第28回代数的組合せ論シンポジウム報告集

2011年6月20－22日

於　大分大学VBLセミナー室

平成23年度文部科学省科学研究費補助金基盤研究（B）

（課題番号　23340021　山形大学　原田昌晃）

まえがき

この報告集は、平成２３年６月２０日（月）から２２日（水）にわたって、大分大学 VBL (ベンチャー・ビジネス・ラボラトリー) セミナー室で行われた「第２８回代数的組合せ論シンポジウム」の講演記録です。研究集会には６１名の参加者がありました。

この報告集の作成にあたっては、
科学研究費補助金　基盤研究（Ｂ）課題番号：23340021 研究代表者 原田昌晃（山形大) から援助を受けました。また、旅費に関しては、
科学研究費補助金　若手研究（Ｂ）課題番号：20740002 研究代表者 田邊顕一朗（北海道大) および
科学研究費補助金　基盤研究（Ｃ）課題番号：21540139 研究代表者 末竹千博（大分大) から援助を受けました。有難うございました。

最後に, 講演者をはじめ、この集会の開催にご協力いただいた皆様に深く感謝いたします。

平成２３年１０月
秋山献之（福岡大学）
末竹千博（大分大学）
田中正紀（崇城大学）

第２８回代数的組合せ論シンポジウム

下記のように研究集会を開催しますので、ご案内申し上げます。

世話人　秋山献之 (福岡大)
末竹千博 (大分大)
田中正紀 (崇城大)

記

日程：　２０１１年6月２０日（月）～２２日（水）
場所：　大分大学 VBL(ベンチャー・ビジネス・ラボラトリー) セミナー室
大分市大字旦野原７００番地

プログラム

6月２０日（月）

14 : 00 ～ 14 : 50　清田正夫 (東京医科歯科大学・教養部), 奥山哲郎 (北海道教育大学旭川校), 和田倶幸 (東京農工大学・工学部)
対称群の 2-ブロックに属する既約 Brauer 指標の高さ

15 : 00 ～ 15 : 30　與口卓志 (千葉大学・理学研究科)
ランク２のシャープ指標について

15 : 40 ～ 16 : 10　飯寄信保 (山口大学・教育学部)
A theorem on monomials over groups and the classification of finite simple groups.

16 : 20 ～ 16 : 50　千吉良直紀 (熊本大学・自然科学研究科)
Rudvalis 群と符号

17 : 00 ～ 17 : 30　入江佑樹 (千葉大学・理学研究科)
グラフの変異 (mutation) が生成する群について

6月２１日（火）

10 : 00 ～ 10 : 50　吉田知行 (北海道大学・理学研究院)
有限群上のランダムウォークと離散統計学への応用

11 : 00 ～ 11 : 30　淺井恒信 (近畿大学・理工学部), 庭崎隆 (愛媛大学)
有限群の斜準同型に関する予想の拡張について

11 : 40 ～ 12 : 10　佐藤巌 (小山高専)
グラフの正則被覆の重み付き散乱行列

12 : 20 ～ 12 : 50　野崎寛 (東北大学・情報科学研究科), 篠原雅史 (鈴鹿高専)
グラフのユークリッド空間への埋め込みと強正則グラフの特徴付け

14 : 30 ～ 15 : 20　Richard M. Wilson (California Institute of Technology)
Diagonal forms for incidence matrices associated with t-uniform hypergraphs

15 : 40 ～ 16 : 10　神保雅一 (名古屋大学・情報科学研究科), 城本啓介 (熊本大学・自然科学研究科)
Mutally orthogonal partial t-designs over $\mathbb{C}$ related to quantum jump codes

16 : 20 ～ 16 : 50　角俊雄 (九州大学・芸術工学研究院), 坂田年男 (九州大学・芸術工学研究院), 宮崎充弘 (京都教育大学・教育学部)
Existence and construction of absolutely nonsingular tensors

17 : 00 ～ 17 : 30　中川暢夫 (近畿大学・理工学部)
On planar functions and bent functions

懇親会

6月22日（水）

10 : 00 ～ 10 : 50　平岡裕章 (九州大学・マス・フォア・インダストリ研究所)
近似最尤推定復号に現れる組合せ論的側面

11 : 00 ～ 11 : 30　島倉裕樹 (愛知教育大学)
Kleinian codes and vertex operator algebras associated with even lattices

13 : 10 ～ 13 : 40　須田庄 (東北大学・情報科学研究科)
半正定値計画法に基づく多重交差集合について

13 : 50 ～ 14 : 20　平峰豊 (熊本大学・教育学部)
cosets に関する difference matrices について
(末竹氏との共同研究)

14 : 30 ～ 15 : 00　谷口浩朗 (香川高専)
On a description of the Buratti-Del Fra dual hyperoval and its quotient

(*)　初日 20 日の集会開始前に大分大学工学部長の挨拶をお願いしています。当日は 13 時 45 分までに会場まで来ていただけると幸いです。

The 28th Symposium on Algebraic Combinatorics

Dares: June20(Mon)–June 22(Wed), 2011
Place: Oita University, Dannoharu Campus
Organizer:K. Akiyama(Fukuoka Univ., email:akiyama@fukuoka-u.ac.jp)
C. Suetake(Oita Univ., email:suetake@csis.oita-u.ac.jp)
M. Tanaka(Sojo Univ., email:mtanaka@ed.sojo-u.ac.jp)

June 20, Monday

14 : 00 – 14 : 50 M.Kiyota(Tokyo Medical and Dental Univ.), T. Okuyama (Hokkaido Univ. of Education Asahikawa Campus), T. Wda(Tokyo Univ. of Agriculture and Technology)
The heights of irreducible Brauer characters in 2-blocks of the symmetric groups

15 : 00 – 15 : 30 T. Yoguchi(Chiba Univ.)
On sharp characters of rank 2

15 : 40 – 16 : 10 N. Iiyori(Yamaguchi Univ.)
A theorem on monomials over groups and the classification of finite simple groups.

16 : 20 – 16 : 50 N. Chigira(Kumamoto Univ.)
Rudvalis group and codes

17 : 00 – 17 : 30 Y. Irie(Chiba Vniv.)
On groups generated by mutations of graphs

June 21, Tuesday

10 : 00 – 10 : 50 T. Yoshida(Prof. Emeritus at Hokkaido Univ.)
Random walks on finite groups and applications to discrete statistics

11 : 00 – 11 : 30 T. Asai(Kinki Univ.), T. Niwasaki(Ehime Univ.)
An extension of a conjecture on crossed homomorphisms of finite groups

11 : 40 – 12 : 10 I. Sato(Oyama National College of Technology)
Weighted scattering matrix of a regular covering of a graph

12 : 20 – 12 : 50 H. Nozaki(Tohoku Univ.), M. Shinohara
(Suzuka National College of Technology)
A characterization of strongly regular graphs from Euclidean representations of graphs

14 : 30 – 15 : 20 Richard M. Wilson(California Institute of Technology)
Diagonal forms for incidence matrices associated with t-uniform hypergraphs

15 : 40 – 16 : 10 M. Jimbo(Nagoya Univ.), K. Shiromoto(Kumamoto Univ.)
Mutally orthogonal partial t-designs over $\mathbb{C}$ related to quantum jumpcodes

16 : 20 – 16 : 50 T. Sumi(Kyushu Univ.), T. Sakata (Kyushu Univ.),
M. Miyazaki(Kyoto Univ. of Education)
Existence and construction of absolutely nonsingular tensors

17 : 00 – 17 : 30 N. Nakagawa(Kinki Univ.)
On planar functions and bent functions

Conference dinner at Oita Univ.(18:00-20:00)

June 22, Wednesday

10 : 00 – 10 : 50 Y. Hiraoka(Kyushu Univ.)
Approximate maximum likelihood decoding and its combinatorial structure

11 : 00 – 11 : 30 H. Shimakura(Aichi Univ. of Education)
Kleinian codes and vertex operator algebras associated with even lattices

13 : 10 – 13 : 40 S. Suda(Tohoku Univ.)
A cross intersection families based on semidefinite programing lattices

13 : 50 – 14 : 20 Y. Hiramine(Kumamoto Univ.)
On difference matrices with respect to cosets
(joint work with C. Suetake)

14 : 30 – 15 : 00 H. Taniguchi(Kagawa National College of Technology)
On a description of the Buratti-Del Fra dual hyperoval and its quotient

目次

1. 清田正夫（東京医科歯科大学), 奥山哲郎（北海道教育大学), 和田倶幸（東京農工大学） ···1
対称群の 2-ブロックに属する既約 Brauer 指標の高さ

2. 與口卓志（千葉大学） ···10
ランク２のシャープ指標について

3. 飯寄信保（山口大学） ···20
A theorem on monomials over groups and the classification of finite simple groups

4. 千吉良直紀（熊本大学） ···24
Rudvalis 群と符号

5. 入江佑樹（千葉大学） ···28
グラフの変異 (mutation) が生成する群について

6. 吉田知行（北海道大学） ···34
有限群上のランダムウォークと離散統計学への応用

7. 淺井恒信（近畿大学), 庭崎隆（愛媛大学） ···46
有限群の斜準同型に関する予想の拡張について

8. 佐藤巌（小山高専） ···50
グラフの正則被覆の重み付き散乱行列

9. 野崎寛（東北大学), 篠原雅史（鈴鹿高専） ···59
グラフのユークリッド空間への埋め込みと強正則グラフの特徴付け

10. Richard M. Wilson (California Institute of Technology) ···65
Diagonal forms for incidence matrices associated with t-uniform hypergraphs

11. 神保雅一（名古屋大学), 城本啓介（熊本大学） ···76
Mutally orthogonal partial t-designs over $\mathbb{C}$ related to quantum jump codes

12. 角俊雄（九州大学), 坂田年男（九州大学), 宮崎充弘（京都教育大学） ···82
Existence and construction of absolutely nonsingular tensors

13. 中川暢夫（近畿大学） ···89
On planar functions and bent functions

14. 平岡裕章（九州大学） ···98
近似最尤推定復号に現れる組合せ論的側面

15. 島倉裕樹（愛知教育大学） …104
Kleinian codes and vertex operator algebras associated with even lattices

16. 須田庄（東北大学） …110
半正定値計画法に基づく多重交差集合について

17. 平峰豊（熊本大学） …118
cosets に関する difference matrices について（末竹氏との共同研究）

18. 谷口浩朗（香川高専） …128
On a description of the Buratti-Del Fra dual hyperoval and its quotient

The heights of irreducible Brauer characters in 2-blocks of the symmetric groups

清田正夫（東京医科歯科大学　教養部）
奥山哲郎（北海道教育大学　旭川校）
和田倶幸（東京農工大学 工学研究院）

1　はじめに

G を有限群，F を標数 $p>0$ の代数的閉体とし, B を FG のブロックでその defect group を D とする．整数 n の p-part を n_p と書く．$|G|_p = p^a$ とし $|D| = p^d$ とおく．φ を B に含まれる任意の既約 Brauer 指標とする．その次数 $\varphi(1)$ は p^{a-d} で割れる．したがって $\varphi(1)_p = p^{a-d+e}$, $\exists e \geq 0$ と書け，e を φ の**高さ (height)** といい，$h(\varphi) = e$ と書く．どのブロックにも高さ 0 の既約 Brauer 指標は存在する (Theorem IV.4.5 [4]).

B に属する既約通常指標 χ にも同じことが成り立ち，$\chi(1)_p = p^{a-d+f}$, $\exists f \geq 0$ と書け，$f = h(\chi)$ をやはり高さという．$\chi(1) \mid |G|$ であることから，$0 \leq h(\chi) \leq d$ となり，有名な Brauer の height zero 予想や Alperin-McKay 予想はこの通常指標の高さに関する予想である．しかし既約 Brauer 指標 φ については，$\varphi(1)$ は必ずしも $|G|$ を割らないため，$h(\varphi) \not\leq d$ である．実際，Thackray によると，$G = \mathrm{McL}, p = 2$ のとき主 2-ブロック B には $\varphi(1)_2 = 2^9$ をみたす既約 Brauer 指標があり，$|G|_2 = 2^7$ より，$a = d = 7$ であるが，$h(\varphi) = 9 > 7 = d$ となる (p.166 [4]).

一般にブロックに含まれる既約 Brauer 指標で高さ 0 のものは，どれくらいあるだろうか？ $\mathrm{SL}(2, 2^n)$ の 2-ブロックのように，ただ一つのこともあり，$\mathrm{SL}(2, p)$, p : odd のとき full defect の p-ブロックのように，$(p-1)/2$ 個すべてが高さ 0 のこともある．対称群の 2-ブロックについて，次の定理を得た．

定理 1 (Kiyota-Okuyama-W [11]). $G = \mathfrak{S}_n$ を n 次対称群とし，$p = 2$ とする．すると各 2-ブロック B に含まれる既約 Brauer 指標で高さが 0 のものは，ただ一つである．

定理 1 を考えるに至った動機については最後の節で述べる．既約通常指標の次数に関しては hook formula という公式があり，既約通常指標を与える Young diagram から次数が計算できる．既約 Brauer 指標の次数を求める公式はまだ知られていない．対

称群のモジュラー表現については，分解行列を決定せよという未解決問題がある．既約 Brauer 指標の次数が分かっていないことが，分解行列を求めることを困難にしている．定理 1 の証明の難しさもここにある．$n \leq 17$ の場合には既約 Brauer 指標の次数が知られているが，定理 1 の主張が成り立つかどうかを，すべてのブロックについてチェックするだけでも大変である．定理 1 が今までに知られていなかったのも無理はないと思われた．

定理 1 は次の Fong, James の定理を一般化した定理である (James の論文について越谷さんから教えて頂いたことに感謝致します)．

定理 2 (Fong [5], James [7]). G を有限群とし，F を完全体で $\mathrm{char}(F) = 2$ とする．V を絶対既約な非自明な FG-加群とする．もし V が self-dual ならば，$\dim_F(V)$ は偶数である．

対称群の既約 FG-加群は素体上で絶対既約で，しかも self-dual であることから，この定理の直接の系として，次の定理が成り立つ．

定理 3 (Fong [5], James [7]). $\mathfrak{S}_n$ を n 次対称群とし，F は標数 2 の体とする．V を非自明な既約 FG-加群とすると $\dim(V)$ は偶数である．

注 1.1 定理 1 は定理 3 がブロックごとに成り立つことを示している．定理 1 は p が奇素数のときは必ずしも成り立たない．次のような例がある．以下 $\mathrm{IBr}(B)$ で B に属する既約 Brauer 指標全体の集合とし，B_0 を主ブロックとする．また既約 Brauer 指標を数字で表してあるが，それは次数を表し，同じ次数の指標が二つ以上ある時は，さらにインデックスを付けている．

(1) $p = 3$ のとき

(1.1) $n = 3, 4$ のとき $\mathrm{IBr}(B_0) = \{1_1, 1_2 = \mathrm{sign}\}$ すべて高さ 0

(1.2) $n = 5$ のとき $\mathrm{IBr}(B_0) = \{1_1, 4_1\}$ すべて高さ 0

(1.3) $n = 6$ のとき $\mathrm{IBr}(B_0) = \{1_1, 1_2, 4_1, 4_2, 6\}$ 高さ 0 は 4 個，高さ 1 が 1 個

(1.4) $n = 7$ のとき $\mathrm{IBr}(B_0) = \{1_1, 1_2, 13_1, 13_2, 20\}$ すべて高さ 0，$13 \nmid |G|$

(2) $p = 5$ のとき

(2.1) $n = 5$ のとき $\mathrm{IBr}(B_0) = \{1_1, 1_2, 3_1, 3_2\}$ すべて高さ 0

(2.2) $n = 6$ のとき $\mathrm{IBr}(B_0) = \{1_1, 1_2, 8_1, 8_2\}$ すべて高さ 0

注 1.2 定理 1 の主張は既約通常指標については成り立たない．$p = 2$ のとき，単位指標と符号指標は mod 2 reduction で共に単位指標となるので，主ブロックに属し共に高さ 0 である．よって高さ 0 の既約通常指標は主ブロックの中に 2 個以上はある．

対称群のモジュラー表現に関して，最近いくつかの重要な結果，特にカテゴリカルな結果がある．Scopes は [14] で，対称群のブロックについては Donovan 予想が成り立つことを証明した．Chuang-Rouquier は [1] で，対称群 $\mathfrak{S}_n$ のブロック B と，B の weight を w とするとき，$\mathfrak{S}_{pw}$ の主 p-ブロック $\tilde{B}$ は derived equivalent になることを証明した．しかしこれらの結果から直ちに定理 1 が導けるようには思われない．モジュラー表現の次数や次数の p-part は derived equivalence で変わってしまうためである．

そこで我々が定理の証明に対して取った方法は，Green 対応と symplectic bilinear form の構成，そして James の定理を利用した n に関する帰納法という古典的な方法である．

2 Preliminaries

対称群のモジュラー表現に関する基本的な言葉や結果を導入し，定理 1 を適切な表現に改める．James の [8] や James-Kerber の [10] を参照してください．F を標数 2 の体とし，$\Omega = \{1, 2, \ldots, n\}$ とする．(ここで述べる結果は F の標数が 2 である必要がないことが多いが，我々の結果が標数 2 の場合なので，標数 2 としておきます．)

$\mu = (\mu_1, \mu_2, \ldots)$ が n の partition であるとは，$\mu_1, \mu_2, \ldots$ は 0 以上の整数で，$\mu_1 \geq \mu_2 \geq \cdots, \mu_1 + \mu_2 + \cdots = n$ を満たすことをいう．このとき第一行目が μ_1 個の箱，第二行目が μ_2 個の箱，... のように，左側をそろえて，箱の作る行列を $[\mu]$ とかき，μ に関する Young diagram という．

M^μ を $\mathfrak{S}_n$-set $[\mathfrak{S}_\mu \backslash \mathfrak{S}_n]$ による F 上の置換加群とする．ここで，$\mathfrak{S}_\mu \simeq \mathfrak{S}_{\mu_1} \times \mathfrak{S}_{\mu_2} \times \cdots$ を μ に関する Young subgroup という．M^μ は μ-tabloids とよばれる Young diagram の各箱に $1, 2, \ldots, n$ の文字を任意に入れた μ-tableau t を，row stabilizer で動かした同値類を basis とする．

M^μ の submodule で，μ-polytabloids とよばれる，μ-tabloids に符号を付けて加えたものを basis とするものを Specht module といい，S^μ と書く．もし F の標数が 0 のときは，S^μ がすべての既約 $F\mathfrak{S}_n$ 加群となる．

n の partition $\mu = (\mu_1, \mu_2, \ldots)$ が 2-regular とは，$\mu_1 > \mu_2 > \cdots$ を満たすときに言う．μ が 2-regular のとき，またそのときにかぎり，Specht module S^μ は unique な既約 quotient module D^μ をもつ．D^μ がすべての既約 $F\mathfrak{S}_n$-加群となる．Young diagram $[\mu]$ は 2-weight w と 2-core δ_k をもつ．Young diagram $[\mu]$ の右側にある階段状の箱達から，2-rim hook とよばれる縦または横に二個並んだ箱を取り除いたとき，$[\mu]$ の残部がふたたび Young diagram となるように，できるかぎり 2-rim hook を取り除いていく．もうこれ以上取り除けないとき，取り除いた 2-rim hooks の個数が $[\mu]$ の weight w である．さらにそのときに残った残部が 2-core δ_k である．2-rim hooks の取り除き方は一意的でないが，w と δ_k は一意的に定まる．(2-core は $[\delta_k]$ と書くべきかもしれません．weight と core は本来 Young diagram $[\mu]$ に対して定まるものですが，partition

μ に対しても同様に μ の weight w, 2-core δ_k と言うことにします．hook, weight, core という言葉は中山正が導入した言葉のようです．[15])

Nakayama Conjecture (Conjecture と呼ばれているが，最初 G. de B.Robinson, Brauer により証明され，その後も多数の人により証明されている.) S^λ と S^μ が $\mathfrak{S}_n$ の中で同じ 2-ブロックに属する $\Longleftrightarrow$Young diagram $[\lambda]$ と $[\mu]$ が同じ 2-cores と同じ 2-weights をもつ.

例 2.1 $\mathfrak{S}_5$ には 7 個の partition がある．2-regular なものには $\circ$ をつけた．取り除く 2-rim hook については最初のものを $*$ で，次に取り除くものを $\diamond$ でその位置を表すことにする．残った部分を $\bullet$ で表す．これが 2-core となる.

すると二つの 2-ブロック B_1, B_2 があり，$k(B)$ を既約通常指標の個数，$l(B)$ を既約 Brauer 指標の個数，$w(B)$ を weight，$d(B)$ を defect (i.e. defect group の位数の指数部分, 第 1 節では d と書いた) とすると，右の表のようになっている.

$2-regular$	$[\mu]$	w	$core$
$\circ$ $[5]$	$\bullet\ \diamond\ \diamond\ *\ *$	2	$[1]$
$\circ$ $[4,1]$	$\bullet\ \bullet\ *\ *$ $\bullet$	1	$[2,1]$
$\circ$ $[3,2]$	$\bullet\ \diamond\ \diamond$ $*\ *$	2	$[1]$
$[3,1^2]$	$\bullet\ \diamond\ \diamond$ $*$ $*$	2	$[1]$
$[2^2,1]$	$\bullet\ *$ $\diamond\ *$ $\diamond$	2	$[1]$
$[2,1^3]$	$\bullet\ \bullet$ $\bullet$ $*$ $*$	1	$[2,1]$
$[1^5]$	$\bullet$ $\diamond$ $\diamond$ $*$ $*$	2	$[1]$

	B_1	B_2
$k(B)$	5	2
$l(B)$	2	1
$w(B)$	2	1
$d(B)$	3	1

以下はいずれもよく知られている．箇条書きにしていく.

1. 2-core は 0 以上の整数 k があって $\delta_k = (k, k-1, k-2, \ldots, 2, 1)$ という形をしている．ただし $k = 0$ のときは $\delta_0 = [0]$ とする．すると箱の個数は，$k > 0$ のときは $|\delta_k| := m = k(k+1)/2$ より三角数である．

2. $D(B)$ を B の defect group (定義は避けるが B に付随して定まる G の 2-部分群) とすると，$D(B) \simeq D \in \mathrm{Syl}_2(\mathfrak{S}_{2w})$ となり，Chuang-Rouquier [1] により，B は $\mathfrak{S}_{2w}$ の主 2-ブロックに derived equivalent である．

3. $\mathcal{P}(n)$ を n の partition 全体の集合とする．$\mu_0 := (k+2w, k-1, \ldots, 2, 1)$ という n の patition がある．これは 2-regular で 2-core が δ_k となるような partition である．

4. $\mathcal{P}(n)$ には次のような自然な全順序がある．$\lambda, \mu \in \mathcal{P}(n)$ に対し $\lambda < \mu \overset{def}{\Longleftrightarrow} \lambda_1 = \mu_1, \ldots, \lambda_{i-1} = \mu_{i-1}, \lambda_i < \mu_i, \ldots$ とする．すると μ_0 は δ_k を 2-core にもつ 2-regular な partition の中で最大のものである．

5. μ_0 に関して，$M^{\mu_0} = S^{\mu_0} \oplus M'$ と分解し，ここで $M' \notin B$ である．このとき $S^{\mu_0} = D^{\mu_0}$ を満たしている．さらに次が分かる．

Lemma D^{μ_0} は高さ 0 の既約 $F\mathfrak{S}_n$-加群で，その vertex は $D(B)$ で source は trivial module $F_{D(B)}$ である．

ここで定理 1 を改めて詳細に述べる．

定理 1 (Kiyota-Okuyama-W). $\mathfrak{S}_n$ を n 次対称群とし，$p = 2$ とする．B を $\mathfrak{S}_n$ の任意の 2-ブロックで 2-core を δ_k とする．すると D^{μ_0} は B に属する高さ 0 の unique な既約 $F\mathfrak{S}_n$-加群である．

注 2.1 定理 1 は Fong, James の定理 3 から，b が主 2-ブロックの時は正しい．また Fong, James の定理 3 は，full defect の 2 ブロックは主ブロックしかないことも言っている．

3 定理 1 と同値な二つの定理

ここでは定理 1 と同値な二つの定理について述べる．後に定理 1 を証明するとき，二つの場合に分ける．それぞれの場合について，同値な定理を証明する．

定理 3.1 $\mu \in \mathcal{P}(n)$ を 2-regular とし，その 2-core を δ_k とする．このとき，S^μ (通常既約指標) の $p=2$ に関する高さが正である $\Longleftrightarrow$ 分解定数 $d_{\mu\mu_0}$ が偶数になる．

もう一つの定理を述べるには，もう少し言葉や結果が必要である．やはり $\mu \in \mathcal{P}(n)$ は 2-regular で，その 2-core を δ_k とする．

$\Omega = \{1, 2, \ldots, n\}$ とし，$G = \mathfrak{S}_n = \mathfrak{S}_\Omega$ とする．$\Omega_{2w} = \{1, 2, \ldots, 2w\}$ とし，$G_{2w} = \mathfrak{S}_{\Omega_{2w}}$ とする．さらに $\Omega'_m = \{2w+1, \ldots, 2w+m\}$ とし，$K = \mathfrak{S}_{\Omega'_m}$ とする．ただし $m = |\delta_k| = k(k+1)/2$ である．すると $\Omega = \Omega_{2w} \sqcup \Omega'_m$ である．

D^μ を B に属する既約 $F\mathfrak{S}_n$-加群でその 2-core を δ_k とする．Q を D^μ の vertex とする．すると $N_G(Q) \subseteq G_{2w} \times K$ となる．したがって $(G, Q, G_{2w} \times K)$ に関する D^μ の Green 対応子 $f(D^\mu)$ を考えることができる．$f(D^\mu)$ は直既約 $F(G_{2w} \times K)$-加群である．

$f(D^\mu)$ は，T^μ という直既約 FG_{2w}-加群があって，$T^\mu \otimes_F S$ に同型になる．ここで，S は D^{δ_k} に同型な K の defect 0 の 2-ブロックに属する既約 FK-加群である．するともう一つの同値な定理は次のようになる．

定理 3.2 B に属する既約 FG-加群 D^μ は，$\mu \neq \mu_0$ ならば，対応する T^μ は偶数次元となる．

定理 3.1 と定理 3.2 は共に定理 1 と同値になる．ここでは証明は省略する．

4 定理 1 の証明の概略

$G = \mathfrak{S}_n$ の任意の 2-ブロック B に属する高さ 0 の既約 FG-加群を D^μ とする．ただしその 2-core を δ_k とする．次の二つの場合に分けて，$\mu = \mu_0$ であることを言う．以下 FG-加群は右加群とする．

Case 1. μ が少なくとも $k+1$ 個の nonzero part をもつとき

このときは $S^\mu e_1$ という F-space に symplectic bilinear form を構成する．ここで，e_1 は FK の primitive idempotent で Young symmetrizer と呼ばれる．それは standard δ_k-tableaux 全体の中で自然な全順序に関して最大の standard tableau t_1 に対応するものである．すると $D^\mu e_1 \simeq S^\mu e_1 / (S^\mu \cup S^{\mu\perp}) e_1$ 上に nonsingular な symplectic bilinear form が定義され，$D^\mu e_1$ が偶数次元となって定理 3.2 の証明が得られる．(この辺の言葉や結果は，H.Weyl の [16] にあり，岩堀先生の著書 [6] に詳しく書かれています．岩

堀先生のご冥福を祈ります．)

Case 2. μ がちょうど k 個の nonzero parts をもつとき
次の James の定理を用いて n に関する induction で定理 3.1 を証明する．

Theorem (James [9]). $\mu = (\mu_1, \ldots, \mu_k), \nu = (\nu_1, \ldots, \nu_k)$ を n の partition で，$\mu_k \neq 0, \nu_k \neq 0$ とする．μ は 2-regular とする．すると $\overline{\mu} = (\mu_1 - 1, \ldots, \mu_k - 1), \overline{\nu} = (\nu_1 - 1, \ldots, \nu_k - 1)$ は $n-k$ の partition となり，$\overline{\mu}$ は 2-regular となる．このとき $d_{\nu\mu} = d_{\overline{\nu}\,\overline{\mu}}$ が成り立つ．

5 関連する結果

定理 1 に関連する結果と，定理 1 が成り立つのではないかと考えるに至った動機について述べる．

1 Question (Danz, Külshammer, Zimmermann [2],[3]). F を標数 2 の体で λ を n の 2-regular partition とする．D^λ を既約 $F\mathfrak{S}_n$-加群とする．D^λ の source V は，もし non-trivial ならば，偶数次元か？

定理 1 より，もし $\lambda = \mu_0$ のときは，D^λ は trivial source をもつ．もし $\lambda \neq \mu_0$ ならば，D^λ は正の高さをもつ．有限群 G の既約 FG-加群 S について，S が p-ブロック B に属するとする．B の defect group を D とする．次の村井の定理 [12] が知られている．S が正の高さをもつための必要十分条件は，S の vertex P が，$P < D$ であるか，そうでなければ source V は偶数次元である．$P < D$ のときは，V が trivial かまたは偶数次元かどうかは分からず，彼らの question が正しいかどうかは現時点では分からない．V は直既約 FP-加群なので，一般には V は 1 より大きな奇数次元になり得る．

2 次の proposition がある．
Proposition (Okuyama-W [13]). G を有限群，B を G の p-ブロックとし，C_B を B のカルタン行列とする．B の defect を d とする．このとき

$$\sum_{\varphi \in \mathrm{IBr}(B)} \left(\frac{\varphi(1)}{p^{a-d}}\right)^2 \not\equiv 0 \pmod{p} \Longrightarrow \mathrm{Tr}(p^d C_B^{-1}) \not\equiv 0 \pmod{(\pi)}$$

が成り立つ．特に C_B のある固有値 ρ で，$p^d/\rho \not\equiv 0 \pmod{(\pi)}$ を満たすものがある．

Proposition の主張で，条件 $\displaystyle\sum_{\varphi \in \mathrm{IBr}(B)} \left(\frac{\varphi(1)}{p^{a-d}}\right)^2 \not\equiv 0 \pmod{p}$ を $(*)$ とおく．G が p-可解群ならば，その任意の p-ブロックは $(*)$ を満たす．しかし $(*)$ は一般には成り立

たない．例えば $G = \mathrm{SL}(2,p), p > 3$ のとき，B を full defect の p-ブロックとすると，D は位数 p の巡回群だが，$(*)$ は成り立たない．さらにカルタン行列のすべての固有値 ρ について $p/\rho \equiv 0 \pmod{(\pi)}$ が成り立つ．同じ結果が $G = \mathfrak{S}_p, p > 3$ で B が主 p-ブロックのときに成り立つ．

$p = 2$ でこのような例があるだろうか？ 特に対称群ではどうなのだろうか？という疑問がこの問題を考えるきっかけとなった．定理 1 を得た結果，次が成り立つ．

Corollary. 対称群 $\mathfrak{S}_n$ に対し任意の 2-ブロック B は，$(*)$ が成り立つ．

参考文献

[1] J. Chuang and R. Rouquier, Derived equivalences for symmetric groups and sl_2-categorification, Ann. Math., (2) 167(2008), 245–298.

[2] S. Danz and B. Külshammer, Vertices of simple modules for symmetric groups: A Survey, Proceedings of the International Conference on Modules and Representation Theory, "Babes-Bolyai" Presa University Clujeană, Cluj-Napoca,(2009), 61–77.

[3] S. Danz, B. Külshammer and R. Zimmermann, On vertices of simple modules for symmetric groups of small degrees, J. Algebra 320(2008), 680–707.

[4] W. Feit, The representation Theory of Finite Groups, North-Holland, Amsterdam, New York, Oxford, 1982.

[5] P. Fong, On decomposition numbers of J_1 and $R(q)$, Sympos. Math. Vol. XIII(1974), 414–422, Acad. Press.

[6] 岩堀　長慶, 対称群と一般線型群の表現論, 岩波書店, 1978.

[7] G.D. James, Representations of the Symmetric Groups over the Field of Order 2, J. Algebra 38(1976), 280–308.

[8] G.D. James, The Representation Theory of the Symmetric Groups, Lecture Notes in Mathematics, 682, Springer-Verlag, 1978.

[9] G.D. James, On the decomposition matrices of the symmetric groups, III, J. Algebra 71(1981) 115–122.

[10] G.D. James and A. Kerber, The representation theory of the symmetric groups, Encyclopedia of Mathematics and Its Applications, 16, Addison-Wesley, 1981.

[11] M. Kiyota, T. Okuyama and T. Wada, The heights of irreducible Brauer characters in 2-blocks of the symmetric groups, preprint, 2011.

[12] M. Murai, Block induction, normal subgroups and characters of height zero, Osaka J.Math., 31(1994), 9–25.

[13] T. Okuyama and T. Wada, Eigenvalues of Cartan matrices of blocks in finite groups, Contemporary Mathematics, 524(2010), 127–138, Amer. Math. Soc., Proceedings of Conference on Character Theory of Finite Groups – In Honor of Martin Isaacs – held at University of Valencia, June 3-5, 2009.

[14] J. Scopes, Cartan matrices and Morita equivalence for blocks of the symmetric gorups, J. Algebra 142(1991), 441-455.

[15] B. Srinivasan, Modular representations of finite groups of Lie type in a non-defining characteristic, Groups-Canberra 1989, Springer Lect. Notes 1456(1990), 96–105.

[16] H. Weyl, The Classical Groups; Their Invariants and Representations, Princeton University Press, 1946.

ランク 2 のシャープ指標について

千葉大学大学院理学研究科　與口卓志 (Takashi Yoguchi)
Graduate School of Science,
Chiba University

1. 導入

本稿では G を有限群とし, その中心を $Z = Z(G)$ で表す. 有限群の sharp 指標とは, Cameron-清田 [2] によって置換群論における sharp permutation group の一般化として導入された概念であり, 以下のように定義される: G の通常表現の指標 χ に対し,

$$L = L(\chi) := \{\chi(g) \mid 1 \neq g \in G\} \tag{1.1}$$

を χ の型 (type) という. このとき,

$$sh(\chi) := \prod_{\ell \in L} (\chi(1) - \ell) \tag{1.2}$$

という積を考えると, $sh(\chi)$ は必ず非負の有理整数値になり, かつ $|G|$ の倍数になることが知られている. 特に $sh(\chi) = |G|$ が成り立つとき, (G, χ) は type L の sharp pair であると呼ばれる.

Remark 1. 1_G を G の単位指標とするとき, $sh(\chi + 1_G) = sh(\chi)$ が成り立つ. 従って, sharp 指標を考える際は常に $(\chi, 1_G)_G = 0$ と仮定してよい. 本稿でも断らない限り $(\chi, 1_G)_G = 0$ のもののみを扱う.

Remark 2. $L \not\subset \mathbb{Z}$ であるような sharp pair はすべて分類されている (cf. [1]). このときの G は二面体群 D_{2m} や $\mathrm{SL}(2,5)$ など非常によく知られた群に限られ, また χ は高々 2 個の既約指標の和である.

上の Remark より, sharp 指標の研究においては $L \subset \mathbb{Z}$ のときが重要になる. 計算機等を用いて少し探してみれば, sharp 指標の例はあちこちに見つかる. 反面, これらの指標が

ごくありふれたものなのか, あるいは sharp 指標を持つ有限群が特別な種類のものに限られるのか……などの疑問にははっきりとした答えが得られていない.

χ が有理整数値の sharp 指標であるとき, $|L|$ を χ の rank と呼ぶ. 2009 年の信州大学における講演 [6] において, 筆者は

$$L = \{-1, p-1\} \text{ or } \{1-p, 1\} \quad (p: \text{奇素数}), \text{ かつ } \ Z(G) > 1 \tag{1.3}$$

という条件の下で sharp pair の分類を行い, その成果としてそれまで知られていなかった sharp pair の例を一般の p に対して発見した. このとき $Z = Z(G)$ は位数 p の巡回群になり, G は以下のいずれかの群と同型になる:

(i) $Z \times \mathrm{D}_{2p}$;

(ii) $Z \times \mathrm{PSL}(2, q)$ with $q = p \pm 1$ or $2p \pm 1$;

(iii) $Z \times \mathrm{Sz}(p+1)$;

(iv) $Z \times \mathrm{PSL}(3, 4)$;

(v) M_{10} または M_{22} の triple cover;

(vi) $\mathrm{ES}(p^3, p^2)$ の自己同型群;

(vii) 位数 108 の可解群で, G/Z が Frobenius 群であるもの

(ここで, $\mathrm{Sz}(q)$ は q 元体上の Suzuki 群を, $\mathrm{ES}(p^3, p^2)$ は位数 p^3, exponent p^2 の非可換群を, M_{10} および M_{22} はそれぞれ 10 次および 22 次の Mathieu 群を表す). 上に登場する群の大部分は Z と非可換単純群 S との直積であり, S は比較的小さな π_1-part を持つものに限られる (cf. [6, 命題 8]). こうした例は他にも構成できるのであろうか? たとえば, 条件をもう少し弱めて分類問題を考えたとき, やはり同種の新しい群が見つかるのか否かは興味を惹かれることである.

本稿の目的は, 型に関する条件を少し一般化して $L = \{\ell, \ell + p\}$ かつ $Z(G) > 1$ という条件の下で sharp pair を分類することである. その結果として, 当初の動機からすればやや残念なことでもあるが, 次の定理を得た:

定理 1. (G, χ) を type $\{\ell, \ell + p\}$ (p : 奇素数) の sharp pair とし, かつ $Z = Z(G) > 1$ とする. このとき $|Z| = p$ であり, さらに次のいずれかが成り立つ:

(1) $\ell = -1$ or $1 - p$;

(2) $\ell = -2$, G は $\mathrm{ES}(p^3, p^2)$ の自己同型群と同型.

つまり, $L = \{\ell, \ell + p\}$ と仮定した場合も最終的に得られる有限群はすべて既知のものに限られることが分かった. そのため新しい sharp pair の例が得られたわけではないが, これも 1 つの成果と考え, 定理 1 の証明およびその中で得た新しいアイディアなどを報告する.

2. 有理整数値の指標に関する補題

主定理の証明を開始する前に, 本節では rank 2 の有理整数値の指標を調べる上で有益な命題を 2 つ準備する. 以降, $n \in \mathbb{Z}$ に対し n の素因数全体のなす集合を $\pi(n)$ で表し, また, いくつかの素数からなる集合 π に対し π に含まれない素数全体のなす集合を π' で表す.

2.1 中心の素数位数の元

一般に, χ が G の有理整数値の指標で, かつ G が自明でない中心を持つとき, 次のような χ の分解を構成することができる.

命題 1. χ を有限群 G の有理整数値の指標, z_0 を $Z(G)$ に含まれる素数位数の元とする. $o(z_0) = p$, $Z_0 = \langle z_0 \rangle$ とおく. さらに, Z_0 の 1_{Z_0} と異なる既約指標 λ_0 を 1 つ選び固定する. このとき,

$$\chi = \psi + (\theta_1 + \cdots + \theta_{p-1}) \tag{2.1}$$

という分解であって, 以下の条件を満たすものが存在する:

(i) ψ, θ_i は指標であるか, または 0;

(ii) $\mathrm{Ker}\,\psi \geq Z_0$, かつ $i = 1, 2, \ldots, p-1$ に対して $(\theta_i)_{Z_0} = \theta_i(1)\lambda_0^i$;

(iii) ψ は有理整数値, $\{\theta_1, \theta_2, \ldots, \theta_{p-1}\}$ は代数的共役に関して単一の類をなす;

(iv) $i = 1, 2, \ldots, p-1$ に対して $\mathrm{Im}\,\theta_i \subset \mathbb{Z}[\omega]$ $(\omega = \lambda_0(z_0))$. 特に, G の任意の p'-元 g に対して $\theta_i(g) \in \mathbb{Z}$ である.

Proof. $i = 1, 2, \ldots, p-1$ に対し, $\mathrm{Irr}(G, \lambda_0^i) := \{\varphi \in \mathrm{Irr}(G) \mid (\varphi_{Z_0}, \lambda_0^i)_{Z_0} > 0\}$ と定義し, さらに

$$\theta_i = \sum_{\varphi \in \mathrm{Irr}(G, \lambda_0^i)} (\chi, \varphi)_G\, \varphi \tag{2.2}$$

とおく. $\psi = \chi - \sum_{i=1}^{p-1} \theta_i$ とおけば, ψ, θ_i は (2.1), および (i), (ii) を満たす. この ψ, θ_i が (iii), (iv) を満たすことも容易に確認できる. □

命題 1 の分解は z_0 と λ_0 の組 (z_0, λ_0) によって決定される．この分解が有用であるのは，ψ や θ_i の取る値を χ を用いて明示することができるためである．これ自体は既知の事実であるから，結果だけを述べる．

補題 2. 命題 1 と同じ記号の下で以下が成り立つ:

$$\theta_1(1) = \frac{\chi(1) - \chi(z_0)}{p}, \quad \psi(1) = \theta_1(1) + \chi(z_0). \tag{2.3}$$

補題 3. $g \in G - Z_0$ とする．このとき，

$$\psi(g) = \frac{1}{p} \sum_{z \in Z_0} \chi(gz) \tag{2.4}$$

が成り立つ．特に，$\min L(\chi) \leqq \psi(g) \leqq \max L(\chi)$ である．

補題 4. $g \in G - Z_0$, $\omega = \lambda_0(z_0)$ とする．命題 1.(iv) より $\theta_1(g) \in \mathbb{Z}[\omega]$ だから，$\theta_1(g) = \sum_{j=1}^{p-1} m_j \omega^j$ $(m_j \in \mathbb{Z})$ とおく．このとき，次が成り立つ:

$$m_j = \frac{\chi(gz_0^{-j}) - \chi(g)}{p}. \tag{2.5}$$

特に，$j = 1, 2, \ldots, p-1$ に対して $\chi(gz^{-j}) \equiv \chi(g) \pmod{p}$ である．

本稿の主定理のように与えられた型を持つ指標 χ について考察しようというとき，χ を単独で扱っているだけでは得てして有効な手掛かりは得られない．一足飛びに χ の既約分解が得られればもちろん非常に強力な手掛かりとなるだろうが，そこまでの幸運もまた期待しがたい．そのため，命題 1 のような手軽な分解は重宝するのである．

裏をかえせば，これは定理 1 の条件から $Z(G) > 1$ という条件をなかなか落とせない理由でもある．ただし，命題 1 自体は $Z(G) = 1$ の場合においても役に立てる余地がある．なぜなら，適当な元 $g \in G$ を選んでその中心化群への χ の制限を考えれば，分解に必要な z_0 はいつでも調達できるからである．次の命題の証明がまさにその例である．

2.2 $|\mathrm{C}_G(g)|$ に関する補題

χ を G の有理整数値の指標とする．もし $L(\chi) = \{\ell, \ell + m\}$ $(\ell, m \in \mathbb{Z})$ ならば，任意の $\pi(m)'$-元 $x \in G$ に対して

$$o(g) \mid \chi(1) - \chi(x) \tag{2.6}$$

が成り立つことは古くから知られていた. 特に, $x, y \in G - \{1\}$ が $\chi(x) \neq \chi(y)$ を満たすような $\pi(m)'$-元であるならば, x と y は必ず非可換である.

これまで注目されてこなかったが, 実際にはより強く次の事実が成り立つ:

命題 5. χ を有限群 G の type $\{\ell, \ell+m\}$ $(\ell, m \in \mathbb{Z})$ の指標とする. このとき, G の自明でない $\pi(m)'$-元 x に対して

$$|\mathrm{C}_G(x)| \mid \chi(1) - \chi(x). \tag{2.7}$$

が成り立つ. 特に, $o(x) \mid \chi(1) - \chi(x)$ である.

Proof. 必要ならば χ の代わりに χ の $\mathrm{C}_G(x)$ への制限 $\chi_{\mathrm{C}_G(x)}$ を考えることにより, 最初から $x \in Z(G)$ と仮定してよい (もし $|L(\chi_{\mathrm{C}_G(x)})| = 1$ ならば, 単に

$$|\mathrm{C}_G(x)| \mid sh(\chi_{\mathrm{C}_G(x)}) = \chi(1) - \chi(x) \tag{2.8}$$

とするだけである). $Z_0 = \langle x \rangle$, $1_{Z_0} \neq \lambda_0 \in \mathrm{Irr}(Z_0)$ とする.

(x, λ_0) を用いて補題 1 と同じ分解 $\chi = \psi + \theta_1 + \cdots + \theta_{p-1}$ を作る. 明らかに $|G|$ の p-part $|G|_p$ は $sh(\chi)$ を割り切る. 仮定より $p \mid \chi(1) - \chi(x)$ かつ $p \nmid m$ なので, $|G|_p \mid \chi(1) - \chi(x)$ である. 一方, $\ell \not\equiv \ell + m \pmod p$ より, (2.5) において $\chi(gx^{-j}) \neq \chi(g)$ となるような g, j は存在しない. 従って任意の $g \in G - Z_0$ に対し $\theta_i(g) = 0$ である. 特に, $q \in \pi(G) - \{p\}$, $Q \in \mathrm{Syl}_q(G)$ に対し

$$|Q| \mid sh((\theta_i)_Q) = \theta_i(1) = \frac{\chi(1) - \chi(x)}{p} \tag{2.9}$$

が成り立つ. 以上より, $\chi(1) - \chi(x)$ は $|G|$ の倍数である. □

本稿の主旨から少し外れるが, 次の系が成り立つ.

系 6. $L = \{\ell, \ell+m\}$ かつ $sh(\chi) = c|G|$ とする. もし $0 < 2c < |G|$ ならば, $\pi(Z(G)) \subseteq \pi(m)$ である.

Proof. 仮に $p \in \pi(Z(G))$ であって m を割り切らないものがあったとする. $Z(G)$ の位数 p の元 z_0 を 1 つ決めて ψ, θ_i を命題 5 の証明と同様に作る. また, $\theta = \chi - \psi$, $\chi(1) - \chi(z_0) = t|G|$ $(t \in \mathbb{N})$ とおく.

$\chi = \psi + \theta$ という分解は [5, 命題 4] の条件 (i), (ii) を満たす. これより, $(\theta, \theta)_G \leqq c$ であることが示せる. 一方, $(\theta_1)_{Z_0} = \theta_1(1)\lambda_0$ かつ θ_1 は Z_0 の外で 0 のみをとるから,

$$(\theta_1, \theta_1)_G = \frac{p\theta_1(1)^2}{|G|} = \frac{t^2|G|}{p} \tag{2.10}$$

である．よって，

$$c \geqq (\theta,\theta)_G = \frac{p-1}{p}t^2|G| \geqq \frac{|G|}{2} \tag{2.11}$$

となり仮定に反する．以上より，このような p は存在しない． □

3. G/Z の構造

これ以降，(G,χ) は定理 1 と同じ仮定を満たすとする．すなわち，(G,χ) は type $\{\ell,\ \ell+p\}$ (p : 奇素数) の sharp pair であり，$Z = Z(G) > 1$ を満たすとする．この節では定理 1 の証明に必要な補題を幾つか用意する．

補題 7. (G,χ) を定理 1 の通りとする．このとき，Z は p-群である．さらに，$k = (\chi(1)-\ell)/p$ とおけば，$k \in \mathbb{N}$ かつ $|G| = p^2k(k-1)$ が成り立つ．

Proof. 系 6 より，$|Z|$ は p-ベキでなければならない．特に，$|G|$ は p の倍数である．さらに，sharp 指標の定義より

$$|G| = sh(\chi) = (\chi(1)-\ell)(\chi(1)-\ell-p) \tag{3.1}$$

であるから，$\chi(1)-\ell$ も p の倍数でなければいけない．これより直ちに補題が従う． □

有限群 H が与えられたとき，H の素数グラフ $\Gamma(H)$ を次で定義する: $\Gamma(H)$ の頂点集合は $\pi(H) := \pi(|H|)$ であり，2 つの頂点 $p,\ q \in \pi(H)$ は H が位数 pq の元を持つときに辺で結ばれる．このとき，以下が知られている:

定理 2 (Williams[4])**.** H を有限群，π_1 を $\Gamma(H)$ の連結成分のうち 2 を含むものとする．もし $\Gamma(H)$ が非連結なグラフならば，H は次のいずれかの構造を持つ:

(a) Frobenius 群，または 2-Frobenius 群;

(b) 非可換単純群;

(c) π_1-群の単純群による拡大;

(d) 単純群の π_1-群による拡大;

(e) π_1-群の単純群による拡大を，さらに π_1-群で拡大したもの．

ここで，H が 2-Frobenius 群であるとは，H の自明でないある正規部分群 M, N が存在して，(i) M は N を Frobenius 核とする Frobenius 群であり，かつ (ii) H/N は M/N を

Frobenius 核とする Frobenius 群であることをいう.

[6] の主結果の証明において, G/Z の素数グラフが非連結であることを示して定理 2 を適用することは最重要事項であった. 実は, 前節で準備した命題 5 を利用すれば, 以下の事実を ([6] におけるそれと比べても) はるかに簡単に導くことができる.

補題 8. $x \in G$ を自明でない p'-元とする. このとき, 以下が成り立つ:

(1) $o(x)$ は k または $k-1$ のいずれかの約数である;

(2) $o(x) \mid k$ ならば, $\chi(x) = \ell$, かつ $|\mathrm{C}_G(x)| \mid pk$;

(3) $o(x) \mid k-1$ ならば, $\chi(x) = \ell + p$, かつ $|\mathrm{C}_G(x)| \mid p(k-1)$.

Proof. 命題 5 を χ にそのまま適用するだけである. □

補題 9. (G, χ) を定理 1 の通りとするとき, 以下が成り立つ:

(1) $|Z| = p$;

(2) G/Z の素数グラフ $\Gamma(G/Z)$ は非連結である;

(3) もし $p^3 \nmid |G|$ ならば, p は $\Gamma(G/Z)$ の孤立点である.

Proof. $\bar{G} = G/Z$ とおく. $k = 2$ ならば明らかなので $k > 2$ としてよい. $k_1 \in \{k, k-1\}$ を $p \nmid k_1$ となるように選び, 自明でない $\pi(k_1)$-元 $x \in G$ を勝手に取る. このとき $Z \leq \mathrm{C}_G(x)$ であるが, 補題 8 より $|\mathrm{C}_G(x)|$ は p^2 で割り切れない. ゆえに (1) を得る.

また, $|\mathrm{C}_G(x) : Z|$ が k_1 の約数であるから, $\mathrm{C}_{\bar{G}}(\bar{x})$ は $\pi(k_1)$-元のみを含む. ゆえに, 任意の $q \in \pi(k_1)$, $r \in \pi(G) - \pi(k_1)$ に対し $\bar{G}$ は位数 qr の元を持たない. よって (2) が成り立つ. 最後に, k と $k-1$ の両方が p と互いに素であるならば, それぞれを k_1 と見て上と同じ議論を行うことによって $\bar{G}$ は位数 pq $(q \in \pi(G) - \{p\})$ の元を持たないことが分かる. □

補題 9 より, G/Z は定理 2 の (a)–(c) のいずれかの構造を持つことが分かる. G/Z の構造をさらに絞り込むためには, $\mathrm{O}_{p'}(G/Z) = 1$ であることを証明する必要がある. $p^3 \nmid |G|$ のときは次のように直接示すことができる.

補題 10. もし p が $\Gamma(G/Z)$ の孤立点であるならば, $\mathrm{O}_{p'}(G/Z) = 1$ である. 特に, $p^3 \nmid |G|$ のとき $\mathrm{O}_{p'}(G/Z) = 1$.

Proof. $\bar{G} = G/Z$, $\bar{P} \in \mathrm{Syl}_p(\bar{G})$ とする. 仮に $1 \neq \bar{N} \lhd \bar{G}$ かつ $p \nmid |\bar{N}|$ であったとしよう.

このとき $\bar{P}$ は $\bar{N}$ へ fixed-point-free に作用するから $\bar{N}$ は巾零である．従って，補題 8 より

$$|\bar{N}| \mid k \text{ or } k-1 \tag{3.2}$$

でなければならない．もし $|\bar{N}| \mid k-1$ ならば，任意の $q \in \pi(k)$, $\bar{Q} \in \mathrm{Syl}_q(\bar{G})$ について

$$|\bar{Q}| \mid |\bar{N}|-1 \tag{3.3}$$

が成り立つから，$k \mid |\bar{N}|-1 \leqq k-2$ となり矛盾する．よって $|\bar{N}| \mid k$ であるが，このときも同様の議論により $|\bar{N}| = k$ を得る．ゆえに $p \mid k-1$ となるが，$|\bar{G}| = pk(k-1)$ であるから結局 $p(k-1) \mid k-1$ となり矛盾が生じる． □

$p^3 \mid |G|$ の場合は別のアプローチを取る必要がある．$|Z| = p$ であるから，$1 \neq z_0 \in Z$ と $1_Z \neq \lambda_0 \in \mathrm{Irr}(Z)$ を選んで命題 1 を適用し

$$\chi = \psi + (\theta_1 + \cdots + \theta_{p-1}) \tag{3.4}$$

と χ を分解しておく．ここで，ψ, θ_i は必ずしも既約ではないが，それ以外は [7, §2] の分解とまったく同じ条件を満たす (cf. [7, §5])．

補題 11. $p^3 \mid |G|$ とする．このとき，$g \in G - Z$ に対して次が成り立つ:

(1) $p \mid o(g)$ ならば，$\theta_i(g) = 0$;

(2) $p \nmid o(g)$ ならば，$|\theta_i(g)| \leqq 1$.

Proof. (1) は [7] の系 5, 補題 6, 15, 17 から，(2) は [7] の系 9 から得られる． □

補題 12. $p^3 \mid |G|$ とする．このとき，θ_i は既約である．

Proof. 補題 11 より，

$$|G|(\theta_i, \theta_i)_G \leqq p\theta_i(1)^2 + |G - Z| < 2|G| \tag{3.5}$$

を得る．よって，θ_i は既約である． □

もし θ_i が既約指標であれば，[6] のときと同様に θ_i が G の principal p-block に属することを利用して $\mathrm{O}_{p'}(G/Z) = 1$ を導くことができる．従って，$p^3 \mid |G|$ のときも $\mathrm{O}_{p'}(G/Z) = 1$ が成り立つ．こうして $\Gamma(G/Z)$ と $\mathrm{O}_{p'}(G/Z)$ に関する重要な補題が $L = \{\ell, \ell + p\}$ の場合にも成り立つことが，結果として主定理の結果に繋がるのである．

4. 主定理の証明の概略

以上の準備のもとで定理 1 を証明する．ただし，残りの議論の大部分は [7] の §4 の内容をそのまま真似るだけであるから，ここでは概略を紹介するに留める．

以下，$\bar{G} = G/Z$ とおく．また，$\Gamma(\bar{G})$ の連結成分のうち 2 を含むものを π_1 で表す．前節で見たように，$\bar{G}$ は定理 2 の (a)–(e) のいずれかの構造を持つ．まず最初に，このうち (d), (e) の構造は起こりえないことを示す．

補題 13. $\bar{G}$ は自明でない正規 π_1-部分群を持たない．特に，$\bar{G}$ が定理 2 の (d), (e) の構造を持つことはない．

Proof. $1 \neq \bar{N} \triangleleft \bar{G}$, かつ $\pi(\bar{N}) \subseteq \pi_1$ と仮定する．このとき，補題 10 の証明と同様に $\bar{N}$ が巾零であることが示せる．しかし，もし $\bar{N}$ が巾零ならば，その Sylow 2-部分群は $\bar{G}$ の自明でない正規 p'-部分群となってしまう．これは $\mathrm{O}_{p'}(\bar{G}) = 1$ に反する． □

補題 14. $\bar{G}$ が定理 2 の (b), (c) の構造を持つならば，G は §1 の (i)–(v) のいずれかの群と同型である．

Proof. $p^3 \nmid |G|$ のときは [7, 補題 25] の議論を修正なしに適用することができる．$p^3 \mid |G|$ のとき，[7, 補題 26] の Step 4 において

$$p \nmid |\bar{G} : \bar{S}| \tag{4.1}$$

を示す箇所のみ (ψ の既約性を用いているため) 変更が必要である．

$p \mid |\bar{G} : \bar{S}|$ と仮定する．$\bar{S}$ の素数グラフの連結成分のうち，2 を含むものを π_1^S, p を含むものを π_2^S とし，$\pi = \pi_1^S \cup \pi_2^S$ とおく．$\bar{S}$ は $\mathrm{PSL}(2,q)$ または $\mathrm{Sz}(q)$ と同型であるから，π の候補は数通りしかない．$\{k, k-1\}$ のうち p で割り切れるものを k_0, 割り切れないものを k_1 とすると，

$$|\bar{S}|_\pi \mid k_0 \quad \text{かつ} \quad k_1 \mid |\bar{S}|_{\pi'} \tag{4.2}$$

でなければならないことが容易に分かる．これらの条件と $|k_0 - k_1| = 1$ を同時に満たす $\bar{S}$, π が存在しないため，結局 $p \nmid |\bar{G} : \bar{S}|$ と結論付けられる． □

最後に，$\bar{G}$ が Frobenius または 2-Frobenius であるときも，G が §1 の (i), (vi), (vii) のいずれかと同型になることを確認できる．この後，§1 の (vi) の群を除いて必ず $\ell \in \{-1, 1-p\}$

となることを確かめるのであるが, これらを示すにはあまり本質的とは言い難い煩雑な議論を続けなければならないため本稿では証明を割愛する.

参考文献

[1] D. Alvis and S. Nozawa, *Sharp characters with irrational values*, J. Math. Soc. Japan 48 (1996) 567–591.

[2] P.J. Cameron and M. Kiyota, *Sharp characters of finite groups*, J. Algebra 115 (1988) 125–143.

[3] N. Iiyori and H. Yamaki, *Prime graph components of the simple groups of Lie type over the field of even characteristic*, J. Algebra 155 (1993) 335–343.

[4] J.S. Williams, *Prime graph components of finite groups*, J. Algebra 69 (1981) 487–513.

[5] T. Yoguchi, *On determining the sharp characters of some finite groups*, JP J. Algebra, Number Theory and Applications 11 (2008), 85-98.

[6] T. Yoguchi, Rank 2 のシャープ指標を持つ有限群について, 代数的組合せ論および関連する群と代数, 信州大学, 2009 年 11 月 17 日〜11 月 20 日

[7] T. Yoguchi, *On sharp characters of type* $\{\ell, \ell+p\}$, Kyushu Journal of Mathematics Vol.65 no.1 (2011), 179–195.

群上の単項式に関する一定理と有限単純群の分類定理

山口大学　飯寄信保
(Yamaguchi University, Iiyori, Nobuo)

1

有限単純群の分類定理とは、有限単純群は次に挙げる単純群のいずれかと同形であるというものである：(1) 素数位数の巡回群、(2) 5次以上の次数の交代群、(3)Lie型の単純群、(4)(1)〜(3) に挙げた群以外の単純群（すべて判明している)。

有限単純群の分類定理に出てくる群について詳細なデータは、例えば、P. Kleidman-M. Liebeck 著 "The Subgroup Structure of the Finite Classical Groups" の文献リストに論文・本に豊富に見つけることができる。これらの知識を用いて群論等に関する諸問題を解決しようという試みが数多くなされているが、このようにして得られた結果をもとに新たな理論が生まれることが重要であると筆者は思う。しかし分類定理を用いて解かれた問題について別視点からの考察・再証明等はなかなか行われていない。講演において、有限単純群の分類定理を用いて解かれた問題の分類定理を用いない証明を与える一例について解説した。分類定理を用いた部分以外にも整理しできるだけ美しい証明を与えようと試みた。これは、素数グラフ及びその一般化についての考察の成果の一つである。

2

講演において紹介したのは、次の定理である。

主定理. pを素数とし、Gは、位数がpで割り切れるような有限群とする。$\sigma \in G$を位数pの元とする。Gにおける単項式 $f(X)$ を $f(X) = (X\sigma)^p$ で定義する。単項式 $f(X)$ が $f(G_{p'}) = \{1\}$ を満たすならば、Gは、p-冪零でありかつ、 $O_{p'}(G)$ は、冪零である。

主定理に出てくる用語の説明を簡単にしておく。Gを群、Fを自由群とする。Gにおける単項式とは、GとFの自由積 $F * G$ の元のことであり、主定理においてのFは不定元Xで生成される階数1の自由群である。

主定理の場合、Gの元はそのまま移しXを$g \in G$に移すような写像は一意に定まる。これをg^*とおけば、g^*は$F*G$からGへの準同形写像である。Gにおける単項式$f(X)$に対し、$f(g) = g^*(f(X))$と定義する。

この主定理は、次に挙げるKegelによる定理の拡張である。尚、Kegelの定理は、有名なThompsonによるFrobenius核が冪零であるという定理の拡張になっている。

Kegelの定理　pを素数とし、Gは、指数pの正規部分群Hをもつ有限群とする。もし$G-H$が位数pの元から成っているならば、Hは冪零群である。

主定理は、昔、熊本大学で行われた研究集会において有限単純群の分類定理の応用として証明の概略とともに紹介したものである。簡単にこのとき紹介した証明を紹介する。

主定理を証明するためには、まず次の特殊な場合に制限した命題を考える。この命題は、Kegelの定理の直接の拡張である。

命題　pを奇素数とし、Gを有限群G_0の指数pの正規部分群とする。$\sigma \in G_0 - G$を位数pの元、$f(X) = (X\sigma)^p$と単項式を定義する。もし、単項式$f(X)$が$f(G_{p'}) = \{1\}$を満たすとすれば、Gはp-冪零であり、$O_{p'}(G)$は冪零である。

上の命題を証明するため、順番からいうとまず、Gが可解である場合に考察することになる。これについては、後程別に少し詳しく述べることにするが、Gを可解と仮定すると、上の命題から主定理を導くのは容易なので、主定理を証明したことになる点に注意してもらいたい。また、$p = 2$の場合は、主定理及び上の命題は容易に検証することができるのでpを奇素数として考えても問題はない。

以下、Gを可解でないと仮定する。さらに、Gを命題の最小位数の反例とおいて矛盾を導く。Nを極大なGのG_0-不変正規部分群とする。もしNを非自明とすれば、G_0/N及び$N\langle\sigma\rangle$は命題の仮定を満たすので、Gは可解となり矛盾である。よってGは、非自明なG_0-不変正規部分群を持たない。Gは単純群でないとする。$\langle\sigma\rangle$は、Gの成分の集合に可移に作用するので成分の一つをSとすれば、$1 \neq x \in S_{p'}$に対して、

$$f(x) = x \cdot x^{\sigma} \cdot x^{\sigma^2} \cdots x^{\sigma^{p-1}} \cdots\cdots (\sharp)$$

かつS^{σ^i} $(0 \leq i \leq p-1)$は互いに異なる成分なので$f(x) \neq 1$を得る。これは矛盾である。

Gが単純群であると分かったので、直接、分類定理を用いることが可能になり最終的な矛盾を得ることができる。具体的にいうと、シローp-部分群Pが非可換であること、Pの中心の部分群の中心化群と正規化群が一致することなどを示すことができるので、これらが単純群に対して成り立たないことを見ればよいことになる。大急ぎであったが以上が命題の証明が完結した。

主定理の証明に戻る。G を主定理の最小位数の反例として矛盾を導く。N を σ を含む正規部分群とすれば、$f(X)N = X^pN$ が G/N 上で成り立つので G/N は、p-群でなければならない。G の最小性より、$G = N$ が成り立つ。また、M を G の G と異なる正規部分群で σ を含まないものとする。$\langle\sigma\rangle M \neq G$ であれば、G/M 及び $\langle\sigma\rangle M$ は主定理が成り立つので可解になる。G は、可解でないので矛盾である。よって $G = \langle\sigma\rangle M$ となるが、先に示した命題により、矛盾を得る。以上より、G は単純群となる。有限単純群の分類定理により最終的な矛盾を得るわけであるが、検証方法によって異なるかもしれないが、ほとんど先に示した命題を検証する方法と同じ議論で検証することができると思う。

講演で紹介した分類定理を使わない証明もほとんど上で紹介した証明と一致する。異なる点は、単純群と限定するあたりからである。（本質的には、単純群に関する考察の部分からといってよい。）P を σ を含む G（または、G_0）のシロー p-部分群とする。このとき $N_G(ZJ(P))$ は σ を含み、仮定より $N_G(ZJ(P))$ が、p-冪零であることがわかる。Thompson の有名な定理（鈴木通夫著「群論」5 章定理 4.15 等を参照のこと）により、G は、p-冪零となり矛盾が生じる。以上で証明が完結する。

3

この節では、主定理を導くために示した「命題」の G が可解である場合について考えてみる。繰り返しになるが示すべき命題を示すことにする。

命題　p を奇素数とし、G を有限可解群 G_0 の指数 p の正規部分群とする。$\sigma \in G_0 - G$ を位数 p の元、$f(X) = (X\sigma)^p$ と単項式を定義する。もし、単項式 $f(X)$ が $f(G_{p'}) = \{1\}$ を満たすとすれば、G は p-冪零であり、$O_{p'}(G)$ は冪零である。

以下、G_0 を最小位数の反例とし、$S = \langle\sigma\rangle$ とする。節 2 で説明した議論を用いれば、G の最小性から G は S-不変な正規部分群 N で次を満たすものを持つ：G/N は S-既約な基本 q-可換群、G_0-既約な N は基本 p-可換部分群である。Q を G のシロー q-部分群とすると、Clifford の定理と節 2 で (‖) 式を用いて議論した方法を用いると N は Q-既約であることを示すことができる。N は Q-既約であったので、Q は位数 q の巡回群であり、G は Frobenius 核が N である Frobenius 群であることがわかる。ここで重要なのは、Q は $\mathrm{End}_{\mathbf{F}_p}(N)$ の部分集合であるということである。$\mathcal{F} = \mathrm{span}_{\mathbf{F}_p} Q$ と置くと $\mathcal{F}$ は元の個数が $|N|$ である有限体になる。$1 \neq z \in C_N(S)$ を固定し、

$$\varphi : \mathcal{F} \to N \ (x \to z^x)$$

と定義すると、φ は S-加群同形であることがわかる。

$$\mathrm{Tr}(v) = \Pi_{\tau \in S} v^\tau$$

と置く。このTrと$f(X)$との関係について説明しよう。$1 \neq u \in Q$に対し、$g \in G_0$と$w \in N$で$gu\sigma g^{-1} = w\sigma$を満たすものが存在する。このとき$v \in N$に対し、

$$f(vu) = \mathrm{Tr}_S(v^{g^{-1}})^g$$

が成立する。写像φを介して、TrはGalois拡大体$\mathcal{F}/\mathcal{F}^S$のトレースと同一視ができる。Hibertの定理90によれば、トレースは全射である。これは、命題の仮定に矛盾する。以上により命題の証明が完結する。

$\mathcal{F} = \mathrm{span}_{\mathbf{F}_p} Q$とした部分について注意しておく。この$\mathcal{F}$は、$G$の部分集合ではない。$G$上の単項式で1を代入して1になるようなものの集合を$\mathcal{S}$とする。$\mathcal{S}$の元の定義域をNに制限すると、NからNへの写像となる。$\mathcal{S}$は、写像の合成により半分配環となる。Nがアーベル群であるので$\mathcal{S}$は環となり、$\mathcal{S} = \mathcal{F}$となる。このように、$\mathcal{F}$は群の単項式論の立場から見ると極、自然なものである。

以上が、単純群の分類定理を用いて証明された問題の再証明の一例である。詳細については、Communications in Algebra 38: 1695-1698, 2010 N. Iiyori, Characterization of p-Nilpotent Groups by Monomials of Finite Groups をご覧ください。

Rudvalis群と符号

千吉良直紀
熊本大学大学院自然科学研究科

1 Introduction

散在型単純群 Ru が作用する符号の存在は、北詰正顕氏による 2008 年の代数学シンポジウムの講演で触れられている [2]。ここではその符号についての詳しい考察と、関連して得られた Ru の別の構成について述べる。この研究は北詰氏との共同研究である。

2 符号

有限群 G が集合 Ω に作用するとする。$g \in G$ に対して、

$$\mathrm{Fix}(g) = \{i \in \Omega \mid i^g = g\}$$

とおく。また、$I(G)$ で G の位数 2 の元 (involution) 全体の集合とする。

$|\Omega| = n$ であるとき、Ω の部分集合全体の集合 $\mathcal{P}(\Omega)$ を対称差で $\mathbb{F}_2^n$ とみなす。この部分空間（2 元体上の符号）として、

$$C(G,\Omega) = \langle \mathrm{Fix}(u) \mid u \in I(G)\rangle^{\perp}$$

を考える。ここで、$\perp$ は標準内積に関する直交補空間である。

定理 1 ([1]). G が Ω に作用するとする。長さ $n = |\Omega|$ の self-orthogonal code（自己直交符号）C が G 不変ならば、$C \subseteq C(G,\Omega)$ である。

この定理を用いて $n = |\Omega| \leq 1000$ で、散在型単純群が作用するような自己直交符号を求めた（詳細は、[1] を参照のこと）。

3 Rudvalis群

Rudvalis 群 Ru は位数 $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$ の散在型単純群である。Ru は 4060 点上の rank 3 のグラフの自己同型群として構成されている。1 点の固定部分群は ${}^2F_4(2) = {}^2F_4(2).2$ (non-split) である。このグラフについて復習をしておく。

$H = {}^2F_4(2)$ には involution の class が 2 つある。ATLAS にしたがって $2A$, $2B$ とおくと、

u	$C_H(u)$
$2A$	$2.2^4.2^5:(5:4)$
$2B$	$2^3.2^6:S_3$

である。u が $2A$ であるとき、$C_H(u)$ は H の極大部分群であり、$|H:C_H(u)|=1755$ である。また、H には $L_2(25).2_3$ (non-split) と同型な極大部分群 K が存在する。$|H:K|=2304$ である。

$2A=\{u \mid u\in 2A\}$ と $\mathcal{K}=\{K^h \mid h\in H\}$ とさらに 1 点 $*$ を付け加えて $1+1755+2304=4060$ 点を頂点とするグラフを以下のように定義する。

- $*$ joins all $u\in 2A$
- for $u_1,u_2\in 2A$, $\quad u_1$ joins $u_2 \Leftrightarrow o(u_1u_2)=2$, or 4
- for $u\in 2A$, $K\in\mathcal{K}$, $\quad u$ joins $K \Leftrightarrow C_H(u)\cap K\cong D_{20}$
- for K_1, $K_2\in\mathcal{K}$, $\quad K_1$ joins $K_2 \Leftrightarrow |K_1\cap K_2|=16$

このグラフ Γ_{Ru} を Ru-graph といい、

$$\mathrm{Aut}(\Gamma_{Ru})=Ru$$

である。

4 Ru の作用する符号

$G=Ru$ とし、Ω を 4060 点集合とする。$C(G,\Omega)$ を調べるために $u,v\in I(G)$ に対して $\mathrm{Fix}(u)\cap\mathrm{Fix}(v)$ の様子を調べることにする。

$\mathrm{Fix}(u)\cap\mathrm{Fix}(v)\neq\emptyset$ である場合を考察すればよいので、$u,v\in H={}^2F_4(2)$ であるとしてよい。

H の部分群である $L_2(25).2_3$ は $2A$-element を含まない。このことから、$u\in 2A$ は $\mathcal{K}$ の元を固定しないことが分かる。また、$u_1,u_2\in 2A$ のとき

$$|C_H(u_1)\cap C_H(u_2)\cap 2A|=3,5,11,\text{ or }27$$

となる。u_1,u_2 ともに $*$ を固定しているので、

- $u_1,u_2\in 2A$ のとき、$|\mathrm{Fix}(u_1)\cap\mathrm{Fix}(u_2)|=4,6,12,$ or 28

であることが分かる。

$u\in 2A$, $w\in 2B$ のときには、

$$|C_H(u)\cap C_H(w)\cap 2A|=1,3,11,\text{ or }27$$

となるので、

- $u \in 2A$, $w \in 2B$ のとき、$|\mathrm{Fix}(u) \cap \mathrm{Fix}(w)| = 2, 4, 12,$ or 28

であることが分かる。

$w_1, w_2 \in 2B$ のときには、$|C_H(w_1) \cap C_H(w_2) \cap 2A|$ と $\sharp\{K \in \mathcal{K} \mid w_1, w_2 \in K\}$ を考えると、

- $w_1, w_2 \in 2B$ のとき、$|\mathrm{Fix}(u) \cap \mathrm{Fix}(w)| = 2, 4, 6, 12,$ or 28

であることが分かる。以上より、

$$u, v \in I(G) \text{ に対して、} |\mathrm{Fix}(u) \cap \mathrm{Fix}(v)| = 0, 2, 4, 6, 12, \text{ or } 28$$

となる。したがって

命題 1. $\langle \mathrm{Fix}(u) \mid u \in I(G)\rangle$ は doubly even である。

$U \cong U_3(3) \subset Ru$ をとると、$|I(U)| = 63$ であり、

$$\dim(\langle \mathrm{Fix}(u) \mid u \in I(U)\rangle) = 63$$

となる。G には次の性質を満たす $P \in Syl_5(G)$ が存在する。

- $U \cap U^x = 1$ for $1 \neq x \in P$

$\{U^x \mid x \in P\} = \{U_1, \cdots, U_{125}\}$, $F_i = \langle \mathrm{Fix}(u) \mid u \in U_i\rangle$ とすると、

- $F_i \cap F_j = \{0\}$
- $\dim(\bigoplus_{i=1}^{32} F_i) = 63 \times 32 = 2016$, $\dim(\bigoplus_{i=1}^{33} F_i) = 2029$

以上より次のことがいえる。

命題 2. $\langle \mathrm{Fix}(u\rangle \mid u \in I(G)\rangle$ は doubly even $[4060, 2029]$ code である。

系 1. $C(G, \Omega)$ は $[4060, 2031]$ code である。

このことから、$\langle \mathrm{Fix}(u) \mid u \in I(G)\rangle$ と $C(G, \Omega)$ との間に self-dual code がある。すなわち、

定理 2. Ru 不変な self-dual $[4060, 2030]$ code が 3 つ存在する。

注意 1. 自己同型群はそれぞれ Ru であることも分かる。

5 $U_3(3)$ からの Ru の構成

Ru の作用する self-dual code の次元を計算する際に、$U_3(3)$ がいい働きをしている。そこで、$U_3(3)$ を使って Ru を詳しく調べてみた。Ru と $U_3(3)$ の関係として特筆すべきことは、Ru が $\mathbb{F}_2$ 上 28 次元の表現を持っていて、うまく部分群 $U_3(3)$ をとると、$U_3(3)$ の $3^3 + 1 = 28$ 次の置換表現が、Ru の $\mathbb{F}_2$ 上２８次元のベクトル空間の、座標の置換として作用していることである。

$U_3(3)$ の作用する次のようなデザインを考える。

D		Blocks	Aut
2-(28, 4, 1)	1-(28, 4, 9)	63	$U_3(3):2$
2-(28, 9, 96)	1-(28, 9, 324)	1008	$U_3(3)$
2-(28, 16, 640)	1-(28, 16, 1152)	2016	$U_3(3)$
2-(28, 17, 272)	1-(28, 17, 459)	756	$U_3(3)$
2-(28, 20, 95)	1-(28, 20, 135)	189	$U_3(3):2$

$U_3(3)$ の作用する 28 点を加えると、

$$28 + 63 + 1008 + 2016 + 756 + 189 = 4060$$

である。これらの blocks（28 点も block と思って）から任意の２つの X, Y に対して

$$X \text{ joins } Y \iff |X \cap Y| \equiv |X| \times |Y| \pmod 2$$

と定めると、グラフが出来る。例えば $\{1\}$ と結ばれる集合は $|\{1\} \cap |Y|| \equiv |Y| \pmod 2$ なので、$|Y|$ が奇数ならば、$1 \in Y$, $|Y|$ が偶数ならば $1 \notin Y$ となるような Y である。したがってその総数は

$$(63 - 9) + 324 + (2016 - 1152) + 459 + (189 - 135) = 1755$$

となる。

このグラフを Δ とすると、次のことが成り立つ。

定理 3.
- $\Delta \cong \Gamma$
- $\mathrm{Aut}(\Delta) \cong Ru$

このようにうまく $U_3(3)$ を使って Ru-graph が構成できる。

参考文献

[1] N. Chigira, M. Harada and M. Kitazume, Permutation groups and binary self-orthogonal codes, J.Algebra **309** (2007), 610–621.

[2] 北詰正顕, 散在型単純群の周辺, 第５３回代数学シンポジウム報告集

グラフの変異 (mutation) が生成する群について

入江 佑樹 Yuki Irie*

1 はじめに

変異 (mutation) は, 有向グラフに対する鏡映 (矢印の向きを逆にする操作) を変形した操作であり, Fomin と Zelevinsky がクラスター代数において導入した [6]. グラフ Γ から mutation を繰り返して得られるグラフ全体を Γ の mutation 同値類 と呼ぶ. このとき mutation は Γ の mutation 同値類上の位数 2 の置換となる.

本研究の目的は, mutation を mutation 同値類上の置換とみて, その群構造を計算・考察することである.

その結果, ほとんどの場合に交代群または対称群となるが, $\mathbb{Z}$ 上で頂点数が 4 の倍数の場合に 2 つの交代群の直積が現れる場合があることがわかった. また, $\mathbb{F}_q$ で頂点数が 3 の場合に例外的に $PSL(2,p)$ または $PGL(2,p)$ (p, q は素数) が現れる系列を発見し, 一般に証明した. その際に, 3 頂点の場合の mutation 不変量を得た.

2 mutation の定義

R を可換環とし, R から R への写像 $|\cdot|$ は

$$|a| = |-a| \in \{a, -a\} \ (\forall a \in R)$$

を満たすとする. また, $a \in R$ に対して $|a| = a$ のとき $a \geq 0$, $|a| = -a$ のとき $a \leq 0$ と表すことにする.

$\Gamma := (b_{ij})$ を成分が R の m 次交代行列とし, 隣接行列が Γ のグラフと同一視する. このとき, 頂点 $k \in \{1, 2, \ldots, m\}$ による Γ の mutation を次の m 次交代行列 $\Gamma^{\tau_k} := (b'_{ij})$ で定義する:

$$b'_{ij} := \begin{cases} -b_{ij} & (i = k \text{ or } j = k), \\ b_{ij} + |b_{ik}|b_{kj} & (b_{ik}, b_{kj} \geq 0 \text{ or } b_{ik}, b_{kj} \leq 0), \\ b_{ij} & (\text{otherwise}). \end{cases}$$

Γ に mutation を繰り返し施して得られる行列全体を Γ の mutation 同値類と呼び, O_Γ と表す. このとき, 各 mutation は, O_Γ 上の位数 2 の置換となる. そこで, $\tilde{G}_\Gamma := \langle \tau_k : O_\Gamma \to O_\Gamma \mid k \in \{1, 2, \ldots, m\} \rangle$ とおく. このとき, $\{\{\lambda, -\lambda\} \mid \lambda \in O_\Gamma\}$ は $\tilde{G}_\Gamma$ のブロック系になるので, このブロック系への作用の核 K で $\tilde{G}_\Gamma$ を割った群を G_Γ と表し, Γ の mutation が生成する群と呼ぶ.

O_Γ は一般には有限とは限らないが, ここでは有限となる場合のみを扱う.

* 千葉大学理学研究科 email: irie@chiba-u.jp

3 $\mathbb{Z}$ 上の mutation($R = \mathbb{Z}$ の場合)

本節では, $\mathbb{Z}$ 上で mutation 同値類が有限となるグラフの分類の先行研究を紹介した後, それらの mutation が生成する群の計算結果を述べる. 以下, $m = 2$ の場合は自明なため, $m > 2$ とする.

3.1 有限となるグラフの分類

$\mathbb{Z}$ 上の mutation について, Buan と Reiten は 有限次元代数の表現論を応用し, mutation 同値類 O_Γ が有限となる tree の分類をした [3].

定理 3.1 (Buan, Reiten, 2006). Γ が tree のとき O_Γ が有限となるのは, Γ から矢印を除いた無向グラフ[*1]が Coxeter-Dynkin 図形 $A_n, D_n, E_{6,7,8}$ とその拡大になる場合に限る.

さらに一般のグラフについては, Felikson らが分類した [5].

定理 3.2 (Felikson, Shapiro, Tumarkin, 2008). O_Γ が有限となるのは, block decomposable なものか, Coxeter-Dynkin 図形 $E_{6,7,8}, \tilde{E}_{6,7,8}, E_{6,7,8}^{(1,1)}$ と $X_{6,7}$ になる場合に限る.

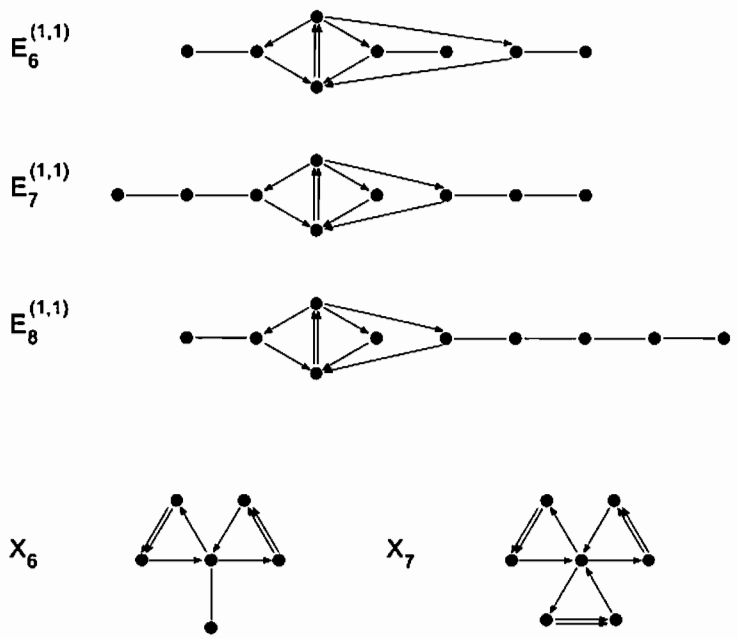


図 1 例外的に有限となるグラフ (向きの入っていない辺はどちら向きでも良いことを意味する)

[*1] tree の場合, 矢印の向きを任意に変えても mutation 同値である.

なお，グラフが block decomposable とは図 2 の 6 種類のグラフの白丸同士を有限回同一視してできることを指す (黒丸は同一視できず，一度同一視した白丸は黒丸になる)．白丸同士を同一視してできる block decomposable なグラフの例を図 3 に挙げる．

図 2　block decomposable

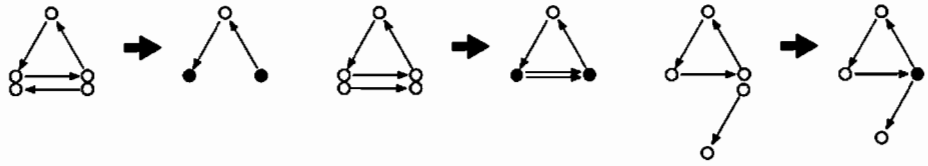


図 3　白丸を同一視してできる block decomposable なグラフ

3.2　mutation が生成する群

mutation 同値類が有限となるグラフの内，頂点数が 8 点以下の tree とその他いくつかの場合について群の構造を決定した．表 1 と表 2 が結果である．

Γ	G_Γ
A_3	S_7
A_4	$(A_{36} \times A_{36}) : 2$
A_5	S_{990}
A_6	A_{17160}
A_7	A_{360360}
A_8	A_{360360}
A_8	$(A_{4455360} \times A_{4455360}) : 2$
D_4	A_{25}
D_5	A_{1092}
D_6	A_{20160}
D_7	A_{451440}
D_8	$A_{11891880}$

表 1　A_n, D_n

Γ	G_Γ
$\tilde{D}_4$	S_{135}
$\tilde{D}_5$	A_{8100}
$\tilde{D}_6$	S_{198450}
$\tilde{D}_7$	$A_{5715360}$
E_6	A_{21420}
$\tilde{E}_6$	A_{252000}
$E_6^{(1,1)}$	$(A_{294000} \times A_{294000}) : 2$
E_7	$A_{1048320}$
$\tilde{E}_7$	$A_{21168000}$
E_8	$(A_{15800400} \times A_{15800400}) : 2$
X_6	A_{780}
X_7	A_{840}

表 2　$\tilde{D}_n, E_n, \tilde{E}_n, E_n^{(1,1)}$

mutation 同値類や群構造は GAP を用いて計算した．ここで，対称群や交代群は表のように次数が大きい場合でも短時間で判定できる[*2]．また，E_8 など 2 つの交代群の直積が現れる場合は，次の方法で決定できた:

(1) Γ を m 頂点グラフとし，H を G_Γ の指数 2 の部分群 $\langle \tau_1\tau_2 K, \tau_1\tau_3 K, \ldots, \tau_1\tau_m K\rangle$ とする．

(2) H の軌道は 2 つあり，同じ大きさ n であることがわかるので，それらを O_1, O_2 とする．そして，各軌道に H を制限すると n 次交代群になることを確認する．

(3) O_1 の元のみ動かす H の元 h を次のようにして作る:

(a) 2 から m までをランダムに並べたものを $i_1, i_2, \ldots, i_{m-1}$ とする．

(b) $\sigma := \tau_1\tau_{i_1}\tau_1\tau_{i_2}\cdots\tau_1\tau_{i_{m-1}}K$ とおく．

(c) σ^l が O_1 の元のみ動かすような最小の正整数 l を求め，h を σ^l とする．

(4) 上の方法でいくつかの h を作り，これらが生成する群が n 次交代群となることを確認する．

4 3 頂点グラフ

本節では，3 頂点グラフで例外的に群が射影群となる系列を紹介する．はじめにこの系列を見つけた実験を紹介する．

4.1 $\mathbb{F}_p$ における実験結果

100 以下の奇素数 p に対して，$\mathbb{F}_p$ 上で 3 頂点の全てのグラフについて mutation が生成する群を GAP を用いて計算した．その際，$|\cdot| : \mathbb{F}_p \to \mathbb{F}_p$ は次とした:

$$|a| := \begin{cases} a & (a \in \{1, 2, \cdots, \frac{p-1}{2}\}), \\ -a & (\text{otherwise}). \end{cases}$$

その結果，ほとんど全ての場合で交代群か対称群 (あるいはこれらに 2 群や 3 群がついた群) となった．
しかし，次の 2 つの場合のみ例外的に $PGL(2,7)$ となった:

- $p = 43$, $\Gamma = (2, 19, 19)$,
- $p = 97$, $\Gamma = (2, 30, 30)$.

ここで (a,b,c) は次を表す:

$$(a,b,c) := \begin{bmatrix} 0 & a & -c \\ -a & 0 & b \\ c & -b & 0 \end{bmatrix}$$

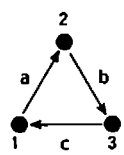


図 4 (a,b,c) の有向グラフによる表現

[*2] GAP 内部では Jordan による「次数 n の原始群がある素数 $p < n-2$ に対して p-cycle を持てば，n 次の対称群または交代群」という結果を応用している．

4.2 mutation 不変量

$\Gamma=(a,b,c)$ に対して, $a,b,c\geq 0$ または $a,b,c\leq 0$ のとき, Γ を cycle と呼び, そうでないとき acycle と呼ぶことにする. 3 頂点の場合, mutation で不変な量が存在する.

定義 4.1. $\Gamma=(a,b,c)$ に対して, $n:=\#\{x\in\{a,b,c\}\mid x\leq 0\}$ とし, m_Γ を次で定義する:

$$m_\Gamma:=\begin{cases} a^2+b^2+c^2-abc & (n=0,1),\\ a^2+b^2+c^2+abc & (n=2,3)\end{cases}$$
$$=\begin{cases} a^2+b^2+c^2-|a||b||c| & (\Gamma\text{は cycle}),\\ a^2+b^2+c^2+|a||b||c| & (\Gamma\text{は acycle}).\end{cases}$$

定理 4.2. m_Γ は mutation で不変.

講演後 Beineke, Brüstle, Hille らが m_Γ の形を簡単にした $C(a,b,c):=a^2+b^2+c^2-abc$ を用いて, 3 頂点グラフにおける mutation 同値類を研究していたことを知った. $C(a,b,c)$ は Markov equation と呼ばれるもので, mutation では不変ではない. しかし, mutation の定義を少し変形すると, グラフが cycle の間は不変になる. この事実を用いて彼らは 3 頂点グラフが acycle と mutation 同値となる必要十分条件を決定した [1].

4.3 $PGL(2,p), PSL(2,p)$

p を奇素数, 体 K は $\alpha^p=1$ なる元 $\alpha\neq 1$ を含むとする. $a_i:=\alpha^i+\alpha^{-i}$, $\Gamma:=(a_0,a_1,a_1)$ とする. さらに $a_i>0$ となるように, 写像 $|\cdot|:K\to K$ を取る.

このとき, m_Γ を考えることで次の補題を得る.

補題 4.3. (1) $(a_i,a_{i\pm j},a_j)^{r_1}=-(a_i,a_{i\mp j},a_j)$,
$(a_i,a_j,a_{i\pm j})^{r_2}=-(a_i,a_j,a_{i\mp j})$,
$(a_{i\pm j},a_i,a_j)^{r_3}=-(a_{i\mp j},a_i,a_j)$.

(2) $O_\Gamma=\{\pm(a_i,a_j,a_{i\pm j})\mid i,j\in\{0,1,\ldots,\frac{p-1}{2}\}\}\setminus\{\pm(a_0,a_0,a_0)\}$, 特に $|O_\Gamma|=p^2-1$.

(3) 任意の $(a_i,a_j,a_h)\in O_\Gamma$ に対して, $\{\pm(a_{ni},a_{nj},a_{nh})\mid n\in\{1,2,\ldots,\frac{p-1}{2}\}\}$ は G_Γ のサイズ $p-1$ の非原始ブロック.

補題の非原始ブロックからなるブロック系への作用の核で G_Γ を割った群を $\bar{G}_\Gamma$ と表すと, $\bar{G}_\Gamma$ は次になる.

定理 4.4.

$$\bar{G}_\Gamma\cong\begin{cases} PSL(2,p) & (p=1 \pmod 4),\\ PGL(2,p) & (p=3 \pmod 4).\end{cases}$$

5 今後の課題

今後, 上の PGL, PSL 以外の例外的な群や頂点数が 4 以上の場合の不変量の探索, 頂点数が 4 の倍数のときに 2 つの交代群が現れることの理由やクラスター代数との関係を解明したい.

講演後 $\mathbb{F}_2$ 上の場合, すなわち無向グラフの場合, mutation は local complementation と呼ばれる操作に等しいことを東北大の宗政先生が教えてくださった. この場合, 各グラフには graph code という $\mathbb{F}_4$ 上の

self-dual additive code を対応させることができる (逆に, $\mathbb{F}_4$ 上の self-dual additive code はある graph code と同値である). ここで, 2 つの $\mathbb{F}_4$ 上の self-dual additive codes が同値である必要十分条件は, 対応するグラフが mutation 同値[*3] であることを Bouchet は示した [2]. さらに, Danielsen と Parker はこの事実を用いて, 長さ 12 以下の $\mathbb{F}_4$ 上の self-dual additive codes の分類を行った [4]. 今後, この方向からの研究も考えていきたい.

謝辞

今回の講演にあたって旅費を援助してくださった, 大分大の末竹先生に感謝いたします.

本研究は第 22 回有限群論草津セミナーで筑波大の宮本先生がお話されたことが出発点となっており, きっかけを与えてくださったことに感謝しております.

参考文献

[1] A. Beineke, T. Brüstle, and L. Hille. Cluster-cyclic quivers with three vertices and the markov equation. *Algebras and Representation Theory*, 14:97–112, 2011. 10.1007/s10468-009-9179-9.

[2] A. Bouchet. Graphic presentations of isotropic systems. *J. Comb. Theory, Ser. B*, 45(1):58–76, 1988.

[3] A. B. Buan and I. Reiten. Acyclic quivers of finite mutation type. *International Mathematics Research Notices*, 2006.

[4] L. E. Danielse and M. G. Parker. On the classification of all self-dual additive codes over gf(4) of length up to 12. *J. Comb. Theory Ser. A*, 113:1351–1367, October 2006.

[5] A. Felikson, M. Shapiro, and P. Tumarkin. Skew-symmetric cluster algebras of finite mutation type. *ArXiv e-prints*, November 2008.

[6] S. Fomin and A. Zelevinsky. Cluster algebras I: Foundations. *J. Amer. Math. Soc.*, 15:497–529, 2002.

[*3] 正確には, 片方のグラフを mutation で移すともう片方のグラフと同型になることが必要十分条件.

有限群上のランダムウォークと離散統計学への応用
Random walks on finite groups and applications to discrete statistics

吉田知行 (Tomoyuki YOSHIDA 北大・理)

2011/06/21 Oita 大分

1 はじめに

1.1 代数統計ことはじめ

今世紀に入り,「代数統計」あるいは「計算代数統計」という統計学の分野が勃興してきた．これは，統計学への群論や環論，代数幾何の応用と言える．さらに代数統計は，何よりも実用を目指した統計学である．したがって抽象代数学の威力を発揮する場にもなっている．

これまでにも多変量解析への線形代数や線形群の応用があった．代数統計はそれと異なり，コンピュータとネットワークの時代の統計学である．ブートストラップ法を初めとするリサンプリング法，マルコフ連鎖モンテカルロ (MCMC) 法，ベイズ統計といった分野と密接に関係している．

代数統計が大きく発展するきっかけになったのが，グレブナー基底による分割表の列挙と分割表検定への実用化が両期となった．これについては，

日比『グレブナー基底の現在』([日比 06])
第 3 章 統計学におけるグレブナー基底 (竹村彰通，青木敏)
第 4 章 高次元配列データ解析とグレブナー基底 (坂田年男)

の章に詳しく説明されている．

私にとって代数統計は，比較言語学への有限群論の応用から始まった．統計学の言葉では，正方分割表の一致率検定のための並べ替え検定であった．その p-値 (有意確率，実際の一致数が偶然得られる確率) をいかに正確に求めるかという問題である．偶然の一致数の高次モメント，したがって一致数の分布自体が，対称群で完全に記述できる，というのが当時得られた成果である (1980 ころ『数理科学』)．

現代統計の考え (リサンプリング法) によれば，「偶然の一致数」を何らかの方法で大量に発生させれば，それから p-値の近似値が得られる．比較言語学の方でそのような方法 (シフト検定法) を提案したのが Oswalt である (1971 ころ)．ところが一致数の大量発生の必要さえない．一致数の p-値 (有理数) は，${}_2F_0$ 型の超幾何多項式の計算で正しい値が得られる．

それなら，一般の分割表の場合はどうか．分割表を大量に作り出し，それを使ってもとの分割表に関する統計量の分布を調べる．大量生成の方法を提供し，大量生成された分割表の品質を調べるのには，多項式環の理論，とくにグレブナー基底の理論を使うのが今では標準な方法である．しかし対称群と分割表の関係が分かった今では，分割表のランダムサンプリングよりは置換のランダムサンプリングの方がはるかに易しい．ランダム性の度合いは，対称群の表現論により完全に記述できる．

一方対称群やより一般に群上のランダムウォークの理論として，Diaconis の成果がある．

P.Diaconis, "Group Representatioins in Probability and Statistics," IMS(1988).
T.Ceccherini-Silberstein, etc., "Harmonic Analysis on Finite Groups," Cambridge(2008)

不思議なことに，分割表に関する MCMC 法と対称群上のランダムウォークの理論が結びついていない．Diaconis など両方の分野に精通している有力な研究者がいるにもかかわらずである．

この数年，主に統計関係の研究集会で似たタイトルの講演をしてきた．次のような代数関係の集まりでも話している．

「分割表の一致率検定への有限群論と組合せ論の応用」代数学シンポジウム (2007/8 神戸) 「有限群上のランダムウォークと統計学への応用」第 25 回代数的組合せ論シンポジウム (2008/6/24 於北大)

「有限 Gelfand 対と Markov 連鎖モンテカルロ法」(2009/8/28 於北大) 数研講究録 1689 (2010)

この講演では，これらの発表のあとに得られた成果を加えながら，理論の概要を解説した．

1.2 マルコフ連鎖

マルコフ連鎖 (Markov chain, MC) は三つ組 (X, μ_0, P) からなる．ここで X は状態空間 (state space) とよばれる離散集合．その元を**状態**ということがある．$\mu_0 : X \to [0,1]$ は，**初期分布** (initial distribution) とよばれる X 上の確率分布:

$$0 \le \mu_0(x) \le 1, \quad \sum_{x \in X} \mu_0(x) = 1$$

最後に $P = (p(x,y))_{x,y \in X}$ は，**遷移確率行列** (transition matrix) とよばれる確率行列:

$$0 \le p(x,y) \le 1, \quad \sum_{y \in X} p(x,y) = 1 \ (\forall x \in X)$$

確率過程としては次のように描かれる．まず出発点 x_0 を確率 $\mu_0(x_0)$ に従って選ぶ:$\mathrm{Prob}(x = x_0) = \mu_0(x_0)$．ある x_n まで決まったとき，x_{n+1} を確率 $p(x_n, x_{n+1})$ に従って選ぶ．

$$\mathrm{Prob}(x = x_{n+1} | x_n) = p(x_n, x_{n+1})$$

これによって X の元の列

$$x_0 \to x_1 \to \cdots \to x_n \to x_{n+1} \to \cdots$$

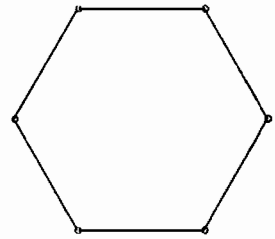
ができる．

行列 P の n-乗を

$$P^n = (p^{(n)}(x,y))$$

としたとき，$p^{(n)}(x,y)$ は，x から n-ステップ後に y に移動する確率を表す．マルコフ連鎖の理論で大事なのは，n-ステップ遷移確率行列 P^n の漸近的挙動である．とくに極限分布 $\lim_{n\to\infty} \mu_0 P^n$ である．ここで初期分布 μ_0 を行ベクトルと見なした．

例． サイクル $Z_m = \mathbb{Z}/m\mathbb{Z} = \{0, 1, \cdots, m-1\}$ 上の RW を考える．点 $x_0 = 0$ から出発し，確率 1/2 で隣り合ったどちらかの点に移動する．



すなわち x から y への推移確率は

$$p(x,y) = \begin{cases} 1/2 & x - y = \pm 1 \\ 0 & \text{else} \end{cases}$$

したがって推移確率行列 $P = (p(x,y))_{x,y \in Z_m}$ は次の形になる．

$$P = \begin{bmatrix} 0 & 1/2 & 0 & 0 & \cdots & 1/2 \\ 1/2 & 0 & 1/2 & 0 & \cdots & 0 \\ 0 & 1/2 & 0 & 1/2 & \cdots & \\ & \ddots & \ddots & \ddots & \ddots & \\ 0 & \ddots & \ddots & \ddots & 0 & 1/2 \\ 1/2 & 0 & & 0 & 1/2 & 0 \end{bmatrix}$$

$P^n = (p^{(n)}(x,y))_{x,y}$ を n-ステップ推移確率行列とする．このとき

$$p^{(n)}(x,y) = \frac{1}{n} \sum_{z \in 0}^{m} \cos^n \left[\frac{2\pi z}{m}\right] \cos\left[\frac{2\pi z(x-y)}{m}\right]$$

離散フーリエ変換により次の定理を得る．

定理． (Diaconis): m が奇数で $n \ge m^2$ ならば，

$$\|P^n - U\|_1 \le 2\exp\left(-\frac{\pi^2 n}{2m^2}\right)$$

これは，P^n が急速に一様分布 U に収束することを意味する．

この例では，$p(x) := p(0,x)$ としたとき $p(x,y) = p(y-x)$ である．また，乗法群 $C_m\langle g\rangle$ の群環の中で $\widehat{P} := \frac{1}{2}(g+g^{-1})$ と置けば，$p^{(n)}(x,y) = p^{(n)}(0,y-x)$ は，$\widehat{P}^n \in \mathbb{C}C_n$ における g^{y-x} の係数である．

1.3 マルコフ連鎖モンテカルロ (MCMC) 法

これは現代統計の中でおそらく最も重要な方法である．統計分野における乱数発生法と言える．乱数を簡単に発生させる最も簡単な方法として，次の漸化式を使う方法がある:

$$x_{n+1} \equiv ax_n + b \pmod N$$

これによって，初期値 x_0 から始めて，0 から $N-1$ の範囲の疑似乱数 $x_0, x_1, x_2, \cdots$ が得られる．

何かの値を求めたいとき，疑似乱数とモンテカルロ法を組み合わせて，近似値を求めることができる．有名なのは円周率の近似値を求めるためのビュホンの針である．また次のような NP 問題に対する近似解を求めることもできる．

例. $G = (V,E)$ を単純グラフとする．G における独立部分集合のサイズの平均値 μ を求めたい．MCMC 法でこの問題を次のようにして解く．空集合から始めて，独立部分集合のランダムな列を順に構成して行く．

$$\emptyset = S_0 \to S_1 \to \cdots \to S_n \to S_{n+1} \to \cdots \to S_N$$

ある独立部分集合 S_n があったとして，S_{n+1} を作る．そのために

1. ある頂点 v をランダムに選ぶ．
2. コインを投げる．
3. コインが表でしかも $E(v) \cap S_n = \emptyset$ であれば $S_{n+1} := S_n \cup \{v\}$ とし，そうでなければ $S_{n+1} := S_n - \{v\}$ とする．
4. 充分な数の独立部分集合が得られたら，$(|S_1| + |S_2| + \cdots + |S_N|)/N$ が μ の近似値である．

方法はできたが問題点がある．

a) この近似値は，$N \to \infty$ のとき μ に収束するか?
b) 収束するならその速さはどの程度か?

2 代数

2.1 単位区間上の線形代数としてのマルコフ連鎖

まずマルコフ連鎖を代数の言葉で書き換えておこう．確率や確率過程の理論は代数やっている人にはなかなか理解しづらい．ここでは，確率や統計の方を代数の言葉で書き表す．こうすれば例えば，有限群上のマルコフ連鎖の理論に有限群の表現論を使うのが楽になる．確率統計の人はかえって理解しづらくなったと考えるかも知れない．

ここでは単位区間を Δ で表す．$\Delta = I = [0,1]$ である．X, Y は有限集合を表す．∇X によって X 上の確率分布の集合を表す:

$$\nabla X := \left\{ \mu : X \to \Delta \,\middle|\, \sum_{x \in X} \mu(x) = 1 \right\}$$

また

$$\Delta X := \left\{ \widehat{\mu} := \sum_{x \in X} \mu(x) x \mid \mu \in \nabla X \right\}$$

をマルコフ空間と呼ぶ．ただしあまり確率論でも標準的な述語ではないようだ．$\mu \leftrightarrow \widehat{\mu}$ によって ∇X と ΔX は一対一に対応している．Dirac 測度 δ_x が頂点 $\widehat{\delta_x} = x \in X \subset \Delta X$ に対応している．∇X も ΔX も単体で，とくに凸多面体である．

マルコフ写像 $\boldsymbol{P} : \Delta X \to \Delta Y$ とはアファイン写像のことである．したがって線分を線分に写す:

$$\boldsymbol{P}(r\boldsymbol{\mu} + (1-r)\boldsymbol{\nu}) = r\boldsymbol{P}(\boldsymbol{\mu}) + (1-r)\boldsymbol{P}(\boldsymbol{\nu})$$

マルコフ写像 $\boldsymbol{P}$ は，頂点の行き先 $\boldsymbol{P}(x), x \in X$ さえ決まれば一意的に決まる．

マルコフ写像 $\boldsymbol{P} : \Delta X \to \Delta Y$ の表現行列を $P = (p(x,y))$ とすると

$$\boldsymbol{P} = \widehat{P} : x \mapsto \sum_{y \in Y} P(x,y) y,$$

$$\widehat{\mu} \mapsto \widehat{\mu P} := \sum_{x,y} \mu(x) P(x,y) y$$

$$\widehat{PQ} = \widehat{Q} \circ \widehat{P}$$

である．

マルコフ空間とマルコフ写像の言葉を使うなら，(有限) マルコフ連鎖とは三つ組

$$(\triangle X, \mu_0, P)$$

ここで $\mu_0 \in \triangle X$ で，$P : \triangle X \to \triangle X$ はマルコフ作用素 (自己マルコフ写像) である．このような三つ組があれば疑似乱数の生成と同様に，初期分布 μ_0 から始めて，P を次々に作用させることによりマルコフ空間 $\triangle X$ の点列

$$\mu_0 \to \mu_1 \to \mu_2 \cdots \to \mu_n \to \cdots$$

が得られる．重要なのは，n ステップ目の点 μ_n が，直前の μ_{n-1} だけで決まること (マルコフ性) $\mu_{n+1} = P(\mu_n)$ である．$\mu_0 = \widehat{\mu_0}$，$P = \widehat{P}$ とすれば，(X, μ_0, P) は普通の意味のマルコフ連鎖である．

マルコフ連鎖 $(\triangle X, \mu_0, P)$ が**既約**であるとは，$P(\triangle A) \subset \triangle A$ を満たす部分集合 $A \subset X$ が $\emptyset$ と X に限ることをいう．推移確率行列 P の言葉では，任意の $x, y \in X$ に対し，ある $n > 0$ が存在して $P^n(x, y) > 0$ となることである．

マルコフ連鎖 $(\triangle X, \mu_0, P)$ が**非周期的**であるとは，推移確率行列の言葉で

$$\gcd\{n > 0 \mid P^n(x, x) > 0\} = 1 \quad (\forall x \in X)$$

であることをいう．既約かつ非周期的マルコフ連鎖を**エルゴード的**という．

定常分布とは $P(\widehat{\pi_0}) = \widehat{\mu}$ を満たす $\pi_0 \in \nabla X$ のことである．

定理． エルゴード的マルコフ連鎖は，初期分布によらず，ただひとつの定常分布に収束する:

$$\lim_{n \to \infty} P^n(\pi_0) = \pi_0$$

いろいろな証明が知られているが，最も簡単なものは非負行列に対する Perron-Frobenius の定理を使うものだろう．マルコフ作用素 $P : \triangle X \to \triangle X$ の考えを使うなら，まず P はコンパクト集合上の縮小写像である．したがって

$$C := \bigcap_{n=1}^{\infty} P^n(\triangle X) \subset \emptyset$$

である．今の場合，C は凸多面体で，P は C の頂点に可移に作用する．既約性と非周期的より C の頂点はひとつだけ．これは P^n が $\triangle X$ 上の定数写像 π_0 に収束することを意味する．

O.Häggström, "Finite Markov Chains ...", London M. Soc., 2002.

2.2 有限群の作用をともなうマルコフ連鎖

G を有限群，X を有限 (ℓ) G-集合，$p \in \nabla G$ とする．このとき

$$\widehat{p} := \sum_{g \in G} p(g) g \in \triangle G$$

は X 上のマルコフ作用素

$$\triangle_X(p) : \triangle X \to \triangle X; \mu \mapsto \mu \widehat{p}$$

を誘導する．

このときマルコフ連鎖 $(\triangle X, \mu_0, \triangle_X(p))$ を (p から誘導された) X 上の**ランダムウォーク** (RW)) という．その遷移確率行列 $P = (P(x, y))$ は

$$P(x, y) = \sum_{g : xg = y} p(g)$$

で与えられる．すなわち，G の元のランダムサンプリング $g_0, g_1, g_2, \cdots$ (生起確率は p) は X 上の RW

$$x_0 \to x_0 g_1 \to x_0 g_1 g_2 \to \cdots$$

を誘導する．

この RW の漸近的挙動は，群環におけるベキ $\widehat{p}^n \in \mathbb{C}G$ $(n = 1, 2, \cdots)$ の性質に大きく影響を受ける．ただしエルゴード的でない $\widehat{p}$ を使うこともある．その場合は X 上の初期分布 μ_0 の影響も受ける．

Diaconis などがやっているように，群環を考えずに G の確率分布のままで計算するのは見通しが悪い．実際，$p, q \in \nabla G$ に対し，

$$\widehat{p} \cdot \widehat{q} = \widehat{(p * q)}$$
$$(p * q)(g) := \frac{1}{|G|} \sum_{h \in G} p(gh^{-1} q(h)$$

なので，たたみ込みベキ $p^{(*n)} = p * p * \cdots * p$ (n 回) の計算が必要になる．それよりは群環の中でのベキ $\widehat{p}^n$ を計算する方がはるかに楽である．

2.3 $\widehat{p}^n$ と $p^{(*n)}$ の計算

p を G 上の複素数値類関数とする:

$$p(a^{-1}ga) = p(g) \quad \forall a, g \in G$$

このとき

$$\widehat{p} = \sum_{g \in G} p(g) g \in Z(\mathbb{C}G)$$

$\mathrm{Irr}(G)$ を，G の既約指標全体とする．このとき，$\widehat{p}$ のスペクトル分解は

$$\widehat{p} = \sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(\widehat{p}) e_\chi,$$

となる．ここで $\chi \in \mathrm{Irr}(G)$ に対し，

$$\omega_\chi : \mathbb{C}G \to \mathbb{C}; g \mapsto \chi(g)/\chi(1)$$

は線形写像で，

$$e_\chi := \frac{\chi(1)}{|G|} \sum_{g \in G} \overline{\chi(g)} g = \frac{\chi(1)}{|G|} \widehat{\overline{\chi}}$$

は $\mathbb{C}G$ の中心原始ベキ等元である．したがって

$$e_\chi e_\theta = \delta_{\chi,\theta} e_\chi, \quad 1 = \sum_\chi e_\chi$$

注意． ω_χ は $Z(\mathbb{C}G)$ 上の多元環準同形写像である．より強く，$a \in \mathbb{C}G, b \in Z(\mathbb{C}G)$ なら $\omega_\chi(ab) = \omega\chi(a)\omega_\chi(b)$ である．また C を G の共役類，$x \in C$，類和 $\widehat{C} := \sum_{c \in C} c$ について

$$\omega_\chi(\widehat{C}) = |C| \frac{\chi(x)}{\chi(1)}$$

は代数的整数である．

スペクトル分解ができれば $\widehat{p}^n$ の計算は容易である．$\widehat{p}^n = (p^{(*n)})\widehat{}$ なので，$p^{(*n)}$ も容易に求められる．実際，$\{e_\chi \mid \chi \in \mathrm{Irr}(G)\}$ が中心 $Z(\mathbb{C}G)$ の直交原始ベキ等元なので，

$$\therefore \widehat{p^{(*m)}} = \widehat{p}^m = \sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(\widehat{p})^m e_\chi$$

$$\therefore p^{(*m)}(g) = \sum_{\chi \in \mathrm{Irr}(G)} \omega_\chi(\widehat{p})^m \frac{\chi(1)}{|G|} \overline{\chi}$$

2.4 $\lim_{n \to \infty} p^{(*n)}$ の収束の評価と極限分布

p を G 上の確率分布で，しかも類関数であるとする．この場合の $p^{(*n)}$ の極限分布について考える．

p の台を

$$S := \mathrm{supp}(p) = \{g \in G \mid p(g) \neq 0\}$$

とする．p が類関数なので S は共役類の和集合である．$S \neq \emptyset$ である．さらに

$$N := \langle S^{-1}S \rangle = \langle s^{-1}t \mid x, t \in S \rangle \lhd G$$

とすれば，N は G の正規部分群である．G 上の確率分布 q を次で定義する:

$$q(g) = \begin{cases} 1/|N| & (g \in Ng_0) \\ 0 & (\mathrm{else}) \end{cases}$$

とくに $N = G$ の場合，q は一様分布 u_G である．

定理． (1) $p^{(*n)}$ が一様分布に収束するための必要十分条件は $N = G$ である (Diaconis).
(2) $p^{(*n)} \approx q^{(*n)} + C\rho^n$．ここで

$$\rho := \max_{\substack{\chi \in \mathrm{Irr}(G) \\ g \in G - \mathrm{Ker}_\chi}} \left| \frac{\chi(g)}{\chi(1)} \right|$$

このことは，

$$\omega_\chi(\widehat{p}) = \sum_{g \in S} p(g)\chi(g)/\chi(1)$$
$$|\omega_\chi(\widehat{p})| = 1 \Leftrightarrow N \subset \mathrm{Ker}(\chi).$$

から分かる．

2.5 マルコフ・ヘッケ環

K を有限群 G の部分群，

$$\mathcal{H}(G, K) := e_K \mathbb{C}G e_K \cong \mathrm{End}_{\mathbb{C}G}(e_K \mathbb{C}G)$$

をヘッケ環とする．ここで

$$e_K := (1/|K|) \sum_{k \in K} \in \Delta K$$

はベキ等元．マルコフ・ヘッケ環を

$$\Delta\mathcal{H}(G, K) := e_K \Delta G e_K$$

で定義する．これは凸多面体で，ヘッケ環での積に関して閉じている．

ヘッケ環 $\mathcal{H}(G,K)$ が可換なとき，(G,K) をゲルファント対という．以下 (G,K) はゲルファント対であると仮定する．

X を有限 G-集合とする．$p \in \nabla G$ を両側 K-不変とする．すなわち

$$p(kgk') = p(g) \quad \forall g \in G, k, k' \in K$$

このとき $\widehat{p} = e_K \widehat{p} e_K \in \Delta\mathcal{H}(G,K)$ について，やはりスペクトル分解がある．

$$\widehat{p} = \sum_{\chi \leq 1_K^G} \omega_{K,\chi}(e_K \widehat{p} e_K) e_K e_\chi,$$

ここで，置換指標 1_K^G の既約成分 χ に対し，

$$\omega_{K,\chi}(e_K g e_K) := \frac{\chi(e_K g e_K)}{\chi(e_K)}$$

は線形写像．ゲルファント対の場合，$\omega_{K,\chi}$ は，$\mathcal{H}(G,K)$ 上の多元環準同形を与える．

X を (右) G-集合とすれば，p は K-軌道の集合 X/K 上のマルコフ連鎖を誘導する:

$$\begin{aligned}\Delta_{X/K}(p) : \Delta(X/K) &\to \Delta(X/K) \\ ; xK &\mapsto \sum_{g \in G} p(g) e_K g x K\end{aligned}$$

その遷移確率行列は

$$\nabla_{X/K}(p)(xK, yK) = \sum_{xg \in yK} p(g)$$

である．

結論として

$$\Delta_{X/K}(p)^n = \sum_{\chi \leq 1_K^G} \omega_{K,\chi}(e_K \widehat{p} e_K)^n e_K e_\chi,$$

$S := \mathrm{supp}(p)$, $N := \langle SS^{-1} \rangle$ と置く．$|\omega_{K,\chi}(\widehat{p})| \leq 1$ と，$|\omega_{K,\chi}(\widehat{p})| = 1 \Leftrightarrow N \subset \mathrm{Ker}(\chi)$ である．このことから，N が，X/K に可移に作用していれば，

$$\nabla_{X/K}(p)^{(*n)} \to u_{X/K}$$

である．

2.6 他の分野との関係

有限 G-集合上のランダムウォークに関係する，あるいは関係しそうな分野をいくつかあげておく．

●凸多面体． X 上のマルコフ連鎖は X を頂点集合とする単体 ΔX 上のマルコフ作用素であった．しかしより一般の凸多面体上の凸写像 (アファイン写像) についても，マルコフ連鎖に類似の理論ができる可能性がある．例えば，マルコフ連鎖のエルゴード性は，凸多面体の間の縮小 (凸) 写像が定数関数に収束する条件を与えている．確率論的に意味のある拡張なのかは分からない．

代数的には，単体とマルコフ写像のカテゴリーより，凸多面体と凸写像のカテゴリーの方がはるかに豊かな性質を持っている．後者は Cartesian closed category であって，より集合や加群のカテゴリーに近い．実際，ふたつの凸多面体の間の凸写像全体は，凸多面体である．

●距離正則グラフ． (V,E) を次数 k の正則グラフとする．結合行列 A の固有値で $|\lambda| = k$ を満たすものは $\lambda = k$ だけしかないと仮定する．このとき $P = (1/k)A$ は確率行列で，

$$\lim_{n \to \infty} P^n = (1/|V|) J_V$$

すなわち，P を推移確率行列とするマルコフ連鎖は一様分布に収束する．グラフ理論とマルコフ連鎖の理論のつながりが見えてきた．

砂田利一「分割の幾何学」日本評論社 (2000)
熊谷隆「確率論」共立出版 (2003)

●係数「体」$\triangle$ の変更． これまで考えてきた係数「体」$\triangle[0,1] \subset \mathbb{R}$ の持つ性質を考えるなら，$\triangle$ を，体，環，ブール代数，分配束といったものに置き換えた理論が考えられる．代数で同様の理論を作るなら，p-進整数環 $\mathbb{Z}_p$ がよいかも知れない．

●量子ウォーク． もう一つの $\triangle$ の取り替えとして，$\mathbb{C}^2$ における球体

$$\triangle = \{u \in \mathbb{C}^2 \mid ||u|| \leq 1\}$$

を採用することが考えられる．マルコフ空間に相当するのは

$$\triangle X = \left\{ \sum_{x \in X} \psi(x) x \,\middle|\, \sum_{x \in X} ||\psi(x)||^2 = 1 \right\}$$

ユニタリ行列 $U = (u_{xy})_{x,y\in X}$ に対応する量子マルコフ作用素を

$$\nabla U : \triangle X \to \triangle X; \psi x \mapsto \sum_{y\in X} u_{xy} y$$

で定義する．詳細は次を参照のこと．

今野紀雄「量子ウォークの数理」(産業図書 2008)

3 統計

3.1 データセット

(2 次元) **データセット** (data set, DS) とは写像の対 $[f,g]$ のことである．ここで，$f : N \to \mathcal{L}, g : N \to \mathcal{M}$．$N := \{1,2,\cdots,n\}$ は観測あるいは観測番号の集合．$\mathcal{L}$ と $\mathcal{M}$ は構造のない離散集合である．

注意． 統計と数学では，同じ概念を異なる言葉で呼んだり，場合によっては違う意味で呼ぶことがある．統計では，上に出てきた集合 $\mathcal{L}$ と $\mathcal{M}$ を「変数」(あるいは「変量」「属性」など) と呼ぶ．どちらも構造を持たないので，「カテゴリカル変数」である．また，「確率変数」という用語も良く出てくるが，これは確率空間から別の集合への単なる写像であると考えた方が分かりやすい．ここではややこしくなるので，このような統計用語はあまり使わない．

より一般に，d-次元のデータセットも考えられる．2 次元データセット $[f,g]$ は，1 次元データセット $[\langle f,g\rangle : N \to \mathcal{L}\times\mathcal{M}]$ と考えられる．

2 次元データセット $[f,g]$．ここで $f : N \to \mathcal{L}, g : N \to \mathcal{M}$ を考える．$\mathcal{L}\times\mathcal{M}$-型配列

$$X[f,g] := \left(|f^{-1}(\lambda)\cap g^{-1}(\mu)|\right)_{\lambda\in\mathcal{L},\mu\in\mathcal{M}}$$

を**分割表** (contingency table) という．

1 次元データセット $[f]$ と $[g]$ を $[f,g]$ の**周辺データセット**という．

$$X[f] := \left(|f^{-1}(\lambda)|\right)_{\lambda\in\mathcal{L}}$$
$$X[g] := \left(|g^{-1}(\mu)|\right)_{\mu\in\mathcal{M}}$$

は $[f]$ と $[g]$ の**度数分布表** (frequency table) である．それらを分割表 $X[f,g]$ の**周辺分布** (mariginal distribution) という．

以下しばらく，$N = \{1,2,\cdots,n\}$, $\mathcal{L},\mathcal{M}$ を固定しておく．非負整数ベクトル $\boldsymbol{a} = (a_\lambda)_{\lambda\in\mathcal{L}}$，$\boldsymbol{b} = (b_\mu)_{\mu\in\mathcal{M}}$ で，条件

$$\sum a_\lambda = n, \sum b_\mu = n$$

を満たすものを取る．

$$\mathsf{DS}(\boldsymbol{a},\boldsymbol{b}) := \{[f,g] \mid X[f] = \boldsymbol{a}, X[g] = \boldsymbol{b}\}$$
$$\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b}) := \{(x_{\lambda,\mu}) \mid x_{\lambda,+} = a_\lambda, x_{+,\mu} = b_\mu\}$$

とする．ここで，$x_{\lambda,\mu}$ は非負整数である．$\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})$ は，周辺分布が $\boldsymbol{a},\boldsymbol{b}$ であるようなデータセットの集合であり，$\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ は，周辺分布が $\boldsymbol{a},\boldsymbol{b}$ であるような $\mathcal{L}\times\mathcal{M}$-型配列の集合である．ただし，

$$x_{\lambda,+} := \sum_\mu x_{\lambda,\mu}, x_{+,\mu} = \sum_\lambda x_{\lambda,\mu}$$

とした．

分割表を対応させる写像がある:

$$X : \mathsf{DS}(\boldsymbol{a},\boldsymbol{b}) \to \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$$

定理． (1) $S_n \times S_n$ は，次の作用で $\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})$ に可移に作用する:

$$([f,g],(\sigma,\tau)) \mapsto [f\sigma, g\tau]$$

(2) 任意の $\boldsymbol{x} \in \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ の逆像 $X^{-1}(\boldsymbol{x})$ は，${S_n}^\Delta$-軌道になっている．ここで ${S_n}^\Delta$ は $S_m \times S_n$ の対角部分群．とくに X は全射で次のように分解する:

$$X : \mathsf{DS}(\boldsymbol{a},\boldsymbol{b}) \longrightarrow \mathsf{DS}(\boldsymbol{a},\boldsymbol{b})/DS_n \cong \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$$

(3) 固定した $[f,g]$ に対し，写像

$$\alpha : S_n \to \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b}); \sigma \mapsto X[f\sigma, g]$$

は $(S_n, U) \to (\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b}), \mathrm{MHGD})$ を与える．ここで U は S_n の一様分布，MHGD は超幾何分布である．すなわち $X = (x_{\lambda,\mu}) \in \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ に対し，

$$\frac{1}{n!}|\alpha^{-1}(X)| = \mathrm{MHGD}(X) = \frac{\boldsymbol{a}!\boldsymbol{b}!}{n!\boldsymbol{x}!}$$

ここで

$$\boldsymbol{a}! := \prod_\lambda a_\lambda!,\ \boldsymbol{x}! := \prod_{\lambda,\mu} x_{\lambda,\mu}!$$

この定理の証明はそう難しいものではないが，**抽象バーンサイド環の理論が役に立つ.**

T.Yoshida, On the Burnside rings of finite groups and finite categories, "Commutative algebra and combinatorics (Kyoto, 1985), ASPM11, North-Holland, 1987

データセットをスライスカテゴリー $\mathrm{set}/\mathcal{L}, \mathrm{set}/\mathcal{L}\times\mathcal{M}$ などの対象と考える．データセット同士の同型をこのカテゴリーでの同型で定義する．例えばデータセット $[f],[f'] \in \mathrm{DS}(\boldsymbol{a})$, $[f,g],[f',g'] \in \mathrm{DS}(\boldsymbol{a},\boldsymbol{b})$ に対し，

$$[f] \cong [f'] \Leftrightarrow \exists\sigma \in S_n; f = f'\circ\sigma$$
$$[f,g] \cong [f',g'] \Leftrightarrow \exists\pi \in S_n; f = f'\circ\pi, g = g'\circ\pi$$

このとき抽象バーンサイド環の理論により，次の同型判定がある．

補題. 上のデータセット $[f],[f'],[f,g],[f',g']$ に対し

(1) $[f] \cong [f'] \Leftrightarrow X[f] = X[g]$

(2) $[f,g] \cong [f',g'] \Leftrightarrow X[f,g] = X[f',g']$

離散統計の重要な応用として分割表の検定がある．古くはカイ二乗検定などがあったが，現在では分割表の大量サンプリングによるモンテカルロ法が主流である．定理の (3) は，多項超幾何分布にもとづく分割表のランダムサンプリングが，対称群の元のランダムサンプリング (一様分布にもとづく) から得られることを意味する．分割表のランダムサンプリングよりは置換のサンプリングの方が遙かに容易であり，理論的にも扱いやすい．

3.2 ランダムな互換

対称群上のマルコフ連鎖で一様分布に収束するものがあれば，上の定理により多項超幾何分布に収束する分割表上のマルコフ連鎖ができる．

最も簡単なのは，互換をランダムに取り $\tau_1,\tau_2,\cdots$ をれを順次乗じて置換の列を作ることである:

$$1, \tau_1, \tau_1\tau_2, \cdots, \tau_1\cdots\tau_n, \cdots$$

この連鎖は周期的ではないが，分割表の連鎖に飛ばして得られる

$$X[f,g], X[f,g\tau_1], X[f,g\tau_1\tau_2], \cdots$$

の分布は，統計的にあり得ない例外を除けば，多項超幾何分布に収束する．

非負整数ベクトル $\boldsymbol{a},\boldsymbol{b}$ のすべての成分が 1 以下，ということはないと仮定する．以下，考えるデータセットはすべて $\mathrm{DS}(\boldsymbol{a},\boldsymbol{b})$ に属するものとする．$G = S_n$ とし，C を G の互換全体のなす共役類とする．このとき $[f,g] \mapsto [f\sigma,g]$ $(\sigma \in C)$ は，$\mathrm{DS}(\boldsymbol{a},\boldsymbol{b})$ 上のランダムウォークを誘導する．その極限分布は多項超幾何分布 MHGD である．

互換 $\tau = (i,j) \in C, f(i) = \lambda, g(j) = \mu$ を取ると

$$X[f\tau,g] = X[f,g] + \begin{array}{c|cc} & \mu & \mu' \\ \hline \lambda & +1 & -1 \\ \lambda' & -1 & +1 \end{array}$$

である．これは，分割表の集合上の有名なマルコフ連鎖である．右辺に出てくる 4 つの成分だけが ±1 で他の成分がゼロであるような行列 $B_{\lambda,\lambda',\mu,\mu'}$ をマルコフ基底という．

日比「グレブナー基底の現在」数学書房 (2006)

の第 3 章 (竹村・青木) と第 4 章 (坂田) 参照．対称群上のマルコフ連鎖の理論を使うと，このマルコフ連鎖の収束について次が言える:

定理. 上のマルコフ連鎖の収束率 ρ を

$$\|P^m - MHGD\|_2^2 \le C\rho^m$$

で定義すると，

$$\rho = \mathrm{Max}_\chi\left\{\left|\frac{\chi(\tau)}{\chi(1)}\right| : \chi < 1_{S_f}^{S_n}, \chi < 1_{S_g}^{S_n}\right\} \le \frac{n-3}{n-1}$$

既約指標 χ の型を $1^{m_1}2^{m_2}\cdots$，その共役を $1^{m'_1}2^{m'_2}\cdots$ とすれば，

$$\frac{\chi(\tau)}{\chi(1)} = \frac{1}{n(n-1)}\sum_i i^2(m_i - m'_i)$$

である (フロベニウス)．$\rho \le 1 - 2/(n-1)$ なので，ρ は 1 に近い．このことからこのマルコフ連鎖の収束は悪いと見込まれる．しかし，最初の分割表に 4 以下の成分がないなどの条件があれば，収束は良くなると思われるが，厳密な評価は今後の課題である．

3.3 平方分割表のトレースと一致率検定

$\mathcal{L} = \mathcal{M}$ であるようなデータセット $[f, g : N \to \mathcal{L}]$ とその分割表 $X[f,g] = (|f^{-1}(\lambda) \cap g^{-1}(\mu)|)$ を考える．周辺分布を $\boldsymbol{a} = (a_\lambda) = (|f^{-1}(\lambda)|) = X[f]$, $\boldsymbol{b} = (b_\lambda) = (|g^{-1}(\mu)|) = X[g]$ とする．このとき**一致数** (coincidence number) を

$$x_0[f,g] := \mathrm{Tr}(X) = \sharp\{i \in N \mid f(i) = g(i)\}$$

で定義する．

一般に 1 次元データセット $[f]$ と $[g]$ が近ければ，一致数 $x_0[f,g]$ は n に近いであろう．とくにちょうど n なら，$[f] = [g]$ である．$n - x_0[f,g]$ は Hamming 距離である．

G を N に作用する有限群とし，各 $\pi \in G$ に対し，

$$x_0(\pi) := x_0[f\pi, g]$$

と置く．$\pi \in G$ を勝手に取ったとき，$[f\pi]$ はデータ $f(1), f(2), \cdots, f(n)$ を勝手にかき混ぜたデータである．したがってそれと $[g]$ との一致数は偶然の一致数と考えられる．このようにデータを置換によってかき混ぜて検定することを**並べ替え検定** (permutation test) という．これはデータの分布型を仮定しないのでノンパラメトリック法のひとつである．計算機の高速化とともに急速に研究・応用が発展してきた．

定理 (平均値公式). G が N に可移に作用していると仮定する．このとき $\{x_0(\pi) \mid \pi \in G\}$ の平均値について次が成り立つ:

$$\boldsymbol{E}_{\pi \in G}[x_0(\pi)] = \frac{1}{n} \sum_\lambda a_\lambda b_\lambda (=: m)$$

(証明)

$$\sharp := \sharp\{(\pi, i) \in G \times N \mid f(i) = g(\pi i)\}$$

を二通りの方法で数える．まずこの値は

$$\sum_{\pi \in G} x_0[f, g\pi] = |G| \boldsymbol{E}_{\pi \in G}[x_0(\pi)]$$

に等しい．一方

$$\begin{aligned}
\sharp &= \sharp\{(\pi, i, j) \in G \times N \mid f(i) = g(j), j = \pi i\} \\
&= (|G|/n)\sharp\{(i,j) \in G \times N \mid f(i) = g(j)\} \\
&= (|G|/n) \sum_{\lambda \in \mathcal{L}} \sharp\{(i,j) \in G \times N \mid f(i) = g(j) = \lambda\} \\
&= (|G|/n) \sum_{\lambda \in \mathcal{L}} |f^{-1}(\lambda) \times g^{-1}(\lambda)| \\
&= (|G|/n) \sum_{\lambda \in \mathcal{L}} a_\lambda b_\lambda
\end{aligned}$$

両辺を比べて平均値公式を得る．

定理 (モメント公式). G が N に t-重可移に作用していると仮定する．このとき $\{x_0(\pi) \mid \pi \in G\}$ の組み合わせモメントについて次が成り立つ:

$$\boldsymbol{E}_\pi \left[\binom{x_0(\pi)}{t} \right] = \frac{(n-t)!}{n!} \sum_{\sum t_\lambda = t} \prod_\lambda \binom{a_\lambda}{t_\lambda} \binom{b_\lambda}{t_\lambda} t_\lambda!$$

(証明) G は $N^{(t)}$ (相異なる t-元集合) の上に可移に作用する．結果は平均値公式から得られる．

系. G が対称群 S_n の場合，一致数 $x_0[f,g]$, ただし $[f,g] \in \mathsf{DS}(\boldsymbol{a}, \boldsymbol{b})$ の分布は，周辺分布 $\boldsymbol{a}, \boldsymbol{b}$ によって一意的に決まる．

3.4 正確な p-値

正方分割表で考える．$\boldsymbol{a} = (a_\lambda), \boldsymbol{b} = (b_\lambda)$ とする．一致数 $x_0 = x_0[f_0, g_0]$ ($[f_0, g_0] \in \mathsf{DS}(\boldsymbol{a}, \boldsymbol{b})$) の検定，すなわち x_0 が偶然得られる確率を知りたい．そのための方法として，Cohen のカッパ検定が知られている．ここでは正確な有意確率 (p-値) を

$$P(x_0) := \frac{\sharp\{[f,g] \in \mathsf{DS}(\boldsymbol{a}, \boldsymbol{b}) \mid x_0[f,g] \geq x_0\}}{|\mathsf{DS}(\boldsymbol{a}, \boldsymbol{b})|}$$

で定義する．正確な p-値を何らかの方法で求める検定法は，Fisher の正確確率法と呼ばれる．

$$P(x_0) = \frac{1}{n!}\sharp\{\pi \in S_n \mid x_0(\pi) \geq x_0\}$$

ここで

$$x_0(\pi) := x_0[f, g\pi]$$

まず，次の多項式を定義する:

$$F_{a,b}(z) = {}_2F_0(-a, -b; z) = \sum_{k \geq 0} \binom{a}{k} \binom{b}{k} k!\, z^k$$

$$F(z) := \prod_\lambda F_{a_\lambda, b_\lambda}(z) = \sum_{k \geq 0} \binom{n}{k} k! q(k)\, z^k$$

a, b が非負整数なので，$F_{a,b}(z)$ は多項式である．

定理. $q(0) = 1, q(1) = n$ と置く．このとき

$$\sum_{k\geq 1} P(k)\, z^{k-1} = \sum_{k\geq 1} q(k)\,(z-1)^{k-1}$$

すなわち多項式計算で p-値 $P(r)$, $r = 0, 1, 2, \cdots, n$ が求まる．

例. 基礎 200 語で上古日本語と中期朝鮮語の語頭音の一致数を求める．ある規準によれば，一致数 $x_0 = 53$ である．この一致数が偶然得られる確率 $P(x_0 \geq 53)$ (p-値であった) をいろいろな方法について比べてみる．

(a) 0.00238. ポリヤの二項検定．二項分布．
(b) 0.00156169. 正確確率法．多項超幾何の和．
(c) 0.000554. コーエンのカッパ検定．正規分布．

分布名は，それぞれの方法で想定した一致数の分布である．二項検定は p-値が大きい．すなわち検出力に劣る．安全だが，関係を見落とす可能性がある．カッパ検定は検出力があるが，逆に言えば関係のない言語を関係ありと誤って判断する可能性がある．計算の手間がかかるが正確確率法は，一番信頼性がある．どの方法を使っても日本語と朝鮮語に関係があるのと判断に違いはない．

正確確率法の場合，誤差のない p-値を計算できる．今の場合，正確な p-値は次の分数で与えられる．分母は 120 桁である．

710729 5597652737 0489065992 0483635346
9525868318 0916330016 9726237291 6284217027
2509552467 3709043666 5097707182 3270606663
6218087567 3110146023 4413202960 8028882983
7045484170 7272110637 5207655256 5847222890
4396826948 2790028836 8064738734 5546300000

一致数の検定にリサンプリング法を始めて使ったのはオズワルト (1972) である．次いで安本美典が日本語の起源問題に使った (1978)．そこでは G として巡回置換 $(1, 2, \cdots, n)$ で生成される群を使っている．そのため，単語の並べ方によって標準偏差が変化する．また語順を，英語のアルファベット順に並べたため，英語に近い言語 (インドヨーロッパ語族) で，偶然の一致数 (背景点) の分布が正規分布からややゆがんだ形になる．安本は二項検定法も使っている．これだと単語の並べ方の問題は生じない．

3.5 カイ二乗検定

分割表の検定で最も使われるのはカイ二乗独立政権邸であろう．$\mathcal{L} \times \mathcal{M}$-型分割表 $\boldsymbol{x} = (x_{\lambda,\mu}) \in \mathsf{TAB}(\boldsymbol{a}, \boldsymbol{b})$ のカイ二乗統計量 とは

$$\chi^2(\boldsymbol{x}) = \sum_{\lambda,\mu} \frac{(x_{\lambda\mu} - a_\lambda b_\mu/n)^2}{a_\lambda b_\mu}$$

のことである．この場合は正確な p-値

$$P(x_0) := \frac{\sharp\{[f,g] \in \mathsf{DS}(\boldsymbol{a},\boldsymbol{b}) \mid \chi^2(X[f,g]) \geq x_0\}}{|\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})|} = \frac{1}{n!}\sharp\{\pi \in S_n \mid \chi^2(X[f_0, g_0\pi]) \geq x_0\}$$

$([f_0, g_0] \in \mathsf{DS}(\boldsymbol{a}, \boldsymbol{b}))$ を求めるのは不可能であろう．一致率の場合，その線形性がものを言った．ただし，$P(x_0)$ の最小値を与える (すなわち $\chi^2(X[f,g])$) が最大になる) データセット $[f, g]$ は特徴的な 2 部グラフの構造を持つ．

したがって正確な p-値が求められないカイ二乗検定の場合は，マルコフ連鎖によるランダムサンプリングで分割表を大量に生成し，そのうちで $\chi^2(\boldsymbol{x}) \geq x_0$ となるものの割合を p-値の近似値とする．対称群上の互換のランダムサンプリングから近似値を求めるのがグレブナー基底に基づく通常の MCMC 法である．しかしこれは収束性が悪い．互換のかわりに，長さ n とか長さ $(n-1)$ の巡回置換を使う方が収束はきわめて速い．残念ながら，そのような巡回置換のランダムサンプリングの方法が問題になるし，収束の評価んも完全にはできていない．これらは今後の課題であろう．

3.6 高次分割表

高次元データセットや高次元分割表の定義は 2 次元の場合と同様である．例として 3 次元の場合を考える．3 次元データセットとは，写像の三つ組 $[f : N \to \mathcal{L}, g : N \to \mathcal{M}, h : N \to \mathcal{N}]$ のことである．$[f], [g], [h]$ を 1 次元の周辺分布，$[f, g], [g, h], [f, h]$ を 2 次元の周辺分布という．$[f, g, h]$ の **3 次元分割**

表とは，3 次元配列

$$X[f,g,h] := (|f^{-1}(\lambda)|, |g^{-1}(\mu)|, |h^{-1}(\nu)|)_{\lambda,\mu,\nu}$$

のことである．

$\mathsf{DS}^{(1)}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$ を 1 次元周辺分布 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$ を持つ 3 次元データセットの集合とする．同様に $\mathsf{DS}^{(2)}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})$ を 2 次元周辺分布 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}$ を持つ 3 次元データセットの集合とする．

$\mathsf{DS}^{(2)}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})$ あるいは，$\mathsf{TAB}^{(2)}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})$ 上の MCMC 法の構成は難しい．これは離散統計学の大問題で，統計ではある程度方法が開発されている (竹村など)．対称群の言葉では，

$$S_f\backslash(S_fS_g\cap S_fS_h) \cong (S_f\cap S_g)\backslash(S_g\cap S_fS_h)$$

上のランダムウォークと同じである．ここで

$$S_f := \{\pi\in S_n \mid f\pi = f\}$$

はヤング部分群である．$S_g\cap S_fS_h$ からのランダムサンプリングが難しい．そもそもヤング部分群 S_g の要素が S_hS_h に入るかどうやって判定するのだろうか．

$\mathsf{DS}^{(1)}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$ あるいは，$\mathsf{TAB}^{(1)}(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$ の場合は，2 次元の場合とそれほど変わらない．この場合，$S_n\times S_n$ からのランダムサンプリングから分割表のランダムサンプリングができる．そのほか，一致数の正確な p-値を ${}_3F_0$ 型超幾何多項式を用いて計算できる．

高次元の分割表のランダムサンプリングの方法について，今は少し研究が停滞しているように感じる．有限群論がどこまでこの問題に切り込めるかに興味がある．

3.7 ブートストラップ法

現代統計学を特徴付ける方法のひとつがブートスラップ法である．

例として，データセット $[f,g]$ ($f: N\to\mathcal{L}, g: N\to\mathcal{M}$) から得られる分割表の一致数 $x_0[f,g]$ の検定にブートストラップ法を使ってみる．

$N=\{1,2,\ldots,n\}$ 上の重複順列の集合を T_n とする．すなわち T_n は N から N への写像の全体である．T_n を対称半群と言うこともある．並べ替え検定の場合と同様に，偶然による一致数を求めたい．そのために，$\sigma,\tau\in T_n$ をランダムに選び $x_0[f\sigma,g\tau]$ を偶然による一致数と見なす．

これはすなわち，新たに n 対の観測データ

$$(f(\sigma(1)),g(\tau(1))),\cdots(f(\sigma(n)),g(\tau(n)))$$

を作り，それから一致数

$$x_0[f\sigma,g\tau] = \sharp\{i\in N \mid f\sigma(i)=g\tau(i)\}$$

を求める．σ,τ をランダムにたくさん取れば，大量の一致数が得られる．

この場合の正確な p-値は

$$P(x_0) = \frac{1}{n^{2n}}\sharp\{(\sigma,\tau)\in T_n\times T_n, x_0[f_0\sigma,g_0\tau]\geq x_0\}$$

である．ここで，$[f_0,g_0]$ は最初に与えられたデータセットで，$x_0 = x_0[f,g]$．ブートストラップ法の場合，周辺分布 $X[f],X[g]$ は変化することに注意しておく．実は，一致数 $x_0[f\sigma,g\tau]$ ($\sigma,\tau\in T_n$) の分布は二項分布 $B(n,p)$ である．ここで

$$p = \frac{1}{n^2}\sum_{\lambda} a_\lambda b_\lambda$$

ブートストラップ法は，並べ替え検定に比べると，割と単純である．そのため，統計学的には順列をランダムにとる方法とか，$p\in\nabla T_n$ から誘導されるデータセット上のランダムウォーク

$$\widehat{p}: \Delta\mathsf{DS}(N;\mathcal{L}\times\mathcal{M}) \to \Delta\mathsf{DS}(N;\mathcal{L}\times\mathcal{M}); [f,g]\mapsto[f,g]\widehat{p}$$

の収束性や収束の速さについて考える必要はあまりなさそうである．

理論的には，次の問題が考えられる．

(a) T_n の生成元．対称群の場合は，互換が理論的にも実用的にもよい生成元の集合であった．対称半群ではそのような生成元の集合はあるのだろうか．

(b) 対称群の場合と同様に，対称半群の理論をブートストラップ法の研究に使えないか．例えば，対称半群の複素既約表現は対称群の既約表現から来ている．

$$\mathbb{C}T_n/J(\mathbb{C}T_n) \cong \bigoplus_{k=0}^{n}\mathbb{C}S_k$$

そうなると，ブートストラップ法によるデータセットのサンプリングは，根基から来るベキ零部分，収束する部分，振動する部分に分解できることになる．それなら，根基 $J(\mathbb{C}T_n)$ のベキ零指数 e はどうなっているのだろう．この部分が並べ替え検定と違う部分である．

4 系統樹

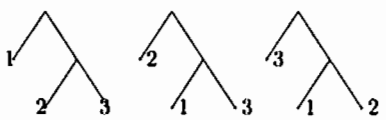
4.1 系統樹と完全マッチング

すでに枚数を超過しているので，簡単に触れる．分割表のサンプリングに出てきたゲルファント対は $(S_n \times S_n, S_n{}^{\Delta})$ であった．その表現は結局対称群 S_n の表現と変わらない．

それなら他のゲルファント対はどうであろう．有名な所では $(S_{2m}, C_2^m \cdot S_m)$ がある．これに関連する統計は，系統樹である．**系統樹** (phylogenetic tree) とは，葉にラベルが付いている根付き二分木である．葉の個数が n であるような系統樹の集合を $\mathcal{T}_n$ とする．このとき $\mathcal{T}_{n+1}$ と $2n$-点集合の完全マッチングは一対一に対応ししている (Diaconis など)．したがって

$$|\mathcal{T}_{n+1}| = (2n-1)!! = \frac{(2n)!}{2^n n!} = |S_{2n}/C_2^n \cdot S_n|$$

Diaconis, Holmes, Random walks on trees and matichings, J.Probabi.7(2002)



4.2 系統樹上のランダムウォーク

現代の系統分類学では，いろいろな生物の DNA データから，生物の系統樹を作る．多数の生物の系統樹を作るための現代的な方法は，トポロジーの違う系統樹を大量に発生させ，それらの系統樹が実際の DNA データに合っているかの適合度 (例えばブートストラップ確率) を計算する．系統樹の中から最も適合度の高い系統樹を採用する．

分割表の場合と同様，系統樹を作るには S_{2n} の元をたくさん作ればよい．最も簡単なのは，ランダムに互換を作りそれから対応する系統樹を作ることである．そこでヘッケ環 $\mathcal{H}(G,K)$ を考える．ここで $G = S_{2n}, K = C_2^n \cdot S_n$．中心原始ベキ等元は $e_K e_{2\lambda}$ の形をしている．ここで $e_K = |K|^{-1}\sum_{k\in K} k$ で，$e_{2\lambda}$ は $2n$ の分割 2λ (λ は n の分割) に付随するは $\mathbb{C}S_{2n}$ の中心原始ベキ等元．

定理. $p \in \nabla S_{2n}$ を

$$p(\pi) = \begin{cases} 1/\binom{n}{2} & \pi \text{ が互換のとき} \\ 0 & \text{それ以外} \end{cases}$$

とする．このとき $\hat{p}$ が誘導する $\mathcal{T}_{n+1}$ 上のランダムウォークは一様分布に収束する．収束率は

$$\rho = \max_{\lambda} |\omega_{K,\lambda 2\lambda}(\hat{p})| = \frac{2n-4}{2n}$$

である．

分子系統学において，組み合わせ論的方法が散見する．参考書を上げておく．

・Z.Yang「分子系統学への統計的アプローチ」共立 (2009)
・斉藤成也「ゲノム進化を考える」(SGC ライブラリ 53) サイエンス社 (2007)
・根井・クマー「分子進化と分子系統学」培風館 (2006)
・Pachter/Sturmfels(ed.) "Algebrai Statistics for Computation Biology" Cambridge (2005)

DNA データから，分子系統樹を作るのよく使われるのが近隣結合法 (NJ 法) である．斉藤成也によって開発された．組み合わせ論的な方法である程度よい系統樹を作る方法である．ただ，それが何らかの最適問題の解になっているかは証明されていないようである．数学者がこの方法を発見できなかったことは少し残念である．

有限群の斜準同型に関する予想の拡張について

An extension of a conjecture on crossed homomorphisms of finite groups

近畿大学　淺井 恒信 (Tsunenobu Asai)
Kinki University

愛媛大学　庭崎 隆 (Takashi Niwasaki)
Ehime University

本講演の内容は, 竹ヶ原裕元氏 (室蘭工業大学), 千吉良直樹氏 (熊本大学) との共同研究によるものである.

1　はじめに

有限群の間の斜準同型写像の個数に関する合同式を考える. A, G を有限群とし, A は G に作用しているとする. A から G への斜準同型写像全体のなす集合を $Z^1(A,G)$ で表わす. 即ち

$$Z^1(A,G) = \{\lambda : A \to G \mid \lambda(aa') = \lambda(a) \cdot {}^a(\lambda(a')) \quad \text{for } a, a' \in A\}.$$

斜準同型写像の個数に関して, 次の予想が考えられている.

予想　A, G を有限群とし, A は G に作用しているとき,

$$|Z^1(A,G)| \equiv 0 \qquad \bmod \gcd(|A/A'|, |G|)$$

が成り立つ. ここで, A' は A の交換子群である.

本講演では, 予想における交換子群を, A の一般の正規部分群 A_1 に置き換えて, 合同式

$$|Z^1(A,G)| \equiv 0 \qquad \bmod \gcd(|A/A_1|, |G|)$$

が成り立つ条件を考察し, 次の結果を得た. ここで, 自然数 n に対し, n_p は n を割る最大の p 巾を表す. ($\bar{\varphi}$ 等の定義は次節.)

主定理　$|A/A_1|$ を割る全ての素数 p に対して, $A_1 \leq B \trianglelefteq A$ で $|A/B| = |A/A_1|_p$ なる B が存在して, 任意の $\varphi \in Z^1(A,G)$ と $C_G(\bar{\varphi}(B))$ の部分群で $\bar{\varphi}(A/B)$ 不変な任意の p-部分群 K に対して,

$$|Z^1_{\varphi}(A/B, K)| \equiv 0 \qquad \bmod \gcd(|A/B|, |K|)$$

が成り立つとする. このとき

$$|Z^1(A,G)| \equiv 0 \qquad \bmod \gcd(|A/A_1|, |G|)$$

が成り立つ.

なお, 全ての素数 p について部分群 B が存在することは, A/A_1 が巾零群であることと同値であることに注意する.

2 いくつかの定義と準備

以下の議論においては, G や A を半直積群 GA の部分群として扱うと理解しやすい. G は共役により GA に作用しているので, $Z^1(A,G)$ にも次のように作用する.

定義 1 G は $Z^1(A,G)$ に

$$\begin{array}{ccc} G \times Z^1(A,G) & \longrightarrow & Z^1(A,G) \\ (g,\lambda) & \longmapsto & {}^g\lambda : A \to G \\ & & \quad a \mapsto g \cdot \lambda(a) \cdot {}^a g^{-1} \end{array}$$

で作用する.

B を A の部分群, $\mu \in Z^1(B,G)$ とする. A から G への斜準同型写像のうち, B への制限が μ となるものの全体のなす集合を $Z^1(A,G;B,\mu)$ で表わす.

$$Z^1(A,G;B,\mu) = \{\lambda \in Z^1(A,G) \mid \lambda|_B = \mu\}$$

写像 $\tilde{\mu} : B \to GA$ を $b \mapsto \mu(b)b$ で定める. これは群の準同型となる.

以降この節では, B は A の正規部分群とし, 任意に $\lambda \in Z^1(A,G;B,\mu)$ を取り, 固定する. また, $\bar{A} = A/B$, $\bar{a} = aB \in \bar{A}$, $H = C_G(\tilde{\mu}(B))$ とおく.

定義 2 $\bar{A}$ は H に, ${}^{\bar{a}}g = \lambda(a) \cdot {}^a g \cdot \lambda(a)^{-1}$ ($\bar{a} \in \bar{A}$, $g \in H$) として作用する. この作用による斜準同型写像全体のなす集合を $Z^1_\lambda(\bar{A},H)$ で表わす.

命題 3 $Z^1(A,G;B,\mu)$ と $Z^1_\lambda(\bar{A},H)$ は 1 対 1 に対応する. その対応は次で与えられる.

$$\begin{array}{ccc} Z^1(A,G;B,\mu) & \longrightarrow & Z^1_\lambda(\bar{A},H) \\ \eta & \longmapsto & \Delta\eta : \bar{A} \to H \\ & & \quad \bar{a} \mapsto \eta(a)\lambda^{-1}(a) \end{array}$$

この対応により, $Z^1(A,G;B,\mu)$ と $Z^1_\lambda(\bar{A},H)$ を同一視して扱う.

定義 4 K を H の部分群とする. $\eta_1, \eta_2 \in Z^1_\lambda(\bar{A},H)$ に対して,

$$\eta_1 \approx_K \eta_2 \overset{\text{def}}{\Longleftrightarrow} {}^\forall a \in A, \quad \eta_1(a) \in K\eta_2(a)$$

$$\eta_1 \approxeq_K \eta_2 \overset{\text{def}}{\Longleftrightarrow} {}^\exists k \in K, \quad \eta_1 \approx_K {}^k\eta_2$$

と定める. これらはいずれも $Z^1_\lambda(\bar{A},H)$ における同値関係となる.

命題 5 $\varphi \in Z^1_\lambda(\bar{A},H)$, K を H の部分群とする. このとき, 次の等式が成り立つ.

(1) $\#\{\eta \in Z^1_\lambda(\bar{A},H) \mid \eta \approx_K \varphi\} = |Z^1_\varphi(\bar{A}, K_{\tilde{\varphi}(\bar{A})})|$

(2) $\#\{\eta \in Z^1_\lambda(\bar{A},H) \mid \eta \approxeq_K \varphi\} = (K : K_{\tilde{\varphi}(\bar{A})}) \cdot |Z^1_\varphi(\bar{A}, K_{\tilde{\varphi}(\bar{A})})|$

ここで, $K_{\tilde{\varphi}(\bar{A})}$ は K の $\tilde{\varphi}(\bar{A})$ 不変な最大の部分群 $\bigcap_{\bar{a}\in\bar{A}} {}^{\tilde{\varphi}(\bar{a})}K = \bigcap_{a\in A} \varphi(a) \cdot {}^a K \cdot \varphi(a)^{-1}$ を表す.

3 主定理の証明の概略

$|A/A_1|$ を割る全ての素数 p に対して

$$|Z^1(A,G)| \equiv 0 \mod \gcd(|A/A_1|_p, |G|)$$

が成り立てば, 主定理が成り立つ. p を $|A/A_1|$ を割る素数, B を $A_1 \leq B \trianglelefteq A$ で $|A/B| = |A/A_1|_p$ なる正規部分群とする.

$$\begin{aligned} |Z^1(A,G)| &= \sum_{\mu \in Z^1(B,G)} |Z^1(A,G;B,\mu)| \\ &= \sum_{\mu \in Z^1(B,G)/\sim_G} (G : C_G(\tilde{\mu}(B))) \cdot |Z^1(A,G;B,\mu)| \end{aligned}$$

ここで和は G 共役 (定義 1 の作用) の代表を動く. 任意に $\lambda \in Z^1(A,G;B,\mu)$ を固定する. 前節と同様に, $\bar{A} = A/B$, $\bar{a} = aB \in \bar{A}$, $H = C_G(\tilde{\mu}(B))$ とおき,

$$(G : C_G(\tilde{\mu}(B))) \cdot |Z^1(A,G;B,\mu)| = (G : H) \cdot |Z^1_\lambda(\bar{A}, H)|$$

を考える. K を H の Sylow p-部分群とし, $Z^1_\lambda(\bar{A}, H)$ を $\approx_K$ で類別する. $\varphi \in Z^1_\lambda(\bar{A}, H)$ に対して

$$\#\{\eta \in Z^1_\lambda(\bar{A}, H) \mid \eta \approx_K \varphi\} = (K : K_{\widetilde{\varphi(\bar{A})}}) \cdot |Z^1_\varphi(\bar{A}, K_{\widetilde{\varphi(\bar{A})}})|$$

となる. ところが, 主定理の仮定より

$$|Z^1_\varphi(\bar{A}, K_{\widetilde{\varphi(\bar{A})}})| \equiv 0 \mod \gcd\left(|\bar{A}|, |K_{\widetilde{\varphi(\bar{A})}}|\right)$$

が成り立っているから,

$$\begin{aligned} \#\{\eta \in Z^1_\lambda(\bar{A}, H) \mid \eta \approx_K \varphi\} &\equiv 0 \mod (K : K_{\widetilde{\varphi(\bar{A})}}) \cdot \gcd\left(|\bar{A}|, |K_{\widetilde{\varphi(\bar{A})}}|\right) \\ &\equiv 0 \mod \gcd\left(|\bar{A}|, |K|\right) \\ &\equiv 0 \mod \gcd\left(|\bar{A}|, |H)|\right) \end{aligned}$$

となる. ここで, $|\bar{A}| = |\bar{A}|_p$ と $|K| = |H|_p$ を使った. よって

$$|Z^1_\lambda(\bar{A}, H)| \equiv 0 \mod \gcd\left(|\bar{A}|, |H|\right)$$

であり

$$\begin{aligned} |Z^1(A,G)| &\equiv 0 \mod (G : H) \cdot \gcd\left(|\bar{A}|, |H|\right) \\ &\equiv 0 \mod \gcd\left(|\bar{A}|, |G|\right) \\ &\equiv 0 \mod \gcd(|A/A_1|_p, |G|) \end{aligned}$$

を得る. 従って, 主定理が成り立つ. □

この主定理を用いることにより，以下のことが証明できる (または同様の議論が証明に使われた).

定理 6 全ての素数 p と，アーベル p 群 A, 及び一般の有限群 G に対し，

$$|Z^1(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A|, |G|_p)$$

が成り立つならば，予想は正しい.

定理 7 ([3]) 一般の有限群 A, G に対して，

$$|Z^1(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A/A' : \Phi(A/A')|, |G|)$$

が成り立つ．ここで．$\Phi(A/A')$ は A/A' のフラッチニ部分群である.

命題 8 A の正規部分群 B と，A/B が作用する G の任意の部分群 H に対し，

$$|Z^1(A/B, H)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A/B|, |H|)$$

が成り立つならば，

$$|Z^1(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A/B|, |G|)$$

が成り立つ.

命題 9 G の部分群 K に対し，K_A を A 不変な細大の K の部分群とする．このとき，もし

$$|Z^1(A, K_A)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A|, |K_A|)$$

が成り立つならば，

$$|Z^1(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A|, |K|)$$

が成り立つ.

注意 10 位数 8 の四元数群 Q が自分自身に自明に作用している場合を考える．このとき

$$|Z^1(Q,Q)| = |\mathrm{Hom}(Q,Q)| = 28 \not\equiv 0 \bmod |Q|$$

である．従って，仮に A が p 群であっても，主定理の仮定は満たされない場合があることが分かる.

参考文献

[1] T. Asai and Y. Takegahara, On the number of crossed homomorphisms, *Hokkaido Math. J.* **28** (1999), 535–543.

[2] T. Asai and Y. Takegahara, $|\mathrm{Hom}(A,G)|$, IV, *J. Algebra* **246** (2001), 543–563.

[3] T. Asai and T. Yoshida, $|\mathrm{Hom}(A,G)|$, II, *J. Algebra* **160** (1993), 273–285.

[4] R. Brauer, On a theorem of Frobenius, *American Math. Monthly* **76** (1969), 12–15.

[5] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1935), 468–501.

WEIGHTED SCATTERING MATRICES OF REGULAR COVERINGS OF GRAPHS

Iwao SATO
Oyama National College of Technology, Oyama, Tochigi 323-0806, JAPAN

October 17, 2011

1 Introduction

Graphs treated here are finite. Let $G = (V(G), E(G))$ be a connected graph (possibly multiple edges and loops) with the set $V(G)$ of vertices and the set $E(G)$ of unoriented edges uv joining two vertices u and v. For $uv \in E(G)$, an arc (u, v) is the oriented edge from u to v. Set $D(G) = \{(u, v), (v, u) \mid uv \in E(G)\}$. For $e = (u, v) \in D(G)$, set $u = o(e)$ and $v = t(e)$. Furthermore, let $e^{-1} = (v, u)$ be the *inverse* of $e = (u, v)$.

A *path P of length n* in G is a sequence $P = (e_1, \ldots, e_n)$ of n arcs such that $e_i \in D(G)$, $t(e_i) = o(e_{i+1})(1 \le i \le n-1)$, where indices are treated *mod* n. Set $\mid P \mid = n$, $o(P) = o(e_1)$ and $t(P) = t(e_n)$. Also, P is called an $(o(P), t(P))$*-path*. We say that a path $P = (e_1, \ldots, e_n)$ has a *backtracking* if $e_{i+1}^{-1} = e_i$ for some $i(1 \le i \le n-1)$. A (v, w)-path is called a *v-cycle* (or *v-closed path*) if $v = w$. The *inverse cycle* of a cycle $C = (e_1, \ldots, e_n)$ is the cycle $C^{-1} = (e_n^{-1}, \ldots, e_1^{-1})$.

We introduce an equivalence relation between cycles. Two cycles $C_1 = (e_1, \ldots, e_m)$ and $C_2 = (f_1, \ldots, f_m)$ are called *equivalent* if there exists k such that $f_j = e_{j+k}$ for all j. The inverse cycle of C is in general not equivalent to C. Let $[C]$ be the equivalence class which contains a cycle C. Let B^r be the cycle obtained by going r times around a cycle B. Such a cycle is called a *power* of B. A cycle C is *reduced* if both C and C^2 have no backtracking. Furthermore, a cycle C is *prime* if it is not a power of a strictly smaller cycle. Note that each equivalence class of prime, reduced cycles of a graph G corresponds to a unique conjugacy class of the fundamental group $\pi_1(G, v)$ of G at a vertex v of G.

For $u \in \mathbf{C}$ with $\mid u \mid$ sufficiently small, the *Ihara zeta function* of a graph G is defined to be

$$\mathbf{Z}(G, u) = \mathbf{Z}_G(u) = \prod_{[C]} (1 - u^{|C|})^{-1},$$

where $[C]$ runs over all equivalence classes of prime, reduced cycles of G(see [9]).

In [9], Ihara showed that the reciprocal of the zeta function of a graph is an explicit polynomial. A zeta function of a regular graph G associated with a unitary representation of the fundamental group of G, was developed by Sunada [16,17]. Hashimoto [8] treated multivariable zeta functions of bipartite graphs. Bass [2] generalized Ihara's result on the zeta function of a regular graph to an irregular graph, and showed that its reciprocal is again a polynomial.

Theorem 1 (Bass) *Let G be a connected graph. Then the reciprocal of the zeta function of G is given by*

$$\mathbf{Z}(G, u)^{-1} = (1 - u^2)^{r-1} \det(\mathbf{I} - u\mathbf{A}(G) + u^2(\mathbf{D} - \mathbf{I})),$$

where r and $\mathbf{A}(G)$ are the Betti number and the adjacency matrix of G, respectively, and $\mathbf{D} = \mathbf{D}_G = (d_{ij})$ is the diagonal matrix with $d_{ii} = \deg v_i$ where $V(G) = \{v_1, \ldots, v_n\}$.

Stark and Terras [15] gave an elementary proof of Theorem 1, and discussed three different zeta functions of any graph. Furthermore, various proofs of Bass' Theorem were given by Foata and Zeilberger in [4], Kotani and Sunada in [10].

The spectral determinant of the Laplacian on a quantum graph is closely related to the Ihara zeta function of a graph(see [3,5,7,14]) .

Smilansky [14] considered a certain determinant on the bond weighted scattering matrix of a regular graph G, and expressed it by using the characteristic polynomial of its weighted Laplacian of G.

We state a short review for the bond weighted wave functions which are used to compute eigenvalues of the weighted Laplacian along [14]. Let G be a connected graph with n vertices and m unoriented edges, and let $V(G) = \{v_1, \ldots, v_n\}$. Then we consider an $n \times n$ matrix $\mathbf{W} = (w_{ij})_{1 \le i,j \le n}$ with ij entry nonzero complex number w_{ij} if $(v_i, v_j) \in D(G)$, and $w_{ij} = 0$ otherwise. The matrix $\mathbf{W} = \mathbf{W}(G)$ is called the *weighted matrix* of G. Furthermore, let $w(v_i, v_j) = w_{ij}$, $v_i, v_j \in V(G)$ and $w(e) = w_{ij}$, where $e = (v_i, v_j) \in D(G)$. For each path $P = (e_1, \ldots, e_r)$ of G, the *norm* $w(P)$ of P is defined to be $w(P) = w(e_1) \cdots w(e_r)$.

Assume that $\mathbf{W} = \mathbf{W}(G)$ is a symmetric weighted matrix of G with all non-negative elements. Then $\mathbf{W}(G)$ is called a *non-negative* symmetric weighted matrix of G. Set $D(G) = \{e_1, \ldots, e_m, e_1^{-1}, \ldots, e_m^{-1}\}$. and

$$d_j = \sum_{o(e)=v_j} w(e) \ for \ j = 1, \ldots, n.$$

Furthermore, let

$$\mathbf{D}_w = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}.$$

The *weighted Laplacian (matrix)* $\mathbf{L}_w = \mathbf{L}_w(G)$ of G is defined by

$$\mathbf{L}_w = \mathbf{L}_w(G) = -\mathbf{W}(G) + \mathbf{D}_w.$$

If $w = \mathbf{1}$, i.e., $w(e) = 1$ for each $e \in D(G)$, then the weighted Laplacian of G is the Laplacian of G. Let λ be an eigenvalue of $\mathbf{L}_w$ and $\phi = (\phi_1, \ldots, \phi_n)$ the eigenvector corresponding to λ. For each arc $b = (v_j, v_l)$, one associates a *(bond) weighted wave function*

$$\phi_b(x) = \frac{1}{\sqrt{w(b)}}(a_b e^{i\pi x/4} + a_{b^{-1}} e^{-i\pi x/4}), \ x = \pm 1$$

under the condition

$$\phi_b(1) = \phi_j, \phi_b(-1) = \phi_l.$$

We consider the following three conditions:

1. *uniqueness*: The value of the eigenvector ϕ_j at the vertex v_j, computed in the terms of the bond wave functions, is the same for all the arcs emanating from v_j.

2. *ϕ is an eigenvector of* $\mathbf{L}_w$;

3. *consistency*: The linear relation between the incoming and outgoing coefficients, given in (1) must be satisfied simultaneously at all vertices.

By uniqueness, we have

$$\frac{1}{\sqrt{w(b_1)}}(a_{b_1}e^{i\pi/4}+a_{b_1^{-1}}e^{-i\pi/4})=\cdots=\frac{1}{\sqrt{w(b_{p_j})}}(a_{b_{p_j}}e^{i\pi/4}+a_{b_{p_j}^{-1}}e^{-i\pi/4})=\phi_j,$$

where $b_1, b_2, \ldots, b_{p_j}$ are arcs emanating from v_j, $p_j = \deg v_j$, and $i = \sqrt{-1}$.

By condition 2, we have

$$-\sum_{k=1}^{p_j}\frac{w(b_k)}{\sqrt{w(b_k)}}(a_{b_k}e^{-i\pi/4}+a_{b_k^{-1}}e^{i\pi/4})=(\lambda-d_j)\frac{1}{p_j}\sum_{k=1}^{p_j}\frac{1}{\sqrt{w(b_k)}}(a_{b_k}e^{i\pi/4}+a_{b_k^{-1}}e^{-i\pi/4}).$$

Thus, for each arc b with $o(b) = v_j$,

$$a_b=\sum_{t(c)=v_j}\sigma_{bc}^{v_j}(\lambda)a_c, \tag{1}$$

where

$$\sigma_{bc}^{v_j}(\lambda)=i(\delta_{b^{-1}c}-\frac{2}{d_j}\frac{1}{1-i(1-\lambda/d_j)}\sqrt{w(b)}\sqrt{w(c)}),$$

where $\delta_{b^{-1}c}$ is the Kronecker delta. Then the *(bond) weighted scattering matrix* $\mathbf{U}(\lambda) = (U_{ef})_{e,f\in D(G)}$ of G is defined by

$$U_{ef}=\begin{cases} i(\delta_{e^{-1}f}-x_{o(e)}\sqrt{w(e)}\sqrt{w(f)}) & \text{if } t(f)=o(e),\\ 0 & \text{otherwise,}\end{cases}$$

where

$$x_{v_j}=x(v_j)=x_j=\frac{2}{d_j}\frac{1}{1-i(1-\lambda/d_j)}$$

for each $j = 1, \ldots, n$.

By consistency, we have

$$\mathbf{U}(\lambda)\mathbf{a}=\mathbf{a},$$

where $\mathbf{a} = {}^t(a_1, a_2, \ldots, a_n)$. This holds if and only if

$$\det(\mathbf{I}_{2m}-\mathbf{U}(\lambda))=0.$$

Smilansky in [14] stated a formula, without proof, for the following determinant on the weighted scattering matrix of a graph G.

Theorem 2 (Smilansky) *Let G be a connected graph with n vertices and m unoriented edges and let $\mathbf{W}(G)$ be a non-negative symmetric weighted matrix of G. Then, for the weighted scattering matrix of G,*

$$\det(\mathbf{I}_{2m}-\mathbf{U}(\lambda))=\frac{2^m i^n\det(\lambda\mathbf{I}_n+\mathbf{W}(G)-\mathbf{D}_w)}{\prod_{j=1}^n(d_j-id_j+\lambda i)},$$

where $V(G) = \{v_1, \ldots, v_n\}$.

In Section 2, we give a decomposition of a determinant for the weighted scattering matrix of a regular covering of G. In Section 3, we define an L-function of G, and give a determinant expression of it. As a corollary, we express the determinant of the weighted scattering matrix of a regular covering of G by means of its L-functions.

For a general theory of the representation of groups and graph coverings, the reader is referred to [13] and [6], respectively.

2 Weighted scattering matrix of a regular covering of a graph

Let G be a connected graph, and let $N(v) = \{w \in V(G) \mid (v,w) \in D(G)\}$ denote the neighbourhood of a vertex v in G. A graph H is called a *covering* of G with projection $\pi : H \longrightarrow G$ if there is a surjection $\pi : V(H) \longrightarrow V(G)$ so that for any vertices $v \in V(G)$ and $v' \in \pi^{-1}(v)$, there exist neighborhoods $N(v), N(v')$ so that $\pi|_{N(v')} : N(v') \longrightarrow N(v)$ is a bijection.

Let Γ be a group of automorphisms of a graph G. An automorphism $\gamma : V(G) \longrightarrow V(G)$ of Γ acts on G as follows: $\gamma(e) = (\gamma(u), \gamma(v))$ for each $e = (u,v) \in D(G)$. When a finite group Π acts on a graph G, the *quotient graph* G/Π is a graph whose vertices are the Π-orbits on $V(G)$, with two vertices adjacent in G/Π if and only if some two of their representatives are adjacent in G. A covering $\pi : H \longrightarrow G$ is said to be *regular* if there is a subgroup B of the automorphism group $Aut\,H$ of H acting freely on H such that the quotient graph H/B is isomorphic to G.

Let G be a graph and Γ a finite group. Then a mapping $\alpha : D(G) \longrightarrow \Gamma$ is called an *ordinary voltage assignment* if $\alpha(v,u) = \alpha(u,v)^{-1}$ for each $(u,v) \in D(G)$. The pair (G,α) is called an *ordinary voltage graph*. The *derived graph* G^α of the ordinary voltage graph (G,α) is defined as follows: $V(G^\alpha) = V(G) \times \Gamma$ and $((u,h),(v,k)) \in D(G^\alpha)$ if and only if $(u,v) \in D(G)$ and $k = h\alpha(u,v)$. The *natural projection* $\pi : G^\alpha \longrightarrow G$ is defined by $\pi(u,h) = u$. The graph G^α is called a *derived graph covering* of G with voltages in Γ or a Γ-*covering* of G. The natural projection π commutes with the right multiplication action of the $\alpha(e), e \in D(G)$ and the left action of Γ on the fibers: $g(u,h) = (u,gh), g \in \Gamma$, which is free and transitive. Thus, the Γ-covering G^α is a $\mid \Gamma \mid$-fold regular covering of G with covering transformation group Γ. Furthermore, every regular covering of a graph G is a Γ-covering of G for some group Γ(see [6]).

Let G be a connected graph, Γ a finite group and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. In the Γ-covering G^α, set $v_g = (v,g)$ and $e_g = (e,g)$, where $v \in V(G), e \in D(G), g \in \Gamma$. For $e = (u,v) \in D(G)$, the arc e_g emanates from u_g and terminates at $v_{g\alpha(e)}$. Note that $e_g^{-1} = (e^{-1})_{g\alpha(e)}$.

Let $V(G) = \{v_1, \ldots, v_n\}$, $D(G) = \{e_1, \ldots, e_l, e_1^{-1}, \ldots, e_l^{-1}\}$ and $\mathbf{W} = \mathbf{W}(G)$ a weighted matrix of G. Set $\Gamma = \{g_1 = 1, g_2, \ldots, g_m\}$. Then we define the *weighted matrix* $\tilde{\mathbf{W}} = \mathbf{W}(G^\alpha) = (\tilde{w}(u_g, v_h))$ of G^α *derived from* $\mathbf{W}$ as follows:

$$\tilde{w}(u_g, v_h) := \begin{cases} w(u,v) & \text{if } (u,v) \in D(G) \text{ and } h = g\alpha(u,v), \\ 0 & \text{otherwise.} \end{cases}$$

Let λ be an eigenvalue of $\mathbf{L}_{\tilde{w}}(G^\alpha) = \mathbf{D}_{\tilde{w}} - \mathbf{W}(G^\alpha)$ and $\tilde{\phi} = (\phi_{v_1,g_1}, \ldots, \phi_{v_1,g_m} \ldots, \phi_{v_n,g_1}, \ldots, \phi_{v_n,g_m})$ the eigenvector corresponding to λ. For each arc $b_g = (v_g, z_{g\alpha(b)})$ $(b = (v,z))$ of G^α, the weighted wave function of b_g is

$$\phi_{b_g}(x) = \frac{1}{\sqrt{w(b)}}(a_{b_g} e^{i\pi x/4} + a_{b_g^{-1}} e^{-i\pi x/4}), \ x = \pm 1$$

under the condition

$$\phi_{b_g}(1) = \phi_{v,g}, \phi_{b_g}(-1) = \phi_{z,g\alpha(b)}.$$

Similarly to the above, for each arc b_g with $o(b_g) = v_g$,

$$a_{b_g} = \sum_{t(c_h) = v_g} \sigma^{v_g}_{b_g c_h}(\lambda) a_{c_h},$$

where

$$\sigma^{v_g}_{b_g c_h}(\lambda) = i(\delta_{b_g^{-1} c_h} - \frac{2}{d_{v_g}} \frac{1}{1 - i(1 - \lambda/d_{v_g})} \sqrt{w(b)}\sqrt{w(c)}).$$

By the definition of $\tilde{w}$, we have

$$d_{v_g} = \sum_{o(e_g)=v_g} \tilde{w}(e_g) = \sum_{o(e)=v} w(e) = d_v$$

for eavh $v \in V(G)$ and each $g \in \Gamma$. Thus,

$$\frac{2}{d_{v_g}} \frac{1}{1 - i(1 - \lambda/d_{v_g})} = \frac{2}{d_v} \frac{1}{1 - i(1 - \lambda/d_v)}.$$

Let

$$x_v = \frac{2}{d_v} \frac{1}{1 - i(1 - \lambda/d_v)}, v \in V(G).$$

Then the weighted scattering matrix $\tilde{\mathbf{U}}(\lambda) = (U(e_g, f_h))$ of G^α is given by

$$\begin{aligned} U(e_g, f_h) &:= \begin{cases} i(\delta_{e_g^{-1} f_h} - x_{o(e)}\sqrt{w(e)}\sqrt{w(f)}) & \text{if } t(f_h) = o(e_g), \\ 0 & \text{otherwise.} \end{cases} \\ &= \begin{cases} i(\delta_{e_g^{-1} f_h} - x_{o(e)}\sqrt{w(e)}\sqrt{w(f)}) & \text{if } t(f) = o(e), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

For $g \in \Gamma$, let the matrix $\mathbf{W}_g = (w_{uv}^{(g)})$ be defined by

$$w_{uv}^{(g)} := \begin{cases} w(u,v) & \text{if } \alpha(u,v) = g \text{ and } (u,v) \in D(G), \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, let $\mathbf{U}_g = (U^{(g)}(e,f))$ be given by

$$U^{(g)}(e,f) := \begin{cases} i(\delta_{e^{-1} f} - x_{o(e)}\sqrt{w(e)}\sqrt{w(f)}) & \text{if } t(f) = o(e) \text{ and } \alpha(f) = g, \\ 0 & \text{otherwise.} \end{cases}$$

Mizuno and Sato [12] presented a decomposition formula for the determinant of the weighted scattering matrix of a regular covering of a graph. The *Kronecker product* $\mathbf{A} \bigotimes \mathbf{B}$ of matrices $\mathbf{A}$ and $\mathbf{B}$ is considered as the matrix $\mathbf{A}$ having the element a_{ij} replaced by the matrix $a_{ij}\mathbf{B}$.

Theorem 3 (Mizuno and Sato) *Let G be a connected graph with n vertices and l unoriented edges, $\mathbf{W} = \mathbf{W}(G)$ a non-negative symmetric weighted matrix of G, Γ a finite group and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. Set $|\Gamma| = m$. Furthermore, let $\rho_1 = 1, \rho_2, \cdots, \rho_k$ be the irreducible representations of Γ, and f_i the degree of ρ_i for each i, where $f_1 = 1$. Suppose that the Γ-covering G^α of G is connected. Then, for the weighted scattering matrix of G^α,*

$$\det(\mathbf{I}_{2lm} - \tilde{\mathbf{U}}(\lambda)) = \det(\mathbf{I}_{2lm} - \mathbf{U}(\lambda)) \prod_{i=2}^{k} \det(\mathbf{I}_{2lf_i} - \sum_h {}^t\rho_i(h) \bigotimes \mathbf{U}_h)^{f_i}$$

$$= \frac{2^{lm} i^{nm} \det(\lambda \mathbf{I}_n + \mathbf{W}(G) - \mathbf{D}_w)}{\prod_{j=1}^{n}(d_j - id_j + \lambda i)^m} \prod_{i=2}^{k} \det(\lambda \mathbf{I}_{nf_i} + \sum_{h \in \Gamma} \rho_i(h) \bigotimes \mathbf{W}_h - \mathbf{I}_{f_i} \bigotimes \mathbf{D}_w)^{f_i}.$$

3 L-functions of graphs

Let G be a connected graph with n vertices and l unoriented edges, $\mathbf{W} = \mathbf{W}(G)$ a non-negative symmetric weighted matrix of G, Γ a finite group and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. Furthermore, let ρ be a unitary representation of Γ and d its degree. The *L-function* of G associated with ρ and α is defined by

$$\mathbf{Z}_S(G, \lambda, \rho, \alpha) = \det(\mathbf{I}_{2ld} - \sum_{h \in \Gamma} {}^t\rho(h) \bigotimes \mathbf{U}_h)^{-1}.$$

Here the subscript "S" means the weighted scattering matrix of G.

If $\rho = \mathbf{1}$ is the identity representation of Γ, then the L-function of G is a determinant on the weighted scattering matrix of G.

A determinant expression for the L-function of G associated with ρ and α is given as follows.

Theorem 4 (Mizuno and Sato) *Let G be a connected graph with n vertices and l unoriented edges, $\mathbf{W}(G)$ a non-negative symmetric weighted matrix of G, Γ a finite group and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. Furthermore, let ρ be a representation of Γ and d the degree of ρ. Then the reciprocal of the L-function of G associated with ρ and α is*

$$\mathbf{Z}_S(G, \lambda, \rho, \alpha)^{-1} = \frac{2^{ldi^{nd}}}{\prod_{j=1}^{n}(d_j - id_j + \lambda i)^d} \det(\lambda \mathbf{I}_n + \sum_{g \in \Gamma} \rho(g) \bigotimes \mathbf{W}_g - \mathbf{I}_d \bigotimes \mathbf{D}_w).$$

By Theorems 3 and 4, there

Corollary 1 (Mizuno and Sato) *Let G be a connected graph with l edges, $\mathbf{W}(G)$ a non-negative symmetric weighted matrix of G, Γ a finite group with order m and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. Then we have*

$$\det(\mathbf{I}_{2lm} - \bar{\mathbf{U}}(\lambda)) = \prod_{\rho} \mathbf{Z}_S(G, \lambda, \rho, \alpha)^{-\deg \rho},$$

where ρ runs over all inequivalent irreducible representations of Γ.

4 The Euler product for the L-function $\mathbf{Z}_S(G, \lambda, \rho, \alpha)$ of a graph

Mizuno and Sato [12] presented the Euler product for the L-function of a graph introduced in Section 3.

Foata and Zeilberger [4] gave a new proof of Bass's Theorem by using the algebra of Lyndon words. Let X be a finite nonempty set, $<$ a total order in X, and X^* the free monoid generated by X. Then the total order $<$ on X induces the lexicographic order $<^*$ on X^*. A *Lyndon word* in X is defined to a nonempty word in X^* which is prime, i.e., not the power l^r of any other word l for any $r \geq 2$, and which is also minimal in the class of its cyclic rearrangements under $<^*$(see [11]). Let L denote the set of all Lyndon words in X.

Foata and Zeilberger[4] gave a short proof of Amitsur's identity [1].

Theorem 5 (Amitsur) *For square matrices $\mathbf{A}_1, \cdots, \mathbf{A}_k$,*

$$\det(\mathbf{I} - (\mathbf{A}_1 + \cdots + \mathbf{A}_k)) = \prod_{l \in L} \det(\mathbf{I} - \mathbf{A}_l),$$

where the product runs over all Lyndon words in $\{1, \cdots, k\}$, and $\mathbf{A}_l = \mathbf{A}_{i_1} \cdots \mathbf{A}_{i_p}$ for $l = i_1 \cdots i_p$.

By Theorem 5, the following result follows.

Theorem 6 (Mizuno and Sato) *Let G be a connected graph with n vertices and l unoriented edges, $\mathbf{W}(G)$ a non-negative symmetric weighted matrix of G, Γ a finite group and $\alpha : D(G) \longrightarrow \Gamma$ an ordinary voltage assignment. For each path $P = (e_1, \cdots, e_r)$ of G, set $\alpha(P) = \alpha(e_1)\cdots\alpha(e_r)$. Furthermore, let ρ be a representation of Γ and d the degree of ρ. Then*

$$\mathbf{Z}_S(G, \lambda, \rho, \alpha) = \prod_{[C]} \det(\mathbf{I}_d - {}^t\rho(\alpha(C))a_C(\lambda))^{-1},$$

where $[C]$ runs over all equivalence classes of prime cycles of G, and

$$a_C(\lambda) = \sigma_{e_1e_n}^{o(e_1)}\sigma_{e_ne_{n-1}}^{o(e_n)}\cdots\sigma_{e_2e_1}^{o(e_2)},\ C = (e_1, e_2, \ldots, e_n)$$

5 Example

Finally, we give an example. Let $G = K_3$ be the complete graph with three vertices v_1, v_2, v_3 and six arcs $e_1 = (v_1, v_2), e_2 = (v_2, v_3), e_3 = (v_3, v_1), e_1^{-1} = (v_2, v_1), e_2^{-1} = (v_3, v_2), e_3^{-1} = (v_1, v_3)$. Furthermore, let

$$\mathbf{W}(K_3) = \begin{bmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{bmatrix}.$$

Then we have $d_{v_1} = a + b$, $d_{v_2} = a + c$, $d_{v_3} = b + c$ and

$$\mathbf{D}_w = \begin{bmatrix} a+b & 0 & 0 \\ 0 & a+c & 0 \\ 0 & 0 & b+c \end{bmatrix}.$$

Furthermore,

$$x_{v_1} = \frac{2}{(a+b) - (a+b)i + \lambda i}, x_{v_2} = \frac{2}{(a+c) - (a+c)i + \lambda i}, x_{v_3} = \frac{2}{(b+c) - (b+c)i + \lambda i}.$$

Thus,

$$\mathbf{U}(\lambda) = \begin{bmatrix} 0 & 0 & -ix_{v_1}\sqrt{ab} & i(1 - x_{v_1}a) & 0 & 0 \\ -ix_{v_2}\sqrt{ac} & 0 & 0 & 0 & i(1 - x_{v_2}c) & 0 \\ 0 & -ix_{v_3}\sqrt{bc} & 0 & 0 & 0 & i(1 - x_{v_3}b) \\ i(1 - x_{v_2}a) & 0 & 0 & 0 & -ix_{v_2}\sqrt{ac} & 0 \\ 0 & i(1 - x_{v_3}c) & 0 & 0 & 0 & -ix_{v_3}\sqrt{bc} \\ 0 & 0 & i(1 - x_{v_1}b) & -ix_{v_1}\sqrt{ab} & 0 & 0 \end{bmatrix}.$$

By Theorem 2, we have

$$\begin{aligned} \det(\mathbf{I}_6 - \mathbf{U}(\lambda) &= \tfrac{2^6 i^3}{pqr}\det(\lambda\mathbf{I}_3 + \mathbf{W}(K_3) - \mathbf{D}_w) \\ &= \tfrac{2^6 i^3}{pqr}\det\left(\begin{bmatrix} \lambda - (a+b) & a & b \\ a & \lambda - (a+c) & c \\ b & c & \lambda - (b+c) \end{bmatrix}\right) \\ &= \tfrac{2^6 i^3}{pqr}\lambda(\lambda^2 - 2(a+b+c)\lambda + 3(ab+bc+ac)), \end{aligned}$$

where $p = (a+b)(1-i) + \lambda i$, $q = (a+c)(1-i) + \lambda i$ and $r = (b+c)(1-i) + \lambda i$.

Let $\Gamma = Z_3 = \{1, \tau, \tau^2\}(\tau^3 = 1)$ be the cyclic group of order 3, and let $\alpha : D(G) \longrightarrow Z_3$ be the ordinary voltage assignment such that $\alpha(v_1, v_2) = \tau$ and $\alpha(v_2, v_3) = \alpha(v_3, v_1) = 1$. The characters of $\mathbf{Z}_3$ are given as follows: $\chi_i(\tau^j) = (\xi^i)^j$, $0 \leq i, j \leq 2$, where $\xi = \frac{-1+\sqrt{-3}}{2}$.

Now, we consider the L-function $\mathbf{Z}_S(K_3, \lambda, \chi_1, \alpha)^{-1}$ of K_3 associated with χ_1 and α. Theorem 4 implies that

$$\begin{aligned}
\mathbf{Z}_S(K_3, \lambda, \chi_1, \alpha)^{-1} &= \tfrac{2^6 i^3}{pqr} \det(\lambda \mathbf{I}_3 + \textstyle\sum_{j=0}^{2} \chi_1(\tau^j) \mathbf{W}_{\tau_j} - \mathbf{D}_w) \\
&= \tfrac{2^6 i^3}{pqr} \det \left(\begin{bmatrix} \lambda - (a+b) & a\xi & b \\ a\xi^2 & \lambda - (a+c) & c \\ b & c & \lambda - (b+c) \end{bmatrix} \right) \\
&= \tfrac{2^6 i^3}{pqr} (\lambda^3 - 2(a+b+c)\lambda^2 + 3(ab+bc+ac)\lambda - 3abc).
\end{aligned}$$

Similarly, we have

$$\mathbf{Z}_S(K_3, \lambda, \chi_2, \alpha)^{-1} = \frac{2^6 i^3}{pqr} (\lambda^3 - 2(a+b+c)\lambda^2 + 3(ab+bc+ac)\lambda - 3abc).$$

By Corollary 1, it follows that

$$\begin{aligned}
\det(\mathbf{I}_{18} - \tilde{\mathbf{U}}(\lambda)) &= \det(\mathbf{I}_6 - \mathbf{U}(\lambda)) \mathbf{Z}_S(K_3, \lambda, \chi_1, \alpha)^{-1} \mathbf{Z}_S(K_3, \lambda, \chi_2, \alpha)^{-1} \\
&= \frac{2^{18} i}{p^3 q^3 r^3} \lambda (\lambda^2 - 2(a+b+c)\lambda + 3(ab+bc+ac)) \\
&\quad \times (\lambda^3 - 2(a+b+c)\lambda^2 + 3(ab+bc+ac)\lambda - 3abc)^2.
\end{aligned}$$

Acknowledgment

We would like to thank Professor Chihiro Suetake, Professor Kenji Akiyama and Professor Masaki Tanaka for inviting me to the 28 th Conference of Algebraic Combinatorics at Oita University.

References

[1] S. A. Amitsur, On the characteristic polynomial of a sum of matrices, Linear and Multilinear Algebra 8 (1980), 177-182.

[2] H. Bass, The Ihara-Selberg zeta function of a tree lattice, Internat. J. Math. 3 (1992), 717-797.

[3] A. Comtet, J. Desbois and C. Texier, Functionals of the Brownian motion, localization and metric graphs, preprint [arXiv: cond-mat/0504513v2].

[4] D. Foata and D. Zeilberger, A combinatorial proof of Bass's evaluations of the Ihara-Selberg zeta function for graphs, Trans. Amer. Math. Soc. 351 (1999), 2257-2274.

[5] J. Desbois, Spectral determinant on graphs with generalized boundary conditions, Eur. Phys. J. B 24 (2001), 261-266.

[6] J. L. Gross and T. W. Tucker, Topological Graph Theory, Wiley-Interscience, New York, 1987.

[7] J. M. Harrison, U. Smilansky and B. Winn, Quantum graphs where back-scattering is prohibited, J. Phys. A:Math. Theor. 40 (2007), 14181-14193.

[8] K. Hashimoto, Zeta Functions of Finite Graphs and Representations of p-Adic Groups, in "Adv. Stud. Pure Math". Vol. 15, pp. 211-280, Academic Press, New York, 1989.

[9] Y. Ihara, On discrete subgroups of the two by two projective linear group over p-adic fields, J. Math. Soc. Japan 18 (1966), 219-235.

[10] M. Kotani and T. Sunada, Zeta functions of finite graphs, J. Math. Sci. U. Tokyo 7 (2000), 7-25.

[11] M. Lothaire, Combinatorics on Words, Addison-Wesley, Reading, Mass., 1983.

[12] H. Mizuno and I. Sato, Weighted scattering matrices of regular coverings of graphs, Linear Multilinear Algebra 58 (2010), 927-940.

[13] J. -P. Serre, Trees, Springer-Verlag, New York, 1980.

[14] U. Smilansky, Quantum chaos on discrete graphs, J. Phys. A: Math. Theor. 40 (2007), F621-F630.

[15] H. M. Stark and A. A. Terras, Zeta functions of finite graphs and coverings, Adv. Math. 121 (1996), 124-165.

[16] T. Sunada, L-Functions in Geometry and Some Applications, in "Lecture Notes in Math"., Vol. 1201, pp. 266-284, Springer-Verlag, New York, 1986.

[17] T. Sunada, Fundamental Groups and Laplacians(in Japanese), Kinokuniya, Tokyo, 1988.

グラフのユークリッド空間への埋め込みと強正則グラフの特徴付け

野崎　寛
東北大学大学院情報科学研究科
日本学術振興会特別研究員 PD
nozaki@ims.is.tohoku.ac.jp

篠原　雅史
鈴鹿工業高等専門学校
shinohara@genl.suzuka-ct.ac.jp

1　概要

ユークリッド空間 $\mathbb{R}^d$ 上の有限集合 X に対して，距離の集合を

$$A(X) := \{d(x,y) | x, y \in X, x \neq y\}$$

と定義する．ここで，$d(x,y)$ は x, y のユークリッド距離を表わしている．このとき，X が s-距離集合（s-distance set）と呼ばれるのは，$|A(X)| = s$ のときである．一つの s-距離集合 X が与えられたとき，X を拡大・縮小したものや，平行移動した集合 X' もやはり s-距離集合である．ここでは，相似変換で移り合う二つの集合を同型とし，その同型類について考える．次元 d と距離の個数 s を固定し，頂点数が最大となる s-距離集合を発見・分類することは s-距離集合の基本的な問題の一つである．最大な距離集合はアソシエーションスキームや強正則グラフと密接に関係しており，頂点数の大きな距離集合を代数的な視点などから特徴づけたいといというのが主な研究目標である．

この稿では 2-距離集合を主に扱う．2-距離集合の短い距離で結ばれている 2 頂点を辺で結ぶことで，距離集合に自然にグラフの構造を入れることが出来る．距離集合からグラフが与えれることは自然だが，同じグラフの構造をもつ 2-距離集合が，同型を除いて，どれくらい存在しているのかという問題は自明でない．その答えとして，Einhorn-Schoenberg [2] はグラフの 2 距離集合としての埋め込みの理論を確立した．この理論について，Section 2 で紹介したい．さらに，最近，Roy [4] は隣接行列の固有空間の情報を用いて，埋め込みの次元を明白に記述した．そこでは，固有空間のいくつかのパラメーターにより，グラフの特徴づけがされている．それについては Section 3 で述べる．

2-距離集合と関係の深い代数的な構造として，強正則グラフが知られている．強正則グラフから得られる 2-距離集合としての埋め込みは常に一つの球面に乗ることが知られる．

グラフの埋め込みがいつ一つの球面に乗るかの必要十分条件を，Roy が埋め込みの次元の記述に用いたグラフの特徴づけを用いて，決定することができた (Section 3)．さらに，その結果と埋め込みのある性質を用いて，新たな強正則グラフの特徴づけを与えることに成功した (Section 4)．

2 グラフのユークリッド空間への埋め込み

$G=(V,E)$ を単純グラフ（向き無し，ループ無し，重複辺無し）であるとする．G の隣接行列 A とは，V で行と列が添え字づけられている行列で，その成分が

$$A_{xy}=\begin{cases}1, \text{ if } \{x,y\}\in E,\\ 0, \text{ otherwise}\end{cases}$$

であるものである．$\bar{A}$ をその補グラフ $\bar{G}$ の隣接行列であるとする．本稿では，A と $\bar{A}$ の両方が零行列でないものを考えたいため，G は完全グラフ（全ての 2 頂点が辺で結ばれる），孤立点の集合（辺が一本もない）のどちらでもないと仮定する．単純グラフ G と $b\geq 0$ に対して，次のように行列 $M_b(G)$ を定義する．

$$M_b(G)=M_b:=A+b\bar{A}.$$

n 頂点グラフ G がユークリッド空間 $\mathbb{R}^d$ に representable であるとは，ある b に対して，

$$d(x_i,x_j)^2=M_b(i,j)$$

を満たす頂点集合 V から $\mathbb{R}^d$ への埋め込み $X=\{x_1,\ldots,x_n\}$ が存在するときにいう．ここで $M_b(i,j)$ は M_b の (i,j) 成分を表わす．つまり，M_b がある $X\subset\mathbb{R}^d$ の距離行列となるときに，G を representable であるという．ここで得られる埋め込み X は $b\neq 0,1$ のときに 2-距離集合となる．$b=0,1$ のとき，埋め込みは 1-距離集合となる．また $b\neq 0$ ならば埋め込みは単射である．

ここで，いつ M_b が $X\subset\mathbb{R}^d$ の距離行列に成りえるかを議論したい．もっと一般に，対角成分が全て 0 かつその他の成分が全て非負の対称行列 M に対して，Schoenberg [5] の定理（Theorem 2.1）が知られている．行列 M が $\mathbb{R}^d$ に representable であるとは，ある $X=\{x_1,\ldots,x_n\}\subset\mathbb{R}^d$ が存在して，

$$M(i,j)=d(x_i,x_j)^2$$

を満たすときに言う．二次形式

$$F_M(\xi)=F_M(\xi_2,\ldots,\xi_n):=\sum_{i,j=2}^{n}(M(1,i)+M(1,j)-M(i,j))\xi_i\xi_j$$

を準備する．

Theorem 2.1. M が *representable* であることと，任意の実数 $\xi_2, \ldots, \xi_n$ に対して，

$$F_M(\xi) \geq 0 \tag{2.1}$$

となることが同値である．さらに，M が (2.1) を満たしかつ，F_M のランクが k のとき，M は $\mathbb{R}^k$ に *representable* であるが，$\mathbb{R}^{k-1}$ に *representable* でない．

Theorem 2.1 を用いることで，b を固定したときに M_b が何次元に埋め込み可能であるかが計算できる．

次のような関数を考える．

$$\Phi(b) := \min_{\xi:\sum_{i=2}^{n}\xi_i^2=1} F_{M_b}(\xi) \ (b \geq 0).$$

ここで，$\Phi(b) \geq 0$ であることと，M_b が representable であることが同値であることに注意されたい．さらに，$\Phi(b) = 0$ となるとき，またはその時に限って，M_b は $\mathbb{R}^{n-2}$ に representable である．

Lemma 2.2. $\Phi(b)$ は上に凸の関数である．

Proof. ξ を固定した時に，$F_{M_b}(\xi)$ は b を変数とする一次関数である．$\Phi(b)$ は b に関する一次関数の無限集合 L の最小値をとる関数であることに注意する．$\Phi((x+y)/2) < (\Phi(x)+\Phi(y))/2$ となる $x, y \geq 0$ が存在すると仮定する．そのとき，$((x+y)/2, \Phi((x+y)/2))$ を通って，$(x, \Phi(x))$ の上部を通る，または交わる直線 l が L に存在している．l は $(y, \Phi(y))$ の下部（交わらない）を通るため，関数 Φ の最小性に矛盾する． □

$b = 1$ のとき，M_b は n 点 1-距離集合を表わすから，埋め込み可能であり，その埋め込みの次元は $n-1$ となる．よって，$\Phi(1) > 0$. $b = 0$ のとき，完全多部グラフ（complete multipertite graph）のときのみ埋め込み可能となり，その埋め込みは単射でないため，埋め込みの次元は $n-2$ 以下となる．それ以外のグラフでは，$b = 0$ のとき埋め込みは不可である．したがって $\Phi(0) \leq 0$. $b \to \infty$ については，補グラフの $b = 0$ の状況と対応しているから，$\Phi(\infty) \leq 0$ となる．無限大の議論を避けるために，$0 \leq b \leq 1$ としてやっても，その補グラフを考えることで一般性を欠かない．以上の状況と，中間値の定理から，次の定理が直ちに成り立つ．

Theorem 2.3 (Einhorn-Schoenberg [2]). G を完全グラフ，孤立点の集合のどちらでもない単純グラフであるとする．そのとき $n-2$ 次元以下のユークリッド空間への埋め込み可能な $M_b (0 \leq b < 1)$ は唯一つ存在する．

$0 \leq c < 1$ を $\Phi(c) = 0$ となる実数であるとする．そのとき，$c < b \leq 1$ を満たす b について，M_b は $n-1$ 次元に埋め込まれることを注意されたい．

3 グラフの埋め込みの極小次元と球面埋め込み

Theorem 2.3 で存在性が示された極小次元の埋め込みの次元は，隣接行列 A の固有空間のあるパラメータにより，明白に記述される [4]．その定理に必要な記号を準備したい．A の

i 番目に小さい固有値を τ_i とし，その重複度を m_i とする．E_i を τ_i に対する固有空間とし，P_i を E_i への直交射影行列とする．固有値 τ_i の main angle β_i は

$$\beta_i := \frac{1}{\sqrt{n}}\|P_i \cdot j\|$$

で定義される値である．ここで，j は成分が全て 1 の縦ベクトル，$\|x\| := \sqrt{x^T x}$ としている．そのとき，極小な 2-距離集合としての埋め込みの次元 d，$A(X) = \{1, c\}$ ($\Phi(c) = 0$ となる $c > 1$) は以下の様に書ける（ここでは，$c > 1$ と仮定していることに注意されたい）．

Theorem 3.1 (Roy [4]). (1) もし $\beta_1 = 0$ ならば，$c = \tau_1/(\tau_1 + 1)$, $d = n - m_1 - 1$.

(2) もし $\beta_1 \neq 0$ かつ $m_1 > 1$ ならば，$c = \tau_1/(\tau_1 + 1)$，$d = n - m_1$.

(3) もし $\beta_2 = 0$, $m_1 = 1$, $\tau_2 < -1$，かつ

$$\frac{\beta_1^2}{\tau_2 - \tau_1} = \sum_{i \geq 3} \frac{\beta_i^2}{\tau_i - \tau_2}$$

ならば，$c = \tau_2/(\tau_2 + 1)$，$d = n - m_2 - 2$.

(4) もし $\beta_2 = 0$, $m_1 = 1$, $\tau_2 < -1$，かつ

$$\frac{\beta_1^2}{\tau_2 - \tau_1} > \sum_{i \geq 3} \frac{\beta_i^2}{\tau_i - \tau_2}$$

ならば，$c = \tau_2/(\tau_2 + 1)$，$d = n - m_2 - 1$.

(5) それ以外のとき，$\tau_1/(\tau_1 + 1) < c$, $c \neq \tau_2/(\tau_2 + 1)$, $d = n - 2$.

Theorem 3.1 の番号を用いて，単純グラフ G または 2-距離集合は Type (1)–(5) に特徴づけられる．この Type (1)–(5) を用いて，いつ埋め込みが一つの球面に乗るかが明らかになった．

Theorem 3.2 (野崎-篠原). (1) *Type (1), (2), (4)* の極小次元埋め込みは一つの球面に乗る．

(2) *Type (3), (5)* の極小次元埋め込みは一つの球面には乗らない．

(3) 極小次元の埋め込みでない $n - 1$ 次元埋め込みは，一つの球面に乗る．

4 強正則グラフの特徴づけ

単純グラフ G がパラメーター (v, k, λ, μ) の強正則グラフ（strongly regular graph）と呼ばれるのは，G が次の性質を満たす時である．

(1) 頂点集合のサイズが n,

(2) k-正則（全ての頂点が，k 本の辺で結ばれている），

(3) 全ての結ばれている 2 頂点に対して，その 2 頂点と同時に辺で結ばれている頂点の数が λ,

(4) 全ての結ばれていない 2 頂点に対して，その 2 頂点と同時に辺で結ばれている頂点の数が μ.

強正則グラフの Bose–Mesner 代数（又は隣接代数）とは，単位行列 I，隣接行列 A, 補グラフの隣接行列 $\bar{A}$ を基底に，複素数体 $\mathbb{C}$ 上で生成される代数のことである．強正則グラフの隣接行列 A は異なる固有値が，丁度 3 つしかないことが知られている．そのうち，k は自明な固有値であり，重複度は 1 である．A の P_i（直交射影行列）は Bose–Mesner 代数の元であることが知られており，この P_i が 2-距離集合としての極小次元の埋め込みのグラム行列（集合の元で添え字づけられていて，成分が標準内積）になっている．

一般の n 頂点単純グラフに対して，埋め込みの極小次元を d_1, 補グラフの埋め込みの極小次元を d_2 としたときに，$n \leq 1 + d_1 + d_2$ が成立する．強正則グラフに対しては，この不等式の等号が成り立つ．では逆に，この不等式の等号を達成する様なグラフは，どの様なものがあるのかという問題が考えられる．もし，その極小次元の埋め込みたちが，どちらも球面に乗るならば，強正則グラフであることが分かった．

Theorem 4.1 (野崎–篠原). G の極小次元の埋め込み X_1 の次元を d_1，その補グラフの極小次元の埋め込み X_2 の次元を d_2 とする．X_1, X_2 の両方が球面に乗りかつ，$n = 1 + d_1 + d_2$ を満たすならば，G は強正則グラフとなる．

5 これからの問題

等式 $n = 1 + d_1 + d_2$ を満たしかつ，極小次元埋め込みが球面に乗るときは，強正則グラフであると特徴づけられたが，$n = 1 + d_1 + d_2$ を満たし，埋め込みが球面に乗らないときは，どの様なグラフが存在しているのだろうか．$n = 1 + d_1 + d_2$ を満たすグラフの埋め込みに対して次のようなことが分かった．

Theorem 5.1. G を $n = 1 + d_1 + d_2$ を満たす単純グラフであるとする．そのとき，極小次元の埋め込み X_1, X_2 は適当に原点を選ぶことで，ウエイト一定の *Euclidean 2-design* となる．

強正則グラフの埋め込みは spherical 2-design であり，Euclidean 2-design はその一般化にあたる．この章では，強正則グラフ以外で $n = 1 + d_1 + d_2$ となる発見された例を紹介する．

Example 5.2. K_{n_1}, K_{n_2} を異なるサイズ（$n_1 \neq n_2$）の完全グラフであるとする．そのとき，disjoint union $K_{n_1} \cup K_{n_2}$ は $n = 1 + d_1 + d_2 (= n_1 + n_2)$ を満たす．実際に，$d_1 = n - 2$ (Type (5)), $d_2 = 1$ (Type (1)) となっている．

Example 5.3. Lisoněk [3] が与えた $\mathbb{R}^8$ 上の 45 点 2-距離集合（Type (3)）は $n = 1 + d_1 + d_2$ を満たしている．このとき，補グラフの埋め込みとして，$\mathbb{R}^{36}$ 上の 2-距離集合（Type (4)）が存在している．

Example 5.4. Lisoněk [3] は距離の比が黄金比になる元の個数が最大の距離集合を小さい次元で分類している．$\mathbb{R}^4$ 上では 9 点の 2-距離集合が同型を除いて 3 種類（すべて Type (3)）与えられていた．それに付随するグラフをそれぞれ G_1, G_2, G_3 とする．このとき，$G_1 = \bar{G}_1$, $G_2 = \bar{G}_3$ となっている．よって，それらのグラフは，$n = 1 + d_1 + d_2$ を満たしている．

強正則グラフの埋め込みは，spherical 2-design かつ 2-距離集合であり，逆に spherical 2-design かつ 2-距離集合は強正則グラフの構造を持つことが Delsarte–Goethals–Seidel [1] により示されている．$n = 1 + d_1 + d_2$ を満たす Examples 5.2, 5.3, 5.4 は，コヒアラント配置（強正則グラフの一般化）の構造を持つことが観察できる．一般に Eulidean 2-design かつ 2-距離集合である，ユークリッド空間上の有限集合に対して，コヒアラント配置の構造をもつと結論付けることが出来るだろうか．また，今のところ具体例が多くないため，具体例の構成も今後の課題である．

References

[1] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), no. 3, 363–388.

[2] S.J. Einhorn and I.J. Schoenberg, On euclidean sets having only two distances between points. I. II. *Nederl. Akad. Wetensch. Proc. Ser. A* 69=*Indag. Math.* 28 (1966), 479–488, 489–504.

[3] P. Lisoněk, New maximal two-distance sets, *J. Combin. Theory, Ser. A* 77 (1997), 318–338.

[4] A. Roy, Minimal Euclidean representation of graphs, *Discrete math.* 310 (2010), 727–733.

[5] I.J. Schoenberg, Remarks to Maurice Fréchet's article "Sur la définition axiomatique d'une classe d'espace distanciés vectoriellement applicable sur l'espace de Hilbert", *Ann. of Math.* (2) 36 (1935), no. 3, 724–732.

Diagonal forms of incidence matrices associated with t-uniform hypergraphs

Richard M. Wilson and Tony W. H. Wong
California Institute of Technology

The 28th Symposium on Algebraic Combinatorics, June 20–22, 2011, Oita University

Abstract

This paper is a summary of a talk given by the first author at the 28th Symposium on Algebraic Combinatorics at Oita University in 2011. We introduce Smith form and diagonal form of integer matrices and explain the connection to solving systems of linear equations in integers. Previous results on a diagonal form for a $(0,1)$-incidence matrix arising from a t-uniform hypergraph are generalized and applied to a certain zero-sum Ramsey-type problem. Proofs are not given here but will appear elsewhere [14].

1 Smith and diagonal form

Two integer matrices A and B of the same size are $\mathbb{Z}$-equivalent when there exist unimodular matrices (square integer matrices that have integer inverses, or what is the same have determinants ± 1) E and F so that $EAF = B$. This is equivalent to stating that B can be obtained from A by a sequence of $\mathbb{Z}$-row operations and $\mathbb{Z}$-column operations (permuting rows/columns, adding an integer multiple of one row or column to another row or column, or multiplying a row or column by -1).

Given A, there is a unique diagonal integer matrix D that is $\mathbb{Z}$-equivalent to A such that the diagonal entries $d_1, d_2, d_3, \ldots$ are nonnegative integers and where d_i divides d_{i+1} for $i = 1, 2, \ldots$. Here 'diagonal' means that the (i,j)-entry of D is 0 unless $i = j$, but D has the same shape as A and is not necessarily square. This unique diagonal matrix is called the *integer Smith normal form*, or simply the *Smith form*, of A. (The Smith form D is unique; the unimodular matrices E and F so that $EAF = D$ are not. See any advanced text on modern algebra for proofs of existence and uniqueness.)

The diagonal entries of the Smith form, in the order of divisibility (with all 0's necessarily at the end) are called the *invariant factors*, or the *elementary divisors* of A.

As a simple example, the Smith form of $A = \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix}$ is $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$ because

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 \\ 1 & -1 & -1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}.$$

The invariant factors of A are 1 and 5.

We call any diagonal matrix D that is $\mathbb{Z}$-equivalent to A a *diagonal form* for A.

The connection between the Smith form and diagonal forms of a matrix A is as follows. Integers $d_1, d_2, \ldots, d_r$ are the diagonal entries of a diagonal form for A if and only if

$$\mathbb{Z}^r/\mathrm{col}_{\mathbb{Z}}(A) \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r},$$

where $\mathrm{col}_{\mathbb{Z}}(A)$ is the $\mathbb{Z}$-module (abelian group) generated by the columns of A. (Of course, $\mathbb{Z}_1 = \{0\}$ and $\mathbb{Z}_0 = \mathbb{Z}$.) There are unique nonnegative integers $s_1, \ldots, s_r$ so that s_i divides s_{i+1} and such that the above group is isomorphic to $Z_{s_1} \oplus \cdots \oplus Z_{s_r}$, and these are the invariant factors of A.

As we have defined them above, the number of invariant factors of a matrix A, or the number of diagonal entries of a diagonal form of A, is equal to the minimum of the number of rows and the number of columns of A. But there are numerous times when it is desirable to consider the number of invariant factors to be equal to, say, the number n of columns of a k by n matrix A even if $k < n$. In this case, the invariant factors s_i with $k < i \leq n$ are to be understood as 0. This agrees with the result when $n-k$ or more rows of all zeros are appended to A (and this does not change the $\mathbb{Z}$-span of the rows). To illustrate with the example above),

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 \\ 1 & -1 & -1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now the invariant factors of the middle matrix on the left are $1, 5, 0$. The context should make it clear whether we are thinking of k or n as the number of invariant factors.

The Smith form of A may be obtained from any diagonal form D of A by a sequence of operations that replace two diagonal entries a and b by $g = \gcd(a, b)$ and $ab/g = \mathrm{LCM}(a, b)$. This can be effected by $\mathbb{Z}$-row and column operations, as we indicate by the sequence of 2 by 2 matrices below. First write $g = sa + tb$ with s and t integral.

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & tb \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & sa+tb = g \\ 0 & b \end{pmatrix} \to$$

$$\begin{pmatrix} a & g \\ -ab/g & 0 \end{pmatrix} \to \begin{pmatrix} 0 & g \\ -ab/g & 0 \end{pmatrix} \to \begin{pmatrix} g & 0 \\ 0 & ab/g \end{pmatrix}$$

2 The Smith (or diagonal) form in combinatorics

The invariant factors, and hence the rank modulo p, of a matrix A do not change on permutation of the rows and columns (or transposition) of a

matrix. Thus they do not depend on the ordering of the vertices when A is the adjacency matrix of a graph G, or on the ordering of points and blocks when A is the incidence matrix of some design S, etc. The invariant factors of the adjacency matrix of a graph G, or the incidence matrix of S, are therefore *invariants* of G or S, respectively; they are the same for two isomorphic graphs or incidence structures.

So, for example, two graphs may be shown to be nonisomorphic by showing that their adjacency matrices have different invariant factors. Brouwer and Van Eijl [2] give Smith forms or p-ranks for various strongly regular graphs with the same parameters but different invariant factors. For example, there are four nonisomorphic graphs that are strongly regular graphs with the same parameters as the triangular graph $T(8)$. One is $T(8)$ itself and the other three are called the Chang graphs. The invariant factors of each of the three Chang graphs are 1^8, 2^{12}, 8^7, 24^1, and these are different from those of $T(8)$.

Another example is the two Hadamard matrices of order 36 in N. J. A. Sloane's table [8] called "had.36.pal2" and "had.36.will". These can be downloaded and the invariant factors computed as

$$1^1,\ 2^{17},\ 18^{17},\ 36^1 \quad \text{and} \quad 1^1,\ 2^{15},\ 6^4,\ 18^{15},\ 36^1,$$

respectively. The computation shows instantly that the matrices are not equivalent (under row and column permutations and/or multiplication of rows or columns by -1).

We remark that the invariant factors of "random" square integer matrices (including e.g. n by n matrices of 0's and 1's) tend to be 1's followed by a single large factor. But matrices arising from combinatorial designs often have more interesting invariant factors. See [13] for more on diagonal forms of incidence matrices of designs.

Here we will be interested in the subject of the following section.

3 Solutions of linear systems in integers and modulo p

Diagonal forms are related to solutions of systems of linear equations or congruences in integers. This, in fact, was the topic of H. J. S. Smith's original paper on the subject.

Let A be an r by m integer matrix. Suppose $EAF = D$ where E and F are unimodular and D is diagonal with diagonal entries $d_1, d_2, \ldots$. The system $A\mathbf{x} = \mathbf{b}$ is equivalent to $(AF)(F^{-1}\mathbf{x}) = \mathbf{b}$, and this has integer solutions $\mathbf{x}$ if and only if $(AF)\mathbf{z} = \mathbf{b}$ has an integer solution $\mathbf{z}$. This in turn will have integer solution if and only if $EAF\mathbf{z} = E\mathbf{b}$, or $D\mathbf{z} = E\mathbf{b}$, has integer solutions.

In other words, if we let $\mathbf{e}_i$ denote the i-th row of E, the system $A\mathbf{x} = \mathbf{b}$ has integer solutions if and only if

$$\mathbf{e}_i\mathbf{b} \equiv 0 \pmod{d_i} \quad \text{for } i = 1, 2, \ldots, r.$$

As a simple example,

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 \\ 1 & -1 & -1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

and so the system of equations

$$\begin{cases} 3x + y + 4z = a \\ 4x - 2y + 7z = b \end{cases}$$

has an integer solution if and only if $a \equiv 0 \pmod 1$ (that is, a is an integer) and $2a + b \equiv 0 \pmod 5$.

A similar argument proves the following lemma.

Lemma 1 *Let A be an integer matrix and $\mathbf{c}$ a integer row vector. Assume $EAF = D$ where E and F are unimodular and D diagonal with diagonal entries d_j, $j = 1, 2, \ldots, n$.* (i) *The equation $\mathbf{y}A = \mathbf{c}$ has an integer solution $\mathbf{y}$ if and only if the j-th entry of $F\mathbf{c}$ is divisible by d_j for every j.* (ii) *Given a prime p, the system of congruences $\mathbf{y}A \equiv \mathbf{c} \pmod p$ has an integer solution $\mathbf{y}$ if and only if the j-th entry of $F\mathbf{c}$ is divisible by p whenever p divides d_j.*

4 Diagonal form of certain inclusion matrices

For integers t, k, n with $0 \le t \le k \le n$, let W_{tk} or $W_{tk}(n)$ denote the $\binom{n}{t}$ by $\binom{n}{k}$ matrix whose rows are indexed by the t-subsets of an n-set X, whose columns are indexed by the k-subsets of X, and where the entry in row A and column B is

$$W_{tk}(A, B) := \begin{cases} 1 & \text{if } A \subseteq B, \\ 0 & \text{otherwise.} \end{cases}.$$

For example, the matrix $W_{23}(6)$ is shown below.

$$\begin{array}{c} \{1,2\} \\ \{1,3\} \\ \{2,3\} \\ \{1,4\} \\ \{2,4\} \\ \{3,4\} \\ \{1,5\} \\ \{2,5\} \\ \{3,5\} \\ \{4,5\} \\ \{1,6\} \\ \{2,6\} \\ \{3,6\} \\ \{4,6\} \\ \{5,6\} \end{array} \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The columns are indexed by the 3-subsets $\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \ldots, \{4,5,6\}$.

Theorem 2 (Wilson [9]) *Given t, k, n with $t \leq k \leq n-t$, one diagonal form for $W_{tk}(n)$ has diagonal entries*

$$\binom{k}{t}^1, \binom{k-1}{t-1}^{n-1}, \binom{k-2}{t-2}^{\binom{n}{2}-n}, \ldots, \binom{k-t}{0}^{\binom{n}{t}-\binom{n}{t-1}}.$$

(Here the exponents indicate multiplicities.)

For example, a diagonal form for $W_{23}(6)$ has diagonal entries

$$3,\ 2,\ 2,\ 2,\ 2,\ 2,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1.$$

This was later generalized matrices arising for t-uniform hypergraphs as follows.

Given H be a t-uniform hypergraph on n vertices X, let $N_t(H)$ be the matrix whose rows are indexed by the $\binom{n}{t}$ t-subsets of X, whose columns are indexed by the images of H under the symetric group S_n, and where the entry in row T and column H' is 1 if T is an edge of H' and 0 otherwise.

For example, let $n = 4$, $t = 2$, and let G be a path-graph of length 2 plus an isolated vertex. Then $N_2(G)$ is the 6×12 matrix partially shown below. Here abc denotes the path-graph with edges $\{a,b\}$ and $\{b,c\}$.

	213	214	314	123	124	324	132	234	134	...
$\{1,2\}$	1	1	0	1	1	0	...			
$\{1,3\}$	1	0	1	0	0	0	...			
$\{1,4\}$	0	1	1	0	0	0	...			
$\{2,3\}$	0	0	0	1	0	1	...			
$\{2,4\}$	0	0	0	0	1	1	...			
$\{3,4\}$	0	0	0	0	0	0	...			

The matrix $W_{23}(6)$ is equal to $N_2(G)$ where G is the graph (2-uniform hypergraph) on six vertices consisting of a triangle and three isolated vertices. In general, the matrix $W_{tk}(n)$ is $N_t(H)$ where H is a complete t-uniform hypergraph on k vertices plus $n-k$ isolated vertices. In notation to be used later,

$$W_{tk}(n) = N_t((K_k^{(t)})^{\uparrow n}).$$

Theorem 3 (Wilson [11]) *Suppose a t-uniform hypergraph H has at least t isolated vertices. Then one diagonal form for $N_t(H)$ has diagonal entries*

$$(g_0)^1,\ (g_1)^{n-1},\ (g_2)^{\binom{n}{2}-n} \ldots,\ (g_t)^{\binom{n}{t}-\binom{n}{t-1}}.$$

where g_i is the gcd *of all entries of $W_{it}N_t$.*

This talk deals with the case when H does not have as many as t isolated vertices.

One instance of the matrix $N_2(G)$ for a graph without two isolated vetices in the lierature is a result of Brouwer and Van Eijl that gives the Smith form of the adjacency matrix of the line graph of K_m, which is $H_2(G)$ when $G = K_{2,m-2}$ and $n = \binom{m}{2}$. Here there are no isolated vertices.

Theorem 4 (Brouwer and Van Eijl [2]). *Let A be the adjacency matrix of the line graph of K_m. Then a diagonal form for A has diagonal entries*

$$(1)^{n-2}, \quad (2)^{\binom{n}{2}-2n+2}, \quad (h)^1, \quad (2g)^{n-2}, \quad (mg/h)^1.$$

where

$$m = 2(n-2), \quad g = n-4, \quad h = \gcd\{2, n-2\}.$$

(A diagonal form for the adjacency matrix of the complement of $L(K_m)$ follows from Theorem 3.)

5 The matrices $N_t(\mathbf{h})$

It is convenenient to consider more general integer matrices, where the columns are images of a single column vector under and action of S_n. Fix t and consider integer column vectors $\mathbf{h}$ where the coordinates of $\mathbf{h}$ are indexed by the t-subsets of an n-set X. We may call such a vector $\mathbf{h}$ a *t-vector* based on the set X. By $N_t(\mathbf{h})$ we mean the matrix whose rows are indexed by the t-subsets of X and whose columns are the images $\mathbf{h}'$ of $\mathbf{h}$ under the symmetric group S_n acting on the t-subsets of X.

An example when $n = 3$ and $t = 1$ is

$$N_1 = \begin{pmatrix} 3 & 5 & 9 & 3 & 5 & 9 \\ 5 & 9 & 3 & 9 & 3 & 5 \\ 9 & 3 & 5 & 5 & 9 & 3 \end{pmatrix}.$$

This matrix has invariant factors $34, 2, 1$.

Normally, one need only use the *distinct* images of $\mathbf{h}$ as the columns of N_t, but, for our purposes, it will not matter if N_t has repeated columns. In fact, it is sometimes convenient for the purposes of induction to assume that N_t has $n!$ columns indexed by the set of all permutations of X.

Examples of N_t are integer matrices in the association algebras of Johnson schemes $J(m,t)$.

Given a t-uniform hypergraph with vertex set X, let $N_t(H) = N_t(\mathbf{h})$ where $\mathbf{h}$ is the *characteristic t-vector* of H. Here $\mathbf{h}$ is a $(0,1)$-vector.

Theorem 3 remains valid for $N_t(\mathbf{h})$ where $\mathbf{h}$ is any t-vector with at least t isolated vertices [11]. The g_i's are defined the same: g_i is the gcd of all

entries of $W_{it}N_t(\mathbf{h})$, which is the same as the gcd of the entries of a single column $W_{it}\mathbf{h}$.

A Smith form in the case $t = 1$ is given by the following easy theorem.

Theorem 5 *Let* $\mathbf{h}$ *be the* 1*-vector* $[a_1, a_2, \ldots, a_n]^\top$. *Then a diagonal form for the* $n \times n!$ *matrix* $N_1(\mathbf{h})$ *is*

$$\begin{pmatrix} mg/h & 0 & 0 & \ldots & 0 & 0 \\ 0 & g & 0 & \ldots & 0 & 0 \\ 0 & 0 & g & \ldots & 0 & 0 \\ \vdots & & & \ddots & \vdots & \\ 0 & 0 & 0 & \ldots & g & 0 \\ 0 & 0 & 0 & \ldots & 0 & h \end{pmatrix},$$

where

$$\begin{aligned} m &= a_1 + \cdots + a_n, \\ h &= \gcd(a_1, \ldots, a_n), \quad \textit{and} \\ g &= \gcd_{1 \le i,j \le n}(a_i - a_j). \end{aligned}$$

6 A zero-sum Ramsey-type problem

The following problem was introduced by N. Alon and Y. Caro [1] in 1993. Given a simple t-uniform hypergraph H on k vertices and a prime p which divides the number of edges of H, determine the least integer $n \ge k$ (called $R_p(H)$) so that the row space over $\mathbb{F}_p$ of $N_t(H^{\uparrow n})$ does not contain a nowhere-zero vector. In particular, $R_2(H)$ is the least integer n so that the binary code generated by $N_t(H^{\uparrow n})$ does not contain the vector $\mathbf{1}$ of all ones.

Here $H^{\uparrow n}$ is the hypergraph obtained by adjoing isolated vertices to get a total of n vertices.

This is our terminology. Alon and Caro originally asked for the least integer $R_p(H)$ so that if $n \ge R_p(H)$ and the edges of the complete t-uniform hypergraph $K_n^{(t)}$ on n vertices are colored with the elements of $\mathbb{F}_p$, then there exists a subhypergraph H' isomorphic to H so that the sum of the colors on the edges of H' is 0 modulo p.

(It follows from the classical Ramsey's Theorem that such an integer exists when p divides the number of edges of H.)

Theorem 6 (Y. Caro [3]) *When* $\binom{k}{t}$ *is even,* $R_2(K_k^{(t)}) \le k + t$.

In [12], the value of $R_2(K_k^{(t)})$ was given exactly and the following proved.

Theorem 7 (Wilson [12]) *For any* t*-uniform hypergraph* H *with* k *vertices and an even number of edges,* $R_2(H) \le k + t$.

Theorem 7 is proved using results from [11] about diagonal forms of incidence matrices $N_t = N_t(H)$. One motivation for the current work is to use this approach to give an alternate proof of the following theorem of Y. Caro.

Theorem 8 (Y. Caro [4]) *Let G be a simple graph with k vertices and an even number of edges. Then*

$$R_2(G) = \begin{cases} k+2 & \text{if } G \text{ is complete,} \\ k+1 & \text{if } G \text{ is the union of two complete graphs,} \\ k+1 & \text{if } G \neq K_k \text{ has all vertices of odd degree,} \\ k & \text{otherwise.} \end{cases}$$

Thus it is rare when $R_2(G) \neq k$.

Our idea is to use a diagonal form of the matrix $N_t(H^{\uparrow n})$ and Lemma 1 to answer the question of whether $\mathbf{1}$ is in the row space of $N_t(H^{\uparrow n})$ modulo p, or what is the same, whether the congruence $\mathbf{y}N_t \equiv \mathbf{1} \pmod{p}$ has a solution $\mathbf{y}$. This would give us information about $R_2(H)$. We prove Theorems 10 and 14 below using this idea.

Lemma 1, however, requires not only a diagonal form D for a matrix A, but also unimodular matrices E and F so that $EAF = D$. We must know something about these unimodular matrices for our proofs. But to save space in this paper, we omit all mention of these matrices.

7 New results

Let $\mathbf{h}$ be an t-vector based on a set X. We say that $\mathbf{h}$ is *primitive* when the gcd of $\langle \mathbf{f}, \mathbf{h} \rangle$ over all integer t-vectors $\mathbf{f}$ in the null space of $W_{t-1,t}$ is equal to 1. In general, we say that the gcd γ of all entries of $M_{t-1,t}N_t$ is the *index of primitivity* of $\mathbf{h}$. We say that a t-uniform multihypergraph H is primitive when its characteristic t-vector is primitive. It should be noted that the primitivity of a hypergraph may change when isolated vertices are added or deleted. In general, an *isolated vertex* of a t-vector $\mathbf{h}$ is a point $x \in X$ so that $\mathbf{h}(T) = 0$ for all t-subsets $T \subseteq X$ with $\mathbf{x} \in T$.

The *shadow* of a t-vector $\mathbf{h}$ is the $(t-1)$-vector $W_{t-1,t}\mathbf{h}$ and the j-th shadow is $W_{t-j,t}\mathbf{h}$. In particular, the shadow of a graph is the vector (1-vector) of its degrees.

Theorem 9 ([14]) *If a t-vector $\mathbf{h}$ and all of its shadows $\mathbf{h}^{(j)}$, $j = 0, 1, 2, \ldots, t$, are primitive or multiples of primitive t-vectors, then the diagonal entries of one diagonal form for $N_t(\mathbf{h})$ are given by*

$$(g_0)^1,\ (g_1)^{n-1},\ (g_2)^{\binom{n}{2}-n} \ldots,\ (g_t)^{\binom{n}{t}-\binom{n}{t-1}},$$

where, as above, g_i is the gcd *of all entries of $W_{it}N_t(\mathbf{h})$.*

Theorem 10 *If a t-uniform hypergraph H and all of its shadows are primitive or multiples of primitive multihypergraphs, and if p divides g_0, the number of edges of H, then $\mathbf{1} \notin \mathrm{row}_p(N_t(H))$. Hence $R_2(H) \leq k + t$.*

It can be seen that every t-uniform hypergraph with at least t isolated vertices is primitive or a multiple of a primitive t-uniform hypergraph, Thus Theorem 7 is a consequence of Theorem 10.

Integer vectors in the null space of W_{tk} are called *null designs* or *trades*. This module is generated over $\mathbb{Z}$ by vectors of a certain type that were called (t,k)-*pods* by Graver and Jurkat [6], *cross-polytopes* by Graham, Li, and Li [5], and *minimal trades* by Khosravshahi et. al. [7]. For our purposes, we need only to know a generating set for the integer null space of $W_{t-1,t}$, and we restrict our attention to this case. Here, we describe these vectors only for $t = 0, 1, 2$.

The $\mathbb{Z}$-null space of $W_{01} = [1, 1, \ldots, 1]$ is generated by 1-vectors of the form $\mathbf{h}$ where

$$\mathbf{h}(\{i\}) = 1, \quad \mathbf{h}(\{j\}) = -1, \quad \mathbf{h}(\{\ell\}) = 0 \ \text{ otherwise,}$$

and where i and j are distinct points.

The $\mathbb{Z}$-null space of W_{12} is generated by 2-vectors of the form $\mathbf{g}$ where

$$\mathbf{g}(\{a,b\}) = \mathbf{g}(\{c,d\}) = 1, \quad \mathbf{g}(\{b,c\}) = \mathbf{g}(\{d,a\}) = -1,$$

$$\mathbf{g}(\{x,y\}) = 0 \ \text{ otherwise,}$$

where a, b, c, d are four distinct vertices.

A 1-vector $\mathbf{h}$ based on $X = \{1, 2, \ldots, n\}$ is primitive when the gcd of the quantities $\mathbf{h}(i) - \mathbf{h}(j)$ is 1.

A graph (or signed multigraph) G, or 2-vector $\mathbf{g}$, is primitive when the gcd of the quantities

$$\mathbf{g}(\{a,b\}) + \mathbf{g}(\{c,d\}) - \big(\mathbf{g}(\{b,c\}) + \mathbf{g}(\{d,a\})\big)$$

over all choices of four distinct vertices a, b, c, d is 1.

A 3-uniform hypergraph H or 3-vector $\mathbf{h}$ is primitive when the gcd of all quantities

$$\begin{aligned} &\mathbf{h}(a_1,a_2,a_3) + \mathbf{h}(a_1,b_2,b_3) + \mathbf{h}(b_1,a_2,b_3) + \mathbf{h}(b_1,b_2,a_3) \\ &- \Big(\mathbf{h}(b_1,b_2,b_3) + \mathbf{h}(b_1,a_2,a_3) + \mathbf{h}(a_1,b_2,a_3) + \mathbf{h}(a_1,a_2,b_3)\Big) \end{aligned}$$

over all choices of six distinct vertices $a_1, a_2, a_3, b_1, b_2, b_3$ is 1.

8 Diagonal forms for simple graphs

Theorem 11 ([14]) *A simple graph G is primitive unless G is isomorphic to a complete graph, an edgeless graph, a complete bipartite graph, or the disjoint union of two complete graphs.*

Theorem 9 does not immdiately give us a diagonal form for $N_2(G)$ for primitive graphs G because the shadow of a primitive graph (the 1-vector that gives the degrees of its vertices) may not be primitive; for example, G may be regular.

Theorem 12 *Let G be a primitive simple graph with m edges and degrees $\delta_1, \delta_2, \ldots, \delta_n$. Let h denote the* gcd *of the degrees δ_i and m; let g denote the* gcd *of all differences $\delta_i - \delta_j$, $i, j = 1, 2, \ldots, n$. Then the invariant factors of $N_2(G)$ are*

$$(1)^{\binom{n}{2}-n}, \quad (h)^1, \quad (g)^{n-2}, \quad (mg/h)^1.$$

Thus for the Petersen graph P ($n = 10$), $N_2(P)$ has diagonal form entries 1^{35}, 3^1, 0^8, 15^1, while for the graph P_1 ($n = 11$) consisting of the Petersen graph plus an isolated vertex, $N_2(P)$ has invariant factors 1^{44}, 3^{10}, 15^1.

Nonprimitive graphs may be considered separately. Here is one case.

Theorem 13 *Let G be the complete bipartite graph $K_{r,n-r}$, where $2 \le r \le n-2$. Define m, g, and h as in the statement of Theorem 12, so in this case*

$$m = r(n-r), \quad g = n - 2r, \quad h = \gcd\{r, n-r\}.$$

Then the diagonal entries of one diagonal form for $N_2(G)$ are

$$(1)^{n-2}, \quad (2)^{\binom{n}{2}-2n+2}, \quad (h)^1, \quad (2g)^{n-2}, \quad (mg/h)^1.$$

In the case $r = 2$, the matrix N_2 is square; it is the adjacency matrix of the line graph of the complete graph K_n, and we have reproved the result of Brouwer and Van Eijl [2] (the case $r = 2$).

Theorem 14 *Given a simple graph G with at least four vertices and a prime p such that $p|m$, $\mathbf{1}$ is in the row space of $N_2(G)$ over $\mathbb{F}_p$ if and only if either of the following holds:*

(i) *G is primitive with $p|g$ but $p \nmid h$,*

(ii) *$G = K_n$,*

(iii) *$G = K_{1,n-1}$ with $p > 2$,*

(iv) *$G = K_1 \sqcup K_{n-1}$ with $p \nmid n-2$ or $p = 2$,*

(v) *$G = K_r \sqcup K_{n-r}$, $2 \le r \le \frac{n}{2}$, with ($p|g$ but $p \nmid h$) or $p = 2$.*

References

[1] N. Alon and Y. Caro, On three zero-sum Ramsey-type problems, *J. Graph Th.* **17** (1993), 177–192.

[2] A. E. Brouwer and C. A. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, *J. Alg. Combinatorics* **1** (1992), 329–346.

[3] Y. Caro, A complete characterization of the zero-sum (mod 2) Ramsey Numbers, *J. Combinat. Thy. Ser. A* **68** (1994), 205–211.

[4] Y. Caro, Binomial coefficients and zero-sum Ramsey numbers, *J. Combinatorial Th., Series A* **80** (1997), 367–373.

[5] R. L. Graham, S.-Y. R. Li, and W.-C. W. Li, On the structure of t-designs, *SIAM J. Alg. Disc. Meth.* **1** (1980), 8–14.

[6] J. E. Graver and W. B. Jurkat, The module structure of integral designs, *J. Combinatorial Theory* **15** (1973), 75–90.

[7] G. B. Khosrovshahi and Ch. Maysoori, On the bases for trades, Linear Algebra and its Appl., **226–228** (1995), 731–748.

[8] Neil J. A. Sloane, A Library of Hadamard Matrices, http://www2.research.att.com/~njas/hadamard/ (accessed 20 June 2010).

[9] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combinatorics* **11** (1990), 609–615.

[10] Richard M. Wilson, On set systems with restricted intersections modulo p and p-ary t-designs. Discrete Math. **309** (2009), 606–612.

[11] Richard M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices. Des. Codes Cryptogr. **17** (1999) 289–297.

[12] Richard M. Wilson, Some applications of incidence matrices of t-subsets and hypergraphs, Proceedings of the Third Shanghai Conference on Combinatorics, *Discrete Math.*, to appear.

[13] Richard M. Wilson, Codes and modules associated with designs and t-uniform hypergraphs, p.404–436 in: Information Security, Coding Theory, and Related Combinatorics, Dean Crnković and Vladimir Tonchev, eds., Nato Science for Peace and Security Series D Vol. 29, IOS Press, 2010.

[14] Richard M. Wilson and Tony W. H. Wong, Diagonal forms for incidence matrices arising from t-uniform hypergraphs, to appear.

Mutually orthogonal partial t-designs over $\mathbb{C}$ related to quantum jump codes

Masakazu Jimbo, Nagoya University
jimbo@is.nagoya-u.ac.jp
and
Keisuke Shiromoto, Kumamoto University
keisuke@kumamoto-u.ac.jp

The 28th Symposium on Algebraic Combinatorics, June 20-22, 2011, Oita University

Abstract

A quantum jump code was introduced by Alber *et al.* (2001). It has a close connection with combinatorial designs.

A combinatorial design $(V, \mathcal{B})$ is considered as a map $f : \binom{V}{k} \to \{0, 1\}$ according as a block $B \in \binom{V}{k}$ being a member of block set $\mathcal{B}$ or not. In this paper, firstly, we define a family of mutually orthogonal partial t-designs (t-MOD) $\{(V, f_i) | i = 1, 2, \ldots, m\}$ with membership functions $f_i : \binom{V}{k} \to \mathbb{C}$, which is "equivalent" to a quantum jump code. An upper bound for the number of designs was given by Beth *et al.* (2003). Secondly, we derive a sharp bound of t-MODs for a series of parameters and also give a construction of t-MODs attaining the bound.

1 Mutually orthogonal partial t-designs over $\mathbb{C}$

Let V be a v-set and $0 < k \leq v$ be an integer. Let $f : \binom{V}{k} \to \mathbb{C}$ be a map, where $\mathbb{C}$ is the set of complex numbers. A pair (V, f) is called a *configuration* over $\mathbb{C}$ and f is called the *membership function* of a configuration (V, f). If we restrict the image of f to $\{0, 1\} (\subset \mathbb{C})$, (V, f) is called a *binary* configuration.

An *inner product* of two configurations (V, f_1) and (V, f_2) is defined by

$$f_1 \cdot f_2 = \sum_{B \in \binom{V}{k}} \overline{f}_1(B) f_2(B),$$

where $\overline{f}$ is the complex conjugate of f. The *norm* of a configuration (V, f) is defined by $\|f\| = \sqrt{f \cdot f}$.

For a configuration (V, f), let $0 \leq \ell < k$ be an integer and E be an ℓ-subset of V. For $B' \in \binom{V \setminus E}{k-\ell}$, we define $f|_E(B') = f(B' \cup E)$.

$(V \setminus E, f|_E)$ is called a *derived* (or *induced*) configuration by E of (V, f).

Note that $f|_\emptyset = f$ for $E = \emptyset$.

A *normalized membership function* is defined by:

$$f^*|_E = \begin{cases} \frac{f|_E}{\|f\|}, & \text{if } \|f\| > 0, \\ 0, & \text{if } \|f\| = 0, \end{cases}$$

For a positive integer $t \leq k$, let $\mathcal{T} = \cup_{\ell=0}^{t} \binom{V}{\ell}$ and fix an *index function* $\mu : \mathcal{T} \to \mathbb{R}_{\geq}$, where $\mathbb{R}_{\geq}$ is the set of nonnegative real numbers.

For a family of m configurations (V, f_i) $(i = 1, 2, \ldots, m)$, $(V; f_1, \ldots, f_m)$ is called a *family of mutually orthogonal t-designs*, denoted by t-$[v, k, \mu; m]$ *MOD*, if for any $E \in \mathcal{T}$ and for any i and j,

$$f_i^*|_E \cdot f_j^*|_E = \frac{f_i|_E \cdot f_j|_E}{\|f_i\| \, \|f_j\|} = \delta_{ij}\mu(E)$$

holds.

Especially, if we restrict the image of f_i to $\{0, 1\}$, a t-MOD is said to be *binary*. In this case, we can identify f_i with $\mathcal{B}^{(i)} = \{B | f_i(B) = 1\}$. Hence, a t-MOD $(V; f_1, \ldots, f_m)$ is also written by $(V; \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)})$.

A t-MOD with $m = 1$ is called a t-$[v, k, \mu]$ *design*. Especially, if $\mu(E)$ depends only on the size of E, that is, $\mu(E) = c_{|E|}$, then the index function μ is completely determined only by c_t. Hence we write it as t-$[v, k, c_t]$.

Lemma 1 A t-$[v, k, c_t]$ design is a $(t-1)$-$[v, k, c_{t-1}]$ design where $c_{t-1} = \frac{v-t+1}{k-t+1} c_t$.

When we restrict the image of f to $\{0, 1\}$, (V, f) is a usual (binary) t-(v, k, λ) design with $\lambda = c_t \|f\|^2$.

A t-$[v, k, \mu; m]$ MOD is also called a $(v, m, t)_k$-*quantum jump code* or a t-error correcting quantum jump code with length v, dimension m and weight k.

Especially, if we restrict the image of f to $\{0, 1\}$, a $(v, m, t)_k$-quantum jump code is called a *t-SEED* (*t-spontaneous emission error design*), denoted by t-$(v, k; m)$ *SEED*. For quantum jump codes, see [1, 2, 3, 4, 5].

Example 1 Let $V = \{0, 1, \ldots, 6\}$ and define f_i's as follows:

| | | |

Example 2 Let $V = \{0,1,2,3,4,5\}$ and define f_1 and f_2 as follows:

f_1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
f_2	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	0	1	0	1	0	1	1	1	0	0	1	0	1	0
2	1	1	0	0	0	1	1	0	1	0	0	0	1	1	1	0	0	1	0	1
3	0	1	1	0	0	0	1	1	0	1	1	0	0	1	1	1	0	0	1	0
4	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	0	1	0	0	1
5	0	0	0	1	1	0	1	0	1	1	1	1	1	0	0	1	0	1	0	0

Then $(V; f_1, f_2)$ is a 2-$[6, 3, \frac{2}{10}; 2]$ MOD.

Example 3 In Example 2 define f_1 and f_2 as follows:

f_1	$\sqrt{3}$	1	1	1	1	1	1	1	1	1	$\sqrt{3}$	1	1	1	1	1	1	1	1	1
f_2	$-\sqrt{3}$	1	-1	-1	1	1	-1	-1	-1	-1	$\sqrt{3}$	-1	1	1	-1	-1	1	1	1	1
0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
1	1	0	0	0	1	1	0	1	0	1	0	1	1	1	0	0	1	0	1	0
2	1	1	0	0	0	1	1	0	1	0	0	0	1	1	1	0	0	1	0	1
3	0	1	1	0	0	0	1	1	0	1	1	0	0	1	1	1	0	0	1	0
4	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	0	1	0	0	1
5	0	0	0	1	1	0	1	0	1	1	1	1	1	0	0	1	0	1	0	0

Then $(V; f_1, f_2)$ is a 2-$[6, 3, \mu; 2]$ MOD. Actually, $\|f_i\|^2 = 24$ and

$$\mu(E) = \begin{cases} \frac{12}{24}, & \text{for } |E| = 1, \\ \frac{6}{24}, & \text{for } |E| = 2,\ |E \cap \{0,1,2\}| = 2, \text{ or } 0, \\ \frac{4}{24}, & \text{for } |E| = 2,\ |E \cap \{0,1,2\}| = 1. \end{cases}$$

It is readily checked that $f_1|_E \cdot f_2|_E = 0$ holds for $|E| \leq 2$. Hence, this design is a 2-MOD of "group divisible" type.

2 Fundamental properties and an upperbound of a t-MOD

For the results below, we refer the reader to Beth *et al.* [2].

Lemma 2 (Complement design) For a $(V; f_1, \cdots, f_m)$ is a t-$[v, k, \mu; m]$ MOD, let $f_i^c(B) = f_i(B^c)$ for any $B \in \binom{V}{k}$. Then, $(V; f_1^c, \cdots, f_m^c)$ is a t-$[v, v-k, \mu^c; m]$ MOD for some μ^c.

Lemma 3 (Derived design) If $(V; f_1, \ldots, f_m)$ is a t-$[v, k, \mu; m]$ MOD and let $E \in \mathcal{T}$, then $(V \setminus E; f_1|_E, \ldots, f_m|_E)$ is a $(t-\ell)$-$[v-\ell, k-\ell, \mu|_E; m]$ MOD, where $\ell = |E|$ and $\mu|_E(E'') = \mu(E'' \cup E)$.

Theorem 1 (Beth *et al.* [2]) The number of designs m of a $\mathcal{T}$-$[v,k,\mu;m]$ MOD is bounded by

$$m \le \min\left\{\binom{v-t}{k-t}, \binom{v-t}{k}\right\} \le \binom{v-t}{\lfloor \frac{v}{2} \rfloor - t}, \tag{1}$$

where $t = \max\{|E| \mid E \in \mathcal{T}\}$.

Proof. A t-$[v,k,\mu;m]$ MOD has m function f_i's which are mutually orthogonal $\binom{v}{k}$ demensional vectors. Moreover for any $E \in \mathcal{T}$ with $|E| = t$, $f_i|_E$'s are considered to be m mutually orthogonal $\binom{v-t}{k-t}$ demensional vectors. Hence, $m \le \binom{v-t}{k-t}$. Also, by Lemma 1, a t-$[v, v-k, \mu^c; m]$ MOD exists, which means $m \le \binom{v-t}{v-k-t} = \binom{v-t}{k}$. □

Our problem is to know whether there exists a design attaining the bound, or not.

In the case of $t = 1$, the following is known by [3].

Lemma 4 (Beth *et al.* [3]) A 1-$[2k, k, \frac{1}{2}; \binom{2k-1}{k-1}]$ MOD attaining the upperbound (1) exists for any positive integer k.

For a t-MOD, $1 \le t \le k-1$ must hold. In the case of $t = 1$, Lemma 4 assures the existence of 1-MOD attaining the bound (1). Now we consider the case of $t = k-1$. In this case, to attain the latter upperbound (1), $v = 2k$ or $2k+1$ must hold. Here, we devote the case of $v = 2k = 2(t+1)$, that is, a t-$[2(t+1), t+1, \mu; m]$ MOD. In this case, $m \le t+2$ holds by the upperbound (1). Hence the following problem arises.

Problem 1 Does a t-$[2(t+1), t+1, \mu; t+2]$ MOD exist?

For the case of $t = 2$, Beth *et al.* [3] showed that there does not exist a 2-$[6,3,\mu;4]$ MOD. When t is even, we can show more general and stronger results.

Theorem 2 When t is a positive even integer, there does not exist a t-$[2(t+1), t+1, \mu; m]$ MOD over $\mathbb{C}$ for any $m \ge 3$.

Remark: As a corollary, we can show that a 2-$[6,3,\mu;3]$ MOD does not exist, which improve the result by Beth *et al.* [3].

Brief proof of therorem 2: Assume that there exists at least three f_i's. When t is even, some argument gives us an equality

$$\overline{f}_i(B) f_j(B) = -\overline{f}_i(B^c) f_j(B^c) \tag{2}$$

for any $B \in \binom{V}{k}$ and $i \ne j$.

In the case of even t, if $m \ge 3$ then by multiplying equations (2) for $(i,j) = (1,2), (2,3), (3,1)$ we obtain

$$\|f_1^*(B) f_2^*(B) f_3^*(B)\|^2 = -\|f_1^*(B^c) f_2^*(B^c) f_3^*(B^c)\|^2,$$

which means that

$$\|f_1^*(B)f_2^*(B)f_3^*(B)\| = 0 \tag{3}$$

holds for any $B \in \binom{V}{3}$.

Similarly to (2), we obtain

$$\|f_1(B)\| + \|f_1(B^c)\| = \cdots = \|f_m(B)\| + \|f_m(B^c)\|. \tag{4}$$

Equations (3) and (4) imply that $f_1^*(B) = f_2^*(B) = f_3^*(B) = 0$ for any $B \in \binom{V}{3}$, which contradicts to the fact that there are at least three $f_i/\equiv 0$'s.

Hence, $m \leq 2$ for any even t. □

3 Existence of a t-$[2(t+1), t+1, \mu; 2]$ MOD

We can show the following theorem.

Theorem 3 There exists a t-$[2(t+1), t+1, \mu; 2]$ MOD over $\mathbb{C}$ for any integer t.

Proof. Take an $(t+1) \times 2^t$ orthogonal array O_1 with strength t and 2-symbols. And take another orthogonal array O_2 which is disjoint to O_1.

4 Open problems

Unfortunately, the existence of a t-$[2(t+1), t+1, \mu; 2]$ MOD for odd t is not determined yet. It is known that for $t = 1$, a 1-$[4, 2, \frac{1}{2}; 3]$ MOD exists, which attains the upper bound (1).

In case of $t = 3$, the following problem arises.

Problem 2 Does there exist a 3-$[8, 4, \mu; 5]$ MOD over $\mathbb{C}$ for some μ?

This problem is equivalent to the following:

Problem 3 Does there exist a 2-$[7, 3, \mu; 5]$ MOD over $\mathbb{C}$ for some μ?

Remark: It is known that a binary 2-$[7, 3, \frac{1}{7}; 3]$ MOD exists but no binary 2-$[7, 3, \frac{1}{7}; m]$ MOD exists for $m \geq 4$.

Problem 2 is genaralized to the problem below:

Problem 4 Find the maximum value of m such that there exists a t-$[2(t+1), t+1, \mu; m]$ MOD over $\mathbb{C}$ for a given odd integer t?

The upperbound (1) is sharp for $t = 1$. Moreover, if there exists a "large set of binary Steiner t-design", then it attains the upperbound. But only a few resluts are known for the existence of large sets of Steiner t-designs.

Problem 5 Can we find a t-MOD attaining the upperbound (1) except for large sets of Steiner t-designs? Or, can we improve the upperbound (1)?

Acknowledgements. The work of the first author was supported in part by JSPS under Grant-in-Aid for Scientific Research (B)22340016 and Grant-in-Aid for Challenging Exploratory Research 22654031.

References

[1] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes, *Physical Review Letters*, **86** (2001) 4402 4405.

[2] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Detected-jump-error-correcting quantum codes, quantum error designs, and quantum computation. *Physical Review A*, **68** (2003), 012316.

[3] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado, M. Mussinger, A new class of designs which protect against quantum jumps. *Designs, Codes and Cryptography*, **29** (2003), 51–70.

[4] O. Kern and G. Alber, Suppressing decoherence of quantum algorithms by jump codes, *European Physical J. D*, **36** (2005) 241–248.

[5] M. Jimbo and K. Shiromoto, Quantum jump codes and related combinatorial designs. In D. Crnkovic and V. Tonchev eds. Nato Series - D: ICS Vol. 29, *Information Security, Coding Theory and Related Combinatorics*, (2011) 285-311.

Existence and construction of absolutely nonsingular tensors

T. Sumi (Kyushu Univ.), T. Sakata (Kyushu Univ.), and
M. Miyazaki (Kyoto Univ. of Education)

1 序

ベクトルを1次元配列，行列を2次元配列と見ることができる．3次元配列を3-テンソルと呼ぶ．行列のランクはいろいろな方法で定義ができるが，その1つの定義の拡張として，3-テンソルの階数を定義する．3-テンソルのランクを決定するのは非常に難しい．3-テンソルのサイズを決めたときの最大階数でさえ決定できていない．

本論では，実数体上のテンソルの最大階数を考察したときに必要となった，絶対正則な3-テンソルを定義し，その存在と構成について議論する．

2 3-テンソルとその階数

正整数 m,n,p に対し，

$$\mathbb{A} = (a_{ijk})_{1\le i\le m,\ 1\le j\le n,\ 1\le k\le p}$$

なる3次元配列を，$m\times n\times p$ 型テンソルと呼ぶ．基礎体 $\mathbb{F}$ に対し，$m\times n\times p$ 型テンソル全体のなす集合を $\mathbb{F}^{m\times n\times p}$ と表す．

3-テンソル $\mathbb{A}$ において，k を固定すると

$$(a_{ijk})_{1\le i\le m,\ 1\le j\le n}$$

は行列となる．これを A_k と表すとき，テンソル $\mathbb{A}$ を

$$(A_1;A_2;\ldots;A_p)$$

と記す．

構造が簡単なテンソルの例として

$$(x_iy_jz_k)_{1\le i\le m,\ 1\le j\le n,\ 1\le k\le p} =: (x_i)_{1\le i\le m}\odot(y_j)_{1\le j\le n}\odot(z_k)_{1\le k\le p}$$

があげられる．(x_i), (y_j), (z_k) がゼロベクトルでないとき、このようなテンソルを階数1という．いずれかのベクトルがゼロベクトルであれば、$(x_iy_jz_k)$ の成分はすべて0となるため、その階数は0とする．テンソル $\mathbb{A}=(A_1;A_2;\ldots;A_p)$ の階数が1であることは，階数1の行列 A_{k_0} があり，それ以外の行列は，A_{k_0} のスカラー倍（$A_k = c_kA_{k_0}$）であることと同値である．

Example 1

$$
\begin{aligned}
(a_{ijk}) &= \sum_{i,j,k} a_{ijk} \boldsymbol{e}_m^{(i)} \odot \boldsymbol{e}_n^{(j)} \odot \boldsymbol{e}_p^{(k)} \\
&= \sum_{j,k} (\sum_i a_{ijk} \boldsymbol{e}_m^{(i)}) \odot \boldsymbol{e}_n^{(j)} \odot \boldsymbol{e}_p^{(k)} \\
&= \sum_{i,k} \boldsymbol{e}_m^{(i)} \odot (\sum_j a_{ijk} \boldsymbol{e}_n^{(j)}) \odot \boldsymbol{e}_p^{(k)} \\
&= \sum_{i,j} \boldsymbol{e}_m^{(i)} \odot \boldsymbol{e}_n^{(j)} \odot (\sum_k a_{ijk} \boldsymbol{e}_p^{(k)})
\end{aligned}
$$

ただし，$\boldsymbol{e}_m^{(i)}$ は m 次単位ベクトルの第 i 列とする．

よって，任意の 3-テンソルは，高々 $\min(mn, np, pm)$ 個の階数 1 のテンソルの和として表すことができる．ここで，基礎体 $\mathbb{F}$ 上の 3-テンソル $\mathbb{A}$ の階数 $\mathrm{rank}_{\mathbb{F}}\mathbb{A}$ を，階数 1 のテンソルの和として表すときに必要な階数 1 のテンソルの数の最小数と定める．特に，階数 0 のテンソルはすべての成分が 0 のものに限るとする．

$p=1$ のとき，$m \times n \times p$ 型テンソルは $m \times n$ 行列とみなすことができるが，特異値分解から，3-テンソルとしての階数は，行列としての階数と一致する．

Proposition 1 $(A_1;\ldots;A_{p-1};A_p)$ の階数は $(A_1;\ldots;A_{p-1})$ の階数以上である．

ここで注意しないといけないのは，テンソルの階数は，基礎体に依存することである．次の節でこの例を示す．

3 $m \times n \times 2$ 型テンソル

$m \times n \times 1$ 型テンソルの階数は，基礎体に依存せず行列の階数であった．この節では，$m \times n \times 2$ 型テンソルの階数について考える．結論としては，$m \times n \times 2$ 型テンソルについては，Kronecker-Weierstrass 理論があり，階数を決定することが可能である．

Theorem 1 ([Gan59, (30) in §4, XII]) $m \times n$ 行列 A, B に対し，$m \times n \times 2$ 型テンソル

$$P(A;B)Q = (PAQ;PBQ)$$

は，ブロック対角型

$$\mathrm{Diag}((S_1;T_1),\ldots,(S_r;T_r)),$$

で表すことができるような，正則行列 P, Q が存在する．ただし，各テンソル $(S_j;T_j)$ は次のような形をしている．

(1) $k \times \ell \times 2$ 型零テンソル $(O;O)$,

(2) $k \times k \times 2$ 型テンソル $(\alpha E_k + J_k; E_k)$,

(3) $2k \times 2k \times 2$ 型テンソル $(C_k(c,s) + J_k \otimes E_2; E_{2k})$, $s \neq 0$,

(4) $k \times k \times 2$ 型テンソル $(E_k; J_k)$,

(5) $k\times(k+1)\times 2$ 型テンソル $((\mathbf{0},E_k);(E_k,\mathbf{0}))$,

(6) $(k+1)\times k\times 2$ 型テンソル $(\begin{pmatrix}\mathbf{0}^\top\\ E_k\end{pmatrix};\begin{pmatrix}E_k\\ \mathbf{0}^\top\end{pmatrix})$.

E_k は $k\times k$ 単位行列で，J_k, $C_k(c,s)$ は，それぞれ，次で定まる $k\times k$ 行列，$2k\times 2k$ 行列である．

$$J_k=\begin{pmatrix}0 & 1 & & O\\ \vdots & \ddots & \ddots & \\ \vdots & & \ddots & 1\\ 0 & \cdots & \cdots & 0\end{pmatrix}$$

$$C_k(c,s)=E_k\otimes\begin{pmatrix}c & -s\\ s & c\end{pmatrix}=\mathrm{Diag}(\begin{pmatrix}c & -s\\ s & c\end{pmatrix},\ldots,\begin{pmatrix}c & -s\\ s & c\end{pmatrix})$$

$m\times n\times 2$ 型テンソルのランクと，ペンシル理論との関係は，[Ja'79a, Ja'79b, SMS09] を参考にされたい．

$m\times n\times 2$ 型テンソルの階数は基礎体にすることを示そう．

Example 2 $T_1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $T_2=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ とする．$2\times 2\times 2$ 型テンソル $\mathbb{T}=(T_1;T_2)$ に対して，

$$\mathrm{rank}_{\mathbb{C}}\mathbb{T}=2\quad \mathrm{rank}_{\mathbb{R}}\mathbb{T}=3$$

が成り立つ．

実際，

$$\begin{aligned}\mathbb{T}&=\begin{pmatrix}1\\ \sqrt{-1}\end{pmatrix}\odot\begin{pmatrix}1\\ -\sqrt{-1}\end{pmatrix}\odot\frac{1}{2}\begin{pmatrix}1\\ \sqrt{-1}\end{pmatrix}+\begin{pmatrix}1\\ -\sqrt{-1}\end{pmatrix}\odot\begin{pmatrix}1\\ \sqrt{-1}\end{pmatrix}\odot\frac{1}{2}\begin{pmatrix}1\\ -\sqrt{-1}\end{pmatrix}\\ &=\begin{pmatrix}0\\ -2\end{pmatrix}\odot\begin{pmatrix}1\\ 0\end{pmatrix}\odot\begin{pmatrix}0\\ 1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1\\ -1\end{pmatrix}\odot\begin{pmatrix}1\\ -1\end{pmatrix}\odot\begin{pmatrix}1\\ -1\end{pmatrix}+\frac{1}{2}\begin{pmatrix}1\\ 1\end{pmatrix}\odot\begin{pmatrix}1\\ 1\end{pmatrix}\odot\begin{pmatrix}1\\ 1\end{pmatrix}\end{aligned}$$

と表すことができ，

Proposition 2 $\mathrm{rank}_{\mathbb{F}}(E_n;T)=n$ であることは，$\mathbb{F}$ 上 T が対角化可能であることと同値である．

が成り立つからである．

4 テンソルの同値関係

$P=(p_{ij})\in GL(n)$, $Q=(q_{ij})\in GL(m)$, $R=(r_{ij})\in GL(p)$ に対し，(P,Q,R) の作用

$$(b_{ijk})=(P,Q,R)\cdot(a_{ijk})$$

を

$$b_{ijk}=\sum_{s=1}^{m}\sum_{t=1}^{n}\sum_{u=1}^{p}p_{is}q_{jt}r_{ku}a_{stu}$$

にて定める.

すると

$$(P,Q,R)\cdot(A_1;\ldots;A_p)=(\sum_{u=1}^{p} r_{1u}PA_uQ^{\top};\ldots;\sum_{u=1}^{p} r_{pu}PA_uQ^{\top})$$

が成り立つ.

Definition 1 2つの $m\times n\times p$ 型テンソル A,B が同値であるとは，$B=S\cdot A$ を満たす，$S\in GL(m)\times GL(n)\times GL(p)$ が存在することをいう.

$$(P,Q,R)\cdot(x_iy_jz_k)=P(x_i)\odot Q(y_j)\odot R(z_k)$$

より，テンソルのランクは同値類で決まる．$m\times n\times 2$ 型テンソル $(A;B)$ に対し，Theorem 1 の形がわかれば，$\mathrm{rank}_{\mathbb{R}}(A;B)$ は求まる.

$m\times n\times 3$ 型テンソルの階数について，１９７０年代後半から１９８０年代に主に研究がなされた．$m\times n\times 3$ 型テンソルの分類は不可能とされているし，テンソルに関する問題の殆どは NP 困難であることが示されている [HL10].

5 絶対正則テンソル

Definition 2 基礎体 $\mathbb{R}$ において，$\sum_{k=1}^{p} x_kA_k$ が特異なのは，$(x_1,\ldots,x_p)=(0,\ldots,0)$ のときに限るとき，$n\times n\times p$ 型テンソル $A=(A_1;\ldots;A_p)$ を絶対正則という.

$2\times 2\times 2$ 型絶対正則テンソルの同値類はただ 1 つのみで，

$$(E_2;\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix})$$

で代表される．しかし，型を大きくすれば同値類は無限に存在する.

Atkinson-Stephens [AS79] は，証明なしで，$n\times n\times 3$ 型複素テンソルのランクは $2n-1$ 以下であると主張した．絶対正則は，Atkinson-Stephens の結果が実数体上ではどうなるのかを考察しているときに，生じた条件である.

Theorem 2 ([SMS10]) $n\times n\times 3$ 型実テンソルが，絶対正則でなければ，ランクは，$2n-1$ 以下である.

$3\times 3\times 2$ 型テンソルの最大階数は 4 であるのに対し，$3\times 3\times 3$ 型テンソルの最大階数は 5 である．いかにうまく階数 1 のテンソルをとらないと 5 個の和で書けそうにないかが想像できるであろう.

Theorem 3 絶対正則テンソル全体のなす集合は，ユークリッド位相をもつ $\mathbb{R}^{n\times n\times p}$ において，開集合である（空集合かもしれない）.

次は容易にわかる.

Proposition 3 $(A_1;\ldots;A_p)$ を $n\times n\times p$ 型絶対正則テンソルとするとき，次が成り立つ.

- $1 \leq q \leq p$ に対し，$(A_1;\ldots;A_q)$ は $n \times n \times q$ 型絶対正則テンソルである．
- $s \geq 1$ に対し，$(\mathrm{Diag}(A_1,\ldots,A_1);\ldots;\mathrm{Diag}(A_p,\ldots,A_p))$ は $sn \times sn \times p$ 型絶対正則テンソルである．

以降，$n \times n \times p$ 型テンソル $A = (A_1;\ldots;A_p)$ を，変数 $x_1,\ldots,x_p$ に関する行列 $\sum_{k=1}^{p} x_k A_k$ と同一視する．例えば，

$$x_1 E_2 + x_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$$

の表す $2 \times 2 \times 2$ 型テンソルは，

$$(E_2; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix})$$

である．

さて，絶対正則テンソルの例をあげよう．

Example 3 次は，可換な division algebra からくる例である．

$$\begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & x_4 & -x_3 \\ -x_3 & -x_4 & x_1 & x_2 \\ -x_4 & x_3 & -x_2 & x_1 \end{pmatrix}$$

$n = 8$ では，可換な division algebra は存在しないが，

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ -x_2 & x_1 & -x_4 & x_3 & -x_6 & x_5 & x_8 & -x_7 \\ -x_3 & x_4 & x_1 & -x_2 & -x_7 & -x_8 & x_5 & x_6 \\ -x_4 & -x_3 & x_2 & x_1 & -x_8 & x_7 & -x_6 & x_5 \\ -x_5 & x_6 & x_7 & x_8 & x_1 & -x_2 & -x_3 & -x_4 \\ -x_6 & -x_5 & x_8 & -x_7 & x_2 & x_1 & x_4 & -x_3 \\ -x_7 & -x_8 & -x_5 & x_6 & x_3 & -x_4 & x_1 & x_2 \\ -x_8 & x_7 & -x_6 & -x_5 & x_4 & x_3 & -x_2 & x_1 \end{pmatrix}$$

は $8 \times 8 \times 8$ 型絶対正則テンソルである．

数 $\beta(n)$ を $n \times n \times m$ 型絶対正則テンソルが存在するような最大の整数とする．

Proposition 4 $\beta(n) \leq n$, $\beta(sn) \geq \max(\beta(s), \beta(n))$.

Theorem 4 V, W を絶対正則テンソルとし，$VW = WV$ を満たすならば，

$$\begin{pmatrix} B & A \\ -A^{\mathrm{T}} & B^{\mathrm{T}} \end{pmatrix}$$

も絶対正則である．

$$R_1(x_1,x_2) = M_1(x_1,x_2) = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix},$$

$$C_1(x_1,x_2) = \begin{pmatrix} x_1 & x_2 \\ x_2 & -x_1 \end{pmatrix}$$

を初期設定とし，帰納的に

$$R_{k+1}(x_1,x_2) = \begin{pmatrix} R_k(x_1,x_2) & O \\ O & R_k(x_1,x_2) \end{pmatrix},$$

$$C_{k+1}(x_1,x_2) = \begin{pmatrix} O & C_k(x_1,x_2) \\ (-1)^k C_k(x_1,x_2) & O \end{pmatrix},$$

$$M_{k+1}(x_1,\ldots,x_{2k+2}) = \begin{pmatrix} M_k(x_1,\ldots,x_{2k}) & R_k(x_{2k+1},x_{2k+2}) \\ -R_k(x_{2k+1},x_{2k+2})^\top & M_k(x_1,\ldots,x_{2k})^\top \end{pmatrix}$$

と定める．このとき，つぎがいえる．

Theorem 5 $n = 2^s$ に対して，以下で与えられる B は $n \times n \times *$ 型絶対正則テンソルである．

(1) $s \equiv 1,2 \mod 4$ のとき $B = M_s(x_1,\ldots,x_{2s})$

(2) $s \equiv 3 \mod 4$ のとき

$$B = M_s(x_1,\ldots,x_{2s}) + C_s(x_{2s+1},x_{2s+2}) =: N_s(x_1,\ldots,x_{2s+2}).$$

(3) $s \equiv 0 \mod 4$ のとき $B = \tilde{M}_s(x_1,\ldots,x_{2s+1})$. ただし，

$$\tilde{M}_s(x_1,\ldots,x_{2s+1}) = \begin{pmatrix} N_{s-1}(x_1,\ldots,x_{2s}) & x_{2s+1}E_{2^{s-1}} \\ -x_{2s+1}E_{2^{s-1}} & N_{s-1}(x_1,\ldots,x_{2s})^\top \end{pmatrix}.$$

6 追補

講演後，宗政氏に直交デザイン，吉荒氏に双線形写像との関連を指摘して頂いた．それをもとに，色々と調べた結果，$\beta(n)$ は既に，Hurwitz-Radon 数 $\rho(n)$ として知られていることがわかった．

$\rho(n)$ は，n を $2^{4a+b}c$，c は奇数，$b = 0,1,2,3$ と表したとき，

$$\rho(n) = 2^b + 8a$$

で定義される．直交デザインは，絶対正則テンソルを定める．Geramita-Seberry の本 [GS79] の例，もしくは Theorem 5 から，$n \times n \times \rho(n)$ 絶対正則テンソルが存在することがわかる．その一方，Adams [Ada62, ALP65] の結果から，$n \times n \times p$ 絶対正則テンソルが存在すれば，$p \le \rho(n)$ が従う．よって，$\beta(n) = \rho(n)$ である．

Theorem 2 から，次がいえる．

Theorem 6 n が 4 の倍数でないならば，$n \times n \times 3$ 型テンソルの最大階数は $2n-1$ 以下である．

今回は紹介できなかったが，$n \times n \times m$ 型絶対正則テンソルの存在は，$m \times n \times (m-1)n$ 型実テンソルの典型ランクと関係している．

References

[Ada62] J. F. Adams, *Vector fields on spheres*, Ann. of Math. (2) **75** (1962), 603–632. MR 0139178 (25 #2614)

[ALP65] J. F. Adams, Peter D. Lax, and Ralph S. Phillips, *On matrices whose real linear combinations are non-singular*, Proc. Amer. Math. Soc. **16** (1965), 318–322. MR 0179183 (31 #3432); *Correction*, **17** (1966), 945–947. MR 0201460 (34 #1344)

[AS79] M. D. Atkinson and N. M. Stephens, *On the maximal multiplicative complexity of a family of bilinear forms*, Linear Algebra Appl. **27** (1979), 1–8. MR 545717 (80i:15019)

[Gan59] F. R. Gantmacher, *The theory of matrices. Vols. 1, 2*, Translated by K. A. Hirsch, Chelsea Publishing Co., New York, 1959. MR 0107649 (21 #6372c)

[GS79] Anthony V. Geramita and Jennifer Seberry, *Orthogonal designs*, Lecture Notes in Pure and Applied Mathematics, vol. 45, Marcel Dekker Inc., New York, 1979, Quadratic forms and Hadamard matrices. MR 534614 (82a:05001)

[HL10] C. J. Hillar and L.-H. Lim, *Most tensor problems are NP hard*, arXiv:09111393v2 (2010).

[Ja'79a] Joseph Ja'Ja', *An addendum to Kronecker's theory of pencils*, SIAM J. Appl. Math. **37** (1979), no. 3, 700–712. MR 549150 (81e:15013)

[Ja'79b] ———, *Optimal evaluation of pairs of bilinear forms*, SIAM J. Comput. **8** (1979), no. 3, 443–462. MR 539263 (80e:68109)

[SMS09] Toshio Sumi, Mitsuhiro Miyazaki, and Toshio Sakata, *Rank of 3-tensors with 2 slices and Kronecker canonical forms*, Linear Algebra Appl. **431** (2009), no. 10, 1858–1868. MR 2567796 (2010m:15041)

[SMS10] ———, *About the maximal rank of 3-tensors over the real and the complex number field*, Ann. Inst. Statist. Math. **62** (2010), no. 4, 807–822. MR 2652318

On planar functions and p-ary bent functions

Nobuo Nakagawa

2011/06/21

Department of Mathematics, Faculty of Science and Technology,
Kinki University

Section1 Introduction

Boolean bent functions were first introduced by Rothaus in 1976 in [5]. They have been extensively studied for their important applications in cryptography. such functions have the maximum Hamming distance to the set of all affine functions. In [4], the authors generalized the notion of a bent function to be defined over a finite field of arbitrary characteristic.

On the other hand, planar functions were first introduced by Ostrom and Dembouski in 1968 in [2] to characterize a finite affine plane with a regular automorphism group.

A planar function is defined between finite groups of same order. However all known examples are planar functions between elementary abelian p-groups for odd prime p. In the below, let p be an odd prime and f be a function from $GF(p^n)$ into $GF(p^n)$. For $a \in GF(p^n)$, the difference function $\Delta_a(f)$ of f with respect to a, is defined by

$$\Delta_a(f)(x) := f(x+a) - f(x) \qquad (x \in GF(p^n)),$$

and f is called *planar* if $\Delta_a(f)$ is bijective for any $a \in GF(p^n)^*$.

Moreover let f be a function from $GF(p^n)$ to $GF(p)$. The Walsh transformation of f is the complex valued function $\hat{f} : GF(p^n) \mapsto \mathbf{C}$ defined by

$$\hat{f}(b) := \sum_{x \in GF(p^n)} \zeta_p^{f(x)+\mathrm{Tr}(bx)} \qquad (b \in GF(p^n))$$

where ζ_p is a primitive p-th root of unity and $\mathrm{Tr}(x)$ is the absolute trace function. The function f is called $p-ary\ bent$ if every Walsh coefficient $\hat{f}(b)$

has magnitude $p^{\frac{n}{2}}$, namely $|\hat{f}(b)| = p^{\frac{n}{2}}$ for all $b \in GF(p^n)$. Moreover, f is called *reglur* if there exsists some function $f^* : GF(p^n) \mapsto GF(p)$ such that $\hat{f}(b) = p^{\frac{n}{2}}\zeta_p^{f^*}(b)$, and f is called to be weakly regular if $\hat{f}(b) = up^{\frac{n}{2}}\zeta_p^{f^*(b)}$ for some constant $u \in \mathbf{C}$ with $|u| = 1$.

The quadratic bent functions and most monomial p-ary bent functions are weakly regular, except one sporadic non-weakly regular example. Recently, interesting weakly bent functions on $GF(p^{4k})$ are constructed by Helleseth and Kholosha as the following ([3]).

$$g(x) = \mathrm{Tr}(x^2 + x^{p^{3k}+p^{2k}-p^k+1})$$

Is $g_\alpha(x) := \mathrm{Tr}(\alpha(x^2 + x^{p^{3k}+p^{2k}-p^k+1}))$ bent for what element α ? It seems that it is an important problem.

In Section 2 we mention a relation of planar functions and p-ary bent functions and a necessary and sufficient condition that a function is bent. Moreover a conjecture related to the function constructed by Helleseth and Kholosha is given.

In Section 3 we mention strongly regular graphs coming from p-ary weakly bent functions satisfying some conditions by constructed by Chee, Tan and Zhang and a sketch of the proof.

In section 4 we argue the non-isomorphism problem between the strongly regular graphs constructed from the quadratic trace function and those constructed from the function by Helleseth and Kholosha.

Section2 Planar functions and p-ary bent functions

Let f be a function from $GF(p^n)$ into $GF(p)$. Define

$$\Delta_a(f)(x) := f(x+a) - f(x), \ (x \in GF(p^n))$$

The following theorem gives a necessary and sufficient condition that f is bent.

Theorem 1 *If f is p-ary bent,*

$$|\Delta_a(f)^{-1}(\alpha)| = p^{(n-1)}$$

for any $a \in GF(p^n)^*$ and any $\alpha \in GF(p)$. And the converse is true.

The following theorem shows that a planar function correspond to a family of p-ary bent functions.

Theorem 2 *Let F be a planar function on $GF(p^n)$. We identifies $GF(p^n)$ with $GF(p)^n$ by a suitable basis of $GF(p^n)$ over $GF(p)$. We may write as $F(x) = (f_1(x), f_2(x), \cdots, f_n(x))$ where each f_i is a function from $GF(p^n)$ into $GF(p)$. Then*

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_n f_n$$

is a bent function for any $(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq \mathbf{0}$. The converse is true.

Here we give a conjecture. Set $G(x) := x^2 + x^{p^3+p^2-p+1}$ where $G(x)$ is a function from $GF(p^4)$ into $GF(p^4)$.
[Conjecture 1] $\mathrm{Tr}(\alpha G(x))$ is bent if and only if $\alpha \in GF(p^2)^*$.

Section 3 Stronly regular graphs from p-ary bent functions
We consider the typical quadratic bent function as the following.

$$f(x_1, x_2, \cdots, x_n) := x_1^2 + x_2^2 + \cdots + x_n^2$$

Then f is a weakly regular bent function from $GF(p^n)$ to $GF(p)$. Because

$$\sum_{x_1 \in GF(p)} \cdots \sum_{x_n \in GF(p)} \zeta_p^{(x_1^2+\cdots+x_n^2)} = \begin{cases} p^{n/2} & \text{if } p \equiv 1 \pmod 4 \\ -p^{n/2} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

For $b = (b_1, \cdots, b_n)$,

$$\hat{f}(b) = \sum_{x_1 \in GF(p)} \cdots \sum_{x_n \in GF(p)} \zeta_p^{x_1^2+\cdots+x_n^2+b_1x_1+\cdots+b_nx_n}$$

$$= \begin{cases} p^{n/2}\zeta_p^{\frac{-1}{4}f(b)} & \text{if } p \equiv 1 \pmod 4 \\ -p^{n/2}\zeta_p^{\frac{-1}{4}f(b)} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

In this example,

$$\hat{f}(b) = (u\zeta_p^{f^*(b)})p^{n/2}$$

where if $p \equiv 1 \pmod 4$ then $u = 1$, and if $p \equiv 3 \pmod 4$ then $u = -1$, moreover $f^*(x) = -\frac{1}{4}f(x)$. Thus f^* is also a weakly regular bent function.

Definition 3 *Let G be a finite group and D be a subset of G. If it holds that*

$$DD^{(-1)} = k1_G + \lambda D + \mu(G - D - 1_G)$$

in the group ring $\mathbf{C}[G]$, then D is called (k, λ, μ)-partial difference set in G.

Under the assumptions above, we define a graph constructed by G and D.

Definition 4 *Suppose that $1_G \notin D$ and $D^{-1} = D$. We take G as the set of vertices, and for $x, y \in G$, $x \sim y$ (x is adjacent to y) $\iff xy^{-1} \in D$*

We denote this graph by $\Gamma(G, D)$ which is called Caley graph generated from G and D.

Theorem 5 *Let G be a group, D is a subset of G, $1_G \notin D$ and $D^{(-1)} = D$. Then D is a (k, λ, μ)-partial difference set if and only if the Caley graph $\Gamma(G, D)$ is a (k, λ, μ)-stronly regular graph(SRG).*

We consider weakly regular bent functions satisfying the following condition.

Condition A $f : GF(p^{2k}) \mapsto GF(p)$

$$\hat{f}(b) = \varepsilon \zeta_p^{\varphi(b)} p^k \text{ where } \varepsilon \in \{\pm 1\}$$

$f(0) = 0$, $f(-x) = f(x)$ $(\forall x \in GF(p^{2k}))$, $f(\alpha x) = \alpha^\ell f(x)$ $(\forall \alpha \in GF(p))$ where ℓ is a positive integer s.t. $gcd(\ell - 1, p - 1) = 1$.

Then φ is also a weakly regular bent function and $\varphi(\alpha x) = \alpha^h \varphi(x)$ holds for some h such that $gcd(h - 1, p - 1) = 1$.

In the below at section 3, we consider a function satisfying the condition A and $p \equiv 1 \pmod 4$. However we may argue similarly in the case $p \equiv 3 \pmod 4$.

Definition 6 $D_i := \{x \in GF(p^{2k}) \mid f(x) = i\}$ $(i \in GF(p))$
$S := \{a^2 \mid a \in GF(p)^*\}$, $D_S := \cup_{i \in S} D_i$

Theorem 7 *(Y.M.Chee, Y.Tan and X.D.Zhang [1]) Let f be a bent function satisfying the condition A. Then Caley graph $\Gamma(GF(p^{2k}), D_S)$ is SRG with parameters $(h, \lambda, \mu) = ((n+1)r, r^2 + 3r - n, r^2 + r)$ with $\varepsilon = 1$ or with parameters $(h, \lambda, \mu) = ((n-1)r, r^2 - 3r + n, r^2 - r)$ with $\varepsilon = -1$, where $n = p^k$, $r = \frac{1}{2}p^{k-1}(p-1)$.*

Here $h = |\Gamma_1(0)| = \frac{1}{2}p^{k-1}(p-1)(p^k - \varepsilon)$, $\lambda = \frac{1}{4}(p^{k-1}(p-1))^2 + \frac{3-p}{2}p^{k-1}\varepsilon$, and $\mu = \frac{1}{4}(p^{k-1}(p-1))^2 - \frac{1}{2}p^{k-1}(p-1)\varepsilon$. The former is called of negative Latin

Square type and the latter is called of Latin Square type and known examples of negative Latin Square type are very few.

A sketch of the proof

By theorem 5 we may prove that $D_S D_S = h1_G + \lambda D_S + \mu(G - D_S - 1_G)$. where $G = GF(p^{2k})$, $1_G = 0$. Set

$$L_t := \sum_{x \in GF(p^{2k})} x\zeta^{tf(x)} = \sum_{i=0}^{p-1} D_i \zeta^{ti}.$$

By solving conversely, $D_i = \frac{1}{p}\sum_{t=0}^{p-1} L_t \zeta^{-it}$

(Step 1)

(1), $L_t L_s = up^k L_v$ if $st(s+t) \neq 0$, here v is an unique element s.t. $s^{1-h} + t^{1-h} = v^{1-h}$ and $u = u(t,s,v) \in \{\pm 1\}$.

(2), $L_t L_{-t} = p^{2k}$ $(\forall t = 1, \cdots, p-1)$

(3), $\sum_{t=1}^{p-1} L_t L_0 \zeta_p^{-at} = (p|D_a| - p^{2k})GF(p^{2k})$.

We obtains (1) in the following. For $\forall \chi_b \in Char(GF(p^{2k}))$, $\chi_b(L_t) = u_t p^k \zeta_p^{t^{1-h}\varphi(b)}$ wherer $u_t \in \{\pm 1\}$. Thus $\chi_b(L_t L_s) = \chi_b(u_{t,s,v} p^k L_v)$ for any χ_b. (It is used effectively that f is weakly bent.)

(Step 2)

From (3) of (Step 1),

$$(p|D_a| - p^{2k})GF(p^{2k}) = \sum_{t=1}^{p-1} L_t L_0 \zeta_p^{-at} =$$

$$\sum_{t=1}^{p-1} L_t L_0 (\zeta_p^{-ab^{-1}})^{-bt} = (p|D_b| - p^{2k})GF(p^{2k}).$$

Thus $|D_a| = |D_b|$ (if $ab \neq 0$). Moreover

$$\hat{f}(b) = \sum_{i=1}^{p-1} (\sum_{x \in D_i} \zeta_p^{\mathrm{Tr}(bx)}) \zeta_p^i = \chi_b \cdot \eta(R)$$

where $\eta \in Char(GF(p))$ and $R := \{(x, f(x)) \mid x \in GF(p^{2k})\}$. Here we set $b = 0$.

$$\varepsilon p^k \zeta_p^{\varphi(0)} = |D_0| + |D_1|(\zeta_p + \cdots + \zeta_p^{p-1})$$

Hence we have $|D_0| = p^{2k-1} + \varepsilon p^{k-1}(p-1), |D_a|\ (a \neq 0) = p^{k-1}(p^k - \varepsilon)$. Now $p^2 D_a D_b = \sum_{s,t=0}^{p-1} L_t L_s \zeta_p^{-at-bs}$. We compute to divide three cases of $s+t=0$, $st=0$ and $st(s+t) \neq 0$. Then we have

$$p^2 D_a D_b = \sum_{s=1}^{p-1} p^{2k} \zeta_p^{s(a-b)} + (2p|D_a| - p^{2k})\mathbf{F}_{p^{2k}} +$$

$$\sum_{st(s+t)\neq 0, s^{1-h}+t^{1-h}=v^{1-h}} u_{s,t,v} p^k \zeta_p^{-at-bs} L_v$$

(Step 3)
We set $T := GF(p)^* \setminus S$. It holds $S^2 = \frac{p-1}{2} + \frac{p-5}{4}S + \frac{p-1}{4}T$, $T^2 = \frac{p-1}{2} + \frac{p-1}{4}S + \frac{p-5}{4}T$, and $ST = \frac{p-1}{4}(S+T)$ at $GF(p)$.
(There are just $\frac{p-1}{2}$ 0 in $S+S$, $\frac{p-5}{4}$ each nonzero squares and $\frac{p-1}{4}$ each nonzero non-squares in $S+S$.)

Set $m = \sum_{a\in S} \zeta^{-a}$. Then we have $m^2 + m = \frac{p-1}{4}$.

From $p^2 D_a D_b$ of (Step 2)

$$p^2 D_S^2 = \frac{p^{2k}(p+1)(p-1)}{4} + (\frac{p(p-1)^2}{2}|D_1| - \frac{p^k(p-1)^2}{4})GF(p^{2k})$$

$$+\varepsilon p^k \sum_{a,b\in S} \sum_{st(s+t)\neq 0, s^{1-h}+t^{1-h}=v^{1-h}} \zeta_p^{-at-bs} L_v$$

We set $\Omega := \{(s,t) \mid st(s+t) \neq 0, s^{1-h} + t^{1-h} = v^{1-h}\}$. and set $v := \sigma(s,t)$ for v such that $s^{1-h} + t^{1-h} = v^{1-h}$.

The third term $(T3)$ of the right of the above equation is the following.

$$(T3) = \sum_{a,b\in S} \sum_{(s,t)\in\Omega} \zeta_p^{-at-bs} L_{\sigma(s,t)} =$$

$$\sum_{(s,t)\in\Omega\cap(S\times S)} m^2 L_{\sigma(s,t)} + \sum_{(s,t)\in\Omega\cap(T\times T)} (1+m)^2 L_{\sigma(s,t)} - \sum_{(s,t)\in\Omega\setminus((S\times S)\cup(T\times T))} m(1+m) L_{\sigma(s,t)}.$$

Hence we have

$$(T3) = A(\sum_{u\in S} L_u) + B(\sum_{u\in T} L_u)$$

$$= \sum_{i=0}^{p-1} \{A(\sum_{u\in S} \zeta_p^{ui}) + B(\sum_{u\in T} \zeta_p^{ui})\} D_i = \frac{1-p}{2}(\mathbf{F}_{p^{2k}} - D_s) + \frac{p+1}{2} D_S$$

where $A = \frac{p-5}{4}m^2 + \frac{p-1}{4}(1+m)^2 - \frac{p-1}{2}m(1+m)$, and
$B = \frac{p-1}{4}m^2 + \frac{p-5}{4}(1+m)^2 - \frac{p-1}{2}m(1+m)$. Therefore we obtain

$$p^2 D_S D_S^{(-1)} = C_1 + C_2 D_S + C_3 GF(p^{2k})$$

where $C_1 = \frac{p^{2k}(p-1)(p+1)}{4}, C_2 = \varepsilon p^{k+1}$ and $C_3 = \frac{p^{2k}(p-1)^2}{4} - \frac{\varepsilon p^{k+1}(p-1)}{2}$.

Section4 The non-isomorphism problem between two SRGs coming from exponents of bent functions

In the below, we argue strongly regular graphs(SRG) constructed from bent functions and show that the non isomorphism betweem SRGs coming two typical bent functions for relative small odd primes p.
Put $n = 2k$ for a positive integer k.

We construct a graph $\Gamma(f,p) = \Gamma(GF(p^{2k}), D_S)$ by using a p-ary bent function f from $GF(p^{2k})$ to $GF(p)$ satisfying the condition (A) as we mentioned in Section 3, where S is the non-zero squares of $GF(p)$. Then this graph is that defined as the following.

The vertices set is $GF(p^{2k})$ and a vertex x is adjacent to a vertex y iff $f(x-y) \in S$.

In below we suppose $k = 2$ and set $F := GF(p^4)$. Then $\Gamma(f,p)$ is SRG with parameters

$$(p^4, \frac{p(p^2+1)(p-1)}{2}, \frac{p(p^2+3)(p-2)}{4}, \frac{p(p^2-p+2)(p-1)}{4})$$

if f satisfies the condition (A) from Theorem 7.

Now there are two interesting bent functions satisfying the condition (A), one of them is $f(x) := Tr(x^2)$ and another one is $g(x) := Tr(x^2 + x^{p^3+p^2-p+1})$ which is constructed by Helleseth and Kholosha.

Theorem 8 *Let p be an odd prime which is less than 20. Then the graph $\Gamma(f,p)$ is not isomorphic to the graph $\Gamma(g,p)$.*

The outline of the proof is the following.
The autmorphism groups of $\Gamma(f,p)$ and $\Gamma(g,p)$ contain the translation group $\mathbf{T} := \{t_a | a \in F\}$ and the scalar multiplication group $\mathbf{M} := \{m_\alpha | \alpha \in GF(p)^*\}$ where $t_a(x) = x + a$ and $m_\alpha(x) = \alpha x$.

Besides $Aut(\Gamma(f,p))$ contains the orthogonal group $G := O^-(F)$ of minus type with respect to a non-degenerate bilinear mapping $b(x,y) := Tr(xy)$. We note $f(x) = b(x,x)$.

Then F has a orthgonal basis $\{u_i | 1 \leq i \leq 4\}$ such that $b(u_i, u_i) = 1$ for $i = 1,2,3$ and $b(u_4, u_4) = \gamma_0$ for a fixed $\gamma_0 \notin S$.

$O^-(F)$ is isomorphic to the following.

$$\{A = (a_{i,j}) | {}^tAE'A = E' \} \text{ where}$$

${}^tAE'A =$

$$\begin{pmatrix} a_{1,1} & a_{2,1} & a_{3,1} & a_{4,1} \\ a_{1,2} & a_{2,2} & a_{3,2} & a_{4,2} \\ a_{1,3} & a_{2,3} & a_{3,3} & a_{4,3} \\ a_{1,4} & a_{2,4} & a_{3,4} & a_{4,4} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \gamma_0 \end{pmatrix} \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \gamma_0 \end{pmatrix}.$$

Set

$$\Omega(\alpha, \beta) := \{y = \sum_{i=1}^{4} \beta_i u_i \in F | b(y,y) = f_0(y) = \alpha,\ \beta = \beta_1\}$$

for $\alpha \in S$ and $\beta \in F$. It hold that $\mathbf{T}$ is transitive on F $\cdots(1)$,

$< G, \mathbf{M} >$ is transitive on the 1-st neighborhood of 0 $\cdots(2)$,

G_{u_1}(the stabilizer of u_1) is transitive on $\Omega(\alpha, \beta)$ for $\alpha \in S,\ \beta \in F$ $\cdots(3)$.

We denote a triangle $\{a, b, c\}$ which satisfies "any two vertices in {a,b,c} are adjacent each other" by $\Delta(a, b, c)$.

For a triangle $\Delta(a, b, c)$, we denote the cardinality of $\{v \in F | v$ is adjacent to a, b and $c\}$ by $N(\Delta(a, b, c))$.

We take a triangle $\Delta(a', b', c')$ of $\Gamma(g, p)$.

If there is an isomorphism ψ from $\Gamma(g,p)$ to $\Gamma(f,p)$, then we may asumme $\psi(a') = 0$ from (1), $\psi(b') = u_1$ from (2) and $\psi(c') = y_{\alpha,\beta}$ for $y_{\alpha,\beta} \in \Omega(\alpha, \beta)$ for some α and β from (3).

Therefore if

$$N(\Delta(a', b', c')) \notin \{N(\Delta(0, u_1, y_{\alpha,\beta})) | \alpha \in S,\ \beta \in F\}$$

for a certain $\Delta(a', b', c')$ of $\Gamma(g, p)$, it means the non-isomorphism between $\Gamma(f, p)$ and $\Gamma(g, p)$.

We used Magma to compute $N(\Delta(0, u_1, y_{\alpha,\beta}))$ for each $\alpha \in S, \beta \in F$.

In the case of $p = 19$, there are exactly 81 $y_{\alpha,\beta} \in \Omega(\alpha, \beta)$ which are adjacent to the vertex 0 and vertex u_1.

Among them, differnt values of $N(\Delta(0, u_1, y_{\alpha,\beta}))$ are just 13 as the following.

{13851, 13882, 13896, 18915, 13920, 13946, 13958, 13972, 13977, 13996,

14003, 14124, 14034}

On the other hand, there exists triangles $\{a_i, b_i, c_i\}$ $(i = 1, 2, 3)$ in $\Gamma(g, p)$ such that $N(\Delta(a_1, b_1, c_1)) = 13801$, $N(\Delta(a_2, b_2, c_2)) = 13934$, $N(\Delta(a_3, b_3, c_3)) = 14281$.

References

[1] Y.M.Chee, Y. Tan and X.D. Zhang, Strongly Regular Graphs Constructed from p-ary Bent Functions, to appear in Journal of Algebraic Combinatorics.

[2] Dembowski P. and Ostrom G.T., Planes of Order n with Collineation Groups of Order n^2. Math. Z. 103 (1968), 239-258.

[3] T.Helleseth and A.Kholosha, New binomial bent functions over the finite fields of odd characteristic, Information Theory, IEEE Transactions on, 56(9): 4646-4652, sep.2010.

[4] P.V.Kumar, R.A.Scholtz and L.R.Welch, Generalized bent functions and their properties, J.Combin. Theory Ser.A,40(1): 90-107,1985.

[5] O.S.Rothaus, On "bent" functions, J.Combin. Theory Ser.A, 20(3): 300-305, 1976.

近似最尤推定復号に現れる組合せ論的側面

平岡裕章（九州大学 IMI／JST さきがけ）
林和則（京都大学情報学研究科）

この講演では誤り訂正符号理論へ力学系的視点を導入することで得られた幾つかの成果を報告する．結果の詳細は [1] を参照されたい．

1 通信路モデル

符号理論では通常図 1 で表される通信システムを考察する．信号源がメッセージ

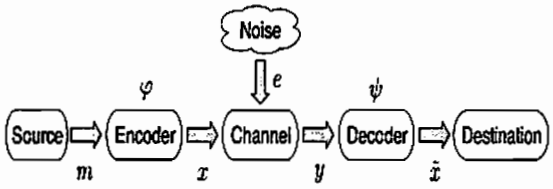


図 1: 通信システム

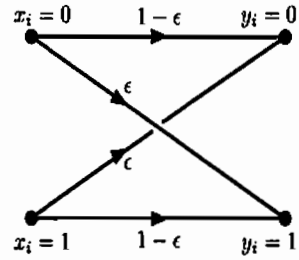


図 2: 2 元対称通信路（BSC）

$m = (m_1, \cdots, m_k)$ を目的地に伝送する際，通信路に存在するノイズ e の影響を軽減させる為に送信側で符号化 $x = (x_1, \cdots, x_n) = \varphi(m), k < n$, をおこなう．ここで符号化を表す写像 $\varphi : \mathbb{F}_2^k \to \mathbb{F}_2^n$ は単射とする（$\mathbb{F}_2 = \{0, 1\}$）．受信側ではノイズが加わった受信信号 $y = x + e \in \mathbb{F}_2^n$ が到達するが，復号操作 $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ によって推定語 $\tilde{x} = \psi(y)$ をもとめる．誤り訂正符号理論の目的は与えられた通信路に対して，冗長度 $k < n$ を使うことで可能な限りノイズの影響を除去できる符号化と復号化の対 (φ, ψ) を構成することである．ここで本講演では通信路モデルとして図 2 で表されている 2 元対称通信路（BSC）を考察する．つまり各ビットの入出力対応を表す条件付き確率を $P(y_i|x_i) = \epsilon$ もしくは $P(y_i|x_i) = 1 - \epsilon$ として図のように定め，ビット列に対しては無記憶性（$P(y|x) = P(y_1|x_1) \cdots P(y_n|x_n)$）を仮定する．

2 線形符号

符号化が線形写像 $\varphi = G = (g_1 \cdots g_n)$ で与えられる符号を線形符号とよぶ（G を生成行列と呼ぶ）．ここで $g_i = (g_{1i} \cdots g_{ki})^t$ は行列 G の列ベクトルを表すものとする．このとき全ての符号語の集合 $\mathcal{C}$ は次の 2 つの方法で表すことができる：

$$\mathcal{C} = \{(x_1 \cdots x_n) = (m_1 \cdots m_k)G \mid m_i \in \mathbb{F}_2\} = \{(x_1 \cdots x_n) \mid (x_1 \cdots x_n)H^t = 0\}.$$

ここで H はパリティ検査行列と呼ばれる $m \times n$ 行列（$m = n - k$）で，その行ベクトルは生成行列 G の行ベクトルが定める部分空間の直交補空間の基底で与えられる．

3 最尤推定（Maximum Likelihood）復号

最尤推定復号（以下 ML 復号）とは各ビットごとに次のルールで与えられる復号法 $\psi : \mathbb{F}_2^n \ni y \mapsto \hat{x} \in \mathbb{F}_2^n$ のことである：

$$\hat{x}_i = \psi_i(y) := \begin{cases} 1, & \sum_{x \in \mathcal{C},\ x_i = 0} P(y|x) \leq \sum_{x \in \mathcal{C},\ x_i = 1} P(y|x) \\ 0, & \text{その他} \end{cases}, \quad i = 1, \cdots, n. \tag{1}$$

最大の特徴として ML 復号は任意の符号化に対してビット誤り率の最小値を実現することが知られている．一方で式 (1) から明らかなようにその計算量は $O(2^k)$ でありこのままの形では実用化は不可能である．この ML 復号を「高精度かつ低演算に近似する」ことが本研究の動機の一つである．その戦略は，ML 復号を写像として定式化しその写像の構造をうまく反映させた近似法を考察することである．以下にその説明を行う．

4 主結果

まず初めに各符号語 $x \in \mathcal{C}$ に対して符号語多項式 $F_x(u_1, \cdots, u_n)$ を

$$F_x(u_1, \cdots, u_n) := \prod_{i=1}^{n} \rho_i(u_i), \qquad \rho_i(u_i) = \begin{cases} u_i, & x_i = 1, \\ 1 - u_i, & x_i = 0 \end{cases}$$

で定める．この符号語多項式を用いて次のような有理写像 $f : I^n \to I^n$, $I = [0, 1]$, を定義する：

$$\begin{aligned} & f : (u_1, \cdots, u_n) \mapsto (u'_1, \cdots, u'_n), \\ & u'_i = f_i(u) := \frac{\sum_{x \in \mathcal{C}, x_i = 1} F_x(u)}{H(u)}, \quad i = 1, \cdots, n, \\ & H(u) := \sum_{x \in \mathcal{C}} F_x(u). \end{aligned} \tag{2}$$

ここで $u = (u_1, \cdots, u_n)$ である．この有理写像が本研究で最も重要な働きをすることになる．

この有理写像の特徴の一つとして ML 復号を再現できることが挙げられる．受信語 $y \in \mathbb{F}_2^n$ に対して点 $u^0 \in I^n$ を

$$u_i^0 = \begin{cases} \epsilon, & y_i = 0 \\ 1 - \epsilon, & y_i = 1 \end{cases}, \quad i = 1, \cdots, n,$$

で定めよう．ここでϵはBSCの遷移確率である．するとML復号(1)は次のルールで与えられる復号法と同値であることが示せる：

$$\psi : \mathbb{F}_2^n \ni y \mapsto \tilde{x} \in \mathbb{F}_2^n,$$
$$\tilde{x}_i = \psi_i(y) := \begin{cases} 1, & f_i(u^0) \geq 1/2 \\ 0, & f_i(u^0) < 1/2 \end{cases}, \quad i = 1, \cdots, n. \tag{3}$$

これにより有理写像(2)はML復号と関係を持つことになるが，この橋渡しを通じて写像の力学系的性質が符号理論としての意味をもつことになる．有理写像力学系として重要になってくる性質を幾つかまとめておく．

命題 1 自然な埋め込み$\mathbb{F}_2^n \hookrightarrow I^n$のもとで有理写像(2)について以下が成り立つ．

1. $p = (1/2, \cdots, 1/2) \in I^n$は不動点．
2. $u \in \mathbb{F}_2^n$とする．このときuが不動点である必要十分条件はuが符号語であることである．更にこの不動点は安定である．
3. 有理写像の極は次で与えられる：

$$S := \left\{ u \in \partial(I^n) \;\middle|\; \begin{array}{l} (x_{i_1}, \cdots, x_{i_l}) = (u_{i_1}, \cdots, u_{i_l}) \text{ となる符号語 } x \in \mathcal{C} \text{ は存在しない．} \\ \text{ここで } u_{i_1}, \cdots, u_{i_l} \in \mathbb{F}_2, \text{かつ } 0 < u_i < 1,\ i \neq i_1, \cdots, i_l, \text{ である} \end{array} \right\}.$$

   特に非符号語は極である（$\mathbb{F}_2^n \setminus \mathcal{C} \subset S$）．

4. $u \in \mathrm{Int}(I^n)$が有理写像の不動点である必要十分条件は勾配系$du/dt = \mathrm{grad}(\log H(u))$の不動点であることである．

また不動点pの安定／不安定部分空間は直接求めることが可能であるが，それらは復号過程として重要な意味を持つことになる．この点については講演中に詳細に解説を行う．

ここで本講演の主結果の説明を行う．有理写像(2)の不動点pでのテイラー展開

$$f(u) = p + Jv + f^{(2)}(v) + \cdots + f^{(l)}(v) + O(v^{l+1}), \tag{4}$$

を考察しよう．ここで$v = (v_1, \cdots, v_n)$の各成分は$v_i = u_i - 1/2, i = 1, \cdots, n$，$J$はヤコビ行列，$f^{(i)}(v)$は$i$次項，$O(v^{l+1})$は$(l+1)$次以上の高次項を表す．高次項$O(v^{l+1})$を打ち切った有理写像(2)の近似写像

$$\tilde{f}(u) = p + Jv + f^{(2)}(v) + \cdots + f^{(l)}(v), \tag{5}$$

を用いることで，l次近似ML復号$\tilde{\psi}$が(3)の$f(u)$を$\tilde{f}(u)$で置き換えることにより得られる：

$$\tilde{\psi} : \mathbb{F}_2^n \ni y \mapsto \tilde{x} \in \mathbb{F}_2^n,$$
$$\tilde{x}_i = \tilde{\psi}_i(y) := \begin{cases} 1, & \tilde{f}_i(u^0) \geq 1/2 \\ 0, & \tilde{f}_i(u^0) < 1/2 \end{cases}, \quad i = 1, \cdots, n.$$

ML 復号を「高精度かつ低演算に近似する」ことが本研究の動機の一つであることは既に述べたが，これより式 (5) に対して次の要求が生まれる：

1. 高精度という観点から l は大きく取りたい

2. 低演算という観点から出来る限り非線形項の係数は 0 であってほしい

次の定理はこの 2 つの要望に答える為には生成行列を制御すればよいことを明らかにしている．

定理 2 $l \geq 2$ とする．もし生成行列 $G = (g_1 \cdots g_n)$ の全ての異なる l 個の列ベクトルが一次独立であるならば，有理写像のテイラー展開 (4) は次の形で与えられる：

$$f(u) = p + Jv + f^{(l)}(v) + O(v^{l+1}).$$

ここで $f^{(l)}(v)$ の各 i 番目の座標成分 $f_i^{(l)}(v)$ は次で与えられる：

$$f_i^{(l)}(v) = \sum_{(i_1,\cdots,i_l)\in\Theta_i^{(l)}} (-2)^{l-1} v_{i_1} \cdots v_{i_l} = -\frac{1}{2} \sum_{(i_1,\cdots,i_l)\in\Theta_i^{(l)}} (1-2u_{i_1}) \cdots (1-2u_{i_l}),$$

$$\Theta_i^{(l)} = \{(i_1,\cdots,i_l) \mid 1 \leq i_1 < \cdots < i_l \leq n,\ i_k \neq i\ (k=1,\cdots,l),\ g_i + g_{i_1} + \cdots + g_{i_l} = 0\}.$$

この定理によりパリティ検査行列の列ベクトルの一次独立性を制御する代数幾何符号の手法がそのまま近似 ML 復号の設計に使えることがわかる．またパリティ検査行列／生成行列間の双対性が符号化／復号化の双対性として有理写像を通じて現れていることにも注意したい．

5 数値計算結果

ここでは提案復号方式を実用化の際重要な指標となるビット誤り率特性の観点から性能比較をしてみる．比較対象としては現在様々な場面で実用化が進められている BCH 符号-Berlekamp-Massey 復号のペアを用いた．まずはじめに BSC の遷移確率を $\epsilon = 0.16$ に固定して符号化率に対するビット誤り率特性を調べる数値計算を行った．結果は図 3 で与えられる．

ここで横軸は符号化率 $r = k/n$，縦軸はビット誤り率であり，各プロットは $\times$：ランダム符号-3 次近似 ML 復号，$+$：ランダム符号-2 次近似 ML 復号，$*$：BCH 符号-Berlekamp-Massey 復号である．ここで近似 ML 復号に対する符号化方式としてランダム符号を選んでいる理由は，純粋に復号能力のみを調べるという目的からは符号化の際に不必要な構造を入れたくないからである．これにより符号化法によらない復号性能の平均的な振る舞いを特徴づけることが出来る．

図 3 から明らかなように，3 次近似 ML 復号特性は BCH 符号の特性より優れていることが見てとれる．ここで注意すべき点としては，あくまで近似 ML 復号で用い

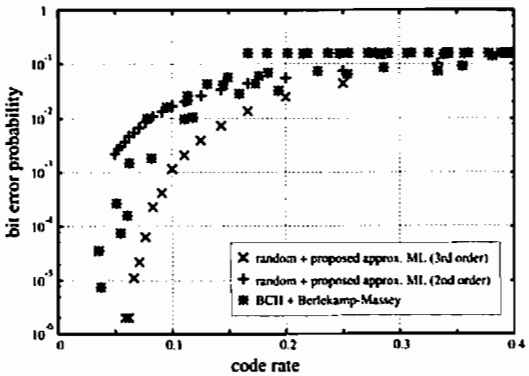


図 3: 遷移確率 $\epsilon = 0.16$ での数値計算．横軸：符号化率 $r = k/n$．縦軸：ビット誤り率．×：ランダム符号-3 次近似 ML 復号．＋：ランダム符号-2 次近似 ML 復号．∗：BCH 符号-Berlekamp-Massey 復号．

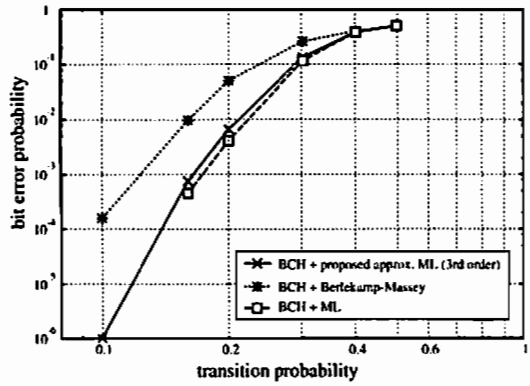


図 4: $k = 7, n = 63$ の BCH 符号に対する復号性能比較．横軸：遷移確率 ϵ．縦軸：ビット誤り率．×: 3次近似ML．∗: Berlekamp-Massaey 復号．□: ML．

ている符号化はランダム符号であることである．つまりこの提案復号方式を生かす符号化法を考察し適用することで，更にビット誤り率特性は良くなると思われる．

次に同じ BCH 符号に対して ML，近似 ML，Berlekamp-Massey 復号の性能を比較した数値計算結果が図 4 である．横軸は遷移確率であり，縦軸はビット誤り率，ここで新たに出てきたプロット □ は ML 復号である．まずはじめにプロット × (3 次近似 ML) と ∗ (Berlekamp-Massaey 復号) を比較してわかるように，提案復号方式は Berlekamp-Massey 復号よりも優れた特性を示している．特に遷移確率 $\epsilon = 0.1$ 付近では 2 桁も誤り率特性が改善されている点に注目されたい．また提案復号方式は誤り率の最小を実現する ML 復号（欠点は計算量が指数オーダーであり実用化は不可能）と極めて近い特性を示している．計算量についての数学的に厳密な議論はここでは行わないが，3 次近似 ML 復号の実行計算時間は ML 復号と比べてとても高速であり，Berlekamp-Massey 復号と同程度（状況によってはそれより高速）である．定性的な説明としては，近似 ML 復号の計算量は写像 (5) の非零係数の個数 $\Theta_i^{(l)}$ で定まるが，これは 1 次関係式を満たす生成行列の列ベクトルの組で与えられる．一方でそのような高余次元な事象がおこることはまれであるためにほぼ全ての係数は零となり本質的な係数のみが非線形項に現れることになる．これにより低演算型の復号が実現できることになる．

これまでの議論をまとめるとこれらの数値計算結果は，提案復号方式である 3 次近似 ML 復号が ML 復号を「高精度かつ低演算」で近似していることを示している．

6 今後の課題

今後の課題について，特に力学系との接点という視点でまとめてみる．最大の課題はここでの提案復号方式を軸にして，シャノン限界（通信路容量）を実現する符号-復号対の列を具体的に構成することである．そこで本提案復号方式の特徴を生かす符号化法を逆に考えることになるが，その為には有理写像 (2) に関する以下の力学系的考察が重要になってくる．

1. 符号語に対応する安定不動点のアトラクター領域の特徴付け
2. 非符号語に対応する極のブローアップ解析
3. 点 $p = (1/2, \cdots, 1/2)$ でのより大域的なダイナミクスの理解
4. 点 $p = (1/2, \cdots, 1/2)$ での標準形と代数幾何符号

これらのついての詳細は講演中に解説を行う．

謝辞

この研究は Topology, Informatics, and Network 勉強会 [2] での継続的な議論をもとに始められたものである．ここに参加メンバーの方々，原晋介（大阪市大），国府寛司（京大），桶谷賢吾（NEC），荒井迅（北大），石井豊（九大），小川知之（阪大）氏に感謝したい．

参考文献

[1] K. Hayashi and Y. Hiraoka, Rational Maps and Maximum Likelihood Decodings, http://arxiv.org/pdf/1006.5688v1

[2] `http://www.mis.hiroshima-u.ac.jp/~hiraoka/tin.htm`

Kleinian codes and vertex operator algebras associated with even lattices

島倉 裕樹 (Hiroki Shimakura)

愛知教育大学
Aichi University of Education
e-mail: shima@auecc.aichi-edu.ac.jp

本稿では格子から得られる VOA の同型問題について論じた [Sh] の解説を行う．特に [島倉] では述べられていない Kleinian 符号との関係を中心に述べる．

1 問題背景

頂点作用素代数 (VOA) の重要な例の一つであるムーンシャイン VOA がリーチ格子から構成されていることからわかるように，VOA と組合せ論との関係は非常に深い．したがって，次の問題は非常に重要である．

問題 1.1. 二元符号，格子と頂点作用素代数の間の類似や関係を見つけよ．

例 1.2. (拡張) ゴレイ符号，リーチ格子，ムーンシャイン頂点作用素代数は対応する対象物であると考えられる．その一つの理由は "一意性" にある．ゴレイ符号は長さ 24 の重偶自己双対符号で最小重みが 8 である一意的な二元符号であり，[1] リーチ格子は階数 24 のユニモジュラ偶格子で最小ノルムが 4 である一意的な格子である．[2] そして，ムーンシャイン頂点作用素代数は中心電荷が 24 の正則 VOA で最小重みが 2 である一意的な頂点作用素代数と予想されている ([FLM88])．また，これらの自己同型群にマシュー群，コンウェイ群，モンスター群というような散在型有限単純群が現れることも偶然ではないであろう．別の類似として，これら 3 つには $24 = 8 \times 3$ に対応する $\mathbb{F}_2$ 上の二次形式を持つ空間を用いた記述がある ([MS77, LM82, Sh11])．

例 1.3. 重偶自己双対符号の最小重みの上限 ([MS73])，ユニモジュラ偶格子の最小ノルムの上限 ([MOS75])，正則 VOA の最小共形重みの上限 ([Hö95]) には類似がある．具体的には，符号の長さ，格子の階数，VOA の中心電荷を n としたときに，次が上界となる:

$$4\lfloor\frac{n}{24}\rfloor + 4, \quad 2\lfloor\frac{n}{24}\rfloor + 2, \quad \lfloor\frac{n}{24}\rfloor + 1.$$

[1] もちろん，座標の置換による同値を除く．
[2] もちろん，24 次の直交群の作用による同型を除く．

例 1.4. 符号にはブロックデザイン, 格子には球面上のデザインが定義されることがよく知られている. その "ある種" の類似として VOA に付随する共形デザインが定義できる ([Hö08]). そして, 共形デザインにも Assmus-Mattson の定理の類似が成り立つ事が示されている. しかしながら, 類似として理解するためには, さらなる研究が必要と思われる.[3]

そして, Höhn は次の提案をしている.

提案 1.5. [Hö03] Kleinian 符号を二元符号の前に来る対象物として考えよう.

例 1.6. Hexacode が対応するゴレイ符号等に対応する対象物である. また, 自己双対偶 Kleinian 符号の最小重みの上界, 一般化されたデザインの理論等の様々な類似が確認されている ([Hö03]).

[Sh] の主定理から次が得られた.

結果 1.7. 同型問題を通じて, Kleinian 符号から得られる二元符号, 二元符号から得られる格子, 格子から得られる VOA の間の一つの類似が見つかった.

2 Kleinian 符号

本稿で必要な Kleinian 符号に関する定義を思い出す. 詳細は [Hö03] を参照にされたい. $\mathbb{K} = \{0, a, b, c\}$ でクラインの四元群 $\mathbb{Z}_2 \times \mathbb{Z}_2$ を表すこととする.

定義 2.1. 長さ n の (線形) **Kleinian 符号** とは $\mathbb{K}^n \cong \mathbb{Z}_2^{2n}$ の部分群のことである.

$\mathbb{K}^n$ の元 x を座標表示を用いて $x = (x_i)$ のように書くこととする. x の**重さ**とは 0 でない成分の個数である. Kleinian 符号 K が**偶**であるとは, K の任意の元の重さが偶数となることである. 双線形対称形式を $\mathbb{K}^n \times \mathbb{K}^n \to \mathbb{F}_2$, $(x, y) \mapsto x \cdot y = \sum_{i=1}^n x_i \cdot y_i$, $a \cdot b = b \cdot a = 1$, $a \cdot c = c \cdot a = 1$, $c \cdot b = b \cdot c = 1$, その他は 0 で定める. Kleinian 符号が**自己双対**とは, 直交補空間と一致することである.

長さが 8 以下の Kleinian 符号は [Hö03] で分類されている. 特に, 次が成立する.

例 2.2. [Hö03]

(1) 長さ 2 の自己双対偶 Kleinian 符号は同値[4]を除いて唯一つである. それは $\epsilon_2 = \langle (aa), (bb) \rangle$ である.

(2) 長さ 4 の自己同対偶 Kleinian 符号は同値を除いて丁度二つある. それらは ϵ_2^2 と $\delta_4^+ = \langle (aa00), (a0a0), (a00a), (bbbb) \rangle$ である.

注意 2.3. 例 2.2 は, 二元符号における長さ 8 の自己双対重偶符号が (同値を除いて) 拡張ハミング符号 e_8 の唯一つであり, 長さ 16 の自己双対重偶符号が (同値を除いて) 丁度二つで e_8^2 と d_{16}^+ であることに対応している.

[3]例えば, 現在の共形デザインの定義には VOA が必要であるが, ブロックデザインや球面デザインには符号や格子は不要である. ゆえに, 現在の定義が "最良" かどうかはよく分からない.

[4]一般に, 二つの Kleinian 符号が同値であるとは, 座標の置換と各座標における $\{a, b, c\}$ の置換の作用で移り合うときをいう. すなわち $S_3 \wr S_n$ の作用で同値を入れている.

3 二元符号, 格子, VOA の構成法

本章では Kleinian 符号, 二元符号, 格子から二元符号, 格子, VOA の構成法について簡単に述べる.

3.1 Kleinian 符号を用いた二元符号の構成法

自然数 m に対して,

$$d_4^m = \{(0000),(1111)\}^m \subset \mathbb{F}_2^{4m}, \quad (d_4^m)_0 = \{c \in d_4^m \mid \mathrm{wt}(c) \in 8\mathbb{Z}\}$$

と置く.

長さ m の Kleinian 符号 K に対して

$$\begin{aligned} \mathcal{C}(K) &= \hat{K} + d_4^m \subset \mathbb{F}_2^{4m}, \\ \mathcal{C}^+(K) &= \hat{K} + (d_4^m)_0 \subset \mathbb{F}_2^{4m}, \end{aligned}$$

は長さ $4m$ の二元符号となる. ただし, $\hat{}$ は $\mathbb{K} \to \mathbb{F}_2^4, 0 \mapsto (0000), a \mapsto (1100), b \mapsto (1010), c \mapsto (0110)$ を各座標成分毎に適用して得られる写像である. すると, 次が成立する.

補題 3.1. [Hö03]

(1) K が自己双対ならば $\mathcal{C}(K)$ も自己双対である.

(2) K が偶ならば $\mathcal{C}(K)$ と $\mathcal{C}^+(K)$ は重偶である.

3.2 二元符号を用いた格子の構成法

長さ n の二元符号 C に対して,

$$\begin{aligned} \mathcal{L}(C) &= \frac{1}{\sqrt{2}}\{(x_i) \in \mathbb{Z}^n \mid (\overline{x_i}) \in C\}, \\ \mathcal{L}^+(C) &= \frac{1}{\sqrt{2}}\{(x_i) \in \mathbb{Z}^n \mid (\overline{x_i}) \in C, \sum_{i=1}^n x_i \in 4\mathbb{Z}\}, \end{aligned}$$

は階数 n の格子となる. ただし $\bar{}$ は自然な写像 $\mathbb{Z} \to \mathbb{Z}_2$ である.

補題 3.2. [CS99]

(1) C が自己双対ならば $\mathcal{L}(C)$ はユニモジュラである.

(2) C が重偶であれば $\mathcal{L}(C)$ と $\mathcal{L}^+(C)$ は偶である.

3.3 格子を用いた VOA の構成法

階数 n の偶格子 L に対して, V_L で中心電荷 n の格子 VOA ([FLM88]) を表す. 格子の -1 倍する自己同型の V_L の持ち上げを θ とすると, 固定部分空間 $V_L^+ = \{v \in V_L \mid \theta(v) = v\}$ は部分 VOA となる.

補題 3.3. [Do93] L がユニモジュラならば V_L は正則である.

注意 3.4. 二元符号における重偶, 格子における偶に対応する性質は VOA の定義の中の「整数で次数付けされている」に対応する.[5]

注意 3.5. 今までに見てきた構成法が対応することを意味する一つの例は $\mathcal{C}(\epsilon_2) \cong e_8$, $\mathcal{L}(e_8) \cong E_8$, V_{E_8} がそれぞれある種の性質をもつ一意的な対象物であることがある. また $\mathcal{C}^+(\mathcal{C}_6) \subset G_{24}$, $\mathcal{L}^+(G_{24}) \subset \Lambda$, $V_\Lambda^+ \subset V^\natural$ のように, "拡大"することでゴレイ符号, リーチ格子, ムーンシャイン VOA が順々に得られる. ただし $\mathcal{C}_6$ は Hexacode である. さらに, 重み関数, テータ級数, 指標においても対応が読み取れる.

4 同型問題

前章で得られた格子、VOA に対する同型問題の答えは次のようになる.

定理 4.1. [Sh] L, N を階数 n の偶格子とする.

(1) $V_L \cong V_N \Leftrightarrow L \cong N$.

(2) $V_L^+ \cong V_N^+ \Leftrightarrow L \cong N$ or $\{L, N\} = \{E_8^{\oplus 2}, D_{16}^+\}$.

(3) $V_L^+ \cong V_N \Leftrightarrow \exists C \subset \mathbb{F}_2^n$ s.t. $L \cong \mathcal{L}(C)$ and $N \cong \mathcal{L}^+(C)$.

定理 4.2. [KKM91, Sh] C, D を長さ n の重偶符号とする.

(1) $\mathcal{L}(C) \cong \mathcal{L}(D) \Leftrightarrow C \cong D$.

(2) $\mathcal{L}^+(C) \cong \mathcal{L}^+(D) \Leftrightarrow C \cong D$ or $\{C, D\} = \{h_8^{\oplus 2}, d_{16}^+\}$.

(3) $\mathcal{L}^+(C) \cong \mathcal{L}(D) \Leftrightarrow \exists K \subset \mathbb{K}^{n/4}$ s.t. $C \cong \mathcal{C}(K)$ and $D \cong \mathcal{C}^+(K)$.

これら結果の比較から, 丁度 Kleinian 符号が二元符号の一つ前の対象物となるだろう事が読み取れる.[6]

証明の中で鍵となった補題は次の通りである. これらの補題を用いて, VOA の議論から格子の議論, 二元符号の議論, そして Kleinian 符号の議論へ持って行き, 証明を分かりやすくしている,

[5]例えば, 奇格子に対応する概念が超 VOA である. 奇格子の任意の元が整数ノルムを持つことに対応して, 超 VOA は半整数で次数付けされている.

[6][島倉] では Kleinian 符号を用いていないために, あまり整理されてない主張になっている.

補題 4.3. [Sh06] L を階数 n の偶格子とする. このとき $L \cong \mathcal{L}^+(C)$ となる長さ n の重偶二元符号 C が存在するための必要十分条件は $|(\lambda+L)(2)| \geq 2n+|L(2)|$ を満たすような $\lambda+L \in (L^* \cap L/2)/L$ が存在することである.

さらに, このとき, $L+\mathbb{Z}\lambda \cong \mathcal{L}(C)$ が成立する.

補題 4.4. [Sh] C を長さ n の重偶二元符号とする. このとき $C \cong \mathcal{C}^+(K)$ となる長さ $n/4$ の偶 Kleinian 符号 K が存在するための必要十分条件は $|(x+C)(4)| \geq n/4+|C(4)|$ を満たすような $x+C \in C^\perp/C$ が存在することである.

さらに, このとき, $C+\mathbb{F}_2 x \cong \mathcal{C}(K)$ が成立する.

類似の視点から, 例えば次の問題が残っている.

- V_L から $\mathbb{Z}_2$-軌道体構成法で得られる VOA と $\mathcal{L}(C)$ の近傍として得られる偶格子との間の対応や類似の性質の研究.
- 既約加群の重さ 1 の空間の次元を用いた V_L^+ の特徴付け.

VOA を符号や格子の類似として捉える事で, 様々なアイデアを導入することが出来る一方で, VOA まで含めた視点で符号と格子の類似を見直すことで, 新しい成果が得られることが期待される.

参考文献

[CS99] J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, 3rd Edition, Springer, New York, 1999.

[Do93] C. Dong, Vertex algebras associated with even lattices, *J. Algebra* **161** (1993), 245–265.

[FLM88] I. Frenkel, J. Lepowsky and A. Meurman, Vertex operator algebras and the Monster, Pure and Appl. Math., Vol.134, Academic Press, Boston, 1988.

[Hö95] G. Höhn, Selbstduale Vertexoperatorsuperalgebren und das Babymonster, Dissertation, Rheinische Friedrich-Wilhelms-Universitat Bonn, Bonn, 1995.

[Hö03] G. Höhn, Self-dual codes over the Kleinian four group, *Math. Ann.* **327** (2003), 227–255.

[Hö08] G. Höhn, Conformal designs based on vertex operator algebras, *Adv. Math.* **217** (2008), 2301–2335.

[KKM91] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly-even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[LM82] J. Lepowsky and A. Meurman, An E_8-approach to the Leech lattice and the Conway group, *J. Algebra* **77** (1982), 484–504.

[MOS75] C.L. Mallows, A.M. Odlyzko and N.J.A. Sloane, Upper bounds for modular forms, lattices, and codes, *J. Algebra* **36** (1975), 68–76.

[MS77] F.J. MacWilliams, and N.J.A. Sloane, The theory of error-correcting codes, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977

[MS73] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Information and Control* **22** (1973), 188–200.

[Sh06] H. Shimakura, The automorphism groups of the vertex operator algebras V_L^+: general case, *Math. Z.* **252** (2006), 849–862.

[Sh11] H. Shimakura, An E_8-approach to the moonshine vertex operator algebra, *J. London Math. Soc.* **83** (2011), 493–516.

[Sh] H. Shimakura, On isomorphism problems for vertex operator algebras associated with even lattices , to appear in *Proc. Amer. Math. Soc.*, arXiv:1104.0714.

[島倉] 島倉裕樹, Even lattices obtained from doubly even codes and VOAs obtained from even lattices. 数理解析研究所講究録 **1656** (2009), 74–83.

半正定値計画法に基づく多重交差集合について

東北大学大学院情報科学研究科　須田庄

1 序

1961 年に Erdős,Ko,Rado[2] によって示された交差族に関する定理はそれ以降, 様々な研究者により一般化されている. 本報告集では Matsumoto-Tokushige[6] によって与えられた定理の半正定値計画法を用いた別証明を与える. 現段階では真に新しい結果ではないものの, ここで提唱する方針により未解決である $t \geq 2$ の場合や考えている空間を変えた場合に対する多重交差集合の定理を示せる可能性が十分に見込まれる. 本研究は東北大学の田中太初氏との共同研究に基づくものである.

2 Cross intersection families

v, d_1, d_2, t を $2 \leq t \leq d_1 \leq d_2 \leq v/2$ を満たす整数とする. $\Omega = \{1, 2, \ldots, v\}$ とし, $i = 1, 2$ に対して $\binom{\Omega}{d_i}$ を Ω の d_i 点からなる部分集合全体とする. $\binom{\Omega}{d_i}$ の部分集合 $Y_i (i = 1, 2)$ が cross t-intersecting とは, 任意の $x_1 \in Y_1, x_2 \in Y_2$ に対して $|x_1 \cap x_2| \geq t$ を満たすときとする. 考えたい問題は cross t-intersecting である Y_1, Y_2 に対して,Y_1, Y_2 のサイズを v, d_1, d_2, t を用いて上から押えること, さらにその不等式で等号が成立するときの Y_1, Y_2 に関する条件を求めることである. $d := d_1 = d_2$ かつ $Y := Y_1 = Y_2$ のとき, 上記の cross t-intersecting は単に t-intersecting と呼ばれ, このときに Wilson[11] により次の定理が得られている.

Theorem 2.1. $v > (t+1)(d-t+1)$ とし,Y を *t-intersecting* とする. このとき $|Y| \leq \binom{v-t}{d-t}$ が成立ち, 等号成立の必要十分条件は Y が Ω のある t 点部分集合を含む d 点部分集合全体からなるときに限る.

交差族の問題は Johnson graph の部分集合に対して width を固定したとき, その部分集合のサイズを上から評価すること, さらには等号成立するときの特等付けを行うことと同値である. この視点でのアソシエーションスキームにおける統一的な展開としては [9] を参照されたい.

$d := d_1 = d_2$ の cross の場合には数多くの結果が知られており, 次の Wang-Zhang[10] による結果が決定的である.

Theorem 2.2. $Y_1, Y_2, \ldots, Y_n$ を $\binom{\Omega}{d}$ の部分集合で相異なる i, j に対して Y_i, Y_j は *cross t-intersecting* とする．このとき次の不等式が成立つ：

$$\sum_{i=1}^{n} |Y_i| \leq \begin{cases} \binom{v}{d} & n \leq \frac{\binom{v}{d}}{\binom{v-t}{d-t}} \text{のとき}, \\ n\binom{v-t}{d-t} & n \geq \frac{\binom{v}{d}}{\binom{v-t}{d-t}} \text{のとき}. \end{cases}$$

$d_1 < d_2, t = 1$ の cross の場合には Matsumoto-Tokushige により次の定理も示されている．

Theorem 2.3. $Y_i (i = 1, 2)$ を $\binom{\Omega}{d_i}$ の部分集合で Y_1, Y_2 は *cross 1-intersecting* とする．このとき次の不等式が成立つ：

$$|Y_1||Y_2| \leq \binom{v-1}{d_1-1}\binom{v-1}{d_2-1}.$$

等号成立の必要十分条件は $i = 1, 2$ に対して Y_i は Ω のある一点を含む d_i 点部分集合全体からなるときである

本稿で焦点に当てたいのは Matsumoto-Tokushige によって与えられてたサイズの積に関する多重交差族の定理の別証を与えることである．用いる手法は半正定値計画法である．Wilson は線形計画法を用いて t-intersecting family に関する最良の結果を得ていたように，多重交差族に半正定値計画法を適用することは非常に自然な発想といえる．実際,Wang-Zhang の結果ほどは良くないものの,[8] によって多数の P- and Q-polynomial association scheme に対して $\sum_{i=1}^{n} \sqrt{|Y_i|}$ を上から評価する多重交差族の定理が半正定値計画法を用いて得られている．

t-intersecting families Y_1, Y_2 に代数的な手法を適用するため，次のような設定を考える．$X = \{0, 1\}^v$ とする．$\binom{\Omega}{d_i}$ の元をその特性ベクトルと同一視することによって X の元とみなすことにする．これにより Y_i の特性ベクトルを χ_i とすると，次の条件は同値である：

(1) Y_i, Y_2 は cross t-intersecting.

(2) $\chi_1^T A_h \chi_2 = 0$ $(d_1 + d_2 - 2t < h \leq v)$.

ここで A_h は X を頂点集合とする Hamming scheme の隣接行列である．この後者の性質を用いて多重交差族に関する考察を半正定値法を用いて行う．

3 Terwilliger algebra of the Hamming scheme

整数 $0 \leq i \leq v$ に対して，X 上の二項関係 R_i を次で定める：$R_i = \{(x, y) : d(x, y) = i\}$．ここで X の元 $x = (x_i)_{i=1}^v, y = (y_i)_{i=1}^v$ に対して，$d(x, y) = |\{i \mid 1 \leq i \leq v, x_i \neq y_i\}|$ である．各 R_i に対して (一般に勝手な二項関係に対して) 行と列が X の元で添え字付けられている正方行列で成分が $0, 1$ の隣接行列 A_i が定まる：

$$(A_i)_{x,y} = \begin{cases} 1 & (x, y) \in R_i \text{のとき}, \\ 0 & \text{そうでないとき}. \end{cases}$$

このとき有限集合と二項関係の組 $(X, \{R_i\}_{i=0}^v)$ はアソシエーションスキームになる (次の性質がアソシエーションスキームの公理である)：

(1) $R_0, \ldots, R_v$ は $X \times X$ の分割である.

(2) $R_0 = \{(x,x) : x \in X\}$.

(3) 任意の i に対し i' が存在して $R_i^T := \{(x,y) : (y,x) \in R_i\} = R_{i'}$ が成立つ.

(4) i,j,k を任意に固定したとき,$(x,y) \in R_k$ に対して $p_{i,j}^k := |\{z \in X : (x,z) \in R_i, (z,y) \in R_j\}|$ の値は i,j,k にのみ依存して決まり,$(x,y) \in R_k$ の取り方によらない.

(5) 任意の i,j,k に対して $p_{i,j}^k = p_{j,i}^k$ が成立つ.

アソシエーションスキームを定める二項関係の隣接行列が $\mathbb{C}$ 上で生成する代数を Bose-Mesner 代数と呼ばれる. ここで定義された $(X, \{R_i\}_{i=0}^v)$ は Hamming scheme と呼ばれている.

次に Hamming scheme の Terwilliger algebra を定義しよう. $x := (0, \ldots, 0)$ に対して対角行列 $E_i^* = E_i^*(x)$ を次で定める：

$$(E_i^*)_{y,y} = \begin{cases} 1 & (x,y) \in R_i \text{のとき}, \\ 0 & \text{そうでないとき}. \end{cases}$$

このとき $E_i^* A_k E_j^* (0 \le i,j,k \le v)$ で生成される Bose-Mesner 代数の部分代数 $\boldsymbol{T}$ を x における Terwilliger 代数と呼ぶ. これはある coherent configuration の coherent algebra になることが知られている. Coherent configuration とはアソシエーションスキームの一般化であり, 上記のアソシエーションスキームの公理の (5) を取り除き,(2) を次の性質に変えた有限集合と二項関係の組のことである：

$$\{(x,x) : x \in X\} \text{ はある } R_i \text{達の合併集合になる}.$$

Coherent algebra とは coherent configuratin の二項関係の隣接行列が生成する代数である. Hamming scheme の Terwilliger algebra が定める coherent configuration とは二項関係の隣接行列が $E_i^* A_k E_j^*$ となるものである.

4 Positive semidefinite matrix associated with a subset in a coherent configuration

Hobart [3] は coherent configuration を定める有限集合の部分集合に対して, その inner distribution から半正定値行列が定まることを示した. これはアソシエーションスキームの部分集合の inner distribution の MacWilliam 変換である dual inner distribution が非負実数値ベクトルになる, という現象を coherent configuraiton へ拡張したものである.

Coherent configuration を $(X, \{f_i\}_{i \in I})$ とし,f_i の隣接行列を A_i とする. 各 i に対して,$m_i = |f_i|$ とおく. Y を X の部分集合とし,Y の inner distribution$(b_i)_{i \in I}$ を次で定める：

$$b_i = |\{(x,y) \in Y \times Y : (x,y) \in f_i\}|.$$

このとき, 次の定理が成立つ. 証明は [3, Theorem 2. 2] を参照されたい.

Theorem 4.1. $D(Y) := \sum_{i\in I} \frac{b_i}{m_i} A_i$ は半正定値行列である.

定理 4.1 を Hamming scheme の Terwilliger algebra が成す coherent algebra と t-intersecting である Y_1, Y_2 に適用する. $T_{d_1,d_2} = (E^*_{d_1} + E^*_{d_2})T(E^*_{d_1} + E^*_{d_2})$ とする. T_{d_1,d_2} は T の頂点集合を $\binom{\Omega}{d_1} \cup \binom{\Omega}{d_2}$ へ制限したもので, 再び coherent algebra になる. Cross t-intersecting である Y_1, Y_2 の特性ベクトルをそれぞれ χ_1, χ_2 としたとき, 定理 4.1 を $y := \frac{\chi_1}{|\chi_1|} + \frac{\chi_2}{|\chi_2|}$ に適用する. $y^h_{ij} = \frac{\chi_i}{|\chi_i|}^T A_h \frac{\chi_j}{|\chi_j|}$ とする. このとき

$$\sum_{i=0}^{d_1} \frac{y^{2i}_{11}}{\binom{v}{i,i,d_1-i,v-d_1-i}} E^*_{d_1} A_{2i} E^*_{d_1} + \sum_{i=0}^{d_2} \frac{y^{2i}_{22}}{\binom{v}{i,i,d_2-i,v-d_2-i}} E^*_{d_2} A_{2i} E^*_{d_2}$$
$$+ \sum_{i=0}^{d_1-t} \frac{y^{d_2-d_1+2i}_{12}}{\binom{v}{i,d_1-i,d_2-d_1+i,v-d_2-i}} (E^*_{d_1} A_{d_2-d_1+2i} E^*_{d_2} + E^*_{d_2} A_{d_2-d_1+2i} E^*_{d_1}) \quad (4.1)$$

は半正定値行列であることがわかる.

Schriver[7] により T_{d_1,d_2} の Wedderburn 分解が求められているのでそれを用いると (4.1) の半正定値性は次の行列の半正定値性と同値である：

$$\begin{pmatrix} \sum_{i=0}^{d_1} y^{2i}_{11} \cdot Q_r(i;\alpha_1,\beta_1,d_1) & \sum_{i=0}^{d_1-t} y^{d_2-d_1+2i}_{12} \cdot Q_r(i;\alpha_2,\beta_2,d_1) \cdot \sqrt{\frac{(-d_1)_r(d_2-v)_r}{(-d_2)_r(d_1-v)_r}} \\ \sum_{i=0}^{d_1-t} y^{d_2-d_1+2i}_{12} \cdot Q_r(i;\alpha_2,\beta_2,d_1) \cdot \sqrt{\frac{(-d_1)_r(d_2-v)_r}{(-d_2)_r(d_1-v)_r}} & \sum_{i=0}^{d_2} y^{2i}_{22} \cdot Q_r(i;\alpha_2,\beta_2,d_2), \end{pmatrix} \quad (4.2)$$

$0 \le r \le d_1$,

$$\left(\sum_{i=0}^{d_2} y^{2i}_{22} \cdot Q_r(i;\alpha_2,\beta_2,d_2). \right) \quad (4.3)$$

$d_1 < r \le d_2$. ここで

$$Q_n(x;\alpha,\beta,N) = {}_3F_2\left(\begin{matrix} -n, n+\alpha+\beta+1, -x \\ \alpha+1, -N \end{matrix} \middle| 1 \right) \quad (0 \le n \le N),$$

$$\alpha_1 = d_1 - v - 1,\ \beta_1 = -d_1 - 1,\ \alpha_2 = d_2 - v - 1,\ \beta_2 = -d_2 - 1,$$

である. これより次の半正定値計画問題が設定できる:

$$\begin{array}{ll} \text{maximize} & \sum_{i=0}^{d_1-t} y^{d_2-d_1+2i}_{12} = \sqrt{|Y_1||Y_2|} \\ \text{subject to} & y^h_{ij} \ge 0 \text{ for all } i,j,h, \\ & y^0_{11} = y^0_{22} = 1, \\ & (4.2), (4.3) \text{ are positive semidefinite for } 0 \le r \le d_2. \end{array} \quad (\mathrm{P})$$

$F_0, F_1, \ldots, F_{d_1} \in S\mathbb{R}^{2\times 2}$, $f_{d_1+1}, f_{d_1+2}, \ldots, f_{d_2} \in \mathbb{R}$ とすると, 上記の双対問題は次で与えられる：

$$
\begin{aligned}
\text{minimize} \quad & \operatorname{tr}\left(\sum_{r=0}^{d_1} F_r\right) + \sum_{r=d_1+1}^{d_2} f_r \\
\text{subject to} \quad & F_0 \succcurlyeq \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}, F_1, \ldots, F_{d_1} \succcurlyeq 0, \quad f_{d_1+1}, f_{d_1+2}, \ldots, f_{d_2} \geq 0 \\
& \sum_{r=0}^{d_1} Q_r(i; \alpha_1, \beta_1, d_1)(F_r)_{11} \leq 0 \quad (1 \leq i \leq d_1) \\
& \sum_{r=0}^{d_1} Q_r(i; \alpha_2, \beta_2, d_1)\sqrt{\tfrac{(-d_1)_r(d_2-v)_r}{(-d_2)_r(d_1-v)_r}}(F_r)_{12} \leq 0 \quad (0 \leq i \leq d_1 - t) \\
& \sum_{r=0}^{d_1} Q_r(i; \alpha_2, \beta_2, d_2)(F_r)_{22} + \sum_{r=d_1+1}^{d_2} Q_r(i; \alpha_2, \beta_2, d_2) f_r \leq 0 \quad (1 \leq i \leq d_2)
\end{aligned}
\tag{D}
$$

実際, 次のように双対性を確認できる. 表記を簡単にするため $F_h := \begin{pmatrix} 0 & 0 \\ 0 & f_h \end{pmatrix}$ $(d_1 + 1 \leq h \leq d_2)$, $D_h := (y_{ij}^{d_j - d_i + 2h})_{1 \leq i,j \leq 2}$ $(0 \leq h \leq d_2)$, $Q_{h\ell} := (Q_{h\ell}^{ij})_{1 \leq i,j \leq 2}$ $(0 \leq h, \ell \leq d_2)$ とおく. 型が同一の行列 A, B に対して, $A \bullet B := \operatorname{Tr} AB^T$ としたとき,

$$
\begin{aligned}
\operatorname{tr}(\textstyle\sum_{\ell=0}^{d_2} F_\ell) &= (\textstyle\sum_{\ell=0}^{d_2} Q_{0\ell} \circ F_\ell) \bullet I_2 \\
&\geq (\textstyle\sum_{\ell=0}^{d_2} Q_{0\ell} \circ F_\ell) \bullet D_0 \\
&\geq \textstyle\sum_{h=0}^{d_2} (\sum_{\ell=0}^{d} Q_{h\ell} \circ F_\ell) \bullet D_h \\
&= \sum_{\ell=0}^{d_2} (\sum_{h=0}^{d_2} Q_{h\ell} \circ D_h) \bullet F_\ell \\
&\geq (\textstyle\sum_{h=0}^{d_2} D_h) \bullet \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \\
&= \sum_{i=0}^{d_1 - t} y_{12}^{d_2 - d_1 + 2i}.
\end{aligned}
$$

従って $|Y_1||Y_2|$ の上界を求めるためには双対問題の feasible parameters$F_r (0 \leq r \leq d_2)$ を与えればよい.

5 Main theorem

Theorem 5.1. $Y_1 \subset \binom{\Omega}{d_1}, Y_2 \subset \binom{\Omega}{d_2}$ を *cross t-intersecting* とする. このとき $v \geq d_1 + 2d_2 - 1$ であれば $|Y_1||Y_2| \leq \binom{v-1}{d_1-1}\binom{v-1}{d_2-1}$ が成立つ. 更に等号成立の必要十分条件は各 Y_i が Ω のある一点を含む Ω の d_i 点部分集合全体からなるときである.

Proof. 次によって定める $F_r := (f_r^{ij})_{1\le i,j\le 2}$ が (D) の条件を満たすことを見ればよい：

$$f_r^{11} = \frac{\sqrt{\binom{v-1}{d_1-1}\binom{v-1}{d_2-1}}}{2}\frac{\binom{v}{r}(v-2r+1)\left(\binom{v-d_1}{d_1}-(-1)^r\binom{v-d_1-r}{d_1-r}\right)}{(v-r+1)\binom{v-d_1}{d_1}\binom{v}{d_1}},$$

$$f_r^{22} = \frac{\sqrt{\binom{v-1}{d_1-1}\binom{v-1}{d_2-1}}}{2}\frac{\binom{v}{r}(v-2r+1)\left(\binom{v-d_2}{d_2}-(-1)^r\binom{v-d_2-r}{d_2-r}\right)}{(v-r+1)\binom{v-d_2}{d_2}\binom{v}{d_2}},$$

$$f_r^{12} = \frac{(-1)^r(v-2r+1)(-v-1)_{d_1+1}(d_2-r+1)_r}{2(v+1)r!(-v+r-1)_{d_1+1}}\sqrt{\frac{(-d_2)_r(-v+d_1)_r}{(-d_1)_r(-v+d_2)_r}}.$$

ここで,$F_0 = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$ であり,$1 \le r \le d_i$ に対して f_r^{ii} は非負である. $1 \le i \le j \le 2$ に対して, Q^{ij} を正方行列で (r,h) 成分が次で与えられているとする：$Q_r(h;\alpha_j,\beta_j,d_i)\sqrt{\frac{(-d_i)_r(d_j-v)_r}{(-d_j)_r(d_i-v)_r}}$. このとき Q^{ij} は正則行列である [4]. よって P_{hk}^{ij}, P_k^{ij} をそれぞれ $(Q^{ij})^{-1}$ の (h,k)-成分,k-列とすると, $(f_r^{ij})_{r=0}^{d_i}$ は次を満たす：

$$(f_r^{11})_{r=0}^{d_1} = \frac{\sqrt{\binom{v-1}{d_1-1}\binom{v-1}{d_2-1}}}{2}\left(\frac{1}{P_{00}^{11}}P_0^{11} + \frac{1}{P_{0d}^{11}}P_d^{11}\right),$$

$$(f_r^{22})_{r=0}^{d_2} = \frac{\sqrt{\binom{v-1}{d_1-1}\binom{v-1}{d_2-1}}}{2}\left(\frac{1}{P_{00}^{22}}P_0^{22} + \frac{1}{P_{0d}^{22}}P_d^{22}\right),$$

$$(f_r^{12})_{r=0}^{d_1} = \frac{1}{2P_{0d}^{12}}P_d^{12}.$$

(feasible parameter を見つける際にはこのように $(Q^{ij})^{-1}$ の列ベクトルの一次結合でうまく書けないかと思って探したわけである.) この表現を用いて体的な計算により双対問題の半正定値性以外の条件については確認できる.

最後に半正定値性であるが, 各 F_r の行列式が非負であることを見る.

$$\begin{aligned}
&\det(F_r)\\
&= f_r^{11}f_r^{22} - (f_r^{12})^2\\
&= \frac{1}{4}\frac{\binom{v}{r}^2(v-2r-1)^2}{(v-r-1)^2}\frac{\prod_{i=1}^2\left(\binom{v-d_i}{d_i}-(-1)^r\binom{v-d_i-r}{d_i-r}\right)-\prod_{i=1}^2\left(\frac{v}{d_i}\binom{v-d_1-r}{d_i-r}\right)}{\frac{v}{d_1}\frac{v}{d_2}\binom{v-d_1}{d_1}\binom{v-d_2}{d_2}}.
\end{aligned}$$

ここで $g(v,r) = \prod_{i=1}^2\left(\binom{v-d_i}{d_i}-(-1)^r\binom{v-d_i-r}{d_i-r}\right)-\prod_{i=1}^2\left(\frac{v}{d_i}\binom{v-d_1-r}{d_i-r}\right)$ とおく. $g(v,r)$ が非負であることをみればよい. 明らかに $g(v,1)=0$ である. r が奇数のとき,

$$\begin{aligned}
\binom{v-d_i}{d_i} - \left(\frac{v}{d_1}-1\right)\binom{v-d_i-r}{d_i-r} &> \binom{v-d_i}{d_i} - \left(\frac{v}{d_1}-1\right)\binom{v-d_i-3}{d_i-3}\\
&> \binom{v-d_i-3}{d_i-3}\frac{v-d_i}{d_i}\left(\frac{(v-d_i-1)(v-d_i-2)}{(d-1)(d-2)}-1\right)\\
&> 0.
\end{aligned}$$

次に $r \geq 2$ が偶数のときは明らかに $g(v, r+2) > g(v, r)$ であり,$g(v, 2)$ についてはつぎの

$$g(v,2) = \frac{\binom{v-d_1-2}{d_1-2}\binom{v-d_2-2}{d_2-2}(v-2)}{d_1 d_2 (d_1-1)(d_2-1)}(-2d_1d_2 + (d_1+d_2+3d_1d_2)v - 2(d_1+d_2)v^2 + v^3).$$

現在課している仮定の $v \geq d_1 + 2d_2 - 1$ により $-2d_1d_2 + (d_1+d_2+3d_1d_2)v - 2(d_1+d_2)v^2 + v^3$ が正だとわかる. よって $g(v, 2)$ も正であり結局 $g(v, r)$ が正だとわかった. 従って $\det(F_1) = 0$, $\det(F_2) > 0, \ldots, \det(F_{d_1}) > 0$ が成立つ.

よって $\sqrt{|Y_1||Y_2|} \leq \mathrm{tr}(\sum_{r=0}^{d_1} F_r) + \sum_{r=d_1+1}^{d_2} f_r^{22} = \sqrt{\binom{v-1}{d_1-1}\binom{v-1}{d_2-1}}$ が示された.

等号成立するとき $y_{ii}^{2d_i} = 0$ かつ $\sum_{h=0}^{d_i} y_{ii}^{2h} \cdot Q_r(h; \alpha_i, \beta_i, d_i) = 0$ が $2 \geq r \geq d_i$ の範囲で成立つ. このとき各 Y_i は Johnson graph$J(v, d_i)$ における width $d_i - 1$, dual width 1 の decendant と呼ばれている対象となり, それらは Ω の一点を含む d_i 点部分集合全体となること同値であることが Meyrerowitz により示されている [1]. □

ここでは $t = 1$ における多重交差族について考察した. 半正定値計画法は $t > 1$ についても設定できるため,$t > 1$ における多重交差族については feasible parameters$f_r^{i,j}$ を求めることが出来ればよいが, 現段階ではそのようなものはまだ見つかっていない.

参考文献

[1] A. E. Brouwer, C. D. Godsil, J. H. Koolen and W. J. Martin, Width and dual width of subsets in polynomial association schemes, J. Combin. Theory Ser. A 102 (2003), 255–271.

[2] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. (2) 12 (1961) 313–320.

[3] S. A. Hobart, Bounds on subsets of coherent configurations, Michigan Math. J. 58 (2009) 231–239.

[4] R. Koekoek and R. F. Swarttouw, The Askey scheme of hypergeometric orthogonal polynomials and its q-analog, report 98-17, Delft University of Technology, The Netherlands, 1998.

[5] W. J. Martin and H. Tanaka, Commutative association schemes, European J. Combin. 30 (2009) 1497–1525.

[6] M. Matsumoto and N. Tokushige, The exact bound in the Erdős-Ko-Rado theorem for cross-intersecting families, J. Combin. Theory Ser. A 52 (1989) 90–97.

[7] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859–2866.

[8] S. Suda, and H. Tanaka, A cross-intersection theorem for Q-polynomial distance-regular graphs based on semidefinite programming, unpublished.

[9] H. Tanaka, The Erdős-Ko-Rado theorem for twisted Grassmann graphs, preprint; arXiv:1012.5692.

[10] J. Wang and H. Zhang, Cross-intersecting families and primitivity of symmetric systems, J. Combin. Theory Ser. A 118 (2011), 455–462.

[11] R. M. Wilson, The exact bound in the Erdős–Ko–Rado theorem, Combinatorica 4 (1984) 247–257.

Coset 型の difference matrix について

熊本大学　　平峰 豊
大分大学　　末竹 千博

1 Introduction

Definition 1.1 U を位数 u の群として $k, \lambda \in \mathbb{N}$ とする.

$k \times u\lambda$ 行列 $H = \begin{bmatrix} d_{1,1} & \cdots & d_{1,u\lambda} \\ \vdots & & \vdots \\ d_{k,1} & \cdots & d_{k,u\lambda} \end{bmatrix}$ が 群 U 上の $(u, k; \lambda)$-difference matrix であるとは $d_{ij} \in U$ $(\forall i, j,\ 1 \le i \le k,\ 1 \le j \le u\lambda)$ でかつ次の条件をみたすことをいう.

$$\sum_{1 \le j \le u\lambda} d_{i_1 j}\, {d_{i_2 j}}^{-1} = \lambda U \in \mathbb{Z}[U] \quad (1 \le i_1 \ne i_2 \le k).$$

$(u, k; \lambda)$-difference matrix に関して k と $u\lambda$ の間に次の関係が知られている.

Result 1.2 (D. Jungnickel [3]) $k \le u\lambda$.

次は difference matrix に関する目標の一つとなっている.

問題. 与えられた u, λ に対して k の最大値はどうなるか？

$k = u\lambda$ である difference matrix, つまり $(u, u\lambda; \lambda)$-difference matrix を U 上の**一般アダマール行列**といい, $\mathrm{GH}(u, \lambda)$ over U で表す.

Example 1.3 次は A $(3, 6; 2)$-difference matrix (i.e. $\mathrm{GH}(3, 2)$ 行列) over of $GF(3)^+$ である.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 1 & 0 & 2 \\ 1 & 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 2 & 1 & 2 & 0 & 1 \end{bmatrix}$$

次が知られている.

Result 1.4 (D.A. Drake [5]) U を偶数位数 u の群で $2 \nmid \lambda$ とする. U の Sylow 2-群が cyclic で $(u, k; \lambda)$-difference matrix over U が存在すれば $k \le 2$ である.

小さな u, λ については次が確かめられている.

Result 1.5 (P.H.J. Lampio and P.R.J. Östergard [4])
(i) $(3, k; 5)$-difference matrices over $\mathbb{Z}_3$ が存在すれば $k \leq 9$.
(ii) $(5, k; 3)$-difference matrices over $\mathbb{Z}_5$ が存在すれば $k \leq 8$.
(iiii) $(6, k; 2)$-difference matrices over $\mathbb{Z}_6$ が存在すれば $k \leq 6$.

Difference Matrices の同値性
群 U 上の 2 つの difference matrices が次の変換で移りうるとき同値であるという.

(i) 任意の 2 行の置換

(ii) 任意の 2 列の置換

(iii) 任意の行に左から群の 1 つの元をかける

(iv) 任意の列に右から群の 1 つの元をかける

2 coset に関する difference matrices

Definition 2.1 H を群 U 上の $(u, k; \lambda)$-difference matrix とする. また, H の行全体の集合を R で表し, $R \subset U^{u\lambda}$(U の $u\lambda$ 個の直積群) とみる. このとき, H が $U^{u\lambda}$ の部分群 W に関して **coset 型** であるとは次の条件がみたされることをいう:

(i) $W \subset R$ である.

(ii) $w \in W$ かつ $r \in R$ ならば $rw \in R$ である.

また, w を H のある行とするとき H が w で生成される巡回群 $\langle w \rangle$ に関して coset 型であれば, H は**行 w に関して coset 型である**と省略していう.

Remark 2.2 (i) R はいくつかの右 cosets gW $(g \in U^{u\lambda})$ の和集合である.

(ii) $1_{u\lambda} := (\overbrace{1, \cdots, 1}^{u\lambda}) \in R$ であり, U は exponent p の p-群である.
$(\because w \in W \longrightarrow w^0, w, w^2, \cdots \in R)$
(iii) $1_{u\lambda}$ と異なる任意の行 w は U の各元をちょうど λ 個含む.
$(\because w = w(1_{u\lambda})^{-1})$
(iv) H が W に関して coset 型 $\Longleftrightarrow$ H は任意の $w(\in W)$ に関して coset 型.

Example 2.3 $U = \{0, 1, a, b\}$ を $GF(4)$ の加法群とする．次は $(4, 8; 6)$-difference matrix over U である．

$$\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & a & a & a & a & a & a & b & b & b & b & b & b \\ 0 & 1 & a & 0 & 1 & a & 1 & b & b & 1 & b & b & 1 & a & b & 1 & a & b & 0 & 0 & a & 0 & 0 & a \\ 0 & 1 & a & 0 & 1 & a & 0 & a & a & 0 & a & a & b & 0 & 1 & b & 0 & 1 & b & b & 1 & b & b & 1 \\ 0 & 0 & 1 & a & a & b & 1 & a & a & b & 0 & 1 & b & b & 0 & 1 & a & b & 0 & 1 & 1 & a & b & 0 \\ 0 & 0 & 1 & a & a & b & 0 & b & b & a & 1 & 0 & 1 & 1 & a & b & 0 & 1 & b & a & a & 1 & 0 & b \\ 0 & 1 & b & a & b & 1 & 0 & 1 & 1 & a & b & a & a & 1 & b & 0 & 0 & 0 & 0 & 1 & b & a & b & a \\ 0 & 1 & b & a & b & 1 & 1 & 0 & 0 & b & a & b & 0 & b & 1 & a & a & a & b & a & 0 & 1 & 0 & 1 \end{bmatrix}$$

この例において各行 h_i $(0 \le i \le 7)$ を直積群 $U^{24} = U \oplus \cdots \oplus U$ の元とみるとき，$W := \{h_0, h_1, h_2, h_3\}$ は U^{24} の位数 4 の部分群であり，$h_4 + W = \{h_4, h_5, h_6, h_7\}$ は W の直積群 U^{24} における剰余類である．従って W に関する coset 型の difference matrix とみることができる．

coset 型の difference matrices に関して de Launey ([1]) は行全体 R が群となる $GH(u, \lambda)$ 行列を考察して group Hadamard matrix と呼んだ．
また，McDonough-Mavron-Pallikaros ([2]) は $\mathrm{GH}(u, \lambda)$ 行列 H over U が coset 型なら，U は elementary abelian p-group となることを示した．

Example 2.4 $q = p^n$ で p を素数とする．$U = \{g_1, \cdots, g_q\}, g_1 = 1$ を位数 q で exponent p の p-group とする．このとき，ある行に関する $(q, p; \lambda)$-difference matrix H は次に同値である．

$$H = \begin{bmatrix} w^0 \\ w^1 \\ \vdots \\ w^{p-1} \end{bmatrix},$$

ここで $w = (Jg_1, Jg_2, \cdots, Jg_q)$，$J = (1, \cdots, 1)(= 1_\lambda)$．この例では λ が任意であることに注意されたい．

Question 2.5 $q = p^n$ を素数 p のべきとして，H が coset 型の $(q, k; \lambda)$-difference matrix で $k > p$ とき λ にはどのような制限がつくか．$p \mid \lambda$ が成り立つか．

上の Question に関して $k = u\lambda$ なら次を示すことができる．

Theorem 2.6 H が U 上の $(u, u\lambda; \lambda)$-difference matrix で，H がある行に関して coset 型ならば $\lambda = 1$ かまたは $\exp(U) \mid \lambda$ である．

(証明の概略) $H=[h_{ij}]$, $k=u\lambda$ とおく．さらに $g=(g_1,\cdots,g_k)\in U^k$, $x\in U$ に対して，$gx=(g_1x,\cdots,g_nx)$ と定める．また H の第 i 行を $h_i=(h_{i1},\cdots,h_{ik})$ とおいて $h_i\in U^k$ とみる．H から得られる結合構造 $(\mathbb{P},\mathbb{B})$ の点集合 $\mathbb{P}$，ブロック集合 $\mathbb{B}$ を次で定める．

$$\mathbb{P}=\{(i,x)\mid 1\le i\le k,\ x\in U\},\ |\mathbb{P}|=ku$$
$$\mathbb{B}=\{B_{j,y}\mid 1\le j\le n,\ y\in U\},\ |\mathbb{B}|=u^2\lambda$$
$$B_{j,y}=\{(1,h_{1j}y),(2,h_{2j}y),\cdots,(n,h_{kj}y)\}$$

ここで結合関係は通常の包含関係として定義する．従って次が成り立つ．

$$(i,a)\in B_{j,b}\iff a=h_{ij}b$$

点 (i,a)，ブロック $B_{j,b}$ への元 $x\in U$ の作用 $\rho(x)$ を次で定める．

点：$(i,a)^{\rho(x)}=(i,ax)$
ブロック：${B_{j,b}}^{\rho(x)}=B_{j,bx}$

H が行 h_m に関して coset 型のとき，点 (i,a)，ブロック $B_{j,b}$ への作用 $\theta(h_m)$ を次で定める．

点：$(i,a)^{\theta(h_m)}=(\ell,a)$，ただし $h_ih_m=h_\ell$.
ブロック：${B_{j,b}}^{\theta(h_m)}=B_{j,h_{mj}^{-1}b}$

このとき

$$\mathcal{C}_i=\{(i,x)\mid x\in U\}\ (1\le i\le k)$$
$$\mathcal{B}_j=\{B_{j,x}\mid x\in U\}\ (1\le j\le k)$$

とおけば，$(\mathbb{P},\mathbb{B})$ は $\{\mathcal{C}_i\}$ を点クラス，$\{\mathcal{B}_j\}$ をブロッククラスにもつ resolvable な transversal design $\mathrm{TD}_\lambda(k,u)$([3] 参照) となることが示され，かつ

$$G:=\rho(U)\times\langle\theta(h_m)\rangle\le\mathrm{Aut}(\mathbb{P},\mathbb{B})$$

で G は $\mathbb{P}$ 上 semi-regular に作用することが証明できる．

以上の事実を仮定すれば，Theorem 2.6 は次のように証明できる：
$\lambda>1$ と仮定する．Remark 2.2(ii) より $p=\mathrm{o}(w)$ ($\mathrm{o}(w)$ の位数) は素数である．また，H が行 w に関して coset 型であるとすると $W=\langle w\rangle$ は $\lambda>1$ であるから W が各ブロックごとに固定する 2 ブロッククラス $\mathcal{B}_i,\mathcal{B}_j$ がとれる．このとき $B\in\mathcal{B}_i$, $C\in\mathcal{B}_j$ とすれば W は点集合 $B\cap C$ に semi-regular に作用する．従って $|W|\mid|B\cap C|=\lambda$. $\therefore\ p=|W|\mid\lambda$ となる． □

k が十分に大きいとき同じことが $(u,k;\lambda)$-difference matrix についても成り立つか興味がある．

Example 2.7 Theorem 2.6 で $\lambda = 1$ と $\lambda > 1$ の例をみる.
(i) $F = GF(p^n)^+ = \{k_1(=0), k_2(=1), \cdots, k_q\}$ を位数 q の有限体の加法群として $q \times q$ 行列 $H = [h_{ij}]$ を $h_{ij} = h_i h_j$ で定める. このとき H は $(q, q; 1)$-difference matrix であることが容易に確かめられる. H は de Launcy が定義した group Hadamard matrix の 1 つであり, 従って coset 型でもあるが, $p \nmid \lambda = 1$ である.
(ii) 次の行列 H は $W = \langle w \rangle$ に関する $U = \langle a \rangle (\simeq \mathbb{Z}_3)$ 上の $(3, 18; 6)$-difference matrix である. ここで w は H の第 2 行である. また, 任意の $i \in \{0, 1, 2, 3, 4, 5\}$ について $3i+1, 3i+2, 3i+3$ 行は直積群 U^{18} における部分群 $\langle w \rangle$ の coset となっていて $3 \mid \lambda = 6$ である.

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & a & a & a & a & a & a & a^2 & a^2 & a^2 & a^2 & a^2 & a^2 \\
1 & 1 & 1 & 1 & 1 & 1 & a^2 & a^2 & a^2 & a^2 & a^2 & a^2 & a & a & a & a & a & a \\
1 & 1 & a & a^2 & a & a^2 & 1 & a^2 & a^2 & a & a & 1 & 1 & a & 1 & a & a^2 & a^2 \\
1 & 1 & a & a^2 & a & a^2 & a & 1 & 1 & a^2 & a^2 & a & a^2 & 1 & a^2 & 1 & a & a \\
1 & 1 & a & a^2 & a & a^2 & a^2 & a & a & 1 & 1 & a^2 & a & a^2 & a & a^2 & 1 & 1 \\
1 & a^2 & a^2 & a & a & 1 & 1 & a & 1 & a & a^2 & a^2 & 1 & 1 & a & a^2 & a & a^2 \\
1 & a^2 & a^2 & a & a & 1 & a & a^2 & a & a^2 & 1 & 1 & a^2 & a^2 & 1 & a & 1 & a \\
1 & a^2 & a^2 & a & a & 1 & a^2 & 1 & a^2 & 1 & a & a & a & a & a^2 & 1 & a^2 & 1 \\
1 & a & 1 & a & a^2 & a^2 & 1 & 1 & a & a^2 & a & a^2 & 1 & a^2 & a^2 & a & a & 1 \\
1 & a & 1 & a & a^2 & a^2 & a & a & a^2 & 1 & a^2 & 1 & a^2 & a & a & 1 & 1 & a^2 \\
1 & a & 1 & a & a^2 & a^2 & a^2 & a^2 & 1 & a & 1 & a & a & 1 & 1 & a^2 & a^2 & a \\
1 & a & a^2 & a^2 & 1 & a & 1 & a & a^2 & a^2 & 1 & a & 1 & a & a^2 & a^2 & 1 & a \\
1 & a & a^2 & a^2 & 1 & a & a & a^2 & 1 & 1 & a & a^2 & a^2 & 1 & a & a & a^2 & 1 \\
1 & a & a^2 & a^2 & 1 & a & a^2 & 1 & a & a & a^2 & 1 & a & a^2 & 1 & 1 & a & a^2 \\
1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a \\
1 & a^2 & a & 1 & a^2 & a & a & 1 & a^2 & a & 1 & a^2 & a^2 & a & 1 & a^2 & a & 1 \\
1 & a^2 & a & 1 & a^2 & a & a^2 & a & 1 & a^2 & a & 1 & a & 1 & a^2 & a & 1 & a^2
\end{bmatrix}$$

3 $(p, k; \lambda)$-matrices with p a prime

以下では次を仮定する.

Hypothesis 3.1

(i) H は素数位数 p の群 $U \simeq \mathbb{Z}_p$ 上の $(p, k; \lambda)$-difference matrix である.

(ii) H は H のある行 w に関して coset 型であり, かつ $k = pr, r > 1$.

(iii) $w = (J, Ja, \cdots, Ja^{p-1}) \in U^{p\lambda}$, ここで $J = (1, \cdots, 1) \in U^{\lambda}$.

w の形に合わせて H の任意の行 v を常に次の形で表す:

$$v = (v_0, v_1, \cdots, v_{p-1}) \in (U^{\lambda})^p, \quad \text{ただし } v_i \in U^{\lambda}.$$

この v_i を v の i-part と呼ぶ.

$z=(z_1,\cdots,z_m)\in U^m$ に対して, $\widehat{z}$ を次で定める.

$$\widehat{z}=z_1+\cdots+z_m\in\mathbb{Z}[U]$$

$h_0:=(1,\cdots,1)\in U^{p\lambda}$ とおくと, $R=h_0\langle w\rangle\cup h_1\langle w\rangle\cup\cdots\cup h_{r-1}\langle w\rangle$ であるから, 次を仮定してよい.

$$H=[M,w]:=\begin{bmatrix} M \\ Mw \\ \vdots \\ Mw^{p-1}\end{bmatrix},\quad \text{ここで } M=\begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{r-1}\end{bmatrix} \tag{1}$$

明らかに $R:=h_0\langle w\rangle\cup h_1\langle w\rangle\cup\cdots\cup h_{r-1}\langle w\rangle$ は H の行全体である.

以下では (1) の形の difference matrix $H(=[M,w])$ を 群 U 上の $w=(J,Ja,\cdots,Ja^{p-1})$ に関する coset 型 $(p,k;\lambda)$-difference matrix の**標準型**と呼ぶことにする. 任意の coset 型 $(p,k;\lambda)$-difference matrix は §1 で述べた同値変形の範囲で必ず標準型にできるので, 最初から標準型だけを考えてよいことは明らかである.

H を標準型とするとき次が成り立つ.

$$\widehat{h_jw^i}=\lambda U\quad\forall(i,j)\neq(0,0)$$

$i_1\neq i_2$ に対して $v=h_{i_1}{h_{i_2}}^{-1}$ として $v=(v_0,\cdots,v_{p-1})$, $v_i\in U^\lambda$ とおく.
$vw^t=h_{i_1}(h_{i_2}w^{-t})^{-1}$ かつ $h_{i_2}w^{-t}\in R$ であるから, $\widehat{vw^t}=\lambda U$ がなりたつ.
また, $\widehat{v_i}=m_{i,0}1+m_{i,1}a+m_{i,2}a^2+\cdots+m_{i,p-1}a^{p-1}$ とおく. ここで全ての m_{ij} は 0 以上の整数である.
このとき, 各 m_{ij} を変数とみて, 次の p^2+p 個の等式を得る:

$$m_{i,0}+m_{i,1}+\cdots+m_{i,p-1}=\lambda \tag{2}$$
$$(0\le i\le p-1)$$

(2) の証明:
v_i の成分の個数が λ なので明らか.

$$m_{0,s}+m_{1,s-t}+m_{2,s-2t}+\cdots+m_{p-1,s-(p-1)t}=\lambda \tag{3}$$
$$(0\le\forall s,t\le p-1)$$

(3) の証明:
vw^t の第 i-part について $w=(J,Ja,\cdots,Ja^{p-1})$, $v=(v_0,v_1,\cdots,v_{p-1})\in(U^\lambda)^p$ より $(Ja^i)^t=(a^{it},\cdots,a^{it})$ は w^t の第 i-part である.
さらに, $\widehat{v_i}=m_{i,0}1+m_{i,1}a+m_{i,2}a^2+\cdots+m_{i,p-1}a^{p-1}$ より

$\widehat{vw^t} = \sum_{0\le i\le p-1}\sum_{0\le j\le p-1}(m_{i,j}\,a^j)a^{it} = \sum_{0\le i,j\le p-1} m_{i,j}\,a^{j+it}$ $(=\lambda U)$ である.
また, $j+it\equiv s \iff j\equiv s-it \pmod p$ であるから, $\sum_{0\le i\le p-1} m_{i,s-it} = \lambda \quad (0\le s,t\le p-1)$ が成り立つ. □

この p^2 変数 m_{ij} からなる p^2+p 個の等式より $m_{ij}=\lambda/p \quad (\forall i,j)$ を導くことにより次を示す.

Lemma 3.2 $p\mid\lambda$ かつ $\widehat{v_i}=(\lambda/p)U \quad (0\le i\le p-1)$.

(証明) $i_0, j_0\in\{0,1,\cdots,p-1\}$ を任意に選び固定して, $m_{i_0,j_0}=\lambda/p$ が成り立つことを示す. $S_a=\{(i,j)\in\mathbb{Z}_p\times\mathbb{Z}_p \mid ia+j=i_0a+j_0\}$ $(a\in\mathbb{Z}_p)$ とおけば次が成り立つ.

(i) $|S_a|=p$, $S_a\cap S_b=\{(i_0,j_0)\}$, $a\ne b$.

(ii) $S_a\ \cap\ \{i_0\}\times\mathbb{Z}_p = S_a\ \cap\ \mathbb{Z}_p\times\{j_0\}=\{(i_0,j_0)\}, \forall a\ne 0$.

(iii) $i\ne i_0, j\ne j_0 \implies \exists_1 a(\ne 0)\in\mathbb{Z}_p$ s.t. $(i,j)\in S_a$

ここで $S_a=\{(i,j_0-(i_0-i)a)\mid i\in\mathbb{Z}_p\}=\{(i,j_0-ia)\mid i\in\mathbb{Z}_p\}$ であるから (3) を用いて $\sum_{(i,j)\in S_a} m_{i,j}=\lambda$. 従って, $\sum_{1\le a\le p-1}\left(\sum_{(i,j)\in S_a} m_{ij}\right)=(p-1)\lambda$.
よって, (i) と (ii) より $(p-1)m_{i_0,j_0}+\sum_{i\ne i_0,\,j\ne j_0} m_{ij}=(p-1)\lambda$.
両辺に $\sum_{j\in\mathbb{Z}_p} m_{i_0,j}(=\lambda)$ と $\sum_{i\in\mathbb{Z}_p} m_{i,j_0}(=\lambda)$ を加えることにより (iii) から $pm_{i_0,j_0}+\sum_{i,j\in\mathbb{Z}_p} m_{ij}=(p+1)\lambda$ が分かる. これより $m_{i_0,j_0}=\lambda/p$ であることが分かる. 従って Lemma が成り立つ. □

以上のことを用いて次の結果を得る.

Theorem 3.3 H を素数位数 p の群 U 上の coset 型の $(p,k;\lambda)$-difference matrix $(k>p)$ とすると次が成り立つ.

(i) $p\mid\lambda$.

(ii) U 上の normalized $(p,k/p;\lambda/p)$-difference matrices $H_0,H_1,\cdots,H_{p-1}$ が存在して H は次に同値:

$$\begin{bmatrix} (H_0,H_1,\cdots,H_{p-1}) \\ (H_0,H_1,\cdots,H_{p-1})w \\ \vdots \\ (H_0,H_1,\cdots,H_{p-1})w^{p-1} \end{bmatrix} \tag{4}$$

$$(w=(J,Ja,\cdots,Ja^{p-1})\in U^{p\lambda},\ J=(1,\cdots,1)\in U^{\lambda})$$

逆に，任意に与えられた U 上の normalized $(p, k/p; \lambda/p)$-difference matrices $H_0, H_1, \cdots, H_{p-1}$ に対して (4) で与えられる行列は w に関する U 上の $(p, k; \lambda)$-difference matrix である．

(証明) $r = k/p,\ \mu = \lambda/p,\ h_i = (h_{i,0}, h_{i,1}, \cdots, h_{i,p-1}),\ h_{i,j} \in U^{\lambda}\ \ (0 \le i \le r-1)$ とおく．さらに $i_1 \ne i_2$ に対して，$v = h_{i_1} {h_{i_2}}^{-1}$ とおき，$j \in \mathbb{Z}_p$ に対して $v_j = h_{i_1,j} {h_{i_2,j}}^{-1}$ とおくと Lemma 3.2 により $\widehat{v_j} = \mu U$ である．従って，各 $j\ (0 \le j \le p-1)$ に対して $H_j := \begin{bmatrix} h_{0,j} \\ \vdots \\ h_{r-1,j} \end{bmatrix}$ は U 上の $(p, r; \mu)$-difference matrix である．

Example 3.4 次の行列 H は例 2.7 の difference matrix を Theorem 3.3 に従って標準型に並べ替えたもので，$U = \langle a \rangle (\simeq \mathbb{Z}_3)$ 上の行 w(第 7 行目) に関する coset 型 GH(3, 6) 行列である．各 $i \in \{0, 1, 2, 3, 4, 5\}$ に対して $i+1, i+7, i+13$ が直積群 U^{18} における部分群 $\langle w \rangle$ に関する coset となっている．

$$H = \left[\begin{array}{cccccc|cccccc|cccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & a & a^2 & a & a^2 & 1 & a^2 & a^2 & a & a & 1 & 1 & a & 1 & a & a^2 & a^2 \\
1 & a^2 & a^2 & a & a & 1 & 1 & a & 1 & a & a^2 & a^2 & 1 & 1 & a & a^2 & a & a^2 \\
1 & a & 1 & a & a^2 & a^2 & 1 & 1 & a & a^2 & a & a^2 & 1 & a^2 & a^2 & a & a & 1 \\
1 & a & a^2 & a^2 & 1 & a & 1 & a & a^2 & a^2 & 1 & a & 1 & a & a^2 & a^2 & 1 & a \\
1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a & 1 & a^2 & a \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & a & a & a & a & a & a & a^2 & a^2 & a^2 & a^2 & a^2 & a^2 \\
1 & 1 & a & a^2 & a & a^2 & a & 1 & 1 & a^2 & a^2 & a & a^2 & 1 & a^2 & 1 & a & a \\
1 & a^2 & a^2 & a & a & 1 & a & a^2 & a & a^2 & 1 & 1 & a^2 & a^2 & 1 & a & 1 & a \\
1 & a & 1 & a & a^2 & a^2 & a & a & a^2 & 1 & a^2 & 1 & a^2 & a & a & 1 & 1 & a^2 \\
1 & a & a^2 & a^2 & 1 & a & a & a^2 & 1 & 1 & a & a^2 & a^2 & 1 & a & a & a^2 & 1 \\
1 & a^2 & a & 1 & a^2 & a & a & 1 & a^2 & a & 1 & a^2 & a^2 & a & 1 & a^2 & a & 1 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & a^2 & a^2 & a^2 & a^2 & a^2 & a^2 & a & a & a & a & a & a \\
1 & 1 & a & a^2 & a & a^2 & a^2 & a & a & 1 & 1 & a^2 & a & a^2 & a & a^2 & 1 & 1 \\
1 & a^2 & a^2 & a & a & 1 & a^2 & 1 & a^2 & 1 & a & a & a & a & a^2 & 1 & a^2 & 1 \\
1 & a & 1 & a & a^2 & a^2 & a^2 & a^2 & 1 & a & 1 & a & a & 1 & 1 & a^2 & a^2 & a \\
1 & a & a^2 & a^2 & 1 & a & a^2 & 1 & a & a & a^2 & 1 & a & a^2 & 1 & 1 & a & a^2 \\
1 & a^2 & a & 1 & a^2 & a & a^2 & a & 1 & a^2 & a & 1 & a & 1 & a^2 & a & 1 & a^2
\end{array}\right]$$

最初の 6 行からなる小行列 M がこの coset の代表元の集合を与える．従って $H = \begin{bmatrix} M \\ Mw \\ Mw^3 \end{bmatrix}$ の形である．

Theorem 3.3 により，次の 3 つの行列はこの行列の部分行列として得られた $U = \langle a \rangle (\simeq \mathbb{Z}_3)$ 上の GH(3, 2) 行列である．

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & 1 & a & a^2 & a^2 \\ 1 & 1 & a & a^2 & a & a^2 \\ 1 & a^2 & a^2 & a & a & 1 \\ 1 & a & a^2 & a^2 & 1 & a \\ 1 & a^2 & a & 1 & a^2 & a \end{bmatrix}$$

Example 3.5 $p = 2$ として H_1 と H_2 を位数 2 の乗法群 $\{\pm 1\} \simeq \mathbb{Z}_2$ 上の任意の n 次 normalized Hadamard matrices とする．このとき，$H = \begin{bmatrix} H_1 & H_2 \\ H_1 & -H_2 \end{bmatrix}$ は H の第 $n+1$ 行 $(\overbrace{1,\cdots,1}^{n},\overbrace{-1,\cdots,-1}^{n})$ に関する $2n$ 次の Hadamard matrix である．

Example 3.6 次の H_1, H_2, H_3, H_4 は $GF(4)^+ = \{0, 1, a, a^2\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ 上の GH(4,3) 行列である．

$$H_1 = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&a&a&a&a^2&a^2&a^2\\
0&0&0&a&a&a&a^2&a^2&a^2&1&1&1\\
0&1&a&1&a&a^2&0&1&a^2&0&a&a^2\\
0&1&a&a&a^2&1&1&a^2&0&a&a^2&0\\
0&1&a&a^2&1&a&a^2&0&1&a^2&0&a\\
0&a&a^2&0&1&a^2&1&a&a^2&a&0&1\\
0&a&a^2&1&a^2&0&a&a^2&1&0&1&a\\
0&a&a^2&a^2&0&1&a^2&1&a&1&a&0\\
0&a^2&1&0&a^2&a&a&1&0&a^2&a&1\\
0&a^2&1&a&0&a^2&0&a&1&1&a^2&a\\
0&a^2&1&a^2&a&0&1&0&a&a&1&a^2
\end{bmatrix}
\quad
H_2 = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&a&a&a&a^2&a^2&a^2\\
0&0&0&a&a&a&a^2&a^2&a^2&1&1&1\\
0&1&a&1&a&a^2&0&1&a^2&0&a&a^2\\
0&1&a&a&a^2&1&1&a^2&0&a&a^2&0\\
0&1&a&a^2&1&a&a^2&0&1&a^2&0&a\\
0&a&a^2&0&1&a^2&a&a^2&1&1&a&0\\
0&a&a^2&1&a^2&0&a^2&1&a&a&0&1\\
0&a&a^2&a^2&0&1&1&a&a^2&0&1&a\\
0&a^2&1&0&a^2&a&0&a&1&a&1&a^2\\
0&a^2&1&a&0&a^2&1&0&a&a^2&a&1\\
0&a^2&1&a^2&a&0&a&1&0&1&a^2&a
\end{bmatrix}$$

$$H_3 = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&a&a&a&a^2&a^2&a^2\\
0&0&0&a&a&a&a^2&a^2&a^2&1&1&1\\
0&1&a&1&a&a^2&0&1&a^2&0&a&a^2\\
0&1&a&a&a^2&1&1&a^2&0&a&a^2&0\\
0&1&a^2&a&0&a^2&a&0&1&a^2&1&a\\
0&a&1&a^2&1&a&0&a^2&1&0&a^2&a\\
0&a&a^2&0&1&a^2&1&a&a^2&a&0&1\\
0&a&a^2&a^2&0&1&a^2&1&a&1&a&0\\
0&a^2&1&0&a^2&a&a&1&0&a^2&a&1\\
0&a^2&1&a^2&a&0&1&0&a&a&1&a^2\\
0&a^2&a&1&a^2&0&a^2&a&1&1&0&a
\end{bmatrix}
\quad
H_4 = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&a&a&a&a^2&a^2&a^2\\
0&0&0&a&a&a&a^2&a^2&a^2&1&1&1\\
0&1&a&1&a&a^2&0&1&a^2&0&a&a^2\\
0&1&a&a&a^2&1&1&a^2&0&a&a^2&0\\
0&1&a^2&a^2&0&a&a&1&0&a^2&1&a\\
0&a&1&a^2&a&1&a^2&0&1&0&a^2&a\\
0&a&a^2&0&1&a^2&a&a^2&1&1&a&0\\
0&a&a^2&1&a^2&0&a^2&1&a&a&0&1\\
0&a^2&1&0&a^2&a&0&a&1&a&1&a^2\\
0&a^2&1&a&0&a^2&1&0&a&a^2&a&1\\
0&a^2&a&a^2&1&0&1&a&a^2&1&0&a
\end{bmatrix}$$

ここで $M = (H_1, H_2, H_3, H_4)$ $(12 \times 48$ matrix over $U = GF(4)^+)$ とおいて $w_0 = (0J, 0J, 0J, 0J)$, $w_1 = (0J, J, aJ, a^2J)$, $w_2 = (0J, aJ, a^2J, J)$, $w_3 = (0J, a^2J, J, aJ)$ とする．ただし，$J = (1, \cdots, 1) \in U^{12}$．このとき次は $W = \{w_0, w_1, w_2, w_3\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ に関する群 U 上の GH(4,12) 行列である．

$$\begin{bmatrix} M + w_0 \\ M + w_1 \\ M + w_2 \\ M + w_3 \end{bmatrix}$$

H の行全体は直積群 U^{48} における部分群 W の 12 個の cosets からなる．

Question 3.7 素数 p に対して $U \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ とおくとき，U 上の coset 型 (p^2, k, λ)-difference matrices の構造について何がいえるか.

参考文献

[1] W. de Launey, Generalized Hadamard Matrices whose rows and columns form a group, In : Casse L. R. A. (Ed.), Combinatorial Mathematics X, Lectue Notes in Mathematics, Springer, Berlin, 1983.

[2] T.P. McDonough, V.C. Mavron and C.A. Pallikaros, Generalised Hadamard matrices and translations, Journal of Statistical Planning and Inference, Vol. 86 (2000), 527-533.

[3] T. Beth, D. Jungnickel and H. Lenz, "Design Theory" Volume I, Second Edition, Cambridge University Press, 1999.

[4] P.H.J. Lampio, P.R.J. Östergard, Classification of difference matrices over cyclic groups, J. Statist. Plann. Inference 141 (2011) 1194-1207.

[5] D.A. Drake, Partial λ-geometries and generalized Hadamard matrices over groups, Canad. J. Math. 31 (1979), 617-727.

On a description of the Buratti-Del Fra dual hyperoval and its quotient

香川高専　谷口浩朗 (Hiroaki Taniguchi)*

1　はじめに

この論説は吉荒聡氏 (東京女子大学) との共同研究 [7] に基づいており，文責は谷口にあります。射影空間 $PG(m,2)$ 内の高次元双対超卵形 (dimensional dual hyperoval，DHO) は C. Huybrechts と A. Pasini [4] により以下のように定義された.

定義 1 ($GF(2)$ 上の DHO). m-次元射影空間 $PG(m,2)$ における d-次元部分空間の集合 S が，$PG(m,2)$ における d-次元双対超卵形であるとは，以下のことが成り立つことである:
(1) S に属するどの 2 個の d-部分空間も 1 点で交わり，
(2) S に属するどの異なる 3 個の d-部分空間も共通点を持たず，
(3) S に属する d-部分空間達は $PG(m,2)$ を生成し，
(4) S は 2^{d+1} 個の d-部分空間から成る.

以下 $d \geq 3$ とする. $GF(2)$ 上の d-次元の双対超卵形が生成する射影空間の次元 n については，$2d \leq n \leq d(d+3)/2$ であろうと予想されている．その最大の次元と考えられる $PG(d(d+3)/2,2)$ には，現在
（1）Huybrechts' DHO [3],
（2）Buratti-Del Fra's DHO [1],[7],
（3）Veronesean DHO [8], [9],
（4）Veronesean DHO の変形 [6],
の 4 種類の（同型でない）双対超卵形が構成されている.

*E-mail address: taniguchi@dg.kagawa-nct.ac.jp

本稿では，まず d が偶数の場合に「(2) Buratti-Del Fra's DHO」の quotient である d-次元双対超卵形を $PG(2d+1,2)$ に構成する（定理1）．[1]また、(2) の扱いやすいモデル S を $PG(d(d+3)/2,2)$ に構成（定理2）し、さらにそのアファイン拡大 $Af(S)$ が halved Hypercube Π により semi-biplane として cover されていることを解説する（定理3）．2次的 (quadratic) な APN 関数から構成される DHO はすべて「(1) Huybrechts' DHO」の $PG(2d+1,2)$ における quotient であることから，(2) の $PG(2d+1,2)$ における quotient も何らかの関数と関係することが期待されている．

2 Huybrechts' DHO と Buratti-Del Fra's DHO

$n \geq d+1 \geq 3$ とし，H を $d+1$ 次元ベクトル空間とする．以下のことが分かっている．

命題 1. $s,t \in H$ にたいし $a(s,t) \in H \oplus (H \wedge H)$ を次を満たすように定める．
(a1) $a(s,s) = (0,0)$,
(a2) $a(s,t) = a(t,s)$,
(a3) $a(s,t) \neq (0,0)$,
(a4) $a(s,t) = a(s',t')$ *if and only if* $\{s,t\} = \{s',t'\}$,
(a5) $\{a(s,t) \mid t \in H\} \cup \{(0,0)\}$ *is a vector space over* $GF(2)$.

このとき，$X(s) := \{a(s,t) \mid t \in H \backslash \{0\}\}$ は $PG(H \oplus (H \wedge H))$ の d-次元部分空間であり $S = \{X(s) \mid s \in H\}$ は d-次元双対超卵形となる．

例 1. *(1). Huybrechts' DHO* は以下の $a(s,t)$ で定められる．

$$a(s,t) = (s+t, s \wedge t).$$

(2). Buratti Del Fra's DHO は以下の $a(s,t)$ で定められる．

$$\begin{aligned} a(s,t) &= (s+t, s \wedge t) \\ &+ x_{\bar{s},\bar{t}} \sum_{w \in J(\bar{s})} (e_0, e_0 \wedge w) + \sum_{w \in J(\bar{t})} x_{w,\bar{s}} (e_0, e_0 \wedge w) \end{aligned}$$

ここに $x_{\bar{s}\bar{t}} \in GF(2)$, $x_{w,\bar{s}} \in GF(2)$ で e_0 は $H \backslash \{0\}$ の固定された元とし，H の基底 $\{e_0, e_1, \cdots, e_d\}$ を定めたとき $J(t) := Supp(t)$ ($|Supp(t)|$ が奇数の場合), または $\{0\} \cup Supp(t)$ ($|Supp(t)|$ が偶数の場合) と定める．

[1] $PG(n_1,2)$ を生成する d-次元 DHO S_1 が $PG(n_2,2)$ を生成する d-次元 DHO S_2 の「quotint」であるとは，S_1 が S_2 の projection $\pi : PG(n_2,2) \to PG(n_1,2)$ による像になっていることである．

例 2 (和公式). *(1). Huybrechts' DHO*について以下の和公式が成り立つ.

$$a(s,t_1)+a(s,t_2)=a(s,s+t_1+t_2).$$

*(2). Buratti Del Fra's DHO*について以下の和公式が成り立つ.

$$a(s,t_1)+a(s,t_2)=a(s,s+t_1+t_2+\alpha\{s,t_1,t_2\}e_0),$$

ここに $\alpha\{s,t_1,t_2\}:=\xi(s+t_1)+\xi(s+t_2)+\xi(t_1+t_2)\in GF(2)$, $\xi(t)$ は集合 $H\backslash\{0,e_0\}$ の特性関数である.

次の命題が大切である.

命題 2. *d-次元 DHO* $S:=\{X(t)\mid t\in H\}$ において $a(s,t):=X(s)\cap X(t)$ が上の和公式 *(1)* または *(2)* を満たすならば, S は *(1). Huybrechts' DHO* または *(2). Buratti Del Fra's DHO* の *quotient* になっている.

3 「Buratti-Del Fra's DHO」の $PG(2d+1,2)$ における quotient

定理 1. . d を $d\geq 2$ である偶数とする. $x,t\in GF(2^{d+1})$ に対し

$$B(x,t):=x^4t+xt^4+xt+(xt)^2$$

と定めると $S_B:=\{X(t)\mid t\in GF(2^{d+1})\}$, ここに $X(t):=\{(x,B(x,t))\mid x\in GF(2^{d+1})\backslash\{0\}\}$ は *Buratti-Del Fra's DHO* の $PG(2d+1,2)$ における *quotient* である.

(筆者達は Gap を用いた探索で, この $B(x,t)$ を含む一連の $GF(2)$-bilinear mapping で S_B が DHO になっているものを発見した.)

[証明] $x\neq 0, t\neq 0$ とする. d が偶数のとき

$$B(x,t)=0\leftrightarrow\begin{cases}x=1 & (\text{ if } t=1),\\ x=t+1 & (\text{ if } t\neq 1)\end{cases}$$

となっている. ξ を集合 $GF(2^{d+1})\backslash GF(2)$ の特性関数とすると,

$$x=t+\xi(t)$$

と表すことが出来る．$a(s,t) := X(s) \cap X(t)$ とおくと

$$a(s,t) = (s+t+\xi(s+t), B(s,t) + (s^4+s^2)(\xi+1))$$

となることが計算に寄って分かり ($e_0 = 1$ とおくと), 和公式

$$a(s,t_1) + a(s,t_2) = a(s, s+t_1+t_2+\alpha\{s,t_1,t_2\}e_0)$$

が成り立つことが証明される．ここに $\alpha\{s,t_1,t_2\} := \xi(s+t_1)+\xi(s+t_2)+\xi(t_1+t_2) \in GF(2)$ である．よって命題 2 より S_B は Buratti-Del Fra's DHO の quotient であることがわかる．

注意 . $d \geq 2$ を偶数，$K := GF(3^{d+1})$ とするとき $B(x,t) := x^9t + xt^9 - xt + (xt)^3$ とおき $X(t) = \{(x, B(x,t)) \mid x \in K\} \subset K \oplus K$ とすると $S = \{X(t) \mid t \in K\} \cup X(\infty)$ は *Coulter-Matthews commutative semifield* の *spread* をさだめる．*Buratti-Del Fra DHO* の *quotient* と似通っているような気がする．

4 「Buratti-Del Fra's DHO」の新しい表現

定理 2. $d \geq 2$ とし H を $GF(2)$ 上の $(d+1)$ 次元ベクトル空間とする．$H \otimes H$ の部分空間 W を $W := \langle (x \otimes y) + (y \otimes x) \ and \ (x \otimes x) + \xi(x)(e_0 \otimes x) \mid x, y \in H \rangle$ と定義する。ここに，ξ は集合 $H \backslash \{0, e_0\}$ の特性関数である．ここで $t \in H$ に対し $H \oplus ((H \otimes H)/W)$ の部分空間 $X(t)$ を

$$X(t) = \{(x, \overline{x \otimes t}) \mid x \in K \backslash \{0\}\}$$

と定める．このとき $S = \{X(t) \mid t \in H\}$ は $PG(d(d+3)/2, 2) = PG(H \oplus ((H \otimes H)/W))$ における d-次元 *DHO* であり，*Buratti-Del Fra's DHO* と同型である．

[証明] $x \neq 0, t \neq 0$ とする. このとき W の定義より

$$\overline{x \otimes t} = 0 \leftrightarrow \begin{cases} x = e_0 & (\text{ if } t = e_0), \\ x = t + e_0 & (\text{ if } t \neq e_0) \end{cases}$$

となっている．ξ を集合 $H \backslash \{0, e_0\}$ の特性関数とすると，

$$x = t + \xi(t)e_0$$

と表すことが出来る．$a(s,t) := X(s) \cap X(t)$ とおき，上の表記を用いて $X(s) \cap X(t)$ を計算すると

$$a(s,t) = (s+t+\xi(s+t)e_0, \overline{(s+t+\xi(s+t)e_0) \otimes s})$$

となって，和公式

$$a(s,t_1) + a(s,t_2) = a(s, s+t_1+t_2+\alpha\{s,t_1,t_2\}e_0)$$

が成り立つことがわかる．よって命題 2 より S は Buratti-Del Fra DHO の quotient であることがわかる．さらに，$S = \{X(t) \mid t \in H\}$ は $PG(d(d+3)/2, 2) = PG(H \oplus ((H \otimes H)/W))$ を生成することにより，S は Buratti-Del Fra DHO と同型であることがわかる．

5 Affine 拡大 $Af(S)$ が Halved Hypecube により cover されること

定義 2.「A semibiplane of order s」とは「connected finite incidence structure $\Sigma = (\mathcal{P}, \mathcal{B})$」(ここで $\mathcal{P}$ は点の集合，$\mathcal{B}$ はブロックの集合とする) であって以下の性質を満たすもののことである：(S1) どの 2 点 (2 ブロック) も 0 個か 2 個の ブロック (点) と incident であり (S2) すべてのブロック (点) は $s+2$ 個の点 (ブロック) と incident である．

以下のような例がある．

例 3. *(1). DHO S のアファイン拡大 $Af(S)$：*

$PG(n,2)$ における d-次元 DHO S に対し，生成空間 $PG(n,2)$ を無限遠超平面とするアファイン空間 $AG(n+1,2)$ を持ってくる．S のアファイン拡大 $Af(S)$ とは以下のように定義された「semibiplane」のことである: (1) 点集合 $\mathcal{P} = AG(n+1,2)$ の点全体．(2) ブロック $\mathcal{B} = AG(n+1,2)$ の $(d+1)$-次元部分空間のうち，無限遠超平面との交わりが S に属する d-部分空間となっているもの全体．このとき $\{\mathcal{P}, \mathcal{B}\}$ は「semibiplane」になる．これを「DHO S のアファイン拡大」という．

(2).「Halved Hypercube Π」：

V を $GF(2)$ 上の 2^{d+1}-次元ベクトル空間とし基底 $\{e_x \mid x \in GF(2^{d+1})\}$ を定めておく．V の部分集合として $\mathcal{P}$, $\mathcal{B}$ を以下のように定義する．

$$\mathcal{P} := \{\sum_{x \in GF(2^{d+1})} v_x e_x \mid v_x \in GF(2), \sum_{x \in GF(2^{d+1})} v_x = 0\}$$

$$\mathcal{B} := \{\sum_{x \in GF(2^{d+1})} v_x e_x \mid v_x \in GF(2), \sum_{x \in GF(2^{d+1})} v_x = 1\}.$$

また $v := \sum v_x e_x$ と $w := \sum w_x e_x$ に対して「*incidence* $*$」を $v * w \iff |\{x \in GF(2^{d+1}) \mid v_x \neq w_x\}| = 1$. と定める. このとき $\Pi := \{\mathcal{P}, \mathcal{B}\}$ は「*semibiplane*」になる. これを「*halved Hypercube*」という.

semibiplane の 2 点 $\{v_0, v_1\}$ と 2 つのブロック $\{X_0, X_1\}$ が $\{v_0, v_1\} = X_0 \cap X_1$ を満たすとき、$L := (\{v_0, v_1\}, \{X_0, X_1\})$ を直線という.

定義 3 (the wrapping number). v_0 を semibiplane の点, $L := (\{v_0, v_1\}, \{X_0, X_1\})$ を直線とする. ブロック $X \ni v_0$ に対し. ブロック $\gamma_{v_0,L}(X)$ を次のように定義する:

(1) 点 u_0 を $\{v_0, u_0\} = X_0 \cap X$ であるように定める.
(2) ブロック Y を $X_0 \cap Y = \{v_1, u_0\}$ であるように定める.
(3) 点 u_1 を $\{v_1, u_1\} = Y \cap X_1$ であるように定める.
(4) ブロック $\gamma_{v_0,L}(X) := Z$ を $Z \cap X_1 = \{v_0, u_1\}$ であるように定める.

これで写像 $\gamma_{v_0,L} : X \mapsto Z = \gamma_{v_0,L}(X)$ が定まるが The wrapping number とは（ブロックの置換としての）$\gamma_{v_0,L}$ の位数の（$\{(L, v_0) \mid L \ni v_0\}$ を動かしたときの）最大値のことである.

このとき, 定理 2 の Buratti-Del Fra DHO の表現を利用することにより, 「the wrapping number」を計算することが出来る.

補題 1. *S を Buratti-Del Fra's DHO の quotient とする. このとき $Af(S)$ の「the wrapping number」は「1」である.*

さらに次のことが知られている.

命題 3 (Pasini, Pica [5]). 「*Wrapping number of $Af(S)$ が 1*」 $\Longrightarrow$ 「*$Af(S)$ は Π によって cover される.*」.

以上より, 次が成り立つことが分かった.

定理 3. *Buratti-Del Fra's DHO のどのような quotient$S$ に対しても, $Af(S)$ は Halved Hypercube Π によって（semibiplane として）cover される.*

以上の内容は以下の preprint [7] に基づいています.

References

[1] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, Advances in Geometry. 3 (2003), 245–253.

[2] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, European Journal of Combinatorics. 26 (2005), 173–194.

[3] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Mathematics. 255 (2002), 503–532.

[4] C. Huybrechts and A. Pasini, Frag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40. (1999), 503–532.

[5] A. Pasini and G. Pica, Wrapping polygons in polygons, Annals of Combinatorics, 2 (1998), 325–349.

[6] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, Discrete Mathematics, 309(2009), 418–429.

[7] H. Taniguchi, S. Yoshiara, A simpler description of the d-dimensional Buratti-Del Fra dual hyperoval and its quotient in $PG(2d+1, 2)$, preprint.

[8] J. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, The Quarterly Journal of Mathematics, Oxford. 55 (2004), 99–113.

[9] S. Yoshiara, Ambient spaces of dimensional dual arcs, Journal of Algebraic Combinatorics. 19 (2004), 5–23.