus all the relations of $\mathcal{X}$ are uniquely determined. □

We remark that the relation R_1 or $R_2 = {}^tR_1$ is essential. Suppose we can determine the relations R_3, R_4 and R_5. For $i, j \in \{3,4,5\}$, consider the equation

$$A_iA_j = \sum_{k=0}^{5} p_{ij}^k A_k = p_{ij}^0 A_0 + p_{ij}^1 A_1 + p_{ij}^2 A_2 + p_{ij}^3 A_3 + p_{ij}^4 A_4 + p_{ij}^5 A_5.$$

Since the intersection numbers satisfy

$$p_{ij}^1 = p_{ij}^2 \quad \text{for} \quad i, j \in \{3,4,5\},$$

the coefficient of A_1 and that of A_2 are equal. Therefore we can not distinguish the relations R_1 and R_2 from the other three relations R_3, R_4 and R_5.

The method to prove Proposition 2.2 is purely combinatorial, and the proof is very long and complicated. (See [15].)

References

[1] E. Bannai, "Algebraic combinatorics: recent topics on association schemes", (in Japanese), Sugaku (Mathematics, a publication of Math. Soc. of Japan), 45 (1993), 55–75; English version, Sugaku Expositions (American Math. Soc.), 7 (1994), 181–207.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin-Cummings, California, 1984.

[3] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer, Berlin-Heidelberg, 1989.

[4] Y. Egawa, Characterization of $H(n,q)$ by the parameters, *J. Combin. Th. (A)* 31 (1981), 108–125.

[5] T. Huang, A characterization of the association schemes of Bilinear forms, *Europ. J. Combin.* 8 (10987), 159–173.

[6] A. A. Ivanov and S. V. Shpectorov, The association schemes of dual polar spaces of type ${}^2A_{2d-1}(p^f)$ are characterized by their parameters if $d \geq 3$, *Lin. Alg. Appl.* **114/115** (1989), 133-139.

[7] A. A. Ivanov and S. V. Shpectorov, A characterization of the association schemes of Hermitian forms, *J. Math. Soc. Japan* **43** (1989), 25–48.

[8] A. Neumaier, Characterization of a class of distance regular graphs, *J.reine angew. Math.* **357** (1985), 182-192.

[9] M. Rassy and P. H. Zieschang, "Basic structure theory of association schemes", preprint, 1994.

[10] S. B. Rao, D. K. Ray-Chaudhuri and N. M. Singhi, "On imprimitive association schemes", pp. 273–291 in : *Combinatorics and applications - Proc. of the Seminar on Combinatorics and Applications in honour of Prof. S. S. Shrikhande, Calcutta, 1982*, Indian Statist. Inst. (K. S. Vijayan & N. M. Singhi, eds.), Calcutta, 1984.

[11] S. S. Shrikhande, On a characterization of the triangular association scheme, *Ann. Math. Stat.* 30 (1959), 39–47.

[12] A. P. Sprague, Characterization of projective graphs, *J. Combin. Th. (B)* 24 (1978), 294–300.

[13] P. Terwilliger, The Johnson graph $J(d, r)$ is unique if $(d, r) \neq (2, 8)$, *Discrete. Math.* 58 (1986), 175-189.

[14] M. Tomiyama, Characterization of the group association scheme of A_5 by its intersection numbers, to appear in *J. Math. Soc. Japan.*

[15] M. Tomiyama, Characterization of the group association scheme of $PSL(2, 7)$, preprint.

[16] M. Tomiyama and N. Yamazaki, Characterization of the group association scheme of the symmetric groups, to appear in *Erop. J. Combin.*

[17] M. Tomiyama and N. Yamazaki, On a condition of the group association scheme of the symmetric group, in preparation.

VERTEX OF NON-PERIODIC MODULES IN THE AUSLANDER-REITEN QUIVER OF FINITE GROUPS

KATSUHIRO UNO

Department of Mathematics, Osaka University,
Toyonaka, Osaka, 560 Japan

This is a joint work with Prof. T.Okuyama. Details will be found in [OU3]. Let kG be the group algebra of a finite group G over a field k of characteristic p, where p is a prime. The stable Auslander-Reiten quiver (AR quiver for short) of kG is a directed graph whose vertices are isomorphism classes of non-projective indecomposable kG-modules and arrows are independent irreducible kG-homomorphisms among them. We denote by $\Gamma_s(kG)$ the stable AR quiver of kG. After Webb published an important paper [W], many results concerning the shape of $\Gamma_s(kG)$ have been obtained. (See [E2], [E3], [ES] and [O1].) Each connected component Γ of $\Gamma_s(kG)$ has a tree T such that Γ is isomorphic as graphs to the graph ZT which is obtained by a specific way from countably many copies of T. This T is uniquely determined up to isomorphisms and called the tree class of Γ.

Main results

Here we announce two results. First one says that the tree classes of connected components of $\Gamma_s(kG)$ have been completely determined, assuming that k is a perfect field. The following should be the final result in this nature.

Theorem A. *Let k be a perfect field. Then the tree class of a connected component of $\Gamma_s(kG)$ is one of the following: A_n, $\tilde{A}_{1,2}$, A_∞, $\tilde{B}_3$, B_∞, D_∞ or A_∞^∞. Moreover, each of the above in fact occurs.*

Remark. For each of above possibilities, the following detail holds. Here Γ is a connected component of $\Gamma_s(kG)$ and D is a defect group of the block to which the modules in Γ belong.

(i) A_n occurs if and only if D is cyclic. Moreover, then we have $\Gamma = \Gamma_s(B)$.

(ii) $\tilde{A}_{1,2}$ or $\tilde{B}_3$ occurs only when D is a four group. In fact, $\tilde{A}_{1,2}$ occurs for kD and $\tilde{B}_3$ occurs when G is the alternating group on 4 letters and k does not contain a cube root of unity.

(iii) B_∞ occurs only when D is dihedral. An example is given in this note.

(iv) A_∞^∞ occurs only when D is dihedral or semidihedral. It occurs for kD.

(v) D_∞ occurs only when D is semidihedral. It occurs for kD.

(vi) If the tree class is A_∞^∞, then we have $\Gamma \cong ZA_\infty^\infty$ unless D is a four group.

(vii) If k is algebraically closed, then one of A_n, A_∞, D_∞ or A_∞^∞ must occur.

(viii) If the modules in Γ are periodic, then its tree class is A_∞.

Parts (i), (vii) and (viii) can be found in [B2]. Erdmann showed in [E3] that A_∞^∞ and D_∞ occur only when the block is tame, i.e., $p = 2$ and D is dihedral, generalized quaternion or semidihedral. The tree classes for tame blocks are studied in [E2]. Consequently, Remarks (iv) and (v) hold. In [ES], they proved that Euclidean diagram appears only when D is a four group. It implies (vi), and since the structure of such blocks are well known, we have (ii). (See also [B2].) Therefore, it has been proved already in several papers that A_n is the only finite Dynkin tree class, $\tilde{A}_{1,2}$ and $\tilde{B}_3$ are only Euclidean tree classes, and the rest are infinite Dynkin tree classes, A_∞, D_∞, A_∞^∞, B_∞ and C_∞. Hence, in order to prove Theorem A, it suffices to give an example of a B_∞-component and to prove the following.

Theorem 1. *Let k be a perfect field. Then there is no component whose tree class is C_∞.*

If k is a perfect field, then a C_∞-component may appear only when the following situation is the case.

(1.1) The Galois action induces an involutive automorphism α of a component Γ of $\Gamma_s(\bar{k}G)$ isomorphic to $\mathbb{Z}D_\infty$ such that α interchanges the two ends of Γ.

On the other hand, it is known that a B_∞-component appears when we have the following situation.

(1.1)' The Galois action induces an involutive automorphism α of a component Γ of $\Gamma_s(\bar{k}G)$ isomorphic to $\mathbb{Z}A_\infty^\infty$ such that α gives a reflection with respect to a certain τ-orbit in Γ.

An example of a B_∞-component is given in the end of this note. Thus (iii) of the previous remark holds.

The second result concerns the distribution of vertices of modules in a single component, we have the following, which would be also the final result for non-periodic components.

Theorem B. *Let k be a perfect field, and let Γ be a connected component of $\Gamma_s(kG)$. Suppose that it is not a tube, i.e., that modules in Γ are not Ω-periodic. Then one of the following holds. Moreover, each of the following in fact occurs.*

(i) *All the modules in Γ have vertices in common.*

(ii) *We can take $T : X_1 - X_2 - X_3 - \cdots - X_n - \ldots$ in Γ with $\Gamma \cong \mathbb{Z}T$ and $vx(X_1) < vx(X_2) = vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots$.*

(iii) *$p = 2$, $\Gamma = \mathbb{Z}A_\infty^\infty$, and only two distinct vertices P and Q occur, with $|P : Q| = 2$. Moreover, one of the following holds.*

(iiia) *Q is a dihedral group of order greater than 4, and the modules with vertex Q lie in a subquiver Γ_Q such that both Γ_Q and $\Gamma \setminus \Gamma_Q$ are isomorphic to $\mathbb{Z}A_\infty$ as graphs.*

(iiib) *Q is a Kleinian four group and P is a dihedral group of order 8, and the modules with vertex Q lie in two or four adjacent τ-orbits.*

Remark. The above (i) and (ii) occur in many cases, (iiia) occurs for a dihedral 2-group. See [(3.3) of E1]. (iiib) occurs for a dihedral group D_8 of order 8 and the symmetric group S_4 on 4 letters. kD_8 has a component satisfying (iiib) above with two adjacent τ-orbits of modules having four group vertex, and kS_4 has a component satisfying (iiib) above with four adjacent τ-orbits of modules having four group vertex. See also [E1] and [E2, V.3].

On the vertices of modules, beginning with the result for p-groups in [E1], there are several developments [U2], [OU2] usinig the generalization of Green correspondence due to Kawata [K1] and the results of vertices of modules in the Auslander-Reiten sequences [U1], [OU1]. The most parts of Theorem B have been proved in [OU2]. More precisely, it has been shown there that there are only three possibilities (i), (ii) and (iii) of which (i) and (iii) are exactly the same as in Theorem B above. However, the part (ii) of the main theorem in [OU2] is as follows.

Statement (ii)'. *We can take $T: X_1 - X_2 - X_3 - \cdots - X_n - \ldots$ in Γ with $\Gamma \cong ZT$ and oneof the following holds.*

(iia) $vx(X_1) < vx(X_2) = vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots,$
(iib) $vx(X_1) < vx(X_2) = vx(X_3) < vx(X_4) = \cdots = vx(X_n) = \ldots,$
(iic) $vx(X_1) = vx(X_2) < vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots$

Thus, in order to prove Theorem B, it suffices to show the possibilities (iib) and (iic) above do not occur. More precisely, it suffices to prove the following.

Theorem 2. *Let k be a perfect field, and let Γ be a connected component of $\Gamma_s(kG)$. Suppose that $\Gamma \cong ZA_\infty$. Then we can take $T: X_1 - X_2 - X_3 - \cdots - X_n - \ldots$ in Γ with $\Gamma \cong ZT$ and $vx(X_1) \leq vx(X_2) = vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots.$*

In the very final remark of [OU2], it is remarked that the above (iib) or (iic) may occur only if the following situation would be the case. See also [E1, Theorem B].

(1.2) The prime p is 2 and a 2-group D is a normal subgroup of a finite group G and a certain element of G induces an involutive graph automorphism α of a component Γ of $\Gamma_s(kD)$ isomorphic to ZD_∞ such that α interchanges the two ends of Γ.

Semidihedral groups

Proofs of Theorems 1 and 2 use some general reduction results [E1], [K1], [K2], [O1], [OU2], [U2] and Galois decent ([B1, 2.33]). Then, we may assume that a defect group D is a normal subgroup of G. Moreover, for Theorem 1, we may suppose that $G = D$. Furthermore, considering (1.1) and (1.2), it suffices to show that no actions on a D_∞-component of $\Gamma_s(kD)$ interchanges its two ends. Then the following is of course useful.

Theorem (Erdmann [E3]). *Let D be a p-group. Suppose that $\Gamma_s(kD)$ has a connected component isomorphic to ZD_∞. Then D is semidihedral.*

In the rest of this section, we assume that D is a semidihedral group of order 2^n, $n \geq 4$ and k is a perfect field of characteristic 2.

Another useful thing is the following. Namely, all the indecomposable kD-modules are already classified.

Theorem (Crawley-Boevey [C]). *All the isomorphism classes of indecomposable kD-modules are classified.*

In [C], it is assumed that $|k| \geq 4$. However, by an easy argument, the result also holds when $|k| = 2$.

By using the above classification, we can prove the following by mostly computation.

Lemma 1. *If indecomposable kD modules X and Y lie in an end of a component isomorphic to $\mathbb{Z}D_\infty$ and have the same predecessor. Then* $\dim_k X \neq \dim_k Y$.

By the above, we have ;

Lemma 2. *Let Γ be a connected component of $\Gamma_s(kD)$ such that $\Gamma \cong \mathbb{Z}D_\infty$. Let α be an automorphism of kD that stabilizes Γ. Then every module in Γ is α-invariant.*

Lemma 2 implies that neither (1.1) nor (1.2) may occur. Therefore Theorems 1 and 2 have been proved.

An example of a B_∞-component

The following gives an example such that its stable AR quiver has a component isomorphic to $\mathbb{Z}B_\infty$. It is due to T. Okuyama ([O2]).

Suppose that k is a perfect field which does not contain a cube root of unity. Let G be a group generated by x, y , z and t with relations:

$$x^2 = y^2 = (xy)^4 = z^3 = t^2 = 1, xz = zx, yz = zy, tx = yt, ty = xt, tz = z^2t$$

Then $|G| = 2^4 3$ and G has normal subgroups

$$D =< x, y > \qquad \text{and} \qquad C =< z > .$$

Then D is a dihedral group of order 8 and C is a cyclic group of order 3. Let $H = D \times C$. Let α be a Galois automorphism such that α interchanges the two cube roots of unity. Since k does not contain a cube root of unity, kC has the unique (up to isomorphisms) simple module T of dimension 2. It is G-invariant, and since G/C is a 2-group, T can be extended to a simple kG-module S. Moreover, it follows that $T \otimes \bar{k} = T_1 \oplus T_2$, where T_1 and T_2 are non-isomorphic simple $\bar{k}C$-modules with $T_1^\alpha = T_2$. However, $S \otimes \bar{k}$ is a simple $\bar{k}G$-module, since $T_1^t = T_2$ and $(S \otimes \bar{k})_C \cong T_1 \oplus T_2$.

Let $X = (x-1)\bar{k}D/s\bar{k}D$ and $Y = (y-1)\bar{k}D/s\bar{k}D$, where s is the sum of all the elements in D. Then X and Y are non-projective indecomposable $\bar{k}D$-modules and we have $X^t = Y$ and $Y^t = X$, but X and Y are invariant under the Galois actions. It is known that X and Y lie in the same connected component of $\Gamma_s(\bar{k}D)$ which is isomorphic to $\mathbb{Z}A_\infty^\infty$. See [W] or [E2]. Now $X \otimes_{\bar{k}} T_1$, $Y \otimes_{\bar{k}} T_1$, $X \otimes_{\bar{k}} T_2$ and $Y \otimes_{\bar{k}} T_2$ are non-isomorphic indecomposable $\bar{k}H$-modules, and we have $(X \otimes_{\bar{k}} T_1)^t = Y \otimes_{\bar{k}} T_2$ and $(Y \otimes_{\bar{k}} T_1)^t = X \otimes_{\bar{k}} T_2$, and $(X \otimes_{\bar{k}} T_1)^\alpha = X \otimes_{\bar{k}} T_2$ and $(Y \otimes_{\bar{k}} T_1)^\alpha = Y \otimes_{\bar{k}} T_2$. Of course, $X \otimes_{\bar{k}} T_1$ and $Y \otimes_{\bar{k}} T_1$ lie in the same component Θ_1, and $X \otimes_{\bar{k}} T_2$ and $Y \otimes_{\bar{k}} T_2$ lie in the same component Θ_2. Both Θ_1 and Θ_2 are isomorphic to $\mathbb{Z}A_\infty^\infty$.

Hence $Z_1 = (X \otimes_{\overline{k}} T_1)^G = (Y \otimes_{\overline{k}} T_2)^G$ and $Z_2 = (X \otimes_{\overline{k}} T_2)^G = (Y \otimes_{\overline{k}} T_1)^G$ are non-isomorphic indecomposable $\overline{k}G$-modules, and we have $Z_1^\alpha = Z_2$. Moreover, we have $\Theta_1^\iota = \Theta_2$ and Z_1 and Z_2 lie in the same component Γ isomorphic to $\mathbb{Z}A_\infty^\infty$.

Finally, we recall that $\Omega(\overline{k}) \otimes_{\overline{k}} T_i$ lies in Θ_i for $i = 1, 2$. Here $\Omega(\overline{k})$ is the Heller translate of the trivial $\overline{k}D$-module $\overline{k}$, i.e., the kernel of the projective cover of $\overline{k}$. We have $(\Omega(\overline{k}) \otimes_{\overline{k}} T_1)^\iota = \Omega(\overline{k}) \otimes_{\overline{k}} T_2$ and $(\Omega(\overline{k}) \otimes_{\overline{k}} T_1)^\alpha = \Omega(\overline{k}) \otimes_{\overline{k}} T_2$. Therefore $(\Omega(\overline{k}) \otimes_{\overline{k}} T_1)^G$ lies in Γ and is α-invariant. Since $Z_1^\alpha = Z_2$ and they lie in Γ, too, it follows that α satisfies the condition in (1.1)'. Thus we have a B_∞-component. In fact, it is the one which contains $\Omega(S)$.

References

[B1] Benson, D.: Modular representation theory : New trends and methods. (Lect. Notes Math., vol.1081) Berlin Heidelberg New York : Springer 1984

[B2] Benson, D.: Representations and cohomology I. (Cambridge Studies in Advanced Math., vol.30) Cambridge : Cambridge University Press 1991

[C] Crawley-Boevey, W.W.: Functiopnal filtrations III. J. London Math. Soc. 40, 31-39 (1989)

[E1] Erdmann, K.: On the vertices of modules in the Auslander–Reiten quiver of p-groups. Math. Z. 203, 321–334 (1990)

[E2] Erdmann, K.: Blocks of tame representation type and related algebras. (Lect. Notes Math., vol.1428) Berlin Heidelberg New York : Springer 1990

[E3] Erdmann, K.: On Auslander-Reiten components for group algebras, J. Pure and Appl. Algebra 104, 149–160 (1995)

[K1] Kawata, S.: Module correspondences in Auslander-Reiten quivers for finite groups. Osaka J. Math. 26, 671–678 (1989)

[K2] Kawata, S.: The modules induced from a normal subgroup and the Auslander-Reiten quiver. Osaka J. Math. 27, 265–269 (1990)

[O1] Okuyama, T.: On the Auslander-Reiten quiver of a finite group. J. Algebra 110, 425–430 (1987)

[O2] Okuyama, T.: The Auslander-Reiten sequences for group algrbras and subgroups. (in Japanese) Proceeding of the 3rd symposium on representations of algebras (M.Sato Ed.) (1988)

[OU1] Okuyama, T., Uno, K.: On vertices of Auslander–Reiten sequences. Bull. London Math. Soc. 22, 153–158 (1990)

[OU2] Okuyama, T., Uno, K.: On the vertices of modules in the Auslander–Reiten quiver II. Math. Z. 217, 121–141 (1994).

[OU3] Okuyama, T., Uno, K.: On the vertices of modules in the Auslander–Reiten quiver III. In preparartion.

[U1] Uno, K.: Relative projectivity and extendibility of Auslander-Reiten sequences. Osaka J. Math. 25, 499–518 (1988)

[U2] Uno, K.: On the vertices of modules in the Auslander–Reiten quiver. Math. Z. 208, 411–436 (1991)

[W] Webb, P.: The Auslander–Reiten quiver of a finite group. Math. Z. 179, 97-121 (1982)

Principal blocks with extra-special defect groups of order 27

Yoko Usami
Ochanomizu University, Department of Mathematics
Otsuka 2-1-1, Bunkyo-ku, Tokyo 112 , Japan

§ 1. Introduction

Let G be a finite group and p be a prime number. Let b be a p-block of G, P be a defect group of b and k(b) (respectively, l(b)) be the number of irreducible ordinary characters (respectively, irreducible Brauer characters) in b. Suppose that

<u>two blocks</u> b <u>and</u> b' <u>of finite groups</u> G <u>and</u> G' <u>respectively,</u> <u>have the common defect group</u> P <u>and their Brauer categories</u> $\mathrm{Br}_{b,P}(G)$ <u>and</u> $\mathrm{Br}_{b',P}(G')$ <u>are equivalent</u> . (1)

(See [FH] for Brauer categories.) On condition (1) there is a question whether we have

$$k(b) = k(b') \quad \text{and} \quad l(b) = l(b') \tag{2}$$

or not. We have a following conjecture.

Conjecture 1. When b and b' are principal blocks satisfying condition (1), the equalities in (2) hold.

When P is an abelian group , it is known that a block b of G and its Brauer correspondent $\mathrm{Br}_P(b)$ in $N_G(P)$ have equivalent Brauer categories (i.e. fusion of b-subpairs of G is controlled by $N_G(P)$ by Proposition 4.21 in [AB]), and Broué conjectured that they are derived equivalent (respectively, isotypic). See Conjecture 6.1 and Question 6.2 in [Br2]. Note that each of these conjectures implies that we have

$$k(b) = k(Br_P(b)) \quad \text{and} \quad l(b) = l(Br_P(b)) \qquad (3)$$

for any block b with abelian defect group P. As is stated in [Br2] neither of Broué's conjectures above does not hold when P is not an abelian group. The principal 2-block b of any one of Suzuki groups Sz(q) and its Brauer correspondent have equivalent Brauer categories (actually, fusion of P is controlled by its normalizer, since 2-Sylow groups are T.I. sets), but they are not derived equivalent nor isotypic ; neventheless (3) holds for them (cf. Consequences 5 and 7 in [A]). Here we have to add one more remark. M.Kiyota pointed out that a group $(Z_3 \times Z_3) \rtimes Q_8$, a semi-direct product of an elementary abelian 3-group of order 9 and a quaternion group of order 8 whose unique involution is acting on $Z_3 \times Z_3$ trivially, has only two 3-blocks (i.e. the principal block b_0 and the other block b_1) and their Brauer categories are equivalent to each other but we have $l(b_0) \neq l(b_1)$.

In this paper we fix P as an extra-special group of order 27 of exponent 3 , and consider principal 3-blocks b having P as a defect group and check Conjecture 1. Note that in this case having equivalent Brauer categories implies having the same inertial quotient E ($\cong N_G(P)/PC_G(P)$ here) and the same fusion of P. At any rate, using the classification of finite simple groups, we determine k(b), l(b) and $k_0(b)$ completely and proves that Conjecture 1 is true for such blocks , and consequently we prove that Dade's conjecture of ordinary form holds for b.(Here $k_0(b)$ is the number of irreducible ordinary characters in b of height zero.

When the author visited l'Universite Paris 7 last year, Lluis Puig suggested an idea to use his construction of characters as functions on local pointed elements in Corollary 4.4, Theorem 5.2 and Theorem 5.6 in [P]. The author uses his idea to prove Theorem 1 below.

In the following we denote a cyclic group of order m by Z_m , a quaternion group of order 8 by Q_8 , a dihedral group of order 8 by D_8 and a semidihedral group of order 16 by SD_{16} respectively.

<u>Theorem</u> 1. Let b be the principal 3-block of a finite group G with an extra-special defect group P of order 27 and of exponent 3. Let E be the inertial quotient of b (i.e. $E \cong N_G(P)/PC_G(P)$) and set $Z(P) = \langle u \rangle$ for an element u in P. Then we have the following.

(1) When $N_G(P) \subseteq C_G(Z(P))$, fusion of P in G is controlled by $N_G(P)$ and one of the following holds:

(i) If $E = 1$, then b is 3-nilpotent and $k(b) = 11$, $k_0(b) = 9$ and $l(b) = 1$.

(ii) If $E \cong Z_2$, then $k(b) = 10$, $k_0(b) = 6$ and $l(b) = 2$. (In this case E acts on P/Z(P) fixed-point-freely.)

(iii) If $E \cong Z_4$, then $k(b) = 14$, $k_0(b) = 6$ and $l(b) = 4$.

(iv) If $E \cong Q_8$, then $k(b) = 16$, $k_0(b) = 6$ and $l(b) = 5$.

(2) When $N_G(P) \nsubseteq C_G(Z(P))$, E is isomorphic with either Z_2 , $Z_2 \times Z_2$ Z_8 , D_8 or SD_{16} and we have an estimate of k(b) as in Table 1 below according to E and the number of conjugacy classes of elements of order 3. When $E \cong Z_2$, E does not act on P/Z(P) fixed-point-freely. In each case $k(b) - l(b)$

takes a constant value. When $E \cong Z_8$, each case is divided into two subcases according to fusion of a basic set of $C_G(u)$ in the extended centralizer $C^*_G(u)$ $(= \{ g \in G \mid u^g = u \text{ or } u^{-1} \})$.

Using the classification of finite simple groups we obtain the following theorem. As is well known, we can assume that $O_{p'}(G) = 1$ when we treat the principal p-block of G.

<u>Theorem 2</u> (Using the classification of finite simple groups). Let G be a finite group with $O_{3'}(G) = 1$ having an extra special 3-Sylow group P of order 27 of exponent 3. Let M be a minimal normal subgroup of G. Then one of the following holds:

(i) $M \cong Z_3$ and Z(P) is a normal subgroup of G and fusion of P in G is controlled by $N_G(P)$. As for the principal 3-block b, k(b) and l(b) are uniquely determined according to its inertial quotient.

(ii) $M \cong Z_3 \times Z_3$ and G/M is embedded in GL(2,3). In particular, G is 3-solvable.

(iii) $M \cong PSL(3,q)$ where $q = 3k + 1$ and $(k,3) = 1$. Furthermore we have

$$PGL(3,q) \leqq G \leqq Aut(PSL(3,q))$$

(iv) $M \cong PSU(3,q\ )$ where $q = 3k -1$ and $(k,3) = 1$. Furthermore we have

$$PGU(3,q) \leqq G \leqq Aut(PSU(3,q)).$$

(.v) $M \cong M_{24}$, Ru or J_4 . Furthermore $G = M$.

(vi) $M \cong PSL(3,3)$, $PSU(3,3)$, ${}^2F_4(2)'$, M_{12} , J_2 or He. Furthermore $G = M$ or Aut(M).

(vii) $M \cong G_2(q)$ where $q = 3k \pm 1$ and $(k,3) = 1$. Furthermore $M \leqq G \leqq Aut(M)$.

(viii) $M \cong {}^2F_4(q)$ where $2^{2m+1} = q = 3k - 1$ and $(k,3) = 1$. Furthermore $M \leqq G \leqq$ Aut (M).

All exact values of k(b) for the principal blocks b above are written in

Table 2. When $N_G(P) \nsubseteq C_G(Z(P))$, we have always $k_0(b) = 9$. Furthermore, Dade's conjecture of ordinary form holds for b in any case.

§ 2.. Remarks on Theorem 1

(1) After the author obtained Theorem 1, Masao Kiyota told the author that several years ago he already determined k(b), $k_0(b)$ and l(b) for principal blocks b when $N_G(P) \subseteq C_G(Z(P))$ by Brauer and Olsson's method using the orthogonality relation between columns of generalized decomposition matrix.

(2) Outline of a proof is as follows. First, list up all possible Broué's (or Alperin's) conjugation families for b-subpairs (with an aid of 3-strongly embedded subgroups) in order to determine fusion of b-subpairs in G ([Brl, CP]). This work means to list up all possible Brauer categories as in [CP]. Note that when b is a principal block, b-subpairs are equivalent to p-subgroups. Second, collect information about blocks b_Q such that

$$(1,b) \subsetneqq (Q,b_Q) \subseteqq (P,e) ,$$

where (P,e) is a fixed maximal b-subpair. Third, construct a Z-basis of generalized characters in b which vanish on 3-regular elements. Here we apply L.Puig's Theorem 5.6 in [P], where he showed some equivalent conditions of a function on local pointed elements to be a generalized character. Fourth, determine the decomposition of each character in the above Z-basis into irreducible characters in order to know k(b), since it is known that any irreducible character in b appears in some gereralized character in this Z-basis. In order to determine these decompositions the author used a computer (with an aid of Hikoe Enomoto) and also checked the elementary divisors of Cartan matrices by a computer. Unfortunately, when $N_G(P) \nsubseteq C_G(Z(P))$, we can not determine k(b) uniquely. There are huge number of possible decompositions. But , as for k(b) , it seems that we can get almost the same estimate of k(b) as this by hand.

(3) When E is of order 2 , either G has a normal subgroup of index 3 , or G is a 3-solvable group of 3-length 1 by S.D.Smith and A.P.Tyrer's theorem in [ST]. (Masao Kiyota informed the author of this theorem after the symposium.)

§ 3. Remarks on Theorem 2

(1) Using the strong assumption that $Z(P) \triangleleft G$, k(b) in (i) is determined . Here we already use the classification of finite simple groups to determine the number of irreducible ordinary characters of a principal 3-block with an elementary abelian defect group of order 9 and with the cyclic inertial quotient of order 8.

(2) If G is a 3-solvable group with $O_{3'}(G) = 1$ and has an extra-special 3-Sylow subgroup of order 27 of exponent 3 , then G is completely determined, that is , either the semidirect product of P and a group E isomorphic with 1, Z_2 , $Z_2 \times Z_2$, Z_4 , Q_8 , D_8 or SD_{16} or $(Z_3 \times Z_3) \rtimes SL(2,3)$ or $(Z_3 \times Z_3) \rtimes GL(2,3)$ (with all faithful actions). (cf. Proposition 53.4 in [Ka] or [Ko]) .

(3) It is not easy to choose the irreducible characters in b among all irreducuble characters in G when G belongs to one of infinite series in (iii), (iv), (vii) and (viii). Fortunately, any nonprincipal 3-block

of a simple group in these infinite series has a proper subgroup of P as a defect group. So using the estimate of k(b) in Theorem 1 and the known facts on the number of irreducible ordinary characters in other 3-blocks and some more information about b itself, we determine k(b) effectively in these cases. The author thanks Ken-ichi Shinoda and Meinolf Geck for information about ${}^2F_4(q)$.

(4) In order to prove Dade's conjecture in this case, we divide the radical 3-chains into two subsets whether the last term of a radical 3-chain is a defect group of the corresponding principal block of the normalizer of the chain or not. Up to G-conjugacy, there is a one-to-one correspondence between a radical 3-chain of length m in the former subset and a radical 3-chain of length m-1 in the latter subset by the Brauer correspondence between corresponding principal blocks. Then by cancellation we get the conclusion (cf. 2.3 in [U]).

(5) There is no perfect isometry between the principal 3-blocks of $P \rtimes Z_8$ and PSU(3,3), but there is a perfect isometry between the principal 3-blocks of PSU(3,3) and J_2. There is no perfect isometry between the principal 3-blocks of $P \rtimes SD_{16}$ and $G_2(4)$, but there is a perfect isometry between the principal 3-blocks of $G_2(4)$ and $G_2(5)$. There are perfect isometries between the principal 3-blocks of $(Z_3 \times Z_3) \rtimes SL(2,3)$ and PGL(3,q) with q=3k+1 and (3,k) = 1 and PGU(3,q') with q'=3k'-1 and (3,k') =1. There is a perfect isometry between the principal 3-blocks of PSL(3,3) and M_{12} .

Table 1 : $N_G(P) \not\subseteq C_G(Z(P))$ $k = k(b)$, $l = l(b)$

Inertial quotient	Fusion of P is controlled by $N_G(P)$	Otherwise		
Z_2	$P-\{1\}$: 6 classes $(k-l=8)$ $k=\boxed{10}$	5 classes $(k-l=7)$ $k=9, \boxed{10}, 11$		
$Z_2 \times Z_2$	$P-\{1\}$: 4 classes $(k-l=7)$ $k=\boxed{11}$	3 classes Case 1 $(k-l=5)$ $k=8, 9, 10, \boxed{11}$ Case 2 $(k-l=6)$ $k=10, 11, 12$	2 classes Case 1 $(k-l=4)$ $7 \leqq k \leqq 12$ Case 2 $(k-l=3)$ $k=6, 7, 8, 9, 10, \boxed{11}$	1 class $(k-l=2)$ $5 \leqq k \leqq 18$
Z_8	$P-\{1\}$: 2 classes $(k-l=5)$ Subcase 1 $k=8, 9, 10, 11, 12, \boxed{13}, 14$ Subcase 2 $k=8, 9, 10, 11, 12$	1 class $(k-l=4)$ Subcase 1 $8 \leqq k \leqq 18$ Subcase 2 $7 \leqq k \leqq 15$		
D_8	$P-\{1\}$: 3 classes $(k-l=8)$ $k=\boxed{13}$	2 classes $(k-l=6)$ $k=9, 10, 11, 12, \boxed{13}$	1 class $(k-l=4)$ $k=7, 8, 9, 10, 11, 12, \boxed{13}, 14, 15$	
SD_{16}	$P-\{1\}$: 2 classes $(k-l=7)$ $k=10, 11, 12, 13, \boxed{14}, 15$	1 class $(k-l=5)$ $k=7, 8, 9, 10, 11, 12, 13, \boxed{14}$		

Table 2 : $N_G(P) \not\subseteq C_G(Z(P))$ $k = k(b)$

<table>
<tr><th>Inertial quotient</th><th>Fusion of P is controlled by $N_G(P)$</th><th colspan="2">Otherwise</th></tr>
<tr><td>Z_2</td><td>$P-\{1\}$: 6 classes
$k = 10$</td><td colspan="2">5 classes
$k = 10$
$PGL(3,q) \subset G \subsetneq Aut(PSL(3,q))$
$q = 3k+1$, $(3,k) = 1$
$(Z_3 \times Z_3) \rtimes SL(2,3)$
$PGL(3,q)$ $q = 3k+1$ $(3, k) = 1$
$PGU(3,q) \cdot$ (odd order) $q = 3k-1$ $(3, k) = 1$</td></tr>
<tr><td>$Z_2 \times Z_2$</td><td>$P-\{1\}$: 4 classes
$k = 11$</td><td>3 classes
Case 1
$k = 11$
$(Z_3 \times Z_3) \rtimes GL(2,3)$
$PGU(3,q) \cdot$ (even order)
$q = 3k-1$ $(3, k) = 1$</td><td>2 classes
Case 2
$k = 11$
$PSL(3,3)$
M_{12}</td></tr>
<tr><td>Z_8</td><td>$P-\{1\}$: 2 classes
Subcase 1
$k = 13$
$PSU(3, 3)$, J_2</td><td colspan="2"></td></tr>
<tr><td>D_8</td><td>$P-\{1\}$: 3 classes
$k = 13$</td><td>2 classes
$k = 13$
M_{24}, $Aut(M_{12})$
$Aut(PSL(3,3))$
He, $Aut(He)$</td><td>1 class
$k = 13$
${}^2F_4'(2)$</td></tr>
<tr><td>SD_{16}</td><td>$P-\{1\}$: 2 classes
$k = 14$
$Aut(PSU(3, 3))$
$G_2(q) \subsetneq G \subsetneq Aut(G_2(q))$
$q = 3k \pm 1$ $(3, k) = 1$
$Aut(J_2)$</td><td colspan="2">1 class
$k = 14$
Ru
${}^2F_4(q) \subsetneq G \subsetneq Aut({}^2F_4(q))$
J_4</td></tr>
</table>

For the characters of groups in Table 2

1. ATLAS
2. B. Chang, The conjugate classes of Chevalley groups of type (G_2), J. Algebra, 9 (1968), 190–211.
3. B. Chang and R. Ree, The characters of $G_2(q)$, Symposia Mathematica XIII, Instituto Nazionale de Alta Mathematica, (1974), 395–413.
4. V. Ennola, On the characters of the finite unitary groups, Ann. Acad. Sci. Fenn. 323, (1963), 1–34.
5. H. Enomoto, The conjugacy classes of Chevalley groups of type (G_2) over finite fields of characteristic 2 or 3, J. Fac. Sci. Univ. Tokyo Sect. I Math., 16 (1970), 497–512.
6. H. Enomoto and H. Yamada, The characters of $G_2(2^n)$, Japan. J. Math. 12 (1986) 325–377
7. K. Shinida, The conjugacy classes of the finite Ree groups of type (F_4), J. Fac. Sci. Univ. Tokyo Sct. IA Math.,22 (1975), 1–15.
8. G. Malle, Die unipotenten Charaktere von $^2F_4(q^2)$, Comm. in Algebra, 18 (7), (1990), 2361–2381.
9. R. Steinberg, The representation of GL(3,q), GL(4,q), PGL(3,q) and PGL(4,q), Canadian J. Math. 3, (1951), 225–235.

References

[A] J. Alperin, Weights for finite groups, Proc. Sympos. Pure Math. 47 (1987), 369-379.

[AB] J. Alperin and M. Broué, Local methods in block theory , Ann. of Math. 110 (1979), 143-157.

[Br1] M. Broué, Theorie locale des blocs d'un groupe fini, Proceedings of the International Congress of Mathematicians, Berkeley, 1986, 360-368.

[Br2] M. Broué, Isométries parfaites, types de blocs, catégories dérivées, Astérisque 181-182 (1990), 61-92.

[CP] M. Cabanes and C. Picaronny, Types of blocks with dihedral or quaternion defect groups , J.Fac.Sci.Univ. Tokyo Sect.IA, Math. 39 (1992), 141-161.

[FH] P. Fong and M. Harris, On perfect isometries and isotypies in finite groups, Invent. Math. 114 (1993), 139-191.

[Ka] G. Karpilovsky, " Structure of Blocks of Group Algebras", Longman Scientific and Technical, 1987

[Ko] S. Koshitani, On group algebras of finite groups, Proc. 4th Internat. Conf. on Representations of Algebras, Springer. Lecture Note Series, 1178, 109-128.

[P] L. Puig, Pointed groups and construction of characters, Math. Z, 176 (1981), 265-292.

[U] Y. Usami, Perfect isometries for principal blocks with abelian defect groups and elementary abelian 2-inertial quotients , J.of Algebra 196 (1997) , 646-681.

Perfect isometries and the Glauberman correspondence

Atumi Watanabe (Kumamoto University)

Introduction

In the character theory of finite groups the Glauberman character correspondence is well known. In this report we construct a correspondence for blocks of finite groups which is given by the Glauberman character correspondence. Between the corresponding blocks, there exists a perfect isometey in the sense of [B].

Let S and G be finite groups such that S acts on G and $(| S |, | G |) = 1$. We put $\Gamma = SG$, the semidirect product of G by S . Let (K, O, F) be a p-modular system such that K is algebraically closed, where p is a prime. As usual we denote by $\mathrm{Irr}(G)$ the set of irreducible characters of G and by $\mathrm{Irr}_S(G)$ the set of S-invariant irreducible characters of G. We recall the Glauberman character correspondence.

Theorem ([G] ; [I], Chapter 13). For every pair (G, S) such that S is solvable and acts on G and $(| G |, | S |) = 1$, there exsits a uniquely determined one-to-one map $\pi(G, S)$: $\mathrm{Irr}_S(G) \to \mathrm{Irr}(C_G(S))$. These maps satisfy the following properties :

(i) If T is a normal subgroup of S and $H = C_G(T)$, then $\pi(G, T)$ maps $\mathrm{Irr}_S(G)$ onto $\mathrm{Irr}_S(H)$.

(ii) In the situation of (i), $\pi(G, S) = \pi(H, S/T)\pi(G, T)$.

In the above let $\beta_\chi = \pi(G, S)(\chi)$, *i.e.*, the Grauberman correspondent of χ $\in\mathrm{Irr}_S(G)$. If S is a cyclic group generated by s, then there exists an extension (for example the canonical extension) $\tilde{\chi}$ of χ to SG such that if $S =< s^i >$, then

$$\tilde{\chi}(s^i c) = \epsilon_\chi \beta_\chi(c) \quad (\forall c \in C_G(S)), \quad \epsilon_\chi = \pm 1.$$

Let $\mathrm{Bl}(G)$ be the set of blocks of G and $\mathrm{Bl}_S(G)$ be the set of S-invariant blocks of G. We mean a block of G a block ideal of OG. For a block B of G we denote by $\mathrm{Irr}(B)$ the set of irreducible characters of G belonging to B. For a central idempotent e of OG, let $\mathcal{R}_K(G, e)$ or $\mathcal{R}_K(G, eOG)$ be the additive group of characters of G afforded by KGe-modules. Under the above notation the following is our main result.

Theorem 2. Suppose that S is solvable and S centralizes a Sylow p-subgroup P of G. Then there exists a unique bijection $\rho(G, S)$ from $\mathrm{Bl}_S(G)$ onto $\mathrm{Bl}(C_G(S))$ such that if $B \in \mathrm{Bl}_S(G)$ corresponds to $b \in \mathrm{Bl}(C_G(S))$ by $\rho(G, S)$, then there exists a perfect isometry R : $\mathcal{R}_K(G, B) \to \mathcal{R}_K(C_G(S), b)$ such that $R(\chi) = \pm\pi(G, S)(\chi)$ for any $\chi \in \mathrm{Irr}(B)$. Moreover if $b = \rho(G, S)(B)$, then B and b have a common defect group.

§ 1. Preliminaries : Perfect isometries and block extensions

Broué's perfect isometry is an important notion in block theory and in this report it is our big concern. The Clifford theory for blocks due to E.C. Dade, what we call block extension, plays a big role in our arguments. In this section we state some results on perfect isometry and block extension which we use to prove our results.

Let G and H be finite groups and e (resp. f) be a central idempotent of OG (resp. OH) and $\mathcal{R}_K((G,e),(H,f))$ be the additive group of generalized characters of $G \times H$ afforded by (KGe, KHf)-bimodules.

Definition ([B]). Let $\mu \in \mathcal{R}_K((G,e),(H,f))$. μ is *perfect* if μ satisfies the following.

(i) $\forall h \in H$ and $\forall g \in G$, $(\mu(g,h)/\mid C_H(h) \mid) \in O$ and $(\mu(g,h)/\mid C_G(g) \mid) \in O$,

(ii) if $\mu(g,h) \neq 0$, then g is p-regular if and only if h is p-regular.

For $\mu \in \mathcal{R}_K((G,e),(H,f))$ let R_μ be a homomorphism from $\mathcal{R}_K(G,e)$ into $\mathcal{R}_K(H,f)$ defined by

$$R_\mu(\alpha)(h) = \frac{1}{\mid G \mid} \sum_{g \in G} \mu(g^{-1},h)\alpha(g) \quad (\forall\, h \in G)$$

for all $\alpha \in \mathcal{R}_K(G,e)$. If $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \cdots, \chi_n\}$, $\mathrm{Irr}(H) = \{\zeta_1, \zeta_2 \cdots, \zeta_m\}$ and $\mu = \sum_{i,j} n_{ij}(\chi_i \times \zeta_j)$ $(n_{ij} \in Z)$, then we have $R_\mu(\chi_i) = \sum_j n_{ij}\zeta_j$ by the orthogonality relations of characters. If μ is perfect and R_μ is a linear isometry from $\mathcal{R}_K(G,e)$ onto $\mathcal{R}_K(H,f)$, then R_μ is called *a* perfect isometry. The following follows from [B], Proposition 1.3.

Lemma. Let L be another finite group and g be a central idempotent of OL and ν be a generalized character of $H \times L$. If R_μ and R_ν are perfect isometries, then the composite $R_\nu \circ R_\mu$ is a perfect isometry from $\mathcal{R}_K(G,e)$ onto $\mathcal{R}_K(L,g)$.

From [B], Theorem 1.5, we have the following.

Theorem ([B]). Let R_μ be a perfect isometry from $\mathcal{R}_K(G,e)$ onto $\mathcal{R}_K(H,f)$. Then

(i) $Z(OGe)$ and $Z(OHf)$ are isomorphic as R-algebras. In particular OGe is a block of G, then OHf is a block of H.

(ii) Suppose that OGe and OHf are blocks, and put $B = OGe$ and $b = OHf$. Then the defects of B and b are equal, and there exists a height-preserving bijiection between the ordinary irredcuible characters in B and b. Moreover the numbers of modular irreducible characcters in B and b are equal.

Next we prepare some results from [D]. Let Γ be a finite group and G be a normal subgroup of Γ. We set $S = \Gamma/G$. Then the group algebra $O\Gamma$ is an S-graded Clifford system with the σ-component $(O\Gamma)_\sigma = \Sigma_{x \in \sigma} Ox$ for $\sigma \in S$. Put $\mathfrak{C} = C(OG \text{ in } O\Gamma) = \{ c \in O\Gamma \mid cx = xc \text{ for all } x \in OG \}$ and $\mathfrak{C}_\sigma = \mathfrak{C} \cap (O\Gamma)_\sigma$. Let B be a fixed block of G with the block idempotent e and put $S[B] = \{\sigma \in S \mid (e\mathfrak{C}_\sigma)(e\mathfrak{C}_{\sigma^{-1}}) = e\mathfrak{C}_1\}$. $S[B]$ forms a subgroup of S and $S[B] \subseteq \Gamma_B/G$, where Γ_B is the stabilizer of B in Γ. Let $\mathfrak{C}[B] = \oplus\Sigma_{\sigma\in S|B|}e\mathfrak{C}_\sigma$. $\mathfrak{C}[B]$ is an $S[B]$-graded Clifford system with $\mathfrak{C}[B]_\sigma = e\mathfrak{C}_\sigma$ for all $\sigma \in S[B]$. For $\sigma \in S[B]$, there exist $c_\sigma \in \mathfrak{C}[B]_\sigma$ and $c_{\sigma^{-1}} \in \mathfrak{C}[B]_{\sigma^{-1}}$ such that $c_\sigma c_{\sigma^{-1}} = e$ by the definition of $S[B]$. Then $(c_{\sigma^{-1}}c_\sigma)^2 = c_{\sigma^{-1}}c_\sigma \neq 0$. Hence $c_{\sigma^{-1}}c_\sigma = e$. For an element s of σ we put $u_s = sc_{\sigma^{-1}}$. Then u_s is a unit of eOG with the inverse $c_\sigma s^{-1}$ and we have $x^{u_s} = (x^s)^{c_\sigma^{-1}} = x^s$ for all $x \in OG$. From this fact we can see that any irreducible character in B is $S[B]$-invariant. Any modular irreducible charcater in B is also $S[B]$-invariant.

Let D be a defect group of B and b be a block of $C_G(D)$ associated with B. Let φ be a unique modular irreducible character in b, $N_\Gamma(D)_\varphi$ be the stabilizer of φ in $N_\Gamma(D)$ and $N_\Gamma(D) < \varphi >$ be the Clifford extension. We denote by $\bar{F}$ the multiplicative group of F. Since $N_G(D)_\varphi$ centralizes $C_\Gamma(D) < \varphi > /\bar{F}$ ($\cong C_\Gamma(D)_\varphi/C_G(D)$), there is a "bilinear" map $\omega : (N_G(D)_\varphi/DC_G(D)) \times (C_\Gamma(D)_\varphi/C_G(D)) \rightarrow \bar{F}$ so that :

$$x^y = \omega(yDC_G(D), x\bar{F})x \quad \forall x \in C_\Gamma(D) < \varphi >, \ \ \forall y \in N_G(D)_\varphi.$$

Let $C_\Gamma(D)_\omega = \{ x \in C_\Gamma(D)_\varphi \mid \omega(N_G(D)_\varphi/DC_G(D), xC_G(D)) = \{ 1 \} \}$. $C_G(D) \subseteq C_\Gamma(D)_\varphi$ and $C_\Gamma(D)_\varphi/C_\Gamma(D)_\omega$ is isomorphic to a subgroup of $\mathrm{Hom}(N_G(D)_\varphi/DC_G(D), \bar{F})$. The following is a part of [D, Corollary (12.6)], which is one of the main results of [D].

Theorem ([D]). Under the above notation we have $S[B] = GC_\Gamma(D)_\omega/G$.

2. Correspondence for blocks

We go back to the situation in Introduction. So we assume that S and G are finite groups such that S acts on G and that S and G have coprime orders.

Proposition 1. Let B be an S-invarinat block of G. If S centralizes a defect group D of B, then we have $S[B] = S$. In particular any $\chi \in \mathrm{Irr}(B)$ is S-invarinat.

Remark By the above Dade's theorem and the Schur-Zassenhause theorem, if $S[B] = S$ then S centralizes a defect group of B.

Proposition 2. Suppose that S is cyclic. Let B be an S-invariant block of G such that S centralizes a defect group D of B. Then we have

(i) Let b be a block of $C_G(S)$ containing $\pi(G,S)(\chi_1)$ for some $\chi_1 \in \mathrm{Irr}(B)$. Then there exists a perfect isometry R from $\mathcal{R}_K(G,B)$ onto $\mathcal{R}_K(C_G(S),b)$ such that $R(\chi) = \pm\pi(G,S)(\chi)$ for any $\chi \in \mathrm{Irr}(B)$.

(ii) In the situation of (i), D is a defect group of b.

Theorem 1. Suppose that S is solvable. Let B be an S-invariant block of G such that S centralizes a defect group D of B. Then there exists a unique block b of $C_G(S)$ such that $\mathrm{Irr}(b) = \{ \pi(G,S)(\chi) \mid \chi \in \mathrm{Irr}(B) \}$. Moreover there exists a perfect isometry $R : \mathcal{R}_K(G,B) \to \mathcal{R}_K(C_G(S),b)$ such that $R(\chi) = \pm\pi(G,S)(\chi)$ for any $\chi \in \mathrm{Irr}(B)$ and D is a defect group of b

Theorem 2 is a direct consequence of the Glauberman correspondence theorem, Lemma and Theorem 1.

Let $B(G)$ denote the principal block of G. In the situation of Theorem 2, $\rho(G,S)(B(G)) = B(C_G(S))$. Hence by Broué's theorem, (ii), $B(G)$ has a unique modular irreducible character if and only if $B(C_G(S))$ has a unique modular irreducible character. Therefore when S is solvable and S centralizes a Sylow p-subgroup of G, if $C_G(S)$ is p-nilpotent, then G is p-nilpotent. N. Chigira of Muroran Institute of Technology generalized this fact by purely group theoretic methods as follows. The below Corollary follows from Theorem 2 and the Feit-Thompson theorem.

Proposition 3 (Chigira). Assume that S centralizes a Sylow p-subgroup of G. If $C_G(S)$ is p-nilpotent, then G is p-nilpotent.

Corollary. Assume that a Sylow p-subgroup P of G is abelian and S centralizes P. There exists a perfect isometry from $\mathcal{R}_K(G, B(G))$ onto $\mathcal{R}_K(C_G(S), B(C_G(S)))$.

For the detail of our results, see [W].

References

[B] M. Broué : Isométries parfaites, types de blocs, catégories dérivées, Astérisque 181-182(1990), 61-92.

[D] E.C. Dade : Block extensions, Illinois J. Math., 17(1973), 198-272.

[G] G. Glauberman : Correspondences of characters for relatively prime operator groups, Canad. J. Math. 20(1968), 1465-1488.

[I] I.M. Isaacs : Character theory of finite groups, Academic Press, New York, San Francisco, London, 1976.

[W] A. Watanabe ; Perfect isometries and the Glauberman correspondence, preprint (in preparation).

Ternary codes and vertex operator algebras

Hiromichi Yamada
Department of Mathematics
Hitotsubashi University

This article is based on my talk about a joint work with M. Kitazume and M. Miyamoto on a certain class of vertex operator algebras related to ternary codes. The details will appear elsewhere.

1 Introduction

Vertex operator algebras have been studied from a wide variety of view point. This implies rich properties of vertex operator algebras. Recently investigation of vertex operator algebras as modules of their subalgebras isomorphic to a tensor product $\otimes_{i=1}^{n} L(c_i, 0)$ of Virasoro vertex operator algebras has been done by several authors. Along this line Miyamoto [M2] constructed a series of vertex operator algebras by combining the minimal vertex operator super algebra $L(\frac{1}{2},0) \oplus L(\frac{1}{2},\frac{1}{2})$ and even binary codes.

In this article we construct vertex operator algebras associated with self orthogonal ternary codes. In order to obtain the vertex operator super algebra $L(\frac{1}{2},0) \oplus L(\frac{1}{2},\frac{1}{2})$, a lattice of rank one generated by an element a such that $\langle a, a\rangle = 1$ is considered in [M2]. Here we begin with a lattice $L = \sqrt{2}(A_2\text{-lattice})$. It is known [DLMN] that the vertex operator algebra V_L contains three mutually orthogonal conformal vectors with central charge $\frac{1}{2}$, $\frac{7}{10}$, and $\frac{4}{5}$ respectively, and the Virasoro element of V_L is the sum of these conformal vectors. These conformal vectors generate a subalgebra T isomorphic to $L(\frac{1}{2},0) \otimes L(\frac{7}{10},0) \otimes L(\frac{4}{5},0)$. Inspecting the action of T we obtain a vertex operator algebra isomorphic to $L(\frac{4}{5},0) \oplus L(\frac{4}{5},3)$ and two of its modules, both of which is isomorphic to $L(\frac{4}{5},\frac{2}{3})$. Combining them with a self orthogonal ternary code, we construct a vertex operator algebra.

The article is organized as follows. In Section 2 we start from a $\sqrt{2}(A_2\text{-lattice})$ L and its cosets in the dual lattice $L^{\perp}$ of L. For a self orthogonal ternary code D, we define a positive definite doubly even lattice Γ_D from these cosets. In Section 3 we review the definition of the Fock space $V_{L^{\perp}}$ and vertex operators $Y(\cdot, z)$. Then in Section 4 we construct a vertex operator.algebra M_D associated with the code D. Finally, in Section 5 we discuss briefly the Griess algebra and its automorphisms of M_D.

2 Lattice Γ_D

We begin with a set of fundamental roots $\{\alpha_1, \alpha_2\}$ of type A_2 with an inner product $\langle \cdot, \cdot \rangle$ such that $\langle \alpha_i, \alpha_i \rangle = 2$ and $\langle \alpha_1, \alpha_2 \rangle = -1$. The root system of type A_2 is $\{\pm\alpha_1, \pm\alpha_2, \pm\alpha_3\}$ with $\alpha_3 = \alpha_1 + \alpha_2$. Let $L = \mathbb{Z}\alpha_1^{\bullet} + \mathbb{Z}\alpha_2^{\bullet}$ be a $\sqrt{2}(A_2\text{-lattice})$, where $\alpha_i^{\bullet} = \sqrt{2}\alpha_i$. For simplicity, we simetimes write $x = \alpha_1^*$ and $y = \alpha_2^*$. The dual lattice

$$L^\perp = \{\alpha \in \mathbb{Q} \otimes_\mathbb{Z} L \,|\, \langle \alpha, L\rangle \subset \mathbb{Z}\}$$

of L has the dual basis $\{\frac{2x+y}{6}, \frac{x+2y}{6}\}$ of the basis $\{x, y\}$ of L, and L has 12 cosets in $L^\perp$. Among them we choose the following three cosets, which are contained in $2L^\perp$.

$$L^0 = L, \quad L^1 = \frac{-x+y}{3} + L, \quad L^2 = \frac{x-y}{3} + L.$$

In fact, $2L^\perp = L^0 \cup L^1 \cup L^2$ and the quotient group $2L^\perp/L = \{L^0, L^1, L^2\}$ is of order 3.

Let D be a ternary code of length n. For each codeword $\delta = (d_1, \ldots, d_n)$, we assign a subset L_δ of the orthogonal sum of n copies of the dual lattice $L^\perp$;

$$L_\delta = L^{d_1} \oplus \cdots \oplus L^{d_n} \subset (L^\perp)^n.$$

Then since $L^i + L^j = L^{i+j}$ for $i, j \in \{0, 1, 2\}$ and D is closed under addition, the union

$$\Gamma_D = \cup_{\delta \in D} L_\delta$$

of all L_δ ; $\delta \in D$ is a sublattice of $(L^\perp)^n$. Note that Γ_D contains $L_{(0,\ldots,0)} = L \oplus \cdots \oplus L$. Since $\langle x, x\rangle = \langle y, y\rangle = 4$ and $\langle x, y\rangle = -2$, it follows that $\langle \alpha, \alpha\rangle \in 4\mathbb{Z}$ if $\alpha \in L^0$ and $\langle \alpha, \alpha\rangle \in \frac{4}{3} + 4\mathbb{Z}$ if $\alpha \in L^1 \cup L^2$. Hence we have

Lemma 2.1 *If D is a self orthogonal ternary code of length n, then Γ_D is a doubly even lattice of rank $2n$, that is $\langle \alpha, \alpha\rangle \in 4\mathbb{Z}$ for $\alpha \in \Gamma_D$ and in particular $\langle \alpha, \beta\rangle \in 2\mathbb{Z}$ for $\alpha, \beta \in \Gamma_D$.*

Note that $\langle \alpha, \beta\rangle \in \frac{4}{3}dg + 2\mathbb{Z}$ if $\alpha \in L^d$ and $\beta \in L^g$ for $d, g \in \{0, 1, 2\}$. Let $\delta = (d_1, \ldots, d_n)$ and $\gamma = (g_1, \ldots, g_n)$ be two codewords of D and choose $\alpha^i \in L^{d_i}$, $\beta^i \in L^{g_i}$. Denote by $\tilde{\alpha}$ and $\bar{\beta}$ the elements $(\alpha^1, \ldots, \alpha^n)$ of L_δ and $(\beta^1, \ldots, \beta^n)$ of L_γ respectively. Then

$$\langle \tilde{\alpha}, \bar{\beta}\rangle = \sum_{i=1}^{n} \langle \alpha^i, \beta^i\rangle \equiv \frac{4}{3}\delta \cdot \gamma \mod 2\mathbb{Z}, \tag{2.1}$$

where $\delta \cdot \gamma = d_1 g_1 + \cdots + d_n g_n$.

Example 2.2 *If $n = 3$ and $D = \{(0,0,0), \pm(1,1,1)\}$, then $\Gamma_D = \sqrt{2}\,(E_6$-lattice). In fact,*

$$-x^i - y^i, \quad x^i;\ i = 1,2,3, \quad \frac{-x^1+y^1}{3} + \frac{-x^2+y^2}{3} + \frac{-x^3+y^3}{3}$$

form the extended Dynkin diagram of type E_6.

Example 2.3 *If $n = 4$ and let*

$$D = C_4 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{bmatrix}$$

be the [4, 2, 3] *ternary tetracode. The codewords are*

$$(0,0,0,0),\quad \pm(1,1,1,0),\quad \pm(1,-1,0,1),\quad \pm(-1,0,1,1),\quad \pm(0,1,-1,1).$$

Then $\Gamma_D = \sqrt{2}\,(E_8\text{-lattice})$ *and*

$$-x^1-y^1,\quad x^1,\quad \frac{-x^1+y^1}{3}+\frac{-x^2+y^2}{3}+\frac{-x^3+y^3}{3},\quad x^3,\quad x^2,$$

$$-x^2-y^2,\quad \frac{x^2+2y^2}{3}+\frac{-x^3-2y^3}{3}+\frac{x^4-y^4}{3},\quad -x^4,\quad x^4+y^4$$

form the extended Dynkin diagram of type E_8. *Here we write* x^i *and* y^i *for* x *and* y *of* i*-th copy of* $L^\perp$ *in the orthogonal sum* $(L^\perp)^n$.

3 Vertex operator $Y(\cdot\,,z)$

We shall consider the Fock space $V_{L^\perp}$ associated with the lattice $L^\perp$ and the vertex operator $Y(v,z)=\sum_{n\in\mathbf{Q}} v_n z^{-n-1} \in (\operatorname{End} V_{L^\perp})\{z\}$ for $v \in V_{L^\perp}$ as in [D, Section 2], [DL, Section 3], [FLM, Chapters 4, 7, 8]. We also consider the subspaces $V^0=V_L$, $V^1=V_{L^1}$ and $V^2=V_{L^2}$ of $V_{L^\perp}$ associated with the cosets $L^0=L$, L^1, and L^2 of L in $L^\perp$. Then (V^0,Y) is a vertex operator algebra associated with the positive definite even, in fact doubly even lattice L, and V^1 and V^2 are irreducible modules for the vertex operator algebra V^0.

For convenience we shall review the definition and some basic properties briefly. We tend to follow [D], [DL], and [FLM]. Here we deal with only the case where the associated commutator map $c_0(\cdot,\cdot)=0$. Thus we do not consider a central extension of $L^\perp$ or a twisted group ring $\mathbb{C}\{L^\perp\}$. Instead, we use the group algebra $\mathbb{C}[L^\perp]$ of $L^\perp$ as a multiplicative group with basis e^α; $\alpha \in L^\perp$ and multiplication $e^\alpha e^\beta = e^{\alpha+\beta}$. View $\mathfrak{h}=\mathbb{C}\otimes_{\mathbf{Z}} L = \mathbb{C}\otimes_{\mathbf{Z}} L^\perp$ as an abelian Lie algebra and form its affine Lie algebra

$$\tilde{\mathfrak{h}} = \oplus_{n\in\mathbf{Z}}(\mathfrak{h}\otimes t^n)\oplus \mathbb{C}c \oplus \mathbb{C}d.$$

Take its Heisenberg subalgebra

$$\hat{\mathfrak{h}}_{\mathbf{Z}} = \oplus_{0\neq n\in\mathbf{Z}}(\mathfrak{h}\otimes t^n)\oplus \mathbb{C}c.$$

It has a decomposition of the form

$$\hat{\mathfrak{h}}_{\mathbf{Z}} = \hat{\mathfrak{h}}_{\mathbf{Z}}^- \oplus \mathbb{C}c \oplus \hat{\mathfrak{h}}_{\mathbf{Z}}^+$$

with $\hat{\mathfrak{h}}_{\mathbf{Z}}^- = \oplus_{n<0}(\mathfrak{h}\otimes t^n)$ and $\hat{\mathfrak{h}}_{\mathbf{Z}}^+ = \oplus_{n>0}(\mathfrak{h}\otimes t^n)$.

Let $M(1)$ be the induced $\hat{\mathfrak{h}}_{\mathbf{Z}}$-module induced from the one dimentional $\mathbb{C}c\oplus\hat{\mathfrak{h}}_{\mathbf{Z}}^+$-module such that $(\alpha\otimes t^n)\cdot 1 = 0$ for $n>0$ and $c\cdot 1 = 1$. As a vector space $M(1)$ is naturally isomorphic to the symmetric algebra $S(\hat{\mathfrak{h}}_{\mathbf{Z}}^-)$ on $\hat{\mathfrak{h}}_{\mathbf{Z}}^-$. Under this isomorphism we shall identify $M(1)$ with $S(\hat{\mathfrak{h}}_{\mathbf{Z}}^-)$. Denote the action of $\alpha\otimes t^n$ on $S(\hat{\mathfrak{h}}_{\mathbf{Z}}^-)$ by $\alpha(n)$. Then

$$[\alpha(m),\,\beta(n)] = \langle\alpha,\beta\rangle m\delta_{m+n,0}.$$

By the definition c acts on $S(\hat{\mathfrak{h}}_{\mathbf{Z}}^{-})$ as the identity.

The Fock space is the tensor product of two vector spaces $V_{L^\perp} = S(\hat{\mathfrak{h}}_{\mathbf{Z}}^{-}) \otimes \mathbb{C}[L^\perp]$. It is $\mathbb{Q}$-graded by the weight, where the weight is defined by

$$\mathrm{wt}\,\alpha(-n) = n \quad \text{and} \quad \mathrm{wt}\, e^\alpha = \langle \alpha, \alpha \rangle / 2.$$

For a subset M of $L^\perp$, let $V_M = S(\hat{\mathfrak{h}}_{\mathbf{Z}}^{-}) \otimes \mathbb{C}[M]$, where $\mathbb{C}[M]$ denotes the subspace of $\mathbb{C}[L^\perp]$ spanned by e^α; $\alpha \in M$. For simplicity we set $V^i = V_{L^i}$; $i = 0, 1, 2$. Then we have $V_{2L^\perp} = V^0 \otimes V^1 \otimes V^2$.

The vertex operator $Y(e^\alpha, z)$ for e^α; $\alpha \in L^\perp$ is defined to be

$$Y(e^\alpha, z) = E^-(-\alpha, z) E^+(-\alpha, z) e^\alpha z^\alpha \in (\mathrm{End}\, V_{L^\perp})\{z\},$$

where

$$E^\pm(\alpha, z) = \exp\Big(\sum_{n \in \pm\mathbf{Z}_{>0}} \frac{\alpha(n)}{n} z^{-n} \Big)$$

and the action of c, $\alpha \otimes t^n$, e^α, z^α on $V_{L^\perp}$ is as follows. For $u \in S(\hat{\mathfrak{h}}_{\mathbf{Z}}^{-})$ and $\beta \in L^\perp$,

$$\begin{aligned} c &: u \otimes e^\beta \longmapsto u \otimes e^\beta, \\ \alpha \otimes t^n = \alpha(n) &: u \otimes e^\beta \longmapsto (\alpha(n) u) \otimes e^\beta \quad \text{for} \quad n \neq 0, \\ \alpha \otimes t^0 = \alpha(0) &: u \otimes e^\beta \longmapsto \langle \alpha, \beta \rangle u \otimes e^\beta, \\ e^\alpha &: u \otimes e^\beta \longmapsto u \otimes e^{\alpha+\beta}, \\ z^\alpha &: u \otimes e^\beta \longmapsto z^{\langle \alpha, \beta \rangle} u \otimes e^\beta. \end{aligned} \tag{3.1}$$

For $\alpha \in L^\perp$, let

$$\alpha(z) = \sum_{n \in \mathbf{Z}} \alpha(n) z^{-n-1} = \alpha(z)^- + \alpha(z)^+$$

with

$$\alpha(z)^- = \sum_{n<0} \alpha(n) z^{-n-1} \quad \text{and} \quad \alpha(z)^+ = \sum_{n \geq 0} \alpha(n) z^{-n-1}.$$

Denote by : : the normal ordered product

$$: \alpha(z) X(z) : = \alpha(z)^- X(z) + X(z) \alpha(z)^+,$$

where $X(z) \in (\mathrm{End}\, V_{L^\perp})\{z\}$. The meaning is that the operators $\alpha(n)$ for all nonnegative integers n are to be placed to the right of $X(z)$. For a general element $v = \alpha^1(-n_1) \cdots \alpha^k(-n_k) \otimes e^\alpha$ of $V_{L^\perp}$, the vertex operator $Y(v, z) \in (\mathrm{End}\, V_{L^\perp})\{z\}$ is defined by

$$\begin{aligned} Y(v, z) = : &\left(\frac{1}{(n_1 - 1)!} \left(\frac{d}{dz} \right)^{n_1 - 1} \alpha^1(z) \right) \cdots \\ &\cdots \left(\frac{1}{(n_k - 1)!} \left(\frac{d}{dz} \right)^{n_k - 1} \alpha^k(z) \right) Y(e^\alpha, z) : . \end{aligned} \tag{3.2}$$

Since $\langle L^\perp, L^\perp\rangle \subset \frac{1}{6}\mathbb{Z}$, we can expand $Y(v,z)$ in the form of

$$Y(v,z) = \sum_{n\in\frac{1}{6}\mathbb{Z}} v_n z^{-n-1}$$

with $v_n \in \mathrm{End}\, V_{L^\perp}$, which is called a component operator. Moreover, since $\langle L, 2L^\perp\rangle \subset 2\mathbb{Z}$, $\langle L^i, L^j\rangle \subset \frac{1}{3}\mathbb{Z}$, and $L^i + L^j = L^{i+j}$, we have

$$Y(u,z)v = \begin{cases} \sum_{n\in\mathbb{Z}} u_n v z^{-n-1} & \text{with} \quad u_n v \in V^i \quad \text{for} \quad u \in V^0, v \in V^i, \\ \sum_{n\in\frac{1}{3}\mathbb{Z}} u_n v z^{-n-1} & \text{with} \quad u_n v \in V^{i+j} \quad \text{for} \quad u \in V^i, v \in V^j. \end{cases} \tag{3.3}$$

Here the superscript $i+j$ is considered to be modulo 3.

The Jacobi identity [DL, (5.11)] gives

$$z_0^{-1}\delta\left(\frac{z_1 - z_2}{z_0}\right) Y(u,z_1)Y(v,z_2)w - z_0^{-1}\delta\left(\frac{-z_2 + z_1}{z_0}\right) Y(v,z_2)Y(u,z_1)w$$
$$= z_2^{-1}\delta\left(\frac{z_1 - z_0}{z_2}\right) Y(Y(u,z_0)v, z_2)w \tag{3.4}$$

for $u \in V^0$ and $v, w \in V_{2L^\perp}$.

Taking Res_{z_0} of the above identity and using

$$z_2^{-1}\delta\left(\frac{z_1 - z_0}{z_2}\right) = z_1^{-1}\delta\left(\frac{z_2 + z_0}{z_1}\right),$$

we obtain a useful formula

$$u_m v_n w - v_n u_m w = \sum_{i=0}^{\infty} \binom{m}{i} (u_i v)_{m+n-i} w \tag{3.5}$$

for $m \in \mathbb{Z}$ and $n \in \frac{1}{3}\mathbb{Z}$.

As a summary we have

Lemma 3.1 *(V^0, Y) is a vertex operator algebra associated with the positive definite even lattice L whose Virasoro element is*

$$\omega = \frac{1}{6}(\alpha_1(-1)^2 + \alpha_2(-1)^2 + \alpha_3(-1)^2),$$

(V^1, Y) and (V^2, Y) are V^0-modules, and

$$\begin{aligned} Y(\cdot, z):\ & V^i \longrightarrow Hom(V^j, V^{i+j})\{z\} \\ & v \longmapsto Y(v,z)|_{V^j} = \textstyle\sum_{n\in\frac{1}{3}\mathbb{Z}} v_n|_{V^j} z^{-n-1} \end{aligned} \tag{3.6}$$

is an intertwining operator of type $\binom{V^{i+j}}{V^i \quad V^j}$.

Let D be a self orthogonal ternary code of length n. For each codeword $\delta = (d_1, \dots, d_n)$ we assign the tensor product $V_\delta = V^{d_1} \otimes \cdots \otimes V^{d_n}$ of vector spaces. For $v^i \in V^{d_i}$, define the tensor product vertex operator

$$Y(v^1 \otimes \cdots \otimes v^n, z) = Y(v^1, z) \otimes \cdots \otimes Y(v^n, z)$$

as in [DL], [FHL]. Set $V_D = \oplus_{\delta \in D} V_\delta$. Then (V_D, Y) is a vertex operator algebra. In fact, it is identical with the vertex operator algebra V_{Γ_D} associated with the positive definite doubly even lattice Γ_D of Section 2.

We shall make some remark. For α, $\beta \in L^\perp$, set

$$S(\alpha, \beta, z_1, z_2) = E^-(-\alpha, z_1)E^-(-\beta, z_2)E^+(-\alpha, z_1)E^+(-\beta, z_2)e^{\alpha+\beta}z_1^\alpha z_2^\beta.$$

Then we have

$$\begin{aligned} Y(e^\alpha, z_1)Y(e^\beta, z_2) &= S(\alpha, \beta, z_1, z_2)(z_1 - z_2)^{(\alpha,\beta)}, \\ Y(e^\beta, z_2)Y(e^\alpha, z_1) &= S(\alpha, \beta, z_1, z_2)(z_2 - z_1)^{(\alpha,\beta)}. \end{aligned}$$

in $(\operatorname{End} V_{L^\perp})\{z_1, z_2\}$. Now let $\delta = (d_1, \dots, d_n)$ and $\gamma = (g_1, \dots, g_n)$ be two codewords of D and take $\alpha^i \in L^{d_i}$, $\beta^i \in L^{g_i}$. Set $\bar{\alpha} = (\alpha^1, \dots, \alpha^n)$ and $\bar{\beta} = (\beta^1, \dots, \beta^n)$. These are elements of L_δ and L_γ respectively. We also set $e^{\bar{\alpha}} = e^{\alpha^1} \otimes \cdots \otimes e^{\alpha^n}$ and $e^{\bar{\beta}} = e^{\beta^1} \otimes \cdots \otimes e^{\beta^n}$, which are elements of V_δ and V_γ respectively. Then by the definition of the tensor product vertex operator, we have

$$\begin{aligned} Y(e^{\bar{\alpha}}, z_1)Y(e^{\bar{\beta}}, z_2) &= S(\alpha^1, \beta^1, z_1, z_2) \otimes \cdots \otimes S(\alpha^n, \beta^n, z_1, z_2)(z_1 - z_2)^{(\bar{\alpha},\bar{\beta})}, \\ Y(e^{\bar{\beta}}, z_2)Y(e^{\bar{\alpha}}, z_1) &= S(\alpha^1, \beta^1, z_1, z_2) \otimes \cdots \otimes S(\alpha^n, \beta^n, z_1, z_2)(z_2 - z_1)^{(\bar{\alpha},\bar{\beta})}. \end{aligned}$$

Since $\langle \bar{\alpha}, \bar{\beta} \rangle \equiv \frac{4}{3}\delta \cdot \gamma \mod 2\mathbb{Z}$ by (2.1), $\langle \bar{\alpha}, \bar{\beta} \rangle$ is an even integer if the two codewords δ and γ are orthogonal. Thus if δ and γ are orthogonal, then

$$(z_1 - z_2)^N Y(e^{\bar{\alpha}}, z_1)Y(e^{\bar{\beta}}, z_2) = (z_1 - z_2)^N Y(e^{\bar{\beta}}, z_2)Y(e^{\bar{\alpha}}, z_1)$$

for some nonnegative integer N, that is $Y(e^{\bar{\alpha}}, z_1)$ and $Y(e^{\bar{\beta}}, z_2)$ are mutually local ([L]).

4 Vertex operator algebra M_D

We shall construct a subalgebra M_D of the vertex operator algebra V_D of the preceding section.

By [DLMN], the Virasoro element ω of V^0 decomposes into a sum of three mutually orthogonal conformal vectors

$$\begin{aligned} \omega^1 &= \tfrac{1}{8}\alpha_1(-1)^2 - \tfrac{1}{4}x_{\alpha_1}, \\ \omega^2 &= \tfrac{1}{40}(-\alpha_1(-1)^2 + 4\alpha_2(-1)^2 + 4\alpha_3(-1)^2) - \tfrac{1}{20}(-x_{\alpha_1} + 4x_{\alpha_2} + 4x_{\alpha_3}), \\ \omega^3 &= \tfrac{1}{15}(\alpha_1(-1)^2 + \alpha_2(-1)^2 + \alpha_3(-1)^2) + \tfrac{1}{5}(x_{\alpha_1} + x_{\alpha_2} + x_{\alpha_3}), \end{aligned}$$

where $x_{\alpha_i} = e^{\alpha_i^\circ} + e^{-\alpha_i^\circ}$. The central charge $c(\omega^i)$ of the conformal vector ω^i is

$$c(\omega^1) = \frac{1}{2}, \quad c(\omega^2) = \frac{7}{10}, \quad c(\omega^3) = \frac{4}{5},$$

and the central charge of ω is $c(\omega) = 2$.

Each conformal vector generates a Virasoro vertex operator algebra

$$\mathrm{Vir}(\omega^i) = \mathrm{span}\,\{\omega^i_n 1 \,|\, n \in \mathbb{Z}_{<0}\} \cong L(c(\omega^i), 0),$$

and V^0 contains the subalgebra

$$T = \mathrm{Vir}(\omega^1) \otimes \mathrm{Vir}(\omega^2) \otimes \mathrm{Vir}(\omega^3) \cong L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \otimes L(\frac{4}{5}, 0).$$

As T-modules, V^i's are completely reducible and each irreducible summand is of the form

$$L(\frac{1}{2}, h_1) \otimes L(\frac{7}{10}, h_2) \otimes L(\frac{4}{5}, h_3),$$

where

$$\begin{aligned} h_1 &\in \{0, \frac{1}{16}, \frac{1}{2}\}, \\ h_2 &\in \{0, \frac{3}{80}, \frac{1}{10}, \frac{7}{16}, \frac{3}{5}, \frac{3}{2}\}, \\ h_3 &\in \{0, \frac{1}{40}, \frac{1}{15}, \frac{1}{8}, \frac{2}{5}, \frac{21}{40}, \frac{2}{3}, \frac{7}{5}, \frac{13}{8}, 3\}, \end{aligned} \qquad (4.1)$$

(see [DMZ], [W]).

The weights of such an irreducible T-module are $h_1 + h_2 + h_3 + n$ with $n \in \mathbb{Z}_{\geq 0}$. In particular, its minimal weight is $h_1 + h_2 + h_3$. More precisely, if a^i is a homogeneous element of $L(c(\omega^i), h_i)$ of weight $h_i + n_i$ with $n_i \in \mathbb{Z}_{\geq 0}$, then $a^1 \otimes a^2 \otimes a^3$ is of weight $h_1 + h_2 + h_3 + n_1 + n_2 + n_3$ and it is an eigenvector of ω^i_1 with eigenvalue $h_i + n_i$.

Calculating the eigenvalues of the action of ω^i_1; $i = 1, 2, 3$ on the weight subspace $(V^0)_{(n)}$ of V^0 of weight $n \leq 3$, we have

Lemma 4.1 *V^0 has the following irreducible T-submodules as direct summands, each of which is of multiplicity one.*

$$\begin{array}{ll} L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \otimes L(\frac{4}{5}, 0), & L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, \frac{3}{5}) \otimes L(\frac{4}{5}, \frac{2}{5}), \\ L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{1}{10}) \otimes L(\frac{4}{5}, \frac{2}{5}), & L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, \frac{3}{5}) \otimes L(\frac{4}{5}, \frac{7}{5}), \\ L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{1}{10}) \otimes L(\frac{4}{5}, \frac{7}{5}), & L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{3}{2}) \otimes L(\frac{4}{5}, 0), \\ L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \otimes L(\frac{4}{5}, 3). & \end{array}$$

The minimal weight of any other direct summand is greater than 3.

Similarly we have

Lemma 4.2 *V^1 has the following irreducible T-submodules as direct summands, each of which is of multiplicity one.*

$$\begin{array}{ll} L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \otimes L(\frac{4}{5}, \frac{2}{3}), & L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, \frac{3}{5}) \otimes L(\frac{4}{5}, \frac{1}{15}), \\ L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{1}{10}) \otimes L(\frac{4}{5}, \frac{1}{15}). & \end{array}$$

The minimal weight of any other direct summand is greater than $\frac{2}{3}$.

The decomposition of V^2 into the direct sum of irreducible T-submodules is the same as that of V^1.

We shall extract a subalgebra from V^0 and also its submodules from V^1 and V^2.

Theorem 4.3 *Set $M^i = \{v \in V^i \,|\, \omega_1^1 v = \omega_1^2 v = 0\}$. Then*

(1) $M^0 = \mathbf{1}_{L(\frac{1}{2},0)} \otimes \mathbf{1}_{L(\frac{7}{10},0)} \otimes (L(\frac{4}{5},0) \oplus L(\frac{4}{5},3))$. *The weight 2 subspace of M^0 is spanned by $\mathbf{v}^0 = \omega^3$.*

(2) $M^1 = \mathbf{1}_{L(\frac{1}{2},0)} \otimes \mathbf{1}_{L(\frac{7}{10},0)} \otimes L(\frac{4}{5},\frac{2}{3})$. *The weight $\frac{2}{3}$ subspace of M^1 is spanned by*

$$\mathbf{v}^1 = e^{\frac{-x+y}{3}} + e^{\frac{2x+y}{3}} + e^{\frac{-x-2y}{3}}.$$

(3) $M^2 = \mathbf{1}_{L(\frac{1}{2},0)} \otimes \mathbf{1}_{L(\frac{7}{10},0)} \otimes L(\frac{4}{5},\frac{2}{3})$. *The weight $\frac{2}{3}$ subspace of M^2 is spanned by*

$$\mathbf{v}^2 = e^{\frac{x-y}{3}} + e^{\frac{x+2y}{3}} + e^{\frac{-2x-y}{3}}.$$

Here $\mathbf{1}_{L(c,0)}$ denotes the vacuum element of $L(c,0)$.

Proof Decompose V^i into the direct sum of irreducible T-submodules and consider the action of ω_1^1 and ω_1^2 on each direct summand. It follows that M^i is a direct sum of subspaces of the form $\mathbf{1}_{L(\frac{1}{2},0)} \otimes \mathbf{1}_{L(\frac{7}{10},0)} \otimes L(\frac{4}{5},h_3)$ with h_3 as in (4.1). The weights of V^0 are nonnegative integers, so we have (1) by Lemma 4.1. Similarly the weights of V^1 and V^2 are in $\frac{2}{3} + \mathbb{Z}_{\geq 0}$, and so (2) and (3) follow from Lemma 4.2. □

Theorem 4.4 (1) *$u_n v \in M^{i+j}$ for $u \in M^i$ and $v \in M^j$.*

(2) *(M^0, Y) is a subalgebra of the vertex operator algebra (V^0, Y) with the Virasoro element ω^3, M^1 and M^2 are M^0-modules, and*

$$\begin{aligned} Y(\cdot, z):\ & M^i \longrightarrow Hom(M^j, M^{i+j})\{z\} \\ & v \longmapsto Y(v,z)|_{M^j} = \textstyle\sum_{n \in \frac{1}{3}\mathbb{Z}} v_n|_{M^j} z^{-n-1} \end{aligned} \tag{4.2}$$

is an intertwining operator of type $\begin{pmatrix} & M^{i+j} & \\ M^i & & M^j \end{pmatrix}$.

Proof The second assertion follows from the first assertion and Lemma 3.1, so it is sufficient to show the first assertion. This can be done by the same argument as in the proof of [M1, Proposition 4.9]. Take $u \in M^i$ and $v \in M^j$. Then $\omega_1^1 u = \omega_1^1 v = 0$. Moreover, Theorem 4.3 implies $\omega_0^1 u = 0$. Hence

$$\begin{aligned} \omega_1^1 u_n v &= \omega_1^1 u_n v - u_n \omega_1^1 v \\ &= (\omega_0^1 u)_{n+1} v + (\omega_1^1 u)_n v \\ &= 0 \end{aligned}$$

by (3.5). Similarly $\omega_1^2 u_n v = 0$. Since $u_n v \in V^{i+j}$, we conclude that $u_n v \in M^{i+j}$. □

Let D be a self orthogonal ternary code of length n. Using M^0, M^1, and M^2 in place of V^0, V^1, and V^2 we obtain a subalgebra (M_D, Y) of the vertex operator algebra (V_D, Y), namely, for each codeword $\delta = (d_1, \ldots, d_n)$ we assign the tensor product $M_\delta =$

$M^{d_1} \otimes \cdots \otimes M^{d_n}$ and set $M_D = \oplus_{\delta \in D} M_\delta$. Then it follows from Theorem 4.4 (1) that the subspace M_D of V_D is closed under component operators of every element of M_D. In the case of $\delta = (0, \ldots, 0)$, M_δ contains an element u^i whose i-th entry is v^0 and the other entries are the vacuum $\mathbf{1}$ of M^0 ;

$$u^i = \mathbf{1} \otimes \cdots \otimes \mathbf{1} \otimes \mathrm{v}^0 \otimes \mathbf{1} \otimes \cdots \otimes \mathbf{1}. \tag{4.3}$$

Set $\hat{\omega} = u^1 + u^2 + \cdots + u^n$. Then

Theorem 4.5 *M_D is a vertex operator algebra with the Virasoro element $\hat{\omega}$.*

5 Griess algebra of M_D

Let v^0, v^1, and v^2 be as in Theorem 4.3. For a self orthogonal ternary code D of length n, the Griess algebra , that is the weight 2 subspace $(M_D)_{(2)}$ of the vertex operator algebra M_D is of dimension $n + k$, where k denotes the number of codewords of weight 3. Let $u^1, \ldots, u^n$ be as in (4.3). For a codeword $\delta = (d_1, \ldots, d_n)$ of weight 3, let

$$x^\delta = x^{d_1} \otimes \cdots \otimes x^{d_n} \in M_\delta,$$

where x^{d_i} denotes the vacuume $\mathbf{1}$ of M^0 if $d_i = 0$ and $x^{d_i} = \mathrm{v}^{d_i}$ if $d_i = 1$ or 2. Then $u^1, \ldots, u^n$ and x^δ with δ being over all cordwords of weight 3, form a basis of the Griess algebra.

To determine the product and the inner product of the Griess algebra of M_D we need to know the first several terms of $Y(\mathrm{v}^i, z)\mathrm{v}^j$. These terms are easily computed:

$$\begin{aligned}
Y(\mathrm{v}^0, z)\mathrm{v}^0 &= \tfrac{2}{5}\mathbf{1}z^{-4} + 2\mathrm{v}^0 z^{-2} + \cdots, \\
Y(\mathrm{v}^1, z)\mathrm{v}^1 &= 2\mathrm{v}^2 z^{-\frac{2}{3}} + \cdots, \\
Y(\mathrm{v}^2, z)\mathrm{v}^2 &= 2\mathrm{v}^1 z^{-\frac{2}{3}} + \cdots, \\
Y(\mathrm{v}^0, z)\mathrm{v}^i &= Y(\mathrm{v}^i, z)\mathrm{v}^0 = \tfrac{2}{3}\mathrm{v}^i z^{-2} + \cdots \quad \text{for} \quad i = 1, 2, \\
Y(\mathrm{v}^1, z)\mathrm{v}^2 &= Y(\mathrm{v}^2, z)\mathrm{v}^1 = 3\mathbf{1}z^{-\frac{4}{3}} + 5\mathrm{v}^0 z^{\frac{2}{3}} + \cdots.
\end{aligned}$$

We consider the automorphism group of the Griess algebra of M_D in the case where the code D is the $[4, 2, 3]$ ternary tetracode (see Example 2.3). In this case the Griess algebra is of dimension 12 and the product $\times$ and the inner product $\langle \cdot, \cdot \rangle$ with respect to the basis $u^1, \dots, u^4, x^\delta$ are as follows ;

$$\begin{aligned}
&u^i \times u^j = 2\delta_{ij} u^i, \\
&u^i \times x^\delta = \begin{cases} \frac{2}{3} x^\delta & \text{if} \quad d_i \neq 0, \\ 0 & \text{if} \quad d_i = 0, \end{cases} \\
&x^\delta \times x^\gamma = \begin{cases} 8x^{-\delta} & \text{if} \quad \delta = \gamma, \\ 45 \sum_{d_i \neq 0} u^i & \text{if} \quad \delta = -\gamma, \\ 6x^{\delta+\gamma} & \text{if} \quad \delta \neq \pm\gamma, \end{cases} \\
&\langle u^i, u^j \rangle = \frac{2}{5} \delta_{ij}, \\
&\langle u^i, x^\delta \rangle = 0, \\
&\langle x^\delta, x^\gamma \rangle = \begin{cases} 27 & \text{if} \quad \delta = -\gamma, \\ 0 & \text{if} \quad \delta \neq -\gamma. \end{cases}
\end{aligned}$$

From these data we have

Propositon 5.1 *Let D be the* [4,2,3] *ternary tetracode. Then the automorphism group ot the Griess algebra of M_D is isomorphic to $3^2.2S_4$, where $2S_4$ is the automorphism group of the code D and 3^2 is the coordinate automorphism group $GF(3)^4/D^\perp$.*

Here coordinate automorphisms are defined in a similar way as in [M2, Section 5].

References

[D] C. Dong, Vertex algebras associated with even lattices, *J. Algebra* **160** (1993), 245-265.

[DL] C. Dong and J. Lepowsky, *Generalized Vertex Algebras and Relative Vertex Operators*, Progress in Math., Vol. **112**, Birkhäuser, 1993.

[DMZ] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the Moonshine module, *Proc. Symp. Pure Math., Amer. Math. Soc.* **56** II (1994), 295-316.

[DLMN] C. Dong, H. Li, G. Mason and S. P. Norton, Associative subalgebras of the Griess algebra and related topics, preprint (q-alg/9607013).

[FHL] I. B. Frenkel, Y. -Z. Huang and J. Lepowsky, On axiomatic approaches to vertex operator algebras and modules, Memoirs Amer. math. Soc. **104** (1993).

[FLM] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, 1988.

[L] H. -S. Li, Local system of vertex operators, vertex superalgebras and modules, *J. Pure Appl. Alg.*, **109** (1996), 143-195.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 523-548.

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra* **181** (1996), 207-222.

[W] W. Wang, Rationality of Virasoro vertex operator algebras, *Duke Math. J. IMRN*, **71** (1993), 197-211.

On the characterization of certain Cayley graphs

Norio YAMAZAKI*
Kyushu University
(email address: norio@math.kyushu-u.ac.jp)

About two years ago, M. Tomiyama and I have succeeded in [2, 3] the characterization of the group association scheme of the symmetric group $\mathcal{X}(S_n)$ for all n except 4. Roughly speaking, the proof was obtained by proceeding in 3 steps as follows;

(i) We show the non-existence of some configuration of 4 vertices,

(ii) We show the uniqueness of the relation graph Γ corresponding to the conjugacy class of transposition,

(iii) We determine the other relations. (This step is immediately obtained.)

The essential part of this proof is of step (ii). This is divided into two parts: the determination of the local structure, and the determination of global structure from the local structure. Viewing these proofs, we can see that these are independent each other. So it seems to be natural to try to generalize the techniques used in these, separately.

Recentry, Tomiyama [1] had a generalization of the part on the local structure. Namely, under the assumption similar to the one in (i) above, the local structures of the group scheme of almost simple 3-transposition groups (for example, the Weyl groups of type E_i with $i = 6, 7, 8$, the symplectic groups $Sp_{2m}(2)$ with $m \geq 2$, and the orthogonal groups $O^{\epsilon}_{2m}(2)$ with $\epsilon \in \{+, -\}$ and $m \geq 2$) were determined by the intersection numbers. In this proof the characterization result of Fischer spaces by H. Cuypers and J. Hall is used. In fact, in order to get it, we don't need information of all intersection numbers. We only need a condition on the graph distribution of the induced subgraph (of Γ) whose vertex set is of vertices at distance at most 3 from any vertex. See Condition B written later. (In fact, the assumption in [1] is slightly weaker.)

In the following, we shall investigate the graphs having such local structure.

We shall review the proof of the determination of the whole structure of Γ from the local structure in [2].

Let $\tilde{\Gamma} = (S_n, D)$ be the Cayley graph with respect to the set D of all transpositions in S_n, which is just the same as the relation graph corresponding to the conjugacy class D by definition of the group scheme, and let $\Gamma = (V, E)$ be a graph having the same graph distribution (with respect to any vertex) as of $\tilde{\Gamma}$. Note that these two graphs have the common valency and diameter, and that both are bipartite. Let d be the diameter of

*This manuscript was written during this author's visit at the Imperial College of London by the support of the Japan Society for Promotion of Science. (email: n.yamazaki@ic.ac.uk) these two graph. For $g \in S_n$, $x \in V$, and an integer i with $0 \leq i \leq d$, let $\Gamma_i(x)$ (resp. $\tilde{\Gamma}_i(g)$) be the set of all vertices at distance i from x (resp. g). Let $\Gamma_{\leq i}(x) = \cup_{0 \leq j \leq i}(\Gamma_j(x))$, and $\tilde{\Gamma}_{\leq i}(x) = \cup_{0 \leq j \leq i}(\tilde{\Gamma}_j(g))$.

In [2], we construct the graph isomorphism from $\tilde{\Gamma}$ to Γ. (This is the claim of the latter part of step (ii).) More precisely, at first we pick any vertex x in Γ, define $f_0(id) = x$ where id is the identity in S_n, and inductively we construct bijections

$$f_r : \tilde{\Gamma}_{\leq r}(id) \longrightarrow \Gamma_{\leq r}(x)$$

which satisfy the following conditions (I), (II);

(I) If $g \in \tilde{\Gamma}_{\leq r-1}(id)$, then $f_r(g) = f_{r-1}(g)$,

(II) For $g \in \tilde{\Gamma}_{i-1}(id)$ and $h \in \tilde{\Gamma}_i(id)$ with $i \leq r$, g and h are adjacent in $\tilde{\Gamma}$ iff $f_r(g)$ and $f_r(h)$ are adjacent in Γ.

Note that the existence of the map f_1 is guaranteed by step (ii) mentioned in the begining of this paper.

The above method to constract the graph isomorphism seems not to be general. Because in this proof, we check the existence of the maps by labelling permutations of n-letters (i.e., elements of S_n) for vertices of Γ. What method is more general?

Now we prepare some notation.

For a graph Γ, if vertices x, y are adjacent in Γ, we write $x \sim y$. Define the relations R_t's with $t \in \{(1), (2), (2 \times 2), (3), (2 \times 2 \times 2), (2 \times 3), (4)\}$ as the following:

$$\begin{array}{ll}
R_{(1)} = & \{(x,x) \mid x \in \Gamma\}, \\
R_{(2)} = & \{(x,y) \in \Gamma \times \Gamma \mid x \sim y\}, \\
R_{(2\times 2)} = & \{(x,y) \in \Gamma \times \Gamma \mid \partial(x,y) = 2, |R_{(2)}(x) \cap R_{(2)}(y)| = 2\}, \\
R_{(3)} = & \{(x,y) \in \Gamma \times \Gamma \mid \partial(x,y) = 2, |R_{(2)}(x) \cap R_{(2)}(y)| = 3\}, \\
R_{(2\times 2\times 2)} = & \{(x,y) \in \Gamma \times \Gamma \mid \partial(x,y) = 3, |\Gamma_2(x) \cap R_{(2)}(y)| = 3, \\
 & |R_{(2\times 2)}(x) \cap R_{(2)}(y)| = 3\}, \\
R_{(2\times 3)} = & \{(x,y) \in \Gamma \times \Gamma \mid \partial(x,y) = 3, |\Gamma_2(x) \cap R_{(2)}(y)| = 4, \\
 & |R_{(2\times 2)}(x) \cap R_{(2)}(y)| = 3, |R_{(3)}(x) \cap R_{(2)}(y)| = 1\}, \\
R_{(4)} = & \{(x,y) \in \Gamma \times \Gamma \mid \partial(x,y) = 3, |\Gamma_2(x) \cap R_{(2)}| = 6, \\
 & |R_{(2\times 2)}(x) \cap R_{(2)}(y)| = 2, |R_{(3)}(x) \cap R_{(2)}(y)| = 4\},
\end{array}$$

where we let $R_t(x) = \{y \in \Gamma \mid (x,y) \in R_t\}$ for $x \in \Gamma$.

Let $\Lambda = \{(1), (2), (2 \times 2), (3), (2 \times 2 \times 2), (2 \times 3), (4)\}$.

We consider the following conditions:

Condition A. There exists no 4-tuple (x, y, z, u) of vertices in Γ such that $x \sim y \sim z \sim u \sim x$, $(x, z) \in R_{(2\times 2)}$, and that $(y, u) \in R_{(3)}$.

Condition B. The following hold:

(i) R_t is symmetric for $t \in \Lambda$.

(ii) There exist no triangles or pentagons.

(iii) For any $x \in \Gamma$, $\Gamma_2(x) = R_{(2\times2),(3)}(x)$ and $\Gamma_3(x) = R_{(2\times2\times2),(2\times3),(4)}(x)$.

(iv) The value $p^{t_1}_{t_2,t_3} = |R_{t_2}(x) \cap R_{t_3}(y)|$ doesn't depend on the choice of $x, y \in \Gamma$ with $(x,y) \in R_{t_1}$ for $t_2 = (2)$ and $t_1, t_3 \in \Lambda$.

By definition we see that $(p^{(2\times2)}_{(2),(2)}, p^{(3)}_{(2),(2)}, p^{(2\times2\times2)}_{(2),(2\times2)}, p^{(2\times2\times2)}_{(2),(3)}, p^{(2\times3)}_{(2),(2\times2)}, p^{(2\times3)}_{(2),(3)}, p^{(4)}_{(2),(2\times2)}, p^{(4)}_{(2),(3)}) = (2,3,3,0,3,1,2,4)$.

In fact, essentially, we have the following in [2]. (I plan to write the explicit proof of this in [4].)

Proposition. Let Γ be a graph satisfying Conditions A and B, and let

$$\begin{aligned}&(p^{(1)}_{(2),(2)}, p^{(2)}_{(2),(2\times2)}, p^{(2)}_{(2),(3)}, p^{(2\times2)}_{(2),(2\times2\times2)}, p^{(2\times2)}_{(2),(2\times3)}, p^{(2\times2)}_{(2),(4)}, p^{(3)}_{(2),(2\times2\times2)}, p^{(3)}_{(2),(2\times3)}, p^{(3)}_{(2),(4)})\\ = \ &(\tbinom{n}{2}, \tbinom{n-2}{2}, 2(n-2), \tbinom{n-4}{2}, 4(n-4), 4, 0, \tbinom{n-3}{2}, 3(n-3)).\end{aligned}$$

Then Γ is covered with the Cayley graph $\bar{\Gamma} = (S_n, D)$.

In this proof, we regard $\bar{\Gamma}$ not as the graph labelled on vertices but as the $\binom{n}{2}$-coloured graph labelled on edge by D. In general, investigating Cayley graphs, it seems more natural to label edges than to label vertices.

We can observe that $\bar{\Gamma}$ has the following important properties. These are keys of the proof of Proposition.

(1) $\bar{\Gamma}$ is bipartite. In general, the universal cover of graphs satisfying Condition B must be bipartite. Because for any graph of such family, the bipartite double also satisfies this condition.

(2) For all i with $0 \le i \le d$ and for all $x, y \in \bar{\Gamma}$ with $\bar{\partial}(x,y) = i$, there exists a minimal geodetically closed subgraph (i.e. it is unique) of diameter i containing x, y. All of these are Cayley graphs of subgroups of S_n generated by the subsets of D. This property is strongly related to the universality of $\bar{\Gamma}$. I believe that on the study of a Cayley graph with respect to a "good" generators D (for example, the conjugacy class generating the group), it is very important to investigate the Cayley subgraphs with respect to subsets of D which form geodetically closed subgraphs.

(3) Regarding $\bar{\Gamma}$ as a D-edge-labelled graph, we can see the following: For $x \in \Gamma$, let $y_1 = x \cdot a, y_2 = y_1 \cdot b, y_3 = y_2 \cdot a$ with $a, b \in D$, where $x \cdot a$ means the vertex adjacent to x by the edge labelled a. Then, since $aba \in D$, $y_3 \cdot (aba) = x$. Of course, such a situation occurs because D is the conjugacy class.

As the next problem, the following seems interesting.

Problem. Find the universal cover of the family of graphs which satisfy Conditions A and B, and which contains one of the Cayley graphs of $Sp_{2m}(2)$ or $O^{\epsilon}_{2m}(2)$.

It can be conjectured that the Cayley graphs of the Weyl groups of E_6, E_7, E_8 are the universal covers of the Cayley graphs of $O^-_6(2), Sp_6(2), O^+_8(2)$, respectively.

References

[1] M. Tomiyama, On local structures of the group association schemes of 3-trensposition groups, preprint.

[2] M. Tomiyama and N. Yamazaki, Characterization of the group association scheme of the symmetric group, to appear in Europ. J. Combin. (1997) 01, 1-19.

[3] M. Tomiyama and N. Yamazaki, On a condition of the group association scheme of the symmetric group, in preparation.

[4] N. Yamazaki, On Cayley graphs of 3-transpositions, in preparation.

The subgroup complexes for finite groups

Satoshi Yoshiara
Division of Mathematical Sciences
Osaka Kyoiku University

1. The complex of p-radicals with p-constrained normalizers

In this report I am trying to reproduce my 20 minutes talk given at International Christian University on July 17, 1997.

The aim of the report is to propose a mathematical definition for p-local geometry for every finite group, which has been constructed for sporadic finite simple groups as an analogy of buildings but in somewhat ad-hoc manner, and conversely starting from that definition to determine the "local geometries" of the sporadic groups F_3 and F_5 of Thompson and Harada for which such geometries so far have not been found.

In the following G denotes a finite group and let p be a prime divisor of the order $|G|$. A nontrivial p-subgroup P of G is called a *p-radical subgroup* whenever the largest p-normal subgroup $O_p(N_G(P))$ of its normalizer coincides with P. The set of p-radical subgroups of G is denoted by $\mathcal{B}_p(G)$.

$$\mathcal{B}_p(G) = \{P \mid 1 \neq P = O_p(N_G(P))\}$$

The chains of p-radical subgroups (with respect to inclusion) form a simplicial complex $\Delta(\mathcal{B}_p(G))$. It is an important first step for verifying the celebrated Dade conjecture in representation theory to determine the representatives of G-conjugacy classes of $\Delta(\mathcal{B}_p(G))$ for each prime divisor of $|G|$.

When G is a Chevalley group defined over a field of characteristic p, it follows from a theorem by Borel and Tits [BT],[BW] that $\mathcal{B}_p(G)$ coincides with the set of unipotent radicals of parabolic subgroups of G. Thus in this case the simplicial complex $\Delta(\mathcal{B}_p(G))$ is the barycentric division of the building associated with G.

In the conference given at Kyoto RIMS in December, 1998, I addressed the audience on the importance of a minimal complex which is G-homotopy equivalent to $\Delta(\mathcal{B}_p(G))$. Namely, if G is a group of characteristic-p type [1] , every geometry known as a p-local geometry can be obtained in this manner (See [SY]). Thus p-local geometries for simple groups of characteristic-p type are in fact analogue of buildings.

As S. D. Smith and I remarked at the end of that paper [SY], even when a group G is not of characteristic-p type, it looks interesting to consider a smaller simplicial complex $\Delta(\mathcal{B}_p^{cen}(G))$ of chains of p-radical subgroups P whose normalizer $N_G(P)$ is p-constrained [2] , not taking the whole p-radical groups.

[1] This is a notion generalizing Chevally groups defined on fields in characteristic p. Formally a finite group G is called *of characteristic-p type* whenever the generalized Fitting subgroup $F(C_G(x))$ of the centralizer of each element x of order p is a p-group.

[2] a finite group H is called *p-constrained* if the full inverse image Q of $O_p(H/O_{p'}(H))$ in H satisfies $C_H(O_p(H/O_{p'}(H))) \subseteq Q$

Note that for a group G of characteristic-p type we have $\mathcal{B}_p(G) = \mathcal{B}_p^{cen}(G)$. Thus it is natural to examine this subcomplex $\mathcal{B}_p^{cen}(G)$ when one attempts to generalize the above observation made in [SY]. Furthermore, the complex $\mathcal{B}_p^{cen}(G)$ is much easier to handle when we determine it by applying reccursive method.

Another reason why this complex is interesting is a recent result of Dwyer stating that the modulo p cohomology group of G has the alternating decomposition on that complex (see the last section of [SY]).

In this report, I furthermore claim that (minimal) complexes G-homotopy equivalent to the complex $\mathcal{B}_p^{cen}(G)$ are very much interesting geometries by illustrating with some examples. Namely, they can be thought of analogue of buildings. First we make the problem clear.

Problem 1 *For each finite simple group G and each prime divisor p of its order, find minimal complexes which are G-homotopy equivalent to the complex $\Delta(\mathcal{B}_p^{cen}(G))$.*

In the following I will describe results on some sporadic simple groups. I begin with the sporadic simple group Suz found first by Michio Suzuki, according with the aim of the conference.

2. The result for $G = Suz$ and $p = 3$

The maximal 3-local subgroups[3] of the sporadic simple group Suz of Suzuki are classified by Wilson [Wil1] and I (thesis for master dgree). There are three classes of subgroups of G of order 3, which are called $3A$, $3B$ and $3C$, accoring to the increasing order of the orders of the centralizers of representatives. The normalizers of representatives of classes $3A$ and $3C$ are of the following shapes respectively:

$$N_G(3A) \cong 3.PSU_4(3).2, \quad N_G(3C) \cong (3^2 : 4 \times A_6).2$$

Let A be a representative of the class $3A$, and let X be the largest normal 3-subgroup of the normalizer of a representative of the class $3C$. We have $X \cong 3^2$ and each subgroup of X order 3 belongs to the class $3C$.

Elementary abelian groups of order 3^2 generated by two subgroups in $3A$ are conjugate to each other, and among four subgroups of order 3 in such a 3^2-subgroup two belong to the class $3A$ and the other belong to $3B$. The normalizer of such a 3^2-subgroup is a semidirect product of a special subgroup $U \cong 3^{2+4}$ with a complement of shape $2(A_4 \times 2^2).2$.

$$N_G(U) \cong 3^{2+4} : (2(A_4 \times 2^2).2), \quad U \cong 3^{2+4}.$$

That normalizer contains the normalizer of a representative of $3B$. Furthermore, there is an elementary abelian subgroup E of order 3^5 containing twelve subgroups in the class $3A$ with normalizer a split extension of the Mathieu group M_{11} by E.

[3] maximal one with repspect to inclusion among the 3-local subgroups, that is, the noramalizers of a non-trivial 3-subgroups

$N_G(E) \cong 3^5 : M_{11}, \quad E \cong 3^5.$

It is known that the above four normalizers $N_G(A)$, $N_G(3C) = N_G(X)$, $N_G(U)$ and $N_G(E)$ consist the complete set of representatives of maximal 3-local subgroups of G. Note that among them $N_G(3C) = N_G(X)$ is the unique maximal 3-local subgroup which is not 3-constrained.

Next we will determine 3-radical subgroups using the above informations. In that process, the following simple lemma is fundamental.

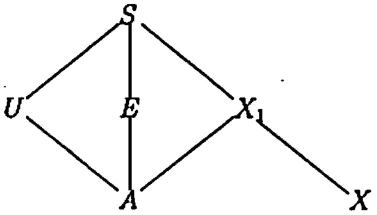
Lemma 1 (Lemma 1.9(2) in [SY]) *If the normalizer of a p-radical subgroup P of a group G is contained in a p-local subgroup; $N_G(P) \le N_G(U)$ for some p-subgroup $U \neq 1$, then either $P = U$ or P/U is a p-radical subgroup of $N_G(U)/U$.*

Using this lemma and the classification of maximal 3-local subgroups menthioned above, the problem to determine the 3-rdical groups of $G = Suz$ can be reduced to those for smaller groups $U_4(3)$, A_4, M_{11} and A_6. Eventually we can get the following result.

Result 1 *The 3-radical subgroups of the sporadic Suzuki group $G = Suz$ form the following six conjugacy classes. Among them X is the unique representative with non-3-constrained normalizer, and $\mathcal{B}_3^{\rm con}(G)$ consists of the five classes other than the class of X.*

A (a subgroup of order 3 in the class $3A$), $U \cong 3^{2+4}$, $E \cong 3^5$,
$X \cong 3^2$, $X_1 := X \times Z(U) \cong 3^4$, A Sylow subgroup S of G isomorphic to $3^5 : 3^2$.

Taking suitable represenatives, we have the following inclusion relations among them.



Thus the complex $\mathcal{B}_3(G)$ of chains of them is of dimension 2 and each simplex has one of the following 19 types.

(6 vertices) S, U, E, X_1, A, X:

(9 1-simplexes) (U,S), (E,S), (X_1,S), (A,S),(X,S),
(A,U), (A,E), (A,X_1), (X,X_1):

(4 2-simplexes) (A,U,S), (A,E,S), (A,X_1,S), (X,X_1,S):

We are now collapsing some simplexes in turn using the following fact.

Lemma 2 (Lemma 2.1 in [RSY]) *In a simplicial complex Δ with type, let τ be a simplex of codimension 1. Assume that there is a unique maximal (with respect to inclusion) simplex σ containing τ. Then the process removing σ and τ from Δ (called* collapsing*) is a homotopy equivalence.*

Furthermore, assume that a group G acts on Δ preserving type. Then the process simultaneously removing all the simplices with the same type as σ and τ is a G-homotopy equivalence.

For example, we can verify that there is a unique (maximal) simplex of type (X, X_1, S) containing a simplex of type (X_1, S). Thus via collapsing $\Delta(\mathcal{B}_3(G))$ is G-homotopy equivalent to the subcomplex which is obtained by simultaneously removing all simplexes of these two types. The latter subcomplex can be furthermore reduced by applying similar processes for the simplexes of types (X_1) and (X_1, X); (A, S) and (A, E, S); and (A, X_1) and (A, X_1, S). In the resulting subcomplex there is a unique simplex of type (S, E) (which is maximal in that complex) containing a simplex of type (S). Then by removing them we conclude that the following complex Δ' with simplexes of 9 types is G-equivalent to the original complex $\Delta(\mathcal{B}_3(G))$.

(4 vertices) U, E, A, X:

(4 1-simplexes) (U, S), (X, S), (A, U), (A, E):

(1 2-simplexes) (A, U, S):

To see the plausibility of the result (though this does not verify the correctness of the result), we calculate the Euler characteristic $\chi(\Delta') = \chi(\Delta(\mathcal{B}_3(G)))$ (the alternating sum of the numbers of simplexes of fixed dimensions). The result is $\chi(\Delta') = -3^7.67843$, which is certainly divisible by the 3-part 3^7 of $|G|$ [4]

On the other hand, as for the 3-radical subgroups with 3-constrained normalizers, it follows from the results above that $\Delta(\mathcal{B}_3^{\mathrm{cen}}(G))$ consists of simplices of the following 15 types.

(5 vertices) A, U, E, X_1, S:

(7 1-simplexes) (A, U), (A, E), (A, X_1), (A, S), (U, S), (E, S), (X_1, S):

(3 2-simplexes) (A, U, S), (A, E, S), (A, X_1, S):

In $\Delta(\mathcal{B}_3^{\mathrm{cen}}(G))$, we note the uniqueness of simplexes of type (A, X_1, X) (resp. (A, E, S) and (E, S)) containing a simplex of type (A, X_1) (resp. (A, S) and (S)). Then via collapsing $\Delta(\mathcal{B}_3^{\mathrm{cen}}(G))$ is G-homotopy equivalent to the following complex Δ''.

[4] The vertual $\bar{F}_p[G]$-module defined as the alternating sum of the G-permutation modules with simplexes of $\Delta(\mathcal{B}_3(G))$ of fixed dimensions is projective, and hence its character degree, the Euler characteristic, is a multiple of the p-part of $|G|$.

(3 vertices) A, U, E:

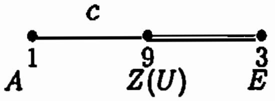
(3 1-simplexes) (A, U), (A, E), (U, S):

(1 2-simplexes) (A, U, S):

As there is a unique conjugate of E which is a subgroup of S containing U, there is a one to one correspondence between the simplex of type (S, U) and the chains of type $(Z(U), E)$. By the same reason the simplices of type (A, S, U) bijectively correspond to the chains of type $(A, Z(U), E)$. Hence the complex Δ'' is nothing more than the complex $\mathcal{L}_3(Suz)$ defined as follows:

The vertices of $\mathcal{L}_3(Suz)$ are the conjugates of $A \cong 3$, $Z(U) \cong 3^2$ and $E \cong 3^5$ (they can be though of as the sets of mutually commuting one, two and twelve $3A$-subgroups respectively), and a simplex is defined to be the chains of them under inclusion.

This complex is called the 3-*local geometry* of the sporadic Suzuki group $G = Suz$, which is a nice geometric object describing some feature of the group. For example, $\mathcal{L}_3(Suz)$ admits a flag-transitively action of G and belongs to the following diagram, in which the residue at a 'point' A is a classical polar space associated with the 4-dimensional unitary space over $\mathbf{F}_9$. Moreover, its collinearity graph on 22,880 points is a distance regular (in fact transitive) graph of diameter 4.



3. Results on the Thompson group $G = F_3$

So far no good geometry have been obtained for the sporadic group $Th = F_3$ of Thompson, except for a 2-local geometry (see [SY, 2.14]). As I explained before, for each prime divisor p of $|G|$, we have enough hope to find something nice by investigating simplicial complexes which are G-homotopy equivalent to the complex of p-radical subgroups with p-constrained normalizers. The results are described in this section. We obtain a natural 3-local geometry $\mathcal{L}_3(G)$ of dimension 2 for $p = 3$.

Complexes of dimension 0 and 1 (just a set or a graph) are not so much interesting to me, so that I only consider the prime divisor p such that p^3 divides $|G|$. Thus $p = 2$, 3 or 5.

p=2. It is known that $G = Th$ is of characteristic-2 type, and hence $\mathcal{B}_2(G) = \mathcal{B}_2^{cen}(G)$. Such a case was already treated in [SY, 2.14][5] , and there it is shown that $\Delta(\mathcal{B}_2(G))$ is G-homotopy equivalent to the following complex Δ of dimension 1.

The vertices of Δ consist of $2A$-elements and a conjugates of certain elementary abelain group of order 2^5, and the simplexes are their chains.

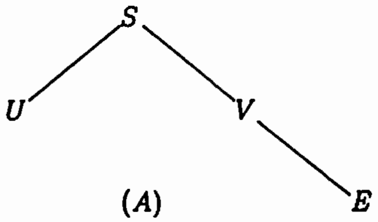
[5] On this occasion, I would like to point out a typo in that paper: the sentence "The spaces ... 2-grops K_{S_i}." in the 7th line from the bottom of Page 365 should be deleted.

p=3. The maximal 3-local subgroups of G are determined by Wilson [Wil2]. Using the lemma described in the previous section, his results enable us to determine the 3-radical subgroups.

Result 2 *The complex $\mathcal{B}_3(G)$ consists of the conjugacy classes of the following five subgroups with the described structures of normalizers (under the ATLAS notation). In particular, A is the unique representative with non-3-constrained normalizer.*

> A *(3A-subgroup),* $U \cong (3^3 \times 3^{1+2})3^{1+2}$,
> $V \cong 3^2[3^7]$, $E \cong 3^5$ *(E contains* 40 *3B-subgroups and* 81 *3C-subgroups),*
> S*, a Sylow* 3*-subgroup of* G
>
> $N_G(A) \cong (3 \times G_2(3)).2$, $N_G(U) = N_G(3B) \cong U : 2S_4$,
> $N_G(V) = N_G(3B^2) \cong V.2S_4$, $N_G(E) = N_G(3C) \cong (3 \times 3^4 : SL_2(9)) : 2$,
> $N_G(S) =\cong S : 2^2$

Below I show the possible inclusion relations among representatives of 3-radical groups. The Euler characteristic is calculated to be $\chi(\mathcal{B}_3(G)) = 3^{10} \cdot 13 \cdot 92227$.



Then we find that $\mathcal{B}_3^{con}(G)$ consists of the following simplexes of nine types.

(4 vertices) E, U, V, S:

(4 1-simplexes) (E, V), (E, S), (U, S), (V, S):

(1 2-simplexes) (E, V, S):

Now via collapsing based on the uniqueness of the simplexes of type (U, S) (resp. (E, V, S)) containing a simplex of type (U) (resp. (E, S)) the original complex $\mathcal{B}_3^{con}(G)$ is G-homotopy equivalent to the subcomplex Δ' of simplexes of types E, U, V, (E, V) and (V, S).

Observe that U is a unique conjugate of U containd in S and that $Z(U) \leq Z(V)$ if (S, V) is a simplex. Thus there is a bijective correspondence between the simplices of type (V, S) and the pairs (U, V) with $Z(U) \subseteq Z(V)$.

We define a complex $\mathcal{L}_3(Th)$ as follows:

Theree types of vertices:
the conjugates of $Z(U)$ (they are $3B$-subgroups), $Z(V) \cong 3^2$ (they are $3B$-pure[6]) and $E \cong 3^5$,
simplexes are their chains under inclusion.

Then the above remark implies that $\mathcal{L}_3(Th)$ is isomorphic to the subcomplex Δ'' of $\mathcal{B}_3^{cen}(G)$ consisting of simplices of types U, V, E, (V, S), (E, S), (V, E) and (E, V, S), where the simplexes of type (V, S) (resp. (E, S) and (E, V, S)) correspond to the chains of type $(Z(U), Z(V))$ (resp. $(Z(U), E)$ and $(Z(U), Z(V), E)$).

Since in Δ'' there is a unique simplex of type (E, V, S) containing a simplex of type (E, S), the complex Δ'' is G-homotopy equivalent to its subcomplex Δ'. Thus via Δ' we establish the G-homotopy equivalence of $\mathcal{L}_3(Th)$ with $\mathcal{B}_3^{cen}(Th)$.

This property shows a mathematical significance of the geometry $\mathcal{L}_3(Th)$ naturally defined on some 3-subgroups generated by $3B$-subgroups. My talk at ICU seems the first time to give a definition of the geometry $\mathcal{L}_3(Th)$ and to show its analogy with buildings. It is required to analize the properties of this geometry in detail.

The gemetry $\mathcal{L}_3(Th)$ is of dimension 2 and admits a flag-transitive action of G. However, as there is a unique simplex of type $(Z(U), Z(V), E)$ containing $(Z(U), E)$, this geometry does not satisfy the residual connectedness which is usually assumed when one considers geometries. Namely, $Z(V)$ can be thought of as a 2-dimensional space over $\mathbf{F}_3$ with the structure of a 1-dimensional vector space over $\mathbf{F}_9$, while $Z(U)$ is just a vector of $Z(V)$ considered as a space over $\mathbf{F}_3$.

It may be worthwile to mention that the situation is quite similar to the 2-local geometry $\mathcal{L}_2(J_3)$ for the J_3. In this case, $\mathcal{L}_2(J_3)$ is of dimension 2 admitting a flag-transitive action of J_3, and it is J_3-homotopy equivalent to $\Delta(\mathcal{B}_2(J_3))$ (in fact J_3 is of characteristic-2 type [SY, 2.11]). However it does not satisfy the residual connectedness (see [Yo, §2] for the details of $\mathcal{L}_2(J_3)$).

The Euler characteristic is calculated as $\chi(\mathcal{B}_3^{cen}(Th)) = -3^9 \cdot 10987 \cdot 11681$, which implies that it has 'defect' 1.

p=5. We have $|G|_5 = 5^3$ and $\mathcal{B}_5(G) = \mathcal{B}_5^{cen}(G)$. The complex $\Delta(\mathcal{B}_5(G))$ itself is nothing more than the complex of dimension 1 consisting of chains of $5A$-subgroups and $5A$-pure 5^2-subgroups.

4. Results for the Harada's group $G = F_5$

I also investigated complexes homotopy equivalent to the complex of p-radical groups with p-constrained normalizers for the sporadic simple group F_5 for which no good geometries so far have been found. For the odd primes, I only found complexes of dimension 1, which seem not so much interesting. As for $p = 2$, the analysis has not yet completed. So I briefly report the result only for $p = 3$ and 5.

[6] that is, every subgroup of order 3 lies in the class $3B$

p=5. The complex $\mathcal{B}_5(G)$ consists of the following four classes, where $5A$ and $5B$ are subgroups generated by the $5A$ and $5B$ elements under the ATLAS notation.

$5A$, $U := O_5(N_G(5B)) \cong 5^{1+4}$, $V := O_5(N_G(V)) \cong 5^2$, S: a Sylow 5-subgroup

The possible maximal chains are of types (A, U, S) and (V, S), and the Euler characteristic is $\chi(\Delta(\mathcal{B}_5(G))) = -5^6 \cdot 929 \cdot 1049$. Except $5A$, all 5-radical groups have 5-constrained normalizers and it is easy to see that $\Delta(\mathcal{B}_5^{\rm cen}(G))$ is G-homotopy equivalent to the complex $\Delta_5(G)$ of chains of $5B$-subgroups and $5B$-pure 5^2-subgroups, which has the Euler characteristic $\chi(\Delta(\mathcal{B}_5^{\rm cen}(G))) = -5^5 \cdot 17 \cdot 41 \cdot 773$.

p=3. The complex $\mathcal{B}_3(G)$ consists of the following five conjugacy classes, where $3A$ and $3B$ are subgroups generated by the $3A$ and $3B$ elements under the ATLAS notation.

$3A$, a $3A$-pure 3^2-subgroup, $O_3(N_G(3B)) \cong 3^{1+4}$,
a $3B$-pure 3^4-subgroup, S: a Sylow 3-subgroup

Their normalizers are 3-constrained except for $3A$ and a $3A$-pure 3^2-subgroup. It is easy to see that $\Delta(\mathcal{B}_3^{\rm cen}(G))$ is G-homotopy equivalent to the complex $\Delta_3(G)$ of chains of $3B$-subgroups and $3B$-pure 3^4-subgroups with the Euler characteristic $\chi(\Delta(\mathcal{B}_3^{\rm cen}(G))) = -3^4 \cdot 48405321$.

References

[BT] A. Borel and J. Tits, Eléments unipotents et sousgroupes paraboliques des groups réductives, *Inv. Math.*, 12 (1971), 97–104.

[BW] N. Burgoyne and C. Williamson, On theorem of Borel and Tits for finite Chevalley groups, *Arch.Math.* 27 (1976), 489–491.

[RSY] A. Ryba, S. Smith, and S. Yoshiara, Some projective modules determined by sporadic geometries, *J. Algebra*, 129 (1990), 279–311.

[SY] S. D. Smith and S. Yoshiara, Some homotopy equivalences for sporadic geometries, *J. Algebra* 192 (1997), 326–379.

[Wil1] R. A. Wilson, The complex Leech lattice and maximal subgroups of the Sizuki group, *J. Algebra* 84 (1983), 151–188.

[Wil2] R. A. Wilson, Some subgroups of the Thompson group, *J. Austral. Math. Soc.* 44 (1988), 17–32.

[Yo] S. Yoshiara, Some geometries for J_3 and $O'N$, *Europ. J. Combin.* 10 (1989), 499-506.

Exponential Formulas for Finite Groups and Locally Finite Toposes

Tomoyuki YOSHIDA
Department of Mathematics, Hokkaido University,
Kita-10, Nishi-8, Sapporo 060, JAPAN
yoshidat@math.sci.hokudai.ac.jp

1 Introduction

In 1980, the first year of the age of post classification, I published in a Japanese article a project after cla ssification, that is, the categorification of finite group theory.

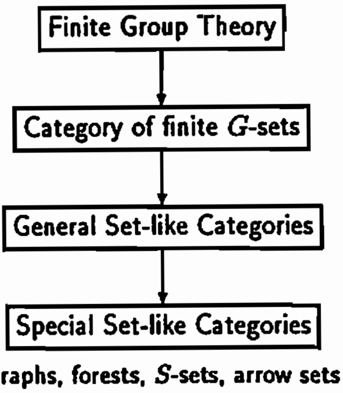

Finite Group Theory
Category of finite G-sets
General Set-like Categories
Special Set-like Categories
graphs, forests, S-sets, arrow sets

Fig 1: Our Project

The first step of our project is to rewrite finite group theory by using the language of categories of G-sets. For example, if $f : G \longrightarrow H$ is a group homomorphism, then it induces a triple of adjoint functor (a so-called essential geometric functor)

$$\begin{tikzcd} \mathrm{Set}_f{}^G \arrow[r, bend left, "f_!"] \arrow[r, phantom, shift left=1.5, "\perp"] \arrow[r, phantom, shift right=1.5, "\perp"] & \mathrm{Set}_f{}^H \arrow[l, "f^*" description] \arrow[l, bend left, "f_*"] \end{tikzcd}$$

Since the finite group G is the automorphism group of a unique projective indecomposamble G-set, there is no loss in such a rewriting.

The category of finite G-sets is very like the category of finite sets. Thus the second step is to generalize the categorified finite group theory to a general theory of some set-like categories. The final step is to apply the general theory obtained by such a way to some special set-like categories. In this article, we start at Wohlfahrt's formula

$$\sum_{n=0}^{\infty} \frac{|\mathrm{Hom}(A, S_n)|}{n!} t^n = \exp\left(\sum_{B \leq A} \frac{t^{(A:B)}}{(A:B)}\right),$$

where $\mathrm{Hom}(A, S_n)$ denotes the set of homomorphisms from a finitely generated group A to a symmetric group S_n and B runs over all subgroup of A of finite index; and then we try to build an abstract theory of generating functions whose exponents belongs to a set-like category.

Here, note that there are two kinds of mathematical theories based on a set-like category, that is, *internal theories* and *external theories*. As a simplest example, we take the theory of natural numbers. The internal natural number object inside the category of sets is just defined by Peano's axiom, and of course it belongs to the category of sets. On the contrary, there are some external definitions of the set of natural numbers; due to Dedekind and Russel the set of natural numbers is the set of isomorphism classes of the category of finite sets (or finite ordinals); thus the external set of natural numbers does not belongs to the category of finite sets.

Let's consider some internal and external definitions based on the category of G-sets and finite G-sets. In the category G-sets, an internal concept of sets is that of G-sets; similarly, an internal vector space is a G-module, and an internal group is a group with G-action. An internal map between internal sets is simply a map between G-sets which is not necessarily a G-map; on the other hand, an external map between two G-sets is a G-map; thus the internal Hom-set is a G-set $Y^X = \mathrm{Hom}(X,Y)$ with G-action defined by ${}^g\lambda(x) = g\lambda(g^{-1}y)$ and the external Hom-set is the set $\mathrm{Map}_G(X,Y)$ of G-maps. The internal power set 2^X of a G-set X is the G-set of all subsets of X; the external power set $\mathrm{Sub}_G(X)$ of a G-set X is the set of G-subsets. I feel that an internal theory in the category of G-sets is too difficult to develop and often falls into abstract nonsense in general.

According to Dedekind and Russel the external set of natural numbers is the set of isomorphism classes of finite G-sets. The external ring of integers is the Grothendieck ring of external natural numbers, that is, the Burnside ring of the finite group G. An internal matrix is a map from $X \times Y$ to a G-algebra A; contrarily, an external positive matrix is a G-map from $X \times Y$ to A; in fact, when the group G is trivial, we can identify such a map $A \longrightarrow X \times Y; a \longmapsto (l(a), r(a))$ with a usual positive integral matrix as follows:

$$(X \xleftarrow{l} A \xrightarrow{r} Y) \longleftrightarrow (|l^{-1}(x) \cap r^{-1}(y)|)x \in X, y \in Y.$$

Furthermore, an external vector space is a Mackey functor (or Green's G-functor), an external G-algebra is a Green functor, an external commutative ring is a Tambara functor, that is, a Mackey functor with multiplicative transfer. One question is what an external polynomial ring and the ring of power series.

Theories	Internal Theories	External Theories
Natural numbers N	N	$\mathsf{Set}_f{}^G/\cong$
Ring of integers Z	Z	Burnside ring $B(\mathcal{E})$
Hom-set	$Y^X := \mathrm{Map}(X,Y)$	$\mathrm{Map}_G(X,Y)$
Power set	2^X	$\mathrm{Sub}_G(X)$
Matrix ring	$A^{X \times Y}$	$X \leftarrow A \rightarrow Y$
Vector space	G-modules	Mackey functor
Ring	G-algebras	Green functor
Commutative ring	commutative G-algebra	Tambara functor
Polynomial ring	$Z[t]$	$Z[(\mathsf{Set}_f{}^G)^{\mathrm{op}}/\cong]$ $\varinjlim B(\mathsf{Set}_f{}^G/2^N)$
Ring of power series	$Z[[t]]$	$Z[[(\mathsf{Set}_f{}^G)^{\mathrm{op}}/\cong]]$ $\varprojlim B(\mathsf{Set}_f{}^G/2^N)$

2 Exponential functions

Let $\mathcal{E}$ be a category in which every hom-set is a finite set and whose isomorphism classes $\mathcal{E}/\cong$ make a set. Such a category is often called a ***skeletally small*** and ***locally finite*** category. A polynomial (resp. power series) with exponents in $\mathcal{E}$ is a finite (resp. infinite) sum

$$\sum_{X \in \mathcal{E}}{}' a_X t^X,$$

where the summation is taken over isomorphism classes of objects of $\mathcal{E}$, the coefficient a_X is in a commutative ring R and t^X denotes a variable corresponding to $X \in \mathcal{E}$ satisfying the condition

$$X \cong Y \quad \Longrightarrow \quad t^X = t^Y.$$

The *exponential generating function* $\mathcal{E}(t)$ associated to $\mathcal{E}$ is defined by a formal infinite summation:

$$\mathcal{E}(t) := \sum_{X \in \mathcal{E}}{}' \frac{1}{|\mathrm{Aut}(X)|} t^X$$

Let $F : \mathcal{E} \longrightarrow \mathcal{S}$ be a functor between skeletally small and locally finite categories. Assume that F has locally finite fibbers:

$$|F^{-1}(N)/\cong| = \sharp\{X \in \mathcal{E}/\cong|\, F(X) \cong N\} < \infty.$$

Then we define a power series

$$\begin{aligned} F_\bullet\left(\sum_{X \in \mathcal{E}}{}' a_X t^X\right) &:= \sum_{X \in \mathcal{E}}{}' a_X t^{F(X)} \\ &= \sum_{N \in \mathcal{S}}{}' \left(\sum_{F(\tilde{X}) \cong N}{}' c_X\right) t^N. \end{aligned}$$

In particular, we put

$$F(t) := F_\bullet(\mathcal{E}) = \sum_{X \in \mathcal{E}}{}' \frac{1}{|\mathrm{Aut}(X)|} t^X$$

Let $F : \mathcal{E} \longrightarrow \mathcal{S}$ be a faithful functor with finite fibers between skeletally small and locally finite categories. then an *$\mathcal{E}$-structure* along F over $N \in \mathcal{S}$ is a pair (X, σ) of $X \in \mathcal{E}$ and an isomorphism $\sigma : F(X) \xrightarrow{\cong} N$. Two $\mathcal{E}$-structures $(X, \sigma), (Y, \tau)$ are *isomorphic* if there exists an isomorphism $f : X \xrightarrow{\cong} Y$ such that the following diagram is commutative:

$$\begin{tikzcd} F(X) \arrow[r, "F(f)"] \arrow[d, "\sigma"'] & F(Y) \arrow[dl, "\tau"] \\ N & \end{tikzcd}$$

The isomorphism $\sigma : F(X) \longrightarrow N$ is called a *labeling/* and N is called a *label set*. We denote by $\mathrm{Str}(\mathcal{E}/N)$ the set of $\mathcal{E}$-structures on N.

Example: Let $F : \mathrm{Graph} \longrightarrow \mathrm{Set}_f$ be the forgetful functor from the category of (simple) graphs to the category of finite sets. Then an isomorphism class of $\mathcal{E}$-structures on N is bijectively correspondent to a labeled graphs on N.

Theorem: *Under the above notation,*

$$F(t) = \sum_{X \in \mathcal{E}}{}' \frac{t^{F(X)}}{|\mathrm{Aut}(X)|} = \sum_{N \in \mathcal{S}}{}' \frac{|\mathrm{Str}(\mathcal{E}/N)/\cong|}{|\mathrm{Aut}(N)|} t^N.$$

Example: Let G be a finitely generated group, $\mathrm{Set}_f{}^G$ the category of finite G-sets, and F : $\mathrm{Set}_f{}^G \longrightarrow \mathrm{Set}_f$ the forgetful functor. Then there is a bijection

$$\mathrm{Str}(\mathrm{Set}_f{}^G/N)/\cong \longleftrightarrow \mathrm{Hom}(G, S_n),$$

and so

$$F(t) = \sum_X{}' \frac{t^{|X|}}{|\mathrm{Aut}(X)|} = \sum_{n=0}^{\infty} \frac{|\mathrm{Hom}(G, S_n)|}{n!} t^n$$

Example: Let Gp be the category of finite groups and $F : \mathsf{Gp} \longrightarrow \mathsf{Set}_f$ the forgetful functor. Then

$$F(t) = \sum_G{}' \frac{t^{|G|}}{|\mathrm{Aut}(G)|} = \sum_{n=0}^{\infty} \frac{n^{n^2} p_n}{n!} t^n,$$

where p_n is the probability that a binary operation on $[n](:= \{1, 2, \ldots, n\})$ makes $[n]$ a group.

3 Exponential formulas

Assume that the skeletally small and locally finite category $\mathcal{E}$ has any finite coproducts. Then the isomorphism classes $\mathcal{E}^{\mathrm{op}}/\cong$ of the dual category make a multiplicative monoid. We denote by t^X the element of $\mathcal{E}^{\mathrm{op}}/\cong$ corresponding to $X \in \mathcal{E}$, so that the multiplication is defined by

$$t^X \cdot t^Y = t^{X+Y},\ t^{\emptyset} = 1$$

($\emptyset$ denotes an initial object). Thus we can define the polynomial ring as the semi-group algebra $R\mathsf{pol}(\mathcal{E}) := R[\mathcal{E}^{\mathrm{op}}/\cong]$. Furthermore, the ring of power series is defined to be the complete semi-group algebra $R\mathsf{pow}(\mathcal{E}) := R[[\mathcal{E}^{\mathrm{op}}/\cong]]$; if $\mathcal{E}$ satisfies the following condition, then the multiplication on the ring of power series is well-defined:

(A) $\sharp\{(A, B) \mid A, B \in \mathcal{E}, A + B \cong X\}/\cong < \infty$ for any $X \in \mathcal{E}$.

An object $I \neq \emptyset$ of $\mathcal{E}$ is *connected* if

$$I \cong A + B \quad \Longrightarrow \quad A \cong \emptyset \text{ or } B \cong \emptyset.$$

The full subcategory of connected objects is denoted by $\mathsf{Con}(\mathcal{E})$. A category $\mathcal{E}$ with any finite coproducts is called a *strict KS-category* if any object $X \in \mathcal{E}$ has a unique coproduct decomposition

$$X \cong I_1 + \cdots + I_m, \quad I_\alpha \in \mathsf{Con}(\mathcal{E}).$$

Here the uniqueness means that if $X \cong J_1 + \cdots + J_n$, then $m = n$ and there exists a unique permutation $\pi \in S_n$ and isomorphisms $f_\alpha : I_\alpha \xrightarrow{\cong} J_{\pi(\alpha)}$ $(\alpha = 1, \ldots, n)$ such that

$$\begin{tikzcd}
I_\alpha \arrow[r, "f_\alpha"] \arrow[d, "\tau_\alpha"'] & J_{\pi(\alpha)} \arrow[dl, "\rho_{\pi(\alpha)}"] \\
X &
\end{tikzcd}$$

is commutative, where $\tau_\alpha : I_\alpha \longrightarrow X$ and $\rho_\beta : J_\beta \longrightarrow X$ denote canonical injections.

Theorem (Exponential formula): *Let $\mathcal{E}$ be a skeletally small and locally finite KS-category satisfying the condition* (A). *Then*

$$\mathcal{E}(t) = \exp(\mathsf{Con}(\mathcal{E})(t)).$$

Corollary: *Assume, furthermore, that a skeletally small and locally finite category $\mathcal{S}$ has any finite coproducts and satisfies the condition* (A). *Let $F : \mathcal{E} \longrightarrow \mathcal{S}$ be a faithful functor with finite fibbers which preserving coproducts. Then*

$$\sum_{N\in\mathcal{S}}{}' \frac{|\mathrm{Str}(\mathcal{E}/N)/\cong|}{|\mathrm{Aut}(N)|} t^N = \exp\left(\sum_{N\in\mathcal{S}}{}' \frac{|\mathrm{Str}(\mathrm{Con}(\mathcal{E})/N)/\cong|}{|\mathrm{Aut}(N)|} t^N\right).$$

Example: Let Surj be the category of surjections of finite sets, that is, an object is defined to be a surjection $A_1 \twoheadrightarrow A_0$ between finite sets A_0, A_1 and a morphism is defined by a commutative diagram

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, two heads] & B_1 \arrow[d, two heads] \\
A_0 \arrow[r] & B_0.
\end{tikzcd}$$

An object $A_1 \twoheadrightarrow A_0$ is connected if and only if A_0 is a one-point set, and so

$$J(n) := ([n] \twoheadrightarrow [1]), \quad n = 1, 2, \ldots$$

are complete representatives of isomorphism classes of connected objects, where

$$[n] := \{1, 2, \ldots\},\ [0] := \emptyset.$$

Then the exponential formula gives the following identity:

$$\sum_{n=0}^{\infty} \frac{Y_n}{n!} t^n = \exp\left(\sum_{i=1}^{\infty} \frac{f g_i t^i}{i!}\right),$$

$$Y_n := \sum_{\mu\vdash n} \frac{n!}{\mu_1! \cdots \mu_n!} \left(\frac{f g_1}{1!}\right)^{\mu_1} \cdots \left(\frac{f g_n}{n!}\right)^{\mu_n}.$$

Here we put $f g_i t^i := t^{J(i)}$. The polynomial Y_n in $f, g_1, g_2, \ldots$ is the Bell polynomial.

Applying the forgetful functor

$$F : \mathrm{Surj} \longrightarrow \mathrm{Set}_f; (A_1 \twoheadrightarrow A_0) \longmapsto A_1,$$

to the above formula, we have another famous formula for Bell numbers:

$$\sum_{n=0}^{\infty} \frac{b(n)}{n!} t^n = \exp(e^t - 1),$$

where $b(n)$ denotes the Bell number, that is, the number of equivalence relation on $[n]$. This formula follows from the fact that

$$|\mathrm{Str}(\mathrm{Surj}/[n])/\cong| = b(n).$$

Example: Let G be a finitely generated group and $F : \mathrm{Set}_f{}^G \longrightarrow \mathrm{Set}_f$ the forgetful functor. Then there is a bijection

$$\mathrm{Str}(\mathrm{Set}_f{}^G/[n])/\cong \quad \longleftrightarrow \quad \mathrm{Hom}(G, S_n).$$

In fact, if $\pi : G \longrightarrow S_n$ is a group homomorphism, then $[n]$ becomes a G-set by $g \cdot i := \pi(g)(i)$, and so $([n], \mathrm{id})$ is a $\mathrm{Set}_f{}^G$-structure over $[n]$ along F; conversely, given a $\mathrm{Set}_f{}^G$-structure (X, σ), we have a homomorphism $\pi \in \mathrm{Hom}(G, S_n)$ defined by $\pi(g)(i) = \sigma(g \cdot \sigma^{-1}(i))$. Thus we have

$$F(t) := \sum_X \frac{t^{F(X)}}{|\mathrm{Aut}(X)} = \sum_{n=0}^{\infty} \frac{|\mathrm{Hom}(G, S_n)|}{n!} t^n.$$

Furthermore, we have

$$\begin{aligned} \mathrm{Con}(\mathrm{Set}_f{}^G)(t) &= \sum_{G/H}{}' \frac{t^{G/H}}{|\mathrm{Aut}(G/H)|} \\ &= \sum_{H \leq G} \frac{t^{G/H}}{(G : H),} \end{aligned}$$

where H runs over all subgroup of G of finite index. Thus our exponential formula implies the Wohlfahrt formula:

$$\sum_{n=0}^{\infty} \frac{|\mathrm{Hom}(G, S_n)|}{n!} t^n = \exp\left(\sum_{H \leq G} \frac{t^{(G:H)}}{(G : H),} \right).$$

This formula is applied to enumerate the solutions of a system of equations on a symmetric group. This formula is also useful to enumerate the numbers of subgroups of given inde of a free group and the modular group $\mathrm{SL}_2(Z)$.

Example: A (binary linear) *code* is a pair (N, C) of a finite set N and a subspace C of $\mathbf{F}_2^N := \{(v_i)_{i \in N} \mid v_i \in\}$. The set N is the set of coordinates. A morphism $f : (M, C) \longrightarrow (N, D)$ between codes is a map $f : M \longrightarrow N$ such that

$$\begin{aligned} &f_*(C) \subseteq D, \quad \text{where} \\ &f_* : \mathbf{F}_2^M \longrightarrow \mathbf{F}_2^N;\ (u_i)_{i \in M} \longmapsto \left(\sum_{i \in f^{-1}(j)} u_i \right)_{j \in N}. \end{aligned}$$

A *self-dual* code is a code (N, C) with $C^\perp = C$, where

$$C^\perp = \{(v_i)_{i \in N} \in \mathbf{F}_2^N \mid \sum_{i \in N} u_i v_i = 0\}.$$

We study the KS-category sdCode of self-dual codes and the faithful functor

$$F : \mathrm{sdCode} \longrightarrow \mathrm{Set}_f;\ (N, C) \longmapsto N.$$

Then an isomorphism class of sdCode-structures over $[n]$ is viewed as a self-dual code in $\mathbf{F}_2^n$, and so we have

$$F(t) = \sum_{n=0}^{\infty} \frac{|\mathrm{Str}(\mathrm{sdCode}/[n])/\cong|}{n!} t^n = \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n,$$

where as is well-known, the number a_n of such self-dual codes is given as follows:

$$a_0 = 1, a_{2n} = \prod_{i=1}^{n-1} (2^i + 1),\ a_{2n+1} = 0.$$

In particular, $f(t)$ satisfies the equation

$$f''(t) = f(\sqrt{2}t) + f(t) - 1.$$

Similarly, define the generating functions for the number of connected self-dual codes as follows:

$$g(t) := \sum_{n=0}^{\infty} \frac{|\mathsf{Str}(\mathsf{Con}(\mathsf{sdCode})/[n])/\cong|}{n!} t^n = \sum_{n=0}^{\infty} \frac{b_n}{n!} t^n.$$

Then the exponential formula gives

$$f(t) = \exp(g(t)),\ g(t) = \log(f(t)).$$

Thus we have the following recurrence formula for $n \geq 1$:

$$\sum_{i=0}^{n} \binom{n}{i} a_{n-i} b_i - \sum_{i,j=1} \binom{n}{i,j} a_{n-i-j} b_i b_j = (2^{n/2} + 1) a_n.$$

Using this recurrence formula, we can calculate $b_2, b_4, b_6, \ldots$.

4 Operations on categories and functors

There are many operations on polynomials and power series; for example, $f(t) + g(t)$, $f(t) \cdot g(t)$, $f(g(t))$, $df(t)/dt$. We can construct the corresponding operations on categories and functors. Let $\mathcal{E}$ and $\mathcal{S}$ be a skeletally small and locally finite category with any finite coproducts; furthermore, let $S, T, \ldots$ denote faithful functors with finite fibers.

(1) *Summations.*

$$(\mathcal{E} \xrightarrow{S} \mathcal{S}) + (\mathcal{F} \xrightarrow{T} \mathcal{S}) := (\mathcal{E} + \mathcal{F} \xrightarrow{S+T} \mathcal{S}),$$

where $\mathcal{E} + \mathcal{F}$ is the disjoint union of categories and the functor $S + T$ is equal to S on $\mathcal{E}$ and to T on $\mathcal{F}$. Furthermore, we have that $(S + T)(t) = S(t) + T(t)$.

(2) *Multiplications.*

$$(\mathcal{E} \xrightarrow{S} \mathcal{S}) \cdot (\mathcal{F} \xrightarrow{T} \mathcal{S}) := (\mathcal{E} \times \mathcal{F} \xrightarrow{S \cdot T} \mathcal{S}),$$

$$\text{where} \quad (S \cdot T)(X, Y) := S(X) + T(Y).$$

Then we have $(S \cdot T)(t) = S(t) \cdot T(t)$.

(3) *Derivations.*

$$(\mathcal{E} \xrightarrow{S} \mathsf{Set}_f)' := (\mathsf{Elts}(S) \xrightarrow{S'} \mathsf{Set}_f),$$

where $\mathsf{Elts}(S)$ is the category of elements, that is, an object has the form (X, s), $X \in \mathcal{E}$ and $s \in S(X)$, and a morphism $f : (X, s) \longrightarrow (Y, t)$ is a morphism $f : X \longrightarrow Y$ in $\mathcal{E}$ such that $S(f)(s) = t$; furthermore, the functor $S' : \mathsf{Elts}(S) \longrightarrow \mathsf{Set}_f$ is defined by $S'(X, s) := S(X) - \{s\}$. Then we have that $S'(t) = dS(t)/dt$. Furthermore, Leibniz's rule holds:

$$(S \cdot T)' \cong S' \cdot T + S \cdot T'.$$

(4) *Partial derivations.* For a functor $S : \mathcal{E} \longrightarrow \mathcal{S}$ and an object I of $\mathcal{E}$, the comma category $I \uparrow S$ has pairs $(I \xrightarrow{\alpha} S(X), X)$, where $X \in \mathcal{E}$, as objects and a morphism from (α, X) to (β, Y) is a morphism $f : X \longrightarrow Y$ such that $S(f) \circ \alpha = \beta$. We write $\partial_I(S)$ for $I \uparrow S$. Then the derivation at I is defined by the functor

$$\partial_I(S) : \partial_I(\mathcal{E}) \longrightarrow \mathcal{S}; (\alpha, X) \longmapsto S(X).$$

The generating function of $\partial_I(S)$ is given by

$$\partial_I(S)(t) = \sum_{X\in\mathcal{E}}{}' \frac{|\mathrm{Hom}(I, S(X))|}{|\mathrm{Aut}(X)|} t^X.$$

If the Hom-functor $\mathrm{Hom}(I, -)$ preserves finite coproducts (e.g., $\mathcal{E}$ is a topos and I is a connected object), then Leibniz's rule holds:

$$\partial_I(S \cdot T) \cong \partial_I(S) \cdot T + S \cdot \partial_I(T).$$

(5) it Exponentials. Let C be any category. Then the exponential $\mathsf{EXP}(C)$ is the category of pairs (M, Y) of a finite set N and a functor $Y : M \longrightarrow C$, where M is viewed as a discrete category; a morphism $(f, \tau) : (M, X) \longrightarrow (N, Y)$ consists of a map $f : M \longrightarrow N$ and a natural transformation $\tau : X \longrightarrow Y \circ f$; the composition is defined by

$$(g, \rho) \circ (f, \tau) := (g \circ f, (\rho * f) \circ \tau),$$

where $\rho * f$ denotes the vertical composition.

The category $\mathsf{EXP}(C)$ is a strict KS-category and its connected objects are bijectively corresponding with objects of C:

$$\mathsf{Con}(\mathsf{EXP}(C)) \cong C.$$

If $\mathcal{S}$ is a category with finite coproducts, then any functor $F : C \longrightarrow \mathcal{S}$ can be uniquely extended to a functor

$$\mathrm{Exp}(F) : \mathsf{EXP}(C) \longrightarrow \mathcal{S};\ (N, Y) \longmapsto \coprod_{i\in N} F(Y_i).$$

Assume that C is skeletally small and locally finite. Then we have

$$\mathsf{EXP}(C)(t) = \exp(C(t)).$$

Assume furthermore that the functor $\mathcal{F} : C \longrightarrow \mathcal{S}$ has finite fibers and that $\mathcal{S}$ has any finite products. Then we have

$$(\mathsf{EXP}(F))(t) = \exp(F(t)).$$

(6) *Substitution.* Let $\mathcal{S}$ be a category with finite coproducts. For two functors $S : \mathcal{E} \longrightarrow \mathrm{Set}_f$ and $T : \mathcal{F} \longrightarrow \mathcal{S}$,the substitution (or composition) is constructed as follows: First define a category $S(\mathcal{F})$ by the pullback diagram:

$$\begin{tikzcd}
S(\mathcal{F}) \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{P.B.}"] & \mathcal{E} \arrow[d, "S"] \\
\mathsf{EXP}(\mathcal{F}) \arrow[r, "\text{rank}"] & \mathrm{Set}_f,
\end{tikzcd}$$

where the functor rank is defined by $(N, Y) \longrightarrow N$. Now the functor $S(T)$ is defined by the composition:

$$S(T) \ : \ S(\mathcal{F}) \longrightarrow \mathsf{EXP}(\mathcal{F}) \xrightarrow{\mathsf{EXP}(T)} \mathcal{S};$$

$$(X, Y) \longmapsto \coprod_{a\in S(X)} T(Y_a).$$

If the generating functions are well-defined, then we have

$$(S(T))(t) = S(T(t)).$$

Furthermore, under the condition that $\mathrm{Hom}(I,-)$ preserves coproducts and that $\mathcal{E}$ is a set-like category, we have

$$\partial_I(S(T)) \cong S'(T) \cdot \partial_I(T).$$

Example. An *arrow set* (X,α), simply X, consists of a finite set X and a map $\alpha : X \longrightarrow X$; a morphism $f : (X,\alpha) \longrightarrow (Y,\beta)$ between arrow sets is a map $f : X \longrightarrow Y$ with $f \circ \alpha = \beta \circ f$; we denote by ASet_f the category of finite arrow sets. A *cyclic set* is a finite set X with a permutation π on X, that is, a finite C-set, where C is an infinite cyclic group; the category of finite cyclic sets is denoted by $\mathsf{Set}_f{}^C$. A *rooted forest* is a disjoint union of finite number of rooted trees; the category of rooted tree (resp. rooted forests) is denoted by RTree ($\mathsf{RForest}$).

A *root* of an arrow set (X,α) is an element $x \in X$ such that $\alpha^i(x) = x$ for some $i \geq 1$; then the set $R(X,\alpha)$ of roots of (X,α) forms a finite cyclic set with permutation α. Furthermore, we can make a rooted forest $F(X,\alpha)$ with roots $R(X,\alpha)$ by connecting x and $\alpha(x)$ for $x \in X - R(X,\alpha)$. Thus we have the following commutative diagram:

$$\begin{tikzcd}
& \mathsf{ASet}_f \arrow[r, "R"] \arrow[d, "F"'] \arrow[dr, phantom, "\text{P.B.}"] & \mathsf{Set}_f{}^C \arrow[d, "S"] \\
\mathsf{RTree} \arrow[r, hook] \arrow[dr, "T"'] & \mathsf{RForest} \arrow[r, "root"] \arrow[d, "T'"] & \mathsf{Set}_f \\
& \mathsf{Set}_f &
\end{tikzcd}$$

where $S : \mathsf{Set}_f{}^C \longrightarrow \mathsf{Set}_f$ is the forgetful functor, root : $\mathsf{RForest} \longrightarrow \mathsf{Set}_f$ is the functor which assigns the set of roots to each rooted forest, $T : \mathsf{RTree} \longrightarrow \mathsf{Set}_f$ and $T' : \mathsf{RForest} \longrightarrow \mathsf{Set}_f$ are the forgetful functors. Clearly, $\mathsf{RForest} \cong \mathsf{EXP}(\mathsf{RTree})$ and $T' \cong \mathsf{EXP}(T)$. Thus we have that $S(\mathsf{RTree}) \cong \mathsf{ASet}_f$ and that

$$S(T) : \mathsf{ASet}_f \xrightarrow{F} \mathsf{RForest} \xrightarrow{T'} \mathsf{Set}_f$$

is equal to the forgetful functor.

Now since

$$\mathsf{Str}(\mathsf{ASet}_f/N) \quad \longleftrightarrow \quad \mathsf{Map}(N,N),$$

we have

$$(S(T))(t) = \sum_{n=0}^{\infty} \frac{n^n}{n!} t^n.$$

Using Wohlfahrt's formula (or counting the number of $\mathsf{Set}_f{}^C$-structures on $[n]$ along S), we have

$$S(t) = \exp\left(\sum_{n=1}^{\infty} \frac{t^n}{n}\right) = \frac{1}{1-t}.$$

Let u_n be the number of labeled rooted trees on $[n]$, so that

$$u(t) := T(t) = \sum_{n=1}^{\infty} \frac{u_n}{n!} t^n.$$

Hence

$$(S(T))(t) = \sum_{n=0}^{\infty} \frac{n^n}{n!} t^n = \frac{1}{1-u(t)}.$$

Now, using the Cayley's formula $u_n = n^{n-1}$, we have the following interesting formula:

$$\sum_{n=0}^{\infty} \frac{n^n}{n!} t^n = \frac{1}{1 - \sum_{n=1}^{\infty} \frac{n^{n-1}}{n!} t^n.}$$

This formula directly follows from Abel's formula

$$\sum_{k=1}^{n} \binom{n}{k} (x+k)^{k-1}(y+n-k)^{n-k} = \frac{(x+y+n)^n - (y+n)^n}{x}.$$

5 Toposes

Now, we first explain the necessity of new definitions of polynomials and power series in order to do substitution and composition without restriction. Let $\mathcal{E}$ be a skeletally small and locally finite category with any finite coproducts and R a commutative (topological) ring. If we need to consider power series, we assume that the following condition holds:

(A) $\sharp\{(A,B) \mid A,B \in \mathcal{E}, A+B \cong X\}/\cong\, < \infty$ for any $X \in \mathcal{E}$.

As stated before, a polynomial (resp. power series) is a finite (resp. infinite) summation of the form:

$$f(t) = \sum_{X \in \mathcal{E}}{}' a_X t^X, \quad a_X \in R$$

Thus the rings of polynomial and power series are the (complete) semi-group algebras:

$$\begin{aligned} R\,\mathsf{pol}(\mathcal{E}) &= R[\mathcal{E}^{\mathrm{op}}/\cong] \\ R\,\mathsf{pow}(\mathcal{E}) &= R[[\mathcal{E}^{\mathrm{op}}/\cong]] \end{aligned}$$

The multiplication is defined by the linear extension of

$$t^X \cdot t^Y = t^{X+Y}, \, t^{\emptyset} = 1.$$

This definition of polynomials (and power series) has two faults as follows:

(1) We can not define the substitutions. What should we substitute for the variable t in $f(t)$? What should we interpret the values, e.g., 2^X, $(-1)^X$? Of course, when $\mathcal{E} = \mathsf{Set}_f$, we can substitute any element of R for t under the identification $t^{[n]} = t^n$.

(2) We can not define the compositions $g(f(t))$. For example, what does $(1+t^X)^Y$ mean ?

In order to solve these two problems, we need the notion of toposes. A category $\mathcal{E}$ is called a *topos* if the following four conditions hold:

(T1) $\mathcal{E}$ has all finite limits, e.g., products $X \times Y$, a terminal object $\mathbf{1}$, pullbacks.
(T1') $\mathcal{E}$ has all finite colimits, e.g., coproducts $X + Y$, an initial object $\emptyset$.
(T2) $\mathcal{E}$ is cartesian closed, that is, for any object A of $\mathcal{E}$, the functor $(-) \times A : X \longrightarrow X \times A$ has a right adjoint (an exponentiation):

$$(-)^A : \mathcal{E} \longrightarrow \mathcal{E};\ X \longmapsto X^A.$$

Thus there is a natural bijection:

$$\mathrm{Hom}(X \times A, Y) \cong \mathrm{Hom}(X, Y^A).$$

(T3) $\mathcal{E}$ has a *subobject classifier* $\mathbf{1} \xrightarrow{t} \Omega$, that is, for any monomorphism $A \rightarrowtail X$, there exists a unique $\chi_A : X \longrightarrow \Omega$ with a pullback diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[d, tail] \arrow[dr, phantom, "\text{P.B.}"] & \mathbf{1} \arrow[d, "t"] \\
X \arrow[r, "\chi_A"] & \Omega
\end{tikzcd}$$

Example. (a) Set (the category of sets) and Set^G (the category of G-sets on a group G) are both toposes. The exponentiation $Y^X = \mathrm{Map}(X, Y)$ is the set of maps from X to Y with G-action ${}^g\lambda(x) = g\lambda(g^{-1}x)$; the subobject classifier $\Omega = \{0, 1\}$, the two element set, and χ_A is the characteristic map of $A \subseteq X$.
(b) Shv(X), the category of sheaves of sets on a topological space X, is a topos.
(c) $C(\mathcal{T})$, the category of sets under higher order intuitional logic. Any topos is equivalent to a topos of this type. Thus a topos is a category of generalized sets, and so we can prove statements on a topos as if the topos is the category of sets. However, in this category, the axiom of choice does not hold and the (external) power set Sub(X) is not a Boolean lattice.
(d) Set$^\Gamma$, the functor category, is a topos; furthermore, the category Shv(Γ, J) of J-sheaves with respect to a Grothendieck topology J.

We are interested only in *locally finite topos*, that is, a topos in which each hom-set Hom(X, Y) is a finite set. A locally finite topos is a strict KS-category.

Example. (a) Set$_f$ (the category of finite sets) is a locally finite topos.
(b) Set$_f{}^G$ (the category of finite G-sets on a group G) is a locally finite toposes. In particular, so is Set$_f{}^C$ (the category of finite cyclic sets). Here a cyclic set is a set equipped with a permutation.
(c) ASet$_f$ (the category of finite arrow sets) is *not* a locally finite topos. Here an arrow set is a set X equipped with a map into itself. However, this category provides all what we need to develop the theory of generating functions.
(d) Set$_f{}^\Gamma$ (the functor category) is a locally finite topos if Γ is a finite category.
(e) DGraph (the category of finite di-graphs) is a locally finite topos; in fact, it is the functor category from the category $(\cdot \rightrightarrows \cdot)$.
(f) Surj (the category of surjections between finite sets) is a locally finite toposes.
(g) RForest$_{\mathrm{ht} \leq n}$ (the category of rooted forests of height at most n) is a locally finite topos. RForest (the category of rooted forests) is not a locally finite topos.

After this, $\mathcal{E}$ denotes a skeletally small and locally finite topos. Then we can regard the set $\mathcal{N}(\mathcal{E}) := \mathcal{E}/\cong$ of isomorphism classes of objects of $\mathcal{E}$ as an external set of natural numbers. Because of cartesian closeness, we have

$$(X + Y) \times Z \cong X \times Z + Y \times Z,\ \emptyset \times Z \cong \emptyset,$$

and so $N(\mathcal{E})$ forms a semi-ring. Furthermore, $N(\mathcal{E})$ has exponentiations Y^X satisfying the usual exponential laws:

$$\begin{gathered}(X \times Y)^A \cong X^A \times Y^A,\ 1^A \cong 1,\\ X^{A+B} \cong X^A \times X^B,\ X^{\emptyset} \cong 1,\\ X^{A\times B} \cong (X^A)^B,\ X^1 \cong X.\end{gathered}$$

$N(\mathcal{E})$ has a poset structure, e.g., by the following way:

$$X \le Y \iff X \twoheadleftarrow A \rightarrowtail Y$$

for some object A. Unfortunately, the ordered semigroup $N(\mathcal{E})$ is not a totally ordered set in general.

6 The Burnside ring of a locally finite topos

Let $\mathcal{E}$ be a skeletally small and locally finite topos. Then the *Burnside ring* $B(\mathcal{E})$ of $\mathcal{E}$ is the Grothendieck ring of $\mathcal{E}$ with respect to coproducts and products, and so it is the abelian group generated by $\mathcal{E}/\cong$ with fundamental relation:

$$[X+Y] = [X] + [Y], \quad [\emptyset] = 0.$$

The multiplication on $B(\mathcal{E})$ is defined by

$$[X]\cdot[Y] = [X \times Y]$$

The Burnside ring $B(\mathcal{E})$ is a free abelian group on $\mathrm{Con}(\mathcal{E})/\cong$, where $\mathrm{Con}(\mathcal{E})$ is the full subcategory of connected objects. The *ghost ring* $Gh(\mathcal{E})$ is the ring of maps from $\mathrm{Con}(\mathcal{E})/\cong$ to Z with pointwise multiplication; we often identify the ghost ring with the product ring of some copies of Z. There is a so-called *Burnside homomorphism*:

$$\begin{aligned}\varphi := (\varphi_I)_I \ &:\ B(\mathcal{E}) \longrightarrow Gh(\mathcal{E})\\ &;\ [X] \longmapsto (|\mathrm{Hom}(I,X)|)_I\end{aligned}$$

Then φ is an injective ring homomorphism. Thus we can regard the Burnside ring as a subring of the ghost ring which is equipped with the product topology of the discrete ring Z. The completion of $B(\mathcal{E})$ is called a complete Burnside ring and is denoted by $\widehat{\Omega}(\mathcal{E})$; the Burnside homomorphism can be extended to the ring homomorphism $\widehat{\varphi}$ on the complete Burnside ring.

Fundamental Theorem. *The complete Burnside homomorphism φ is an injective ring homomorphism and there is an exact sequence as follows:*

$$0 \longrightarrow \widehat{\Omega}(\mathcal{E}) \xrightarrow{\ \widehat{\varphi}\ } Gh(\mathcal{E}) \xrightarrow{\ \psi\ } \prod_I (Z/|\mathrm{Aut}(I)|Z) \longrightarrow 0,$$

where I runs over $\mathrm{Con}(\mathcal{E})/\cong$.

The linear map ψ is called the Cauchy-Frobenius map and is constructed as follows:

$$\psi : (\chi(I))_I \longmapsto \left(\sum_{\sigma\in\mathrm{Aut}(I)} \chi(I/\sigma) \right)_I,$$

where I/σ is the coequalizer of $1, \sigma : I \longrightarrow I$.

7 Substitutions

Let

$$f(t) = {\sum_{A\in\mathcal{E}}}' c_A t^A \in R\mathrm{pol}(\mathcal{E})$$

be a polynomial with exponents in $\mathcal{E}$. Then for any object $X \in \mathcal{E}$, we define the *evaluation at X* by

$$(f \mid [X]\rangle := {\sum_{A\in\mathcal{E}}}' c_A |\mathrm{Hom}(A, X)|.$$

Define the integers $n_I(A)$ $(I \in \mathsf{Con}(\mathcal{E}), A \in \mathcal{E})$ by

$$A \cong {\coprod_{I}}' n_I(A) I,$$

where I runs over $\mathsf{Con}(\mathcal{E})/\cong$. Then clearly we have

$$\mathrm{Hom}(A, X) \cong {\prod_{I}}' \mathrm{Hom}(I, X)^{n_I(A)}.$$

Furthermore, for any $I \in \mathsf{Con}(\mathcal{E})$,

$$\mathrm{Hom}(I, X) \cong {\coprod_{J}}' n_J(X)\mathrm{Hom}(I, J),$$

where J runs over connected objects of $\mathcal{E}$. Note that if I is a connected of a topos, then $\mathrm{Hom}(I, -)$ preserves finite coproducts. Thus we can extend the evaluation of $f(t)$ to $R \otimes B(\mathcal{E})$ and to $R \otimes Gh(\mathcal{E})$:

$$\begin{aligned} (f \mid \sum_J x_J[J]\rangle &:= {\sum_{A\in\mathcal{E}}}' c_A {\prod_{I}}' \left({\sum_{J}}' |\mathrm{Hom}(I, J)| x_J\right)^{n_I(A)}, \quad x_J \in R \\ (f \mid \theta\rangle &:= {\sum_{A\in\mathcal{E}}}' c_A {\prod_{I}}' \theta(I)^{n_I(A)}, \quad \theta \in R \otimes Gh(\mathcal{E}), \end{aligned}$$

where I, J runs over $\mathsf{Con}(\mathcal{E})/\cong$.

If R is a torsion free, then we have an injective R-algebra homomorphism

$$eval : R[\mathcal{E}^{\mathrm{op}}/\cong] \longrightarrow \mathsf{pol}(R \otimes B(\mathcal{E})).$$

We next study the substitution of elements of the Burnside ring and the ghost ring. For any polynomial

$$f(t) = {\sum_{A\in\mathcal{E}}}' c_A t^A \in R\mathrm{pol}(\mathcal{E})$$

and any element $\theta \in R \otimes Gh(\mathcal{E})$, we define the substitution of θ by

$$\begin{aligned} f(\theta) &:= (f(\theta_I))_I, \\ (f(\theta_I)) &:= {\sum_{A\in\mathcal{E}}}' c_A {\prod_{J}}' \theta(J)^{n_J(I\times A)} \\ &= {\sum_{A\in\mathcal{E}}}' c_A \prod_{J|I\times A} \theta(J), \end{aligned}$$

where I, J runs over $\mathsf{Con}(\mathcal{E})/\cong$ and the notation $J|I \times A$ means that J is a connected subobject of $I \times A$. Thus we have a (polynomial) map:

$$subst_f : R \otimes Gh(\mathcal{E}) \longrightarrow R \otimes Gh(\mathcal{E})$$

In particular, restricting the substitution of elements of the ghost ring to those of the Burnside ring, we have

$$f(\varphi[X]) = \sum_{A\in\mathcal{E}}{}' c_A[X^A]$$

Clearly,

$$f(\theta)_1 = \langle f \mid \theta\rangle.$$

Furthermore, if we write

$$f^I(t) := \sum_{A\in\mathcal{E}}{}' c_A t^{I\times A},$$

then

$$f(\theta)_I = \langle f^I \mid \theta\rangle$$

Theorem. *If $R = \widehat{Z}, \widehat{Z}_p, Q, R$, then the substitution of elements of the Burnside ring gives a map:*

$$subst_f : R\otimes\widehat{\Omega}(\mathcal{E}) \longrightarrow R\otimes\widehat{\Omega}(\mathcal{E}); x \longmapsto f(x).$$

8 Plethysm composition

We next define a so-called *plethysm composition* $(g\circ f)(t)$ of polynomials and power series.

Lemma. (1) *Assume that the topos $\mathcal{E}$ satisfies the following condition:*

(a) $I, J \in \mathsf{Con}(\mathcal{E}) \quad\Longrightarrow\quad I\times J \in \mathsf{Con}(\mathcal{E})$.

Then for any polynomial $f(t), g(t) \in R\mathsf{pol}(\mathcal{E})$, there exists a unique $(g\circ f)(t) \in R\mathsf{pol}(\mathcal{E})$ such that

$$(g\circ f)(\theta) = g(f(\theta)), \quad \text{for all } \theta \in R\otimes Gh(\mathcal{E}).$$

(2)*Assume the above condition (a) and the following condition:*

(b) $\mathrm{Hom}(1, X) = \emptyset \quad\Longrightarrow\quad X = \emptyset$.

Then the composition $(g\circ f)(t)$ is defined for power series $f(t), g(t) \in R\mathsf{pow}(\mathcal{E})$ such that $f(0) = 0$.

Example. Let $\mathcal{E} = \mathsf{Surj}$ be the category of surjections between finite sets. Then a connected object of Surj is isomorphic to $J(n) = ([n] \twoheadrightarrow [1])$. Since

$$J(m)\times J(n) \cong J(mn),$$

the condition (a) holds. Furthermore, (b) also holds clearly. Then a power series $f(t) \in Q\mathsf{pol}(\mathcal{E})$ has the form

$$f(t) = \sum_{\mu} c_\mu t^\mu, \; t^\mu = t_1^{\mu_1} t_2^{\mu_2}\cdots,$$

where $t_i := t^{J(i)}$ and $\mu = 1^{\mu_1}2^{\mu_2}\cdots$. Let $g(t) = t^{J(n)} = t_n$. Then the composition $(g\circ g)(t)$ defined in the above lemma is presented as follows:

$$(g\circ f)(t) = \sum_{\mu} c_\mu\, t_n^{\mu_1} t_{2n}^{\mu_2} t_{3n}^{\mu_3}\cdots.$$

The composition of this type is nothing but the classical plethysm composition.

9 New definitions of polynomials and power series

Le $\mathcal{E}$ denote a skeletally small and locally finite topos, and R a (topological) commutative ring. Let $\mathcal{E}_{mon}$ be the dense subcategory of $\mathcal{E}$ in which every morphism is a monomorphism. For an object $X \in \mathcal{E}$, a *comma category* $\mathcal{E}/X$ is defined as a category whose object has the form $A \longrightarrow X$ and in which a morphism from $A \xrightarrow{\alpha} X$ to $B \xrightarrow{\beta} X$ is a morphism $f : A \longrightarrow B$ with $\beta \circ f = \alpha$. Then the comma category $\mathcal{E}/X$ of a topos $\mathcal{E}$ is also a topos. The fundamental theorem of toposes implies that for each morphism $f : X \longrightarrow Y$, there is a triplet of adjoint functors as follows:

$$\begin{tikzcd}
\mathcal{E}/X \arrow[r, bend left=50, "\Sigma_f"] \arrow[r, bend right=50, "\Pi_f"'] \arrow[r, phantom, shift left=2.5, "\perp"] \arrow[r, phantom, shift right=2.5, "\perp"] & \mathcal{E}/Y, \arrow[l, "f^*"']
\end{tikzcd}$$

where the functors Σ_f, f^* are defined by

$$\begin{aligned}
\Sigma_f &: (A \longrightarrow X) \longmapsto (A \longrightarrow X \xrightarrow{f} Y) \\
f^* &: (B \longrightarrow Y) \longmapsto (X \times_Y B \xrightarrow{\mathrm{pr}} Y)
\end{aligned}$$

For an object $N \in \mathcal{E}$, we views $R \otimes B(\mathcal{E}/\Omega^N)$ as the R-module of R-polynomials of degree at most N. Each monomorphism $i : M \rightarrowtail N$ of $\mathcal{E}$ induces a monomorphism $\exists_i : \Omega^M \longrightarrow \Omega^N$ and then a pair of adjoint functors:

$$\begin{tikzcd}
\mathcal{E}/\Omega^M \arrow[r, shift left=1.5, "\Sigma_{\exists_i}"] \arrow[r, phantom, "\perp"] & \mathcal{E}/\Omega^N. \arrow[l, shift left=1.5, "(\exists_i)^*"]
\end{tikzcd}$$

Since these functors preserve coproducts, they furthermore induce a pair of an injective R-linear map and a surjective R-linear map:

$$\begin{aligned}
\Sigma_{\exists_i} &: RB(\mathcal{E})(\mathcal{E}/\Omega^M) \rightarrowtail RB(\mathcal{E})(\mathcal{E}/\Omega^N), \\
(\exists_i)^* &: RB(\mathcal{E})(\mathcal{E}/\Omega^N) \twoheadrightarrow RB(\mathcal{E})(\mathcal{E}/\Omega^M).
\end{aligned}$$

Taking the (co-)limits over $\mathcal{E}_{mon}$, we have the R-module of polynomials and that of power series:

$$\begin{aligned}
R\,\mathsf{Pol}(\mathcal{E}) &:= \varinjlim R \otimes B(\mathcal{E}/\Omega^N) \\
R\,\mathsf{Pow}(\mathcal{E}) &:= \varprojlim R \otimes B(\mathcal{E}/\Omega^N).
\end{aligned}$$

The *degree* of a polynomial $F \in R\,\mathsf{Pol}(\mathcal{E})$ is defined to be a unique (up to isomorphism) minimal object $D \in \mathcal{E}$ with the property $F \in R \otimes B(\mathcal{E}/\Omega^D)$.

Example. Let $\mathcal{E} = \mathrm{Set}_f$, so that $\Omega = 2 = \{0, 1\}$. We identify the exponentiation 2^N with the power set $\{K \subseteq N\}$. Then the map $A \xrightarrow{s} 2^N$ is corresponding to the integral polynomial

$$\sum_{a \in A} t^{|s(a)|} \in Z[t].$$

In order to define the substitution, we need a notion from topos theory. The partial map classifiers $\tilde{X}$ of an object X of a topos is defined by using the Mitchell-Bénabou language:

$$\tilde{X} := \{Y \in \Omega^X \mid \forall x \in X (x \in Y \to Y = \{x\})\},$$

that is, $\tilde{X}$ is the set of 'at most one element set'. Then X is a subobject of $\tilde{X}$ with injection $\eta : X \longrightarrow \tilde{X}$. Furthermore, $\eta : X \longrightarrow \tilde{X}$ is characterized by the property that if $A \supseteq A' \xrightarrow{f} X$ is a partial map from A to X, then there exists a unique $\tilde{f}$ such that the following diagram is a pullback diagram:

$$\begin{tikzcd}
A' \arrow[r, "f"] \arrow[d] \arrow[dr, phantom, "\text{P.B.}"] & X \arrow[d, "\eta"] \\
A \arrow[r, "\tilde{f}"] & \tilde{X}.
\end{tikzcd}$$

In particular, $(1 \longrightarrow \tilde{1}) = (1 \xrightarrow{t} \Omega)$. The assignment $X \longmapsto \tilde{X}$ is functorial.

We can now define a substitution. Let X be an object of the locally finite topos $\mathcal{E}$. For any morphism $s : F \longrightarrow \Omega^N$, define an object $F[X]$ by

$$\begin{tikzcd}
F[X] \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{P.B.}"] & F \arrow[d, "s"] \\
\tilde{X}^N \arrow[r] & \Omega^N.
\end{tikzcd}$$

Taking the colimits, we have the substitution map

$$subst_X : R\,\mathsf{Pol}(\mathcal{E}) \longrightarrow R \otimes B(\mathcal{E}).$$

The substitution $X \longmapsto F[X]$ can be extend to $R \otimes B(\mathcal{E})$, and so we have a map

$$\begin{aligned} subst \ &: \ R\,\mathsf{Pol}(\mathcal{E}) \times R \otimes B(\mathcal{E}) \longrightarrow R \otimes B(\mathcal{E}) \\ &; \ (F, x) \longmapsto F(x). \end{aligned}$$

We can also substitute an element of the ghost ring.

10 Operations on polynomials and power series

The summation of polynomials and power series comes from the R-module structures of $R\,\mathsf{Pol}(\mathcal{E})$ and $R\,\mathsf{Pow}(\mathcal{E})$.

The multiplication is induces by

$$[F \xrightarrow{s} \Omega^M] \cdot [G \xrightarrow{t} \Omega^N] := [F \times G \xrightarrow{s \times t} \Omega^M \times \Omega^N \cong \Omega^{M+N}].$$

This operation is bilinear with respect to coproducts, and so we have an R-bininear map

$$R \otimes \Omega(\mathcal{E}/\Omega^M) \times R \otimes \Omega(\mathcal{E}/\Omega^N) \longrightarrow R \otimes \Omega(\mathcal{E}/\Omega^{M+N})$$

Taking the (co-)limits on $\mathcal{E}_{mon}$, we have the multiplications on $R\,\mathsf{Pol}(\mathcal{E})$ and $R\,\mathsf{Pow}(\mathcal{E})$.

We next define the composition of polynomials and power series. Take two morphisms $(F \xrightarrow{f} \Omega^M)$ and $(G \xrightarrow{g} \Omega^N)$ which are regarded as polynomials of degree as ost M, resp. N. Let $\hat{g} : N \times G \longrightarrow \Omega$ be the the adjoint of $g : G \longrightarrow \Omega^M$ and R_g the subobject of $N \times G$ with characteristic map $\widehat{g}$. We denote by G^* the pullback functor $\mathcal{E} \longrightarrow \mathcal{E}/G$, and by Σ_G (resp. Π_G) the left (resp. right) adjoint functor of G^*. We now define the composition by

$$G \circ F := \Sigma_G((F \times G \xrightarrow{pr} G)^{R_g \longrightarrow G}),$$

accompanied with a morphism $G \circ F \longrightarrow \Omega^{M \times N}$ which is the adjunction of

$$(F \times G \longrightarrow G)^{(R_g \longrightarrow G)} \xrightarrow{f} (G^*(\Omega^M))^{(R_g \longrightarrow G)} \xrightarrow{\exists_j} G^*(\Omega^{M \times N}) = (\Omega^{M \times N} \times G \longrightarrow G)$$

induced by the inclusion $i : R_g \longrightarrow N \times G$.

11 Application to error correcting codes with group action

Let $F := \mathbf{F}_q$ be a q-element field and G a finite group. For a finite G-set N, F^N denotes the F-vector space of maps from N to F, whose element $v : i \longmapsto v_i$ we often write as $(v_i)_{i \in N}$; the right G-action on F^N is defined by $(vg)_i := v_{gi}$ for all $v \in F^N$, $i \in N$, $g \in G$, and so F^N is a righta FG-module. The FG-module F^N has a G-invariant inner product

$$u \cdot v := \sum_{i \in N} u_i v_i.$$

The *support* and *weight* of an element v of F^N is defined by

$$\begin{aligned} supp(v) &:= \{i \in N \mid v_i \neq 0\} \subseteq N \\ |v| &:= wt(v) := |\mathrm{supp}(v)|. \end{aligned}$$

A *G-code* (N, C) consists of a finite G-set N and an FG-submodule C of F^N. The *dual code* of C is defined by

$$C^{\perp} := \{v \in F^N \mid u \cdot v = 0 \quad \text{for all } u \in C\}.$$

Then $\dim C^{\perp} = |N| - \dim C$. Remember that the *weight enumerator* of C is defined by

$$w_C(x, y) := \sum_{u \in C} x^{n-|u|} y^{|u|}, \quad (n := |N|).$$

We can now regard the support map $supp : C \longrightarrow 2^N$ as an element of $Z\,\mathrm{Pol}(\mathrm{Set}_f{}^G)$. Since $\mathrm{Set}_f{}^G$ is Boolean, it is convenient to consider homogeneous polynomials instead of polynomials in one variable; we define the *equivariant homogeneous weight enumerator* $W_C[X, Y]$ by the following pullback diagram:

$$\begin{tikzcd} W_C[X,Y] \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{P.B.}"] & C \arrow[d, "supp"] \\ (X+Y)^N \arrow[r] & 2^N, \end{tikzcd}$$

where $(X + Y)^N \longrightarrow 2^N$ is defined by $\rho \longmapsto \rho^{-1}(Y)$. By an easy calculation, we have

$$|W_C[X, Y]| = w_C(x, y) = \sum_{u \in C} x^{n-|u|} y^{|u|},$$

and so our equivariant weight enumerator $W_C[X, Y]$ is a generalization of the classical one.

Since $(X, Y) \longmapsto W_C[X, Y]$ is polynomial in X, Y, it can be extended to a map on $B(G) \times B(G)$, where $B(G) = B(\mathrm{Set}_f{}^G)$ is the Burnside ring of G.

Equivariant MacWilliams identity. *Assume that* $(q, |G|) = 1$. *Then for any* $x, y \in B(G)$,

$$[C] \times W_{C^\perp}[x, y] = W_C[x + qy, x - y].$$

This theorem is proved by the following way. The detail is found in [Yos 93]. We put $V := F^N$. For any subset $R \subseteq N$ and any subspace $D \subseteq V$, define subspaces as follows:

$$\begin{aligned} V(R) &:= \{v \in V \mid supp(v) \subseteq R\}, \\ D(R) &:= D \cap V(R). \end{aligned}$$

Then there is an exact sequence:

$$0 \longrightarrow C^\perp(R) \xrightarrow{\mathrm{inc}} V(R) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(N - R)^* \longrightarrow 0,$$

where C^* is the dual space and

$$f : v \longmapsto (u \longmapsto u \cdot v).$$

The assignments $R \longmapsto C^\perp(R), V(R), C^*, C(N - R)^*$ are representations of the Boolean algebra 2^N with G-action, and so the above exact sequence can be viewd as an exact sequence in the functor category $[(2^N) \cdot G, \mathrm{Vect}_F]$, where in the category $(2^N) \cdot G$, an object is a subset of N and a hom-set $\mathrm{Hom}(R, S) = \{g \in G \mid gR \subseteq S\}$:

$$0 \longrightarrow C^\perp(-) \xrightarrow{\mathrm{inc}} V(-) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(N - (-))^* \longrightarrow 0.$$

Now we consider the following functor:

$$\begin{aligned} \omega &: [(2^N) \cdot G, \mathrm{Vect}_F] \longrightarrow \mathrm{Set}_f{}^G \\ &: M \longmapsto \widetilde{M} := \coprod_{\rho \in (Z+Y)^N} M(\rho^{-1}(Y)). \end{aligned}$$

In particular, we have

$$\omega : C(-) \longmapsto \widetilde{W}_C[Z, Y] := W_C[Z + Y, Y].$$

Applying the functor ω to the above exact sequence an using the semisimplicity, we have a G-isomorphism of G-sets:

$$C \times \widetilde{W}_{C^\perp}[Z, Y] \cong_G \widetilde{W}_C[F \times Y, Z].$$

This proves the required identity.

References

[Aig 79] Aigner, M, *Combinatorial Theory*, Springer, 1979.

[Bis85] Beissinger, J.S., The enumeration of irreducible combinatorial objects, *J.Combin. Theory*(A), 38 (1985), 143–169.

[Bel 88] Bell, J.L., *Toposes and local Set Theories*, Clarendon Press, 1988.

[Dou 72] Doubilet, P.–Rota, G.-C.–Stanley, R., On the foundations of combinatorial theory (VI), *in "Sixth Berkeley Symp. Math. Stat. and Prob.* II, 267–318, 1972.

[Dre 75] Dress, A., Contributions to the theory of induced representations, Springer LNM 342, 182–240, 1975.

[Dur 86] Dür, A., *Möbius Functions, Incidence Algebras and Power Series Representations*, Springer LNM, 1202, 1986.

[Joh 77] Johnstone, P.T., *Topos Theory*, Academic Press, 1977.

[Joy 81] Joyal, A., Une théorie combinatoire des séries formelles, *Adv. Math.* 42 (1981), 1–82.

[Mac-Moe 92] MacLane,S.-Moerdijk,L, *Sheaves in Geometry and Logic*, Springer, 1992. .

[Nav 87]Nava, O., On the combinatorics of plethysm, *J.Combin. Theory*(A) 46 (1987), 212–251.

[Oda-Yos 97] Oda,F.–Yoshida,T., On crossed G-sets and the crossed Burnside ring of a finite group, (preprint).

[Tam 85] Tambara,D., On multiplicative transfer, *Comm. Algebra*, 171 (1995), 413–425.

[Wil 94] Wilf,H., *generatingfunctionology*, Academic Press, 1994.

[Woh 77] Wohlfahrt, H., Über einen Sats von Dey und die Modulgruppe, *Archiv Math.* 29 (1977), 445–457.

[Yos 87] Yoshida,T., Fisher's inequality for block designs with group action, *J.Fac.Sci. Univ.Tokyo* 34 (1987), 513–544.

[Yos 90] Yoshida,T., The generalized Burnside ring of a finite group, *Hokkaido M.J.* 19 (1990), 509-574.

[Yos 92] Yoshida,T., P.Hall's strange formula for abelian p-groups, *Osaka MAJ.* 29 (1992), 421–431.

[Yos 93] Yoshida,T., MacWilliams identities for linear codes with group action, *Kumamoto J.M.*, 6 (1993), 29–45.

[Yos 96] Yoshida,T., Classical problems in group theory (I), SUGAKU Expositions 9 (1996), 169–184.

[Yos 97] Yoshida,T., Categorical aspects of generating functions, (preprint).

Tits' Classification of the Buildings of Spherical Type in the Light of the Theory of Association Schemes

Paul-Hermann Zieschang
Department of Mathematics
Faculty of Science
Kyushu University 33
Fukuoka 812, Japan

1. Basic Notation. Let X be a set.

We define

$$1 := \{(x,x) \mid x \in X\}.$$

For each $r \subseteq X \times X$, we set

$$r^* := \{(y,z) \mid (z,y) \in r\}.$$

For each $x \in X$, and, for each $r \subseteq X \times X$, we define

$$xr := \{y \in X \mid (x,y) \in r\}.$$

Let G be a partition of $X \times X$ such that $\emptyset \notin G$ and $1 \in G$. Assume that, for each $g \in G$, $g^* \in G$. Then the pair (X,G) will be called an (*association*) *scheme* if, for all d, e, $f \in G$, there exists a cardinal number a_{def} such that, for all y, $z \in X$, $(y,z) \in f$ implies that $|yd \cap ze^*| = a_{def}$.

For the remainder of this note, (X,G) will be a scheme.

For each $g \in G$, we define $n_g := a_{gg^*1}$.

We set

$$\mathrm{O}_\vartheta(G) := \{g \in G \mid n_g = 1\}.$$

The pair (X,G) is called *thin*, if $\mathrm{O}_\vartheta(G) = G$.

For all E, $F \subseteq G$, we define

$$EF := \{g \in G \mid \sum_{e \in E} \sum_{f \in F} a_{efg} \neq 0\}$$

and call it the *complex product* of E and F.

For each $F \subseteq G$, we set $F^* := \{f^* \mid f \in F\}$, we write $F \leq G$ if $F^*F \subseteq F \neq \emptyset$, and we define

$$\langle F \rangle := \bigcap_{F \subseteq H \leq G} H.$$

We set $\mathrm{Inv}(G) := \{g \in G \mid |\langle g \rangle| = 2\}$.[1]

2. Factor Schemes. Let $H \leq G$ be given. For each $x \in X$, we define

$$xH := \bigcup_{h \in H} xh.$$

We set $X/H := \{xH \mid x \in X\}$. For each $g \in G$, we define

$$g^H := \{(yH, zH) \mid z \in yHgH\}.$$

We set $G//H := \{g^H \mid g \in G\}$ and

$$(X, G)^H := (X/H, G//H).$$

In general, $(X, G)^H$ is not a scheme. If $(X, G)^H$ is a scheme, we call it the *factor scheme* of (X, G) *with respect to* H.

If (X, G) is thin or if $|X| \in \mathrm{N}$, $(X, G)^H$ is a scheme.

3. Automorphisms. Let ϕ be a permutation of $X \cup G$ such that $X\phi \subseteq X$ and $G\phi \subseteq G$. Assume that, for all y, $z \in X$ and, for each $g \in G$, $(y, z) \in g$ implies that $(y\phi, z\phi) \in g\phi$. Then ϕ is called an *automorphism* of (X, G).

For each automorphism ϕ of (X, G), we set $\mathrm{Fix}_X(\phi) := \{x \in X \mid x\phi = x\}$ and $\mathrm{Fix}_G(\phi) := \{g \in G \mid g\phi = g\}$.

4. Generators. Let $L \subseteq \mathrm{Inv}(G)$ be such that $\langle L \rangle = G$.

It follows easily from [3; Theorem 1.4.1(i)] and [3; Lemma 1.4.5(i)] that

$$G = \bigcup_{j \in} L^j.$$

In particular, for each $g \in G$, there exists $j \in \mathrm{N}$ such that $g \in L^j$. For each $g \in G$, we define

$$\mu(g) := \min\{j \in \mathrm{N} \mid g \in L^j\}.$$

We now shall define a class of schemes which (according to [3; Theorem E]) can be identified with the class of buildings in the sense of Tits.

[1] Clearly, here, as well as later, $\langle g \rangle$ is an abbreviation for $\langle \{g\} \rangle$.

For all h, $k \in L$ with $h \neq k$, we set

$$M_{hk} := \{j \in \mathbb{N} \setminus \{0\} \mid 1 \in (\{h\}\{k\})^j\}$$

and

$$m_{hk} := \begin{cases} \min M_{hk} & \text{if } M_{hk} \neq \emptyset \\ \aleph_0 & \text{if } M_{hk} = \emptyset. \end{cases}$$

It follows immediately from the definition of m that m is a Coxeter matrix of L (in the sense of [2]).

Let us denote by $\mathbf{F}(L)$ the free monoid over L and by $\mathbf{F}_m(L)$ the set of m-reduced elements in $\mathbf{F}(L)$.

It is easy to see that the power set $\mathbf{R}(G)$ of G is a monoid with respect to the complex multiplication; cf. [3; Lemma 1.2.1(ii)]. We shall denote by ρ the uniquely determined monoid homomorphism from $\mathbf{F}(L)$ to $\mathbf{R}(G)$ such that, for each $l \in L$, $l\rho = \{l\}$.

The pair (X, G) is called a *Coxeter scheme with respect to L* if, for each $\mathbf{f} \in \mathbf{F}_m(L)$, $|\mathbf{f}\rho| = 1$, and if, for all $\mathbf{d}$, $\mathbf{e} \in \mathbf{F}_m(L)$, $\mathbf{d}\rho = \mathbf{e}\rho$ implies that $\mathbf{d}$ and $\mathbf{e}$ are homotopic with respect to m.

Assume that (X, G) is a Coxeter scheme with respect to L. Then (X, G) is called *spherical* if $|G| \in \mathbb{N}$.

It follows from [3; Theorem E] that buildings in the sense of Tits correspond (in a well-understood way) to Coxeter schemes. Moreover, with respect to this correspondence, the buildings of spherical type (in the sense of [1]) correspond to spherical Coxeter schemes.

5. Spherical Coxeter Schemes. The correspondence between buildings and Coxeter schemes mentioned at the end of the last section allows us to give the following formulation of one of the main results of [1].

Theorem 1. [J. Tits] *Let $L \subseteq \mathrm{Inv}(G)$ be such that (X, G) is a spherical Coxeter scheme with respect to L. Assume that $3 \leq |L|$ and that $\{1\} = \mathrm{O}_\vartheta(G)$.*

Then (X, G) is a factor scheme of a thin scheme.

The original proof of Tits' theorem is fairly involved and depends mainly on two reduction theorems. It is the purpose of this section to give a scheme-theoretical proof for the first of these reduction theorems.

Here is the scheme-theoretical version of this theorem.

Theorem 2. *Let $L \subseteq \mathrm{Inv}(G)$ be such that (X, G) is a spherical Coxeter scheme with respect to L. Assume that $\{1\} = \mathrm{O}_\vartheta(G)$.*

Let ϕ be an automorphism of (X, G), and let y, $z \in \mathrm{Fix}_X(\phi)$ be such that $(y, z) \in j$. Then, if $zL \subseteq \mathrm{Fix}_X(\phi)$, $\mathrm{Fix}_X(\phi) = X$.

The remainder of this section is devoted to the proof of Theorem 2. From now on, L will be a subset of $\mathrm{Inv}(G)$ such that (X, G) is a spherical Coxeter scheme with respect to L. In order to prove Theorem 2, we need four elementary results on spherical Coxeter schemes, the proofs of which are left to the reader.

Proposition 1. *There exists a uniquely determined element g in G such that $\mu(g) = \max \mu(G)$.*

We shall denote by j the uniquely determined element in G which satisfies $\mu(j) = \max \mu(G)$. (Note that $j^* = j$.)

Proposition 2. *For each $f \in G$, there exists a uniquely determined element e in G such that $\mu(e) + \mu(f) = \mu(j)$ and $\{j\} = ef$.*

For each $g \in G$, we shall denote by g' the uniquely determined element in G which satisfies $\mu(g') + \mu(g) = \mu(j)$ and $\{j\} = g'g$.

Lemma 1. *For each $g \in G$, we have $g'''' = g$ and $g''j = jg$.*

Lemma 2. *Let y, $z \in X$ be such that $(y, z) \in j$, and let $l \in L$ be given. Then, for each $x \in y\langle l \rangle$, $|xl''' \cap z\langle l'' \rangle| = 1$.*

Proposition 3. *Let ϕ be an automorphism of (X, G), and let y, $z \in \mathrm{Fix}_X(\phi)$ be such that $(y, z) \in j$.*
Let $l \in L$ be such that $yl \subseteq \mathrm{Fix}_X(\phi)$. Then $zl'' \subseteq \mathrm{Fix}_X(\phi)$.

Let us prove Proposition 3. Let $w \in zl''$ be given. Then, as $z \in yj$,

$$w \in yjl'' = ylj = ylll''';$$

see Lemma 1. Therefore, there exists $v \in yll$ such that $w \in vl'''$. It follows that

$$\{w\} = vl''' \cap zl'';$$

see Lemma 2.

By hypothesis, we have $y \in \mathrm{Fix}_X(\phi)$ and $yl \subseteq \mathrm{Fix}_X(\phi)$. Therefore, $l\phi = l$. On the other hand, by Proposition 1, $j\phi = j$. Thus, by Proposition 2, $l''\phi = l''$ und $l'''\phi = l'''$.

By [3; Lemma 1.4.5(ii)], $ll \subseteq \{1, l\}$. Therefore, we have $v \in yll \subseteq \{y\} \cup yl \subseteq \mathrm{Fix}_X(\phi)$. Thus, as $l'''\phi = l'''$, $(vl''')\phi = vl'''$.

On the other hand, we have $z\phi = z$ and $l''\phi = l''$. Thus, $(zl'')\phi = zl''$.

Now we obtain from $\{w\} = vl''' \cap zl''$ that $w\phi = w$.

Since $w \in zl''$ has been chosen arbitrarily, Proposition 3 is proved.

Let us now prove Theorem 2. Assume that $zL \subseteq \mathrm{Fix}_X(\phi)$. Than, as $z \in \mathrm{Fix}_X(\phi)$, $\mathrm{Fix}_G(\phi) = G$. (We shall use this later.)

Suppose, by way of contradiction, that ϕ is not the identity on X. Then there exists $n \in \mathrm{N}$ such that $zL^n \not\subseteq \mathrm{Fix}_X(\phi)$. We choose $n \in \mathrm{N}$ minimal subject to this property.

Since $z \in \mathrm{Fix}_X(\phi)$, $1 \leq n$. From the hypothesis that $zL \subseteq \mathrm{Fix}_X(\phi)$ we then obtain that $2 \leq n$.

Let $x \in L^n$ be given. Then there exist h, $k \in L$ and $g \in L^{n-2}$ such that $x \in zghk$. Thus, there exist $v \in zg$ and $w \in xk$ such that $(v, w) \in h$.

Since $(y, z) \in j$ and $\{j\} = g''g'$, there exists $u \in X$ such that $\{u\} = yg'' \cap zg'^{*}$. Since y, $z \in \mathrm{Fix}_X(\phi)$ and g', $g'' \in \mathrm{Fix}_G(\phi)$, we now have $u \in \mathrm{Fix}_X(\phi)$.

On the other hand, $v \in zg$ and $z \in ug'$. Thus, $v \in ug'g = uj$. From $v \in zL^{n-2}$ we also know that $vh \subseteq zL^{n-2}h \subseteq zL^{n-1} \subseteq \mathrm{Fix}_X(\phi)$. Thus, by Proposition 3, $uh'' \subseteq \mathrm{Fix}_X(\phi)$. Status: RO

Since we are assuming that $\{1\} = \mathrm{O}_\vartheta(G)$, we have $n_{h''} \neq 1$. Thus, as $(v, w) \in h$ and $(v, u) \in j$, there exists $t \in u\langle h''\rangle$ such that $(v, t) \in j$ and $(w, t) \in j$; see Lemma 2.

Since $(v, t) \in j$ und $vk \subseteq \mathrm{Fix}_X(\phi)$, $tk'' \subseteq \mathrm{Fix}_X(\phi)$; see Proposition 3. Since $(t, w) \in j$ und $tk'' \subseteq \mathrm{Fix}_X(\phi)$, $wk \subseteq \mathrm{Fix}_X(\phi)$; see Proposition 3 and recall that, by Lemma 3, $k'''' = k$.

Since $x \in wk$, we thus have $x\phi = x$.

Since $x \in L^n$ has been chosen arbitrarily, we have shown that $L^n \subseteq \mathrm{Fix}_X(\phi)$, contrary to the choice of n.

This contradiction finishes the proof of Theorem 2.

References

1. J. Tits: *Buildings of Spherical Type and Finite BN-Pairs.* (Lecture Notes in Math. 386) Springer, Berlin Heidelberg New York, 1974.

2. J. Tits: A local approach to buildings. pp. 519-547 in: *The Geometric Vein (The Coxeter Festschrift)* (C. Davies, B. Grünbaum, and F. A. Sherk, eds.), Springer, Berlin, 1981.

3. P.-H. Zieschang: *An Algebraic Approach to Association Schemes.* (Lecture Notes in Math. 1628) Springer, Berlin Heidelberg New York, 1996.

Appendix A

Group Theory in Japan

参考資料：私信１

坂内君

松山での宿の予約をして戴いた由有難う、19 日の午後 2 時過ぎに松山に着く予定です。話の準備として 1952 年までに発表された群論関係の論文の List をつくってみましたので同封します。完全なものではないのですが興味のある人には copy を差し上げようと思ったのです。実は今日ここにとどいていた彌永先生の御論文集をみていたら (1939) が抜けているのに気づきました。disc をもって来なかったので、新しい system にうち変えねば修正出来ないのが残念です。1940 年までのは主に Zentralblatt にたよったので位相群関係の論文が多く入っていますが Math. Rev. になってからはそれは省いてあります。1940 年で一つきった理由は Math. Rev. の発刊とか、戦争とかありますが、1941 年になると、岩澤先生の御論文や、中山先生の中山予想に関するものなどすぐれた論文が発表され日本の群論にとって一期を画する時だったからです。次に、1952 年には我々の世代が論文を発表はじめた年だし、日本の群論にとっては伊藤昇氏が 1950 ~ 1952 に驚くべき多数 (11) の、しかも示唆に富むすぐれた論文を相ついで発表され、ここに日本の群論がまさに世界の最先端に立っていることをほこらかに示した記念すべき年だと思います。そのあとも群論関係の論文を集めてみたのですが多くなりすぎて、それに Math. Rev. を調べれば出てくることなので、あまり意味がないと思いやめてしまいました。

一昨夕大磯に着いて、まだ時差になれていないようです。Padova ではたのしく一ヶ月すごしました。群とグラフという題で 8 回 seminar で話しました。Out$G$ が任意の群になるという松本君の定理も一題目として話したのですがその時丁度 Obraztsov という O‘lschanski(?) のお弟子さんが来ていて、その人は前に Tarski Monster T を適当に選べば Out$T$ が任意の有限群になるという定理を証明しているのですが、翌日には、Tarski Monster ではないけれど、同じような “単純群” S を適当にとれば Out$S$ が任意の群になるということが証明出来るといって来ました。勿論自分の仕方の方が簡単だ、S が単純群になるといっていました。私はこのような無限群には直観がないので、どこが証明にきいて来るのか分かりません。松本君の論法だと理由がはっきりしていると思うのですが、与えられた有限群 A に対して Out$G \cong A$ となる “有限群” G があるでしょうか。松本君にしろ Obraztsov にしろ無限群をうまくつかってるようです。

では近くお会い出来るのをたのしみに、みなさまによろしく。

1994 年 6 月 11 日　鈴木通夫

参考資料：私信２

坂内君

松山での会は盛会でたのしく過ごしました。帰途佐藤幹夫さんとこんなに若い人達が大勢集まって熱心に聞いて下さって楽しかった。この中からすぐれた人が出てくれれば良いと話し合ったことでした。どうも有難う。

ずっと前の御便りでは何か報告集のようなものを計画されているとかでしたので原稿の一部をおくります。大体第一日目の話の部分です。コピーはとってないのでこれだけですが、二日目の分も入用でしたらお知らせ下さい。皆様によろしく、十二月にまたお会い出来るのをたのしみにお体お大切に　お元気でお過ごし下さい。

七月二十六日

鈴木通夫

日本の群論
(Remembrance of things past)

鈴木 通夫

日本の有限群論の回顧と展望という主題の会で何か話すように頼まれたので一応「日本の群論」という題をつけました。しかし昔のことはともかく1952年以後は私が日本を離れていますので話が自己中心になってしまうかと心配しています。

題を「日本の群論」として「有限」を省いた理由は無限群を含めて群論を考えるべきだと信じるからです。私は有限群論にしか貢献出来なかったのですが私の論文の中にも、無限群論から Hint を得たものがあります。日本でもこれから、昔の日本の群論がそうであったように、有限群だけにとらわれない群論一般にわたる発展を期待したいと思います。

（副題は、そのまま日本語に直訳して下されば私の思っていることに近いので、つけました。実はこれは借り物です。御存じの方も多いと思いますがこの副題は、T と P とを大文字に変えたものが Proust の有名な小説の英語訳についている題なのです。もとの題は À la recherche du temps perdu。私は perdu という言葉のもつ感じが良く分からないのですがこの本の日本語訳についている題がもっているかと思われる感傷的な気持ちを附加しているわけではありません。）

Zentralblatt と Math. Review をざっと調べた所、日本人で群論関係の論文を書いた人の数は1979年までで約225人でした。Zentralblatt では位相群も群論に入っていたため、1940年までは位相群に関する論文も数えましたが Math. Review になってからは位相群関係の論文は省きました。代数群関係の論文も入っているのがありますが、その範囲はあまりはっきりせず、その時の気分で分けてしまいましたので、正確なものではありません。統計をまとめると次のようになります。

	人数	論文数
1940以前	21(17)	84(67)
1941 ～ 1952	35	91
1953 ～ 1960	48	99
1961 ～ 1970	89	244
1971 ～ 1979	128	362
合計	223	880(863)

戦前の雰囲気

此の前、岩澤先生から1933年に当時の岩波講座「数学」の月報(7月)に竹田さんが書かれた「有限群論の参考書その他」という一文のコピーを戴きました。その当時の雰囲気がつたえられるかと思いますので一部を紹介します。

> "抽象代数学的立場から有限群論だけに焦点を合わせた本が現れると良いと思うのであるが、現在此の如き本が無いので ...有限群論に関する委しい理論特にその細かいしかも綺麗な定理の幾多を味わって見度いと御思いになる方の為に ..."

と Burnside, Speiser, Miller-Blichfeldt-Dickson, 園先生（高等代数学上）をあげ、それらの特色を正確にのべています。そして

> "今若し有限群論の本を唯一冊だけ読んで、しかもその理論の尖端まで達したいと云われる方があるならば 私は Speiser の本を推薦するに躊躇しない"

と書いてあります。最後に群の歴史にもふれ

> “「不遇の間に夭折した二人の天才の手によって播かれた種は今日空の鳥を宿す
> 程の大樹になった」と言っても過言では無かろう”

と結んでいます。

群論の歴史

Galois の大きな功績の一つは単純群という概念を発見したことであると思います、Galois は方程式の群—今の言葉でいえば可分方程式の分解体のガロア群—を根の上の置換群として把握しており、最小の非可換単純群の位数が 60 であることを知っていました。しかし、それが今皆さんがお考えのように、5 次の交代群であると Galois が意識していただろうかと Peter Neumann が疑問を提出しています。Galois にとって興味ある群は合同一次分数変換群つまり $z' = \frac{az + b}{cz + d}$ という形の変換の集まりで、変数 a, b, c, d は整数で、ある素数 p を法として考え $ad - bc \equiv 1 \pmod{p}$ をみたすもの。この群は一般に可解群ではなく、特に $p = 5$ の場合に位数 60 の単純群が得られることを証明したのです。

Galois 以後群論は多方面に分流して発展していきます。今述べた合同変換群の方向では Jordan の “置換論”(1870) から Dickson の “線形群”(1901) を経て Dieudonne の “線形群の幾何”(1940 以降) に達し第二の分流 Lie 群の理論と合わさって現代の代数群論に発展します。Lie 群の理論からは一般の位相群論も発生しました。第三が Kronecker, Frobenius による抽象群論です。

今世紀はじめの古典的有限群論の成果は Burnside の本に委しく述べられています。1920 年代の中ばに Schreier による群の拡大理論や、自由積の定義などが発表され、1928 年には P. Hall の最初の論文が出て、ここに近代群論、有限群論が始まりました。この P. Hall の可解群の理論、のちの (1933 年) 巾零群の理論は 1937 年に刊行された Zassenhaus の “群論” の中に紹介され、その後の群論の発展に大きな影響を与えたと思います。私もこの本で群論を勉強しました。P. Hall はその後も可解群、その他について基本的な論文を発表して近代有限群論を造り上げ、1940 年には、Wielandt の移送定理なども現れたのですが戦争のため群論の発展は一時中断されました。

日本の群論 (1940 以前)

この間における日本の群論の様子を見てみましょう、位相群に関して角谷さんの不変距離が導入されるための条件 (1936)、淡中さんの相対定理 (1938) などのすぐれた研究があります。数論関係では荒又さんの、ζ 関数の整除性定理 (1933)、彌永先生によるイデアル単項化定理のきれいな証明 (1934) など共に群論の定理に言い変えて証明されたものです。また有限群の表現論の基礎についての正田、浅野、大島、中山の諸氏の著しい結果があります。

有限群論に関する主な結果は竹田さんの M- 群の可解性の証明 (1930) および正田先生による忠実な既約表現をもつ有限群の決定 (1930–1931) だと思います。M-群というのはすべての既約表現が単項表現つまり部分群の一次指標から誘導された表現と同値なる有限群のことです。既に Burnside の本にも、素数巾位数の有限群、一般に有限巾零群は、M-群になるという Blichfeldt の定理がのっていますし、Speiser の本には M-群 G の交換子群 G' は 1 であるか、又は G の真の部分群になるという定理が証明されています。竹田さんの定理はこの定理を或る意味で完成したもので本質的な進歩といえると思います。竹

田さんの論文には、Blichfeldt の定理の拡張も証明され、M-群ではない可解群もあることが例示されています。

Burnside の本の第2版 (1911) には巻末にいくつかの Notes がついています。有名なものは第13番目の Note M で奇数位数の有限群は可解であるという、いわゆる Burnside の予想に関するものです。第6番目の Note F では忠実な既約表現をもつ有限群について、まずそのような有限群の中心は巡回群であることを証明し、この逆は必ずしも成り立たないことを例示しています。そして一般にこのような群の構造を決定することは未解決の問題であると述べています。さらに素数巾位数の群の中心が巡回群ならば忠実な既約表現があること、非可換単純群の直積は忠実な既約表現をもつこと、および忠実な既約表現をもたない有限群は、ある素数 p について、位数が p 巾の極小正規部分群を少なくとも2つもっていることなどを証明しています。このようなヒントにもかかわらず忠実な既約表現をもつ群の構造についての研究は1930年まで全く進展しませんでした。それは、このような有限群の構造を調べるためには表現論的な方法が必要となり、そこで使える表現論が1920年代の後半にやっと完成したためだと思います。正田先生は有限群 G が既約な忠実表現をもつための条件を次のように述べました。G の極小正規部分群のうち可換群であるもの全体が生成する正規部分群を A とします、G が既約な忠実表現をもつために必要かつ充分な条件は：

> A の部分群 H があって、A/H は巡回群、H に含まれている G の正規部分群は1に限る

ことである。この条件は次のように述べることも出来ます。いま G の可換極小正規部分群の一つを V とします。Schur の補題により $F = End_G(V)$ は斜体で V は F 上のベクトル空間となります。そこで V の F 上の次元を $d = d(V)$ と書きましょう。A は可換な極小正規部分群の直積ですが、その直積因子のうち V と作用同形になるものの数を $r = r(V)$ とすれば、上の2条件は "すべての V について $d(V) \geq r(V)$" と同値になります。正田先生も同様な結果を書いておられるが不完全で、上の形は秋月によるものです。この辺のいきさつについて私は当事者達から直接うかゞったことはないのですが、間接的に聞いた話によれば、正田先生の論文が発表された時点で秋月は既に定理の上述の形を知っていたらしい。この条件が前述の2条件と同値であることの組み合わせ論的な一証明が次の恒等式を用いて得られます。q 元体上の r 次元ベクトル空間に含まれる i 次元の部分空間の数を $\varphi(r,i;q)$ と書けば

$$\sum_{i=1}^{r} \varphi(r,i;q)(X-1)(X-q)\ldots(X-q^{i-1}) = X^r - 1.$$

この竹田、正田の定理は以上のべたことから明らかなように当時の有限群論から一歩進んだ独自の研究といえると思いますが、日本の数学が孤立していたためと、偶然でしょうが丁度1930年に発刊された Zentralblatt には取り上げられなかったため一般の注意を引くに至らなかったのが残念に思われます。1937年には Speiser の本の第3版が出たのですがそこでも M-群に関する記述はもとのままの不完全な形でした。竹田の定理を最初に取り入れた教科書は岩波の高等代数学上 (1952) で外国語では Curtis-Reiner の表現論が最初と思います。このことについて一言つけ加えさせて戴きます。Curtis-Reiner のもとの本が出版される2～3年前のことですが、Marshall Stone から Curtis-Reiner の原稿を出版社のために読むことを頼まれました。その時の原稿の内容は出版された現在のものよりずっと少なく、たぶんに "お座なり" ともいえる感じのものでした。そこで若気の至りで、これも入れた方が良い、あれも入れた方が良いとずい分勝手な注文を書いて返した中の一つが竹田の定理でした。Curtis-Reiner が取り上げたことが1960年代になって、M-群

に関する興味がふえて来たことの一つの理由になっているかも知れないと思っています。Speiserの第3版に名前ののっている日本人は高木、正田の二先生だけです。Zassenhausの教科書には彌永先生による単項イデアル定理の証明が紹介されています。1959年に出たM. Hallの“群論”でも日本人の定理は岩澤先生の一定理が証明されているだけです。1960年代になるとHuppert, Gorenstein, Kuroschなどの本に日本人の仕事が数多く紹介されるようになりました。

私がM-群に興味をもつようになったのは伊藤さんの影響によると思います。あとで述べますが伊藤さんは1950 ～ 1952年に11編ものすぐれた論文を発表しておられますが、そのうちの一つでSylow群がすべて可換群となるような可解群はM-群であることを証明して後の発展の糸口を与えました。当時は春秋の日本数学会が東京と京都で交互に開催されていたのですが交通事情が今の様ではなく、会に出席するのはかなり困難でした。しかし学会の折に阪大、名大の人達と会えるのがたのしみで、工面して会に出かけたものです。その或る時、伊藤さんから、M-群の話をうかゞい、M-群の部分群（正規部分群だったでしょうか）は必ずしもM-群にならない例などを教えて戴きました。又同様な会の時本郷の食堂で極小非p-巾零群の構造を教えて戴いた時のことなど、なつかしく思い出します。このように伊藤さんから多くの問題の本質的なところを習ふことが出来たことは大変有益でした。

1941 ～ 1952

1941年を境として日本の群論は世界の最前線に顔を出します。それは戦前の活動により、日本数学会の地位が全体として上がったことにもよると思われますが主として中山先生による対稱群のモジュラー表現の研究および岩澤先生の最初の3つの論文が1941年に発表され世界の群論学者の注目をあびたことによると思います。発表されてまもなく戦争が始まり一般の注意を引くのにやや時間がかかりました。中山先生の数ある論文の中でも私はこの対稱群に関する論文が大好きなのですがここで提出された予想は後日モジュラー表現論の進歩によりBrauer-Robinsonにより証明されました、中山–大島両氏による別証明もあります。

私達が大学に入学した当時の情況について附記します。私が入学したのは1945年4月、東京はそのすぐ前3月10日の大空襲で下町の大半が焼かれてしまったので、東大数学教室は諏訪湖の近くの長地村に疎開し、そこの小学校を借りて授業をうけました。岩澤先生がはじめて代数の講義をなさった年でvan der Waerden式のとても良くまとまった御講義で最後にeの超越性の証明がついていたと思います。入学した時は、あとどれだけの間勉強を続けられるかと思っていたのですが、夏休みの間に終戦となり、秋には本郷にもどって途中でとぎれることなく講義を続けてうけることが出来たのは幸いでした。

私達の世代が群論研究を始めた時点つまり1948年から1952年の頃には日本の研究水準は既に世界のレベルに達していたと思います、それはひとえに、正田、中山、高橋、大島、岩澤...の諸氏の御努力のお陰によるものです。私達はすぐに当面の問題に取り組めたし、その問題を解くための筋道についてもかなり具体的なプランがたてられたのは大変幸運であったと思います。

1952年を一時期の終わりというか、新時代の出発点とみて時期を画した理由は、それが戦後の私達の世代が論文を発表し出した時で、日本の群論研究がまさに最先端にあることをはっきりと示した時だからです。なかでも伊藤さんは1950 ～ 1952年の短期間に11編もの、表現論からp群の性質まで広範囲にわたる、すぐれた論文を発表されました。その中には、今でも伊藤の定理として引用されるきれいな定理もあるし、群の積分解や、p可解という概念など当時大きな進歩を与えただけでなく、これらを発展させる試みが伊藤

さん自身を含め多くの人達により進められ群論の大きな部門に発展して行きました。この辺のことについては伊藤さんにお話をうかがえるかと思います。

私自身のことについていえば、始めて印刷された論文はpartitionをもつ有限群の構造を調べたものです。群Gのpartitionとは部分群の集まり$\mathcal{H}$で$|\mathcal{H}| > 1$かつGの非単位元は$\mathcal{H}$の唯一の部分群に含まれるという条件をみたすものです。私がこの概念を習ったのは、ある年の数学会の年会で高橋さんが群の自由積がpartitionをもつ無限群という定理をお話になった時です。その話しを聞いてまもなく、partitionをもつ無限群は多いが有限群ではさほど多くないということについて論文を書きました。それから10数年たって、KegelやThompsonなどのpartitionと関連した結果をつかって、partitionをもつ有限群の構造をすっかり解明することが出来ました。はじめのいくつかの論文のうち一番苦労したのは単純群$PSL(2,p)$が真の部分群の構造によって決定されるという定理です。$PSL(2,p)$の真の部分群の構造は既にBurnsideの本に、その表が出ています。或る時、岩澤先生のお宅にうかゞった時、先生が、この逆の問題つまり単純群Gの真の部分群がその表のうちの一つに同形である時、或る素数$p > 3$に対して$G \cong PSL(2,p)$となるかという問題を考えたことがあるというお話をうかゞいました。そして、その時シロー群の構造までは決まったのですよと教えて下さいました。家に帰ってから考えてみたら、シロー群の構造までは分かったのですがそれから先が仲々進みません、大分長い間ガタガタしたあげく、こんなことをしても新しい情報は得られないだろうと思っていた方法によって、Gの既約表現の性質がすこしずつ分かって来た時の気持ちを昨日のように思い出します。あとでBrauerとの文通によって、丁度いわゆる例外指標が出ていたことがはっきり分かったのですがその時は強い仮定のもとで計算していたため、例外指標の出て来る仕組みをはっきりつかめていなかったのです。問題の条件を弱くして考えると良いことがあるという一つの例です。

戦後日本の有限群論で一つの中心問題となったのはBrauerのblock理論の諸定理に証明をつけることでした。Brauerは1944年から1946年にかけてblockの理論について3つのNotesをProc. NASに発表し多くの定理を証明なしに述べました。これらの定理はblock理論の核にある重要な定理です。証明がついていなかったので、その証明をつけることが当面の問題となりました。そのうち第一主定理は証明出来たのですが第二主定理の証明はなかなか出来ず、大島、飯塚、永尾などの諸氏の努力によって、数年後飯塚さんがとうとう証明されました。これが、第二主定理の証明のなかで一番はじめに印刷されたものだと思います。Brauerの原証明はずっと複雑であったこともあって、Brauer自身の証明はずっとおくれて発表されました。そのあとすぐに 永尾さんによる加群的なしかし同値な定理が証明され、これがGreenによるモジュラー表現論のリストラに近いため標準的な証明となっています。

私は1952年1月から イリノイ大学のBaer先生の所に留学しました。これには中山先生のお陰が大きいと思います。中山先生は1950年に米国のCambridgeであったICMに出席されたあとイリノイ大学に1年おられ、Hochschildと一緒に類体論のコホモロジー的研究をなさっていました。そこで私のために大学のfellowshipを出すにあたって色々御力ぞえ戴いたのです。当時イリノイではBaer先生のところでD. G. Higmanがfocal部分群について学位論文を丁度書き上げた所でした。Higmanはその前に部分群の束の準同型対応に関する論文を書いていたので名前を知っていたこともあってすぐ友達になりました。 イリノイ大学の春学期は後年Brauer-Suzuki-Wallの論文(1958)に書かれている定理の第2の場合の拡張に当たる定理を証明したり、Brauerのblockに関する第一主定理の証明の整理などで過ごしました。

1952年の夏学期には、Brauer先生がMichigan大学に呼んで下さったので、2ヶ月アナーバーで過ごしました。 丁度先生がMichiganからHarvardに移られる前の夏でした。着いたらすぐ電話するようにとのお言葉に甘えて、駅から電話したらすぐ迎えにきて下

さり、初対面の学生の下宿探しまで手つだって戴き今から思っても冷や汗が流れることでした。

その時日本でblock理論に証明をつけようと多くの人達が努力しているがまだ第二主定理の証明は出来ないと話したところ、興味があるならといって先生の原稿を見せて下さいました、まず驚いたのはわら半紙のような紙に大きな字で鉛筆で手書きされた原稿の分厚かったこと、そしてその最後の頁に、checkされた日附けが1、2年程の間をおいて2つも入っていたことでした。証明を書き上げてからも、何度も読み返して万全を期され、改良の余地を求めておられたのだと思います。2、3日後に原稿を返してほしいとのことで、先生の証明は勉強出来なかったのですが、Brauer先生のInduction定理の最初の証明のように複雑なものだったように思います。

後日Brauer-Suzuki-Wallの論文にまとめられたWallの論文の原稿もこの夏には出来上がっていたと聞いています。この辺のいきさつについてはSandy Greenが書いたBrauerのObituaryに載っています。

夏の間、週1回か2回、それまでに私のした数学の紹介をさせられました。何しろ英語で話をするのははじめてだったのでBrauer先生も困られたことと思います。とにかく私が話して一区切りになると、Brauer先生がそれを解説して下さるという言ってみれば英語を英語に翻訳するという奇妙なゼミでした。Feitが丁度大学院生で、このひどいゼミを聞かされた学生の一人でした。

Zassenhausとの出合い (1955)

昭和26年(1951年)秋に京都での学会で話した$LF(2,p)$の特長づけについての論文は、岩澤先生に出して戴いた問題を解いたもので私にとって思い出深い論文ですが、この岩澤先生の問題の解にはもう一つ思い出があります。それは私がZassenhausに始めてあった時のことです。あれは1955年で、ZassenhausはカナダのMcGill大学にいたのですが、Sabbaticalの休みをとって1年、Princetonの研究所に来ていました。そしてPrincetonに一日話に来るようにとまねかれ、Zassenhausに始めて会いました。20年も前にあの群論の教科書を書いた人だからばく然と老大家のように思っていたのですが会ってみるとその若いのにまずびっくりしました、当時まだ45才になっていなかったのではないでしょうか。思いがけず、$LF(2,p)$の特長づけの論文の話が出て、Zassenhausもあの論文を読んでくれたと知って、とても嬉しかったことを思い出します。最後にGが$PSL(2,p)$に同形になることを示すのにモジュラー表現をつかったのはどういう理由ですかと聞かれました。論文を書いた時はモジュラー表現論しか武器をもっていなかったのです。しかしZassenhausに会った時は後日いわゆるZassenhaus群を調べる時活躍した構造関係式、つまりZassenhaus自身が2重可移群を調べる時使った方法の拡張をつかって、Frob核が可換なZassenhaus群の構造を決定したばかりの時でしたので、“あなたが2重可移のZassenhaus群の分類に用いた方法でも出来ます”と答えることが出来ました。その時Zassenhausも核が可換の場合の分類は出来ているといっていました。この定理は、何年かたってからFeitにより再（々）発見されました(1960)。

当時Zassenhausは2つのsubnormalな部分群から生成される部分群が必ずしもsubnormalでないという最初の例をつくった所で、食事をしながらその群の生成関係などナプキンに書いて熱心に説明してくれました。そのナプキンはまだ大切にとってあります。

CA 群の論文 (1954 ~ 1956)

CA 群の論文といえば、あの証明を思いつくまでに一年程あれこれと、さまざまなことをしてみたのですがうまく行かず、半ばあきらめかけていたのですが、ある日ぱっと証明の筋道が目の前に浮かび、証明の正しいことは全く自明のことのように見えました。Poincareが何かに書いていますが、馬車のステップに足をかけた途端、ある一つの定理の証明全体が頭に浮かんだというのと同じことだと思います。論文を書き上げて、Proceedingsのeditorをしていた Brauer 先生に送ったのですが一年たっても一年半たっても返事がありませんでした。そのうち1956年の秋から Brauer 先生の所へ勉強に行くことになりその夏の終わりにハーバードに行きました。会うなり Brauer 先生が“あの論文は refereeが自分には読めないといって送り返してきた。そこで私が自分で読もうと思うが、丁度ここに来ているのだからセミナーで話して下さい”と言われ、びっくりしました。論文の証明が間違っている筈はないし、と思って読み返してみたら、証明が完成するまでの長い間、ごたごた考えていたことで、この証明にはいらないことが澤山書いてあって非常に不透明な論文になっていました、そこを整理して書き直したら２時間程ですっかり説明できるようになりました。ゼミが終わったら Brauer 先生が“こんな簡単なことをあの referee はどうしてわからなっかたのだろう”と言われましたが、それは referee のせいではなく、論文の書き方が悪かったからです。このため CA 群の論文は証明出来たと思ってから３年たった1957年に印刷されました。Harvardにいる間は Brauer 先生のはたで一生懸命勉強しました。岩澤先生も近くにおられ、はげましていただけたのは幸いでした。

1957 ~ 1960

Harvardから帰った年の秋(1957)から秋月がシカゴ大学に客員教授として一年来たので、週末にはシカゴに行くことが多くなりました。そのことを知った MacLane から土曜の午后にシカゴ大学で MacLane の学生達のために群論の話をするように頼まれました。何人かとても熱心な学生がいましたが、そのうちで特に熱心な学生が Thompson でした。ある時など翌日曜日に訪ねて来て“昨夜一晩中 officeで考えていたのだが”と前日の話の続きを議論しに来たりしました。その頃の思索がまとまって、Frobenius 核の巾零性に関する彼の学位論文となり、ここに現代有限群論が本格的に始まったといえると思います。

またこのことが源となって Albert と MacLane が世話役となり、1959年春に、始めて有限群論を中心とする学会が NewYork で開かれました。この会には、その時ミシガン大学に来ておられた永尾さんも参加されました。Albertは引き続いて有限群論の会を計画しました。それは有限群論の若い研究者達を一年シカゴ大学に集め、教える時間など出来るだけ少なくして研究に専心出来るようにしたものです。会の期間中に Brauer や Wielandt も短期間来られました。この会がその後の有限群論の発展にどれだけ有益であったかは歴史が明示している通りです。日本からこの会に伊藤さんが来られ、この期間中の最大の収穫であった Zassenhaus 群の分類に大きな貢献をなさいました。この年は彌永先生もシカゴ大学の客員教授として来ておられましたので、まるで日本にいるような気分で有益だった一年を過ごしました。

その次の年には伊藤さんにイリノイ大学に来て戴いてまた、楽しい一年を過ごしました。イリノイ大学に来た日本の数学者は多数いますが、有限群関係では、佐藤正次さんが1955年から３年間、1962年に伊藤さん、1964年から２年間都筑さん、1970年に原田さん、最近では宮本君が来られました。短期間ではありましたが1970年代に榎本、坂内、五味君達、最近には山田、飯寄君らが来て下さいました。

Zassenhaus 群の分類のきっかけとなったのは、シカゴの会の半年程前の1960年１月

に Zassenhaus 群の一系列（鈴木群）が発見されたことでした。その頃 CN 群の分類を完成させようとし努力したのです。ところが $SL(2,2^n)$ と似た群がでて来てそれが SL になることを証明すれば分類が完成するという段階になりました、あとから見ればこれは間違った方向に進もうとしていたわけです。考えられるがぎりの手段をつくしているうち、そのことが証明出来たと思えたので、大そう喜んで Brauer 先生と Thompson にこんなことが出来たと手紙を書いてしまいました。ところが 2、3 日たって読み返してみたら見落としのあることを発見して、あわてて訂正の手紙を出しました。Thompson には "何か、non-trivial なことが証明されているようだ" と書いたそうです。今ではどうしてこんなことを書いたのか分かりません。あとで鈴木群の構成を知った Thompson が "こんなに non-trivial なこととは思わなかった" と電話してくれました。

シカゴの会のあとには群論の集会がしばしば開かれるようになりました。1968年にはプリンストンの研究所で一年間代数群と有限群を主題とした会がありました。この会は日本から岩堀さんと原田君が参加されました。これより前から岩堀さんは松本君達と協力して代数群を中心に研究を進められ、岩掘部分群などの概念を発見されました、これらのことについては、この会で横沼さんのお話がありますのでそちらにゆずります。又、この頃以後の日本の群論研究の様子は他の講演によって明らかになると思います。ただ 1974 年に谷口資金を主とした有限群論の会が札幌、京都で開かれたことを一言述べておきます。この会には外国からも多数参加し、日本の群論関係者達の献身的な御努力によってとても盛会でした。会で、当時の単純群論の成果が相ついで発表されただけでなく、その時の参加者達の活気ある熱心な討論によって、それからあとの単純群論の発展に非常に大きな影響を与えたことが特記されるべき点だと思います。

結び

日本の（有限）群論について述べよという坂内君からのお話でしたが、やはり、話が自己中心となり、かたよった見方になってしまったかと思います。現在、有限単純群の分類は一応完成したとはいえ、単純群の性質について何かを証明しようとすれば、個々の単純群を調べてみなくてはならないというのが今の状態です。これからは、分類定理を利用して一般の有限群を調べる方向と共に、単純群のもっている性質をもっと解明することが大切だと思います。もう一度三十年前にさかのぼって有限群論の発展をかえりみることもあながち無用のことではないように思われます。

1994 年 7 月 20 日、21 日
代数的組合せ論サマースクール（愛媛）にて

Appendix B

Publications by Japanese Mathematicians in Group Theory before 1952

(with Professor Michio Suzuki's Memo)

Group Theory in Japan before 1941

Source: Proc. Imp. Acad. Tokyo, Japanese J. Math. and
Zentralblatt für Mathematik Band 1 (1930) - Band 28 (1944)

[A]

Aramata Hideo: Über die Teilbarkeit der Zetafunktionen gewisser algebraischer Zahlkörper, Proc. Imp. Acad. Japan 7 334-336 (1931). *A special case of the theorem proved in the next paper.*
—: Über die Teilbarkeit der Dedekindschen Zetafunktionen, Proc. Imp. Acad. Japan 9 31-34 (1933). *Divisibility of zeta-functions in the Galois extension of a number field: a proof of the equivalent statement in character theory.*
—: Über die Eindeutigkeit der Artinschen L-Funktionen, Proc. Imp. Acad. Japan 15 124-126 (1939). *The uniqueness of Artin's L-function when $Gal(K/k)$ is $LF(2,p)$.*

Asano Keizo: Über die Darstellungen einer endlichen Gruppe durch reelle Kollineationen, Proc. Imp. Acad. Japan 9 574-576 (1933). *Determination of the cohomology group of the 2-cocycles over the real numbers which is an elementary abelian 2-group.*

Asano Keizo, and Shoda Kenjiro: Zur Theorie der Darstellungen einer endlichen Gruppe durch Kollineationen, Comp. Math. 2 230-240 (1935). *Existence of the representation group is proved over an algebraically closed field in a new fashion; a new proof on the bound of the number of isomorphism classes of the representation groups; when the characteristic of the field is prime to the order of G, a method is given to find all representations in collineation groups.*

Asano Keizo, Osima Masaru, and Takahasi Mutuo: Über die Darstellung von Gruppen durch Kollineationen in Körper der charakteristik p, Proc. Phys-Math. Soc. Japan III 19 199-209 (1937). *A representation group G of a group H in characteristic p is defined as a group having a normal subgroup A such that $A \subset Z(G) \cap G'$, $G/A \cong H$ and $|A|$ is equal to the number of classes of equivalent factor sets over an algebraically closed field of characteristic dividing $|H|$. Existence is proved as in the characteristic zero case; denoting the corresponding groups in characteristic zero by G_0 and A_0, it is proved that $G \cong G_0/S$ where $S \in Syl_p(A_0)$. The number of essentially different irreducible projective representations over a given factor set is determined. Proof uses twisted group rings.*

[I]

Iyanaga Shokiti: Zum Beweis des Hauptidealsatzes, Abh. Math. Sem. Hamb. Univ. 10 349-357 (1934).

Simplified proof of the principal ideal theorem using the improved version of transfer theory and the splitting groups due to Artin.

[K]

Kakutani Shizuo: Über die Metrization der topologischen Gruppen, Proc. Imp. Acad. Japan 12 82–84 (1936). *Every Hausdorff group with the first countability axiom possesses a left invariant metric.*

Kawada Yukiyosi: Charaktere linearer Gruppen, Proc. Imp. Acad. Japan 15 71–75 (1939). *The characters are computed for the group of the type $Px = w^i x + \alpha$ where w is a fixed element of a finite field F and $\alpha \in F$; some applications on Artin's L-functions.*
—: Über die Überlagerungsgruppe und die stetige projektive Darstellung topologischer Gruppen, Japan J. Math. 17 139–164 (1940).

Kodaira Kunihiko: Über die Differenzierbarkeit der einparametrigen Untergruppen Liescher Gruppen, Proc. Imp. Acad. Japan 16 165–166 (1940).

Komatu Atuo: Über einige Komponenten Gruppen, die topologische Invarianten sind, Proc. Phys. Math. Soc. Japan III 19 210–214 (1937). *Topology.*

Kondo Koiti: Über die Zerlegung der Charaktere der alternierenden Gruppe, Proc. Imp. Acad. 16 131–135 (1940) *The decomposition of characters of A_n into the subgroup A_{n-1}.*
—: Table of characters of the symmetric group of degree 14, Proc. Phys-Math. Soc. Japan III 22 585–593 (1940).

[N]

Nakayama Tadasi: Some studies on regular representations, induced representations and modular representations, Ann. of Math. II 39 361–369 (1938). *Study on general algebras; generalizations of Frobenius reciprocity theorem for nonsemisimple algebras and their applications to representation theory of finite groups.*
—: A remark on representations of groups, Bull. AMS 44 233–235 (1938). *A theorem corresponding to the Frobenius reciprocity theorem is proved for the ring of almost periodic functions on a group.*
Nakayama Tadasi and Shoda Kenjiro: Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen, Japanese J. Math. 12 109–122 (1936).

[O]

Osima Masaru: Beweis eines Satzes in der Darstellungstheorie, Proc. Imp. Acad. Japan 13 121–124 (1937). *The p-modular representations induced from the irreducible representations of a normal subgroup H of index prime to p are completely reducible and the number of nonequivalent ones is equal to the number of conjugacy classes of p-regular elements that are contained in H.*
—: Über die Darstellung einer Gruppe durch halblineare Transformationen, Proc. Phys-Math. Soc. Japan III 20 1–5 (1938). *A study of representations by semilinear transformations in terms of the representation induced on the fixed subgroup.*

Osima Masaru, in Asano-Osima-Takahasi

[S]

Shoda Kenjiro: Über die Automorphismen einer endlichen Abelschen Gruppe, Math. Ann. 100 674–686 (1929–30). *Detailed study of the group of automorphisms of a finite abelian p-group, particularly when $p = 2$; a condition for the solvability of the group of automorphisms is given.*
—: Über die charakteristischen Untergruppen einer endlichen Abelschen Gruppe, Math. Z. 31 611–624 (1929). *Let A be a finite abelian group, $\mathfrak{o}$ = End A, G = Aut A, and $\mathfrak{g}$ the ring generated by G. Then, $\mathfrak{g}$ may be different from $\mathfrak{o}$; when A is a p-group, a necessary and sufficient condition for $\mathfrak{g} = \mathfrak{o}$ is found. All characteristic subgroups of A are found.*
—: Über die zugehörige Gruppe eines endlichen Ringes, Proc. Imp. Acad. Japan 5 103–104 (1929). *Announcement of the results to appear in Math. Ann. 102.*
—: Über die Einheitengruppe eines endlichen Ringes, Math. Ann. 102 273–282 (1929). *Maximal nilpotent subrings of End A is studied for an abelian p-group A: they correspond to Sylow p-subgroups of Aut A.*
—: Über das Holomorphie einer endlichen Abelschen Gruppe, Proc. Imp. Acad. Japan 5 314–317 (1929). *Representation of the unit group of End(A) for a finite abelian p-group A in terms of matrices, similar to the case of an elementary abelian p-group.*
—: Über den Automorphismenring bzw, die Automorphismengruppe einer endlichen Abelschen Gruppe,

Proc. Imp. Acad. Japan 6 9-11 (1930).

—: Über die Einheitengruppe eines endlichen Ringes II, Proc. Imp. Acad. Japan 6 93-96 (1930). *If A is a finite abelian p-group, then a maximal nilpotent subgroup of the unit group that is defined similar to the group of triangular matrices is a Sylow p-subgroup and the structure of derived series is determined.*

—: Bemerkungen über die Frobeniusche Komposition der Charakter einer endlichen Gruppe, Proc. Imp. Acad. Japan 6 187-189 (1930). *Remarks on equivalence of the results of Frobenius' two papers on group characters.*

—: Gruppentheoretischer Beweis des Äquivalenz- und Enthaltenseinsatzes in der Theorie der Matrizen mit ganzen Koeffizienten, Proc. Imp. Acad. Japan 6 217-219 (1930). *Application of group theory to matrix theory.*

—: Über die Automorphismen einer endlichen zerlegbaren Gruppe, J. Fac. Sci. Univ. Tokyo 2 25-50 (1930).

—: Über direct zerlegbare Gruppen, J. Fac. Sci. Univ. Tokyo 2 51-72 (1930). *Let G be a finite group. The group G has a faithful irreducible complex representation if and only if the union U of all abelian minimal normal subgroups of G contains a subgroup V such that U/V is cyclic and core V = 1; the paper states a condition which claimed to be equivalent to the conditions stated above in terms of the groups induced in the minimal normal subgroups.*

—: Über die irreduziblen Substitutionsgruppen deren Grade Primzahl sind, J. Fac. Sci. Univ. Tokyo 2 179-201 (1931). *A finite irreducible group of unimodular linear substitution groups of prime degree is either monomial or primitive: in the case of a monomial group, the structure of a maximal abelian normal subgroup is completely determined, in the case of a primitive group, less precise result is obtained; from these results, solvable groups of this nature are determined.*

—: Bemerkungen über vollständig reduzible Gruppen, J. Fac. Sci. Univ. Tokyo 2 203-209 (1931). *A study on completely reducible groups with a correction to earlier paper on the Shoda-Akizuki Theorem.*

—: Über die monomialen Darstellungen einer endlichen Gruppe, Proc. Phys-Math. Soc. Japan III 15 249-257 (1933). *The transitive monomial representation corresponds to an ideal of the group ring; using this presentation, equivalence or irreducibility of monomial representations are studied with applications to the representation of a metabelian groups.*

—: Über die Äquivalenz der Darstellungen endlicher Gruppen durch halblineare Transformationen, Proc. Imp. Acad. Japan 14 278-280 (1938). *Every representation G of a group by semilinear transformations gives rise to a faithful representation G^{*} by linear transformations on vriables x_j, x_j^{t} with $x_j^{t} = \sum a_{jk}^{t} x_k^{\tau t}$. Relations between the equivalence of G and H and that of G^{*} and H^{*} are studied.*

—: Über die Invarianten der endlichen Gruppen halblinearer Transformationen, Proc. Imp. Acad. Japan 14 281-285 (1938). *Let G be a group of semilinear transformations over a field K of char(K) = p with $A \subset Aut(K)$, H the fixed subgroup and k the fixed field of A. Then, there exists finitely many polynomials $F_1, \cdots, F_n$ such that invariants of H are polynomials of F_i with coefficients in K and invariants of G are polynomials of F_i in K.*

—: Über die Invarianten endlicher Gruppen linearer Substitutionen im Körper der Charakteristik *p*, Japan J. Math. 17 109-115 (1940). *A new proof of theorem of Noether on finite generation of invariants of a finite group. It is generalized for finite groups of collineations.*

—, in Asano-Shoda

—, in Nakayama-Shoda

Suetuna Zyoiti: Zerlegung der Charaktere einer Gruppen in die Ihres Normalteilers, Japan J. Math. 12 95-98 (1935). *For a group G with normal subgroup H such that G/H is abelian, a concept equivalent to the inertia group of an irreducible character of H is defined and Clifford type theorems are proved.*

—: Abhängigkeit der *L*-Funktionen in gewissen algebraischen Zahlkörper, J. reine. angew. Math. 177 6-12 (1937). *Character decomposition when G/N is the congruence group mod p.*

—: Über die Zerlegung der Gruppencharaktere, Japan J. Math. 16 63-69 (1939). *A detailed study of decomposition of characters when G/N is the congruence group modulo p of order p(p − 1)/q.*

—: Über die Zerlegung der Gruppencharaktere II, Japan J. Math. 16 79-91 (1939). *The decomposition of characters when $G/N \cong A_5$.*

Sugeno Torao: Beweis eines Satzes über Charakter, Proc. Phys.-Math. Soc. Japan III 15 233-234 (1933). *A proof of the theorem that the group of prime residue classes modulo a natural number has a non-principal character.*

[T]

Taketa Kiyosi: Über die Potenzsumme der charaktere einer Permutationsgruppe, Proc Imp. Acad. Japan 4 34–35 (1928). *The sum of the k-th power of the character of a permutation group G over the group is divisible by the order $|G|$.*

—: Über die Gruppen, deren Darstellungen sich sämtlich auf monomiale Gestalt trans formieren lassen, Proc. Imp. Acad. Japan 6 31–33 (1930). *An M-group is solvable; if a finite group G contains an abelian normal subgroup A such that G/A is supersolvable, then G is an M-group; and not all solvable group is an M-group ($SL(2,3)$ is not an M-group).*

—: Über die Primitivität einer auflösbaren Permutationsgruppe, Proc. Imp. Acad. Japan 7 31–32 (1931). *Proof of a theorem that a transitive solvable permutation group is primitive if and only if it has a transitive minimal normal subgroup.*

—: Über die monomiale Darstellung einer auflösbaren Gruppen, Proc. Imp. Acad. Japan 7 129–132 (1931). *A metabelian group is an M-group.*

—: Über die auflösbaren linearen Substitutionsgruppe, Proc. Imp. Acad. Japan 7 179–181 (1931). *A technical result related to Clifford type theorem.*

—: Neuer Beweis eines Satzes von Herrn Fürtwängler über die metabelischen Gruppen, Jap. J. Math. 9 199–218 (1932). *A new proof of the principal ideal theorem.*

—: Über die Struktur der metabelischen p-Gruppen, Proc. Imp. Acad. Japan 9 480–481 (1933). *Construction of a p-group G having a given abelian group A as a maximal abelian normal subgroup and $\Gamma = G/A$ as abelian of largest possible order.*

—: Über die Struktur der metabelischen Gruppen I, Jap. J. Math. 13 129–232 (1937). *Study of maximal abelian substitution groups over $GF(p^s)$.*

Tannaka Tadao: Über den Dualitätssatz der nichtkommutativen topologischen Gruppen, Tohoku Math. J. 45 1–12 (1938). *The Tannaka duality theorem for compact groups.*

Tazawa Masatada: Einige Bemerkungen Über den Elementarteilersatz, Proc. Imp. Acad. Japan 468–471 (1933).

—: Über eine Eigenschaft der hyperkommutativen Gruppe, Proc. Imp. Acad. Japan 9 472–475 (1933). *Hypercommutative (= nilpotent): A finite group is nilpotent if and only if it contains a normal subgroup of every possible order; a new proof of a theorèm of Burnside that such a group is a direct product of Sylow subgroups.*

—: Über die Darstellung der endlichen verallgemeinerten Gruppen, Sci. Rep. Tohoku Univ. I 23 76–88 (1934). *Determination of all representations relative to a given factor set. Twisted group ring is used.*

—: Remarks to some theorems of Burnside, Proc. Imp. Acad. Japan 10 307–310 (1934). *Algebraic proofs of two theorems due to Burnside on the composition of representations of a finite group.*

—: Über die monomial darstellbaren endlichen Substitutionsgruppen, Proc. Imp. Acad. Japan 10 397–398 (1934). *Let $|H| = p^n q^m \cdots$ with $p < q < \cdots$ and abelian Sylow subgroups $P, Q, \cdots$. Let $\theta(P) = (p-1)(p^2-1)\cdots(p^r-1)$ where r is the rank of P. If $\theta(P)$ is prime to h/p^n, $\theta(Q)$ is prime to $h/p^n q^m, \cdots$, then H is an M-group.*

—: Remarks on Frobenius' and Kulakoff's theorems on p-groups, Sci. Rep. Tohoku Univ. I 23 449–476 (1934). *The number of subgroups of order p is congruent to $1+p+p^2 \pmod{p^3}$ if $p > 3$, $\Phi(G)$ is cyclic, and $|G:\Phi(G)| \geq p^3$.*

—: II Sci. Rep.Tohoku Univ.I 24 161–163 (1935). *The number of subgroups of order p^m for $1 < m < n-1$ is congruent to $1+p+2p^2 \pmod{p^3}$ when G has no subgroup of order p^4 of a special type.*

—: Über die Darstellung der beliebigen Gruppen gebrochene lineare Transformationen, Sci. Rep. Tohoku Univ. I 24 352–371 (1935). *With help of von Neumann's theory of almost periodic functions the author studies the almost periodic (bounded) representations of an arbitrary group by linear fractional transformations.*

—: Über einen Satz der abgeschlossenen Gruppen, Tohoku Math. J. 45 154–156 (1938). *Let $M = C^*$. For any finite noncyclic simple group H, there is at least one group G such that $Z(G) = M$ and $G/M \cong H$ with nonsplit extension.*

—: Über die isomorphe Darstellung der endlichen Gruppe, Tohoku Math. J. 47 87–93 (1940) A characterization of those finite groups which admit an faithful representation having exactly n irreducible components.

Toyoda Koshichi: On the adjoint groups of Lie's continuous groups, Sci. Rep. Tohoku Univ. I 24 269–283

(1935).

—: On Casimir's theorem of semi-simple continuous groups, Jap. J. Math. 12 17–20 (1935).

—: On the universal covering group of Lie's continuous groups, Proc. Imp. Acad. Japan 11 405–406 (1935).

—: On the structure of Lie's continuous groups, Sci. Rep. Tohoku Univ. I 25 338–343 (1936). *A new proof of E. Cartan's theorem.*

—: On differential operators permutable with Lie continuous groups of transformations, Proc. Imp. Acad. Japan 13 172–175 (1937). *A new proof of a theorem of Casimir.*

—: On axioms of mean transformations and automorphic transformations of abelian groups, Tohoku Math. J. 46 239–251(1940).

—: On affine geometry of abelian groups, Proc. Imp. Acad. Tokyo 16 161–164 (1940).

—: On linear functions of abelian groups, Proc. Imp. Acad. Japan 16 524–528 (1940). *Axiomatic study of linear functions on abelian groups.*

[W]

Watanabe Sigekatu: Sur les formes spatiales de Clifford-Klein, Japan J. Math. 8 65–102 (1931).

—: Sur un espace qui admet comme groupe d'isométries un groupe donné, continu d'ordre fini, simplement transitif I and II, Japan J. Math. 10 133–150 151–162 (1933).

[Y]

Yamada Kaneo: Über Gruppen mit Bases, Tohoku Math. J. 44 406–109 (1938). *Groups with base are defined, and proved that they are solvable. If the order is odd, G is abelian.*

—: Über die Gruppen mit basen II, Tohoku Math. J. 45 308–309 (1939). *Conditions for a group to be solvable when it is a product of cyclic groups.*

—: Ein Kriterium für die Nichteinfachheit der Gruppen, Tohoku Math. J. 46 44–45 (1939). *Let H be a subgroup of index n of a group G. If G has an element of order $p^r q^s \cdots$ with $p^r + q^s + \cdots > n$, G cannot be simple.*

Yamanouchi Takahiko: On the construction of unitary irreducible representations of the symmetric group, Proc. Phys-Math. Soc. Japan III 19 436–450 (1937). *Inductive construction of irreducible representations of S_n.*

Yosida Kosaku, A note on the continuous representation of topological groups, Proc. Imp. Acad. Japan 12 329–331 (1936).

—: A remark on a theorem of B. L. van der Waerden, Tohoku Math J. 43 411–113 (1937). *A very elegant purely group theoretical characterization of compact simple Lie groups.*

—: A theorem concerning the semi simple Lie groups, Tohoku Math J. 44 81–84 (1937).

—: On the group embedded in the metrical complete ring, Japan J. Math. 13 459–172 (1937). *Let G be a locally bicompact connected topological group and D a continuous representation of G in a complete metric ring. Then, D is a Lie representation.*

—: A problem concerning the second fundamental theorem of Lie, Proc Imp. Acad. Japan 13 152–155 (1937). *If the system $X_1, \cdots, X_n$ is irreducible, so is the group germ in the neighborhood of 1.*

—: On the fundamental theorem of the tensor calculus, Proc. Imp. Acad. Japan 14, 211–213 (1938). *If G is a connected, simply connected semisimple Lie group and D a connected group of matrices to which G is continuously homomorphic, then the homomorphism is open and D is a Lie group.*

—: A note on the differentiability of the topological group, Proc. Phys-Math. Soc. Japan III 20 6–10 (1938). *A multiplicative subgroup of a complete metric ring is a Lie group if it is complete and differentiable.*

Group Theory in Japan 1941–1952

Source: Math. Reviews

[H]

Hattori Akira: On invariant subrings, Japan J. Math. 21 121–129 (1951). *A generalization of the theorem of Cartan-Brauer-Hua.*

—: On the multiplicative group of simple algebras and orthogonal groups of three dimension, J. Math.

Soc. Japan 4 205–217 (1952). *If B is a simple subalgebra of a simple algebra A of finite rank over its center F such that $F \neq B \neq A$, and if $[B]$ denotes the set of subalgebras F-isomorphic to B, the group $I(A)$ of inner automorphisms of A acts faithfully on $[B]$, in particular $[B]$ is an infinite set. Normal subgroups of $O_3^+(Q)$ of the form of index 0 are given.*

Honda Kinya: On finite groups, whose Sylow groups are all cyclic, Proc Japan Acad. 25 154–159 (1949). *Announcement of results on the details of the structure of finite groups in the title.*

—: On finite groups, whose Sylow-groups are cyclic, Comment. Math. Univ. St. Paul 1 5–39 (1952). *Proofs of the results announced in the above paper.*

Inaba Eizi: Über modulare Verba'nde, welche die Untergruppen einer endlichen Gruppe bilden I, Proc. Imp. Acad. 19 528–532 (1943). *If a lattice L is a direct union of lattices in which every interval is a chain or contains no neutral elements (like $L(G)$ of finite abelian groups), then every element of L is a join of elements c with the interval c/0 is a chain; some other properties of such a lattice.*

Iseki Kiyoshi: On simply ordered groups, Portuugaliae Math. 10 86–88 (1951). *If every cut of a linearly ordered group is continuous, it is isomorphic to the additive group of real numbers.*

Isiwata Takesi: Non-discrete linearly ordered groups, Kodai Math. Sem. Rep. 1950 84–88. *Discussions of the relationship among properties of linearly ordered groups, locally compactness etc.*

Ito Noboru: Note on p-groups, Nagoya Math. J. 1 113–116 (1950). *There exists an infinite chain of p-groups $G_1, G_2, \cdots$ such that p odd, G_1 elementary abelian of order p^3, and $G_n \cong G_{n+1}/\theta(G_{n+1})$ where $\theta_n(X)$ is the nth derived group of X.*

—: Some studies on group characters, Nagoya Math. J. 2 17–28 (1951). *In the case when $N \triangleleft G$ and $|G : N| = p$, a prime, a construction is given to associate a block of characters of G to that of N; as applications, for a solvable group G, if $O_p(G) = 1$ for $p|g = |G|$, G has a p-block whose defect is not the maximal one; if the Sylow p-subgroups are TI, there is a p-block of defect zero; if the degrees of all irreducible characters are prime to p, then the S_p-subgroup is normal.*

—: On the degrees of irreducible representations of a finite group, Nagoya Math. J. 3 5–6 (1951). *If A is an abelian normal subgroup of G, the degree of any irreducible character divides $|G : A|$.*

—: On the characters of soluble groups, Nagoya Math. J. 3 31–48 (1951). *A sufficient condition for a solvable group to have a p-block of defect zero; similar results for a positive defect.*

—: A theorem on the alternating group $A_n (n \geq 5)$, Math. Japon. 2 59–60 (1951). *Proof that every element of $A_n (n \geq 5)$ can be expressed as a single commutator.*

—: Remarks on factorizable groups, Acta Sci. Math. (Szeged) 14 83–84 (1951). *If $G = HK$ with H nilpotent and K abelian or a p-group, then G is solvable: this marks a great step forward.*

—: Note on (LM)-groups of finite orders, Kodai Math. Sem. Rep. 1951 1–6 *The paper gives the structure of minimal p-nilpotent groups, of LM-groups, of minimal LM-groups, and others.*

—: Note on A-groups, Nagoya Math. J 4 79–81 (1952). *If all Sylow subgroups of a solvable group G are abelian, G is an M-group; the set of elements x such that $\chi(x) \neq 0$ for any irreducible character generates the maximal nilpotent normal subgroup.*

—: On a theorem of L. Rèdei and J. Szèp concerning p-groups, Acta Sci. Math. (Szeged) 14 186–187 (1952). *If H is a subgroup of a p-group G such that $D(H) \neq D(G)$, then $D(\Phi(G)H) \neq D(G)$: this was followed by works of Hobby-Wright, Hill, and Janko.*

—: Remarks on O. Grün's paper "Beiträge zur Gruppentheorie III", Math. Nachr. 6 319-325 (1952). *Many results concerning p-normality, p-regularity and p-hyperregularity: among them, the weak closure of the center of a S_p-subgroup P in P of a solvable group is abelian.*

—: On II-structures of finite groups, Tohoku Math. J. (2) 4 172–177 (1952). *Sylow type theorems for p-separable groups (under the assumption of the validity of the conjugacy statement of Schur-Zassenhaus theorem; some results on conjugate complex of Grün.*

Ito Noboru and Nagata Masayoshi: Note on groups of automorphisms, Kodai Math. Sem. Rep. 3 37–39 (1949). *If G is a complete group that is indecomposable with minimal condition for normal subgroups then $Aut(G \times G) = (G \times G) < y >$ where $y^2 = 1$ and $y(a,b)y^{-1} = (b,a)$. Furthermore, $Aut(G \times G)$ is indecomposable, and complete unless $G = S_3$.*

Ito Seizo: Unitary representations of some linear groups, Nagoya Math. J. 4 1–13 (1952). *The explicit determination of the irreducible unitary representation of the group of sense preserving rigid motions in plane.*

Iwahori Nagayoshi: Non-representability of real general linear groups in higher dimensional Lorentz groups, Sci. Papers Coll. Gen. Ed. Univ. Tokyo 2 13-23 (1952). *Which groups $GL(n,F)$ are isomorphic to subgroups of $O(m,k,F)$ fixing the form $x_1^2+\cdots+x_m^2-x_{m+1}^2-\cdots-x_{m+k}^2$? Theorem. There is no continuous monomorphism of $GL(n,\mathbb{R})$ into $O(m,1,\mathbb{R})$ if $n\geq 3$.*

Iwasawa Kenkiti: Über die Einfachheit der speziellen projektiven Gruppen, Proc. Imp. Acad. Japan 17 57–59 (1941). *Simplicity of $PSL(n,K)$ except $n=2$ and $|K|<3$ is proved elegantly.*

—: Über die endlichen Gruppen und die Verbande ihrer Untergruppen, J. Fac. Sci. Imp. Univ. Tokyo I 4 171–199 (1941). *Determination of finite groups with $L(G)$ modular and other numerous new results on the subgroup lattice of a finite group.*

—: Über die Structur der endlichen Gruppen deren echte Untergruppen sämtlich nilpotent sind, Proc. Phys-Math. Soc. Japan III 23 1–4 (1941). *Structure of such groups is completely determined.*

—: Einige Sätze über freie Gruppen, Proc. Imp. Acad. Japan 19 272–274 (1943). *A proof that any free group is residually finite p-groups for any given prime p.*

—: On the structure of infinite M-groups, Japanese J. Math. 18 709–728 (1943). *Determination of the structure of infinite groups with modular lattice of subgroups. The result is complete when there is an element of infinite order, for torsion groups, one need to assume that every section of finite length is a finite group. (This assumption is really needed due to the existence of the Tarski Monsters.)*

—: On the structure of conditionally complete lattice-groups, Japanese J. Math. 18 777–789 (1943). *A proof of Birkhoff's conjecture that a conditionally complete lattice-group is commutative.*

Kawada Yukiyosi: Über den Dualitätssatz der charaktere nichtkommutativer Gruppen, Proc. Phys-Math. Soc. Japan III 24 97–109 (1942). *An approach different from Tannaka's to the duality theorems.*

Kinosita Yosihisa: On an enumeration of certain subgroups of a p-groups J. Osaka Inst. Sci. Tech. 1 13–20 (1949). *A formula, slightly different from the known one, expressing the number of subgroups of given type of an abelian p-group in terms of the type invariants is obtained.*

Kondo Koiti—: Decomposition of the characters of some groups I, Proc. Phys-Math. Soc. Japan III 23 265–271 (1941). *Formulas for the recurrent calculation of the characters of the hyperoctahedral group.*

—: Decomposition of the characters of some groups II, Proc. Phys-Math. Soc. Japan 23 783–787 (1941). *Decomposition of an irreducible representation of $O(n)$ into irreducible representations of $O(n-1)$. A similar reduction is given for $O^+(n)$ and for $S_p(n)$.*

Kurosaki Tiyoko—: Über die mit einer Kollineation vertauschbaren Kollineationens Proc. Imp. Acad. Japan 17 24–28 (1941).

Matsushita Shin-ichi—: On the foundation of orders in groups, J. Inst. Polytech Osaka City Univ. Math. 2 19–22 (1951).

Michiura Tadashi: On a definition of lattice ordered groups, J. Osaka Inst. Sci. Tech. 1 27 (1949). *A condition should be added to those of a theorem of Birkhoff.*

—: On a definition of lattice- ordered groups II, J. Osaka Inst. Sci. Tech. 1 117–119 (1949). *Various axiom systems for l-groups in terms of $a \to a* = a \cup 0$ in addition to group axioms.*

—: Sur les groupes semi-ordonnés, C. R. Acad. Sci. Paris 231 1403–1404 (1950). *A theorem on G/M where G is a commutative non-Archimedean dean l-group and M a maximal convex subgroup.*

—: On simply ordered groups, Portugaliae Math 10 89–95 (1951). *Study on a particular class of ordered groups.*

—: Remark on a representation of simply ordered groups, Nederl. Acad. Wetensch. Proc. 54 (= Indagationes Math. 13) 386–387 (1951).

—: Sur les groupes ordonnés II, et III, C. R. Acad. Sci. Paris 234 1422–1423 1521–1522 (1952). *Study on 'strongly archimedean' partly ordered groups with additional conditions.*

Morita Kiiti: A remark on the theory of general fuchsian groups, Proc. Imp. Acad. Tokyo 17 233-237 (1941). *A generalization of Fuchscian groups to matrices of larger degrees.*

—: On group rings over a modular field which possess radicals expressible as principal ideals, Sci. Rep. Tokyo Bunrika Daigaku, A4 177–194 (1951) *A necessary and sufficient condition for a ring with minimum condition to have its radical principal as a left as well as right ideal; the group ring over an algebraically closed field of characteristic p has this condition iff $G/O_{p,p'}(G)$ is cyclic of order prime to p.*

Nagai Osamu: Note on Brauer's theorem of simple groups, Osaka Math. J. 4 113–120 (1952). *A simple* *group of order $p(p-1)(1+np)/t$ having t classes of elements of order p and $1+np$ S_p-subgroups with $n < p+2$ is either $LF(2,p)$ or $LF(2,2^m)$.*

Nagao Hirosi: Über die Beziehungen zwischen dem Erweiterungssatz von O. Schreier und dem von K. Shoda, Proc Japan Acad. 21 359-362 (1945/49). *The extension theories of Schreier and of Shoda are equivalent.*

—: A note on extensions of groups, Proc. Japan Acad. 25 11-14 (1949). *Let $N \triangleleft G$ with $A = G/N$ and $Z = Z(N)$. Then, G/Z is determined by N and A: G/Z is a subgroup of $(AutN) \times A$.*

—: On the theory of representation of finite groups, Osaka Math. J. 3 11-20 (1951). *New proofs for the orthogonality relations, for the Kronecker products and for reciprocity theorems for induced representations which apply to the modular theory as well as for the study of representations of the group by collineations as given Asano-Shoda and Asano-Osima-Takahasi.*

Nagata Masayoshi: Note on groups with involutions, Proc. Japan Acad. 28 564-566 (1952). *A group having an involutive automorphism σ fixing only the identity is abelian if one of the following conditions is satisfied: (a) every element is of finite order, (b) $< g, \sigma(g) >$ is always nilpotent, or (c) a technical condition is satisfied.*

Nagata Masayoshi, in Ito-Nagata

Nakano Hidegorô: Teilweise geordnete Algebra, Japanese J. Math. 17 425-511 (1941). *A self-contained exposition on partly ordered algebraic systems.*

Nakayama Tadasi: On some modular properties of irreducible representations of a symmetric group I and II Jap. J. Math. 17 165-184 and 411-423 (1941). *The exact power of the prime p which divides the degree of the irreducible representation corresponding to a Young diagram T is determined in terms of p-hooks in the first paper: although the explicit formula is known, great combinatorial difficulties have to be overcome in finding the exponent of p; this is applied in the second paper for the case $n/2 < p \leq n$ and the Nakayama Conjecture is stated.*

—: Note on lattice-ordered groups, Proc. Imp. Acad. Tokyo 18 1-4(1942). *Every l-group is a distributive lattice; other theorems are proved.*

—: Finite groups with faithful irreducible and directly indecomposable modular representations, Proc. Japan Acad. 23 22-25 (1947). *Natural generalizations of the Shoda-Akizuki theorem.*

—: Note on faithful modular representations of a finite group, J. Math. Soc. Japan 1 10-14 (1948). *A projective indecomposable modular representation is faithful iff it contains the modular representation obtained from a faithful irreducible nonmodular representation.*

Nakayama Tadasi and Matsushima Yozo: Über die multiplikative Gruppe einer p-adischen Divisionsalgebra, Proc. Imp. Acad. Japan 19 622-62 8(1943). *Let D^* be the multiplicative group of a division algebra D over a p-adic number field. Then, $x \in D^*$ belongs to the commutator subgroup if the reduced norm with respect to the center is one (as conjectured by Tannaka).*

Nakayama Tadasi and Osima Masaru: Note on blocks of symmetric groups, Nagoya Math. J. 2 111-117 (1951). *Alternative proof of the Nakayama conjecture.*

Ohnishi Masao: On linearization of ordered groups, Osaka Math. J. 2 161-164 (1950). *Conditions for a group to have admissible order on it.*

—: Linear order on a group, Osaka Math. J. 4 17-18 (1952). *A short proof of Lorenzen's theorem.*

Osima Masaru: Note on the Kronecker product of representations of a group, Proc. Imp. Acad. Tokyo 17 411-413 (1941). *If R is the regular representation of a finite group G and V is a representation of degree m, then $V \times R$ is equivalent to mR. If U_i are projective indecomposable, the product $V \times U_i$ splits completely into representations U_j, proving the Brauer-Nesbit conjecture.*

—: On primary decomposable group rings, Proc. Phys-Math. Soc. (3) 24 1-9 (1942). *The group ring over a field of characteristic p is a direct sum of primary algebras iff G is p-nilpotent; the representation theory of such groups is developed: in particular, irreducible representation of the p-complement induces the projective indecomposable representation of G.*

—: Some notes on the induced representations of a group, Jap. J. Math. 21 191-196 (1952). *If H is a subgroup of a finite group G, D a representation of H, and V a representation of G, then $D^* \times V \cong (D \times V|H)^*$; an extension to representation of G by semi-linear transformations is given.*

—: On induced characters of a group, Proc. Japan Acad. 28 243248 (1952). *Sketches of a proof of Brauer's theorem on induced characters.*

—: On the representations of groups of finite order, Math. J. Okayama Univ. 1 63-68 (1952). *The group algebra is considered as $G \times G$ module and the multiplicities of the irreducible constituents are shown to be Cartan invariants; generalizations and new concept of H-blocks are studied.*

—: On the irreducible representations of the symmetric group, Canadian J. Math. 4 381-384 (1952). *Let T_0 be the p-core of the diagram T. If T is self-associated, so is T_0; the number of self-associated irreducible representations of S_n belonging to the p-block $B(T_0)$ is determined.*

—: On some character relations of symmetric groups, Math. J. Okayama Univ. 1 63-68 (1952). *Description of a basis for the relations $\sum \alpha_i\chi_i(R) = 0$ for all p-regular elements R in the symmetric group S_n with complex coefficients.*

Osima Masaru, in Nakayama-Osima

[S]

Sato Shoji: On groups and the lattices of subgroups, Osaka Math. J. 1 135-149 (1949). *Determination of groups with $L(G)$ upper semimodular and having the property that every section of finite length is finite.*

—: Note on lattice-isomorphisms between Abelian groups and non-Abelian groups, Osaka Math. J. 3,215-220 (1951). *If G is an infinite nonabelian M-group having an element of infinite order, G is lattice-isomorphic to an abelian group.*

—: On the lattice homomorphisms of infinite groups I, Osaka Math. J. 4 229-234 (1952). *A necessary and sufficient condition for the canonical map $G \to G/H$ to induce a L-homomorphism.*

Seki Takejiro: Über die Existenz der Zerfällungsgruppe in der Erweiterungsthorie der Gruppen, Tohoku Math. J. 48 235-238 (1941). *Let G be a group with normal subgroup N. Generalizing Artin's theorem to nonabelian N, it is proved that there is a splitting group.*

Shoda Kenjiro: Bemerkungen Über die induzierten Charaktere endlicher Gruppen, Proc. Imp. Acad. Tokyo 18 336-338 (1942). *Let H and H' be two normal subgroups of a finite group G, χ a character of H, and χ' a character of H'. A necessary and sufficient condition for $\chi^* = \chi'^*$ is given.*

—: Über die Schreiersche Erweiterungstheorie, Proc. Imp. Acad. Tokyo 19 518-519 (1943). *Let N and B be two groups. The paper gives an extension theory (which is proved to be equivalent to Schreier's by Nagao(49)) to construct an extension A of N when B is given by a presentation.*

—: Ein Satz über die Abelschen Gruppen mit.Operatoren, Proc Japan Acad. 28 241-242 (1952). *An algebraic extension of abelian groups is defined and a criterion when an extension cannot be equivalent to a proper subgroup is given.*

Suetuna Zyoiti: Über die sich selbst assoziierten Charaktere der symmetrischen Gruppe, J. Reine Angew, Math. 183 92-97 (1941). *The number and the shape of self-associated characters are given; all for $\leq$ 25.*

—: Zur Theorie der Gruppencharaktere, Japan J. Math. 18 729-744 (1943). *A group-theoretic proof that $m = 1$ if G/N is cyclic; a study of decomposition when G/N is linear mod p^n.*

Suzuki Michio: On the finite group with a complete partition, J. Math. Soc. Japan 2 165-185 (1950). *The determination of nonsimple groups with partition into cyclic subgroups.*

—: The lattice of subgroups of finite groups, *Sugaku* 2 189-200 (1950).

—: A characterization of simple groups $LF(2,p)$, J. Fac. Sci. Univ. Tokyo 6 259-293 (1951). *A noncyclic simple group having the same type of proper subgroups as $LF(2,p)$ is $LF(2,p)$.*

—: On the lattice of subgroups of finite groups, Trans. AMS 70 345-371 (1951). *The paper gives many new theorems to the existing knowledge of the extent to which a finite group is determined by the lattice of its subgroups.*

—: The L-homomorphisms of finite groups, Trans. AMS 70 372-386 (1951). *The structure of finite admitting proper L-homomorphisms are discussed.*

Takahasi Mutuo: Bemerkungen über den Untergruppensatz in freien Produkte, Proc. Imp. Acad. Tokyo 20 589-594 (1944). *A simple proof of the subgroup theorem of free products bases on cancellation argument.*

—: On partitions of free products of groups, Osaka Math. J. 1 49-51 (1949). *A free product of two groups has a partition.*

—: Note on locally free groups, J. Inst. Polytech. Osaka City Univ. Math. 1 65-70 (1950). *The author gives two necessary and sufficient conditions for a locally free group to be free (cf. G. Higman's paper in J. London Math. Soc. 28 (1953)).*

—: Primitive locally free groups, J. Inst. Polytech. Osaka City Univ. Math. 2 1-11 (1951). *A condition is given for a locally free group to be the free product of Q^+.*

—: Note on chain conditions in free groups, Osaka Math. J. 3 221–225 (1951). *With additional restrictions the author proves various chain conditions for free groups.*

—: Note on word-subgroups in free products of groups, J. Inst. Polytech. Osaka City Univ. Math. 2 13–18 (1951). *Let $W(G)$ be the word subgroup for a fixed set of words. If G is the free product of groups A_i, then $W(G) \cap A_i = W(A_i)$. This implies, among others, that the derived group of a free product of abelian groups is a free group.*

Takahashi Shuichi: Cohomology groups of finite abelian groups, Tohoku Math. J. (2) 4 294–302 (1952). *A concise construction of cohomology groups of finite abelian groups.*

Taketa Kiyosi: Über die Existenz einer Untergruppe, deren Ordnung ein Produkt von zwei verschiedenen Primzahlpotenzen ist, Proc. Imp. Acad. Tokyo 19 609–610 (1943). *If $|G| = p^n g$ with $(p, g) = 1$, either G is p-nilpotent, or there is a subgroup of order $p^n q$ with q a prime power $\neq 1$.*

—: Über die Struktur der matabelischen Gruppen II, J. Osaka Inst. Sci. Tech. I 2 1–28 (1950).

—: Über die Struktur der metabelischen Gruppen III, Tohoku Math. J. (2) 410–32 (1952).

Tsuboi Teruo: On the abelian factor group, Sci. Rep. Saitama Univ. 1 1–8 (1952). *If N is a Hall normal subgroup of a finite group G, then G maps onto $N/(N \cap G')$.*

Toyama Hiraku: On commutators of matrices, Kodai Math. Sem. Rep. 5–6 1–2 (1949). *Every element of each of the groups $SU(n)$, $S_p(n)$, or $O^+(n)$ with $n > 2$ is a commutator.*

[Y]

Yamabe Hidehiko: A condition for an abelian group to be a free abelian group with a finite basis, Proc. Japan Acad. 27 205–207 (1951). *The author gives a condition for an abelian group to be free in terms of what Neumanns (B.H. and Hanna in Arch. Math. 4 1953) called a Yamabe function.*

Yamanouchi Takahiko: Tables useful for construction of irreducible representation matrices of symmetric group, J. Phys. Soc. Japan 3 245–253 (1948). *These tables permit rapid numerical computation of the physically significant irreducible representations of the symmetric groups on not more than 6 letters.*