

第 35 回代数的組合せ論シンポジウム報告集

2018年6月18日－20日
於 広島工業大学広島校舎

まえがき

この報告集は 2018 年 6 月 18 日から 20 日にわたり、広島工業大学広島校舎で行われた「第 35 回代数的組合せ論シンポジウム」の講演記録です。研究集会には約 50 名の参加者がありました。

本研究集会は次の援助を受けて開催されました。

若手研究 (B) 研究代表者：奥田隆幸 (課題番号：JP16K17594)

基盤研究 (C) 研究代表者：谷口哲至 (課題番号：JP16K05263)

基盤研究 (C) 研究代表者：島倉裕樹 (課題番号：JP17K05154)

2019 年 1 月

宗政 昭弘 (東北大学)

島倉 裕樹 (東北大学)

谷口 哲至 (広島工業大学)

奥田 隆幸 (広島大学)

第35回代数的組合せ論シンポジウム

標記の研究集会を以下の要領で開催しますので、ご案内申し上げます。

世話人: 宗政 昭弘 (東北大学)
島倉 裕樹 (東北大学)
谷口 哲至 (広島工業大学)
奥田 隆幸 (広島大学)

日時: 2018年6月18日(月)–20日(水)

場所: 広島工業大学 広島校舎 (広島県広島市中区中島町5-7)

プログラム

6月18日(月)

10:00–10:50 阿賀岡 芳夫 (広島大学)

球面と双曲平面のタイリング

(Tilings on the sphere and the hyperbolic plane)

13:30–14:10 山下 文稔 (東京大学)

On modular linear differential operators and their applications to quasi-modular forms

14:20–15:00 小林 雄介 (千葉大学)

Constructions of the McLaughlin graph and of the Co_3 two-graph from the extraspecial group 3_+^{1+4}

15:20–16:00 若竹 昌洋 (近畿大学)

Some remarks on Matsuda's theorem on partial Burnside rings

16:10–16:50 山田 裕史 (熊本大学)

Reduced Fock representation of the Virasoro algebra

6月19日(火)

- 9:00–9:40** 栗原 大武 (北九州工業高等専門学校)
ユニタリ群上の大対蹠集合と Hamming cube
(Hamming cubes and Great antipodal sets on Unitary groups)
- 9:50–10:30** 梶浦 大起 (広島大学)
調和解析的視点からの有限群の部分集合による近似
(Approximation of finite groups by their subsets from the viewpoint of Harmonic analysis)
- 10:40–11:20** Mohamed Fuard Mohamed Sabri (東北大学)
Quantum walks on finite graphs with infinite tails
- 11:30–12:10** 田丸 博士 (広島大学)
Flat quandles, graphs, and subsets in symmetric spaces
- 13:40–14:20** Yan Zhu (上海大学)
Tight t -designs in one shell of Johnson association schemes
- 14:30–15:10** Mohammad Samy Baladram (東北大学)
Simplex designs: a new construction method for spherical designs
- 15:30–16:10** 中田 芳史 (東京大学)
Unitary designs in quantum information science
- 16:20–17:00** 坂内 英一 (九州大学)
On unitary designs and codes

6月20日(水)

9:30–10:10 渡邊 悠太 (宇部工業高等専門学校)
The generalized wreath product of triply-regular association schemes

10:20–11:00 花木 章秀 (信州大学)
Double centralizers of association schemes

11:10–11:50 澤 正憲 (神戸大学)
古典直交多項式に対するカーネル多項式の代数幾何的側面とその応用
(Algebro-geometric aspects of the kernel polynomials for classical orthogonal polynomials, with applications)

12:00–12:40 吉川 昌慶 (兵庫教育大学)
On the closed subset generated by a regular relation

本研究集会は次の援助を受けて開催されます:

- 科研費若手研究 (B) JP16K17594 「擬リーマン対称空間上の固有な群作用の組合せ論的手法を用いた研究」(代表者: 奥田隆幸)
- 科研費基盤研究 (C) JP16K05263 「固有値によるグラフの特徴付け・分類に関する研究」(代表者: 谷口哲至)
- 科研費基盤研究 (C) JP17K05154 「逆軌道体構成法を用いた中心電荷 2 4 の正則頂点作用素代数の一意性の研究」(代表者: 島倉裕樹)

目 次

1. 阿賀岡 芳夫 (広島大学)	1–14
球面と双曲平面のタイリング (Tilings on the sphere and the hyperbolic plane)	
2. 山下 文稔 (東京大学)	15–20
On modular linear differential operators and their applications to quasimodular forms	
3. 小林 雄介 (千葉大学)	21–29
Constructions of the McLaughlin graph and of the Co_3 two-graph from the extraspecial group 3_+^{1+4}	
4. 若竹 昌洋 (近畿大学)	30–37
Some remarks on Matsuda’s theorem on partial Burnside rings	
5. 山田 裕史 (熊本大学)	38–45
Reduced Fock representation of the Virasoro algebra	
6. 栗原 大武 (北九州工業高等専門学校)	46–55
ユニタリ群上の大対蹠集合と Hamming cube (Hamming cubes and Great antipodal sets on Unitary groups)	
7. 梶浦 大起 (広島大学)	56–58
調和解析的視点からの有限群の部分集合による近似 (Approximation of finite groups by their subsets from the viewpoint of Harmonic analysis)	
8. Mohamed Fuard Mohamed Sabri (東北大学)	59–66
Quantum walks on finite graphs with infinite tails	
9. 田丸 博士 (広島大学)	67–73
Flat quandles, graphs, and subsets in symmetric spaces	
10. Yan Zhu (上海大学)	74–78
Tight t -designs in one shell of Johnson association schemes	
11. Mohammad Samy Baladram (東北大学)	79–88
Simplex designs: a new construction method for spherical designs	
12. 中田 芳史 (東京大学)	89–100
Unitary designs in quantum information science	
13. 坂内 英一 (九州大学)	101–108
On unitary designs and codes	
14. 渡邊 悠太 (宇部工業高等専門学校)	109–114
The generalized wreath product of triply-regular association schemes	
15. 花木 章秀 (信州大学)	115–122
Double centralizers of association schemes	
16. 澤 正憲 (神戸大学)	123–127
古典直交多項式に対するカーネル多項式の代数幾何的側面とその応用 (Algebro-geometric aspects of the kernel polynomials for classical orthogonal polynomials, with applications)	
17. 吉川 昌慶 (兵庫教育大学)	128–131
On the closed subset generated by a regular relation	

球面と双曲平面のタイリング

Tilings on the sphere and the hyperbolic plane

阿賀岡 芳夫 広島大学 理学研究科

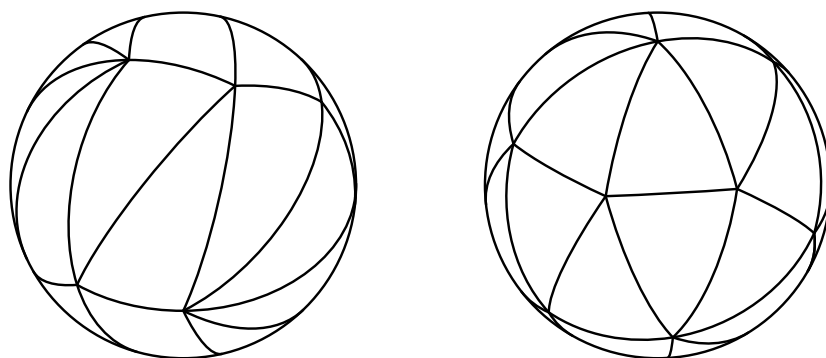
2018年6月18日 於 広島工業大学広島校舎

§1. はじめに

講演のときは、主に平面・球面・双曲平面におけるタイリングの分類結果について話をした。この報告では、そのとき言及できなかった分類の方法論について、その要となるところを簡単に紹介する。球面の3角形タイリングの分類は、組合せ的な議論だけで事実上決着がつくが、4角形・5角形の場合は計量的な条件が本質的に絡むので問題は格段に難しくなる(だから未解決)。

§2. 1種類の3角形を使った球面タイリング

1種類の3角形を使った球面のタイリングには、例えば次のような奇妙なものがある。この図を見ただけで、裏側はどうなっているのか、球面全体の状況が分かってもらえるであろうか。

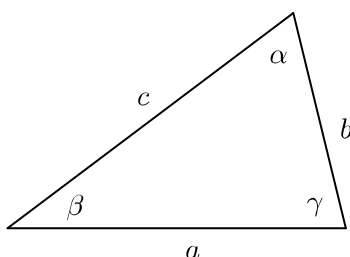


球面の3角形によるタイリングは分類できた¹。それに反して、何故4角形の場合は分類が難しいのか、また何故双曲平面の場合は3角形の場合でも分類が難しいのか、そのからくりについて簡単に説明しよう。

¹詳細な分類結果については論文 [UA2] にある表と図を見て頂きたい。タイリング可能な3角形は10種類、タイリングは20種類存在する。

この節では、まず2次元球面上の1種類の3角形を使ったタイリングについて考察する。ただし、ここで取り扱うタイリングは全て edge-to-edge と仮定する。つまり、1つのタイルの辺の途中で他のタイルの頂点が貼り付くことはない²と仮定する。edge-to-edge の仮定を落とした場合は、3角形の場合でもまだ分類は完了していない。

紙面の制約上、ここでは一番手間のかかる不等辺3角形の場合の分類法について述べることにする。正3角形・2等辺3角形の場合も、不等辺3角形と同様の議論で分類できる。まず下図のように3辺の長さ、3つの内角を定める。



この3角形による edge-to-edge タイリングが存在したとする。するとタイリングにおける1つの頂点の回りは、内角 α, β, γ がいくつかが集まって閉じているので、0以上のある整数 p, q, r が存在して

$$(*) \quad p\alpha + q\beta + r\gamma = 2\pi$$

となる。逆に言うと、(*) を p, q, r についての方程式とみたとき、これらが0以上の整数解をもつような内角 α, β, γ でなければタイリングは存在しないことになる。これは α, β, γ に関する厳しい条件であるが²、球面のタイリングが構成できるためにはこの条件だけではまだ十分でない。今後 (*), あるいは左辺に現れる係数の組 (p, q, r) のことを頂点の型と呼ぶことにする。

もしあるタイリングにおいて、頂点の型が1種類しか現れないとする。すると、全ての頂点において α, β, γ が常に一定個数現れることになる。このような状況にあるタイリングは相当に限定されたものであるから、この種のタイリングは分類できてよさそうに思える³。

一方、あるタイリングにおいて頂点の型が複数出現すると、 α, β, γ に関する (*) のタイプの方程式が複数出てくる。更に球面の場合には $\alpha + \beta + \gamma - \pi$ が3角形の面積になるから、タイリングの面の数を F とすれば、 $\alpha + \beta + \gamma = (1 + 4/F)\pi$ という等式が成り立つ。もしこれらの方程式の中に独立なものが3個含まれておれば α, β, γ の値が一意に定まってしまう。つまり3角形の形が定まるので、それを用いたタイリングが存在するか否かは、おそらく簡単に判定できるであろう。

²平面の場合は $\alpha + \beta + \gamma = \pi$ なので、これは自明な条件になる。

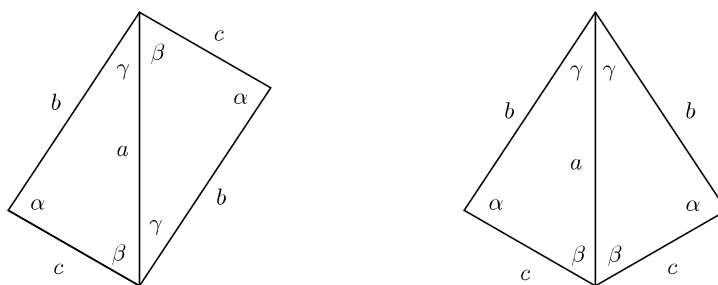
³実際には、4面体の場合しかこのようなことは起こらない。しかし、双曲平面の場合は事情がまるで異なる。

だから(気持ちの上だけの話だが), 1種類の3角形を使った edge-to-edge タイリングの分類は, 数学的に“解ける”問題であるように思われる. そして実際に分類することができた.

以下具体的な分類手順について説明しよう. まず, 次の命題が成り立つ.

命題1. 球面が1種類の不等辺3角形でタイリングされているとする. このときタイリングの各頂点の型 (p, q, r) は, 全て偶数となるか, あるいは全て奇数となるかのいずれかである.

これは例えば, $4\alpha + 3\beta + 2\gamma = 2\pi$ といった型の頂点は存在しないという主張であり, 全て偶数の頂点と, 全て奇数の頂点が一つのタイリングの中に共存することはありうる. 証明については [UA2; Lemma 10, p.505] を見られたい. 組合せ的な議論と帰納法を用いて証明できる. 辺の長さが全て異なるので, 2つの3角形の貼り合わせ方は平行4辺形型(下図左)か, 扇型(下図右)かのいずれかになることが証明のポイントとなる.



命題1を使うと, 更に次の命題が示せる.

命題2. タイリングの面数 F は4より大きいとする. また内角に関して $\alpha > \beta > \gamma$ と仮定する. すると, タイリングの頂点の型は次のいずれかに限る.

$$\alpha + (2q + 1)\beta + (2r + 1)\gamma = 2\pi \quad (q, r \geq 0, \text{ただし } q = r = 0 \text{ を除く}),$$

$$3\alpha + \beta + \gamma = 2\pi,$$

$$4\alpha = 2\pi,$$

$$2\alpha + 2\beta = 2\pi,$$

$$2\alpha + 2s\gamma = 2\pi \quad (s \geq 1),$$

$$2t\beta + 2u\gamma = 2\pi \quad (t, u \geq 0).$$

初めの2つは奇数型, 残りの4つは偶数型の頂点である. 頂点の型にかなりの制約がつくことをこの命題は示している. 実際の証明には結構長い議論が必要だが, ここでは証明の雰囲気分かる程度の説明にとどめる.

奇数型頂点 $(2p+1)\alpha + (2q+1)\beta + (2r+1)\gamma = 2\pi$ が存在する場合. 不等式 $\alpha + \beta + \gamma > \pi$ を使うと⁴, p, q, r のいずれかが 0 になることが簡単に示せる. また, $\alpha + \beta + \gamma = (1 + 4/F)\pi < 2\pi$ より, $p = q = r = 0$ は起こりえないことも分かる.

奇数型頂点に対してこの命題を示すには, $p \geq 1$ の場合を考えれば十分である. $p \geq 1, r = 0$ のときは, 上記 α, β, γ に関する 2 つの等式と不等式 $\alpha > \beta > \gamma$ を使うことにより $p = 1, q = 0$ を導くことができる. 従ってこの場合, 頂点の型は $3\alpha + \beta + \gamma = 2\pi$ となる.

$p, r \geq 1, q = 0$ のときは, 似たような議論によりこのケースは起こりえないことが示せる. これにより奇数型頂点が確定する.

偶数型頂点 $2p\alpha + 2q\beta + 2r\gamma = 2\pi$ についてもほぼ同じ議論を繰り返す. この場合も, p, q, r のうち少なくとも 1 つは 0 になることが示せ, 最終的に命題 2 の結論が得られる.

ここまでの話は 1 頂点の回りだけに限定した, 局所的な議論である. この 1 頂点回りの結果を使って, 次に球面全体の大域的な状況を考察することになる.

前提条件は, 今までと同じ. (1 種類の不等辺 3 角形を使った球面タイリング, $F > 4, \alpha > \beta > \gamma$.) 大きく 2 つの場合に分けて分類作業を行う.

(I) 奇数型の頂点を必ず含む場合.

次の 4 つの事実を, 順に積み重ねながら証明してゆく.

- このタイリングは $\alpha + (2q+1)\beta + (2r+1)\gamma = 2\pi$ ($q, r \geq 0, (q, r) \neq (0, 0)$) 型の頂点を必ず含む.

- このタイリングは $3\alpha + \beta + \gamma = 2\pi$ 型の頂点を含まない.

共に背理法で示す. もし $\alpha + (2q+1)\beta + (2r+1)\gamma = 2\pi$ 型の頂点を含まないとすれば, 命題 2 より $3\alpha + \beta + \gamma = 2\pi$ 型の頂点を必ず含む. この状況のもとでタイルを貼り合せていき, 場合分けしながらタイリングを絞り込んでゆく. 展開図を描き結構長い議論を経て, 最後に矛盾に到達する, 云々.

実際には, 結構広い範囲の展開図を描かないことには矛盾が生じないこともある. また, 2 つ目の事実の証明には球面の位相的性質も絡んでくる. 実際, 境界をもつある非コンパクト正定曲率空間上に, $3\alpha + \beta + \gamma = 2\pi$ 型の頂点をもつタイリングを構成することができる⁵.

- このタイリングは $4\alpha = 2\pi$ 型の頂点を含まない.

⁴球面という性質を, このようなかたちで随所に使っている.

⁵[UA2] の Appendix にその図がある.

• このタイリングにおける $\alpha + (2q + 1)\beta + (2r + 1)\gamma = 2\pi$ ($q, r \geq 0, (q, r) \neq (0, 0)$) 型の頂点においては, $q = 0$ か $r = 0$ かのいずれかが成り立つ.

ここまで示すと, かなり頂点の型が絞り込めたことになる. 繰り返しになるが, ここに至るまでには相当長い議論が必要である.

以上の準備の下で, 奇数型頂点を含むタイリングを全て求める作業に入る. $\alpha + \beta + (2r + 1)\gamma = 2\pi$ ($r \geq 1$) 型の頂点を含む場合と含まない場合とに分けて考察する. ここまで話が絞り込まれていると, 後は必然的にタイルが貼り合わされて, 両者いずれの場合にも 2 種のタイリングが構成できる (合わせて 4 種類).

(II) 全ての頂点が偶数型の場合.

話の流れは奇数型の場合とほぼ同じである. 次の 4 つに場合分けして調べる.

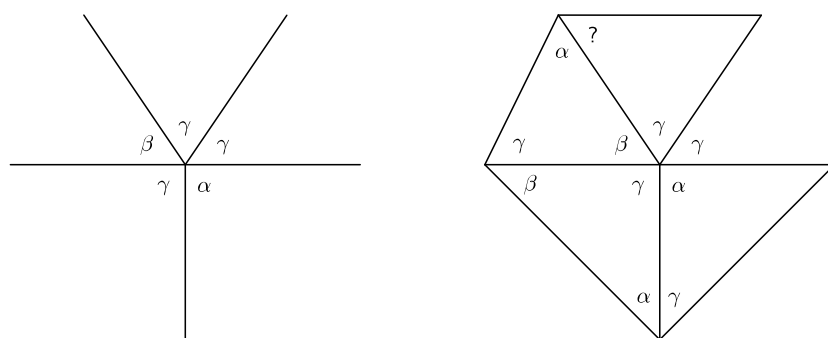
- (a) $\alpha = \pi/2$ で, α は $4\alpha = 2\pi$ 型の頂点にしか現れない.
- (b) $\alpha = \pi/2$ で, α は $4\alpha = 2\pi$ 型以外の頂点にも現れる.
- (c) $\alpha \neq \pi/2$ で, $2\alpha + 2\beta = 2\pi$ 型の頂点が存在する.
- (d) $\alpha \neq \pi/2$ で, $2\alpha + 2\beta = 2\pi$ 型の頂点が存在しない.

いずれのケースからも, いくつかのタイリングが実際に構成される. これらの結果を総合することにより, タイリングの分類が完成する. 証明全体を通じて数学的に難しい議論は一つもないのだが, いかなる手順で話を詰めればよいか, その手順を見つけるところが一番難しい.

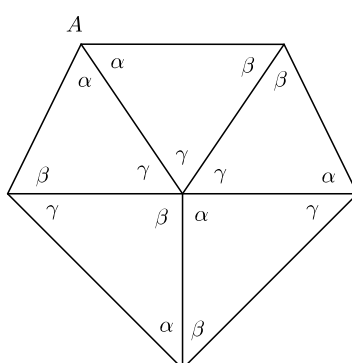
最後に 1 つだけ実例をあげて, 分類の詰めの雰囲気味わってもらおう. (I) の奇数型頂点を含む場合で, 特に $\alpha + \beta + (2r + 1)\gamma = 2\pi$ 型の頂点を含む場合について説明する. 図を簡単にするため, 以下 $r = 1$ として説明する. このとき, タイリングに現れる頂点の型は, 命題 2 と (I) に記した 4 つの事実により

$$\begin{aligned}\alpha + \beta + 3\gamma &= 2\pi, \\ \alpha + (2q + 1)\beta + \gamma &= 2\pi, \\ 2\alpha + 2\beta &= 2\pi, \\ 2\alpha + 2s\gamma &= 2\pi, \\ 2t\beta + 2u\gamma &= 2\pi\end{aligned}$$

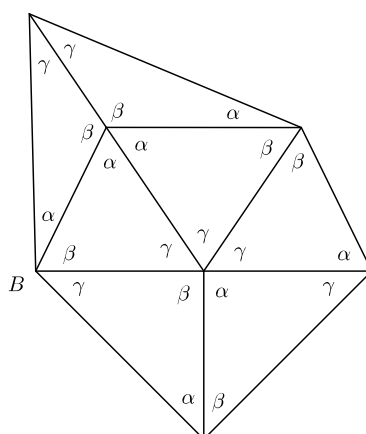
に限られる. $\alpha + \beta + 3\gamma = 2\pi$ 型の頂点からスタートして展開図を描く. この頂点においては, 必ず α と β が隣り合わせにならなくてはいけない. 次の図を見ればその理由は明らかであろう. (2 つの 3 角形の貼り合せ方は, 平行 4 辺形型か 扇型かのいずれかであることを思い出して頂きたい.)



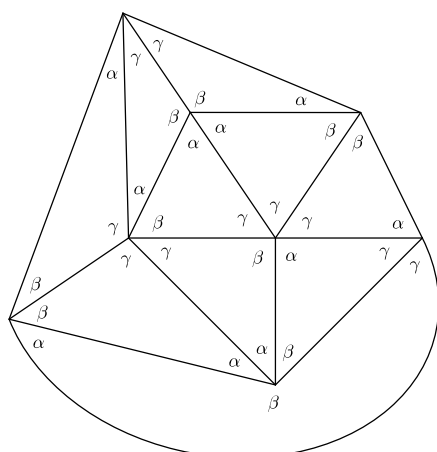
従って次の図から出発してタイリングが構成できるかどうかを調べることになる。



頂点 A には 2α があるから、この頂点の型は $2\alpha + 2\beta = 2\pi$ か $2\alpha + 2\gamma = 2\pi$ のいずれかである。しかし隣の頂点の様子を見ると、ここは $2\alpha + 2\beta = 2\pi$ とするしかないことが分かる。従って次の図のようになる。

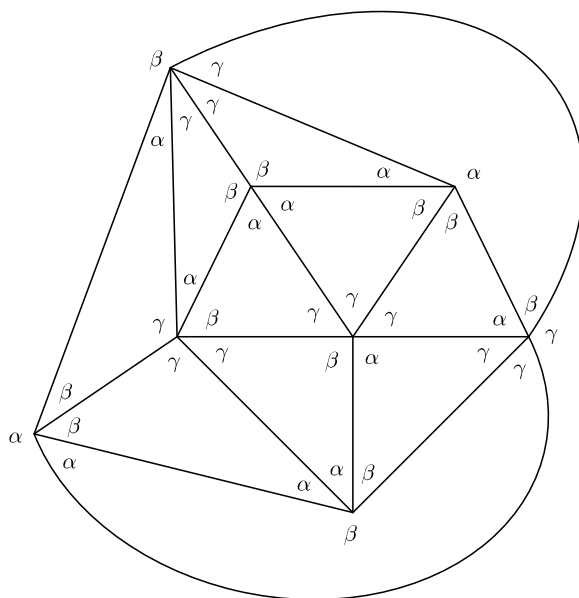


頂点 B には $\alpha + \beta + \gamma$ が集まっている。この空いている隣に β を埋めることはできないから、この頂点の型は $\alpha + (2q + 1)\beta + \gamma = 2\pi$ にはなりえない。既にこの頂点は内角 α, β, γ を含んでいるので、ここは $\alpha + \beta + 3\gamma = 2\pi$ になるしかない。すると、

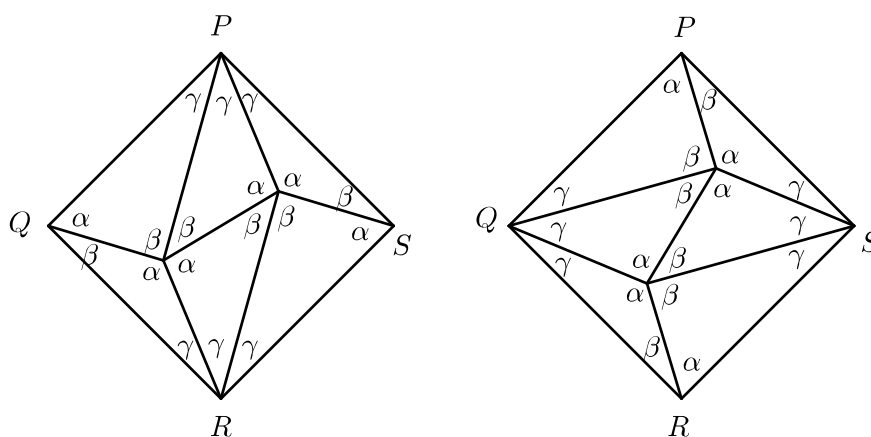


となるところまで一意的に展開図は拡張される. ここで, $\alpha + \beta = \pi$, $\alpha + \beta + 3\gamma = 2\pi$ より, $\alpha + \beta + \gamma = 4\pi/3$ となるので, この3角形の面積は $\pi/3$ である. 従ってこの3角形を使ったタイリングが存在するならば, その面数は $F = 12$ となる. 上の図には既に3角形が10個描かれているので, 上図の境界の外部にある4角形に対角線を引き, 2分割して12面のタイリングを作るしかない.

対角線の引き方は2通りある. 向かい合った $\alpha + 2\beta$ の頂点同志を結び, 確かにタイリングは構成できるのだが, $\alpha + 3\beta + \gamma = 2\pi$ 型の頂点が現れ, $\beta = \gamma = \pi/3$ となってしまふ. これは2等辺3角形になるので不適. 逆の対角線を引くと, 次図のような12面タイリングが得られる.

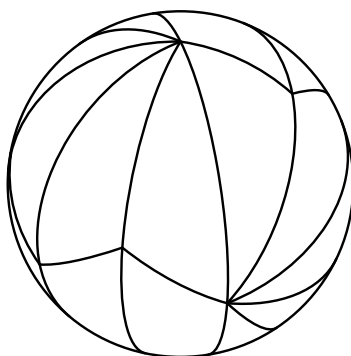


結局このタイリングに現れる頂点の型は $\alpha + \beta + 3\gamma = 2\pi$ と $2\alpha + 2\beta = 2\pi$ だけである. だからこのタイリングは $\alpha + \beta = \pi$ ($\alpha > \beta > \gamma = \pi/3$) を満たす範囲内で変形できる. 上の展開図では全体像がつかみにくいだろうが, これは次の図において同じ記号の頂点同志を貼り合せたものと同じものであることがわかる.



球の半分を剥じって貼り合せてタイリングが構成されていることが分かるだろう。(2つの展開図が同じものであることを確認するには, 上の右図を裏返しにして考えた方が分かりやすい。) これは [UA2] の分類表の中の TG_{12} に該当するものである。

参考までに, $r = 2$ として, $\alpha + \beta + 5\gamma = 2\pi$ 型の頂点を含むタイリングの見取り図 (TG_{20}) を図示しておく。



一般に $r \geq 2$ のときも, $r = 1$ のときと全く同じ議論によりタイリングの存在が確認できる。ただしこの場合は, $r = 1$ のときの最後の詰めにおいて, 4角形に逆向きの対角線を引いたものが不等辺3角形によるタイリングとなる場合がある。それが実はこの原稿の最初のページにある左側の図に他ならない。([UA2] の記号で MTG_{20}^I .)

以上が分類法のラフなスケッチである。証明の詳細を理解するためには原論文 [UA2] を見て頂くしかないが, おおよその雰囲気は分かって頂けたであろうか。全て組合せ的な考察だけで話は詰められたのである。

最後に歴史的なことについても少し触れておく。私が直接知る限りにおいて, 球面の3角形によるタイリングの分類問題に関する先行研究としては Sommerville [S] と Davies [D] しかない。(群作用の条件下で考察した論文が他に若干ある。) S

氏は 2 等辺 3 角形の場合の分類を与え、不等辺 3 角形の場合は各頂点に同じ角が集まっている場合の分類を与えている。後に D 氏が 3 角形の場合の完全な分類結果を表明したが、そこでは証明の詳細は語られておらず、また分類結果に重複もあり、D 氏には申し訳ない言い方になるが、証明の概要を記述した部分にもやや曖昧な点が残されていると私には感じられた。そこで、私の元学生であった上野氏と協力して、分類の完全な証明を与えようと奮闘した成果が [UA2] である。

ちなみに Math. Review にある論文 [D] の評は H.S.M.Coxeter が書いている (MR 0220169, 36 #3235)。そこで C 氏は D 氏の結果を S 氏の duplicate と評しているが、それはちょっと D 氏にはお気の毒としかいいようがない。C 氏によると、分類に関しては更に Hessel という人のドイツ語の論文 (1871 年) があるそうだが、私は未見。

§3. 1 種類の 4 角形を使った球面タイリング

球面の多角形による edge-to-edge タイリングについて、次の定理が成り立つ。

定理 3 [UA1]. n 角形による球面タイリングが存在すれば、 $n = 3, 4, 5$ である。

この定理は、タイルは全て合同という仮定なしに成り立つ。例えばタイルが全て 6 角形の球面タイリングは存在しないことを主張している。証明はオイラーの多面体定理を使うだけの簡単なものである。平面の場合の同様な定理⁶の証明には何らかのかたちで“極限”の概念を使うのだが、それよりはるかにたやすく証明できる。

という訳で、1 種類のタイルを使ったタイリングの分類問題としては $n = 4$ と $n = 5$ のときが残された問題ということになる。この問題については、赤間陽二氏、M. Yan 氏らの精力的な研究があるが、まだ分類が完了するまでには至れていない。この節では、4 角形の場合について基本的なことを簡単にまとめておく。

4 角形の辺の長さを $a \sim d$ の記号を用いて表すことにする。ただし同じ長さのものは同じ記号を使い、長さの異なる場合は異なる記号を用いるものとする。まず次の命題が成り立つ。

命題 4. 1 種類の 4 角形で球面タイリングが可能であれば、そのタイルの 4 辺のうち長さが等しいものがある。(つまり、 $abcd$ 型 4 角形ではタイリング不可能。)

従って、タイリング可能な 4 角形の辺の長さは

$$aaaa, \quad aaab, \quad aabb, \quad aabc$$

⁶平面の場合は $n = 6$ まで可能であった

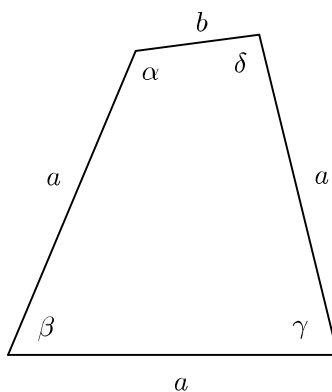
のいずれかである。1つ目はひし形であり、3つ目は平行4辺形型 ($abab$) と、凧型 ($aabb$) があるが、実は平行4辺形型は存在しないことが分かる。4つ目については、向かい合った辺の長さが等しくなることはない。 $aaaa$, $aabb$ 型については、4角形の対角線を引けば合同な2つの3角形に分割されるので、3角形の場合の結果より分類結果が得られる。詳細については [UA1], [SA] をご覧になって頂きたい。

従って残された場合は、 $aaab$ 型と $aabc$ 型の2つである。いずれの場合も分類は未解決だが、どちらかというには $aaab$ 型の方が取り組みやすい問題であるように思える。この場合は長さが b 同志の辺を貼り合わせるしかなく (ただし、貼り合せ方は2通りある)、その結果辺の長さが全て等しい2種類の6角形を使ったタイルを分類する問題に帰着される。この状況は一見3角形の場合に似ているようにも見えるが、大きく異なる点が2つある。

- 現れる内角の種類が、3角形のとくに比べてはるかに多い。従って、内角を集めて 2π を作る組合せの数が多すぎて、場合分けが困難になる。

- 辺の長さが $aaab$ 型であり、各頂点における内角の和が 2π になる展開図がたとえ描けたとしても、それによりタイルの存在が保障されるわけではない。実際、辺の長さが $aaab$ の場合、4つの内角の値には次のような従属関係があり、内角はこの条件を満たさねばならないのである。

命題5. 4角形の辺の長さ、内角を次の図のように定める。



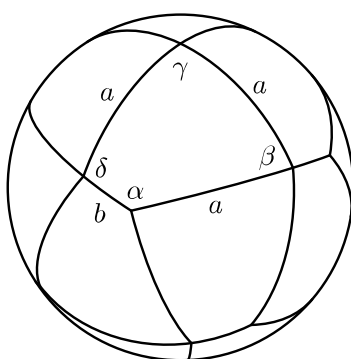
このとき内角 $\alpha \sim \delta$ は次の等式を満たす。

$$(1 - \cos \beta) \cos^2 \alpha - (1 - \cos \beta)(1 - \cos \gamma) \cos \alpha \cos \delta + (1 - \cos \gamma) \cos^2 \delta + \cos \beta \cos \gamma + \sin \alpha \sin \beta \sin \gamma \sin \delta = 1.$$

つまり、内角に関しては $p\alpha + q\beta + r\gamma + s\delta = 2\pi$ 型の等式だけでなく、この3角関数まじりの式も同時に考慮しなくてはならないのである。

分類のための道筋としては、最初はこの3角関数の等式は忘れて、3角形のと
きと同様組合せ的な議論だけで状況を絞り込み、その後で上記の3角関数の条件
式を満たすものをピックアップするという方針が一つ考えられる。しかし、これ
はあまりにも無駄な作業が多すぎるように思われる。つまり組合せ的に絞り込ん
だもののほとんどすべてを、最後の計量的な条件をチェックする段階で捨て去る
ことになるのではなかろうか。3角関数の等式を満たすことは内角に関する相当
厳しい条件であるから、このような事態に陥ることは大いにありうることであ
ろう。組合せ的な議論に入る前に、あらかじめ計量的な条件を使って何かをふるい
落しておくことはできないのだろうか。

ここでは $aaab$ 型の4角形を使ったタイリングの例を1つだけあげておく。



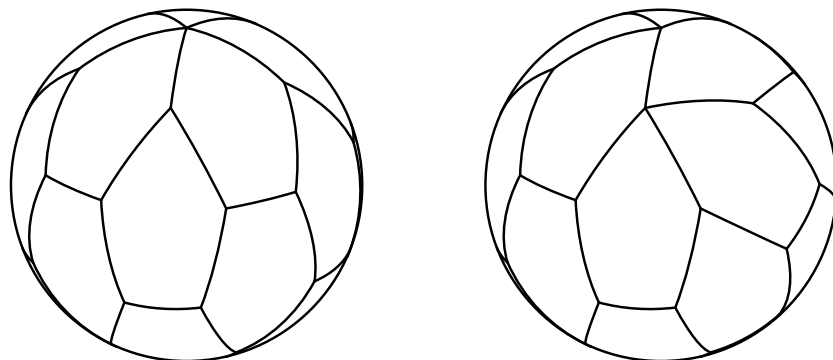
面数は $F = 16$. この4角形の計量的なデータは次で与えられる (球の半径 = 1).

$$a = \cos^{-1} \left(\frac{1}{\sqrt{1+2\sqrt{2}}} \right), \quad b = \cos^{-1} \left(\frac{2\sqrt{2}-1}{\sqrt{1+2\sqrt{2}}} \right),$$

$$\alpha = \frac{3}{4}\pi, \quad \beta = \cos^{-1} \left(\frac{\sqrt{2}-1}{2} \right), \quad \gamma = \frac{1}{2}\pi, \quad \delta = \pi - \beta.$$

この数字を見て、なかなか一筋縄ではゆきそうにない雰囲気を感じとってもらえ
るであろうか。

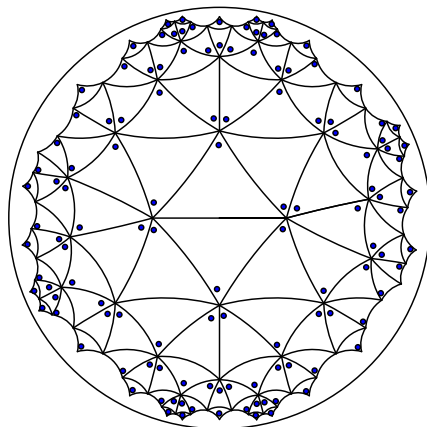
5角形についても4角形と似たような状況にある。これについては図を2つだ
け紹介するにとどめる。右図は、左図の右半分を抜いたもの。



§4. 双曲平面のタイリング

紙面も尽きたし、原稿の締切も過ぎてしまった。双曲平面については、簡単なコメントを述べるだけにする。

双曲平面の場合の難しさは、多くの場合タイリングが作れ過ぎてしまう点にある。例えば $3\alpha + 4\beta = 2\pi$ を満たす $\alpha, \beta > 0$ をとってきたとき、内角が α, β, β の双曲2等辺3角形⁷を使って、全ての頂点の型が $3\alpha + 4\beta = 2\pi$ となるタイリングを双曲平面上に作ることができる。(下図において、点のある内角が α になる。)



すべての頂点が $3\alpha + 4\beta = 2\pi$ では、 α と β の個数のバランスが崩れているように見えるが、双曲平面の場合はそのバランスの崩れを無限大(単位円板の境界近く)におしやってゴマかせるのである。図を見てもらえば、その感触が理解できるであろうか。念のために断っておくと、一見この図にある3角形は大きさがまちまちであるかのように見えるが、実はすべて合同な3角形である⁸。 $3\alpha + 4\beta = 2\pi$ の型を他のものに替えることにより、似たような例が数多く作れる。

多くの場合に、このようにして3角形、4角形、5角形、... を使ってタイリングが構成できる⁹。しかし場合によっては、タイルの貼り合せ作業をいくらすすめても何ら矛盾が生じるわけでもなく、かといって双曲平面全体にタイリングが拡張できる保障が得られるわけでもないといった、どっちつかずの状況に陥ることがしばしばある。また、1枚のタイルを使ったタイリングが存在する場合でも、実に様々なタイリング構成法があるようで、一見法則性が読み取れないような代物すらある。

こういった点が、双曲平面におけるタイリング問題の難しいところであろう。対戦相手としては、なかなか手ごわい。しかしそれが逆に面白いとも言える。

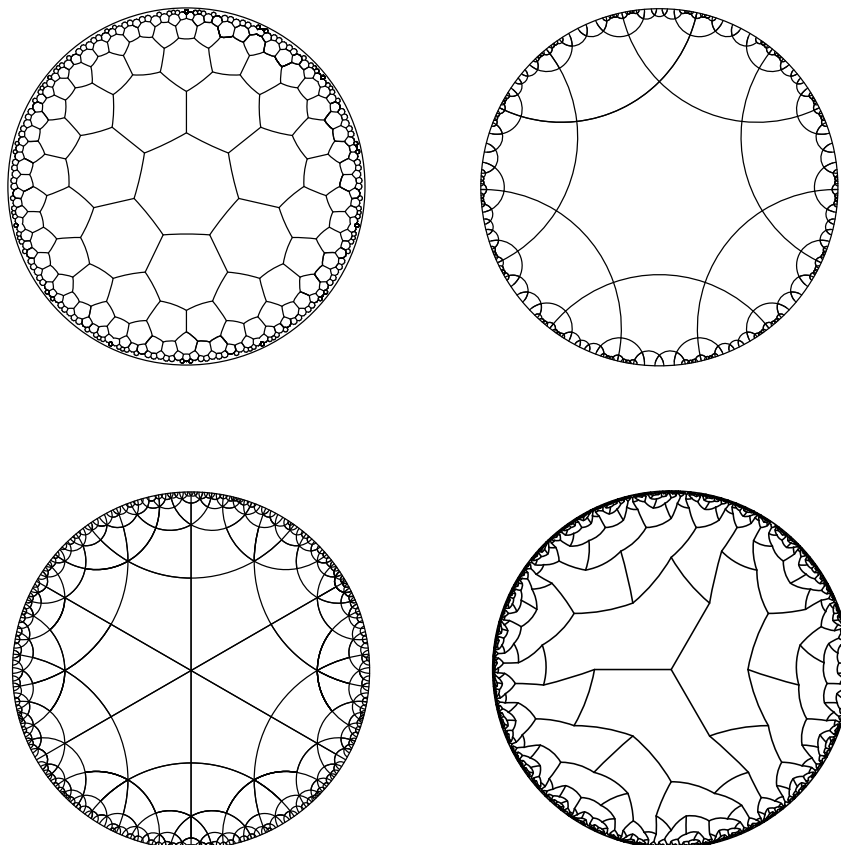
双曲平面においては、タイリング可能なタイルの分類は解決可能な問題かもしれないが、タイリング自体の分類は数学的に解決できる守備範囲(いや、むしろ攻撃範囲か)を超えた問題のようだ。

⁷ $\alpha + 2\beta < \pi$ なので、このような2等辺3角形は存在する。

⁸ただし、角度は正確に実現されている。

⁹双曲平面の場合は、任意の $n \geq 3$ に対して、1種類の n 角形を使ったタイリングが存在する。

最後に双曲平面のタイリングの図を4つ貼り付けておく。右下にある一番最後の図は、私の研究室の元学生平野俊樹氏が見つけたタイリングを、同じく元学生藤城旭氏が作図してくれたもの。図が何を意味するかは、自ずと分かってもらえるであろう。



文 献

- [D] H. L. Davies, Packings of spherical triangles and tetrahedra, in Proceedings of the Colloquium on Convexity (ed. W. Fenchel), 42–51, Københavns Univ. Mat. Inst., Copenhagen, 1967.
- [SA] Y. Sakano, Y. Akama, Anisohedral spherical triangles and classification of spherical tilings by congruent kites, darts and rhombi, Hiroshima Math. J. **45** (2015), 309–339.
https://projecteuclid.org/download/pdf_1/euclid.hmj/1448323768
- [S] D. M. Y. Sommerville, Division of space by congruent triangles and tetrahedra, Proc. Royal Soc. Edinburgh **43** (1922–3), 85–116.

[UA1] Y. Ueno, Y. Agaoka, Examples of spherical tilings by congruent quadrangles, 広島大学総合科学部紀要 IV (理系編) (2001), 135–144.
<http://ir.lib.hiroshima-u.ac.jp/files/public/0/781/2014101612043354659/KJ00000197485.pdf>

[UA2] Y. Ueno, Y. Agaoka, Classification of tilings of the 2-dimensional sphere by congruent triangles, Hiroshima Math. J. **32** (2002), 463–540.
https://projecteuclid.org/download/pdf_1/euclid.hmj/1151007492

連絡先 : agaoka@hiroshima-u.ac.jp

この原稿を準備している最中, 9月14日に Branko Grünbaum 氏が逝去された.
心からご冥福をお祈りします.

On modular linear differential operators and their applications to quasimodular forms

山下 文稔*

1 はじめに

本稿は2018年6月18日に行った講演の内容を一部修正し、加筆したものである。

本稿の主題はモジュラー線形微分方程式 (Modular linear differential equation: MLDE) およびモジュラー線形微分作用素 (Modular linear differential operator: MLDO) である。

MLDE とはモジュラー形式を係数とする上半平面上の線形常微分方程式である。MLDE の特徴的な性質として、その解空間がモジュラー群 $SL(2, \mathbb{Z}) = \{\gamma \in M(2, \mathbb{Z}) \mid \det \gamma = 1\}$ のモジュラー変換で閉じている、ということが挙げられる。

一定の条件を満たす頂点作用素代数 (物理学では共形場理論と呼ぶ) の指標が MLDE の解となることが知られているため ([Z96])、MLDE は頂点作用素代数を分類する研究に応用されている ([MMS88]、[KNS13])。また、MLDE は楕円曲線 ([KZ98]) やベクトル値モジュラー形式 ([M07]) とも関係していることが知られている。特に、上述の [KZ98] で発見された金子・ザギエ方程式 (2階のモニック MLDE) は多くの論文で研究されており、その解と解空間の性質が明らかにされている ([KK03] など)。変数変換によって一部の MLDE を超幾何方程式にすることもできる ([FM16])。MLDE の基本的な性質は [M07] や [FM16] などにまとめられている。

MLDE は具体的には次のような形をしている。

$$(a_n D_k^{(n)} + \cdots + a_1 D_k + a_0) f = 0, \quad (1.1)$$

ここで、 f は未知関数 (上半平面上の有理型関数)、 k は重さと呼ばれる実数値のパラメータ、そして a_i はモジュラー形式であり、(weight of a_i) + $2i$ は i によらず一定である。また、 $D_k^{(n)}$ は階数が n 、重さが k のラマヌジャン・セール作用素と呼ばれる線形微分作用素

$$D_k = \frac{1}{2\pi i} \frac{d}{d\tau} - \frac{k}{12} E_2, \quad (1.2)$$

$$D_k^{(n)} = D_{k+2n-2} \cdots D_{k+2} D_k, \quad (1.3)$$

ただし、 τ は上半平面上の変数、 E_2 は重さ2のアイゼンシュタイン級数 (cf. 第2節) である。数学的な厳密性が欠ける言い方だが、 D_k は重さを2上げる作用素であると

*東京大学大学院数理科学研究科、電子メール：yamast@ms.u-tokyo.ac.jp

見なされる。そのため、 $D_k^{(n)}$ は D_k を単純に n 回合成するのではなく、重さを 2 上げながら n 回合成したものである。

モニック MLDE は特異点をもたないため、 n 階モニック MLDE は線形独立な n 個の正則な解をもつ。しかしモニックでない MLDE の解は正則とは限らず、そもそも上半平面上の大域的な解をもつ保証もない。

MLDE は線形微分方程式であるため、その解空間は線形作用素 $a_n D_k^{(n)} + \dots + a_1 D_k + a_0$ の核である。したがって、この作用素の代数的性質を調べることは重要であると考えられる。しかし、MLDE に関するこれまでの研究には複素解析的な手法を用いるものが多く、作用素が研究の主題となることは少なかった。そのため、筆者は MLDE の微分作用素について研究しようと考えた。

一般に、線形微分方程式を代数的に研究しようとするれば、その作用素のなす環の性質を調べるのは良い方法の一つであると考えられる。しかし MLDE の場合、重さが整合しない作用素の和や積は MLDE の作用素とはならないため、作用素の全体は自然な環の構造をもたない。

そのため、筆者はモジュラー線形微分作用素 (MLDO) と呼ばれる作用素を導入した。大雑把に言えば、MLDO とは MLDE の微分作用素から重さの情報を取り除いたものである。MLDO の全体は環の構造をもち、MLDE は MLDO に関する方程式に変換することができる。MLDO を用いることによって、筆者は MLDE に関する新しい結果をいくつか得ることができた。

2 MLDO の定式化

最初にモジュラー形式に関する基礎的な事実をまとめる。重さ $k \in \mathbb{Z}$ のモジュラー形式とは、(1) 上半平面上の正則関数であり、(2) 重さ k のモジュラー変換で不変であり、さらに (3) 虚軸上の無限遠点 $i\infty$ において有界であるもののことである。重さ k のモジュラー形式の全体を \mathcal{M}_k と表し、 $\mathcal{M} = \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k$ とおく。 E_k を重さ k のアイゼンシュタイン級数とすれば、 $\mathcal{M} = \mathbb{C}[E_4, E_6]$ となることが知られている。特に \mathcal{M} は可換ネーター環である。

なお、 $k \in 2\mathbb{Z}, k > 2$ ならば $E_k \in \mathcal{M}_k$ である。 E_2 はモジュラー形式ではないが、モジュラー形式に似た性質を持っていることが知られており、準モジュラー形式と呼ばれるものの一つである。準モジュラー形式は第 4 節の後半で扱う。

MLDO を作用素として定式化するために、まず作用を受ける関数空間を次のように定める。

$$H = \bigoplus_{k \in \mathbb{R}} H_k, \quad (2.1)$$

ここで、 H_k は上半平面上の正則関数の全体である (k によらない)。 H は自然に (\mathbb{R} を次数とする) 次数付き \mathbb{C} 代数となり、 \mathcal{M} は H の次数付き部分 \mathbb{C} 代数となる。したがって、モジュラー形式は掛け算によって H 上の線形作用素となる。 \mathcal{M} は E_4 と E_6 で生成されているので、この二つに対応する作用素 e_4, e_6 を考えれば十分である。

$$e_4 : H_k \ni (f, k) \mapsto (E_4 f, k + 4) \in H_{k+4}, \quad (2.2)$$

$$e_6 : H_k \ni (f, k) \mapsto (E_6 f, k + 6) \in H_{k+6}. \quad (2.3)$$

更に、ラマヌジャン・セール作用素に対応する H 上の線形作用素を考える。

$$\delta : H_k \ni (f, k) \mapsto (D_k f, k+2) \in H_{k+2}. \quad (2.4)$$

以上の三つの作用素で生成される作用素を MLDO と呼ぶ。また、MLDO 全体のなす非可換 \mathbb{C} 代数を $\mathcal{R} = \langle e_4, e_6, \delta \rangle_{\text{alg}}$ とおき、MLDO 代数と呼ぶことにする。 e_4, e_6, δ にはそれぞれ次数 4, 6, 2 が対応しているので、 $\mathcal{R} = \bigoplus_{k \in \mathbb{Z}} \mathcal{R}_k$ は次数付き代数となる。 \mathcal{M} は自然に \mathcal{R} の次数付き部分代数となっている。

以上のように定式化すれば、上半平面上の正則関数 f に対し、次の同値が成り立つことが分かる。

$$(a_n D_k^{(n)} + \cdots + a_1 D_k + a_0) f = 0 \Leftrightarrow (a_n \delta^n + \cdots + a_1 \delta + a_0)(f, k) = 0. \quad (2.5)$$

つまり、左辺の MLDE は右辺の MLDO ($a_n \delta^n + \cdots + a_1 \delta + a_0 \in \mathcal{R}$) によって表すことができる。対比すると、

- MLDE による表現: 作用素が重さの情報を持ち、関数は重さの情報を持たない、
- MLDO による表現: 作用素は重さの情報を持たず、関数が重さの情報を持つ、ということになる。

3 MLDO 代数の基本的性質

代数 \mathcal{R} の性質を簡単にまとめておく。まず、 $\{e_4^i e_6^j \delta^k \mid i, j, k \in \mathbb{Z}_{\geq 0}\}$ が \mathcal{R} の \mathbb{C} 基底となることが示せる。この基底を用いれば、任意の MLDO は $a_i \in \mathcal{M}$ を用いて $a_n \delta^n + \cdots + a_1 \delta + a_0$ と一意的に表せることが分かる。 δ に関する最高の次数を MLDO の order と呼ぶことにする。

このように、MLDO はモジュラー形式を係数とし、 δ を変数とする多項式のように見なすことができる。実際、 \mathcal{R} は \mathcal{M} と δ からなる歪多項式環 (skew polynomial ring) と同型であることを示すことができる。歪多項式環の理論から、 \mathcal{R} は非可換ネーター整域であることが従う。

MLDO 代数に対しては、余りを許せば割り算を行うことができる。 a, b を MLDO とし、 $b \neq 0$ とする。このとき、 $fa = cb + c'$ および $\text{ord}(c') < \text{ord}(b)$ を満たす $f \in \mathcal{M} \setminus \{0\}$ と $c, c' \in \mathcal{R}$ が存在する。ただしこのような f, c, c' は一意的ではない。

$[\cdot, \cdot]$ を交換子とすれば $[e_4, e_6] = 0$ が成り立つことは明らかである。ラマヌジャンの恒等式を用いれば、 $[\delta, e_4] = -\frac{1}{3}e_6$ と $[\delta, e_6] = -\frac{1}{2}e_4^2$ が分かる。更に、 \mathcal{R} は e_4, e_6, δ を生成元とし、上の三つの交換関係を基本関係式とする \mathbb{C} 代数と同型であることが示せる。

4 主な結果

まず、次の記号を導入しておく。

$$S_k = \{(f, k) \in H_k \mid \text{あるモニックな } a \in \mathcal{R} \setminus \{0\} \text{ が存在して } a(f, k) = 0\}, \quad (4.1)$$

$$\Sigma_k = \{f \mid f \text{ は上半平面上で正則、重さ } k \text{ のモニック MLDE を満たす}\}. \quad (4.2)$$

このとき、上半平面上の正則関数 f に対して、 $(f, k) \in S_k \Leftrightarrow f \in \Sigma_k$ が成り立つ。

定理 1. 1. $S_k + S_k \subset S_k$.

2. $S_k S_l \subset S_{k+l}$.

3. $\mathcal{R}_k S_l \subset S_{k+l}$.

4. $\mathcal{M}_k \subset S_k$.

証明. 概略のみ示す。まず、 $(f, k) \in S_k$ は $\mathcal{R} \cdot (f, k)$ が有限生成 \mathcal{M} 加群であることと同値であることに注意する。(1)–(3)はこの同値と、 \mathcal{M} のネーター性より示すことができる。(4)は $(1, 0) \in S_0$ であること、 $\mathcal{M}_k \subset \mathcal{R}_k$ および (3) によって示すことができる。□

定理 2. 1. $\Sigma_k \subset \Sigma_{k-1}$.

2. $E_2 \Sigma_k \subset \Sigma_{k+1}$.

3. $k - l \in \mathbb{Z}$ かつ $l \leq k$ ならば、 $\Sigma_k + \Sigma_l \subset \Sigma_l$.

証明. (1)(2) $(\delta^2 + \frac{1}{144}e_4)(1, -1) = 0$ かつ $(\delta^3 - \frac{23}{144}e_4\delta - \frac{1}{216}e_6)(E_2, 1) = 0$ が成り立つので、 $1 \in \Sigma_{-1}$ および $E_2 \in \Sigma_1$ である。定理 1 (2) を用いればよい。

(3) (1) より $\Sigma_k \subset \Sigma_l$ である。□

ここで準モジュラー形式 (quasimodular form) について述べておく。重さ k の準モジュラー形式とは、 $f_i \in \mathcal{M}_{k-2i}$ を用いて $\sum_{i=0}^s f_i E_2^i$ と表される正則関数のことである (このような表し方は一意的である)。 E_2 に関する最高の次数を準モジュラー形式の深さという。重さ k のモジュラー形式は重さ k 、深さ 0 の準モジュラー形式であるため、準モジュラー形式はモジュラー形式の一般化となっている。

定理 3. f が重さ k 、深さ s の準モジュラー形式なら $f \in \Sigma_{k-s} \setminus \Sigma_{k-s+1}$.

証明. $f = \sum_{i=0}^s f_i E_2^i$, $f_i \in \mathcal{M}_{k-2i}$, $f_s \neq 0$ とおく。 $f_i E_2^i \in \Sigma_{k-i}$ なので、定理 2 (3) より $f \in \Sigma_{k-s}$ である。 $f \notin \Sigma_{k-s+1}$ は $D_{k-s+1}^{(n)} f$ を計算し、 E_2, E_4, E_6 の代数的独立性を用いることによって示せる。□

[KK03] では、重さ k 、深さ 1 の準モジュラー形式の系列で、重さ $k-1$ のモニック MLDE の解となるものが構成されている。本稿の定理 3 はこの例を一般化するものである。

準モジュラー形式の理論では E_2 の重さは 2 と定義されるが、定理 3 を見ると E_2 の重さは 1 としてもよいのではないか、と思われる。モジュラー形式でない関数に対してその重さをどう定めるかは結局は定義次第だが、 E_2 のモジュラー変換に関連する事実をいくつか挙げることにする。

上半平面上の関数 $f(\tau)$ と $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ に対し、重さ k のモジュラー変換は

$$(f|_k \gamma)(\tau) := (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right) \quad (4.3)$$

である。また、 E_2 は

$$E_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 E_2(\tau) + \frac{12c}{2\pi i}(c\tau + d) \quad (4.4)$$

を満たすことが知られている。したがって、

$$(E_2|_2\gamma)(\tau) = E_2(\tau) + \frac{12c}{2\pi i(c\tau + d)}, \quad (4.5)$$

$$(E_2|_1\gamma)(\tau) = (c\tau + d)E_2(\tau) + \frac{12c}{2\pi i} \quad (4.6)$$

である。この変換を見れば、 E_2 の重さは1とするよりは2とした方が自然ではないかと思われる（ただし好みの問題もある）。更に、 $\Im(\tau)$ を τ の虚部とすれば、 C^∞ 級関数 $E_2 - \frac{3}{\pi\Im(\tau)}$ は重さ2のモジュラー変換で不変である。これは重さ2のマース形式と呼ばれるものであり、 E_2 はそこから標準的に定まる正則部分であることが示せる（なお、マース形式の正則部分をモックモジュラー形式という）。

一方、 E_2 の重さを1と定めれば次のような良い性質がある。つまり、 $\{E_2|_2\gamma \mid \gamma \in \text{SL}(2, \mathbb{Z})\}$ の張る \mathbb{C} 線形空間は無限次元だが、 $\{E_2|_1\gamma \mid \gamma \in \text{SL}(2, \mathbb{Z})\}$ の張る空間は有限次元である。実際、 $\tau E_2 + \frac{12}{2\pi i}$ と E_2 が後者の基底となっている。また、縦ベクトル $F = (\tau E_2 + \frac{12}{2\pi i}, E_2)^t$ を定め、モジュラー変換を成分ごとに定めれば、

$$F|_1\gamma = \gamma F \quad (4.7)$$

が成り立つ。 F は重さ1のベクトル値モジュラー形式と呼ばれるものであり、 E_2 はその成分の一つである。

以上をまとめると、 E_2 に何かを付け加えることによって、重さ2のマース形式にすることもできるし、重さ1のベクトル値モジュラー形式にすることもできる、と言える。

5 その他の結果

定理1-3の結果はすべてモニック MLDE に関するものであるが、モニックとは限らない一般の MLDE に対しても類似した結果が得られる。

MLDE の一般形 (1.1) は次のように書き換えることができる。

$$(D_k^{(n)} + \cdots + \frac{a_1}{a_n} D_k + \frac{a_0}{a_n})f = 0. \quad (5.1)$$

ここで、 a_i/a_n は有理型モジュラー形式と呼ばれるものである。モニックとは限らない一般の MLDE について研究するときは、このように有理型モジュラー形式を係数として考えた方が都合が良い。なぜなら、モジュラー形式の全体 \mathcal{M} はネーター整域であるが、有理型モジュラー形式の全体は次数付き体となるため、 \mathcal{M} よりも性質がよいからである。（詳しい内容は [Y18] の第4.2節）

また、重さ k のモジュラー形式は重さ k のモニック MLDE の解となることが分かったが、その最小の階数については一般的な性質は分かっていない。しかし、特別な場合については次の結果が得られた。

定理 4. $E_4^n, E_6^n, (E_4 E_6)^n$ はそれぞれ重さ $4n, 6n, 10n$ の $n+1$ 階モニック MLDE を満たす。

定理 5. $E_4^m E_6^n$ が重さ $4m+6n$ のモニック MLDE を満たせば、その階数は $\max(m, n)+1$ 以上である。

この定理の証明では、第3節で示した MLDO の割り算が繰り返し使われている。
(詳しい内容は [Y18] の第6節)

様々な m, n で計算したところ、 $E_4^m E_6^n$ は重さ $4m+6n$ の $\max(m, n)+1$ 階モニック MLDE を満たすのではないかと予想される (つまり、定理5において $\max(m, n)+1$ が最小値となっているのだらうと予想される) が、今のところ証明はできていない。先述した通り、全てのモジュラー形式は E_4 と E_6 の多項式として表される。様々なモジュラー形式についてそれが満たすモニック MLDE の最小の階数を計算したが、ある程度の規則性は認められるものの、一般的な性質を求めるのは難しそうである。

謝辞

シンポジウムにおいて発表と議論の場を与えてくださった世話人・関係者の皆様方に感謝いたします。

参考文献

- [FM16] C. Franc and G. Mason: Hypergeometric series, modular linear differential equations and vector-valued modular forms. *Ramanujan J.* **41** (2016), 233–267.
- [KK03] M. Kaneko and M. Koike: On modular forms arising from a differential equation of hypergeometric type. *Ramanujan J.* **7** (2003), 145–164.
- [KNS13] M. Kaneko, K. Nagatomo and Y. Sakai: Modular forms and second order ordinary differential equations: applications to vertex operator algebras. *Lett. Math. Phys.* **103** (2013), 439–453.
- [KZ98] M. Kaneko and D. Zagier: Supersingular j -invariants, hypergeometric series, and Atkin’s orthogonal polynomials. *AMS/IP Studies in Advanced Mathematics* **7** (1998), 97–126.
- [M07] G Mason: Vector-valued modular forms and linear differential equations. *Int. J. Number Theory* **3** (2007), 377–390.
- [MMS88] S. D. Mathur, S. Mukhi and A. Sen: On the classification of rational conformal field theories. *Phys. Lett. B* **213**:3 (1988), 303–308.
- [Y18] F. Yamashita: On modular linear differential operators and their applications. <https://arxiv.org/abs/1807.07204>, arXiv:1807.07204v1 [math.NT], submitted.
- [Z96] Y. Zhu: Modular invariance of characters of vertex operator algebras. *J. Am. Math. Soc.* **9**:1 (1996), 237–302.

Constructions of the McLaughlin graph and of the Co_3 two-graph from the extraspecial group 3_+^{1+4}

小林 雄介 (千葉大学大学院融合理工学府)

1 はじめに

本稿では $McL : 2$ を自己同型群にもつ 275 点上の McLaughlin graph と Co_3 を自己同型群にもつ 276 点上の two-graph を extraspecial group 3_+^{1+4} を用いて構成する方法について述べる.

McLaughlin graph は最大サイズの clique として 5-clique をもち, その固定部分群は $3_+^{1+4} : 4 \cdot S_5$ であり, これは $McL : 2$ の極大部分群のひとつである. 一方, Co_3 two-graph は最大サイズの clique として 6-clique をもち, その固定部分群は $3_+^{1+4} : 4 \cdot S_6$ であり, これは Co_3 の極大部分群のひとつである. 今回の構成には $275 = 5 + 270, 276 = 6 + 270$ であることと次のような群の包含関係が大きく関係している.

$$\begin{array}{ccc} Co_3 & \supset & 3_+^{1+4} : 4 \cdot S_6 \\ \cup & & \cup \\ McL : 2 & \supset & 3_+^{1+4} : 4 \cdot S_5 \end{array}$$

2 強正則グラフと regular two-graph

強正則グラフと regular two-graph の関係性について述べる. 詳しくは [1] を参照してほしい.

定義 1. Γ を完全かつ空でない v 点上のグラフとする. Γ の任意の頂点の隣接数が k で, 任意の異なる 2 頂点 x, y の共通隣接点 x と y がつながっているときに λ 個, x と y がつながっていないときに μ 個であるとき, Γ をパラメータ (v, k, λ, μ) の強正則グラフであるという. Γ の頂点の n 点部分集合 C に対して, C に含まれる任意の 2 頂点がつながっているとき C を n -clique という.

定義 2. \mathcal{P} を集合とし, \mathcal{B} を \mathcal{P} の 3 点部分集合の族 (\mathcal{B} の元をブロックと呼ぶ) とする. \mathcal{P} の任意の 4 点部分集合がブロックを偶数個含むとき, 組 $(\mathcal{P}, \mathcal{B})$ を two-graph という. さらに \mathcal{P} の任意の 2 点部分集合に対して, それを含むブロックの個数が 2 点の取り方に依らず一定であるとき two-graph $(\mathcal{P}, \mathcal{B})$ は regular であるという. \mathcal{P} の n 点部分集合 C に対して, C に含まれる任意の 3 点部分集合がブロックであるとき C を n -clique という.

$D = (\mathcal{P}, \mathcal{B})$ を two-graph とし x を \mathcal{P} の元とする. $\mathcal{P} \setminus \{x\}$ 上のグラフ D_x を

$$y \bullet \text{---} \bullet z \iff \{x, y, z\} \in \mathcal{B}$$

によって定める. 次のことが知られている.

命題 1. *two-graph* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ に対して, 次は同値:

- (i) \mathcal{D} は *regular*;
- (ii) 任意の $x \in \mathcal{P}$ に対して, \mathcal{D}_x は $k = 2\mu$ を満たす強正則グラフ;
- (iii) ある $x \in \mathcal{P}$ に対して, \mathcal{D}_x は $k = 2\mu$ を満たす強正則グラフ.

注意 1. $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ を *regular two-graph* とする. $|\mathcal{P}| = v$ で \mathcal{P} の 2 点を含むブロックの個数が λ とすると, このとき \mathcal{D}_x はパラメータ $(v-1, \lambda, \frac{3\lambda-v}{2}, \frac{\lambda}{2})$ の強正則グラフとなる. 特に C_{03} *two-graph* は *regular* で $\lambda = 112$ であり, そこから今の方法でパラメータ $(275, 112, 30, 56)$ の強正則グラフである *McLaughlin graph* が構成できる.

注意 2. $\Gamma = (V, E)$ をグラフとし, $\binom{V}{3}$ を V の 3 点部分集合全体の集合, ∞ を V に含まれない新たな点とする. $V \cup \{\infty\}$ の 3 点部分集合の族 \mathcal{B} を

$$\mathcal{B} = \{ \{\infty, x, y\} \mid \{x, y\} \in E \} \cup \left\{ B \in \binom{V}{3} \mid B \text{ 内の辺の本数が } 1 \text{ または } 3 \right\}$$

と定める. このとき $\mathcal{D} := (V \cup \{\infty\}, \mathcal{B})$ は *two-graph* となる. この *two-graph* \mathcal{D} を Γ の **extension** という. このようにして逆に *McLaughlin graph* から C_{03} *two-graph* を構成することもできる.

3 extraspecial group 3_+^{1+4}

extraspecial group 3_+^{1+4} について述べる. 一般の *extraspecial group* については例えば [4] を参照してもらいたい.

E を 3_+^{1+4} とする. t を E の中心 $Z(E)$ を生成する位数 3 の元とする. E の中から次の関係式を満たす生成元 x_1, x_2, x_3, x_4 をとってくるができる.

$$\begin{aligned} x_2x_1 &= tx_1x_2, \\ x_4x_3 &= tx_3x_4, \\ x_ix_j &= x_jx_i \text{ unless } \{i, j\} = \{1, 2\} \text{ or } \{3, 4\}, \\ x_i^3 &= 1 \text{ for } i = 1, 2, 3 \text{ and } 4. \end{aligned}$$

E の任意の元 x は

$$x = t^a x_1^{a_1} x_2^{a_2} x_3^{a_3} x_4^{a_4}, \quad a, a_i \in \mathbb{F}_3,$$

という形で一意的に表すことができる. このとき $x = (a \mid a_1, a_2, a_3, a_4)$ と書くことにする.

$x = (a \mid a_1, a_2, a_3, a_4), y = (b \mid b_1, b_2, b_3, b_4) \in E$ に対して,

$$\begin{aligned} xy &= (t^a x_1^{a_1} x_2^{a_2} x_3^{a_3} x_4^{a_4})(t^b x_1^{b_1} x_2^{b_2} x_3^{b_3} x_4^{b_4}) \\ &= t^{a+b} x_1^{a_1} (x_2^{a_2} x_1^{b_1}) x_2^{b_2} x_3^{a_3} (x_4^{a_4} x_3^{b_3}) x_4^{b_4} \\ &= t^{a+b} x_1^{a_1} (t^{a_2 b_1} x_1^{b_1} x_2^{a_2}) x_2^{b_2} x_3^{a_3} (t^{a_4 b_3} x_3^{b_3} x_4^{a_4}) x_4^{b_4} \\ &= t^{a+b+a_2 b_1+a_4 b_3} x_1^{a_1+b_1} x_2^{a_2+b_2} x_3^{a_3+b_3} x_4^{a_4+b_4} \end{aligned}$$

であるから

$$xy = (a + b + a_2 b_1 + a_4 b_3 \mid a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4)$$

となる. また, このことから次のことも分かる.

$$\begin{aligned} xy = yx &\iff a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3 = 0, \\ x^2 = x^{-1} &= (-a + a_1a_2 + a_3a_4 \mid -a_1, -a_2, -a_3, -a_4). \end{aligned}$$

続いて, 次のようにして E から $\tilde{E} := \mathbb{F}_9^2$ への写像を定める.

$$\begin{array}{ccc} E & \longrightarrow & \tilde{E} = \mathbb{F}_9^2 \\ \cup & & \cup \\ x = (a \mid a_1, a_2, a_3, a_4) & \longmapsto & \tilde{x} = (a_1 + a_4i, a_2 + a_3i) \end{array}$$

ただし i は $i^2 = -1$ を満たす \mathbb{F}_9 の元である.

次の補題の E の位数 4 の自己同型は群 $3_+^{1+4} : 4 \cdot S_5$ と $3_+^{1+4} : 4 \cdot S_6$ の “4” に相当するもので, 今回の話の中で重要な役割を果たす.

補題 1. E 上の写像 σ を

$$(a \mid a_1, a_2, a_3, a_4) \xrightarrow{\sigma} (-a + a_1a_2 + a_3a_4 \mid -a_4, -a_3, a_2, a_1)$$

と定めると, これは位数 4 の E の自己同型となる.

注意 3.

$$\begin{aligned} \sigma(\tilde{x}) &= (-a_4 + a_1i, -a_3 + a_2i) \\ &= i(a_1 + a_4i, a_2 + a_3i) \\ &= i\tilde{x}. \end{aligned}$$

E の部分集合 I を次のように定める:

$$I = \{x \in E \mid a + a_1a_2 + a_3a_4 = 0\}.$$

$|I| = 3^4 = 81$, $\tilde{I} = \tilde{E}$ であり, さらに $\sigma(I) = I$ である.

写像 $f : E \setminus Z(E) \rightarrow \mathbb{F}_9 \cup \{\infty\}$ を次のように定める:

$$(a \mid a_1, a_2, a_3, a_4) \xrightarrow{f} \begin{cases} \infty & \text{if } a_2 = a_3 = 0, \\ \frac{a_1 + a_4i}{a_2 + a_3i} \in \mathbb{F}_9 & \text{otherwise.} \end{cases}$$

定義 3. $z \in \mathbb{F}_9 \cup \{\infty\}$ に対して

$$D_z = \{1\} \cup \{x \in I \setminus \{1\} \mid f(x) = z\}$$

と定める.

特に $\sigma(D_z) = D_z$ である.

命題 2. 任意の $z \in \mathbb{F}_9 \cup \{\infty\}$ に対して, D_z は群で $D_z \cong C_3 \times C_3$ となる. ただし C_3 は位数 3 の巡回群を表している. さらに G を E の位数 9 の部分群としたとき

$$\sigma(G) = G \iff \text{ある } z \in \mathbb{F}_9 \cup \{\infty\} \text{ に対して, } G = D_z$$

が成り立つ.

注意 4.

$$\left\{ \tilde{D}_z \mid z \in \mathbb{F}_9 \cup \{\infty\} \right\}$$

は $\tilde{E} = \mathbb{F}_9^2$ の 1 次元空間全体の集合となる.

この 10 個の D_z たちを使って目的の graph や two-graph を構成していくことになる.

4 $\mathbb{F}_9 \cup \{\infty\}$ と $\{1, 2, 3, 4, 5, 6\}$

この節では $\mathbb{F}_9 \cup \{\infty\}$ と 6 点集合 $\{1, 2, 3, 4, 5, 6\}$ の関係性について述べる. ここでの話は例外的な同型対応 $\mathrm{PSL}(2, 9) \cong S_6$ が深く関係している. 詳しくは [3] を参照してもらいたい.

補題 2. E 上の 5 つの写像

$$\begin{aligned} \tau_{+1} &: x \mapsto (a - a_2^2 - a_3^2 \mid a_1 + a_2, a_2, a_3, a_3 + a_4), \\ \tau_{+i} &: x \mapsto (a \mid a_1 - a_3, a_2, a_3, a_2 + a_4), \\ \tau_{-1/z} &: x \mapsto (a - a_1 a_2 - a_3 a_4 \mid a_2, -a_1, -a_4, a_3), \\ \tau_{iz} &: x \mapsto (a + a_1 a_2 + a_3 a_4 + a_1 a_3 - a_2 a_4 \mid \\ &\quad a_1 + a_4, -a_2 + a_3, -a_2 - a_3, -a_1 + a_4), \\ \tau_{z^3} &: x \mapsto (a \mid a_1, a_2, -a_3, -a_4), \end{aligned}$$

は E の自己同型となる. さらに, 任意の $z \in \mathbb{F}_9 \cup \{\infty\}$ に対して,

$$\begin{aligned} \tau_{+1}(D_z) &= D_{z+1}, \\ \tau_{+i}(D_z) &= D_{z+i}, \\ \tau_{-1/z}(D_z) &= D_{-1/z}, \\ \tau_{iz}(D_z) &= D_{iz}, \\ \tau_{z^3}(D_z) &= D_{z^3}, \end{aligned}$$

が成り立つ. ただし $\infty + 1 = \infty + i = -1/0 = i\infty = \infty^3 = \infty, -1/\infty = 0$ とする.

補題 2 より

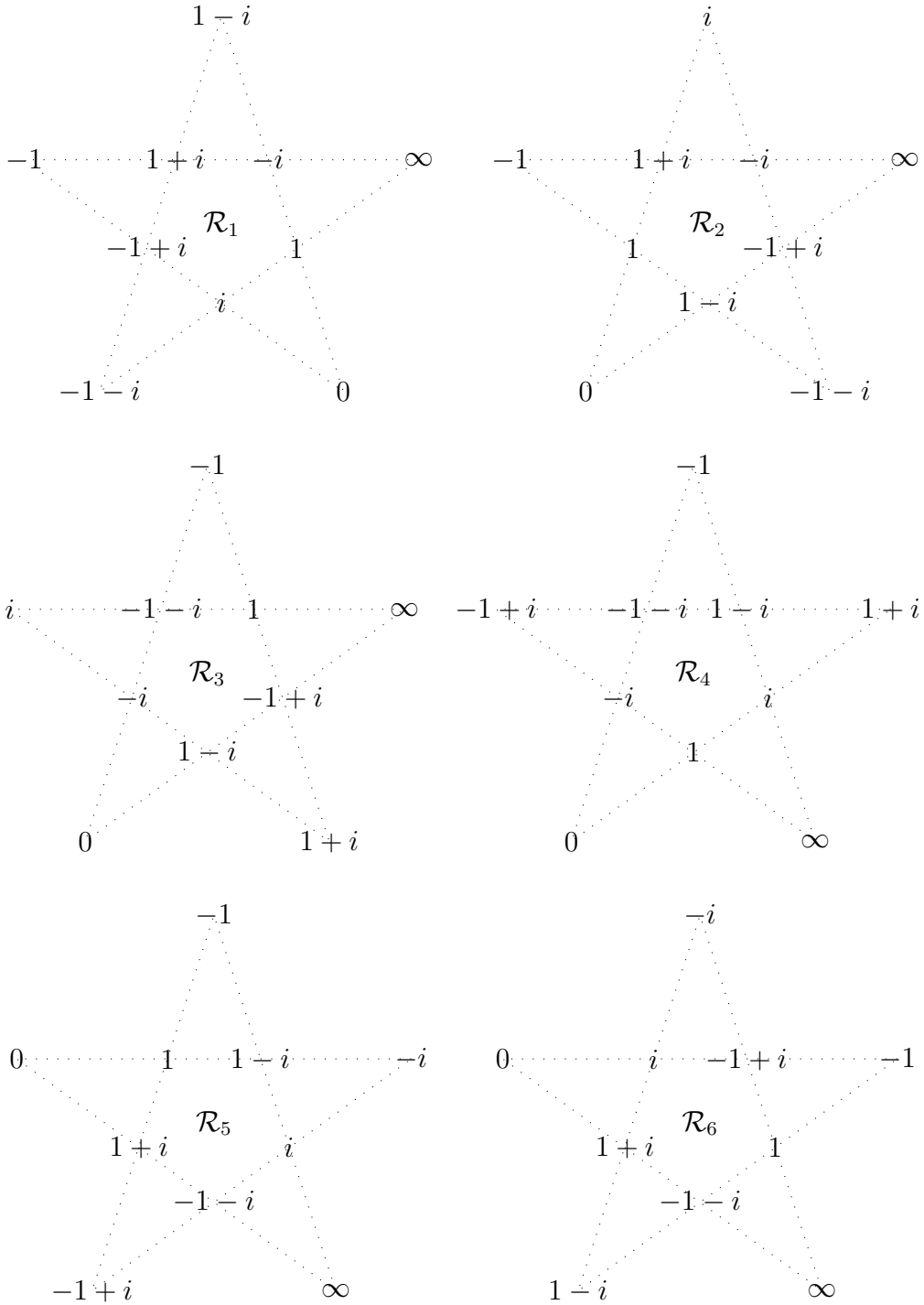
$$H = \langle \sigma, \tau_{+1}, \tau_{+i}, \tau_{-1/z}, \tau_{iz}, \tau_{z^3} \rangle.$$

とすると, H は集合 $\{D_z \mid z \in \mathbb{F}_9 \cup \{\infty\}\}$ に対して, 2 重可移に作用していることが分かる.

定義 4. 集合 $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_6$ を次のように定める:

$$\begin{aligned} \mathcal{R}_1 &= \left\{ \begin{array}{l} \{\infty, -1, -i, 1+i\}, \\ \{\infty, 1, i, -1-i\}, \\ \{1+i, 1-i, -1+i, -1-i\}, \\ \{0, 1, -i, 1-i\}, \\ \{0, -1, i, -1+i\} \end{array} \right\}, & \mathcal{R}_2 &= \left\{ \begin{array}{l} \{\infty, -1, -i, 1+i\}, \\ \{\infty, 0, 1-i, -1+i\}, \\ \{0, 1, i, 1+i\}, \\ \{i, -i, -1+i, -1-i\}, \\ \{1, -1, 1-i, -1-i\} \end{array} \right\}, \\ \mathcal{R}_3 &= \left\{ \begin{array}{l} \{\infty, 1, i, -1-i\}, \\ \{\infty, 0, 1-i, -1+i\}, \\ \{0, -1, -i, -1-i\}, \\ \{1, -1, 1+i, -1+i\}, \\ \{i, -i, 1+i, 1-i\} \end{array} \right\}, & \mathcal{R}_4 &= \left\{ \begin{array}{l} \{1+i, 1-i, -1+i, -1-i\}, \\ \{0, 1, i, 1+i\}, \\ \{0, -1, -i, -1-i\}, \\ \{\infty, -1, i, 1-i\}, \\ \{\infty, 1, -i, -1+i\} \end{array} \right\}, \\ \mathcal{R}_5 &= \left\{ \begin{array}{l} \{0, 1, -i, 1-i\}, \\ \{i, -i, -1+i, -1-i\}, \\ \{1, -1, 1+i, -1+i\}, \\ \{\infty, -1, i, 1-i\}, \\ \{\infty, 0, 1+i, -1-i\} \end{array} \right\}, & \mathcal{R}_6 &= \left\{ \begin{array}{l} \{0, -1, i, -1+i\}, \\ \{1, -1, 1-i, -1-i\}, \\ \{i, -i, 1+i, 1-i\}, \\ \{\infty, 1, -i, -1+i\}, \\ \{\infty, 0, 1+i, -1-i\} \end{array} \right\}. \end{aligned}$$

$\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_6\}$ とする.



H の $\{D_z \mid z \in \mathbb{F}_9 \cup \{\infty\}\}$ 上における作用を $z \in \mathbb{F}_9 \cup \{\infty\}$ 上の作用だと思ふことにする. このとき

$$\begin{aligned} \mathcal{R}_i &\xrightarrow{\sigma} \mathcal{R}_i, & \mathcal{R}_i &\xrightarrow{\tau_{+1}} \mathcal{R}_{(123)(456)i}, \\ \mathcal{R}_i &\xrightarrow{\tau_{+i}} \mathcal{R}_{(123)(465)i}, & \mathcal{R}_i &\xrightarrow{\tau_{-1/z}} \mathcal{R}_{(25)(36)i}, \\ \mathcal{R}_i &\xrightarrow{\tau_{iz}} \mathcal{R}_{(14)(2635)i}, & \mathcal{R}_i &\xrightarrow{\tau_{z^3}} \mathcal{R}_{(14)(25)(36)i}. \end{aligned}$$

が成り立つことから次が示せる.

命題 3. H は \mathcal{R} に対して 6 重可移 に作用している.

さらに次が成り立つ.

命題 4. $H \cong 4 \cdot S_6$.

命題 5. $i \in \{1, \dots, 6\}$ に対して, $H_i := \{g \in H \mid g(\mathcal{R}_i) = \mathcal{R}_i\}$ とする. このとき

$$H_i \cong 4 \cdot S_5.$$

$X_6 = \{1, \dots, 6\}$ とする. 任意の異なる $i, j \in X_6$ に対して, $|\mathcal{R}_i \cap \mathcal{R}_j| = 1$ となっていることが確認できる. 集合 $R_{\{i,j\}}$ を $\{R_{\{i,j\}} = \mathcal{R}_i \cap \mathcal{R}_j$ となるように定める.

$$\begin{aligned} R_{\{1,2\}} &= \{\infty, -1, -i, 1+i\}, & R_{\{1,3\}} &= \{\infty, 1, i, -1-i\}, \\ R_{\{1,4\}} &= \{1+i, 1-i, -1+i, -1-i\}, & R_{\{1,5\}} &= \{0, 1, -i, 1-i\}, \\ R_{\{1,6\}} &= \{0, -1, i, -1+i\}, & R_{\{2,3\}} &= \{\infty, 0, 1-i, -1+i\}, \\ R_{\{2,4\}} &= \{0, 1, i, 1+i\}, & R_{\{2,5\}} &= \{i, -i, -1+i, -1-i\}, \\ R_{\{2,6\}} &= \{1, -1, 1-i, -1-i\}, & R_{\{3,4\}} &= \{0, -1, -i, -1-i\}, \\ R_{\{3,5\}} &= \{1, -1, 1+i, -1+i\}, & R_{\{3,6\}} &= \{i, -i, 1+i, 1-i\}, \\ R_{\{4,5\}} &= \{\infty, -1, i, 1-i\}, & R_{\{4,6\}} &= \{\infty, 1, -i, -1+i\}, \\ R_{\{5,6\}} &= \{\infty, 0, 1+i, -1-i\}. \end{aligned}$$

続いて, P を X_6 の 2 つの 3 点部分集合への分割全体の集合とする. $|P| = 10$ である. $\rho = \{\{i, j, k\}, \{l, m, n\}\} \in P$ に対して, $\rho = (ijk|lmn)$ と書くことにする. このとき任意の $\rho = (ijk|lmn)$ に対して, $R_{\{i,j\}} \cap R_{\{j,k\}} \cap R_{\{k,i\}}$ と $R_{\{l,m\}} \cap R_{\{m,n\}} \cap R_{\{n,l\}}$ はどちらも同じ 1 点集合となる. その元を r_ρ と呼ぶことにする.

$$\begin{aligned} \infty &= r_{(123|456)}, & 0 &= r_{(156|234)}, \\ 1 &= r_{(135|246)}, & -1 &= r_{(126|345)}, \\ i &= r_{(136|245)}, & -i &= r_{(125|346)}, \\ 1+i &= r_{(124|356)}, & 1-i &= r_{(145|236)}, \\ -1+i &= r_{(146|235)}, & -1-i &= r_{(134|256)}. \end{aligned}$$

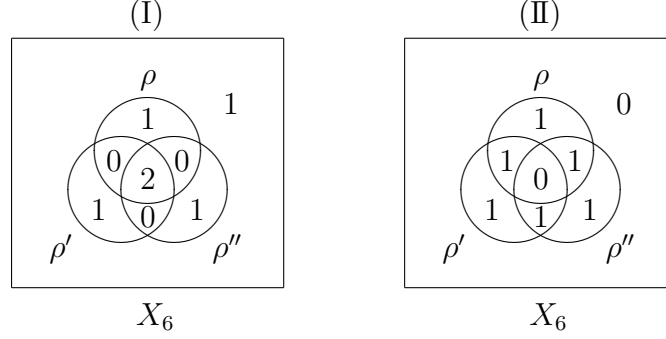
このようにして, 集合 P と集合 $\mathbb{F}_9 \cup \{\infty\}$ を 1 対 1 に対応させる.

注意 5.

$$\begin{aligned} \mathcal{R}_i &= \{R_{\{i,j\}} \mid j \in X_6 \setminus \{i\}\}, \\ R_{\{i,j\}} &= \{r_{(ijk|\dots)} \mid k \in X_6 \setminus \{i, j\}\}. \end{aligned}$$

補題 3. z, z' を $\mathbb{F}_9 \cup \{\infty\}$ の異なる 2 元とし, $z = r_\rho, z' = r_{\rho'}$ ($\rho, \rho' \in P$) であるとする. このとき次が成り立つ.

- (i) ある $i, j \in X_6$ に対して, $\{z, z', z''\} \subset R_{\{i,j\}}$ となるような $z'' = r_{\rho''} \in (\mathbb{F}_9 \cup \{\infty\}) \setminus \{z, z'\}$ が 4 つ存在する. このとき ρ, ρ', ρ'' は X_6 を図 (I) のように 8 分割する.
- (ii) 任意の $i, j \in X_6$ に対して, $\{z, z', z''\} \not\subset R_{\{i,j\}}$ となるような $z'' = r_{\rho''} \in (\mathbb{F}_9 \cup \{\infty\}) \setminus \{z, z'\}$ が 4 つ存在する. このとき ρ, ρ', ρ'' は X_6 を図 (II) のように 8 分割する.



$\{z, z', z''\}$ や $\{\rho, \rho', \rho''\}$ が補題3の (i)(または (ii)) のようになっているとき, それらを *type(I)*(または *type(II)*) と呼ぶことにする.

5 McLaughlin graph と C_{O_3} two-graph の構成

$$\mathcal{W} = \bigcup_{z \in \mathbb{F}_9 \cup \{\infty\}} E/D_z.$$

とする. $|\mathcal{W}| = 3^5/9 \cdot 10 = 27 \cdot 10 = 270$ である. 6点集合 $\mathcal{R} = \{\mathcal{R}_1, \dots, \mathcal{R}_6\}$ と 270点集合 \mathcal{W} を用いて C_{O_3} two-graph を構成する.

$i \in X_6$ と $\rho = (ijk|lmn) \in P$ に対して, $\rho_i := \{j, k\}$ と表すことにする.

定義 5. i, j, k を X_6 の相異なる3元, z, z', z'' を $\mathbb{F}_9 \cup \{\infty\}$ の相異なる3元とし, $z = r_\rho, z' = r_{\rho'}, z'' = r_{\rho''}$ ($\rho, \rho', \rho'' \in P$) とする. さらに $xD_z, x'D_z, x''D_z$ を E/D_z の相異なる3元とし, $yD_{z'} \in E/D_{z'}, wD_{z''} \in E/D_{z''}$ とする.

$\mathcal{R} \cup \mathcal{W}$ 上のブロックの説明を簡単にするために, \mathcal{W} 上のグラフ $\Gamma_{\mathcal{W}}$ を次のように定める:

$$\begin{aligned} xD_z \bullet \text{---} \bullet x'D_z &\iff xD_z = tx'D_z \text{ または } xD_z = t^{-1}x'D_z; \\ xD_z \bullet \text{---} \bullet yD_{z'} &\iff |xD_z \cap yD_{z'}| = 1. \end{aligned}$$

$\mathcal{R} \cup \mathcal{W}$ 上のブロックの集合 \mathcal{B}_E を次のようにして定める:

- (i) $\{\mathcal{R}_i, \mathcal{R}_j, \mathcal{R}_k\} \in \mathcal{B}_E$ (i, j, k の取り方に依らない)
- (ii) $\{\mathcal{R}_i, \mathcal{R}_j, xD_z\} \in \mathcal{B}_E$
 $\iff z \in R_{\{i,j\}}$
 $\iff \rho = (ij \cdot | \dots) \iff j \in \rho_i.$
- (iii) $\{\mathcal{R}_i, xD_z, x'D_z\} \in \mathcal{B}_E$
 $\iff xD_z = tx'D_z \text{ t } xD_z = t^{-1}x'D_z.$
- (iv) $\{\mathcal{R}_i, xD_z, yD_{z'}\} \in \mathcal{B}_E$
 $\iff \begin{cases} |xD_z \cap yD_{z'}| = 1 \text{ かつ ある } j \in X_6 \setminus \{i\} \text{ に対して, } \{z, z'\} \subset R_{\{i,j\}}. \\ \text{または,} \\ |xD_z \cap yD_{z'}| = 0 \text{ かつ 任意の } j \in X_6 \setminus \{i\} \text{ に対して, } \{z, z'\} \not\subset R_{\{i,j\}}. \end{cases}$
 $\iff \begin{cases} |xD_z \cap yD_{z'}| = 1 \text{ かつ } \rho = (ijk|lmn), \rho' = (ijl|kmn). \\ \text{または,} \\ |xD_z \cap yD_{z'}| = 0 \text{ かつ } \rho = (ijk|lmn), \rho' = (ilm|jkn). \end{cases}$
 $\iff |\rho_i \cap \rho'_i| = |xD_z \cap yD_{z'}|.$

$$(v) \{xD_z, x'D_z, x''D_z\} \in \mathcal{B}_E$$

$$\iff \{xD_z, x'D_z, x''D_z\} \text{ によって誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \end{array} \text{ または } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} .$$

$$(vi) \{xD_z, x'D_z, yD_{z'}\} \in \mathcal{B}_E$$

$$\iff \{xD_z, x'D_z, yD_{z'}\} \text{ によって誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \end{array} \text{ または } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} .$$

$$(vii) \{xD_z, yD_{z'}, wD_{z''}\} \in \mathcal{B}_E$$

$$\iff \left\{ \begin{array}{l} \{z, z', z''\} \text{ が type(I) かつ } \{xD_z, yD_{z'}, wD_{z''}\} \text{ によって} \\ \text{誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \end{array} \text{ または, } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} . \\ \text{または} \\ \{z, z', z''\} \text{ が type(II) かつ } \{xD_z, yD_{z'}, wD_{z''}\} \text{ によって} \\ \text{誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \quad \bullet \end{array} \text{ または, } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} . \end{array} \right.$$

$$\iff \left\{ \begin{array}{l} \{\rho, \rho', \rho''\} \text{ が type(I) かつ } \{xD_z, yD_{z'}, wD_{z''}\} \text{ によって} \\ \text{誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagup \quad \diagdown \\ \bullet \quad \bullet \end{array} \text{ または } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} . \\ \text{または} \\ \{\rho, \rho', \rho''\} \text{ が type(II) かつ } \{xD_z, yD_{z'}, wD_{z''}\} \text{ によって} \\ \text{誘導される } \Gamma_{\mathcal{W}} \text{ の部分グラフが } \begin{array}{c} \bullet \\ \diagdown \quad \diagup \\ \bullet \quad \bullet \end{array} \text{ または } \begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} . \end{array} \right.$$

$\mathcal{D} = (\mathcal{R} \cup \mathcal{W}, \mathcal{B}_E)$ とする.

次に 275 点上のグラフを定める.

定義 6. $X_5 := X_6 \setminus \{6\} = \{1, \dots, 5\}$, $\mathcal{R}' := \mathcal{R} \setminus \{\mathcal{R}_6\} = \{\mathcal{R}_1, \dots, \mathcal{R}_5\}$ とする. $z = r_\rho$ に対して $\mathcal{E}_z^{\rho_6} := E/D_z$ とする. グラフ $\Gamma_{\mathcal{M}}$ を $\Gamma_{\mathcal{M}} := \mathcal{D}_{\mathcal{R}_6}$ で定める. つまり, $\Gamma_{\mathcal{M}}$ は $\mathcal{R}' \cup \mathcal{W}$ 上のグラフで $v, v' \in \mathcal{R}' \cup \mathcal{W}$ に対して,

$$v \text{ --- } v' \iff \{\mathcal{R}_6, v, v'\} \in \mathcal{B}_E$$

で辺が定まっている. 詳しく述べると $j, k \in X_5$ ($j \neq k$), $z, z' \in \mathbb{F}_9 \cup \{\infty\}$ ($z \neq z'$), $z = r_\rho, z' = r_{\rho'}$ ($\rho, \rho' \in P$), $xD_z, x'D_z \in E/D_z$ ($xD_z \neq x'D_z$), $yD_{z'} \in E/D_{z'}$ に対して,

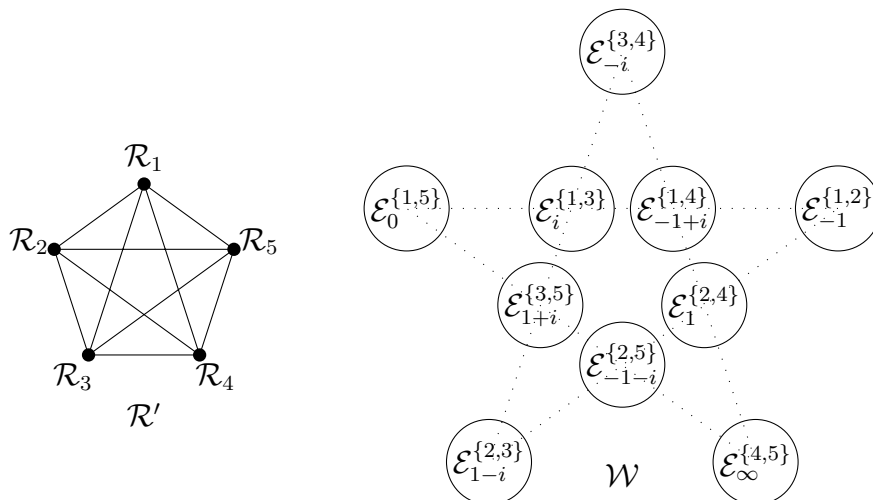
$$(i)' \quad \mathcal{R}_j \text{ --- } \mathcal{R}_k \quad (j, k \text{ の取り方に依らない})$$

$$(ii)' \quad \mathcal{R}_j \text{ --- } xD_z \iff \begin{array}{l} z \in R_{\{6, j\}} \\ \iff j \in \rho_6. \end{array}$$

$$(iii)' \quad xD_z \text{ --- } x'D_z \iff xD_z = tx'D_z \text{ or } xD_z = t^{-1}x'D_z.$$

$$(iv)' \quad xD_z \text{ --- } yD_{z'} \iff \begin{cases} |xD_z \cap yD_{z'}| = 1 \text{ かつ ある } j \in X_5 \text{ に対して, } \{z, z'\} \subset R_{\{6, j\}}. \\ \text{または} \\ |xD_z \cap yD_{z'}| = 0 \text{ かつ 任意の } j \in X_5 \text{ に対して, } \{z, z'\} \not\subset R_{\{6, j\}}. \end{cases}$$

$$\iff |\rho_6 \cap \rho'_6| = |xD_z \cap yD_{z'}|.$$



\mathcal{D} が $\Gamma_{\mathcal{M}}$ の extension になっていることが確認できる. したがって \mathcal{D} は two-graph となる. さらに \mathcal{D} が regular ($\lambda = 112$) になることも確認することができる. [2] で 276 点上の regular two-graph の一意性が証明されているので, 次の主結果が得られる.

定理 1. $\mathcal{D} = (\mathcal{R} \cup \mathcal{W}, \mathcal{B}_E)$ は C_{O_3} two-graph である.

系 1. $\Gamma_{\mathcal{M}}$ は *McLaughlin graph* である.

最後に $x \in E$ に対して,

$$\begin{aligned} \mathcal{R}_i &\xrightarrow{\varphi_x} \mathcal{R}_i; \\ yD_z &\xrightarrow{\varphi_x} xyD_z \end{aligned}$$

と定義された写像 $\varphi_x : \mathcal{R} \cup \mathcal{W} \rightarrow \mathcal{R} \cup \mathcal{W}$ は明らかに $\mathcal{D} = (\mathcal{R} \cup \mathcal{W}, \mathcal{B}_E)$ や $\Gamma_{\mathcal{M}}$ の自己同型になっている. さらに $H \subset \text{Aut}(\mathcal{D})$ や $H_6 \subset \text{Aut}(\Gamma_{\mathcal{M}})$ であることから

$$3_+^{1+4} : 4 \cdot S_6 \subset C_{O_3},$$

$$3_+^{1+4} : 4 \cdot S_5 \subset \text{McL} : 2$$

という 2 つ非自明な包含関係を計算機を用いずに実感することができた.

References

- [1] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Mathematical Society Student Texts 22, Cambridge University Press, Cambridge, 1991.
- [2] J. M. Goethals and J. J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* 12 (1975), 143-158.
- [3] Robert A. Wilson, *The Finite Simple Groups*, Springer, Graduate Mathematics series 251 (2009).
- [4] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.* 2 (1972), no. 2, 159-168.

Some remarks on Matsuda's theorem on partial Burnside rings

近畿大学大学院総合理工学研究科 *

若竹 昌洋

Masahiro Wakatake

Kindai University Graduate School of Science and Engineering

1 はじめに

有限群 G の Burnside 環とは, 推移的 G -集合の同型類を基底にもつ自由 Z -加群に対し, 直積によって積を定義したものである. Burnside 環は整数環 Z の直積環の部分環と同型になることが知られている. したがって Burnside 環の単元群の構造は必ず基本可換 2-群となる. Burnside 環を用いると, シローの定理などいくつかの G の部分群の個数に関する合同式を得られる ([DSY92]). また, Burnside 環の代数的構造と可解性の関係が [Dr69] で述べられており, [to79] では特に奇数位数の有限群に関しては Burnside 環の単元群と可解性との関係が述べられている. 本報告では, Burnside 環の単元群に焦点を当てる.

Burnside 環の単元群に関して, 松田が [Ma82] において様々なことを証明した. さらに Burnside 環の拡張として, 一般 Burnside 環が [Yo90] で定義されており, ある条件のもとで一般 Burnside 環は部分 Burnside 環と呼ばれている. 本報告では, 松田の Burnside 環の単元群に関する結果を部分 Burnside 環に拡張し, それを用いることで得られた結果を紹介する.

2 記号

とくに注意しない限り, 本報告では以下の意味で各記号を用いる.

G : 有限群

1 : (G の) 自明な群

$\text{Sub}(G)$: G の部分群全体

G^c : G の群に関する共役類の集合

\mathcal{D}^c : (G 共役で閉じた) G の部分群の族 \mathcal{D} における群の共役類の集合

(H) : G の部分群 H の共役類

$[X]$: G -集合 X の (G -集合に関する) 同型類

$|X|, \#X$: 有限集合 X の濃度

3 Burnside 環と単元群

Burnside 環の定義はいくつか存在するが, ここでは自由 \mathbb{Z} 加群を用いて Burnside 環を記述したほうが分かりやすいので, 次のように Burnside 環を定義する.

定義 3.1. 有限群 G の Burnside 環 $\Omega(G)$ とは, 推移的 G -集合の同型類たちを基底にもつ自由 \mathbb{Z} -加群

$$\Omega(G) := \langle [G/H] \mid (H) \in G^c \rangle_{\mathbb{Z}}$$

に対し, 積を

$$[G/H] \cdot [G/K] = \sum_{HgK \in H \backslash G/K} [G/g^{-1}Hg \cap K].$$

で定義したものである.

特に非交和 (disjoint union) を和とみなすことで任意の G -集合 (の同型類) は Burnside 環の元とみることができる.

定理 3.2. G を有限群, X, Y を有限 G -集合とする. このとき

$$X \simeq Y \Leftrightarrow |\text{inv}_H(X)| = |\text{inv}_H(Y)| \quad \forall H \leq G$$

となる. ここで, $\text{inv}_H(X) := \{x \in X \mid hx = x, \forall h \in H\}$ である.

各 $H \leq G$ に対し, 写像 $\varphi_H : \Omega(G) \rightarrow \mathbb{Z}$ は環準同型となるので, 定理 3.2 は環準同型写像

$$\varphi = \prod_{(H) \in G^c} \varphi_H : \Omega(G) \rightarrow \prod_{(H) \in G^c} \mathbb{Z}$$

が単射であることを意味する. この写像 φ を **Burnside 準同型写像** という.

この単射性は後述する一般 Burnside 環に対しても同様に成り立つことが示されている ([Yo90]).

さらに, この Burnside 準同型写像から得られる表現行列をマーク行列と呼ぶ. つまりマーク行列 M は,

$$M = (\varphi_H[G/K])_{H, K \in \text{Sub}(G)}$$

である. マーク行列はうまく基底を並び替えることで三角行列となる.

Burnside 準同型写像の単射性より, 次の系を得る.

系 3.3. G を有限群とすると, $\Omega(G)$ は整数環 \mathbb{Z} の直積環の部分環と同型であり, さらに $\Omega(G)$ の単元群 $\Omega(G)^\times$ は基本可換 2-群となる.

これによって Burnside 環の単元群の位数は常に 2 冪となることが分かる. また, [to79] の Problem 1.5.2 で述べられている, Burnside 環の単元群の位数と有限群の構造と密接に関わっていることがわかる定理を紹介する.

定理 3.4 ([to79]). ”非可換単純群の位数が偶数である”ための必要十分条件は, ”奇数位数の群 G に対し, $\Omega(G)^\times = \{\pm 1_{\Omega(G)}\}$ ” となることである.

非可換単純群の位数が偶数であることは既に Feit と Thompson による奇数位数定理の系として得られている, そのため奇数位数の群の Burnside 環の単元群の構造は自明なものであることが分かる. しかし面白いことにこの”非可換単純群の位数が偶数である”ことを予想したのは Burnside なので, Burnside 環を用いて Burnside の予想を証明することが期待される. さらにそこから奇数位数定理の別証明が Burnside 環を用いて出来る可能性がある.

4 部分 Burnside 環

Burnside 環の単元を求めるための計算手法はあまり知られておらず, 群 G の構造が複雑になるほど難しくなってくる. そこで, 研究対象を少しでも小さくするために, Burnside 環の部分環を構成しつつ一般化する方法を述べる.

定義 4.1. G の部分群の族 \mathcal{D} が閉じているとは, 次の 2 つの条件を満たすものとする.

- $H \in \mathcal{D} \Rightarrow H^g \in \mathcal{D} \quad (\forall g \in G)$
- $H, K \in \mathcal{D} \Rightarrow H \cap K \in \mathcal{D}$

特に, G の閉じた部分群族 \mathcal{D} が G を含むとき, \mathcal{D} をコレクションと呼ぶ.

定義 4.2 (一般 Burnside 環と部分 Burnside 環). G を有限群とする. G の閉じた部分群に対し,

$$\Omega(G, \mathcal{D}) := \langle [G/H] \mid (H) \in \mathcal{D}^c \rangle$$

を G の \mathcal{D} に関する一般 Burnside 環と呼ぶ. 特に \mathcal{D} がコレクションであるとき, $\Omega(G, \mathcal{D})$ を部分 Burnside 環と呼ぶ.

一般 Burnside 環に対しても Burnside 環同様に Burnside 準同型 $\varphi^{\mathcal{D}}$ とマーク行列 $M^{\mathcal{D}}$ を定義でき, それぞれ G の \mathcal{D} に関する Burnside 準同型, マーク行列と呼ぶ.

Remark 4.3. 一般 Burnside 環は Burnside 環の単位的とは限らない部分環であり, 部分 Burnside 環は必ず単位的部分環となる. 特に部分群族として $\mathcal{D} = \text{Sub}(G)$ のとき, 部分 Burnside 環と Burnside 環は一致する.

5 拡張版松田の定理

この章では拡張された松田の定理 ([Ma82, Theorem 4.1, 4.2]) を紹介する.

定義 5.1 (基本コレクション). G のコレクション \mathcal{D} が基本コレクションであるとは, 次の 3 つの条件を満たすことを言う.

- $1 \in S$.
- $H \in S$ ならば H は正規部分群.
- 任意の $H, K \in S$ に対し $HK \in S$.

ここで, $HK = \{hk \mid h \in H, k \in K\}$ である.

G を有限群, \mathcal{D} を G のコレクション, S を G の基本コレクションとする. 各 $H \in S$ に対し,

$$S_{\mathcal{D}}(H) := \{F \in \mathcal{D} \mid H \leq F, \text{ if } H' \in S \text{ and } H \leq H' \leq F, \text{ then } H = H'\}.$$

と置く. $S_{\mathcal{D}}(H)$ は閉じた部分群族なので, $\Omega(G, S_{\mathcal{D}}(H))$ は一般 Burnside 環となる. 特に,

$\Omega(G, S_{\mathcal{D}}(H))$ が部分 Burnside 環となるための必要十分条件は $H = G$ である.

松田の定理と同じような方法で, 次の定理が得られる.

定理 5.2 (拡張版松田の定理). G を有限群とし, \mathcal{D} を G のコレクションとする. さらに S を G の基本コレクションとすると,

$$|\Omega(G, \mathcal{D})^\times| = 2 \prod_{H \in S \setminus \{G\}} |\overline{\Omega(G, S_{\mathcal{D}}(H))}|,$$

ここで

$$\overline{\Omega(G, S_{\mathcal{D}}(H))} := \{x \in \Omega(G, S_{\mathcal{D}}(H)) \mid x^2 + 2x = 0\}.$$

さらに,

$$|\Omega(G, \mathcal{D})^\times| = 2 \prod_{H \in S \setminus \{G\}} \left| (M^{S_{\mathcal{D}}(H)})^{-1} \left(\mathbb{Z}'_2^{|S_{\mathcal{D}}(H)|} \right) \cap \mathbb{Z}^{|S_{\mathcal{D}}(H)|} \right|,$$

ここで $M^{S_{\mathcal{D}}(H)}$ は G の $S_{\mathcal{D}}(H)$ に関するマーク行列であり, $\mathbb{Z}'_2 = \{0, -2\} \subseteq \mathbb{Z}$ である. 特に,

$$\{-1_{\Omega(G)}\} \cup \bigcup_{H \in S} \bigcup_{x \in \overline{\Omega(G, S_{\mathcal{D}}(H))} \setminus \{0\}} \{1_{\Omega(G)} + x\}$$

は丁度 $\Omega(G, \mathcal{D})^\times$ を生成する.

6 拡張版松田の定理の応用

この章では, 松田の定理を用いて得られた様々な結果を紹介する.

命題 6.1. G を正規部分群とし, $\text{NS}(G)$ を G の正規部分群全体の集合とする. このとき,

$$|\Omega(G, \text{NS}(G))^\times| = 2^{\#\{H \leq G \mid |G:H| \leq 2\}}.$$

さらに,

$$\{-1_{\Omega(G)}\} \cup \{u_H \mid H \leq G, |G:H| = 2\}$$

は $\Omega(G, \text{NS}(G))^\times$ を生成する. ここで, $u_H = 1_{\Omega(G)} - [G/H]$ である.

Proof. 今 $S := \text{NS}(G)$ とすると S は基本コレクションである. 各 $H \in \text{NS}(G) \setminus G$ に対し, $S_{\text{NS}(G)}(H) = \{H\}$ より $\Omega(G, S_{\text{NS}(G)}(H)) = \mathbb{Z} \cdot [G/H]$ となる. H は正規部分群なので,

$$|\overline{\Omega(G, S_{\text{NS}(G)}(H))}| = \begin{cases} 1 & |G:H| \neq 2, \\ 2 & |G:H| = 2, \end{cases}$$

を得る. □

この命題 6.1 は [Ma82, Example 4.5] の拡張となっている. 実際次の系が得られる.

系 6.2. G を有限可換群とする. このとき,

$$|\Omega(G)^\times| = 2^{\#\{H \leq G \mid |G:H| \leq 2\}}.$$

補題 6.3. G を有限群とし, N を G の正規部分群とする. このとき,

$$\Omega(G/N) \simeq \Omega(G, \text{Sub}(G)_N),$$

ここで $\text{Sub}(G)_N := \{H \leq G \mid N \leq H\}$ である.

Proof. 対応定理より, すぐに計算で確かめられる. □

次の補題もすぐに確かめられる.

補題 6.4. G_1, G_2 を有限群, \mathcal{D} を G_1 のコレクションとする. もし, 全射群準同型写像 $f: G_1 \rightarrow G_2$ が存在するならば, G_2 の部分群族

$$f(\mathcal{D}_{\ker f}) = \{f(H) \leq G_2 \mid H \in \mathcal{D}, \ker f \leq H\}$$

はコレクションとなる.

この 2 つの補題と, 拡張版松田の定理により, 以下が得られる.

定理 6.5 (W.). G_1, G_2 を有限群とし, \mathcal{D} を G_1 のコレクションとする. $f: G_1 \rightarrow G_2$ が全射群準同形写像ならば,

$$\Omega(G_1, \mathcal{D}_{\ker f}) \simeq \Omega(G_2, f(\mathcal{D}_{\ker f})),$$

ここで

$$\mathcal{D}_{\ker f} := \{H \in \mathcal{D} \mid \ker f \leq H\}.$$

$$f(\mathcal{D}_{\ker f}) := \{f(H) \leq G_2 \mid H \in \mathcal{D}, \ker f \leq H\}.$$

さらに次の結果が得られる.

定理 6.6 (W.). G を有限群とすると以下は同値である.

- (1) G が非可換単純群ならば, $|G|$ は偶数.
- (2) $|G|$ が奇数ならば, $\Omega(G)^\times = \{\pm 1_{\Omega(G)}\}$.

(3) $|G|$ が奇数ならば, $\Omega(G)^\times \simeq \Omega(G, \text{NS}(G))^\times$.

(4) $|G|$ が奇数ならば, $\Omega(G)^\times \simeq \Omega(G, \text{Sub}(G)_{G'})^\times$.

ここで, $\text{NS}(G)$ は G の正規部分群の集合, $\text{Sub}(G)_{G'} = \{H \leq G \mid G' \leq H\}$, G' は G の交換子部分群である.

Proof. (1) \Leftrightarrow (2) は [to79] で示されている. 命題 6.1 より, $|G|$ が奇数ならば $|\Omega(G, \text{NS}(G))| = 2$. よって (2) \Leftrightarrow (3). 補題 6.3 より, $\Omega(G, G_{G'}) \simeq \Omega(G/G')$. G/G' は可換群なので, 命題 6.1 より $|\Omega(G/G')| = 2$. したがって (2) \Leftrightarrow (4). \square

Burnside 環に関する写像として次の興味深い写像がある.

定理 6.7 ([DSY92, Theorem 1.]). C_n を位数 n の巡回群, $C := C_{|G|}$ とする. さらに,

$$\alpha = \alpha^G : \Omega(C) \longrightarrow \Omega(G)$$

を各 $K \leq G$ に対し, $\varphi_K^G(\alpha(x)) = \varphi_{C_{|K|}}^C(x)$ で与えられる写像とする. このとき, 写像 α は環準同形写像である. この写像を **Frobenius-Wielandt 準同形写像** と呼ぶ.

Frobenius-Wielandt 準同形写像と拡張版松田の定理を組み合わせることで次の結果を得た.

定理 6.8 (W.). G を位数 n の有限群, C を位数 n の巡回群とする. G がべき零群ならば,

$$\alpha(\Omega(C)^\times) \subseteq \Omega(G, \text{NS}(G))^\times.$$

ここで $\text{NS}(G)$ は G の正規部分群全体, α は **Frobenius-Wielandt 準同形写像** である.

今までに現れた群構造と Burnside 環との関係は可解性であったが, これによって新たにべき零性との関わりも分かった.

参考文献

- [Dr69] A. Dress : *A Characterisation of Solvable Groups*, Math. Z. **110** (1969), 213–217.
- [DSY92] Dress, A.W.M. ; Siebeneicher, C. ; Yoshida, T.: *An application of Burnside rings in elementary finite group theory*, Adv. Math. **90** (1992), 27–44.
- [Ma82] Matsuda, T.: *On the unit groups of Burnside rings*, Japan. J. Math. (N.S.) **8** (1982), no. 1, 71–93.

- [to79] tom Dieck, T. : *Transformation Groups and Representation Theory*, Lecture Notes in Mathematics, **766**, Springer, Berlin, 1979.
- [Yo90] Yoshida, T. : *The generalized Burnside ring of a finite group*, Hokkaido Math. J. **19** (1990), no. 3, 509–574.

Reduced Fock representation of the Virasoro algebra

Hiro-Fumi YAMADA (Kumamoto University)

1 Excuse

The main body of this report is essentially due to Minoru Wakimoto [W]. He considered the basic representation $L(\Lambda_0)$ of the affine Lie algebra $A_1^{(1)}$. He observed that the principal realization of $L(\Lambda_0)$ admits an action of a larger algebra $A_1^{(1)} + \mathcal{V}ir$, which he calls the extended affine Lie algebra. Here $\mathcal{V}ir$ stands for the Virasoro algebra. In this way one has the reduced Fock representation of the Virasoro algebra. Wakimoto succeeded in the irreducible decomposition of it by finding the highest weight vector of each irreducible component. The reduced Fock representation of $\mathcal{V}ir$ is realized on the space of polynomials, and the highest weight vectors are expressed in terms of the Schur functions labeled by the 2-core partitions. This is already beautiful and interesting. However, more amazingly, polynomials in “lower” components are nothing but the Hirota polynomials for the BKP hierarchy. Once Wakimoto told me the story. At first, he had no idea on Hirota polynomials living in the lower components. He computed quite a few examples and made a phone-call to Ryogo Hirota (1932-2015). Knowing that the first nontrivial polynomial is of degree 6, Hirota answered that they must be BKP. At that time it was already known that the Schur functions are deeply related with the KP and the KdV hierarchies. And so I had some uncomfortable feeling hearing that BKP appears in this $A_1^{(1)}$ context.

Now, after 35 years, I know that Schur’s Q-functions are suitable for the BKP hierarchy. It is natural to understand Wakimoto’s theory in the framework of Q-functions and the basic representation of $D_2^{(2)}$, which is isomorphic to $A_1^{(1)}$. The following is an attempt of sweeping my embarrassment away.

2 Reduced Fock representation

Everything is played on the polynomial ring of infinitely many variables:

$$V = \mathbb{R}[t_j; j \geq 1, \text{odd}] = \bigoplus_{n=0}^{\infty} V_n,$$

where V_n denotes the space of homogeneous polynomials of degree n , subject to the counting $\deg t_j = j$. We call this the reduced Fock space. This space is equipped with a symmetric bilinear form

$$\langle F, G \rangle = F(2\tilde{\partial})G(t)|_{t=0},$$

where $\tilde{\partial} = (\frac{\partial}{\partial t_1}, \frac{1}{3}\frac{\partial}{\partial t_3}, \frac{1}{5}\frac{\partial}{\partial t_5} \dots)$. Define operators $a_j : V_n \rightarrow V_{n-j}$ for odd integers j by

$$a_j = \sqrt{2}\partial_j = \sqrt{2}\frac{\partial}{\partial t_j}, \quad a_{-j} = \frac{j}{\sqrt{2}}t_j \quad (j \geq 1, \text{odd}).$$

These satisfy the Heisenberg relation:

$$[a_j, a_k] = j\delta_{j+k,0} \textit{id}.$$

For integers k , define the operators $L_k : V_n \rightarrow V_{n-2k}$ by

$$L_k = \frac{1}{4} \sum_{j \in \mathbb{Z}_{\text{odd}}} : a_{-j} a_{j+2k} : + \frac{1}{16} \delta_{k0} \textit{id} \quad (k \in \mathbb{Z}).$$

Here the symbol $: ** :$ denotes the normal ordering:

$$: a_j a_k : = a_j a_k \text{ if } j \leq k, \quad a_k a_j \text{ if } j > k.$$

These operators satisfy the Virasoro relation:

$$[L_k, L_m] = (k - m)L_{k+m} + \frac{k^3 - k}{12} \delta_{k+m,0} \textit{id}.$$

Namely we have a representation (π, V) of the Virasoro algebra:

$$\mathcal{V}ir = \bigoplus_{k \in \mathbb{Z}} \mathbb{R}\ell_k \oplus \mathbb{R}z$$

by

$$\pi(\ell_k) = L_k, \quad \pi(z) = \textit{id}.$$

We call it the reduced Fock representation of the Virasoro algebra. This is completely reducible, i.e., is decomposed into irreducible components.

Here is concrete form of generators:

$$\begin{aligned} L_0 &= \frac{1}{2} \sum_{j \geq 1} jt_j \partial_j + \frac{1}{16}, \\ L_1 &= \frac{1}{2} \partial_1^2 + \frac{1}{2} \sum_{j \geq 1} jt_j \partial_{j+2}, \\ L_2 &= \partial_1 \partial_3 + \frac{1}{2} \sum_{j \geq 1} jt_j \partial_{j+4}, \\ L_{-1} &= \frac{1}{8} t_1^2 + \frac{1}{2} \sum_{j \geq 3} jt_j \partial_{j-2}, \\ L_{-2} &= \frac{3}{4} t_1 t_3 + \frac{1}{2} \sum_{j \geq 5} jt_j \partial_{j-4}. \end{aligned}$$

With respect to the bilinear form, we have $a_j^* = a_{-j}$ and hence $L_k^* = L_{-k}$. Namely the bilinear form is contravariant for the Virasoro operators. Therefore the reduced Fock representation (π, V) is decomposed into irreducible components which are orthogonal to each other.

We call a homogeneous polynomial $f \in V$ a singular vector if $L_k f = 0$ for $k \geq 1$. A singular vector generates an irreducible component of the reduced Fock representation, i.e.,

$$\{L_{-k_1} L_{-k_2} \cdots L_{-k_\ell} f; \ell \geq 0, k_1 \geq \cdots \geq k_\ell \geq 1\}$$

spans an irreducible highest weight representation with highest weight vector f . By Kac character formula, each irreducible component has formal character $1/\phi(q^2)$, where $\phi(q) = \prod_{k=1}^{\infty} (1 - q^k)$, the Euler function.

To describe the highest weight vector, we recall Schur's Q-functions. For a strict partition $\lambda = (\lambda_1, \dots, \lambda_\ell)$ of n , define

$$Q_\lambda(t) = \sum_{\rho} 2^{\lfloor \frac{\ell(\lambda) - \ell(\rho) + 1}{2} \rfloor} \zeta_{\rho}^{\lambda} \frac{t_1^{m_1} t_3^{m_3} \cdots}{m_1! m_3! \cdots} \in V_n,$$

where the summation runs over all odd partitions $\rho = (1^{m_1} 3^{m_3} \dots)$ of n , and ζ_{ρ}^{λ} denotes the spin character value of the symmetric group

\mathfrak{S}_n , which is an integer. We need the sign alternation coming from the isomorphism $A_1^{(1)} \simeq D_2^{(2)}$ [NY]:

$$\text{alt} : V \longrightarrow V, F(t) \mapsto F^a(t)$$

with

$$F^a(t) = F(t_1, -t_3, -t_5, t_7)$$

with reading t_j as $t_{j(\bmod 8)}$. Here is an example.

$$Q_{(51)}(t) = \frac{1}{180}t_1^6 + \frac{1}{6}t_1^3t_3 - t_3^2 - t_1t_5,$$

and

$$Q_{(51)}^a(t) = \frac{1}{180}t_1^6 - \frac{1}{6}t_1^3t_3 - t_3^2 + t_1t_5.$$

Reflecting the orthogonality relation of spin characters of the symmetric group, the Q-functions satisfy the orthogonality relation:

$$\langle Q_\lambda^a, Q_\mu^a \rangle = 0 \quad \text{if } \lambda \neq \mu$$

This means that the Q-functions form an orthogonal basis for the reduced Fock space V .

Strict partitions are illustrated as bead-configurations on the following abacus:

	1	3	
	2		
	4	5	7
	6		
	8	9	11
	10		
	12	13	15
	14		

Given a bead-configuration on the abacus. Consider the following types of up-moves (resp. down-moves) of the beads:

- (1) Move a bead one place up (resp. down) on a runner.
- (2) Remove (resp. put) a bead on the position 2.
- (3) Remove (resp. put) two beads from (resp. to) the positions 1 and 3 simultaneously.

In any move, beads should not overlap at the same position, because a bead-configuration indicates a strict partition.

A bead-configuration from which no up-moves can be achieved is called a hard-core. One easily sees that the set of the hard-cores is

$$\mathcal{HC} = \{\emptyset, L_r, R_r ; r \geq 1\},$$

where

$$L_r = (4r - 3, 4r - 7, \dots, 5, 1), \quad R_r = (4r - 1, 4r - 5, \dots, 7, 3).$$

Namely, a hard-core is a filling of beads from the top to some place without gap on one of the runners of 1, 3. Note that $|L_r| = r(2r - 1)$ and $|R_r| = r(2r + 1)$.

Theorem 1 (Wakimoto[W] 1983, rephrased by Yamada).

$$L_k Q_\lambda^a = 0 \quad (k \geq 1)$$

for $\lambda \in \mathcal{HC}$.

Let denote by $V(\lambda)$ the irreducible highest weight subrepresentation of V generated by the singular vector $Q_\lambda^a(t)$ ($\lambda \in \mathcal{HC}$). Using the Gauss identity, one computes the character of the direct sum of all found irreducible components as follows.

$$\begin{aligned} \sum_{\lambda \in \mathcal{HC}} ch(V(\lambda)) q^{|\lambda|} &= \frac{1}{\phi(q^2)} \sum_{r=0}^{\infty} q^{\frac{r(r+1)}{2}} \\ &= \frac{1}{\phi(q^2)} \cdot \frac{\phi(q^2)^2}{\phi(q)} \\ &= \frac{\phi(q^2)}{\phi(q)} = ch(V). \end{aligned}$$

This completes the irreducible decomposition:

$$V = \bigoplus_{\lambda \in \mathcal{HC}} V(\lambda).$$

For a given strict partition μ , apply consecutive up-moves until the stalemate. The resulting configuration is a hard-core. This is called the hard-core of μ . Namely, each strict partition has its own hard-core. For $\lambda \in \mathcal{HC}$ denote by \mathcal{SP}^λ the set of strict partitions whose hard-core is λ .

Theorem 2. For each hard-core λ , the irreducible component $V(\lambda)$ has an orthogonal basis consisting of Q-functions:

$$\{Q_\mu^a(t); \mu \in \mathcal{SP}^\lambda\}.$$

3 Hirota polynomials

We recall a remarkable observation of Wakimoto in 1983 [W]. Although this has been proved by using vertex operators [Y], I am still puzzled by the relation of the Virasoro algebra and this kind of integrable systems.

Consider

$$V(\emptyset)^\perp = \bigoplus_{\lambda \in \mathcal{HC}, \lambda \neq \emptyset} V(\lambda) = \bigoplus_{\lambda \in \mathcal{HC}, \lambda \neq \emptyset} \bigoplus_{\mu \in \mathcal{SP}^\lambda} \mathbb{R} Q_\mu^a(t).$$

Take a polynomial $P(t) \in V(\emptyset)^\perp$. Then the Hirota bilinear equations

$$P(\sqrt{2}\tilde{D}) \tau \cdot \tau = 0$$

are the KP hierarchy of type B (BKP for short). Here $\tilde{D} = (D_1, \frac{1}{3}D_3, \frac{1}{5}D_5, \dots)$ denotes the Hirota bilinear differential operator. This means that the BKP hierarchy is nothing but the orthogonality relation of the Virasoro representation, or more basically, that of the spin characters of the symmetric group. Here is an example. Take $Q_{(51)}^a(t)$, the highest weight vector of the irreducible component $V(L_2)$. Then

$$Q_{(51)}^a(\sqrt{2}\tilde{D}) = \frac{2}{45}(D_1^6 - 5D_1^3D_3 - 5D_3^2 + 9D_1D_5).$$

This is the first nontrivial Hirota polynomial for the BKP hierarchy. Hirota polynomials of low degrees for KP, mKP, KdV and BKP hierarchies are tabulated in [JM].

There is one more rather vague remark. We call a homogeneous polynomial $f \in V$ a quasi-singular vector if $L_1 f = 0$. The following is contained in the full set of the quasi-singular vectors:

$$\{Q_\lambda^a(t); \lambda \in \mathcal{HC}\} \cup \{Q_{B_r}(t); r \geq 1\},$$

where $B_r = (2r - 1, 2r - 3, \dots, 3, 1)$. For example

$$Q_{B_2}(t) = \frac{1}{12}t_1^4 - t_1 t_3$$

That $Q_{B_r}(t)$ is quasi-singular is proved in [IMNY]. We know that

$$Q_{B_2}(\tilde{D}) = \frac{1}{12}(D_1^4 - 4D_1 D_3)$$

is the first Hirota polynomial for the KdV hierarchy. It is plausible that the Hirota bilinear equations for the KdV hierarchy are

$$Q_\lambda(\tilde{D}) \tau \cdot \tau = 0$$

for the strict partitions λ with at least one odd part. Therefore the KdV hierarchy, too, could be viewed from the Virasoro representation.

References

- [IMNY] T. Ikeda, H. Mizukawa, T. Nakajima and H.-F. Yamada, Mixed expansion formula for the rectangular Schur functions and the affine Lie algebra $A_1^{(1)}$, *Adv. Appl. Math.* 40 (2008), 514–535
- [JM] M. Jimbo and T. Miwa, Solitons and infinite dimensional Lie algebras, *Publ. RIMS, Kyoto Univ.* 19 (1983), 943–1001
- [NY] T. Nakajima and H. -F. Yamada, Schur's Q-functions and the basic representation of affine Lie algebras, *Adv. Studies in Pure Math.* 28 (2000), 241–256
- [W] M. Wakimoto, Basic representations of extended affine Lie algebras, *RIMS-Kokyuroku* 503 (1983), 36–46

- [Y] H. -F. Yamada, The basic representation of the extended affine Lie algebra of type $A_1^{(1)}$ and the BKP hierarchy, *Lett. Math. Phys.* 9 (1985), 133–137

ユニタリ群上の大対蹠集合と Hamming cube

栗原 大武

北九州工業高等専門学校生産デザイン工学科一般科目

1 序

まずこの報告書で扱う記号を整理しておく. n は 2 以上の整数とし, $[n] := \{1, 2, \dots, n\}$ とおく. $2^{[n]}$ を $[n]$ の冪集合とする. 集合 X に対して $\binom{X}{2} := \{\{x, y\} \mid x, y \in X, x \neq y\}$ とする. また $(\mathbb{Z}^n)_+ := \{\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{Z}^n \mid \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n\}$ とする.

1977 年に Delsarte-Goetals-Seidel [4] によって球面上のデザイン理論が与えられ, その後さまざま多様体上でデザイン理論が考えられてきた. 特に多様体の中でもコンパクト対称空間についてはその上でのデザイン理論が数多く研究されている. この報告書ではコンパクト対称空間としてユニタリー群 $U(n)$ の場合を考える. $U(n)$ の中の性質の良い有限部分集合に大対蹠集合と呼ばれるものがある. 今回大対蹠集合がデザインとしてはどのようなものになるかを調べる. この話はコンパクト対称空間として球面の場合で言えば, S^n の中の対蹠点 $\{x, -x\}$ が $\text{Harm}_{2k+1}(S^n)$ ($k = 1, 2, \dots$) に関するデザインになることに対応する. また $U(n)$ の大対蹠集合に自然な距離構造を入れることで Hamming cube グラフと呼ばれる良く知られたグラフになる. その観点から $U(n)$ と Hamming cube の調和解析の関係を調べる.

2 対称 R 空間と対蹠集合

最初に対称空間について述べる.

定義 2.1. リーマン多様体 (M, g) が対称空間であるとは以下の条件を満たすこと: 各点 $x \in M$ に対して点対称 s_x が存在する. ただし点対称とは,

- (1) $s_x: M \rightarrow M$ は等長変換,
- (2) $s_x \circ s_x = \text{id}_M$,
- (3) x は s_x の孤立不動点.

M の等長変換群 $\text{Isom}(M)$ は Lie 変換群であり, M に推移的に作用する. 一方でリーマン対称空間は特別なリー群の組とみなせる. G を連結リー群, K を G の閉部分群とする. これらの組 (G, K) が次の条件を満たすときこの組をリーマン対称対という:

- (1) 次の条件を満たす対合 $\sigma: G \rightarrow G$ が存在する: $\text{Fix}(\sigma, G)^0 \subset K \subset \text{Fix}(\sigma, G)$. ただし $\text{Fix}(\sigma, G)$ は G の σ による固定部分群, $\text{Fix}(\sigma, G)^0$ は $\text{Fix}(\sigma, G)$ の単位元を含む連結成分である.
- (2) K はコンパクト.

リーマン対称空間 M は $\text{Isom}(M)$ から自然にリーマン対称対を構成できる. 一方でリーマン対称対 (G, K) からは等質空間 G/K と対合 σ を考えることで逆にリーマン対称空間を得る.

定義 2.2. M を連結なコンパクト対称空間とし, s_x を x での点対称とする. M の部分集合 S が対蹠集合であるとは以下の条件を満たすこと: 任意の $x, y \in X$ に対して, $s_x(y) = y$ が成り立つ.

M はコンパクトであり, 各点 $x \in M$ は s_x の孤立不動点なので, 対蹠集合は有限集合になる. Chen–Nagano [3] は M の 2-number を

$$\sharp_2 M := \max\{\#S \mid S \text{ is an antipodal set in } M\},$$

として定めた. $|S| = \sharp_2 M$ である対蹠集合 S を大対蹠集合と呼ぶ. コンパクト対称空間の中で“良い”性質を持ったものを対称 R 空間という. この報告書の中では定義は述べず, 今回の話題に関連する結果のみを紹介する. 対称 R 空間について定義やその他の性質については, Nagano [7], Takeuchi [10], Faraut, et al. [5, §II.1 in Part II]などを参考にせよ.

事実 2.3 (Takeuchi [12]). M が対称 R 空間であるとき,

$$\sharp_2 M = \dim H_*(M, \mathbb{Z}_2)$$

が成り立つ. ただし $H_*(M, \mathbb{Z}_2)$ は \mathbb{Z}_2 係数の M のホモロジー群である.

事実 2.4 (Sánchez [9], Tanaka–Tasaki [13]). $M = G/K$ が対称 R 空間であるとき, 次が成り立つ:

- (1) M の極大対蹠集合は全て大対蹠集合である. すなわち M の任意の対蹠集合 S_0 に対して, $S_0 \subset S$ となる大対蹠集合 S が存在する.
- (2) M の大対蹠集合は G 作用を除き一意的である. すなわち, M の任意の 2 つの大対蹠集合 S, S' に対して, $S' = gS$ となる $g \in G$ が存在する.

この報告書では空間 M がユニタリ群 $U(n)$ の場合を考える. $U(n)$ は以下の対称対との対応により対称空間とみなせる. $U(n) \times U(n)$ 上の写像 $\sigma: (g_1, g_2) \mapsto (g_2, g_1)$ は $U(n) \times U(n)$ の対合的自己同型であり, σ の固定部分群は $\text{diag } U(n) := \{(g, g) \mid g \in U(n)\}$ である. このとき $(U(n) \times U(n), \text{diag } U(n))$ はリーマン対称対である. 今後 $G := U(n) \times U(n)$ and $K := \text{diag } U(n)$ とする. さらに $U(n)$ は対称 R 空間であることも知られている. 事実 2.4 より $U(n)$ 上の大対蹠集合の構造は一意的であり, またその構造は以下のようになることが容易に確かめられる:

$$S := \left\{ \left(\begin{array}{cccc} \epsilon_1 & 0 & \cdots & 0 \\ 0 & \epsilon_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \epsilon_n \end{array} \right) \middle| \epsilon_1, \epsilon_2, \dots, \epsilon_n \in \{\pm 1\} \right\}.$$

$\text{dist}: U(n) \times U(n) \rightarrow \mathbb{R}_{\geq 0}$ を $U(n)$ 上の距離関数とする. 大対蹠集合 S に関して, $U(n)$ 上で S の最小距離を以下のように定義する:

$$\text{dist}_{\min}(S) := \min\{\text{dist}(x, y) \mid x, y \in S, x \neq y\}$$

$\text{dist}_{\min}(S)$ により S に距離構造を入れることより, 次を得る.

定理 2.5 (栗原-奥田 [6]). $E := \{\{x, y\} \in \binom{S}{2} \mid \text{dist}(x, y) = \text{dist}_{\min}(S)\}$ とするとき, (S, E) は Hamming cube Q_n である.

なお [6] において, 他の対称 R 空間の大対蹠集合についてもそれぞれに応じた距離正則グラフの構造が自然に得られることも述べてある.

- $\text{Gr}_k(\mathbb{F}^n)$ の大対蹠集合 ($\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{H}$) \leftrightarrow Johnson graph $J(n, k)$
- $SO(2n)/U(n)$ の大対蹠集合 \leftrightarrow Halved Hamming cube $\frac{1}{2}Q_n$

など.

3 Schur polynomials

ここではヤング図形, 半標準盤, Schur 多項式について復習をする.

3.1 半標準盤

m を正整数とする. 整数 m の n 個の分割 $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ に対して, $m_j(\lambda) := \#\{i \mid \lambda_i = j\}$ とおき, これを重複度という. 今後 λ とヤング図形は同一視する. 写像 $T: \lambda \rightarrow [n]$ が以下の条件を満たすとき, T を λ の半標準盤と呼ぶ:

- $T_{i,j} \leq T_{i,j'}$ for $(i,j), (i,j') \in \lambda$ with $j < j'$,
- $T_{i,j} < T_{i',j}$ for $(i,j), (i',j) \in \lambda$ with $i < i'$.

$\text{SST}_n(\lambda)$ を λ の $[n]$ に関する半標準盤全体の集合とする.

例 3.1. $\text{SST}_3((3,1,0))$ は以下の 15 個の集合からなる.

$$\text{SST}_3((3,1,0)) = \left\{ \begin{array}{c} \boxed{111} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{111} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{112} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{112} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{113} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{113} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{122} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{122} \\ \boxed{3} \end{array}, \right. \\ \left. \begin{array}{c} \boxed{123} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{123} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{133} \\ \boxed{2} \end{array}, \begin{array}{c} \boxed{133} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{222} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{223} \\ \boxed{3} \end{array}, \begin{array}{c} \boxed{233} \\ \boxed{3} \end{array} \right\}$$

3.2 Schur 多項式

$\mathbf{x} = \{x_1, x_2, \dots, x_n\}$ を変数の集合とし, $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ に対して \mathbf{x} の交代式 a_λ を

$$a_\lambda = \det(x_i^{\lambda_j})$$

で定義する. 特に $\delta = (n-1, n-2, \dots, 0)$ のときは a_δ は Vandermonde の行列式になる. $\lambda + \delta := (\lambda_1 + n - 1, \lambda_2 + n - 2, \dots, \lambda_n)$ とおき,

$$s_\lambda := \frac{a_{\lambda+\delta}}{a_\delta}$$

とすることで s_λ は \mathbf{x} の対称多項式となる. これを *Schur 多項式* と呼ぶ.

Schur 多項式は半標準盤を用いて表示できることが知られている. $T \in \text{SST}_n(\lambda)$ に対して, $\mathbf{x}^T := \prod_{i=1}^n x_i^{\#T^{-1}(i)}$ とおく.

事実 3.2 ([8]). $s_\lambda(\mathbf{x}) = \sum_{T \in \text{SST}_n(\lambda)} \mathbf{x}^T$ である.

例 3.3. 例 3.1 により, 次を得る.

$$\begin{aligned} s_{(3,1,0)}(x_1, x_2, x_3) &= x_1^3 x_2 + x_1^3 x_3 + x_1^2 x_2^2 + x_1^2 x_2 x_3 + x_1^2 x_2 x_3 + x_1 x_2^3 + x_1 x_2^2 x_3 \\ &\quad + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 + x_1 x_2 x_3^2 + x_1 x_3^3 + x_2^3 x_3 + x_2^2 x_3^2 + x_2 x_3^3 \\ &= \sum_{i,j} x_i^3 x_j + \sum_{i,j} x_i^2 x_j^2 + 2 \sum_{i,j,k} x_i^2 x_j x_k. \end{aligned}$$

4 再生核

4.1 再生核の定義

ここでは簡単のために, コンパクト群 G (有限群も含む) とその閉部分群 K に限った話を行う. より詳しい話は Bekka-de la Harpe-Grigorchuk [2] を見ていただきたい. $X = G/K$ とおき, μ を X 上のコンパクト台を持つ正の G 不変測度, π をヒルベルト空間を $L^2(X, \mu)$ とする G の標準的なユニタリー表現とする.

π 中の既約表現 \mathcal{H} を一つ固定し, $\mathcal{H}^K := \{\psi \in \mathcal{H} \mid \pi(k)\psi = \psi \text{ for all } k \in K\}$ とおく. さらに今 $\dim_{\mathbb{C}} \mathcal{H}^K = 1$ という仮定もつけておく. なお, (G, K) が対称対で \mathcal{H} が既約表現であるときは上の性質を満たすことが知られている.

\mathcal{H} に以下のような標準的な内積を定義する:

$$\langle \phi \mid \chi \rangle := \int_X \phi(x) \overline{\chi(x)} d\mu.$$

このとき Riesz の表現定理より各 $x \in X$ に対して次の条件を満たす関数 $\varphi_x \in \mathcal{H}$ がただ一つ存在する: 各 $\phi \in \mathcal{H}$ に対して, $\phi(x) = \langle \phi \mid \varphi_x \rangle$. 再生核 $\Phi: X \times X \rightarrow \mathbb{C}$ を $\Phi(x, y) := \langle \varphi_y \mid \varphi_x \rangle = \varphi_y(x)$ により定める. このとき定義から Φ は次の性質を持つことがわかる.

$$\phi(x) = \langle \phi \mid \Phi(\cdot, x) \rangle \text{ for all } \phi \in \mathcal{H} \text{ and } x \in X. \quad (1)$$

\mathcal{H}^K の中から単位ベクトル ξ を一つ選び固定する. \mathcal{H} の帯球関数 $f: G \rightarrow \mathbb{C}$ を

$$f(g) = \langle \pi(g)\xi \mid \xi \rangle;$$

により定義する. このとき f は両側 K 不変関数となる. $\omega \in X$ を標準的な基点とする. つまり $X = G/K$ と見たとき, $\omega = K$ ということである. 再生核と帯球関数には次の関係がある.

命題 4.1 ([2]).

$$\Phi(g\omega, g'\omega) = \frac{\dim_{\mathbb{C}} \mathcal{H}}{\mu(X)} f(g^{-1}g') \quad \text{and} \quad \xi(g\omega) = \sqrt{\frac{\dim_{\mathbb{C}} \mathcal{H}}{\mu(X)}} f(g^{-1})$$

for all $g, g' \in G$.

4.2 Hamming cubes

X を 2 元集合 $\{1, -1\}$ の n 回直積集合とする. *Hamming cube* $Q_n = (X, E)$ を以下のようなグラフとして定義する: 頂点集合は X とし, 2 頂点 $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in X$ の隣接関係 E を

$$(x, y) \in E \Leftrightarrow \#\{i \mid x_i \neq y_i\} = 1$$

により定める. ∂ を Q_n の path-distance とするとき, $\partial(x, y) = j$ と $\#\{i \mid x_i \neq y_i\} = j$ が同値であることはよく知られている.

次に Q_n の調和解析について考える. Q_n には対称群 S_2 と S_n の wreath 積が推移的に作用しており, 4.1 節の枠組みにおいて, $(G, K) = (S_2 \wr S_n, S_n)$ と表せる. 以下で $L^2(Q_n)$ の $S_2 \wr S_n$ による既約表現分解を直接与える. $C(X)$ を X 上の \mathbb{C} 値関数からなるベクトル空間とする. $C(X)$ に標準的な内積を

$$(f, g) = \frac{1}{2^n} \sum_{x \in X} f(x) \overline{g(x)} \text{ for } f, g \in C(X).$$

により定める. なお, X は有限集合で測度は point mass を考えるので $L^2(Q_n)$ は $C(X)$ のまま表すことにする. 各 $i = 1, 2, \dots, n$ に対して, $\varepsilon_i \in C(X)$ を x の i 成分の射影とする. すなわち $\varepsilon_i(x_1, x_2, \dots, x_n) = x_i$ とする. また各 $\alpha \in 2^{[n]}$ に対して

$$\varepsilon_\alpha := \prod_{i \in \alpha} \varepsilon_i.$$

とする. このとき直接計算により $\{\varepsilon_\alpha\}_{\alpha \in 2^{[n]}}$ は $C(X)$ の正規直交基底であることが確かめられる. 各 $j = 1, 2, \dots, n$ に対して, $V_j := \text{Span}_{\mathbb{C}}\{\varepsilon_\alpha \mid \#\alpha = j\}$ とおく. すると $\dim V_j = \binom{n}{j}$, $C(X) = \bigoplus_{j=0}^n V_j$ が成り立つ. $\Phi_j: X \times X \rightarrow \mathbb{C}$ を V_j の再生核とする. このとき $\partial(x, y) = u$ である $x, y \in X$ に対して

$$\Phi_j(x, y) = \sum_{k=0}^{\min\{u, j\}} (-1)^k \binom{u}{k} \binom{n-u}{j-k}$$

であることがわかる. この右辺を変数 u に関する *Krawtchouk* 多項式と呼び, 今後 $K_j(u)$ で表す.

4.3 ユニタリー群

$U(n)$ はコンパクトリー群であり, その既約表現はよく研究されている. ここでは詳しく述べないが最高ウェイト理論により, $U(n)$ の既約表現の同値類の集合 $\widehat{U(n)}$ は $\lambda \in (\mathbb{Z}^n)_+$ と一対一対応がついている. また Weyl の次元公式により index が $\lambda \in (\mathbb{Z}^n)_+$ の既約表現 V_λ の次元は

$$\dim_{\mathbb{C}} V_\lambda = \prod_{1 \leq i < j \leq n} \frac{\lambda_i - \lambda_j + j - i}{j - i}. \quad (2)$$

であることが知られている. この計算例として, $\lambda = (1^\ell) := (\underbrace{1, \dots, 1}_\ell, \underbrace{0, \dots, 0}_{n-\ell})$

のときは $\dim_{\mathbb{C}} V_\lambda = \binom{n}{\ell}$ となる.

$U(n)$ には直積群 $U(n) \times U(n)$ が自然に作用し, それにより $C(U(n))$ を $U(n) \times U(n)$ の (無限次元) 表現とみなすことができる. ここで各 $\lambda \in (\mathbb{Z}^n)_+$ について, $V_\lambda \boxtimes V_\lambda^\vee$ は $U(n) \times U(n)$ の既約表現となる. ただし, V_λ^\vee は V_λ の反傾表現とする. \mathcal{H}_λ を $V_\lambda \boxtimes V_\lambda^\vee$ と同型な $C(U(n))$ の部分表現とする. Peter-Weyl の定理により, そのような空間は一意に定まり, かつ

$$C(U(n)) \underset{\text{dense}}{\supset} \bigoplus_{\lambda \in (\mathbb{Z}^n)_+} \mathcal{H}_\lambda$$

が成り立つ.

各 $\lambda \in (\mathbb{Z}^n)_+$ に対して $\Phi_\lambda: U(n) \times U(n) \rightarrow \mathbb{C}$ を \mathcal{H}_λ の再生核とする. このとき帯球関数 f は既約表現 π_λ を用いて

$$f_\lambda(g_1, g_2) = \pi_\lambda(t_1, t_2, \dots, t_n),$$

と書けることが知られている. ここで t_1, t_2, \dots, t_n は $g_1^{-1}g_2$ の固有値である. したがって

$$\Phi_\lambda(g_1, g_2) = \dim_{\mathbb{C}} \mathcal{H}_\lambda f_\lambda(g_1^{-1}g_2) \quad (3)$$

を得る.

5 主結果

定義 5.1. $\lambda \in (\mathbb{Z}^n)_+$ を一つ固定する. このとき $U(n)$ の有限部分集合 X が λ -design であるとは以下を満たすこと:

$$\int_{U(n)} f d\mu = \frac{1}{\#X} \sum_{x \in X} f(x)$$

for any $f \in \mathcal{H}_\lambda$. なお μ は $U(n)$ 上の正規化した Haar 測度である.

Remark 5.2. $\lambda = (0, \dots, 0)$ のときは $\mathcal{H}_{(0, \dots, 0)}$ は $U(n)$ 上の定数関数からなる集合となるので, $U(n)$ の任意の有限部分集合は $(0, \dots, 0)$ -design である.

再生核や Schur 多項式を用いた λ -design の同値条件が知られている. 以下でそれを紹介する.

命題 5.3. $\lambda \in (\mathbb{Z}^n)_+$ with $\lambda \neq (0, \dots, 0)$ を一つ固定する. $U(n)$ の有限部分集合 X に対して以下は同値:

(1) X は λ -design.

(2) X は以下を満たす.

$$\sum_{x, y \in X} K_\lambda(x, y) = 0.$$

(3) X は以下を満たす.

$$\sum_{x \in X} \pi_\lambda(x) = 0.$$

$\lambda \in (\mathbb{Z}^n)_+$ と $k \in \mathbb{Z}$ に対して, $\lambda + 2k := (\lambda_1 + 2k, \dots, \lambda_n + 2k) \in (\mathbb{Z}^n)_+$ とおく. このとき次が成り立つ.

補題 5.4. $\lambda \in (\mathbb{Z}^n)_+$ と $k \in \mathbb{Z}$ と大対蹠集合の任意の要素 $x \in S$ に対して,

$$s_{\lambda+2k}(x) = s_\lambda(x)$$

が成り立つ. したがって大対蹠集合 S が λ -design ならば, S は $\lambda + 2k$ -design でもある.

Proof. $x = (\epsilon_1, \epsilon_2, \dots, \epsilon_n)$, $\epsilon_i = \pm 1$ とするとき,

$$\begin{aligned}
s_{\lambda+2k}(x) &= \frac{a_{\lambda+\delta+2k}(x)}{a_{\delta}(x)} \\
&= \frac{1}{a_{\delta}(x)} \begin{vmatrix} \epsilon_1^{\lambda_1+n-1+2k} & \epsilon_2^{\lambda_1+n-1+2k} & \dots & \epsilon_n^{\lambda_1+n-1+2k} \\ \epsilon_1^{\lambda_2+n-2+2k} & \epsilon_2^{\lambda_2+n-2+2k} & \dots & \epsilon_n^{\lambda_2+n-2+2k} \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_1^{\lambda_n+2k} & \epsilon_2^{\lambda_n+2k} & \dots & \epsilon_n^{\lambda_n+2k} \end{vmatrix} \\
&= \epsilon_1^{2k} \epsilon_2^{2k} \dots \epsilon_n^{2k} \frac{1}{a_{\delta}(x)} \begin{vmatrix} \epsilon_1^{\lambda_1+n-1} & \epsilon_2^{\lambda_1+n-1} & \dots & \epsilon_n^{\lambda_1+n-1} \\ \epsilon_1^{\lambda_2+n-2} & \epsilon_2^{\lambda_2+n-2} & \dots & \epsilon_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_1^{\lambda_n} & \epsilon_2^{\lambda_n} & \dots & \epsilon_n^{\lambda_n} \end{vmatrix} \\
&= \epsilon_1^{2k} \epsilon_2^{2k} \dots \epsilon_n^{2k} \frac{a_{\lambda+\delta}(x)}{a_{\delta}(x)} \\
&= s_{\lambda}(x).
\end{aligned}$$

であることから従う. \square

$(\mathbb{Z}^n)_+$ に以下のような同値関係を入れる :

$$\lambda \sim \lambda' \Leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } \lambda' = \lambda + 2k$$

$[\lambda]$ を上で入れた同値関係による λ を含む同値類とする. 補題 5.4 より, 大対蹠集合に対しては $[\lambda]$ -design を定義することができる. 一方で, $[(\lambda_1, \lambda_2, \dots, \lambda_n)]$ の偶奇を代表元 λ の成分の総和 $\sum_i \lambda_i$ により定める. これは明らかに well-defined である. また $[\lambda]$ に対して, $\lambda_n = 0, 1$ となる $(\lambda_i) \in [\lambda]$ がただ一つ定まる. 今後はこれを λ_{rep} と表す.

補題 5.5. $(0, \dots, 0) \notin [\lambda]$ である $[\lambda]$ を一つ固定する. $\lambda_{\text{rep}} \in [\lambda]$ と大対蹠集合 S に関して次は同値 :

- (1) S は $[\lambda]$ -design,
- (2) 各 $T \in \text{SST}_n(\lambda_{\text{rep}})$ with weight $w(T) := (\mu_1, \mu_2, \dots, \mu_n)$ に対して, μ_i が奇数となる $i = 1, 2, \dots, n$ が存在する.

この証明は SST を用いた Schur 多項式と S の定義より容易に従う.

これから大対蹠集合が何 design なのかについて言及する. まずは Hamming cube の再生核との関係を調べることで特定の λ が大対蹠集合と相性が良いことを見ていく. $(1^j) := (1, 1, \dots, 1, 0, 0, \dots, 0) \in (\mathbb{Z}^n)_+$ に対して, $K_{(1^j)}$ を $\mathcal{H}_{(1^j)}$ の再生核とする. このとき, $\text{dist}(x_1, y_1) = \text{dist}(x_2, y_2)$ ならば, $K_{(1^j)}(x_1, y_1) = K_{(1^j)}(x_2, y_2)$ であることに注意する (なおこの性質は一般の λ に対しても成り立つ).

定理 5.6. $K_{(1^j)}$ の定義域を $S \times S$ に制限すると, $K_{(1^j)}|_{S \times S}$ は *Hamming cube* の再生核 K_j と一致する. すなわち, $\text{dist}(x, y) = n - u$ である $x, y \in S$ に対して, $K_{(1^j)}(x, y) = K_j(x, y) = K_j(u)$ (*Krawtchouk poly.*) が成り立つ.

Proof. $K_{(1^j)}(x, y)$ を直接計算することで得られる. □

Hamming cube の再生核の性質より容易に次の結果を得る.

系 5.7. 大対蹠集合 S は $[(1^j)]$ -*design* である.

次に $[\lambda]$ の偶奇に注目して大対蹠集合が何 *design* なのかを述べる.

補題 5.8. $U(n)$ 上の大対蹠集合 S に対して次が成り立つ.

(1) $[\lambda]$ が奇数ならば, S は $[\lambda]$ -*design* である.

(2) S が $[\lambda]$ -*design* となる偶数の $[\lambda]$ は高々有限個しかない.

Proof. (1) $[\lambda]$ が奇数ならば, $\sum_i \lambda_i = \sum_i \mu_i$ より必ず奇数の μ_i が存在する. したがって補題 5.5 から S は $[\lambda]$ -*design* であることを得る.

(2) n による帰納法で証明をするが冗長であるためこの報告書においては省略する. □

以下では小さい n に対して, S が $[\lambda]$ -*design* となる偶数 $[\lambda]$ を分類した結果を記載する. なお $n \geq 5$ 以上では計算機を用いて分類した.

例 5.9. 各 n に対して, $U(n)$ 上の大対蹠集合 S が $[\lambda]$ -*design* となる偶数 $[\lambda]$ は以下の通りである.

n	$[\lambda]$
2	$[(1, 1)]$ (1 class)
3	$[(1, 1, 0)], [(2, 1, 1)]$ (2 classes)
4	$[(1, 1, 0, 0)], [(2, 1, 1, 0)], [(1, 1, 1, 1)], [(3, 1, 1, 1)], [(2, 2, 1, 1)], [(3, 3, 3, 1)]$ (6 classes)
5	$[(1, 1, 0, 0, 0)], [(2, 1, 1, 0, 0)], [(1, 1, 1, 1, 0)], [(3, 1, 1, 1, 0)], [(2, 2, 1, 1, 0)], [(3, 3, 3, 3, 0)], [(2, 1, 1, 1, 1)], [(4, 1, 1, 1, 1)], [(3, 2, 1, 1, 1)], [(2, 2, 2, 1, 1)], [(3, 3, 3, 2, 1)], [(4, 3, 3, 3, 1)]$ (12 classes)
6	(26 classes)
7	(48 classes)
8	(91 classes)
9	(158 classes)

問い 5.10. 1, 2, 6, 12, 26, 48, 91, 158, ... という数列に何か意味はあるか. なお *OEIS* に似たような数列が存在するが完全に一致してはいない. (cf. *OEIS* A246584, number of overcubic partitions of n ; 1, 2, 6, 12, 26, 48, 92, 160, ...)

参考文献

- [1] C. Bachoc, R. Coulangéon and G. Nebe. *Designs in Grassmannian spaces and lattices*. J. Algebraic Combin., **16**(1):5–19, 2002.
- [2] Mohammed E. B. Bekka, P. de la Harpe, Pierre and R. Grigorchuk. *Irreducibility of unitary group representations and reproducing kernels Hilbert spaces*. Expositiones Mathematicae, **21**(2):115–149, 2003.
- [3] B.-Y. Chen and T. Nagano. *A Riemannian Geometric Invariant and its Applications to a Problem of Borel and Serre*. Trans. Amer. Math. Soc., **308**(1):273–297, 1988.
- [4] P. Delsarte, J.M. Goethals, and J.J. Seidel. *Spherical codes and designs*. Geom. Dedicata, **6**(3):363–388, 1977.
- [5] J. Faraut, S. Kaneyuki, A. Korányi, Q. Lu and G. Roos. *Analysis and Geometry on Complex Homogeneous Domains*. Progress in Mathematics, **185**, Birkhäuser, 2000.
- [6] H. Kurihara and T. Okuda. *Hermite 対称空間の大対蹠集合におけるアソシエーションスキーム構造*. 数理解析研究所講究録, **2053**:54–63, 2017.
- [7] T. Nagano. *Transformation groups on compact symmetric spaces*. Trans. Amer. Math. Soc, **118**:428–453, 1965.
- [8] B.E. Sagan. *The symmetric group —Representations, combinatorial algorithms, and symmetric functions—*. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1991.
- [9] C.U. Sánchez. *The index number of an R-space: an extension of a result of M. Takeuchi's*. Proc. Amer. Math. Soc., **125**(3):893–900, 1997.
- [10] M. Takeuchi. *Cell decompositions and Morse equalities on certain symmetric spaces*. J. Fac. Sci., Univ. Tokyo, , **Sect. I 12**:81–191, 1965.
- [11] M. Takeuchi. *Modern spherical functions*. Translations of Mathematical Monographs [Translated from the 1975 Japanese original by Toshinobu Nagura], **135**, American Mathematical Society, 1994.
- [12] M. Takeuchi. *Two-number of symmetric R-spaces*. Nagoya Math. J., **115**:43–46, 1989.
- [13] M.S. Tanaka and H. Tasaki. *Antipodal sets of symmetric R-spaces*. Osaka J. Math, **50**(1):161–169, 2013.

調和解析的視点からの有限群の部分集合による近似

広島大学理学研究科専攻修士2年

梶浦 大起 (hikajiura@hiroshima-u.ac.jp)

0 記号のお約束

G を有限群, $X \subset G$ (構造には頓着しないことに注意), $f \in \mathbb{C}^G$, χ_ρ を表現 ρ に対応する指標, \widehat{G} を G の既約表現の共役類全体, 1_G は (既約な) 自明表現とする。

1 本講演の問題と予備知識

最初に, 標語的な形で本講演で紹介する問題とその (部分的な) 答えを述べる:

本講演の問題と答え

問題 G 上の平均を X 上の平均で近似するとき, G の近似しやすさを決定する G の性質は何か?

答え X の近似の上手さに関する尺度をひとつ定義し, 次のような性質を満たすことを示した:
共役類が多い G は近似しやすい。

もう少し詳細に問題を述べる。 G 上の平均 $\mu(f; G)$ と X 上の平均 $\mu(f; X)$ は次で定義される:

$$\mu(f; G) := \frac{1}{\#G} \sum_{x \in G} f(x), \quad \mu(f; X) := \frac{1}{\#X} \sum_{x \in X} f(x).$$

このとき, $\mu(f; G)$ を $\mu(f; X)$ で近似するときの誤差, すなわち

$$\text{Error}(f; X) := |\mu(f; G) - \mu(f; X)|$$

がより小さくなるのはどのような群 G か? という問題である。

$\text{Error}(f; X)$ は f と X どちらにも依存するため, 誤差にどれくらい X の近似の上手さが寄与するかを考えることが難しい。そこで, 少々技巧的であるが, Peter-Weyl の定理による分解 $f = \sum_{\rho \in \widehat{G}} f_\rho$ を考え, 自明表現に対応する部分*1以外の L^2 -ノルムの和 $\|f\|_{\widehat{G}}$ を f の尺度とする*2。

このとき, 次の定理から我々は X の近似の上手さに関する尺度をひとつ定義することができる:

結果 1 (有限群上の Koksma-Hlawka 型不等式) $f \in \mathbb{C}^G$ と $X \subset G$ について, 次の不等式が成り立つ:

$$\text{Error}(f; X) \leq \|f\|_{\widehat{G}} \mathfrak{d}(X).$$

ここで, $\|f\|_{\widehat{G}}$ と $\mathfrak{d}(X)$ は次で定義される:

$$\|f\|_{\widehat{G}} := \sum_{\substack{\rho \in \widehat{G} \\ \rho \neq 1_G}} \|f_\rho\|, \quad \mathfrak{d}(X) := \max_{\substack{\rho \in \widehat{G} \\ \rho \neq 1_G}} \sqrt{\frac{\dim \rho}{\#X^2} \sum_{x, y \in X} \chi_\rho(xy^{-1})}.$$

また, f_ρ は f の Peter-Weyl の定理による分解 $f = \sum_{\rho \in \widehat{G}} f_\rho$ とする。

この結果から, 本講演では「 G を上手く近似できる X 」とは「同濃度の部分集合の中で $\mathfrak{d}(X)$ が最小になるもの」であると考え, その尺度を使って G を上手く近似できる X を調べる。

*1 すなわち, 定数関数部分であり, $\mu(f; G)$ と一致する。

*2 これは f の「変動」のようなものがどれくらい大きいかということを表すような尺度であると思える。

2 本講演の背景

ここでは、Koksma-Hlawka 型不等式を示した背景について述べる。まず最初に、区間 $[0, 1]^s$ 上の“よい”実函数空間 H (少なくとも、可積分は要求されているものとする) における Monte Carlo 積分を以下で定義する:

定義 2 (Monte Carlo 積分) $f \in H$ について、 f の Monte Carlo 積分 $I(f)$ は次で定義される:

$$I_X(f) := \sum_{x \in X} f(x)$$

ここで、 X は $[0, 1]^s$ 上で“ランダムに選んだ”点集合である。

この Monte Carlo 積分はシミュレーション等で様々な工学領域に応用されている。Monte Carlo 積分の収束の速さについて、次のような定理が一般に知られている:

結果 3 (Monte Carlo 積分の収束の速さ [2]) $\left| \int_{[0,1]^2} f(x) dx - I_X(f) \right| = O(\#X^{-1/2})$

これはつまり“ランダムに選んだ”場合は、真の積分値との誤差について 1 桁増やすためには 100 倍の点集合が必要であるということである。これは実用上大きな痛手となりやすい。そのため、quasi-Monte Carlo では、“ランダムに選ぶ”のではなく、 H の元に都合が良い点集合を決定論的に選ぶことでより高速な収束を実現することを研究している。

そこで知られている古典的な定理として Koksma-Hlawka の不等式がある:

結果 4 (Koksma-Hlawka の不等式 [1]) H を区間 $[0, 1]$ 上の“全変動有界”な関数のなす空間とする。また、 $X \subset [0, 1]$ を有限部分集合としたとき、任意の $f \in H$ に対して、

$$\left| \int_{[0,1]^2} f(x) dx - I_X \right| \leq V(f) D^*(X)$$

ここで、 $V(f)$ は f の“全変動”とし、 $D^*(X)$ は star-Discrepancy と呼ばれる X に関する尺度である。

この定理に関して、充分濃度が大きな X について、 $D^*(X) = O((\log \#X)^s / \#X)$ を満たす点列 (すなわち、“ランダムに選ぶ”よりちょっとだけ効率の良い点列) の構成法などが示されている [1]。さらに H を再生核 Hilbert 空間などに限定することで、再生核を用いてより tight な Koksma-Hlawka 型の不等式を示すことなども研究されている [2]。

3 近似しやすい G の性質について

$\mathfrak{d}(X)$ の下限について次のような定理がある:

定理 5 $X \subset G$ について次の不等式が成り立つ:

$$\mathfrak{d}(X) \geq \sqrt{\frac{\#G - \#X}{\#X^2(C-1)}}.$$

ここで、 C は G の共役類の個数である。また、等号成立は各 $\rho \in \hat{G}$ で $\sum_{x,y \in X} \chi_\rho(xy^{-1})$ が一致するときに限る。

この定理は有限群 G そのものに関する「 G の近似しやすさ」みたいなものを理解する不等式とも思える。具体的にいうと、 G の共役類が多ければ多いほど $\mathfrak{d}(X)$ の下限が小さくなり、 $\mathfrak{d}(X)$ がより小さい X (つまり、上手に近似できる X) が存在する可能性があるということがわかる。実験的にも \mathfrak{S}_3 と $\mathbb{Z}/3\mathbb{Z}$ では $\mathbb{Z}/3\mathbb{Z}$ の方がより近似しやすい (つまり、同濃度では $\mathfrak{d}(X)$ が小さくなることが多い) ことを示した。

参考文献

- [1] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, Society for Industrial and Applied Mathematics (SIAM), 1992.
- [2] J. Dick and F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, 2010.

Quantum walks on finite graphs with infinite inflow

Mohamed Sabri¹, Yusuke Higuchi², Etsuo Segawa³, and Yusuke Yoshie¹

¹Graduate School of Information Sciences, Tohoku University, Aoba, Sendai 980-8579, Japan.

²Mathematics Laboratories, College of Arts and Sciences, Showa University 4562
Kamiyoshida, Fujiyoshida, Yamanashi 403-005, Japan.

³Graduate School Education Center, Yokohama National University, Japan.

1 Introduction

Quantum walks are the quantum version of classical random walks. There have been many studies about different kinds of quantum walks for years while one of them is "Grover walks", a widely studied quantum walk. For example the Grover walk on a connected graph from the view point of an application to graph isomorphism problem was studied by Emms, Hancock, Severeni and Wilson [4] in the year 2006 and it has been very useful in several practical applications such as the study of quantum search algorithms [5].

A tailed quantum walk model is introduced and studied by Feldman and Hillery [1] [2]. In these papers the authors suggest the study of l^∞ space which is used in studying the resonant-tunneling phenomenon of quantum walks by Matsue, Matsuoka, Ogurusu and Segawa [6]

In this paper, we restrict our discussion into the tailed model of the Grover walk and we extend the model into a walk with several tails connected to a finite graph. In section 2, we introduce our model and some known results in the model, where in section 3 we discuss the walk on hypercubes and in section 4 we extend our results to distance regular graphs.

Let $G = (V, E)$ be a connected graph, A be the set of arcs induced by E . For any $a \in A$, we denote the inverse arc of a by \bar{a} , origin of a by $o(a)$ and the terminal of a by $t(a)$. We have that $o(\bar{a}) = t(a), t(\bar{a}) = o(a) \in A$. The state space of the Grover walk is generated by the arc set A induced by the set of edges E .

Definition 1 *The dynamics of the Grover walk is defined by the unitary operator U on A defined as follows.*

$$U_{ab} = \begin{cases} \frac{2}{deg(t(b))} - \delta_{\bar{a}\bar{b}} & \text{if } o(a) = t(b) \\ 0 & \text{otherwise} \end{cases} \quad \forall a, b \in A$$

where $deg(u)$ is the degree of the vertex u in G .

Let ψ_n be the state of the walker at time step n . Then we have the following.

$$\forall n \in \mathbb{Z}^+, \psi_n = U\psi_{n-1}$$

It follows that for any given initial state ψ_0 , we have the following.

$$\forall n \in \mathbb{Z}_0^+, \psi_n = U^n\psi_0$$

By the above definition, we have the following expression. For any $l^2(A)$,

$$(U\psi_n)(a) = \sum_{b:t(b)=o(a)} \left(\frac{2}{deg(t(b))} - \delta_{\bar{a}\bar{b}} \right) \psi_{n-1}(b) \quad (1)$$

In general, the above mentioned Grover walk on a finite graph does not converge to a stationary state because U is unitary and hence the spectrum of U lies on the unit circle. We modify the walk in a way that the walk converges to a stationary state.

2 Tailed Grover model on Graphs

Let $G_0 = (V_0, E_0)$ be a finite connected graph and A_0 be the arc set induced by E_0 . We join a semi-infinite length path, called the input tail, by the vertex at the finite end to an arbitrary vertex in G_0 . We denote this path by \mathbb{P}_+ and the common vertex by u_+ . i.e. $u_+ \in V_0 \cap V(\mathbb{P}_+)$ where $V(\mathbb{P}_+)$ is the vertex set of \mathbb{P}_+ . Other than this input tail, we join semi-infinite paths, called the output tails, to the chosen vertices in G_0 .

Let $\tilde{G} = (\tilde{V}, \tilde{E})$ be the total graph we get by joining the infinite tails to G_0 and \tilde{A} be the arc set induced by \tilde{E} . Let $v_0 = u_+$, $v_1 \in V(\mathbb{P}_+)$ such that v_1 is adjacent to v_0 , $v_2 \in V(\mathbb{P}_+)$ such that v_2 is adjacent to v_1 and so on. We set the initial state $\tilde{\psi}_0$ defined on \tilde{A} as follows. For any $a \in \tilde{A}$

$$\tilde{\psi}_0(a) = \begin{cases} 1 & \text{if } o(a) = v_n \text{ and } t(a) = v_{n-1} \text{ for some } n \\ 0 & \text{otherwise} \end{cases}$$

This initial state provides a continuous constant input to the graph throughout each time step through the input tail \mathbb{P}_+ . We study the dynamics of this walk in various classes of graphs with the various configurations of output tails as well as the walk in a general graph. In this study, the following are known by the forthcoming paper [3].

Theorem 1

1.

$$\lim_{n \rightarrow \infty} U^n \tilde{\psi}_0 = \exists \psi_\infty$$

2. If $\delta V \subset V_0$ be the set of vertices connected to tails. Then $\forall a \in \tilde{A}$, $\psi_\infty(a) + \psi_\infty(\bar{a}) = \frac{2}{|\delta V|}$

Remark that the stationary state ψ_∞ satisfies the condition, $U\psi_\infty = \psi_\infty$. In particular, by equation (1) we have the following expression.

$$(U\psi_\infty)(a) = \sum_{b:t(b)=o(a)} \left(\frac{2}{\deg(t(b))} - \delta_{a\bar{b}} \right) \psi_\infty(b) \quad (2)$$

3 Tailed Grover model on Hypercubes

We denote the d -hypercube by $H(d, 2)$ in terms of the Hamming graph. We know that $H(d, 2)$ is d -regular and has the diameter d . Moreover it is a distance regular graph and has a high symmetry. We use these facts to compute the stationary distribution in some special cases.

We use the following notation to study the walk when $G_0 = H(d, 2)$.

For given $j \in \mathbb{Z}$ such that $0 \leq j \leq d$,

$$\Gamma_j = \{v \in V_0 : \text{dist}(v, u_+) = j\}$$

It is clear that $|\Gamma_j| = \binom{d}{j}$. Also we can state that, for given $v \in \Gamma_j$ with $j > 0$, $|\{w \in \Gamma_{j-1} : w \sim v\}| = j$ and for given $v \in \Gamma_j$ with $j < d$, $|\{w \in \Gamma_{j+1} : w \sim v\}| = d - j$. To make our study simple, we join the output tails to $H(d, 2)$ in a way that the symmetry is preserved. i.e. for a given j , $\psi_\infty(a)$ and $\psi_\infty(\bar{a})$ are invariant for any $a \in A_0$ such that $o(a) \in \Gamma_j$ and $t(a) \in \Gamma_{j+1}$. In the remaining sections of this paper, we denote $\psi_\infty(a)$ and $\psi_\infty(\bar{a})$ such that $o(a) \in \Gamma_j$ and $t(a) \in \Gamma_{j+1}$ by $q_{j,j+1}$ and $q_{j+1,j}$ respectively.

In this paper we give the stationary state explicitly in the following cases.

1. When the tails are connected to Γ_0 and Γ_d (Lemma 1)
2. When the tails are connected to all the vertices in A_0 (Lemma 2)
3. When the tails are connected to $\Gamma_0, \Gamma_r, \Gamma_{r+1}, \dots, \Gamma_d$ (Lemma 3)
4. When the tails are connected to $\Gamma_0 = \Gamma_{J_0}, \Gamma_{J_1}, \Gamma_{J_2}, \dots, \Gamma_{J_m} \leq \Gamma_d$ (Theorem 2)

Remark that case 4 contains all the cases above. So we will show these step by step.

3.1 Tails on Γ_0 and Γ_d

In this model we add an output tail to the vertex in Γ_d preserving the symmetricity. Then we have the following lemma.

Lemma 1 For $0 \leq j < d$,

$$q_{j,j+1} = \frac{1}{2} \left\{ 1 + \frac{1}{(d-j) \binom{d}{j}} \right\}$$

and

$$q_{j+1,j} = \frac{1}{2} \left\{ 1 - \frac{1}{(d-j) \binom{d}{j}} \right\}$$

Proof of Lemma 1

Let $1 \leq j < d$. Then by a combinatorial argument on equation (2), the following holds.

$$q_{j+1} = \frac{2}{d} j q_{j-1,j} + \frac{2}{d} (d-j-1) q_{j+1,j} + \left(\frac{2}{d} - 1 \right) q_{j+1,j} \quad (3)$$

Also in this case, we obtain that $q_{j,j+1} + q_{j+1,j} = 1$. Then, by equation (3), it follows that,

$$q_{j,j+1} = \frac{2j q_{j-1,j} + d - 2j}{2(d-j)}.$$

Let $f(j) := q_{j,j+1}$. Then we have the following recursion for $1 \leq j < d$.

$$f(j) = \frac{2j f(j-1) + d - 2j}{2(d-j)}.$$

Now consider the initial condition. By a similar combinatorial argument, the following holds.

$$q_{0,1} = \frac{2}{d+1} + \frac{2}{d+1} (d-1) q_{1,0} + \left(\frac{2}{d+1} - 1 \right) q_{1,0}.$$

Again by using the property $q_{0,1} + q_{1,0} = 1$ and simplifying, we get,

$$f(0) = q_{0,1} = \frac{1+d}{2d}.$$

We can observe that $f(j)$ is of the form,

$$f(j) = \frac{g_{j+1}(d)}{2P(d, j+1)}.$$

where $g_{j+1}(d)$ is a $j+1$ degree polynomial of d and $P(d, j+1)$ denotes the $(j+1)$ -permutations of d . Then it follows that,

$$g_{j+1}(d) = j g_j(d) + (d-2j) P(d, j).$$

By simplifying this, we get,

$$g_{j+1}(d) - P(d, j+1) = j(g_j(d) - P(d, j)).$$

Define $h_j(d) := g_j(d) - P(d, j)$, then we have,

$$h_{j+1}(d) = jh_j(d).$$

It follows that,

$$h_{j+1}(d) = j! h_1(d).$$

From $f(0)$, we have $g_1(d) = d + 1$, hence $h_1(d) = 1$, which follows that $h_{j+1}(d) = j!$. So we have the expression for $g_{j+1}(d)$ as follows,

$$g_{j+1}(d) = j! + P(d, j+1).$$

Then $f(j)$ becomes,

$$f(j) = \frac{j! + P(d, j+1)}{2P(d, j+1)}.$$

By simplifying this, we get,

$$f(j) = \frac{1}{2} \left\{ 1 + \frac{1}{(d-j) \binom{d}{j}} \right\}.$$

So we have the stationary states as follows,

$$q_{j,j+1} = \frac{1}{2} \left\{ 1 + \frac{1}{(d-j) \binom{d}{j}} \right\}.$$

and by using the property $q_{j,j+1} + q_{j+1,j} = 1$, for any $0 \leq j < d$, we have,

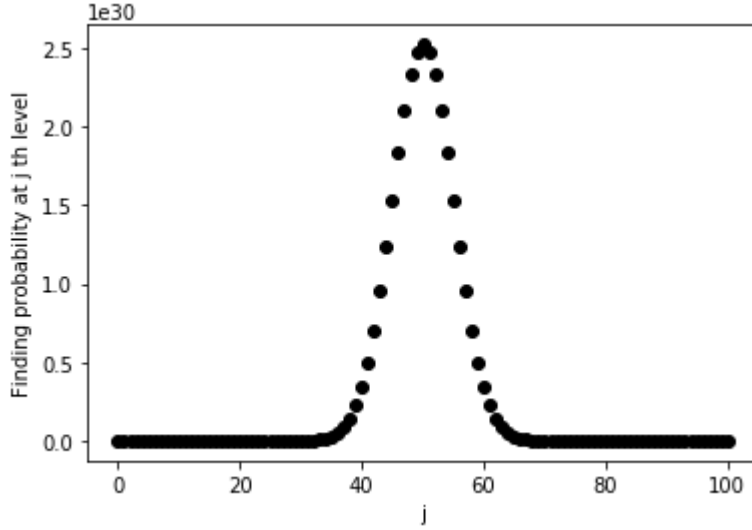
$$q_{j+1,j} = \frac{1}{2} \left\{ 1 - \frac{1}{(d-j) \binom{d}{j}} \right\}.$$

Remark 1 Note that the walk restricted to the internal graph is not unitary hence does not preserve the total probability. But the total probability converges to a constant value.

Without the normalization, we plot the shape of the relative finding probability μ_{Γ_j} of the walker at the j^{th} level as follows.

$$\mu_{\Gamma_j} = \sum_{a \in G_0: t(a) \in \Gamma_j} |\psi_\infty(a)|^2$$

For $d = 100$, the plot of μ_{Γ_j} vs j is as follows.



3.2 Tails on all the vertices

In this case, we add the output tails on all the vertices except u_+ . That is the tails including \mathbb{P}_+ are connected to all the vertices in $H(d, 2)$. It can be noted that the graph preserves the symmetricity after adding the tails. The by a similar argument, we have the following lemma.

Lemma 2 For $0 \leq j < d$

$$q_{j,j+1} = \frac{1}{2^d} \left\{ 1 + \frac{\sum_{k=j+1}^d \binom{d}{k}}{(d-j) \binom{d}{j}} \right\}$$

and

$$q_{j+1,j} = \frac{1}{2^d} \left\{ 1 - \frac{\sum_{k=j+1}^d \binom{d}{k}}{(d-j) \binom{d}{j}} \right\}$$

Proof of Lemma 2

Let $1 \leq j < d$, again by a similar combinatorial argument, we have the following.

$$q_{j,j+1} = \frac{2}{d+1} j q_{j-1,j} + \frac{2}{d+1} (d-j-1) q_{j+1,j} + \left(\frac{2}{d+1} - 1 \right) q_{j+1,j}. \quad (4)$$

In this case we have that $q_{j,j+1} + q_{j+1,j} = 2^{1-d}$. Then by equation (4), it follows that,

$$q_{j,j+1} = \frac{j q_{j-1,j} + 2^{-d} (d-2j-1)}{d-j}.$$

Defining $f(j) := q_{j,j+1}$, we have the following recursion.

$$f(j) = \frac{j f(j-1) + 2^{-d} (d-2j-1)}{d-j}.$$

Now consider the initial condition, We have the following.

$$q_{0,1} = \frac{2}{d+1} + \frac{2}{d+1} (d-1) q_{1,0} + \left(\frac{2}{d+1} - 1 \right) q_{1,0}.$$

Again by using the property $q_{j,j+1} + q_{j+1,j} = 2^{1-d}$, we have,

$$f(0) = q_{0,1} = \frac{1 + 2^{-d} (d-1)}{d}.$$

It can be observed that $f(j)$ is of the form,

$$f(j) = \frac{g_{j+1}(d)}{P(d, j+1)}.$$

It follows that $g_{j+1}(d)$ satisfies the following recursion.

$$g_{j+1}(d) = jg_j(d) + 2^{-d}(d-2j-1)P(d, j).$$

Defining $h_j := g_j(d) - 2^{-d}P(d, j)$, we have the following.

$$h_{j+1} = jh_j - 2^{-d}P(d, j).$$

Solving the above recursion, we have,

$$h_{j+1} = j!h_1 - 2^{-d}j! \sum_{k=0}^j \binom{d}{j-k} + 2^{-d}j!.$$

By the initial condition, we have $g_1(d) = 1 + 2^{-d}(d-1)$ and hence $h_1 = 1 - 2^{-d}$. It follows that,

$$h_{j+1} = j! - 2^{-d}j! \sum_{k=0}^j \binom{d}{j-k}.$$

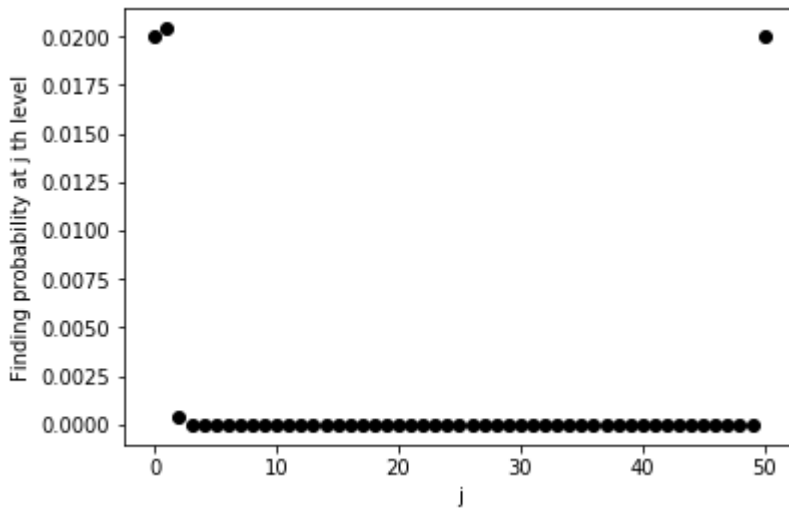
Substituting the above expression, we get the following result.

$$f(j) = q_{j,j+1} = \frac{1}{2^d} \left\{ 1 + \frac{\sum_{k=j+1}^d \binom{d}{k}}{(d-j) \binom{d}{j}} \right\}.$$

By the property $q_{j,j+1} + q_{j+1,j} = 2^{1-d}$ we have,

$$q_{j+1,j} = \frac{1}{2^d} \left\{ 1 - \frac{\sum_{k=j+1}^d \binom{d}{k}}{(d-j) \binom{d}{j}} \right\}.$$

Also in this case we plot the shape of the finding probability of the walker at j^{th} level when $d = 50$



3.3 Tails on $\Gamma_0, \Gamma_r, \Gamma_{r+1}, \dots, \Gamma_d$

In this setting, we join the output tails to all the vertices in $\Gamma_r, \Gamma_{r+1}, \dots, \Gamma_d$, preserving the symmetricity. By a similar argument, we have the following lemma.

Lemma 3 *Let $|\delta V|$ be the number of tails connected. For $0 \leq j < d$*

$$q_{j,j+1} = \begin{cases} \frac{1}{|\delta V|} \left\{ 1 + \frac{|\delta V| - 1}{(d-j) \binom{d}{j}} \right\} & \text{if } 0 \leq j < r \\ \frac{1}{|\delta V|} \left\{ 1 + \frac{|\delta V| - 1 - \sum_{k=r}^j \binom{d}{k}}{(d-j) \binom{d}{j}} \right\} & \text{if } r \leq j < d \end{cases}$$

Proof of Lemma 3

The proof follows by combining the ideas of the proofs of Lemma 1 for $0 \leq j < r$ and Lemma 2 for $r \leq j < d$.

We further generalize Lemma 3 as follows.

3.4 Tails on $\Gamma_0 = \Gamma_{J_0}, \Gamma_{J_1}, \Gamma_{J_2}, \dots, \Gamma_{J_m} \leq \Gamma_d$

In this case we generalize the walk by adding tails to all the vertices in $\Gamma_0 = \Gamma_{J_0}, \Gamma_{J_1}, \Gamma_{J_2}, \dots, \Gamma_{J_m} \leq \Gamma_d$. It can be observed that the walk is symmetric and hence we can use a similar argument to compute the stationary state explicitly. We give the following theorem for the stationary state in this case.

Theorem 2 *Let $|\delta V|$ be the number of tails connected. For $0 \leq j < d$*

$$q_{j,j+1} = \frac{1}{|\delta V|} \left\{ 1 + \frac{\text{Number of tails from } \Gamma_{j+1} \text{ to } \Gamma_d}{\text{Number of edges between } \Gamma_j \text{ and } \Gamma_{j+1}} \right\} \quad (5)$$

and

$$q_{j+1,j} = \frac{1}{|\delta V|} \left\{ 1 - \frac{\text{Number of tails from } \Gamma_{j+1} \text{ to } \Gamma_d}{\text{Number of edges between } \Gamma_j \text{ and } \Gamma_{j+1}} \right\} \quad (6)$$

Proof of Theorem 2

The proof can be done with the combination of the argument in Lemma 1 and induction on m .

We extend this theorem to any distance regular graph

4 Tailed Grover model on Distance regular graphs

Definition 2 *Let $G(V_0, E_0)$ be a distance regular graph with valancy d and diameter D . Let $u_+ \in V_0$ be the vertex to which \mathbb{P}_+ is connected. Define the equitable partitions as follows.*

For given $j \in \mathbb{Z}$ such that $0 \leq j \leq D$,

$$\Gamma_j = \{v \in V_0 : \text{dist}(v, u_+) = j\}$$

By definition of the distance regular graphs, for any given $j \in \mathbb{Z}$ such that $0 \leq j \leq D$ and $v \in \Gamma_j$, $|\{w \in \Gamma_{j-1} : w \sim v\}|$, $|\{w \in \Gamma_j : w \sim v\}|$ and $|\{w \in \Gamma_{j+1} : w \sim v\}|$ are invariant of v . We define the parameters as follows.

$$\begin{aligned} &\text{For all } 0 \leq j < D, c_j = |\{w \in \Gamma_{j-1} : w \sim v\}| \\ &\text{For all } 0 \leq j \leq D, a_j = |\{w \in \Gamma_j : w \sim v\}| \text{ and} \\ &\text{For all } 0 < j \leq D, c_j = |\{w \in \Gamma_{j+1} : w \sim v\}| \end{aligned}$$

We extend Theorem 2 to distance regular graphs.

Theorem 3 Let the tails be connected to $\Gamma_0 = \Gamma_{J_0}, \Gamma_{J_1}, \Gamma_{J_2}, \dots, \Gamma_{J_m} \leq \Gamma_d$ in the distance regular graph. Then the stationary distribution is as follows.

$$q_{j,j+1} = \frac{1}{|\delta V|} \left\{ 1 + \frac{\text{Number of tails from } \Gamma_{j+1} \text{ to } \Gamma_d}{\text{Number of edges between } \Gamma_j \text{ and } \Gamma_{j+1}} \right\} \quad (7)$$

and

$$q_{j+1,j} = \frac{1}{|\delta V|} \left\{ 1 - \frac{\text{Number of tails from } \Gamma_{j+1} \text{ to } \Gamma_d}{\text{Number of edges between } \Gamma_j \text{ and } \Gamma_{j+1}} \right\} \quad (8)$$

To prove this theorem we use the following lemma.

Lemma 4 For a given $k > 0$, for $j_k \leq j < j_{k+1}$,

$$q_{j,j+1} = \frac{1}{|\delta V|} \left\{ 1 + \frac{b_{j_k-1} |\Gamma_{j_k-1}| (|\delta V| q_{j_k-1, j_k} - 1) - |\Gamma_{j_k}|}{b_j |\Gamma_j|} \right\}$$

and for $0 \leq j < j_1$,

$$q_{j,j+1} = \frac{1}{|\delta V|} \left\{ 1 + \frac{|\delta V| - 1}{b_j |\Gamma_j|} \right\}$$

The proof of Lemma 4 is similar to the proof of Lemma 1.

Proof of Theorem 3

We prove the following statement which is equivalent to the equation (7)

For $j_k \leq j < j_{k+1}$

$$q_{j,j+1} = \frac{1}{|\delta V|} \left\{ 1 + \frac{\sum_{\alpha=k+1}^m |\Gamma_{j_\alpha}|}{b_j |\Gamma_j|} \right\} \quad (9)$$

To equation (9), we use induction on k . The results follows by Lemma 4. Also the equation (8) follows by Theorem 1.

References

- [1] Feldman, E. and Hillery, M. (2005) Quantum walks on graphs and quantum scattering theory. *Contemporary Mathematics* 381. p.71
- [2] Feldman, E. and Hillery, M. (2007) Modifying quantum walks: a scattering theory approach. *J. Phys. A: Math. Theor.* **40** 11343
- [3] Higuchi, Yu. and Segawa, E. (in preperation)
- [4] Emms, D., Hancock, E.R., Severini, S. and Wilson, R.C. (2006) A matrix representation of graphs and its spectrum as a graph invariant. *the electronic journal of combinatorics*, 13(1). p.34.
- [5] Portugal, R. (2013) Quantum walks and search algorithms. Springer Science & Business Media.
- [6] Matsue, K., Matsuoaka, L., Ogurisu, O. and Segawa, E. (2017) Resonant-tunneling in discrete-time quantum walk. *Quantum Studies: Mathematics and Foundations* pp.1-10.

対称空間論の離散化とカンドル代数, Part III. *

田丸 博士[†] (広島大学理学研究科)

概要

カンドル (quandle) は, Joyce によって導入された代数系であり, 主として結び目の研究に用いられてきた. 我々の研究テーマは, カンドルを離散的な対称空間と考え, 対称空間論を参考にして, その構造理論を構築することである. 以前の原稿において, カンドルの基本事項に加え, 二点等質カンドルや連結な平坦カンドルに関する結果を紹介した. 本稿では, 等質な平坦カンドルに関する結果を紹介する. 特に, グラフとの関連について述べたい.

1 導入

我々はカンドルを対称空間論の視点から研究している. 本稿は, このような研究の概要を紹介することを目的としている. なお, 本稿は Part I ([7]), Part II ([8]) の続編という位置付けで書いている. しかし, 独立しても読めるように心掛けた積りである.

まずはカンドルの定義を紹介する. カンドルは, 結び目の研究の過程で Joyce ([3]) によって導入された代数系であり, 元々の定義は二項演算の形で与えられている. しかしここでは, 二項演算を “各点に写像を与える対応” に置き換えたものを定義として紹介する. 以下では, $\text{Map}(X, X)$ を X から X への写像全体の集合とする.

定義 1.1. X を集合とし, 写像 $s : X \rightarrow \text{Map}(X, X) : x \mapsto s_x$ を考える. このとき, (X, s) が **カンドル** とは, 以下が成り立つこと:

- (S1) $\forall x \in X, s_x(x) = x$.
- (S2) $\forall x \in X, s_x$ は全単射.
- (S3) $\forall x, y \in X, s_x \circ s_y = s_{s_x(y)} \circ s_x$.

* 第 35 回代数的組合せ論シンポジウム記録集

[†] 2018/10 からの所属は大阪市立大学理学研究科, tamaru@sci.osaka-cu.ac.jp

以前から、連結リーマン対称空間やアフィン対称空間、あるいは k -対称空間 (各点に位数 k の然るべき写像が対応する空間) などがカンドルとなることは知られていた。従ってカンドルはこれらの空間の“離散化”, すなわち、各点に写像 (点対称) が対応しているという条件のみを抽出し、(リーマン) 多様体あるいは位相などの構造を全て忘れたものだと考えることができる。

我々は特に有限カンドルに興味をもち研究を行っているが、何の制約も付けずに一般的な性質を調べることは、恐らく極めて困難である。そこで、対称空間論を参考にして、然るべき良いクラスのカンドルに着目する。Part II ([8]) でも紹介した内容だが、我々は二点等質カンドルおよび平坦カンドルの概念を定式化し、その研究を行っている。そのうち、本稿では平坦カンドルに関連する話題を扱う。

定義 1.2 ([2]). カンドル (X, s) に対して、 $\{s_x \circ s_y \mid x, y \in X\}$ で生成される群を **変位の群** と呼ぶ。また、変位の群が可換群となるとき、カンドルは **平坦** であるという。

リーマン対称空間において平坦な部分多様体 (コンパクトリー群論における極大トーラス) が重要な役割を果たしたことを考えると、平坦カンドルは、カンドルの構造理論において重要な役割を果たすことが期待される。一方で、次章で詳しく述べるが、連結な有限平坦カンドルは極めて限定的なものしかない (離散トーラスに限る)。そこで本稿では、連結性の仮定を等質性に弱めた場合にどうなるか、という問題を考察する。次が本稿で紹介する主結果だが、この結果は、等質性を仮定したとしても、有限平坦カンドルは極めて豊富に存在することを示唆する。

定理 1.3. 任意の単純グラフ G から、非連結な平坦カンドル Q_G を構成することができる。さらに、 Q_G が等質であるための必要十分条件は、 G が頂点推移的であること。

なお、我々は主に念頭に置いているのは有限グラフ (構成されるカンドルが有限カンドル) の場合であるが、定理の主張そのものは無限グラフであっても成立する。また、等質な有限平坦カンドルが全てこの方法で構成できる訳でもない、ということにも注意しておく。等質な有限平坦カンドルの全体像には、多くの未解明な部分が残っている。

2 準備

本稿の主結果は、グラフを用いた非連結な等質平坦カンドルの構成である。ここでは、その問題意識を紹介するとともに、必要な用語の復習をする。平坦性は前章で定義を紹介した。そこでまずは、連結性と等質性の復習のために、準同型の定義から始める。

定義 2.1. カンドル間の写像 $f : (X, s^X) \rightarrow (Y, s^Y)$ が **準同型** であるとは、次が成り立つこと: $\forall x \in X, f \circ s_x^X = s_{f(x)}^Y \circ f$. また、カンドル間の写像が **同型** であるとは、全単射かつ準同型となること.

定義より、各 $x \in X$ に対して、 $s_x : X \rightarrow X$ はカンドルの自己同型写像となる. このことを用いて、以下の群およびカンドルの連結性や等質性が定義される.

定義 2.2. カンドル (X, s) 上の自己同型写像全体の集合を $\text{Aut}(X, s)$ で表し、**自己同型群** と呼ぶ. $\text{Aut}(X, s)$ が X に推移的に作用するとき、 (X, s) は **等質** であるという. また、 $\{s_x \mid x \in X\}$ で生成される群を **内部自己同型群** と呼び、 $\text{Inn}(X, s)$ で表す. $\text{Inn}(X, s)$ が X に推移的に作用するとき、 (X, s) は **連結** であるという.

定義から明らかに $\text{Inn}(X, s) \subset \text{Aut}(X, s)$. 小さい方の群が推移的に作用するなら大きい方の群も推移的に作用するので、次が成り立つ.

命題 2.3. カンドル (X, s) は連結ならば等質である.

カンドルの具体例を構成する一つの手法として、部分カンドルを用いることが挙げられる. 次章でも紹介するが、例えばリーマン対称空間内の有限部分カンドルは、多くの興味深い具体例を供給する.

定義 2.4. (X, s) をカンドルとする. 部分集合 $A \subset X$ が **部分カンドル** であるとは次が成り立つこと: $\forall a \in A, s_a^{\pm 1}(A) \subset A$.

部分カンドルは自動的にカンドルとなる. ここでは球面内の部分カンドルを取り上げる. \mathbb{R}^{n+1} 内の原点 o 中心の単位球を S^n とする. このときのリーマン対称空間としての点対称は、各 $x \in S^n$ に対して直線 ox に関する折り返しで与えられていた.

例 2.5. R_n を S^1 上の n 等分点の集合とすると、これは S^1 内の部分カンドルである (これを **二面体カンドル** と呼ぶ). このとき R_n は等質かつ平坦なカンドルである. また R_n が連結となるための必要十分条件は、 n が奇数であること.

カンドル $(X, s^X), (Y, s^Y)$ に対して、その直積 $X \times Y$ 上には自然にカンドルの構造が入る (記号で書くと $s_{(x,y)}^{X \times Y} := s_x^X \times s_y^Y$). 特に、二面体カンドルの直積 $R_{n_1} \times \cdots \times R_{n_k}$ のことを **離散トーラス** と呼ぶ.

定理 2.6 ([2]). 有限カンドル (X, s) が連結かつ平坦であるための必要十分条件は、奇数位数の離散トーラスと同型となること.

この定理より、連結な有限平坦カンドルは極めて限られたものしかないと分かる。例えば、各点に付いている写像 s_x の位数は、一般のカンドルでは何の制約もなかったにも関わらず、離散トーラスの場合は必然的に対合的 ($s_x^2 = \text{id}$) である。

注意 2.7. 一般に、直積カンドル $X \times Y$ が連結 (または平坦) となるための必要十分条件は、 X と Y が共に連結 (または平坦) となることである。従って、奇数位数の離散トーラスが連結かつ平坦となることは、この一般論から容易に従う。また、偶数位数の離散トーラスは、非連結な平坦カンドルとなる。等質であることも、比較的容易に分かる。

非連結な等質平坦カンドルがどの程度存在するか、というのは、当然次に考えるべき問題である。特に、偶数位数の離散トーラスのようなものしかないか、全く違うタイプのものがあるか、という疑問は自然であろう。本稿の主結果は、離散トーラスとは遠く離れた全く様相の異なる例が存在する、ということを示唆している。

3 有向実グラスマン多様体内の部分カンドルの例

ここでは、有向実グラスマン多様体内の部分カンドルで、等質な有限平坦カンドルとなるものを紹介する。ここで紹介する例は、次章で紹介する「グラフを用いた構成」の発想の基となったものである。まずはグラスマン多様体を復習する。

定義 3.1. \mathbb{R}^n 内の k 次元線型部分空間全体の集合を $G_k(\mathbb{R}^n)$ で表し、これを 実グラスマン多様体 という。また、 \mathbb{R}^n 内の向き付けられた k 次元線型部分空間全体の集合を $G_k(\mathbb{R}^n)^\sim$ で表し、これを 有向実グラスマン多様体 という。

ここで線形空間 V の向きは、 V の順序付き基底 $\{v_1, \dots, v_k\}$ 全体の集合を、 $\text{GL}(k, \mathbb{R})^+$ による右作用で割った商集合の元として定義される。向きを $[(v_1, \dots, v_k)]$ のように表す。記号の簡略化のため、 $\{e_1, \dots, e_n\}$ を \mathbb{R}^n の標準基底とし、次のように書く：

$$(i_1, \dots, i_k) := (\text{span}\{e_{i_1}, \dots, e_{i_k}\}, [(e_{i_1}, \dots, e_{i_k})]) \in G_k(\mathbb{R}^n)^\sim.$$

また、向きが逆のものをマイナスを付けて表す。例えば $(i_2, i_1) = -(i_1, i_2)$ 。

命題 3.2. 各 $V \in G_k(\mathbb{R}^n)$ に対して、 $r_V : \mathbb{R}^n \rightarrow \mathbb{R}^n$ を V に関する折り返しとする。このとき、 r_V を用いて自然に $s_V : G_k(\mathbb{R}^n) \rightarrow G_k(\mathbb{R}^n)$ および $\tilde{s}_V : G_k(\mathbb{R}^n)^\sim \rightarrow G_k(\mathbb{R}^n)^\sim$ を定めると、 $G_k(\mathbb{R}^n)$ および $G_k(\mathbb{R}^n)^\sim$ はカンドルとなる。

ここで r_V は、 $r_V|_V = \text{id}$, $r_V|_{V^\perp} = -\text{id}$ となる線型写像である。 s_V および \tilde{s}_V につい

ては、次をみると感覚が掴めると思われる。

例 3.3. $G_2(\mathbb{R}^n) \sim$ に対して、以下が成り立つ:

- (1) $\tilde{s}_{(1,2)}(1,3) = (\text{span}\{e_1, -e_3\}, [(e_1, -e_3)]) = -(1,3);$
- (2) $\tilde{s}_{(1,2)}(3,4) = (\text{span}\{-e_3, -e_4\}, [(-e_3, -e_4)]) = (3,4).$

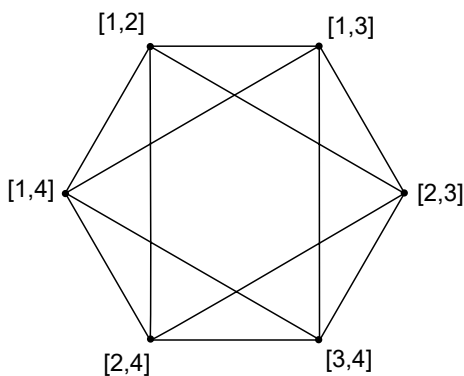
次が本章の主定理である。有向実グラスマン多様体内の部分カンドルで、極めて興味深いものが存在する。単なるグラスマンではなく有向なものを考えているところがポイント。

定理 3.4. 次で定義される $A(k, n)$ は $G_k(\mathbb{R}^n) \sim$ 内の部分カンドルであり、非連結かつ等質な有限平坦カンドル:

$$A(k, n) := \{\pm(i_1, i_2, \dots, i_k) \mid 1 \leq i_1 < \dots < i_k \leq n\}.$$

$A(k, n)$ が部分カンドルであることと非連結であることは、例 3.3 の計算から容易に想像できるはず。平坦であることは、 $\tilde{s}_{\pm(i_1, i_2, \dots, i_k)}$ 同士が可換であることから従う。

例 3.5. $A(2, 4) = \{\pm(1, 2), \pm(1, 3), \pm(1, 4), \pm(2, 3), \pm(2, 4), \pm(3, 4)\}$. またこの場合に、 $[i, j]$ を頂点集合とし、 $s_{\pm(i, j)}$ が $\{\pm(k, l)\}$ に非自明に作用するときに $[i, j]$ と $[k, l]$ を辺で結ぶ。すると次のグラフが得られる:



$A(2, 4)$ のカンドル構造は、グラフをみた方が分かりやすいと思われる。逆に、グラフが与えられると、カンドルを構成することもできる。その構成方法を次章で紹介する。

4 グラフから構成されるカンドル

$G = (V(G), E(G))$ を単純グラフ ($V(G)$ は頂点集合, $E(G)$ は辺集合) とし、その隣接写像を $e : V(G) \times V \rightarrow \mathbb{Z}_2$ とする。ここで $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ であり、 v と w が辺で結ばれて

いれば $e(v, w) = 1$, そうでなければ $e(v, w) = 0$ と定義する.

命題 4.1. $G = (V(G), E(G))$ を単純グラフとする. このとき, 次で定義される写像 s は, $X := V(G) \times \mathbb{Z}_2$ 上のカンドル構造である:

$$s_{(v,a)}(w, b) := (w, b + e(v, w)).$$

上で定義されたカンドルを $Q_G = (V(G) \times \mathbb{Z}_2, s)$ と表し, グラフ G から構成されたカンドルと呼ぶ. これはグラフの各頂点に “ \mathbb{Z}_2 を載せた” もの, と考えることができる. カンドル Q_G の性質を次にまとめる.

定理 4.2. 単純グラフ G から構成されたカンドル Q_G に対して, 以下が成り立つ:

- (1) Q_G は非連結;
- (2) 内部自己同型群 $\text{Inn}(Q_G)$ は可換, 従って特に Q_G は平坦;
- (3) Q_G が等質カンドルであることと, グラフ G が頂点推移的であることは同値.

ちなみに G が辺をもたないグラフ (空グラフ) の場合には, 構成されるカンドル Q_G は自明カンドルである.

例 4.3. G を完全グラフ (全ての頂点同士が辺で結ばれている) とする. もし $\#V(G) = n$ ならば, 構成されるカンドル Q_G は $A(1, n)$ と同型.

証明は, Q_G と $A(1, n)$ のカンドル構造をじっと眺めると, 比較的簡単に分かる. ちなみに $A(1, n)$ は $G_1(\mathbb{R}^n) \sim \cong S^{n-1}$ 内の部分カンドルであった. 同様に, 一般の $A(k, n)$ についても, グラフから構成することができる.

例 4.4. n を自然数, $1 \leq k < n$ とし, $V(G)$ を $\{1, \dots, n\}$ 内の k 点部分集合全体の集合とする. このとき, $v, w \in V(G)$ に対して, $\#(v \setminus w)$ が奇数のときに辺で結び, グラフ G を作る. このグラフから構成されるカンドル Q_G は, $A(k, n)$ と同型.

上で考えているグラフは, $k = 1$ のときは完全グラフ, $k = 2$ のときはジョンソングラフである. 実際に $k = 2$ のとき, $v, w \in V(G)$ が辺で結ばれるための必要十分条件は $\#(v \cap w) = 1 = k - 1$ となる. 一般の k に対して, このグラフに名前が付いているかどうか筆者は知らない.

最後に, グラフから構成されるカンドルの特徴付けを紹介する. 一般のグラフから構成される場合の特徴付けを記述することも可能だが, 複雑になるため, グラフが頂点推移的な場合に限定したものを紹介する.

命題 4.5. カンドル Q に対して, 空でない頂点推移的なグラフ G から構成されるための必要十分条件は, 以下が成り立つこと:

- (1) 内部自己同型群による軌道は全て 2 点集合である;
- (2) 任意の $x, y \in Q$ に対して, “ $s_x(y) = y$ ならば $s_y(x) = x$ ”;
- (3) Q は等質カンドル.

上の条件 (2) の性質は *crossed* と呼ばれており, カンドルの研究にしばしば登場する性質である. ちなみにリーマン対称空間は *crossed* であり, その部分カンドルも自動的に *crossed* となる.

参考文献

- [1] Furuki, K., Tamaru, H.: *Flat homogeneous quandles and vertex-transitive graphs*, preprint.
- [2] Ishihara, Y., Tamaru, H.: *Flat connected finite quandles*, Proc. Amer. Math. Soc., **144** (2016), 4959–4971.
- [3] Joyce, D.: *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra, **23** (1982), 37–65.
- [4] Kamada, S., Tamaru, H., Wada, K.: *On classification of quandles of cyclic type*, Tokyo J. Math., **39** (2016), 157–171.
- [5] Loos, O.: *Symmetric Spaces, I: General Theory*. Benjamin, New York (1969).
- [6] Tamaru, H.: *Two-point homogeneous quandles with prime cardinality*, J. Math. Soc. Japan, **65** (2013), 1117–1134.
- [7] 田丸 博士: 対称空間論の離散化とカンドル代数, Part I, In: Geometry and Analysis 2014 (福岡大学微分幾何研究会) 記録集, 99–107 (2015).
- [8] 田丸 博士: 対称空間論の離散化とカンドル代数, Part II, In: 部分多様体論・湯沢 2014 記録集, 55–60 (2015).
- [9] 田丸 博士: 対称空間論の離散化とカンドル代数, Part IV, In: 部分多様体論・湯沢 2018 記録集, in preparation.
- [10] Vendramin, L.: *Doubly transitive groups and cyclic quandles*, J. Math. Soc. Japan, **69** (2017), 1051–1057.
- [11] Wada, K.: *Two-point homogeneous quandles with cardinality of prime power*, Hiroshima Math. J., **45** (2015), 165–174.

Tight t -designs on one shell of Johnson association schemes

Yan Zhu, Shanghai University

1 Relative t -designs in Q-polynomial association schemes

Given a *semilattice* (\mathcal{L}, \preceq) , we can define a length function $\ell: \mathcal{L} \rightarrow \mathbb{N}$ such that $\ell(y) = \ell(x) + 1$ whenever y covers x . (Here y covers x means that if $x \prec y$ and there is no z such that $x \prec z \prec y$.) Let k be the maximal value of $\ell(x)$, then \mathcal{L} is partitioned into $k + 1$ fibers $\mathcal{L}_0, \mathcal{L}_1, \dots, \mathcal{L}_k$ with $\mathcal{L}_i = \{x \mid \ell(x) = i\}$. We call $X := \mathcal{L}_k$ the top fiber of the semilattice. Delsarte defined regular semilattice as follows.

Definition 1.1 ([2, Definition 9.1]). *The semilattice (\mathcal{L}, \preceq) is called regular if it admits a length function which satisfies the following three properties.*

- (i) *Given $y \in X$, $z \in \mathcal{L}_r$ with $z \preceq y$, $|\{u \in \mathcal{L}_s \mid z \preceq u \preceq y\}| = \mu(r, s)$ is a constant.*
- (ii) *Given $u \in \mathcal{L}_s$, $|\{z \in \mathcal{L}_r \mid z \preceq u\}| = \nu(r, s)$ is a constant.*
- (iii) *Given $y \in X$, $a \in \mathcal{L}_r$ with $a \wedge y \in \mathcal{L}_j$, $|\{(b, z) \in \mathcal{L}_s \times X \mid b \preceq z, b \preceq y, a \preceq z\}| = \pi(j, r, s)$ is a constant.*

Whenever (\mathcal{L}, \preceq) is a regular semilattice, the top fiber X carries an association scheme. Throughout this report, when a Q-polynomial association scheme arises from a regular semilattice, the Q-polynomial ordering we choose, denoted E_0, E_1, \dots, E_k , is always the one associated to length function ℓ . It is known that the top fiber of the Boolean semilattice carries the Johnson association scheme $J(v, k)$.

For $0 \leq j \leq k$, let W_j be the j -th incidence matrix indexed by $\mathcal{L}_j \times X$ whose (x, y) -entry is defined as follows.

$$W_j(x, y) = \begin{cases} 1, & x \preceq y, x \in \mathcal{L}_j, y \in X, \\ 0, & \text{otherwise.} \end{cases}$$

We will present two equivalent definitions of relative t -designs in Q-polynomial association schemes with respect to a fixed point u_0 introduced by Delsarte [3].

Definition 1.2 ([3]). *Let $\mathfrak{X} = (X, \{R_r\}_{0 \leq r \leq k})$ be a symmetric Q-polynomial association scheme associated with a regular semilattice (\mathcal{L}, \preceq) . For any fixed point $u_0 \in X$, a weighted subset (Y, w) is called a relative t -design in \mathfrak{X} with respect to u_0 if the following condition holds.*

$$W_j \chi_{(Y, w)} = \lambda_{j, j_1} \mathbf{1} \text{ for all } 0 \leq j \leq t, \quad (1.1)$$

where λ_{j, j_1} is determined by j and $j_1 = \ell(z \wedge u_0)$.

Definition 1.3 ([3, Theorem 5.9]). *A weighted subset (Y, w) is called a relative t -design in \mathfrak{X} with respect to u_0 if $E_j \chi_{(Y,w)}$ and $E_j \chi_{u_0}$ are linearly dependent for $1 \leq j \leq t$, where*

$$\chi_{(Y,w)}(y) = \begin{cases} w(y), & \text{if } y \in Y, \\ 0, & \text{otherwise.} \end{cases}$$

2 Designs in product association schemes

In this section, we will introduce some definitions and notations about designs in product association schemes given by Martin in [4, 5].

For $1 \leq i \leq m$, let (Y_i, \mathcal{A}_i) be a k_i -class association scheme with the Bose-Mesner algebra \mathcal{A}_i consisting of adjacency matrices. The direct product of these association schemes is

$$(X, \mathcal{A}) = (Y_1, \mathcal{A}_1) \otimes (Y_2, \mathcal{A}_2) \otimes \cdots \otimes (Y_m, \mathcal{A}_m)$$

defined by

$$X = Y_1 \times Y_2 \times \cdots \times Y_m$$

and

$$\mathcal{A} = \{\otimes_{i=1}^m B_i \mid B_i \in \mathcal{A}_i, 1 \leq i \leq m\}.$$

Then (X, \mathcal{A}) always gives an association scheme. Suppose $(\mathcal{L}^{(i)}, \preceq_i)$ is a regular semilattice whose top fiber carries the association scheme (Y_i, \mathcal{A}_i) . Consider the product poset (\mathcal{L}, \preceq) given by

$$\mathcal{L} = \{\underline{x} = (x_1, x_2, \dots, x_m) \mid x_i \in \mathcal{L}^{(i)}\}$$

with partial order $\underline{x} \preceq \underline{y}$ if $x_i \preceq_i y_i$ for each $1 \leq i \leq m$. Let \mathcal{C}_i be the totally ordered chain in $[k_i]$ and define $\mathcal{C} = \mathcal{C}_{k_1} \times \cdots \times \mathcal{C}_{k_m}$. We call a set $\mathcal{T} \subset \mathcal{C}$ a downset in (\mathcal{C}, \preceq) if $\underline{j} \in \mathcal{T}$ and $\underline{i} \preceq \underline{j}$ imply $\underline{i} \in \mathcal{T}$.

If ℓ_i is the length function on $\mathcal{L}^{(i)}$, then it is natural to obtain a vector-valued function $\ell : \mathcal{L} \rightarrow \mathcal{C}$ as follows. For $\underline{x} = (x_1, x_2, \dots, x_m) \in X$ with $\ell_i(x_i) = j_i$, $\ell(\underline{x}) = (j_1, j_2, \dots, j_m)$ gives a length function on \mathcal{L} . Similarly, for $\underline{j} = (j_1, j_2, \dots, j_m)$, we define the incidence matrix $W_{\underline{j}}$ indexed by $\mathcal{L}_{\underline{j}} \times X$ whose (x, y) -entry is given by

$$W_{\underline{j}}(x, y) = \begin{cases} 1, & \text{if } x \preceq y, x \in \mathcal{L}_{\underline{j}}, y \in X, \\ 0, & \text{otherwise,} \end{cases}$$

where

$$\mathcal{L}_{\underline{j}} = \{\underline{x} \in X : \ell(\underline{x}) = \underline{j}\}$$

and

$$X = \{\underline{x} \in X : \ell(\underline{x}) = (k_1, \dots, k_m)\} = Y_1 \times Y_2 \times \cdots \times Y_m.$$

Theorem 2.1 ([5, Theorem 2.3]). *Assume \mathcal{T} is a downset in (\mathcal{C}, \preceq) . Let $\mathfrak{X} = (X, \mathcal{A})$ be a product of some Q -polynomial association schemes, where the Q -polynomial ordering for each component arises from its semilattice structure. Then the weighted subset (Y, w) of X is a weighted \mathcal{T} -design in \mathfrak{X} if one of the following holds.*

(T1') $W_{\underline{j}} \chi_{(Y,w)} = \lambda_{\underline{j}} \mathbf{1}$ for some constant $\lambda_{\underline{j}}$ with $\underline{j} \in \mathcal{T}$.

(T2') $E_{\underline{j}}\chi_{(Y,w)} = 0$ for any $\underline{j} \in \mathcal{T} \setminus \{\underline{0}\}$, where $E_{\underline{j}}$ are the idempotents of \mathfrak{X} .

In particular, (Y, w) is called a weighted t -design in \mathfrak{X} if either (T1') or (T2') holds for

$$\mathcal{T} = \{\underline{j} \in \mathcal{C} : 0 \leq j_1 + \cdots + j_m \leq t\}.$$

3 Relative t -designs on one shell of $J(v, k)$

Given two positive integers v and k with $v \geq 2k$, let $V = \{1, 2, \dots, v\}$ and $X = \binom{V}{k}$ be the set of all k -subsets of V . For any two elements $x, y \in X$, define

$$(x, y) \in R_r \quad \text{if} \quad |x \cap y| = k - r.$$

Then $\mathfrak{X} = (X, \{R_r\}_{0 \leq r \leq k})$ is called a Johnson association scheme $J(v, k)$, which is a \mathbb{Q} -polynomial association scheme and associated with the Boolean semilattice.

Let A_0, A_1, \dots, A_k be the adjacency matrices of $J(v, k)$. The \mathbb{Q} -polynomial ordering of the primitive idempotents are denoted by E_0, E_1, \dots, E_k . Fix a point $u_0 \in X$ arbitrarily and denote the r -th shell of $J(v, k)$ with respect to u_0 by $X_r = \{x \in X : |x \cap u_0| = k - r\}$. Without loss of generality, we may assume $u_0 = \{1, 2, \dots, k\}$. It is known that X_r carries the structure of a product of two smaller Johnson association schemes. Without confusion, we also use X_r to represent the vertex set of the product association scheme X_r . More explicitly, let $v_1 = k$ and $v_2 = v - k$, then we have

- (1) If $2 \leq r \leq \frac{k}{2}$, take $X_r := \{(u_0 - x, x - u_0), x \in X_r\}$, i.e., $X_r = J(v_1, r) \otimes J(v_2, r)$.
- (2) If $\frac{k}{2} < r \leq \frac{v-k}{2}$, take $X_r := \{(x \cap u_0, x - u_0), x \in X_r\}$, i.e., $X_r = J(v_1, k - r) \otimes J(v_2, r)$.
- (3) If $\frac{v-k}{2} < r \leq k - 2$, take $X_r := \{(x \cap u_0, (V - u_0) - x), x \in X_r\}$, i.e., $X_r = J(v_1, k - r) \otimes J(v_2, v - k - r)$.

Our main theorem is Delsarte's generalized Assmus–Mattson Theorem in the case of the Johnson association schemes with weaker assumption.

Theorem 3.1. *Let (Y, w) be a relative t -design in $J(v, k)$ with respect to u_0 on p shells $X_{r_1} \cup X_{r_2} \cup \cdots \cup X_{r_p}$. Put $Y_{r_\nu} = Y \cap X_{r_\nu}$, then (Y_{r_ν}, w) is a weighted $(t + 1 - p)$ -design in the product association scheme X_{r_ν} for $1 \leq \nu \leq p$.*

We give two two proofs of this result. One is a direct proof using Definition 1.2 Another approach makes use of the Terwilliger algebra, based on the work of Tanaka [6].

4 Tight relative t -designs on one shell of $J(v, k)$

By Bannai et al. [1] and Theorem 3.1, we have the following lower bounds.

Theorem 4.1. *If (Y, w) is a relative $2e$ -design in $J(v, k)$ for \mathbb{Q} -polynomial structure on one shell X_r , then*

$$|Y| \geq \begin{cases} \binom{v}{e} - \binom{v}{e-1}, & \text{if } t = 2e, \\ 2 \left(\binom{v-1}{e} - \binom{v-1}{e-1} \right), & \text{if } t = 2e + 1. \end{cases} \quad (4.1)$$

Moreover, equality holds whenever Y contains a pair of (h_1, h_2) -related elements satisfying

$$F(h_1, h_2) = \sum_{j \in \mathcal{E}} Q_j(\underline{h}) = 1 + Q_1^{(1)}(h_1) + Q_2^{(2)}(h_2) = 0,$$

where $Q_j^{(i)}(x) = {}_3F_2\left(\begin{matrix} -j, j - v_i - 2, x \\ -k_i, -v_i + k_i \end{matrix}; 1\right)$. Two points $x, y \in X$ are called \underline{h} -related if $(x, y) \in R_{\underline{h}}$ in \mathfrak{X} .

Definition 4.2. A relative t -design in $J(v, k)$ on one shell is called ‘tight’ if equality in (4.1) holds.

4.1 Tight relative 2-designs on one shell of $J(v, k)$

For $v \leq 1000$, we can give a list of all possible parameters of tight relative 2-designs in $J(v, k)$ on one shell X_r . In the following three tables, the notation $\ell = x \rightarrow y$ means that ℓ takes all the integers from x to y .

Case 1: If $2 \leq r \leq \frac{k}{2}$, then $X_r = J(k, r) \otimes J(v - k, r)$.

v	k	r	$\lambda_{(1,0)}$	$\lambda_{(0,1)}$	$\lambda_{(1,1)}$	$\lambda_{(2,0)}$	$\lambda_{(0,2)}$	(h_1, h_2)
210	77	21	57	33	9	15	5	$(3\ell, 28 - 2\ell), \ell = 4 \rightarrow 7$
210	77	28	76	44	16	27	9	$(14, 25), (21, 20), (28, 15)$
378	117	36	116	52	16	35	7	$(18, 35), (27, 30), (36, 25)$
378	117	45	145	65	25	55	11	$(5\ell, 54 - 3\ell), \ell = 3 \rightarrow 9$
990	345	105	301	161	49	91	26	$(56 + 14\ell, 99 - 9\ell), \ell = 0 \rightarrow 3$
990	345	120	344	184	64	119	34	$(45 + 3\ell, 120 - 2\ell), \ell = 0 \rightarrow 25$

Table 1: Possible parameters for tight mixed 2-designs in X_r for $r \leq \frac{k}{2}$

It seems not easy either to find an example or to prove the non-existence of tight mixed 2-designs with the parameters in the above table, since the classification of either 2- $(k, r, \lambda_{(2,0)})$ designs or 2- $(v - k, r, \lambda_{(0,2)})$ designs is not complete.

Case 2: If $\frac{k}{2} < r \leq \frac{v-k}{2}$, then $X_r = J(k, k - r) \otimes J(v - k, r)$.

In this case, if $\lambda_{(0,2)} = \lambda_{(1,1)} = \lambda_{(2,0)} - 1$, i.e., $h_1 + h_2 = r$, then Y is a tight mixed 2-design in X_r . Namely, Y arises from a symmetric 2- $(v, k, \lambda_{(0,2)})$ design with one block removed. Conversely, if we have a tight mixed 2-design in X_r , then whether $h_1 + h_2 = r$ is true or not becomes an interesting problem. We check this for $v \leq 1000$ and find that all the possible parameters satisfy $h_1 + h_2 = r$ except the following case.

v	k	r	$\lambda_{(1,0)}$	$\lambda_{(0,1)}$	$\lambda_{(1,1)}$	$\lambda_{(2,0)}$	$\lambda_{(0,2)}$	(h_1, h_2)
528	187	165	62	255	30	7	123	$(5\ell, 132 - 12\ell), \ell = 0 \rightarrow 4$

It is still an open question whether we can find an example with the required parameters.

Case 3: If $\frac{v-k}{2} < r \leq k - 2$, then $X_r = J(k, k - r) \otimes J(v - k, v - k - r)$.

v	k	r	$\lambda_{(1,0)}$	$\lambda_{(0,1)}$	$\lambda_{(1,1)}$	$\lambda_{(2,0)}$	$\lambda_{(0,2)}$	(h_1, h_2)	
36	15	12	7	15	3	1	6	$(0,9), (2,6)$	\nexists
100	45	40	11	27	3	1	7	$(3,14), (4,12), (5,10)$	
205	85	70	36	85	15	6	35	$(3\ell, 50 - 5\ell), \ell = 0 \rightarrow 5$	
484	231	165	138	168	48	39	58	$(9\ell, 10(11 - \ell)), \ell = 3 \rightarrow 7$	
676	325	273	108	150	24	17	33	$(35,72), (42,63), (49,54)$	
981	441	297	320	441	144	104	198	$(8\ell, 243 - 9\ell), \ell = 0 \rightarrow 18$	

Table 2: Possible parameters for tight mixed 2-designs in X_r for $\frac{v-k}{2} < r \leq k-2$

Proposition 4.3. *There exists no tight relative 2-design in $J(36, 15)$ on the shell X_{12} .*

4.2 Tight relative 3-designs on one shell of $J(v, k)$

By computer search, for $v \leq 1,000$, the only family that appears is of the following type: $v = 4u$, $k = 2u$, $k_1 = k_2 = r$ and $2 \leq r \leq u$ for any integer $2 \leq u \leq 250$. And the set Λ contains the variables below.

$$\begin{aligned}\lambda_{(1,0)} &= \lambda_{(0,1)} = 4u - 2; \\ \lambda_{(2,0)} &= \lambda_{(0,2)} = \lambda_{(1,1)} - 1 = 2u - 2; \\ \lambda_{(3,0)} &= \lambda_{(0,3)} = \lambda_{(1,2)} - 1 = \lambda_{(2,1)} - 1 = u - 2.\end{aligned}$$

For $2 \leq u \leq 250$, if a Hadamard $2-(4u-1, 2u-1, u-1)$ design exists, then we can construct a tight mixed 3-design in X_u with $v = 4u$ and $k = 2u$.

Problem. Whether there exists a tight mixed 3-design in X_r which is not from Hadamard 2-designs is an open and interesting problem.

References

- [1] E. BANNAI, ET. BANNAI, S. SUDA, H. TANAKA, *On relative t -designs in polynomial association schemes*, Electronic Journal of Combinatorics 33 (2015), no. 4, 4–47.
- [2] P. DELSARTE, *Association schemes and t -designs in regular semilattices*, Journal of Combinatorial Theory, Series A 20 (1976), no. 2, 230–243.
- [3] P. DELSARTE, *Pairs of vectors in the space of an association scheme*, Philips Research Report 32 (1977), no. 5–6, 373–411.
- [4] W. J. MARTIN, *Mixed block designs*, Journal of Combinatorial Designs 6 (1998), 151–163.
- [5] W. J. MARTIN, *Designs in product association schemes*, Designs, Codes and Cryptography 16 (1999), 271–289.
- [6] H. TANAKA, *New proofs of the Assmus-Mattson theorem based on the Terwilliger algebra*, European Journal of Combinatorics 30 (2009), no. 3, 736–746.

Report on 第35回代数的組み合わせ論シンポジウム,
広島工業大学 広島校舎

Presenter : Mohammad Samy Baladram
Title : Simplex designs: a new construction method for
spherical designs
Institution : 東北大学大学院情報科学研究科
Date : June 19, 2018

1 Spherical Design

A **spherical t -design** X is a finite subset of the unit sphere

$$S^{n-1} = \{(x_1, \dots, x_n) \mid x_1^2 + x_2^2 + \dots + x_n^2 = 1\} \subset \mathbb{R}^n$$

such that for any polynomial $f(x) = f(x_1, \dots, x_n)$ of degree $\leq t$

$$\frac{1}{|S^{n-1}|} \int_{S^{n-1}} f(x) d\sigma(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$$

where σ denotes the surface measure on S^{n-1} . It is actually enough to show that the equality holds for all monomial of degree at most t .

Delsarte-Goethals-Seidel [4] in 1977 introduced an analogous concept of combinatorial designs for continuous spheres by defining what they called *spherical t -design*. Regarding the existence of spherical t -design on S^n , there is a method to reduce it to the existence of interval t -designs with certain weight function (i.e. Gegenbauer weight function) for the integral.

For $a, b \in \mathbb{R}$, $a < b$, the subset X is an (a, b) -interval t -design with respect to the weight function $w_m(x)$, if the following holds

$$\frac{1}{\int_a^b w_m(x) dx} \int_a^b f(x) w_m(x) dx = \frac{1}{|X|} \sum_{x \in X} f(x), \quad (1)$$

for any polynomial $f(x)$ of degree at most t . We will be working only on the interval $(-1, 1)$ and $(0, 1)$.

By using $(-1, 1)$ -interval t -design and spherical t -design of a lower dimension, Rabau and Bajnok [6] constructed new spherical t -designs.

Theorem 1 (Rabau-Bajnok, 1991) *Let $Y \subseteq S^{n-1}$ be a spherical t -design, and let $V \subset [-1, 1]$ be an $(-1, 1)$ -interval t -design with weight function $w_{n-2}(x) = (1 - x^2)^{\frac{n-2}{2}}$. Then*

$$Z = \{(\sqrt{1 - v^2}y, v) \mid y \in Y, v \in V\}$$

is a spherical t -design on S^n .

We may conclude that an interval design with certain weight function can elevate any existing spherical design.

G. Kuperberg [5] in 2005 managed to explicitly construct interval t -design for constant weight function. By Rabau-Bajnok Theorem, it is possible to construct a spherical t -design on S^2 for any t . In attempt to generalize this result to higher dimensions, by using a similar set as that of Kuperberg, in 2013, M.S.B and D. Suprijanto [1], some interval t -designs with Gegenbauer weight function $w_k(x)$ for some small t and k need to be constructed. It appears that it is quite difficult to construct interval t -design with non-constant weight function. Bannai–Bannai–Tanaka–Zhu’s survey paper [2] mentioned that other explicit constructions seem not to be solved, except for some special cases. Bondarenko et.all [3] in 2011 proved that for each $N \geq c_d t^d$ there exists a spherical t -design in the sphere S_d consisting of N points, where c_d is a constant depending only on d . Can we find some spherical designs with better size (at least for some special cases)?

Theorem 2 (Rabau-Bajnok, 1991) *Let $Y \subseteq S^{n-1}$ be a spherical t -design, and let $V \subset [-1, 1]$ be an $(-1, 1)$ -interval t -design with weight function $w_{n-2}(x) = (1 - x^2)^{\frac{n-2}{2}}$. Then*

$$Z = \{(\sqrt{1 - v^2}y, v) \mid y \in Y, v \in V\}$$

is a spherical t -design on S^n .

Idea of the proof:

$$\begin{aligned} \int_{S^n} \square &= \int_{S^{n-1}} \square \cdot \int_{-1}^1 \square \\ &\parallel \\ \underbrace{\sum_{z \in Z \subset S^n} \square}_{\text{s. } t\text{-design on } S^n} &= \underbrace{\sum_{y \in Y \subset S^{n-1}} \square}_{\text{spherical } t\text{-designs on } S^{n-1}} \cdot \underbrace{\sum_{v \in V \subset [-1, 1]} \square}_{[-1, 1]\text{-interval } t\text{-design}} \end{aligned}$$

\square s are just monomials.

We can see it as this: let $(n, 1)$ be a composition of $n + 1$.

$$\frac{1}{|S^n|} \int_{S^n} \square = \frac{1}{|S^{n-1}|} \int_{S^{n-1}} \square \cdot \frac{1}{|S^0|} \int_{S^0} \square \cdot \frac{1}{\int_{-1}^1} \int_{-1}^1 \square$$

$$\begin{aligned} & \parallel \\ \underbrace{\frac{1}{|Z|} \sum_{z \in Z \subset S^n} \square}_{\text{s. } t\text{-design on } S^n} &= \underbrace{\frac{1}{|Y|} \sum_{y \in Y \subset S^{n-1}} \square}_{\text{sph. } t\text{-designs on } S^{n-1}} \cdot \underbrace{\frac{1}{|Y'|} \sum_{y' \in Y' \subset S^0} \square}_{\text{sph. } t\text{-designs on } S^0} \cdot \underbrace{\frac{1}{|V|} \sum_{v \in V \subset [-1,1]} \square}_{[-1,1]\text{-interval } t\text{-design}} \end{aligned}$$

Spherical t -designs on S^0 are just $\{\pm 1\}$.

We can do the same process for arbitrary composition of n ? Let (n_1, \dots, n_p) be a composition of n .

$$\begin{aligned} \int_{S^{n-1}} &= \int_{S^{n_1-1}} \cdot \int_{S^{n_2-1}} \cdots \int_{S^{n_p-1}} \cdot \int_{?} \\ & \parallel \\ \underbrace{\sum_{z \in Z \subset S^{n-1}}}_{\text{sph. } t\text{-design on } S^{n-1}} &= \underbrace{\sum_{y_1 \in Y_1 \subset S^{n_1-1}} \cdot \sum_{x \in Y_2 \subset S^{n_2-1}} \cdots \sum_{y_2 \in Y_p \subset S^{n_p-1}}}_{\text{sph. } t\text{-designs on } S^{n_1-1}, \dots, S^{n_p-1}} \cdot \underbrace{\sum_{x \in X \subset ?}}_{? \text{ design}} \end{aligned}$$

Let $\Delta^{p-1} = \{(x_1, \dots, x_p) \mid \sum_{i=1}^p x_i = 1, x_i \geq 0 \text{ for all } i\}$. This is a p -dimensional simplex.

Lemma 3 *Let $n, p, n_i, 1 \leq i \leq p$ be positive integers and (n_1, \dots, n_p) be a composition of n . Also, let $\{k_{i,j}\}_{\substack{1 \leq i \leq p, \\ 1 \leq j \leq n_i}}$ be positive integers. Then,*

$$\begin{aligned} & \frac{1}{|S^{n-1}|} \int_{S^{n-1}} \prod_{i=1}^p \prod_{j=1}^{n_i} z_{i,j}^{2k_{i,j}} d\sigma_{S^{n-1}}(z_{1,1}, z_{1,2}, \dots, z_{1,n_1}, z_{2,1}, \dots, z_{p,n_p}) \\ &= \frac{1}{\int_{\Delta^{p-1}} \prod_{i=1}^p x_i^{\frac{n_i}{2}-1} d\sigma_{\Delta^{p-1}}(x)} \int_{\Delta^{p-1}} \prod_{i=1}^p x_i^{\sum_{j=1}^{n_i} k_{i,j} + \frac{n_i}{2} - 1} d\sigma_{\Delta^{p-1}}(x) \\ & \cdot \prod_{i=1}^p \frac{1}{|S^{n_i-1}|} \int_{S^{n_i-1}} \prod_{j=1}^{n_i} y_{i,j}^{2k_{i,j}} d\sigma_i(y_i). \end{aligned}$$

We can see it as this kind of integrals product:

$$\int_{S^{n-1}} = \int_{S^{n_1-1}} \cdot \int_{S^{n_2-1}} \cdots \int_{S^{n_p-1}} \cdot \int_{\Delta^{p-1}}$$

2 Simplex Design

A finite subset V of Δ^{n-1} is called a *simplex t -design* with weight function $w : \Delta^{n-1} \rightarrow \mathbf{R}$ if

$$\frac{1}{\int_{\Delta^{n-1}} w(x) d\sigma_{\Delta^{n-1}}(x)} \int_{\Delta^{n-1}} f(x) w(x) d\sigma_{\Delta^{n-1}}(x) = \frac{1}{|V|} \sum_{v \in V} f(v) \quad (2)$$

holds for all polynomials $f(x) = f(x_1, x_2, \dots, x_d)$ of degree at most t , where $\sigma_{\Delta^{n-1}}$ denotes the surface measure on Δ^{n-1} .

$$\begin{aligned} \int_{S^{n-1}} &= \int_{S^{n_1-1}} \cdot \int_{S^{n_2-1}} \cdots \int_{S^{n_p-1}} \cdot \int_{\Delta^{p-1}} \\ &\parallel \\ \sum_{\substack{z \in Z \subset S^{n-1} \\ \text{s. } t\text{-design on } S^{n-1}}} &= \underbrace{\sum_{y_1 \in Y_1 \subset S^{n_1-1}} \cdot \sum_{x \in Y_2 \subset S^{n_2-1}} \cdots \sum_{y_p \in Y_p \subset S^{n_p-1}}}_{\text{spherical } t\text{-designs on } S^{n_1-1}, \dots, S^{n_p-1}} \cdot \underbrace{\sum_{x \in X \subset \Delta^{p-1}}}_{\text{simplex } \lfloor \frac{t}{2} \rfloor\text{-design}} \end{aligned}$$

Theorem 4 Let n, p be positive integers, (n_1, \dots, n_p) a composition of n , and Y_i a spherical $(2t+1)$ -design on S^{n_i-1} for $1 \leq i \leq p$. Also, let X be a simplex t -design on Δ^{p-1} with weight function $w(x) = \prod_{i=1}^p x_i^{\frac{n_i}{2}-1}$. Then, the set

$$Z = \{(\sqrt{x_1}y_1, \sqrt{x_2}y_2, \dots, \sqrt{x_p}y_p) \mid y_i \in Y_i, (x_1, \dots, x_p) \in X\}$$

is a spherical $(2t+1)$ -design in S^{n-1} .

Corollary 5 Let d, t be positive integers, $d \geq 2$, and Y a spherical t -design on S^1 for $1 \leq i \leq d$. Also, let X be a simplex $\lfloor \frac{t}{2} \rfloor$ -design on Δ^{d-1} with constant weight function. Then, the following set is a spherical t -design on S^{2d-1} .

$$Z = \{(\sqrt{x_1}y_1, \sqrt{x_2}y_2, \dots, \sqrt{x_d}y_d) \mid y_i \in Y, (x_1, \dots, x_d) \in X\}$$

$$\begin{aligned} \int_{S^{2d-1}} &= \overbrace{\int_{S^1} \cdot \int_{S^1} \cdots \int_{S^1}}^d \cdot \int_{\Delta^{d-1}} \\ &\parallel \end{aligned}$$

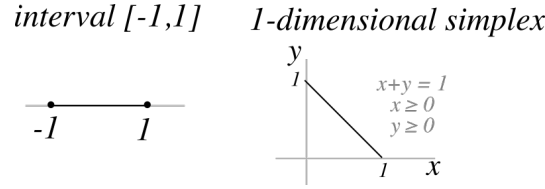
$$\underbrace{\sum_{z \in Z \subset S^{2d-1}}}_{\text{s. } t\text{-design on } S^{2d-1}} = \underbrace{\sum_{y_1 \in Y_1 \subset S^1} \cdot \sum_{x \in Y_2 \subset S^1} \cdots \sum_{y_d \in Y_d \subset S^1}}_{\text{spherical } t\text{-designs on } S^1} \cdot \underbrace{\sum_{x \in X \subset \Delta^{d-1}}}_{\text{simplex } \lfloor \frac{t}{2} \rfloor\text{-design with const. w.f}}$$

Since spherical t -design on S^1 is just a $(t+1)$ -gon, the size of the spherical t -design on S^{2d-1} by this method is

$$|Z| = (t+1)^d \cdot |X|$$

where $|X|$ is a simplex $\frac{t}{2}$ -design with constant weigh function. Recal that Bondarenko et.al [3] in 2011 proved the existence for each $N \geq c_{2d-1} t^{2d-1}$.

We can see it as a linear transformation of interval t -design with constant weight function.



G. Kuperberg in 2005 [5] managed to construct interval t -design for constant weight function.

Theorem 6 (Kuperberg, 2005) *Let $p \geq 2$ be an integer, $P = \{p - (2i + 1) \mid 0 \leq i \leq p - 1\}$. Then, there exists unique constants $a_1 > \cdots > a_t > 0$ such that*

$$X = \{a_1 x_1 + a_2 x_2 + \cdots + a_t x_t \mid (x_1, \dots, x_t) \in P^t\}$$

is an interval $2t$ -design with constant weight.

Corollary 7 *Let t be a positive integer and let Y be a spherical t -design on S^1 and T a $[-1, 1]$ -interval $\lfloor \frac{t}{2} \rfloor$ -design with constant weight function. Then,*

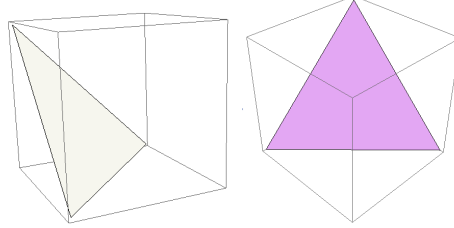
$$Z = \{(\sqrt{\frac{1-t}{2}} y_1, \sqrt{\frac{1+t}{2}} y_2) \mid y_1, y_2 \in Y, t \in T\}$$

is a spherical t -design on S^3 .

Unfortunately, the size is not really good: $(t+1) \cdot 2^{\frac{t}{2}}$.

3 Simplex t -design with constant weight function in Δ^2

This is a representation of Δ^2 on \mathbf{R}^3 .



The question is how can we distribute the points "nicely" on equilateral triangle?

For the set of points V to be a simplex t -design, the equation

$$\frac{1}{\int_{\Delta^{n-1}} d\sigma_{\Delta^{n-1}}(x)} \int_{\Delta^{n-1}} f(x) d\sigma_{\Delta^{n-1}}(x) = \frac{1}{|V|} \sum_{v \in V} f(v) \quad (3)$$

have to hold for all polynomials $f(x) = f(x_1, x_2, \dots, x_d)$ of degree at most t . We can simplify this condition to be as follows:

Lemma 8 Let $n, s, t \in \mathbb{Z}_{>0}$, $n \geq 2$, $(x_{i,j})_{1 \leq i \leq s, 1 \leq j \leq n} \in (0, 1)^{s \times n}$ where $\sum_{j=1}^n x_{i,j} = 1$ for all i . Also,

$$X = \{(x_{i,\pi(1)}, x_{i,\pi(2)}, \dots, x_{i,\pi(n)}) \in \mathbb{R}^n \mid 1 \leq i \leq s, \pi \in C_n\}.$$

Then, the multiset X is a simplex t -design if and only if

$$\frac{1}{sn} \sum_{i=1}^s \sum_{j=1}^n x_{i,j}^k = \frac{(n-1)!k!}{(n+k-1)!} \quad (2 \leq k \leq t). \quad (4)$$

Recall

$$\frac{1}{sn} \sum_{i=1}^s \sum_{j=1}^n x_{i,j}^k = \frac{(n-1)!k!}{(n+k-1)!} \quad (2 \leq k \leq t). \quad (5)$$

Let say we want to find 3 points forming a simplex 2-design, that is (a, b, c) , (b, c, a) , and (c, a, b) . Then, it has to satisfy the following equations:

$$\begin{aligned} a + b + c &= 1 \\ \frac{1}{3}(a^2 + b^2 + c^2) &= \frac{2!2!}{4!} = \frac{1}{6} \end{aligned}$$

It has infinitely many solutions!

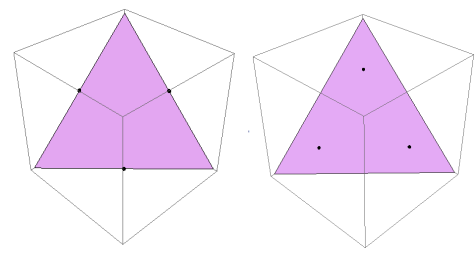
Let's set $b = c$. We need to find a, b that satisfy the following equations:

$$a + 2b = 1$$

$$\frac{1}{3}(a^2 + 2b^2) = \frac{1}{6}$$

that is $(a, b) = (0, 0.5)$ and $(a, b) = (\frac{2}{3}, \frac{1}{6})$.

$(0, 0.5, 0.5), (0.5, 0, 0.5), (0.5, 0.5, 0)$ and $(\frac{2}{3}, \frac{1}{6}, \frac{1}{6}), (\frac{1}{6}, \frac{1}{6}, \frac{2}{3}), (\frac{1}{6}, \frac{2}{3}, \frac{1}{6})$.

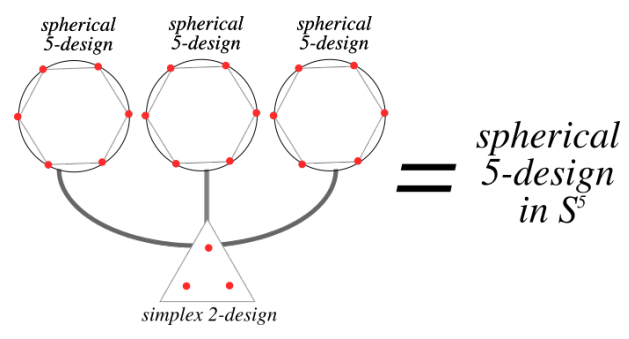


Corollary 9 Let d, t be positive integers, $d \geq 2$, and Y a spherical t -design on S^1 for $1 \leq i \leq d$. Also, let X be a simplex $[\frac{t}{2}]$ -design on Δ^{d-1} with constant weight function. Then, the set

$$Z = \{(\sqrt{x_1}y_1, \sqrt{x_2}y_2, \dots, \sqrt{x_d}y_d) \mid y_i \in Y, (x_1, \dots, x_p) \in X\}$$

is a spherical t -design on S^{2d-1} .

In this corollary, we set $d = 3, t = 5$.



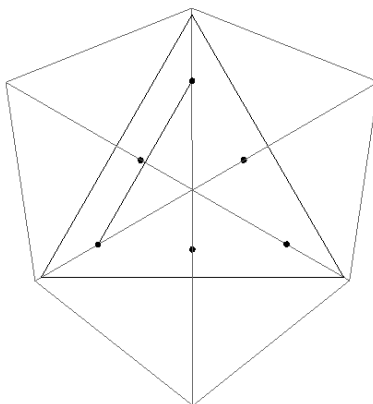
We'd like to construct a simplex 3-designs with 6 points that consist of cyclic permutations of (x_1, x_2, x_2) and (x_3, x_4, x_4) . Then, the points has to

satisfy the following equations:

$$\begin{aligned}x_1 + 2x_2 &= 1, \\x_3 + 2x_4 &= 1, \\ \frac{1}{6}(x_1^2 + 2x_2^2 + x_3^2 + x_4^2) &= \frac{1}{6}, \\ \frac{1}{6}(x_1^3 + 2x_2^3 + x_3^3 + x_4^3) &= \frac{1}{10}.\end{aligned}$$

It only has one solution which is :

$$\begin{aligned}x_1 &= 0.107332, \\x_2 &= 0.446334, \\x_3 &= 0.747031, \\x_4 &= 0.126485.\end{aligned}$$

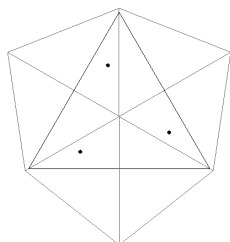


Can we make it with just 3 points that consist of cyclic permutations of (x_1, x_2, x_3) ? Then, the points has to satisfy the following equations:

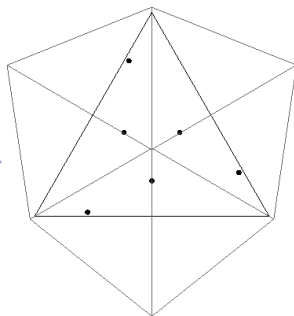
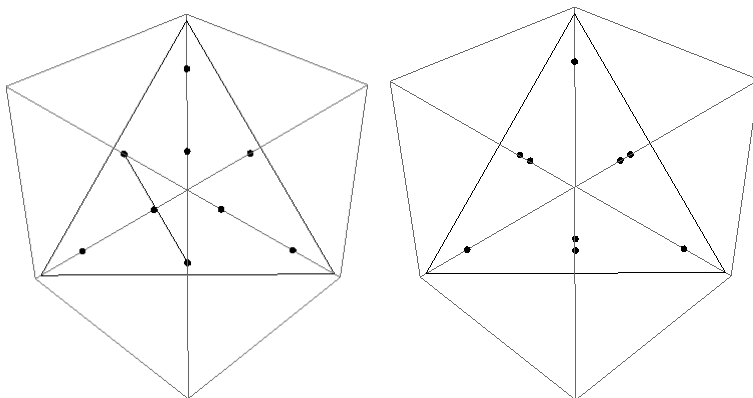
$$\begin{aligned}x_1 + x_2 + x_3 &= 1, \\ \frac{1}{3}(x_1^2 + x_2^2 + x_3^2) &= \frac{1}{6}, \\ \frac{1}{3}(x_1^3 + x_2^3 + x_3^3) &= \frac{1}{10}.\end{aligned}$$

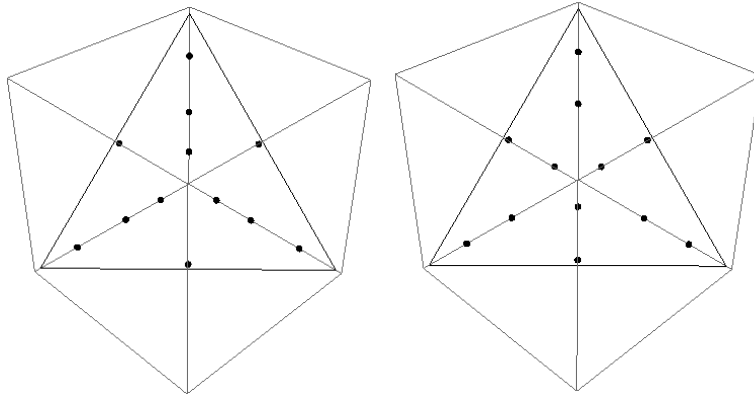
Yes. It has one solution which is :

$$\begin{aligned}x_1 &= 0.659028, \\x_2 &= 0.231933, \\x_3 &= 0.109039.\end{aligned}$$



Can we make it with just 3 points that consist of cyclic permutations of (x_1, x_2, x_2) , (x_3, x_4, x_4) , (x_5, x_6, x_6) ?





Some future problems:

- Is it true that the set of $3s$ points $\{(x_i, y_i, z_i)_\pi \mid 1 \leq i \leq s, \pi \in C_3\}$ always can make a simplex $(s + 1)$ -design?
- Can we do a similar way for non-constant simplex design?

References

- [1] M. S. Baladram and D. Suprijanto, New spherical $(2s + 1)$ -designs from Kuperberg's set: An experimental result. *Applied Mathematics and Computation* **249** (2014), 45–52.
- [2] E. Bannai, Et. Bannai, H. Tanaka, and Y. Zhu. Design theory from the viewpoint of algebraic combinatorics. *Graphs and Combin.* **33**, no. 1 (2017): 1–41.
- [3] A. Bondarenko, D. Radchenko, and M. Viazovska, Optimal asymptotic bounds for spherical designs, *Annals of Mathematics* **178** (2013), 443–452.
- [4] P. Delsarte, J.-M. Goethals, and J. J. Seidel, Spherical codes and designs, *Geom. Ded.* **6** (1977) 363–388.
- [5] G. Kuperberg, Special moments, *Adv. in Appl. Math* **34** (2005), no. 42 853–870.
- [6] P. Rabau and B. Bajnok, Bounds for the number of nodes in Chebyshev type quadrature formulas, *J. Approximation Theory* **67** (1991), 199–214.

Unitary designs in quantum information science

Yoshifumi Nakata (The University of Tokyo)*

Abstract

Unitary designs are recently attracting much attention in quantum information science. In this report, we first overview how unitary designs are used in quantum information science and what is important there. We then explain constructions of approximate unitary designs recently proposed by us. We also present a couple of combinatorial problems we met in our analysis, which may be of independent interest. We hope that this report will motivate fruitful collaborations between design theory and quantum information science.

1. Introduction –quantum information meets design theory–

“Information is physical” – a famous phrase by a physicist Ralph Landauer originally back in 1991 [1] tells us that at the fundamental level of information processing, it is essential to take the laws of physics into account. This is just because information processing is necessarily performed by changing a property of matters. For instance, one bit, 0 or 1, is usually expressed by the existence of electrons or the direction of small magnets in our computers. Thus, information processing in our computers is performed by changing the properties of such physical objects, which is why information processing itself should necessarily obey the fundamental laws of physics. This, in turn, implies that there should be a *physical* limitation to information processing, induced by the fundamental laws of physics. So, what is the limitation?

Quantum information science is the research area that has been trying not only to answer the question but also to realise the ultimate information processing by considering information processing based on quantum mechanics, often called *quantum information processing*. Quantum mechanics is the most fundamental theory in physics, where lots of counter-intuitive phenomena are observed: for instance, the direction of a magnet can be *up and down at the same time*, which may sound contradictory but is possible in some sense in quantum mechanics. Making use of such strange phenomena in quantum mechanics, new types of information processing based on radically different rules become possible, which may be more powerful than what we can currently do.

Quantum information science has rapidly grown up in the past decades, and it was theoretically revealed that quantum phenomena indeed enhance the ability of many information processing, such as communication, cryptography, and computation. Due to this potential, a big race towards quantum information technology has recently get started. However, quantum phenomena are very fragile and are hard to control in practice, implying that it is not so easy to experimentally implement quantum information processing. Hence, despite the high expectation, we are still at the very elementary stage of the race.

A part of this work was supported by JSPS KAKENHI Grant Number 272650 and by CREST, JST, Grant No. JPMJCR1671. Y. N. also acknowledges C. Hirche, M. Koashi, and A. Winter for the fruitful collaboration, and T. Okuda for inviting me to the workshop of combinatorics and also for a careful reading of the report.

* e-mail: nakata@qi.t.u-tokyo.ac.jp

One of the provisional goals towards quantum information technology is to implement *random* quantum dynamics. Randomness is often very useful in information processing, ranging from shuffling cards to algorithmic or cryptographic uses. This is true even in quantum information processing, where randomness is described by a unitary matrix chosen uniformly at random from the unitary group with respect to the Haar measure. Although such a random unitary, which we often call a Haar random unitary, is known to be extremely useful in quantum information processing, experimental implementations of the random dynamics corresponding to a Haar random unitary are yet extremely difficult due to the limitation of experimentally available techniques. Hence, we often replace the Haar random one with approximate ones, namely with *unitary designs*. Fortunately, unitary designs can be used instead of a Haar random unitary in many applications. So, implementing unitary designs is one of the important steps towards the development of quantum information technology.

In this way, quantum information science has met unitary designs. We here emphasise that “implementing” unitary designs has a rather specific meaning in quantum information science. We would like to experimentally implement the physical dynamics that corresponds to a unitary design. Hence, it is of crucial importance to find “experimentally-friendly” constructions of unitary designs. This is a particular problem in quantum information science and hopefully introduces notable perspectives into design theory in mathematics. This report aims to accelerate collaborations between quantum information science and mathematics by providing a brief overview of unitary designs in quantum information science. In particular, we clarify what researchers in the field care about unitary designs.

The report is organised as follows. Section 2 is devoted to preliminaries, where we explain quantum mechanics and unitary designs in brief. We then explain *local unitaries* and *efficiency* of a unitary in Section 3, which are ones of the most essential concepts in quantum information. In Section 4, we provide constructions of approximate or exact unitary designs known in quantum information science. Two mathematical problems, both appeared in the construction of approximate unitary designs, and partial solutions to them are presented in Section 5. The report will be concluded with a summary in Section 6.

Before we start, the author would like to make an excuse that the author is a physicist and am not good at mathematics. Although the author made the best effort to write down everything as mathematically clearly as possible, the author apologises if there are inappropriate expressions.

2. Preliminaries

2.1. Notation

Throughout the report, we consider a finite dimensional Hilbert space \mathcal{H} . A set of all linear operators acting on \mathcal{H} is denoted by $\mathcal{L}(\mathcal{H})$. Following the standard notation in physics, the Hermite conjugate is denoted by \dagger . The unitary group of degree d is denoted by $\mathcal{U}(d)$. As is often the case in physics, we consider only a natural representation of the unitary group. Hence, a unitary $U \in \mathcal{U}(d)$ is always identified with a $d \times d$ unitary matrix acting on a d -dimensional Hilbert space.

For unit vectors, we use the so-called Dirac’s bra-ket notation: a unit vector in a Hilbert space \mathcal{H} is called a *ket* and is denoted by $|\phi\rangle$, and its Hermite conjugate $(|\phi\rangle)^\dagger$ is called a *bra* denoted by $\langle\phi|$. Note that ϕ is just a labelling of the vector and, if needed, can be replaced with anything, e.g. $|a\rangle, |e_1\rangle, |\ominus\rangle, |\otimes\rangle$ etc.

We also use the following standard asymptotic notation. Let $f(n)$ and $g(n)$ be functions from \mathbb{N} to \mathbb{R}^+ . We say $f(n) = O(g(n))$ if there exist $c, n_0 > 0$ such that $f(n) \leq cg(n)$ for all $n \geq n_0$. When there exist $c, n_0 > 0$ such that $f(n) \geq cg(n)$ for all $n \geq n_0$, we say $f(n) = \Omega(g(n))$. If $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$, we denote it by $f(n) = \Theta(g(n))$. If $\lim_{n \rightarrow \infty} f(n)/g(n) = 0$, we write it by $f(n) = o(g(n))$.

For given integers i, j ($i < j$), we denote by $[i, j]$ a sequence of integers from i to j , $[i, j] := \{i, i+1, \dots, j-1, j\}$. For any set S , we denote its cardinality by $|S|$.

2.2. Quantum mechanics in brief

Quantum mechanics consists of three fundamental concepts, *quantum states*, *quantum dynamics*, and *quantum measurements*. Because we use only quantum states and dynamics in this report, we will here explain the very basics of the two.

2.2.1. Quantum states

A quantum state is an abstract object that describes all properties of a physical system, such as energy, charge, momentum, position, and so on. Mathematically, a state is described by a unit vector $|\phi\rangle$ in a Hilbert space¹ \mathcal{H} . The dimension of the Hilbert space depends on the type of quantum systems, which can be infinite. In this report, we consider only quantum systems with finite-dimensional Hilbert spaces. Since a quantum system has different physical properties, e.g. different energy or positions, it can be in a different quantum state, while the Hilbert space itself is fixed. Thus, we sometimes understand that a Hilbert space is attached to each quantum system and that every unit vector in the Hilbert space represents a different quantum state in the system.

When there is more than one quantum system, the Hilbert space for the whole system is described by a tensor product of each Hilbert space. More concretely, if there are N quantum systems, to each of which a Hilbert space $\mathcal{H}^{(j)}$ is attached, the total Hilbert space is given by $\mathcal{H}_N = \bigotimes_{j=1}^N \mathcal{H}^{(j)}$.

2.2.2. Unitary dynamics

In physics, it is important to understand time evolution or dynamics. In quantum mechanics, the most fundamental dynamics is a *unitary dynamics*, which is described by a unitary matrix. If a quantum system is initially in a state $|\psi\rangle \in \mathcal{H}$ and evolves to another state $|\psi'\rangle \in \mathcal{H}$ after some time, then they are related by a unitary $U \in \mathcal{U}(\dim \mathcal{H})$ as $|\psi'\rangle = U|\psi\rangle$. When there are N quantum systems, the unitary dynamics of the whole system is simply described by a unitary $U \in \mathcal{U}(D)$, where D is the dimension of $\mathcal{H}_N = \bigotimes_{j=1}^N \mathcal{H}^{(j)}$.

2.3. Approximate unitary designs

We here briefly overview approximate unitary designs. We define them in the manner commonly used in quantum information science, but they should be essentially equivalent to that in mathematics. We refer to Ref. [2] for a more mathematically-friendly description of designs in quantum information science. A nice summary of various definitions of designs in quantum information science can be found in Ref. [3].

We denote by \mathbb{H} the Haar measure on $\mathcal{U}(d)$. For a given probability measure μ on $\mathcal{U}(d)$, we often denote by $\mathbb{E}_{U \sim \mu}$ a map averaging over the whole unitary group $\mathcal{U}(d)$ with respect to the measure μ . We also introduce the *diamond* norm [4].

¹More precisely, a quantum state is an element of a complex projective space. However, for a historical reason, we often claim that a state is a unit vector in a Hilbert space. We here follow this stupid convention.

Definition 1 (Diamond norm) Let \mathcal{C} be a map from $\mathcal{L}(\mathcal{H})$ to itself. The diamond norm of \mathcal{C} is defined as follows: $\|\mathcal{C}\|_{\diamond} := \sup_k \sup_{X \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H}_k)} \frac{\|(\mathcal{C} \otimes \text{id}_k)(X)\|_1}{\|X\|_1}$, where id_k is the identity map on $\mathcal{L}(\mathcal{H}_k)$, \mathcal{H}_k is a k -dimensional Hilbert space, and $\|X\|_1 := \text{tr}[\sqrt{XX^\dagger}]$ is the trace norm.

An ϵ -approximate unitary t -design ($t \in \mathbb{N}$) is then defined as follows:

Definition 2 (ϵ -approximate unitary t -designs) Let $t \in \mathbb{N}$ and $\epsilon > 0$. A probability measure ν on the unitary group $\mathcal{U}(d)$ is an ϵ -approximate unitary t -design if $\|\mathcal{G}_\nu^{(t)} - \mathcal{G}_H^{(t)}\|_{\diamond} \leq \epsilon$, where $\mathcal{G}_\mu^{(t)}$ for a probability measure μ on $\mathcal{U}(d)$ is defined by $\mathcal{G}_\mu^{(t)}(X) := \mathbb{E}_{U \sim \mu}[U^{\otimes t} X U^{\dagger \otimes t}]$ for any operator $X \in \mathcal{L}(\mathcal{H}^{\otimes t})$.

When $\epsilon = 0$, the design is said to be *exact*. Note that unitary designs are sometimes defined by probability distributions on *finite* sets of unitaries. However, we do not assume in Definition 2 that designs are finite.

3. What is important in quantum information

In quantum information science, we often consider a *qubit*, to which two-dimensional Hilbert space is attached². One qubit is a quantum analogue of one bit and is a basic unit of quantum information. When there are N qubits, the total Hilbert space is a 2^N -dimensional Hilbert space \mathcal{H}_N . For later convenience, we denote by $\mathcal{H}^{(j)}$ the two-dimensional Hilbert space of the j th qubit. So,

$$\mathcal{H}_N = \bigotimes_{j=1}^N \mathcal{H}^{(j)}. \quad (1)$$

In the following, we mostly consider this Hilbert space \mathcal{H}_N except when it is explicitly stated. Note that N is the number of qubits and changes depending on what quantum information processing we are interested in. Hence, precisely speaking, we should consider a family of Hilbert spaces $\{\mathcal{H}_N\}_{N \in \mathbb{N}}$. This is an important point but will be explicitly written only when it is needed. Note also that we are especially interested³ in a large N such as $N = O(10^{10})$.

The tensor product structure of the Hilbert space \mathcal{H}_N introduces the concept of *efficiency* of a unitary acting on \mathcal{H}_N , which is of central importance in quantum information science. We below explain this point in detail.

3.1. Efficiency of unitaries in $\mathcal{U}(2^N)$

According to quantum mechanics, the dynamics in N -qubit systems corresponding to any $U \in \mathcal{U}(2^N)$ is in principle realisable. However, some unitary dynamics are easier to implement than others from an experimental point of view, which introduces the idea of *efficiency* of unitary dynamics.

To be more concrete, we need to introduce *k-local* unitaries. As stated above, we often consider a family $\{\mathcal{H}_N\}_{N \in \mathbb{N}}$ of Hilbert spaces. Correspondingly, we consider a family $\{U_N\}_{N \in \mathbb{N}}$ of unitaries, where $U_N \in \mathcal{U}(2^N)$ is acting on $\mathcal{H}_N = \bigotimes_{j=1}^N \mathcal{H}^{(j)}$. Since it is essential to specify the Hilbert space the unitary acts on, we often explicitly denote the Hilbert spaces in the superscript of a unitary. For instance, if a unitary $u \in \mathcal{U}(2^k)$ for $k \in \mathbb{N}$ is acting on the i_1, i_2, \dots, i_k the Hilbert spaces in \mathcal{H}_N , we denote it by $u^{(i_1, i_2, \dots, i_k)}$.

²We sometimes consider a quantum system with d -dimensional Hilbert space, which is called a *qudit*. However, we consider only qubits in this report for simplicity.

³This will be understood by considering the number of bits in our computer, which is roughly $10^{11} \sim 10^{13}$.

Definition 3 (*k*-local unitaries) Let $k \in \mathbb{N}$ be constant and $\{\mathcal{H}_N\}_{N \in \mathbb{N}}$ be a family of Hilbert spaces as defined above. A family $\{U_N\}_{N \in \mathbb{N}}$ of unitaries, where $U_N \in \mathcal{U}(2^N)$ acts on \mathcal{H}_N , is called a *k*-local unitary if there exists $u \in \mathcal{U}(2^k)$ such that, for any $N \geq k$, the u is acting on $\bigotimes_{m=1}^k \mathcal{H}^{(j_m)}$ where $(j_1, \dots, j_k) \in [1, N]^k$ ($j_m \neq j_n$ for $n \neq m$), by which U_N is written in the following form:

$$U_N = u^{(j_1, \dots, j_k)} \bigotimes_{m \neq j_1, \dots, j_k} I^{(j)}, \quad (2)$$

where $I^{(j)}$ is the 2×2 identity matrix acting on the Hilbert space $\mathcal{H}^{(j)}$.

The point of *k*-local unitaries is that they act non-trivially on a constant number of qubits even when N grows. A family of unitaries $\{U_N\}_{N \in \mathbb{N}}$ is called a local unitary for short if it is *k*-local unitaries for some constant k . A product of two *k*-local unitaries, $\{U_N\}_{N \in \mathbb{N}}$ and $\{V_N\}_{N \in \mathbb{N}}$, is defined simply by $\{U_N V_N\}_{N \in \mathbb{N}}$. In the following, we often refer to a family $\{U_N\}_{N \in \mathbb{N}}$ of unitaries simply as a unitary U_N on N qubits for simplicity.

The dynamics corresponding to a local unitary, which we call *local unitary dynamics*, is important from an experimental point of view. In particular, 2-local dynamics, which are the dynamics corresponding to a 2-local unitary, are essentially the only dynamics we can implement in experiments. A basic fact is that any unitary U_N on N qubits can be written as a product of sufficiently many 2-local unitaries (see, e.g. Ref. [5]), implying that any unitary dynamics can be achieved by combining appropriate 2-local unitary dynamics. However, if the unitary is a product of a huge number of local unitaries, it takes an unrealistically long time to implement the corresponding unitary dynamics. In other words, a unitary $\{U_N\}_{N \in \mathbb{N}}$ is experimentally implementable only when it can be written as a product of a small number of 2-local unitaries.

Based on this idea, the *efficiency* of unitaries is defined.

Definition 4 (Efficient unitaries) A family of unitaries $\{U_N\}_{N \in \mathbb{N}}$ is called efficient if it can be written as a product of local unitaries, where the number of local unitaries is $O(\text{poly}(N))$. Otherwise, it is called inefficient.

The dynamics is called *efficient* if the corresponding unitary is efficient. When there are two efficient unitaries, the one with a shorter product is considered to be more efficient. We here emphasise that the concept of efficiency makes sense only when a Hilbert space has a tensor product structure and when we consider a family of unitaries over N .

In quantum information science, we always care about whether or not a given unitary U_N on N qubits is efficient. Thus, we are concerned with the following two problems:

1. how can a given unitary U_N on N qubits be decomposed into a product of local unitaries?
2. what is the minimum number of local unitaries for U_N ?

The second question arises from the fact that the decomposition of U_N into a product of local unitaries is not unique. Answering these two questions is of crucial importance in quantum information science, while it is in general a hard task to solve.

3.2. Efficient unitary designs

The situation is the same for unitary designs in quantum information. Since we are most interested in a family of unitaries $\{U_N\}_{N \in \mathbb{N}}$, our main interest is in a family $\{\nu_N\}_{N \in \mathbb{N}}$ of unitary t -designs, where ν_N is a unitary t -design in $\mathcal{U}(2^N)$. When we say unitary designs on N qubits, we implicitly mean such a family of designs.

In the same spirit as Definition 4, we can define the efficiency of constructing unitary designs. We say that construction of unitary designs on N qubits is *efficient* if each unitary in the design is efficient, that is, if each unitary has a decomposition into a product of local unitaries, where its length is $O(\text{poly}(N))$. When this is the case, we often refer to such designs as *efficient* unitary designs. Considering the fact that we can experimentally implement only efficient unitaries in realistic timescales, finding efficient unitary designs, as efficient as possible, is one of the most important problems.

We remark on the fact that the Haar measure, which is an exact t -design for any $t \in \mathbb{N}$, is highly inefficient. So, it is out of our scope in practice, although we often use it in theoretical analyses.

4. Efficient constructions of unitary designs

We here provide constructions of exact and approximate unitary t -designs, most of which are on N qubits and are efficient. We first review in Subsection 4.1 important results known in the literature of quantum information. In Subsection 4.2, efficient constructions of approximate unitary t -designs on N qubits proposed by us are explained.

Before we start, we remark on the relation between t and N in quantum information. As explained, we are often interested in a family of designs over N . On the other hand, t is typically set to be a small constant, e.g. $t = 2, 4, 8$ and so on, independent of N , which is because such t -designs are sufficient in the applications.

4.1. Previous results

For unitary 2-designs, a number of efficient constructions are known [6, 7, 8, 9, 10, 11, 12, 13, 14, 15] because of the well-known fact that the Clifford group is a 2-design, which may have been known in mathematics.

Theorem 1 (DiVincenzo, Leung, and Terhal, 2002 [6]) *The Clifford group in $\mathcal{U}(d)$, where d is not necessarily the power of 2, is an exact unitary 2-design.*

The most successful result about efficient constructions of unitary 2-designs on N qubits is the following theorem.

Theorem 2 (Cleve, Leung, Lie, and Wang, 2015 [14]) *There exist efficient constructions of exact unitary 2-designs on N qubits, where each unitary in the designs is a product of the following number of 2-local unitaries:*

- $O(N \log N)$ assuming that the extended Riemann Hypothesis is true.
- $O(N \log^2 N)$ without assuming anything.

We here make a brief comment that the Clifford group in $\mathcal{U}(2^N)$ is also an exact unitary 3-design [16, 17]. However, it fails to be an exact unitary 3-design if the degree of the unitary group is not the power of 2 [17].

In contrast to constructions of unitary 2-designs, little is known about constructions of unitary t -designs on N qubits for $t \geq 3$. For instance, no exact constructions, efficient

	# of local unitaries	It works for
Harrow and Low [18]	$O(t^3 N^4)$	$t = O(N/\log N)$
Brandao, Horodecki, and Harrow [19]	$O(t^{10} N^2)$	$t = O(\text{poly}(N))$
Nakata, Hirche, Koashi, and Winter [20]	$O(tN^2)$	$t = o(N^{1/2})$

Table 1: A comparison of three efficient constructions of approximate unitary t -designs on N qubits. The right-most column provides the condition for the construction to be efficient.

nor inefficient ones, are known for $t \geq 4$ to the best of our knowledge⁴. For approximate ones, essentially three efficient constructions are known [18, 19, 20]⁵. The comparison of three constructions is given in Table 1.

4.2. Efficient constructions of designs based on random diagonal unitaries

We here provide constructions of approximate unitary t -designs proposed in Ref. [20].

4.2.1. Constructing approximate unitary t -designs on $\mathcal{U}(d)$

We first present constructions of ϵ -approximate unitary t -designs in $\mathcal{U}(d)$ for general d . Let us introduce a *Fourier-type pair* of bases in a d -dimensional Hilbert space \mathcal{H} .

Definition 5 (Fourier-type pair of bases) *A pair of orthonormal bases (E, F) in a d -dimensional Hilbert space is called a Fourier-type pair of bases if each vector in $F = \{|f_\alpha\rangle\}_{\alpha \in [1, d]}$ is expanded in the basis of $E = \{|e_k\rangle\}_{k \in [1, d]}$ as follows:*

$$|f_\alpha\rangle = \frac{1}{\sqrt{d}} \sum_{k \in [1, d]} e^{\sqrt{-1}\theta_{k\alpha}} |e_k\rangle, \quad (3)$$

where the phases $\theta_{k\alpha} \in [0, 2\pi)$ satisfy the condition that $\forall k, l, \alpha \in [1, d]$, $\theta_{k+l, \alpha} = \theta_{k\alpha} + \theta_{l\alpha}$. In the index of θ , $+$ should be an additive operation with respect to which $[1, d]$ is an additive group.

The following are two important examples of Fourier-type pairs of bases.

Example 1 *The following pairs of bases are Fourier-type:*

1. any orthonormal basis $\{|e_k\rangle\}_{k \in [1, d]}$ in a d -dimensional Hilbert space and

$$\left\{ d^{-1/2} \sum_k \omega^{\alpha k} |e_k\rangle \right\}_{\alpha \in [1, d]}, \quad (4)$$

where ω is a d th root of unity.

2. let $G = \{|g_0\rangle, |g_1\rangle\}$ be a basis of a two-dimensional Hilbert space. Then, an orthonormal basis $G^{\otimes N} := \{\otimes_{m=1}^N |g_{j_m}\rangle\}$, where $\forall m, j_m \in \{0, 1\}$, in a 2^N -dimensional Hilbert space and $(HG)^{\otimes N} := \{\otimes_{m=1}^N H |g_{j_m}\rangle\}$, where H is the 2×2 Hadamard matrix given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (5)$$

in the basis $\{|g_0\rangle, |g_1\rangle\}$.

⁴For specific dimensions d , several exact designs for $t \geq 4$ are known [2].

⁵Very recently, new efficient designs have been proposed [21], which uses $O(N \log N)$ local unitaries.

We also introduce a unitary matrix $D^E \in \mathcal{U}(d)$ diagonal in a given orthonormal basis E with random eigenvalues:

$$D^E := \text{diag}_E(e^{\sqrt{-1}\phi_1}, e^{\sqrt{-1}\phi_1}, \dots, e^{\sqrt{-1}\phi_d}), \quad (6)$$

where each ϕ_k is independently chosen uniformly at random from $[0, 2\pi)$. This is called a random diagonal unitary in the basis of E . Explicitly, random diagonal unitaries are defined by the uniform measure on the set of all unitaries diagonal in the basis E . Note that such a set forms a subgroup of $\mathcal{U}(d)$.

Theorem 3 (Nakata, Hirche, Koashi, and Winter, 2016 [20]) *Let d, t, ℓ be natural numbers such that $d = \Omega(t^2 t!^2)$, $\epsilon > 0$, and (E, F) be a Fourier-type pair of bases in a d -dimensional Hilbert space. A random unitary $D[\ell]$ defined by*

$$D[\ell] = D_\ell^E D_{\ell-1}^F D_{\ell-1}^E D_\ell^F \dots D_1^E D_1^F D_0^E, \quad (7)$$

where D_j^E and D_j^F ($j \in [0, \ell]$) are all independent random diagonal unitaries in the basis of E and F , respectively, is an ϵ -approximate unitary t -design if

$$\ell \geq \frac{1}{\log d - 2 \log(t!)} \left(t \log d + \log(1/\epsilon) \right), \quad (8)$$

to the leading order of d and t .

4.2.2. Constructing efficient approximate unitary t -designs on N qubits

We now provide efficient approximate unitary t -designs on N qubits, of which Hilbert space is $\mathcal{H}_N = \otimes_{j=1}^N \mathcal{H}^{(j)}$. We first fix an orthonormal basis $E^{(j)}$ of $\mathcal{H}^{(j)}$ by $\{|e_0^{(j)}\rangle, |e_1^{(j)}\rangle\}$. We then denote the orthonormal basis $E^{(i)} \otimes E^{(j)}$ in $\mathcal{H}^{(i)} \otimes \mathcal{H}^{(j)}$ by $E^{(i,j)}$. We also define $u_{\text{diag}}^{(j)}(x) \in \mathcal{U}(2)$ for $x \in [0, 2\pi)$ and $u_{\text{diag}}^{(i,j)}(z) \in \mathcal{U}(4)$ for $z \in [0, 2\pi)$ by

$$u_{\text{diag}}^{(j)}(x) = \text{diag}_{E^{(j)}}(1, e^{\sqrt{-1}x}), \quad (9)$$

$$u_{\text{diag}}^{(i,j)}(z) = \text{diag}_{E^{(i,j)}}(1, 1, 1, e^{\sqrt{-1}z}), \quad (10)$$

which are diagonal in the bases of $E^{(j)}$ and $E^{(i,j)}$, respectively. Note that they are acting on $\mathcal{H}^{(j)}$ and $\mathcal{H}^{(i)} \otimes \mathcal{H}^{(j)}$, respectively. These unitaries are extended to the ones in $\mathcal{U}(2^N)$ in the same way as Eq. (2), which we denote by $U_{\text{diag}}^{(j)}(x) \in \mathcal{U}(2^N)$ and $U_{\text{diag}}^{(i,j)}(z) \in \mathcal{U}(2^N)$, respectively. They are explicitly given by

$$U_{\text{diag}}^{(j)}(x) = u_{\text{diag}}^{(j)}(x) \bigotimes_{k \neq j} I^{(k)}, \quad (11)$$

$$U_{\text{diag}}^{(i,j)}(z) = u_{\text{diag}}^{(i,j)}(z) \bigotimes_{k \neq i,j} I^{(k)}, \quad (12)$$

where $I^{(k)}$ is the 2×2 identity matrix acting on $\mathcal{H}^{(k)}$. They naturally form families $\{U_{\text{diag}}^{(j)}(x)\}_{N \in \mathbb{N}}$ and $\{U_{\text{diag}}^{(i,j)}(z)\}_{N \in \mathbb{N}}$

Using these unitaries, we define a unitary $U_{\text{diag}}(\mathbf{x}, \mathbf{z})$ on N qubits for $\mathbf{x} := (x_j)_{j \in [1, N]} \in [0, 2\pi)^N$ and $\mathbf{z} := (z_{ij})_{i \in [1, N-1], j \in [m+1, N]} \in [0, 2\pi)^{N(N-1)/2}$ as follows:

$$U_{\text{diag}}(\mathbf{x}, \mathbf{z}) = \left(\prod_{k=1}^N U_{\text{diag}}^{(k)}(x_k) \right) \left(\prod_{i=1}^{N-1} \prod_{j=i+1}^N U_{\text{diag}}^{(i,j)}(z_{ij}) \right), \quad (13)$$

which is a product of $N(N+1)/2$ local unitaries by definition. Denoting by $H^{(j)}$ a 2×2 Hadamard matrix on the Hilbert space $\mathcal{H}^{(j)}$, given in Eq. (1) in the basis $E^{(j)}$, we define the Hadamard matrix on N qubits by $H_N := \bigotimes_{j=1}^N H^{(j)}$.

We finally introduce a unitary $U_\ell(\vec{\mathbf{x}}, \vec{\mathbf{z}})$ on N qubits for $\ell \in \mathbb{N}$, $\vec{\mathbf{x}} = (\mathbf{x}_1, \dots, \mathbf{x}_\ell) \in [0, 2\pi)^{N\ell}$, and $\vec{\mathbf{z}} = (\mathbf{z}_1, \dots, \mathbf{z}_\ell) \in [0, 2\pi)^{N(N-1)\ell/2}$ by

$$U_\ell(\vec{\mathbf{x}}, \vec{\mathbf{z}}) = \left(\prod_{l=1}^{\ell-1} U_{\text{diag}}(\mathbf{x}_l, \mathbf{z}_l) H_N \right) U_{\text{diag}}(\mathbf{x}_\ell, \mathbf{z}_\ell) \quad (14)$$

$$= U_{\text{diag}}(\mathbf{x}_1, \mathbf{z}_1) H_N \dots U_{\text{diag}}(\mathbf{x}_{\ell-1}, \mathbf{z}_{\ell-1}) H_N U_{\text{diag}}(\mathbf{x}_\ell, \mathbf{z}_\ell). \quad (15)$$

Based on this unitary, efficient ϵ -approximate unitary t -designs on N qubits can be constructed.

Theorem 4 (Nakata, Hirche, Koashi, and Winter, 2016 [20]) *Let $N, \ell, t = o(N^{1/2})$ be natural numbers, and $\mathcal{V}[t, \ell]$ be a finite set of unitaries in $\mathcal{U}(2^N)$ given by*

$$\mathcal{V}[t, \ell] := \left\{ U_\ell(\vec{\mathbf{x}}, \vec{\mathbf{z}}) : \vec{\mathbf{x}} \in \{2\pi m/(t+1) : m \in [0, t]\}^{N\ell}, \vec{\mathbf{z}} \in \{2\pi m/(\lfloor t/2 \rfloor + 1) : m \in [0, \lfloor t/2 \rfloor]\}^{N(N-1)\ell/2} \right\}. \quad (16)$$

Then, the uniform distribution over $\mathcal{V}[t, \ell]$ is an ϵ -approximate unitary t -design on N qubits if

$$\ell \geq 2\left(t + \frac{1}{N} \log_2 1/\epsilon\right) + 1, \quad (17)$$

to the leading order of N and t .

Note that, by construction, each unitary $U_\ell(\vec{\mathbf{x}}, \vec{\mathbf{z}})$ in $\mathcal{V}[t, \ell]$ is a product of roughly ℓN^2 local unitaries. By setting $\ell = 2\left(t + \frac{1}{N} \log_2 1/\epsilon\right) + 1$, we obtain from Theorem 4 an efficient ϵ -approximate unitary t -design on N qubits, where $\approx tN^2$ local unitaries are needed.

5. Combinatorial problems

In this section, we present two combinatorial problems. One of them is the key problem in the proof of Theorem 4 (see Ref. [20]) and may also be of mathematical interest. The other is not directly related to the construction of designs, but we hope that it is also interesting.

5.1. Local permutation check problems

Let $t, N \in \mathbb{N}$, $K = (K_{sm})_{s \in [1, t], m \in [1, N]}$ and $K' = (K'_{sm})_{s \in [1, t], m \in [1, N]}$ be $t \times N$ matrices with elements in $\{0, 1\}$. For given $s \in [1, t]$ and $I \subset [1, N]$, we denote a subsequence $(K_{sm})_{m \in I}$ of the s th row of K by K_{sI} , and a set $(K_{sI})_{s \in [1, t]}$ of such subsequences over all s by K_I . We use the same notation also for K' . Let Ω be a canonical map that rearranges the subsequences K_I in ascending order, where the subsequences are regarded as binary numbers. For $\mathcal{I} = \{I_j\}$ ($\forall j, I_j \subset [1, N]$), we say that K is an \mathcal{I} -local permutation of K' if $\forall I_j \in \mathcal{I}, \Omega(K_{I_j}) = \Omega(K'_{I_j})$. We say K is a row permutation of K' if $\Omega(K_I) = \Omega(K'_I)$ for $I = [1, N]$, which simply implies that a set of rows of K is a permutation of that of K' . Using this notation, we define local permutation check problems as follows.

Definition 6 (Local permutation check problems) Let $t, N \in \mathbb{N}$, K and K' be $t \times N$ matrices with elements in $\{0, 1\}$. For a given $\mathcal{I} = \{I_j\}$ ($\forall j, I_j \subset [1, N]$), the task of the \mathcal{I} -local permutation check problem is to count the number of pairs (K, K') such that K is not a row permutation but an \mathcal{I} -local permutation of K' . We denote the number of such pairs by $\Lambda_{t \times N}(\mathcal{I})$.

We are interested in the quantity $L(t, N, k, \lambda)$ defined by, for $t, N, k, \lambda \in \mathbb{N}$,

$$L(t, N, k, \lambda) := \min\{J : \exists \mathcal{I} = \{I_j\}_{j=1}^J, \text{ such that } \forall j \in [1, J], I_j \subset [1, N], |I_j| \leq k, \text{ and } \Lambda_{t \times N}(\mathcal{I}) \leq \lambda\}. \quad (18)$$

When there does not exist \mathcal{I} that satisfies the conditions, we define $L(t, N, k, \lambda) = \infty$. A preliminary result is given below:

Theorem 5 (Nakata, Murao, and Koashi, 2014 [22]) Let t, N and k be natural numbers. Then,

$$L(t, N, k, 0) = \begin{cases} \infty & \text{when } k \leq N - 1 \text{ and } t \geq 2^N, \\ \infty & \text{when } k \leq \lfloor \log_2 t \rfloor \text{ and } t \leq 2^N - 1, \\ {}_N C_k & \text{when } k = \lfloor \log_2 t \rfloor + 1 \text{ and } t \leq 2^N - 1, \\ 1 & \text{when } k \geq N, \end{cases} \quad (19)$$

where ${}_N C_k$ is a binomial coefficient.

The reason why we care about $L(t, N, k, \lambda)$ is that it is related to the efficiency of the constructions of approximate unitary t -designs on N qubits based on random diagonal unitaries (see Ref. [20] for details). In Ref. [20], we especially considered the case of $k = 2$ and have proved the following theorem:

Theorem 6 (Nakata, Hirche, Koashi, and Winter, 2016 [20]) Let $N, t \in \mathbb{N}$, and $\mathcal{I}_2(N) := \{\{m, n\} : m \in [1, N - 1], n \in [m + 1, N]\}$. Then, $\Lambda_{t \times N}(\mathcal{I}_2(N)) \leq 2^{2t^2 + (t-1)N}$.

Theorem 6 implies that, for any $N \in \mathbb{N}$, $L(t, N, 2, 2^{2t^2 + (t-1)N}) \leq |\mathcal{I}_2(N)| = N(N - 1)/2$, which was used to obtain Theorem 4.

One of the important open problems about $L(t, N, k, \lambda)$ is whether there exists a constant k independent of N such that $L(t, N, k, \lambda_t 2^{(t-1)N}) = O(N \log N)$, where λ_t can depend on t but not on N (here, t is presumably independent of N). We are very interested in this problem, and any suggestion will be appreciated.

5.2. Covering a hypercube by hyperplanes

We finally provide an interesting problem about covering a hypercube by hyperplanes. A variant of the problem is used in the proof of Theorem 6.

Let $n \in \mathbb{N}$, and $\mathbb{H}^n = \{0, 1\}^n \subset \mathbb{R}^n$ be the n -dimensional hypercube, hence $|\mathbb{H}^n| = 2^n$. The question is what can be its intersection with a k -dimensional linear subspace S of \mathbb{R}^n , namely,

$$H(n, k) := \{t > 0 : \exists k\text{-dimensional hyperplane } S, t = |\mathbb{H}^n \cap S|\}. \quad (20)$$

In Ref. [23], the following quantity was particularly studied:

$$H(\infty, k) := \bigcup_{n \geq k} H(n, k), \quad (21)$$

about which some observations were obtained. For instance,

$$[1, 6] \cup \{8\} \subset H(\infty, 3) \quad (22)$$

$$[1, 10] \cup \{12, 16\} \subset H(\infty, 4) \quad (23)$$

$$[1, 18] \cup \{20, 24, 32\} \subset H(\infty, 5). \quad (24)$$

From these instances, Melo and Winter succeeded to prove the following.

Theorem 7 (Melo and Winter, 2017 [23]) *For any $k \geq 2$, the second largest number in $H(\infty, k)$ is $3 \cdot 2^{k-2}$. It is contained in $H(n, k)$ for all $n > k$.*

They also made a conjecture as follows:

Conjecture 1 (Melo and Winter, 2017 [23])

$$\forall k \in \mathbb{Z}^+, [1, 2^{k-1} + 2] \subset H(\infty, k), \quad (25)$$

which is true at least when $k \leq 5$.

6. Summary

In this report, we have overviewed unitary designs in quantum information science. Although a number of ideas, including definitions, were imported from design theory, designs in quantum information science have developed in a direction slightly different from mathematics. This is mainly because quantum information science has severe restrictions, *local unitaries* and *efficiency*, and we are always interested in efficient constructions of (mostly approximate) unitary designs. We have briefly mentioned that three efficient unitary designs on N qubits have been proposed in quantum information. We have also presented two combinatorial problems, which are not only relevant to efficient constructions of designs but also interesting from the mathematical point of view.

We are still looking for more efficient constructions of designs, which helps the development of quantum information technology. Towards this goal, more and more collaborations between mathematics and quantum information science are desired. We hope this report will motivate such fruitful collaborations.

References

- [1] R. Landauer. Information is Physical. *Physics Today*, 44(5):23, January 2008.
- [2] A. Roy and A. J. Scott. Unitary designs and codes. *Des. Codes Cryptogr.*, 53(1):13–31, 2009.
- [3] R. A. Low. *Pseudo-randomness and learning in quantum computation*. PhD thesis, University of Bristol, 2010. arXiv:1006.5227.
- [4] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society Boston, MA, USA, 2002.
- [5] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm. *arXiv:quant-ph/0505030*, 2005.
- [6] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48:580, 2002.
- [7] W. G. Brown, Y. S. Weinstein, and L. Viola. Quantum pseudorandomness from cluster-state quantum computation. *Phys. Rev. A*, 77(4):040303(R), 2008.

- [8] Y. S. Weinstein, W. G. Brown, and L. Viola. Parameters of pseudorandom quantum circuits. *Phys. Rev. A*, 78(5):052332, 2008.
- [9] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *J. of Math. Phys.*, 48(5):052104, 2007.
- [10] G. Tóth and J. J. García-Ripoll. Efficient algorithm for multiqubit twirling for ensemble quantum computation. *Phys. Rev. A*, 75(4):042311, 2007.
- [11] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, 2009.
- [12] A. W. Harrow and R. A. Low. Random quantum circuits are approximate 2-designs. *Commun. Math. Phys.*, 291:257, 2009.
- [13] I. T. Diniz and D. Jonathan. Comment on “Random quantum circuits are approximate 2-designs”. *Commun. Math. Phys.*, 304:281, 2011.
- [14] R. Cleve, D. Leung, L. Liu, and C. Wang. Near-linear constructions of exact unitary 2-designs. *Quant. Info. & Comp.*, 16(9 & 10):0721–0756, 2016.
- [15] Y. Nakata, C. Hirche, C. Morgan, and A. Winter. Implementing unitary 2-designs using random diagonal-unitary matrices. *J. Math. Phys.*, 58(5):052203, 2017.
- [16] Z. Webb. The Clifford group forms a unitary 3-design. *Quant. Info. & Comp.*, 16(15 & 16):1379–1400, 2016.
- [17] H. Zhu. Multiqubit Clifford groups are unitary 3-designs. *Phys. Rev. A*, 96(062336), 2017.
- [18] A. W. Harrow and R. A. Low. Efficient Quantum Tensor Product Expanders and k -Designs. In *Proc. RANDOM’09*, number 5687, pages 548–561, 2009.
- [19] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.*, 346(2):397–434, 2016.
- [20] Y. Nakata, C. Hirche, M. Koashi, and A. Winter. Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics. *Phys. Rev. X*, 7(2):021006, 2017. see also arXiv:1609.07021.
- [21] A. Harrow and S. Mehraban. Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates. *arXiv:1809.06957*, 2018.
- [22] Y. Nakata, M. Koashi, and M. Muraio. Generating a state t -design by diagonal quantum circuits. *New J. Phys.*, 16:053043, 2014.
- [23] N. Melo and A. Winter. Intersection patterns of linear subspaces with the hypercube. *arXiv:1712.01763*, 2017.

On unitary designs and codes

坂内英一 (Eiichi Bannai)

Kyushu University (emeritus)

and

TGMRC (Three Gorges Mathematical Research Center, Yichang)

October 8, 2018

この原稿は広島における第35回代数学組合せ論シンポジウムの著者の講演のスライドをかなり忠実に再現したものです。英語と日本語のちゃんぽんになっていますがご了承ください。

基本的文献

- [1] Delsarte-Goethals-Seidel: Spherical codes and designs, *Geom. Dedicata* (1977)
- [2] Roy-Suda: Complex spherical codes and designs, *J. of Comb. Designs* (2014)
- [3] Roy-Scott: Unitary codes and designs, *Designs, Codes and Cryptography* (2009)

更に次の文献も参照してください。

- (i) Gross-Audenaert-Eisert: Evenly distributed unitaries: on the structure of unitary designs, *J. Math. Phys.* (2007),
- (ii) Scott: Optimizing quantum process tomography and unitary 2-designs, *J. of Physics A* (2008),
- (iii) Zhu-Kueng-Grassl-Gross: The Clifford group fails gracefully to be unitary 4-design, [arXiv:1609.08172v1](https://arxiv.org/abs/1609.08172v1).

§1. Unitary t -design (Cf. Roy-Scott, 2009).

A finite set $X \subset U(d)$ is called a unitary t -design
 $\iff \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU = \frac{1}{|X|} \sum_{U \in X} U^{\otimes t} \otimes (U^*)^{\otimes t},$
 (where $\int_{U(d)} dU = 1$)
 $\iff \frac{1}{|X|^2} \sum_{U, V \in X} |\text{tr}(U^*V)|^{2t} = \int_{U(d)} |\text{tr}(U)|^{2t} dU$

$\iff \int_{U(d)} f(U) du = \frac{1}{|X|} \sum_{U \in X} f(U),$
 for all $f \in \text{Hom}(U(d), t, t),$
 (and many other equivalent definitions).

Here, $\text{Hom}(U(d), r, s) =$ the space of polynomials that are homogeneous of degree r in the matrix entries of U , and homogeneous of degree s in the matrix entries of $U^*.$

§2. Irreducible representations of $U(d).$

Parametrized by the non-increasing length- d integer sequences:

$\mu = (\mu_1, \mu_2, \dots, \mu_d)$ with $\forall \mu_i \in \mathbb{Z}, \mu_1 \geq \mu_2 \geq \dots \geq \mu_d.$

The degree of the representation μ is given by

$$d_\mu = \prod_{1 \leq i < j \leq d} \frac{\mu_i - \mu_j + j - i}{j - i}.$$

(Note that $d_{(1,0,\dots,0)} = d.$)

• The irreducible representations of $U(d)$ appearing in $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d*})^{\otimes s}$ are those $\mu = (\mu_1, \mu_2, \dots, \mu_d)$ with

$|\mu| = |\mu_1 + \mu_2 + \dots + \mu_d| = r - s$ and $|\mu_+| \leq r,$

where $\mu_+ =$ the sum of those positive μ_i 's.

• $\dim(\text{Hom}(U(d), r, s)) = D(d, r, s) = \sum_{|\mu|=r-s, |\mu_+| \leq r} d_\mu^2.$

$D(d, 0, 0) = 1,$

$D(d, 1, 1) = (d^2 - 1)^2 + 1 = d^4 - 2d^2 + 2,$

$D(d, 2, 2) = \frac{1}{4}(d^8 - 6d^6 + 25d^4 - 28d^2 + 16),$

$D(d, 3, 3) = \frac{1}{36}(d^{12} - 12d^{10} + 103d^8 - 378d^6 + 778d^4 - 600d^2 + 252),$

• $X \subset U(d)$ is a $2s$ -design $\implies |X| \geq D(d, s, s).$

• We call $X \subset U(d)$ to be a **tight** $2s$ -unitary design, if X is a $2s$ -design with $|X| = D(d, s, s).$

• Let $A(X) = \{|tr(U^*V)|^2 \mid U, V \in X, U \neq V\}.$

• We say X is an s -distance set (or an s -code) in $U(d)$, if $|A(X)| = s.$

• If $|A(X)| = s,$ then $|X| \leq D(d, s, s).$

• It is shown that if X satisfies $|A(X)| = s$ and $|X| = D(d, s, s)$ then X is a $2s$ -design.

However, it seems it is not clear, whether X is a tight $2s$ -design implies that X is an s -distance set, except when $s = 1$ (*i.e.*, $t = 2$).

Perhaps, similar as it was discussed in Roy-Suda (Complex spherical designs and codes), the right definition of an s -code is that there is an annihilator polynomial $f(\lambda)$ for X with $f(\lambda) \in \text{Hom}(U(d), s, s)$ (but $f(\lambda)$ is a function on $U(d)$ with many variables). Note that an s -distance set is a very special case of an s -code in this sense.

We are interested in the classification problem of tight unitary t -designs in $U(d)$. (Here, we assume $t = 2s \geq 2$, unless otherwise stated.)

Remarks. No example of tight unitary t -design, for any $t = 2s \geq 2$, is known.

(i) Gross-Audenaert-Eisert conjectures that there is no tight unitary 2-design. Moreover, they conjecture that the actual lower bound of the size of unitary 2-designs is $d^4 - d^2$ (rather than $D(d, 1, 1) = (d^2 - 1)^2 + 1 = d^4 - 2d^2 + 2$).

§3. Tight unitary $2s$ -designs.

We would like to study tight unitary $2s$ -designs for all $s \geq 1$. However, we start with some special cases.

Our first attempt (result) by Eiichi Bannai and Etsuko Bannai.

(i) There exists no tight unitary 4-design which is a 2-distance set.

(ii) There exists no tight unitary 6-design which is a 3-distance set.

(Can we generalize the proof for $2s$ -design which is an s -distance set for $s \geq 4$?)

Note that it is not clear whether an A. S. of class s with relations given by $A(X)$ is always attached with a tight unitary $2s$ -design X .

(This is true for $s = 2$, but it seems open for larger s).

However, we can use the following formulas (Cf. A. J. Scott (2009)).

Let X be a tight $2s$ -design in $U(d)$. We assume that $d \geq t = 2s$.

Then $|X| = D(d, s, s) = f(d)$ (an explicit polynomial of degree $4s$.)

Let $A(X) = \left\{ |tr(U^*V)|^2 \mid U, V \in X, U \neq V \right\} = \left\{ \alpha_1, \alpha_2, \dots, \alpha_s \right\}$.

and let $K_i = |\{(U, V) \mid |tr(U^*V)|^2 = \alpha_i\}|/|X|$ (for $i = 1, 2, \dots, s$).

Then

$$1 + K_1 + K_2 + \dots + K_s = f(d)(= |X|)$$

and

$$d^{2j} + \alpha_1^j K_1 + \alpha_2^j K_2 + \dots + \alpha_s^j K_s = j! f(d)$$

holds for $j = 1, 2, \dots, 2s$.

So, there are $2s + 1$ equations and $2s + 1$ variables:

$K_1, K_2, \dots, K_s, \alpha_1, \alpha_2, \dots, \alpha_s$ and d .

(At least) for $s = 2, 3$, we can eliminate the variables except d , and get a single equation which involves only d . We get the contradiction from the integral condition on d .

The above calculations are fairly involved, and it was not so easy for us to generalize this result for larger s .

We visited ICERM (Brown University, Providence, R.I.) in this April, and met Ziqing Xiang (University of Georgia). So, I asked him whether he can do for general s .

He solved the problem almost completely.

§4. The work of Ziqing Xiang.

We will sketch the argument of Ziqing Xiang.

For a vector $\vec{a} = (a_0, a_1, \dots, a_{2s})$. The Hankel matrix $H(\vec{a})$ is the symmetric matrix of size $(s + 1) \times (s + 1)$ whose entries are defined by

$$H(\vec{a})_{i,j} = a_{i+j} \text{ with } 0 \leq i, j \leq s.$$

Lemma. Let n, s, b and c_ℓ ($0 \leq \ell \leq 2s$) be some constant. Consider the system of equations

$$b^\ell + \sum_{i=1}^s K_i \alpha_i^\ell = n c_\ell \text{ where } 0 \leq \ell \leq 2s.$$

If it has solutions in K_i and α_i and the Hankel matrix $H(\vec{c})$ associated with $\vec{c} = (c_0, c_1, \dots, c_{2s})$ is invertible. Then

$$n = (b^0, b^1, \dots, b^{2s}) H(\vec{c})^{-1} {}^t(b^0, b^1, \dots, b^{2s}).$$

Proof. For a real number α , let $H(\alpha)$ be the Hankel matrix associated to $(\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{2s})$. Then

$$H(\alpha_i) = H((\alpha_i^0, \alpha_i^1, \alpha_i^2, \dots, \alpha_i^{2s})) \text{ has rank at most } 1.$$

Therefore

$$\sum_{i=1}^s K_i H(\alpha_i) \text{ has rank at most } s.$$

Then

$$\begin{aligned} 0 &= \det \left(\sum_{i=1}^s K_i H(\alpha_i) \right) = \det \left(H((c_\ell n - b^\ell)) \right) \\ &= \det \left(n H((c_\ell)) - {}^t(b^0, b^1, \dots, b^s) (b^0, b^1, \dots, b^s) \right) \end{aligned}$$

$$\begin{aligned}
&= \det(nH((c_\ell))) \\
&\quad \times (1 - (b^0, b^1, \dots, b^s) (nH((c_\ell)))^{-1} {}^t(b^0, b^1, \dots, b^s)) \\
&\quad \text{(matrix determinant lemma)} \\
&= n^s \det(H((c_\ell))) \\
&\quad \times (n - (b^0, b^1, \dots, b^s) H((c_\ell))^{-1} {}^t(b^0, b^1, \dots, b^s)).
\end{aligned}$$

Corollary. Let X be an s -distance $2s$ -design in $U(d)$. Then,

$$|X| = (d^0, d^2, d^4, \dots, d^{2s}) H((c_\ell))^{-1} {}^t(d^0, d^2, d^4, \dots, d^{2s}).$$

Proof. Consider the system of equations:

$$d^{2\ell} + \sum_{i=1}^s K_i a_i^\ell = n\ell!$$

where $0 \leq \ell \leq 2s$. Then apply the previous Lemma. Note that $H((c_\ell)) = H((\ell!))$ is shown to be invertible.

Main Theorem (Ziqing Xiang). Suppose that $s \geq 2$ be fixed. With at most $4s - 2$ exceptional $d \geq 2s$, there are no s -distance $2s$ -design on $U(d)$.

Note that the classification of tight $2s$ -design is still open. Also, the case $s = 1$ (i.e., the classification of 1-distance tight 2-design is still open).

Sketch of Proof.

(i) It is calculated that

$$\begin{aligned}
|X| &= (d^0, d^2, d^4, \dots, d^{2s}) \cdot H((c_\ell))^{-1} \cdot {}^t(d^0, d^2, d^4, \dots, d^{2s}) \\
&= \frac{1}{(s!)^2} (d^{4s} - 2s^2 d^{4s-2} + O(d^{4s-3})).
\end{aligned}$$

(ii) It is calculated that

$$D(d, s, s) = \frac{1}{(s!)^2} (d^{4s} - s(s+1)d^{4s-2} + O(d^{4s-3})).$$

Since X is an s -distance $2s$ -design, $|X| = D(d, s, s)$. So, we should have

$$|X| = \frac{1}{(s!)^2} (d^{4s} - 2s^2 d^{4s-2} + O(d^{4s-3})) = \frac{1}{(s!)^2} (d^{4s} - s(s+1)d^{4s-2} + O(d^{4s-3})).$$

Both $D(d, s, s)$ and $(d^0, d^2, d^4, \dots, d^{2s}) H((c_\ell))^{-1} {}^t(d^0, d^2, d^4, \dots, d^{2s})$ are shown to be polynomials in d . So, there are at most $4s - 2$ exceptional d . **Q.E.D.**

§5. Discussion.

So far, the concept of s -distance set X in $U(d)$ was defined by

$$|A(X)| = \{|\text{tr}(U^*V)|^2 \mid U, V \in X, U \neq V\} = s.$$

Is this appropriate?

The following possible definition was suggested by Ziqing Xiang. Namely, How about defining

$$|B(X)| = |\{\text{Re}(\text{tr}(U^*V)) \mid U, V \in X, U \neq V\}| = s.$$

The reason why this definition may be interesting is as follows.

For $U, V \in U(d)$, let $\langle U, V \rangle := \text{tr}(U^*V)$. Then $\|U\| := \sqrt{\langle U, U \rangle}$. Then $\text{dist}(U, V) := \|U - V\|$ seems to be a natural distance on $U(d)$.

Please note that for $U, V \in U(d)$,

$$\begin{aligned} \text{dist}(U, V)^2 &= \|U - V\|^2 = \langle U - V, U - V \rangle = \text{tr}((U - V)^*(U - V)) \\ &= \text{tr}(U^*U + V^*V - U^*V - (U^*V)^*) = 2d - 2\text{Re}(\text{tr}(U^*V)). \end{aligned}$$

§6. Our further study.

Let us set $B(X) = \{a_1, a_2, \dots, a_s\}$ (i.e., an s -distance set in our new sense), and let

$$K_i = |\{(U, V) \mid \text{Re}(\text{tr}(U^*V)) = a_i\}|/|X| \quad (\text{with } i = 1, 2, \dots, s).$$

Then

$$1 + K_1 + K_2 + \dots + K_s = f(d) (= |X| = D(d, s, s)),$$

$$d^i + K_1 a_1^i + K_2 a_2^i + \dots + K_s a_s^i = 0, \quad \text{if } i = \text{odd}, 1 \leq i \leq 2s - 1,$$

$$d^i + K_1 a_1^i + K_2 a_2^i + \dots + K_s a_s^i = i! \frac{\binom{i/2}{2}}{2^i} f(d), \quad \text{if } i = \text{even}, 2 \leq i \leq 2s.$$

Theorem. There is no X in $U(d)$ which is an s -distance set in our new sense, i.e., $|B(X)| = s$, and $2s$ -design, for $s = 1$ and $s = 2$.

Remarks. (i) The method is similar to the one used to prove the non-existence proof of 2-distance 4-design on $U(d)$.

(ii) It is expected that the proof would be generalized for all $s \geq 1$, although we have not completed the proof yet.

The Problems we are trying to work.

(i) Let X be a tight $2s$ -design in $U(d)$. It would be nice if it could be shown that

(a) X is an s -distance set with $|A(X)| = s$, or

(b) X is an s -distance set with $|B(X)| = s$.

(However, it seems very difficult to show this. Also, it is not clear whether this actually

holds.)

(ii) The following result holds.

Proposition (Suda). Let X be a 2-distance 2-design in $U(d)$, then a strongly regular graph is naturally attached.

Question. (i) Is it true that if X is an s -distance $2s - 2$ design in $U(d)$, then an A. S. of class s is naturally attached?

In particular, is it true that if X is an s -distance $2s$ -design (so, tight $2s$ -design) in $U(d)$ then an A. S. of class s is naturally attached?

(So far, these questions seem to be open.)

We could determine the possible feasible list of such strongly regular graphs (with small sizes) coming from 2-distance 2-design in $U(d)$. We tried to find some explicit examples of 2-distance (with $|A(X)| = 2$) unitary 2-design.

(An explicit unitary 2-design giving a strongly regular graph was found (Suda) in this way. (We expect further examples.)

(iii) We can consider the same question, for 2-distance (with $|B(X)| = s$) 2-designs in $U(d)$.

§7. Study of unitary t -designs from the view point of finite groups.

最後に $U(d)$ の有限部分群自身が unitary t -design になっている場合を考えよう。

Let G be a finite subgroup of $U(d)$.

Let $\rho : G \rightarrow U(d)$ be a representation of G , and let χ be the character of the representation ρ .

Then G is called a unitary t -design group, if

$$\frac{1}{|G|} \sum_{g \in G} |\chi(g)|^{2t} = \int_{U(d)} |\text{tr}(U)|^{2t} dU.$$

For $d \geq 3$, it seems no unitary 4-design group G is known.

Obviously, unitary t -design group G is a unitary t -design on $U(d)$.

Clifford groups $Z_8 * 2_+^{1+2m} Sp(2m, 2)$ on $U(2^m)$ are known to be a unitary 3-design group, but not a unitary 4-design group.

Some examples of unitary 3-design groups in $U(d)$.

$d = 3$, $3.A_6$,

$d = 3$, $6.A_7$,

$d = 6$, $6.L_3(4).2_1$,

$d = 12$, $6.Suz$,

$d = 18, 3.J_3$, etc.

$G = 6.Suz$ is very close to a unitary 4-design.

Let $\gamma(t, d) = \int_{U(d)} |tr(U)|^{2t}$. Then $\gamma(4, 12) = 24$, while $\frac{1}{|G|} \sum_{U \in G} |tr(U)|^8 = 25$.

I am wondering whether we can construct unitary 4-designs from $G = 6.Suz$.

• Let ρ be the natural representation of degree d of $U(d)$.

Let $G = 6.Suz$. Then G is known to be a unitary 3-design group in $U(12)$. Moreover, Then $(1, \rho^{\otimes 4} \otimes (\rho^*)^{\otimes 4})_{U(12)} = (\rho^{\otimes 4}, \rho^{\otimes 4})_{U(12)} = 24$, while $(1, \rho^{\otimes 4} \otimes (\rho^*)^{\otimes 4})_G = (\rho^{\otimes 4}, \rho^{\otimes 4})_G = 25$. This implies that there is a unique G -invariant, but not $U(12)$ -invariant $f(z) = f(z, \bar{z}) \in \text{Hom}(U(12), 4, 4)$. Let $x_0 \in U(d)$ be a zero of $f(z)$. Then, if we consider X to be the orbit of $x_0 \in U(12)$ by the action of $G \times G \subset U(12) \times U(12)$, it is a unitary 4-design on $U(12)$. (new result !)

以上に書いたことはシンポジウムの講演の時点で分かっていたことでした。その後 unitary t -design group の分類に関しては、群論的に（有限単純群の分類も用いて） $d \geq 3$ の場合の unitary 4-design group の非存在が示され、更に unitary 2-design group の完全な分類も得られたと思われまます。これに関しては、Eiichi Bannai, Gabriel Navarro, Noelia Rizo, Pham Huu Tiep の4名の共著論文を準備中です。（乞うご期待。）
(追記。The arXiv number is: arXiv: 1810.02507.)

Acknowledgment. The author thanks Ziqing Xiang for allowing the author to sketch the idea of his unpublished work in this workshop and also in this report.

The generalized wreath product of triply-regular association schemes

Yuta Watanabe*

National Institute of Technology, Ube College

1 Notation

In this section, we set up notation and terminology on association schemes and posets. For the definition of association schemes, see [2, 3, 5], and for the theory of posets, see [4].

Let \mathbb{F} be a field. For a finite set Ω , we will denote by $\text{Mat}_\Omega(\mathbb{F})$ the set of matrices whose rows/columns indexed by Ω and whose entries are in \mathbb{F} . For simplicity of notation, we will use the symbols J_Ω, I_Ω to denote the all-ones matrix and the identity matrix in $\text{Mat}_\Omega(\mathbb{F})$, respectively. For a subset \mathbf{A} of $\text{Mat}_\Omega(\mathbb{C})$, we write $\text{Span}_{\mathbb{F}} \mathbf{A}$ for the linear span of \mathbf{A} over \mathbb{F} . An *association scheme* on a finite set Ω is the set \mathbf{A} of $(0, 1)$ -matrices in $\text{Mat}_\Omega(\mathbb{F})$ satisfying the conditions:

1. The sum of all matrices in \mathbf{A} is the all-ones matrix J_Ω ;
2. \mathbf{A} contains the identity matrix I_Ω ;
3. \mathbf{A} is closed under taking matrix transpose;
4. $\text{Span}_{\mathbb{F}} \mathbf{A}$ is closed under matrix multiplication.

By definition, the set $\text{Span}_{\mathbb{F}} \mathbf{A}$ becomes an algebra over \mathbb{F} and we call it the *adjacency algebra* of \mathbf{A} . Fix an element $\omega \in \Omega$. For a matrix $A \in \mathbf{A}$, the notation $\sigma_\omega(A)$ means the diagonal matrix in $\text{Mat}_\Omega(\mathbb{F})$ whose diagonal entry is given by the ω -th row of A . This diagonal matrix is called the *dual idempotent* of \mathbf{A} with respect to ω . Let \mathbf{E}^* denote the set of all dual idempotents of \mathbf{A} with respect to ω . For simplicity of notation, we write $D_\omega = \sigma_\omega(I_\Omega)$, whose (ω, ω) -entry is 1 and 0 everywhere else. Observe that $\text{Span}_{\mathbb{F}} \mathbf{E}^*$ becomes an algebra over \mathbb{F} and we call it the *dual adjacency algebra* of \mathbf{A} with respect to ω . An association scheme \mathbf{A} on a finite set Ω is called *triply-regular* if the set

$$\mathcal{T} = \text{Span}_{\mathbb{F}} \{E^* A F^* \mid E^*, F^* \in \mathbf{E}^*, A \in \mathbf{A}\}$$

*Email: ywatanabe@ube-k.ac.jp

is closed under matrix multiplication for every $\omega \in \Omega$. In this case, the algebra \mathcal{T} is called the *Terwilliger algebra* with respect to ω .

Let (X, \leq) be a nonempty finite poset. A subset Y in X is called an *anti-chain* if any two elements in Y is incomparable. For an anti-chain Y in X , the *down-set* of Y (also known as the *order ideal*) is defined to be

$$\text{Down}(Y) = \{x \in X \mid x < y \text{ for some } y \in Y\}.$$

Note that this definition follows [1] and differs from [4], where $\text{Down}(Y) \cup Y$ is called the down-set of Y .

2 The generalized wreath products

In this section, we review the generalized wreath product of association schemes introduced by R. A. Bailey [1] in 2006. Let X be a finite poset. For each $x \in X$, let \mathbf{A}_x be an association scheme on a finite set Ω_x . Put $\Omega = \prod_{x \in X} \Omega_x$. In this section, we fix an element $\omega = (\omega_x)_{x \in X} \in \Omega$. For each $x \in X$, let \mathbf{E}_x^* denote the set of dual idempotents of \mathbf{A}_x with respect to ω_x . We write the adjacency algebra $\mathcal{A}_x = \text{Span}_{\mathbb{F}} \mathbf{A}_x$ and the dual adjacency algebra $\mathcal{A}_x^* = \text{Span}_{\mathbb{F}} \mathbf{A}_x^*$.

For an anti-chain Y in X , let $\mathbf{A}(Y)$ be the set of matrices in $\text{Mat}_{\Omega}(\mathbb{F})$ of the following form:

$$\bigotimes_{x \in \text{Down}(Y)} J_{\Omega_x} \otimes \bigotimes_{y \in Y} A_y \otimes \bigotimes_{z \in X \setminus (Y \cup \text{Down}(Y))} I_{\Omega_z}, \quad (1)$$

where $A_y \in \mathbf{A}_y \setminus \{I_y\}$ for each $y \in Y$. Then let \mathbf{A} denote the union of $\mathbf{A}(Y)$ for all anti-chains Y in X .

Theorem 1 ([1, Theorem 1]). *With above notation, the union \mathbf{A} is an association scheme on Ω .*

The association scheme in Theorem 1 is called the generalized wreath product of association schemes \mathbf{A}_x over the poset X .

Example 2. *Let $X = \{1, 2\}$ be a poset with $1 < 2$. The set of adjacency matrices corresponding to each anti-chain in the poset X is given as follows.*

anti-chain Y	$\text{Down}(Y)$	$\mathbf{A}(Y)$
\emptyset	\emptyset	$\{I_{\Omega_1} \otimes I_{\Omega_2}\}$
$\{1\}$	\emptyset	$\{A_1 \otimes I_{\Omega_2} \mid A_1 \in \mathbf{A}_1 \setminus \{I_{\Omega_1}\}\}$
$\{2\}$	$\{1\}$	$\{J_{\Omega_1} \otimes A_2 \mid A_2 \in \mathbf{A}_2 \setminus \{I_{\Omega_2}\}\}$

Therefore, the generalized wreath product of association schemes $\{\mathbf{A}_1, \mathbf{A}_2\}$ over the poset X is the (ordinary) wreath product $\mathbf{A}_1 \wr \mathbf{A}_2$.

Example 3. *Let $X = \{a, b\}$ be a poset with $a \not< b$. The set of adjacency matrices corresponding to each anti-chain in the poset X is given as follows.*

<i>anti-chain</i> Y	$\text{Down}(Y)$	$\mathbf{A}(Y)$
\emptyset	\emptyset	$\{I_{\Omega_a} \otimes I_{\Omega_b}\}$
$\{a\}$	\emptyset	$\{A_a \otimes I_{\Omega_b} \mid A_a \in \mathbf{A}_a \setminus \{I_{\Omega_a}\}\}$
$\{b\}$	\emptyset	$\{I_{\Omega_b} \otimes A_b \mid A_b \in \mathbf{A}_b \setminus \{I_{\Omega_b}\}\}$
$\{a, b\}$	\emptyset	$\{A_a \otimes A_b \mid A_a \in \mathbf{A}_a \setminus \{I_{\Omega_a}\}, A_b \in \mathbf{A}_b \setminus \{I_{\Omega_b}\}\}$

Therefore, the generalized wreath product of association schemes $\{\mathbf{A}_a, \mathbf{A}_b\}$ over the poset X is the direct product $\mathbf{A}_a \times \mathbf{A}_b$.

The dual idempotents of the generalized wreath product are given as follows. For an anti-chain Y in X , let $\mathbf{E}^*(Y)$ be the set of matrices indexed by Ω of the following form:

$$\bigotimes_{x \in \text{Down}(Y)} I_{\Omega_x} \otimes \bigotimes_{y \in Y} E_y^* \otimes \bigotimes_{z \in X \setminus (Y \cup \text{Down}(Y))} D_{\omega_z}, \quad (2)$$

where $E_y^* \in \mathbf{E}_y^* \setminus \{D_{\omega_y}\}$ for each $y \in Y$. Then let \mathbf{E}^* denote the union of $\mathbf{E}^*(Y)$ for all anti-chains Y in X . Remark that \mathbf{E}^* depends on ω .

Lemma 4. *With above notation, the union \mathbf{E}^* is the set of dual idempotents of the generalized wreath product of association schemes \mathbf{A}_x over the poset X with respect to ω .*

Proof. Compare the ω -th row of (1) and the diagonal entries of (2). \square

We end this section by the following two lemmas.

Lemma 5 ([1, Lemma 2]). *For a matrix $S \in \bigotimes_{x \in X} \text{Span}_{\mathbb{F}} \mathbf{A}_x$, the following are equivalent.*

1. $S \in \text{Span}_{\mathbb{F}} \mathbf{A}$;
2. Whenever $x < y$, either S_x is a scalar multiple of J_{Ω_x} or S_y is a scalar multiple of I_{Ω_y} .

Lemma 6. *For a matrix $S \in \bigotimes_{x \in X} \text{Span}_{\mathbb{F}} \mathbf{A}_x^*$, the following are equivalent.*

1. $S \in \text{Span}_{\mathbb{F}} \mathbf{A}^*$;
2. Whenever $x < y$, either S_x is a scalar multiple of I_{Ω_x} or S_y is a scalar multiple of D_{ω_y} .

Proof. Similar to the proof of [1, Lemma 2]. \square

3 Main theorem

In this section, we consider when the generalized wreath product becomes triply-regular. We follow the notation used in Section 2. With the notation

$$\mathbf{T} = \{E^* A F^* \mid E^*, F^* \in \mathbf{E}^*, A \in \mathbf{A}\},$$

the generalized wreath product \mathbf{A} is triply-regular if and only if $\text{Span}_{\mathbb{F}} \mathbf{T}$ is closed under matrix multiplication for every $\omega \in \Omega$. To characterize $\text{Span}_{\mathbb{F}} \mathbf{T}$, we carry out several observations.

- Setting $\mathcal{T}_x = \text{Span}_{\mathbb{F}}\{E^*AF^* \mid E^*, F^* \in \mathbf{E}_x^*, A \in \mathbf{A}_x\}$ for $x \in X$, it is clear that $\text{Span}_{\mathbb{F}} \mathbf{T}$ is the subset of $\text{Span}_{\mathbb{F}}(\bigotimes_{x \in X} \mathcal{T}_x)$.
- For a given $E^*, F^* \in \mathbf{E}^*, A \in \mathbf{A}$ and $x, y \in X$ with $x < y$, we have either $E_x^* = I_{\Omega_x}$ or $E_y^* = D_{\omega_y}$, and either $A_x = J_{\Omega_x}$ or $A_y = I_{\Omega_y}$, and either $F_x^* = I_{\Omega_x}$ or $F_y^* = D_{\omega_y}$ by Lemmas 5 and 6. Thus, one of the following five cases occurs:

If $E_x^* = I_{\Omega_x}, A_x = J_{\Omega_x}$ and $F_x^* = I_{\Omega_x}$, then

$$(E^*AF^*)_x = J_{\Omega_x}.$$

If $E_x^* = I_{\Omega_x}, A_x = J_{\Omega_x}$ and $F_y^* = D_{\omega_y}$, then

$$(E^*AF^*)_x \in J_{\Omega_x}\mathcal{A}_x^*, \quad (E^*AF^*)_y \in \mathcal{A}_y^*\mathcal{A}_yD_{\omega_y} = \mathcal{A}_yD_{\omega_y}.$$

If $E_x^* = I_{\Omega_x}, A_y = I_{\Omega_y}$ and $F_x^* = I_{\Omega_x}$, then

$$(E^*AF^*)_x \in \mathcal{A}_x, \quad (E^*AF^*)_y \in \mathcal{A}_y^*.$$

If $E_y^* = D_{\omega_y}, A_x = J_{\Omega_x}$ and $F_x^* = I_{\Omega_x}$, then

$$(E^*AF^*)_x \in \mathcal{A}_x^*J_{\Omega_x}, \quad (E^*AF^*)_y \in D_{\omega_y}\mathcal{A}_y\mathcal{A}_y^* = D_{\omega_y}\mathcal{A}_y.$$

Otherwise, $(E^*AF^*)_y = D_{\omega_y}$ or $(E^*AF^*)_y$ is the zero matrix.

By these observations, we introduce the following notations.

Definition 7. A nonzero matrix $T \in \bigotimes_{x \in X} \mathcal{T}_x$ is called *triply-nice* whenever for $x, y \in X$ with $x < y$, either one of the following holds.

- (TR1) T_x is a scalar multiple of J_{Ω_x} ;
- (TR2) $T_x \in J_{\Omega_x}\mathcal{A}_x^*$ and $T_y \in \mathcal{A}_yD_{\omega_y}$;
- (TR3) $T_x \in \mathcal{A}_x$ and $T_y \in \mathcal{A}_y^*$;
- (TR4) $T_x \in \mathcal{A}_x^*J_{\Omega_x}$ and $T_y \in D_{\omega_y}\mathcal{A}_y$;
- (TR5) T_y is a scalar multiple of D_{ω_y} .

We write \mathbf{N} for the set of triply-nice matrices in $\bigotimes_{x \in X} \mathcal{T}_x$ and $\mathcal{N} = \text{Span}_{\mathbb{F}} \mathbf{N}$.

Then we characterize $\text{Span}_{\mathbb{F}} \mathbf{T}$ as follows.

Lemma 8. *With above notation, we have $\mathcal{N} = \text{Span}_{\mathbb{F}} \mathbf{T}$.*

Proof. By the observation above, we show that $\mathbf{T} \subseteq \mathcal{N}$ and so $\text{Span}_{\mathbb{F}} \mathbf{T} \subseteq \mathcal{N}$. We next check that $\mathbf{N} \subseteq \text{Span}_{\mathbb{F}} \mathbf{T}$. Any matrix $N \in \mathbf{N}$ is a linear combination of triply-nice matrices all of whose components are in

$$\{E^*AF^* \mid E^*, F^* \in \mathbf{E}^* \cup \{I_{\Omega_x}\}, A \in \mathbf{A}_x \cup \{J_{\Omega_x}\}\}.$$

So it suffices to show that $N \in \mathbf{N}$ of this form belongs to \mathbf{T} . Let $N = \bigotimes_{x \in X} E_x^* A_x F_x^*$, where $E_x^*, F_x^* \in \mathbf{E}^* \cup \{I_{\Omega_x}\}$ and $A_x \in \mathbf{A}_x \cup \{J_{\Omega_x}\}$. We consider the all the five cases (TR1), (TR2), ..., (TR5). Take $x, y \in \Omega$ with $x < y$.

- (TR1) Suppose $E_x^* A_x F_x^*$ is a scalar multiple of J_{Ω_x} . Then E_x^*, F_x^* are scalar multiples of I_{Ω_x} ; A_x is a scalar multiple of J_{Ω_x} .
- (TR2) Suppose $E_x^* A_x F_x^* \in J_{\Omega_x} \mathcal{A}_x^*$ and $E_y^* A_y F_y^* \in \mathcal{A}_y D_{\omega_y}$. Then E_x^* is a scalar multiple of I_{Ω_x} ; A_x is a scalar multiple of J_{Ω_x} ; F_y^* is a scalar multiple of D_{ω_y} .
- (TR3) Suppose $E_x^* A_x F_x^* \in \mathcal{A}_x$ and $E_y^* A_y F_y^* \in \mathcal{A}_y^*$. Then E_x^*, F_x^* are scalar multiples of I_{Ω_x} ; A_y is a scalar multiple of I_{Ω_y} .
- (TR4) Suppose $E_x^* A_x F_x^* \in \mathcal{A}_x^* J_{\Omega_x}$ and $E_y^* A_y F_y^* \in D_{\omega_y} \mathcal{A}_y$. Then E_y^* is a scalar multiple of D_{ω_y} ; A_x is a scalar multiple of J_{Ω_x} ; F_x^* is a scalar multiple of I_{Ω_x} .
- (TR5) Suppose $E_y^* A_y F_y^*$ is a scalar multiple of D_{ω_y} . Then E_y^*, F_y^* are scalar multiples of D_{ω_y} ; A_y is a scalar multiple of either I_{Ω_x} or J_{Ω_x} .

Therefore, if E_x^* is not a scalar multiple of I_{Ω_x} , then E_y^* is a scalar multiple of D_{ω_y} . This means $E^* = \bigotimes_{x \in X} E_x^*$ is in \mathbf{E}^* by Lemma 6. Similarly, by Lemmas 5 and 6, we can show that $A = \bigotimes_{x \in X} A_x$ is in \mathbf{A} and $F^* = \bigotimes_{x \in X} F_x^*$ is in \mathbf{E}^* . This means that $N \in \mathbf{T}$. The result follows. \square

By this lemma, we prove that the following theorem.

Theorem 9. *With above notation, if $\text{Span}_{\mathbb{F}} \mathbf{T}_x$ is closed under matrix multiplication for every $x \in X$, then $\text{Span}_{\mathbb{F}} \mathbf{T}$ is also closed under matrix multiplication.*

Proof. By Lemma 8, we need to show that \mathcal{N} is closed under matrix multiplication. Since \mathcal{N} is the span of \mathbf{N} , it suffices to show that the product NM of two matrices N, M in \mathbf{N} is also triply-regular. Indeed, this is true because the multiplication table for the five cases is given as follows.

$N \setminus M$	(TR1)	(TR2)	(TR3)	(TR4)	(TR5)
(TR1)	(TR1)	(TR2)	(TR1)	(TR1)	(TR2)
(TR2)	(TR1)	(TR2)	(TR2)	(TR1)	(TR2)
(TR3)	(TR1)	(TR2)	(TR3)	(TR4)	(TR5)
(TR4)	(TR4)	(TR5)	(TR4)	(TR4)	(TR5)
(TR5)	(TR4)	(TR5)	(TR5)	(TR4)	(TR5)

In this table, we have (TR2) at the intersection of the (TR1)-th row and (TR5)-column. This means that if N is in the case (TR1) and M is in the case (TR5), then the product NM is in the case (TR2). □

By definition of the triply-regularity, Theorem 9 can be rephrased as follows.

Theorem 10. *The generalized wreath product of triply-regular association schemes is also triply-regular.*

References

- [1] R. A. Bailey, *Generalized wreath products of association schemes*, European J. Combin. **27** (2006), no. 3, 428–435.
- [2] Eiichi Bannai and Tatsuro Ito, *Algebraic combinatorics. I: Association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.
- [3] William J. Martin and Hajime Tanaka, *Commutative association schemes*, European J. Combin. **30** (2009), no. 6, 1497–1525.
- [4] Richard P. Stanley, *Enumerative combinatorics. Volume 1*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.
- [5] Paul-Hermann Zieschang, *Theory of association schemes*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

Double centralizers of association schemes *

Akihide Hanaki †(Shinshu University)

アソシエーション・スキームの典型的な例は有限可移置換群から得られ、そのようなものはシユアー的スキームと呼ばれる。アソシエーション・スキームの問題の一つに与えられたアソシエーション・スキームがシユアー的であるかどうかの判定がある。一般にシユアー的であるかどうかを判定するには、その自己同型群を求め、それから得られるアソシエーション・スキームが元のものとは一致するかどうかを見ればよい。しかし自己同型群の計算は簡単ではない。本講演では、アソシエーション・スキームの double centralizer を考える。よく知られているように複素数体上では double centralizer は必ず元のものとは一致するが、正標数の体上では必ずしも一致しない。しかしシユアー的なものに限れば double centralizer は必ず元のものとは一致する。すなわち double centralizer が元のものとは一致しなければシユアー的ではないということが出来る。

ここでは、アソシエーション・スキームの隣接代数がいくつかの特別な形をしているときに、その double centralizer が元のものとは一致することを紹介し、更に元のものとは一致しないときにはどのよになっているのかを見る。

記号などの説明は後ですが、少し例を見てみよう。

$ X $	No.	p	$\dim KS$	$\dim C(C(KS))$
16	19	2	4	5
16	79, 85	2	7	9
16	89, 94	2	7	8
16	90, 95	2	7	12
16	173	2	10	14
18	62	3	8	10
24	56, 57, 58	2	5	7
24	133, 134, 135	2	6	8
24	90, 91, 95, 100, 101	2	6	9

($|X| = 24$ にはまだまだたくさん例が存在する。) ここでは [3] のアソシエーション・スキームの分類を用いている。最後の 2 列の数値が違うことが double centralizer が元とは一致しないことを意味している。例で見ると、一致しないもののうち $\dim KS = |S|$ が最小のものは $\dim KS = 4$ である。実際 $|S| < 4$ では常に $KS = C(C(KS))$ であることを後で説明する。 $|X|$ が小さいときには $KS = C(C(KS))$ となるものが多いが、 $|X|$ が大きい非シユアー的スキームでは $KS \neq C(C(KS))$ となるものが多いことが例の計算から分かっている。

*第 35 回代数的組合せ論シンポジウム、広島工業大学、2018 年 6 月 20 日

†花木章秀、信州大学理学部、hanaki@shinshu-u.ac.jp

1 Centralizers

K を体とする。 $M_n(K)$ で K 上 n 次の全行列環を表す。 $\mathcal{U} \subset M_n(K)$ に対して

$$C(\mathcal{U}) = C_{M_n(K)}(\mathcal{U}) = \{P \in M_n(K) \mid \text{任意の } U \in \mathcal{U} \text{ に対して } PU = UP\}$$

とにおいて、これを \mathcal{U} の ($M_n(K)$ における) **centralizer** という。 $C(\mathcal{U})$ は $M_n(K)$ の部分代数になる。 $C(C(\mathcal{U}))$ を \mathcal{U} の **double centralizer** という。明らかに

$$C(C(\mathcal{U})) \supset \mathcal{U}, \quad C(C(C(\mathcal{U}))) = C(\mathcal{U})$$

が成り立つ。今回考えるのは $C(C(\mathcal{U})) = \mathcal{U}$ という性質である。

2 アソシエーション・スキームとシュアー的スキーム

X を有限集合とし S を $X \times X$ の分割とする。したがって $X \times X = \bigcup_{s \in S} s$ である。組 (X, S) がアソシエーション・スキームであるとは次の条件が成り立つことである。

- (1) $1 := \{(x, x) \mid x \in X\} \in S$
- (2) $s \in S$ ならば $s^* := \{(y, x) \mid (x, y) \in s\} \in S$
- (3) $s, t, u \in S$ に対して $p_{st}^u \in \mathbb{Z}$ が存在して、 $(x, y) \in u$ ならば $\#\{z \in X \mid (x, z) \in s, (z, y) \in t\} = p_{st}^u$

$s \subset X \times X$ に対して、その隣接行列を $\sigma_s \in M_X(\mathbb{Z})$ で表す。すなわち σ_s は行、列ともに集合 X で添字付けられた行列で、その (x, y) 成分は $(x, y) \in s$ のとき 1 で、そうでないとき 0 と定めたものである。(3) の条件は $\sigma_s \sigma_t = \sum_{u \in S} p_{st}^u \sigma_u$ であることと同値である。定義から、アソシエーション・スキーム (X, S) に対して、 σ_s を体 K 上の行列と見て $KS := \bigoplus_{s \in S} K\sigma_s$ とおけば、これは K -代数となる。これを (X, S) の K 上の隣接代数という。 $KS \subset M_X(K)$ と定義されているので、自然な埋込みから標準表現が定まる。対応する加群は X を自然な基底にもつので KX と表され、標準加群と呼ばれる。

G を有限集合 X 上の可移置換群とする。 $g \in G$ の作用を $(x, y)^g = (x^g, y^g)$ で定めて G は $X \times X$ にも作用する。このときの軌道の集合 S は $X \times X$ の分割を定め、これによって (X, S) はアソシエーション・スキームとなる。このようにして得られるアソシエーション・スキームをシュアー的であるという。異なる置換群が同じアソシエーション・スキームを定めることもある (例えば X 上の二重可移置換群による軌道は 2 つだけなのですべて等しくなる)。

(X, S) を置換群 G から得られるシュアー的スキームとする。 G の置換表現を D とする。このとき $KS = C(D(G))$ となることがすぐに分かる。したがってシュアー的スキームに対しては $C(C(KS)) = C(C(C(D(G)))) = C(D(G)) = KS$ が常に成り立つ。

命題 1. アソシエーション・スキーム (X, S) がシュアー的であるならば $C(C(KS)) = KS$ である。

3 係数体の変更

アソシエーション・スキームの表現に関する考察をするとき、面倒を避けるために係数体が代数的閉体であると仮定することが多い。しかし具体的に計算するときには代数的閉体を考えるわけにもいかず適切な体を考える必要がある。Double centralizer に関する性質は係数体に依存しないことを示す。

命題 2. K を体、 L をその拡大体とする。 $\mathcal{U} \subset M_n(K)$ に対して

$$C_{M_n(L)}(L\mathcal{U}) = L \cdot C_{M_n(K)}(\mathcal{U})$$

が成り立つ。特に $\dim_L C_{M_n(L)}(L\mathcal{U}) = \dim_K C_{M_n(K)}(\mathcal{U})$ であり、 \mathcal{U} が部分空間であるならば $C_{M_n(L)}(C_{M_n(L)}(L\mathcal{U})) = L\mathcal{U}$ と $C_{M_n(K)}(C_{M_n(K)}(\mathcal{U})) = \mathcal{U}$ は同値である。

Proof. $C_{M_n(L)}(L\mathcal{U}) \supset L \cdot C_{M_n(K)}(\mathcal{U})$ は明らかである。

$P = (p_{ij}) \in C_{M_n(L)}(L\mathcal{U})$ とする。 $L_0 = \sum_{i,j} K p_{ij}$ とおけば L_0 は L の有限次元 K -部分空間である。 v_1, \dots, v_ℓ を L_0 の K -基底とする。このとき $P = \sum_{i=1}^{\ell} v_i P_i$ ($P_i \in M_n(K)$) と一意的に書くことができる。 $U \in \mathcal{U}$ に対して $PU = UP$ であるから $\sum_{i=1}^{\ell} v_i P_i U = \sum_{i=1}^{\ell} v_i U P_i$ であり、 v_1, \dots, v_ℓ が K 上一次独立であることから $P_i U = U P_i$ ($i = 1, \dots, \ell$) となる。よって $P_i \in C_{M_n(K)}(\mathcal{U})$ であり $P \in L \cdot C_{M_n(K)}(\mathcal{U})$ である。 \square

4 いくつかの特別な場合

4.1 隣接代数が半単純であるとき

(X, S) をアソシエーション・スキームとし K を体とする。隣接代数が半単純であるときを考える。半単純になるための条件は [2] で求められている。命題 2 より K は十分大きいと仮定して構わない。よって $KS \cong \bigoplus_{i=1}^r M_{n_i}(K)$ としてよい。 V_i ($i = 1, \dots, r$) を単純 KS -加群とする。 $\dim_K V_i = n_i$ である。標準加群が $KX \cong \bigoplus_{i=1}^r m_i V_i$ であるとき $C(KS) \cong \bigoplus_{i=1}^r M_{m_i}(K)$ である。 $C(KS)$ の単純加群を W_i ($i = 1, \dots, r$) とする。 ($m_i = 0$ ならば $W_i = 0$ であるが、一般に $m_i > 0$ である。) KX を $C(KS)$ -加群と見れば $KX \cong \bigoplus_{i=1}^r n_i W_i$ である。 KS 加群と見たときとは、単純加群の次元と重複度が入れ替わる。よって $C(C(KS)) = KS$ が成り立つ。

命題 3. 隣接代数 KS が半単純ならば $C(C(KS)) = KS$ が成り立つ。

4.2 隣接代数が uniserial であるとき

K -代数 A が $K[x]/(x^{\ell+1})$ と森田同値であるとき、 A を uniserial であるという。このとき、多くのことが $A = K[x]/(x^{\ell+1})$ の場合に帰着され、この場合もそうである。直既約 $A = K[x]/(x^{\ell+1})$ -加群は

$$U_i = K[x]/(x^{i+1}) \quad i = 0, 1, \dots, \ell$$

である。 $\text{Hom}_A(U_i, U_j)$ は計算でき、 $\dim_K \text{Hom}_A(U_i, U_j) = \min\{i, j\} + 1$ である。 D を A の表現とすると、 $\text{Hom}_A(U_i, U_j)$ を用いて計算すれば $C(D(A))$ や $C(C(D(A)))$ は完全に記述できる。詳細は省くが、次が成り立つ。

命題 4. 隣接代数 KS が *uniserial* ならば $C(C(KS)) = KS$ が成り立つ。

隣接代数の両側イデアルとしての直和因子をブロックという。Centralizer はブロック毎に考えることが出来るので次も成り立つ。

命題 5. 隣接代数 KS のすべてのブロックが *uniserial* または単純ならば $C(C(KS)) = KS$ が成り立つ。

例 6. 島袋-吉川 [5] で Grassmann グラフから得られるアソシエーション・スキーム $J_{pf}(v, d)$ の隣接代数の構造が決定されている。 K が標数 p の体であるとき

$$KJ_{pf}(v, d) \cong K \oplus K[x]/(x^d)$$

である。これはシユアー的スキームなので $C(C(KJ_{pf}(v, d))) = KJ_{pf}(v, d)$ が成り立つことは明らかである。これに対して twisted Grassmann グラフ [6] は非シユアー的であるが Grassmann グラフと同型な隣接代数をもつ。よって命題 5 より twisted Grassmann グラフに対しても $C(C(KS)) = KS$ が成り立つことが分かる。(これらは非同型な標準加群をもつことが、計算機を用いてパラメータが小さい $(p^f, v, d) = (2, 5, 2), (3, 5, 2)$ についてだけ確認されている。)

4.3 $|S| = 2$ のとき

$|S| = 2$ であるアソシエーション・スキーム (X, S) を考える。このとき隣接代数は

$$KS \cong K \oplus K \quad \text{or} \quad K[x]/(x^2)$$

である。したがって命題 5 から次が成り立つ。

命題 7. $|S| = 2$ ならば $C(C(KS)) = KS$ が成り立つ。

4.4 $|S| = 3$ のとき

$|S| = 3$ であるアソシエーション・スキーム (X, S) を考える。このとき K を代数的閉体とすれば [4] より隣接代数は

$$K \oplus K \oplus K, \quad K[x]/(x^2) \oplus K, \quad K \oplus K[x]/(x^2),$$

$$K[x]/(x^3), \quad \text{or} \quad K[x, y]/(x^2, xy, y^2)$$

である。はじめの 4 つの場合は命題 5 から $C(C(KS)) = KS$ が成り立つ。最後の場合は [4] で標準加群 KX の構造も決まっていないので、まずこれを考え、更に $C(C(KS)) = KS$ が成り立つことを説明する。

K を代数的閉体と仮定する。 $KS \cong K[x, y]/(x^2, xy, y^2)$ と仮定する。 KS の直既約表現は分類されている [1, Theorem 4.3.2]。

- 単純表現 V_1

$$x \mapsto (0), \quad y \mapsto (0)$$

- V_{2n+1} ($n = 1, 2, 3, \dots$)

$$x \mapsto \left(\begin{array}{c|ccc} 1 & 0 & & \\ 0 & & \ddots & \ddots \\ \hline & & & 1 & 0 \\ 0 & 0 & & & \end{array} \right), \quad y \mapsto \left(\begin{array}{c|ccc} 0 & 1 & & \\ 0 & & \ddots & \ddots \\ \hline & & & 0 & 1 \\ 0 & 0 & & & \end{array} \right)$$

- V_{2n+1}^* ($n = 1, 2, 3, \dots$)

$$x \mapsto \left(\begin{array}{c|ccc} 0 & & & \\ 0 & 1 & \ddots & \\ \hline & & \ddots & 0 \\ & & & 1 \\ 0 & 0 & & \end{array} \right), \quad y \mapsto \left(\begin{array}{c|ccc} 1 & & & \\ 0 & 0 & \ddots & \\ \hline & & \ddots & 1 \\ & & & 0 \\ 0 & 0 & & \end{array} \right)$$

- $W_{2n}(\alpha)$ ($n = 1, 2, 3, \dots, \alpha \in K$)

$$x \mapsto \left(\begin{array}{c|ccc} 1 & & & \\ 0 & & \ddots & \\ \hline & & & 1 \\ 0 & 0 & & \end{array} \right), \quad y \mapsto \left(\begin{array}{c|ccc} \alpha & 1 & & \\ 0 & & \ddots & \ddots \\ \hline & & & 1 \\ & & & \alpha \\ 0 & 0 & & \end{array} \right)$$

- $W_{2n}(\infty)$ ($n = 1, 2, 3, \dots$)

$$x \mapsto \left(\begin{array}{c|ccc} 0 & 1 & & \\ 0 & & \ddots & \ddots \\ \hline & & & 1 \\ & & & 0 \\ 0 & 0 & & \end{array} \right), \quad y \mapsto \left(\begin{array}{c|ccc} 1 & & & \\ 0 & & \ddots & \\ \hline & & & 1 \\ & & & \\ 0 & 0 & & \end{array} \right)$$

$x = \sum_{s \in S} \sigma_s$ (すべての成分が 1 である行列) と仮定することができる。このとき $\text{rank } x = 1$ である。したがって KX のただ一つの直和因子が x にランク 1 をもつことが分かる。標準加群は自己反傾的 [4, Proposition 5] なので、 x がランクをもつ直既約加群も自己反傾的である。更に標準加群は正則加群を部分加群にもたなければならない。これらの条件をみたす直既約表現は $W_4(\infty)$ しかないことが分かる。他の直既約因子は x にランクをもたないので V_1 または $W_2(\infty)$ である。よって標準表現は

$$W_4(\infty) \oplus aW_2(\infty) \oplus bV_1 \quad (a, b \in \mathbb{Z}_{\geq 0})$$

と表される。ここまで分かれば計算によって $C(KS)$ や $C(C(KS))$ を求めることができるが、参考のために計算の概略を記しておこう。

D を A の表現として $D = D_1 \oplus \cdots \oplus D_r$ を直既約分解とする。

$$\text{Hom}(D_i, D_j) = \{M \mid D_i(a)M = MD_j(a) \text{ for all } a \in A\}$$

とおけば

$$C(D(A)) = \begin{pmatrix} \text{Hom}(D_1, D_1) & \cdots & \text{Hom}(D_1, D_r) \\ \vdots & \ddots & \vdots \\ \text{Hom}(D_r, D_1) & \cdots & \text{Hom}(D_r, D_r) \end{pmatrix}$$

である。また $W_4(\infty), W_2(\infty), V_1$ に対して $\text{Hom}(\bullet, \bullet)$ は

	$W_4(\infty)$	$W_2(\infty)$	V_1
$W_4(\infty)$	$\begin{pmatrix} a & b & d & e \\ a & & d & \\ \hline f & a & c & \\ & & & a \end{pmatrix}$	$\begin{pmatrix} a & b \\ a \\ \hline c \end{pmatrix}$	$\begin{pmatrix} a \\ \hline b \end{pmatrix}$
$W_2(\infty)$	$\begin{pmatrix} a & b & c \\ & & b \end{pmatrix}$	$\begin{pmatrix} a & b \\ a \end{pmatrix}$	$\begin{pmatrix} a \end{pmatrix}$
V_1	$\begin{pmatrix} a & b \end{pmatrix}$	$\begin{pmatrix} a \end{pmatrix}$	$\begin{pmatrix} a \end{pmatrix}$

である¹。これを組合せて $C(KS)$ が分かる。またこれらと可換になるものは KS に限ることも確認できる。

以上をまとめて次が成り立つ。

命題 8. $|S| = 3$ ならば $C(C(KS)) = KS$ が成り立つ。

4.5 $|S| = 4$ のとき - 例

$|S| = 4$ では $KS \subsetneq C(C(KS))$ となる例がある。すべての場合の様子を記述することは難しいので、一番小さい例について、その構造を詳しく見る。

4.5.1 $|X| = 16$, No. 19, $p = 2$

$KS \cong K[x_1, x_2, x_3]/(x_i x_j \mid 1 \leq i, j \leq 3)$ である。(この代数の表現型は wild で、直既約表現を分類することはできない。) $\dim C(KS) = 86$, $C(KS)/J(C(KS)) \cong K \oplus M_2(K)$ が計算でき、したがって標準加群は、二つの非同型な直既約加群 V, W を用いて

$$KX_{KS} = V \oplus W \oplus W$$

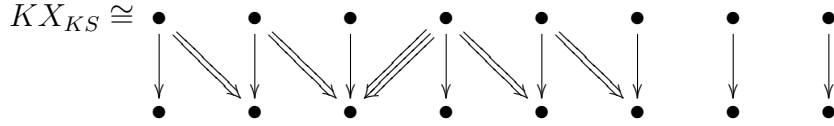
¹表記をわかりやすくするために $W_4(\infty)$ は $x \mapsto \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ で計算している。また $\begin{pmatrix} a & b & c \\ & & b \end{pmatrix}$ などは $\left\{ \begin{pmatrix} 0 & a & b & c \\ 0 & 0 & 0 & b \end{pmatrix} \mid a, b, c \in K \right\}$ の意味である。

と表される。 $\dim C(C(KS)) = 5$ であり

$$C(C(KS)) \cong K[x_1, x_2, x_3, x_4]/(x_i x_j \mid 1 \leq i, j \leq 4)$$

となる。

標準加群の構造を注意深く計算すれば



となることが確認できる。ここで、 \bullet は加群の基底を表し、3種類の矢印がそれぞれ x_1, x_2, x_3 の作用を表している。自己反傾的であること、正則加群を部分加群に含むことも図から理解できる。 $(C(KS))$ については計算機を用いて次元などを計算しただけである。 $C(KS)$ は次元も大きく、その構造を完全に求めることは容易ではないと思われる。)

4.5.2 $|X| = 28$, No. 29, $p = 2$

$KS \cong K[x_1, x_2, x_3]/(x_i x_j \mid 1 \leq i, j \leq 3)$ である。 $\dim C(KS) = 299$, $C(KS)/J(C(KS)) \cong K \oplus M_4(K) \oplus M_4(K) \oplus M_4(K)$ が計算でき、したがって標準加群は

$$KX_{KS} = V \oplus 4W_1 \oplus 4W_2 \oplus 4W_3$$

と表される (直既約因子の構造などは計算していない)。 $\dim C(C(KS)) = 8$ であり

$$C(C(KS)) \cong K[x_1, \dots, x_7]/(x_i x_j \mid 1 \leq i, j \leq 7)$$

となる。

5 補足

ここまでの話とは直接には関係ないが、今後役に立つかもしれないことを補足しておく。

補足 9. $(X, S), (X', S')$ をアソシエーション・スキームとし、 $KS \cong KS'$ と仮定する。更に KS -加群として $KX \cong \bigoplus_{i=1}^r m_i V_i$, $KX' \cong \bigoplus_{i=1}^r m'_i V_i$ ($m_i > 0, m'_i > 0, V_i$ は非同型な直既約加群) とする。このとき $\dim C(C(KS)) = \dim C(C(KS'))$ が成り立つ。特に $C(C(KS)) = KS$ であることと $C(C(KS')) = KS'$ であることは同値である。

補足 10. D_i ($i = 1, 2$) を代数 A の表現とする。 $D = D_1 \oplus D_2$ とする。このとき $C(C(D_i(A))) = D_i(A)$ ($i = 1, 2$) であっても $C(C(D(A))) = D(A)$ となるとは限らない。

この補足から $C(C(KS)) = KS$ という性質は直和因子毎に見ることはできないデリケートなものであることが分かる。

講演後、どのくらいの非シユアー的スキームについて $C(C(KS)) \neq KS$ が成り立つのかを計算してみた。標数 2、 $|X|$ は 4 の倍数、に対して以下の通りである。

$ X $	isomorphism classes	non-schurian	$C(C(KS)) \neq KS$
16	222	16	8
20	95	0	0
24	750	81	60
28	185	61	24
32	18210	13949	13287

ある程度大きな $|X|$ に対して、多くの非シュアー的スキームに対して $C(C(KS)) \neq KS$ であり、この性質がそれなりに意味のある性質であることが分かる。

References

- [1] D. J. Benson, *Representations and cohomology. I*, Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1991.
- [2] A. Hanaki, *Semisimplicity of adjacency algebras of association schemes*, J. Algebra **225** (2000), no. 1, 124–129.
- [3] A. Hanaki and I. Miyamoto, *Classification of association schemes with small vertices*, published on web (<http://math.shinshu-u.ac.jp/~hanaki/as/>).
- [4] A. Hanaki and M. Yoshikawa, *On modular standard modules of association schemes*, J. Algebraic Combin. **21** (2005), no. 3, 269–279.
- [5] O. Shimabukuro and M. Yoshikawa, *Modular adjacency algebras of Grassmann graphs*, Linear Algebra Appl. **466** (2015), 208–217.
- [6] E. R. van Dam and J. H. Koolen, *A new family of distance-regular graphs with unbounded diameter*, Invent. Math. **162** (2005), no. 1, 189–193.

古典直交多項式に対するカーネル多項式の代数幾何的側面とその応用

澤 正憲 (神戸大学)*

1. 序

区間 (a, b) 上の重み関数 w に関する直交多項式列 $\{\Phi_r\}_r$ について,

$$K_r(x, y) := \sum_{k=0}^r h_r h_k^{-1} \Phi_k(x) \Phi_k(y), \quad h_k = \int_a^b \Phi_k(x)^2 w(x) dx$$

で定められる二変数多項式 $K_r(x, y)$ をカーネル多項式という。カーネル多項式は次数 r 以下の多項式の空間に付随する再生核で、関数解析の古典的な研究対象である。またカーネル多項式はガウス求積公式の点配置の特徴付けにも用いられており、矩形求積公式の理論の基本的な道具として古くから研究されている。これらの事実はカーネル多項式が主に解析的な視点から研究されてきたことを示唆している ([15, 16] 等参照)。本稿では古典直交多項式列に関するカーネル多項式の代数幾何的側面に興味がある。本研究は内田幸寛氏 (首都大学東京) との共同研究 [18, 19] に基づいている。

Bochner [3] は Sturm-Liouville 型の 2 階常微分方程式の固有関数になる多項式を分類した。これらの多項式で正定値汎関数に関して直交性をもつものはヤコビ多項式 (一般) ラゲール多項式, エルミート多項式の 3 種に限られ [8], 古典直交多項式と呼ばれている。本稿では有理的多項式, すなわち有理係数の古典直交多項式のみを扱う。

2. 主結果

次の結果は有理的多項式に対するカーネル多項式の代数幾何的特徴付けを与える。

定理 1 ([18]) . 自然数 $r \geq 2$ について K_r を有理係数の古典直交多項式多項式に付随するカーネル多項式とし, K_r を射影化して得られる射影曲線を C_r とおく。このとき次が成り立つ:

- (1) 曲線 C_r は \mathbb{C} 上絶対既約である;
- (2) 曲線 C_r の種数は $(r-1)^2$ である。

定理 1 の前半の主張は, Sturm-Liouville 型微分方程式をはじめ直交多項式の解析的性質を用いて C_r 上の通常特異点を分類した後, Bezout の定理を用いて証明される。後半の証明には Faltings の定理 [4] を用いる。

本稿では, 定理 1 とは一見無関係に見える次の不定方程式系の求解問題にも言及する:

本研究は科研費基盤研究 (C) (課題番号:18K03414) の助成を受けたものである。

* 〒 657-8501 兵庫県神戸市灘区六甲台町 1-1 神戸大学 大学院システム情報学研究科
e-mail: sawa@people.kobe-u.ac.jp

問題1. m, n を自然数とし, 有理的多項式に対応する汎関数 $\mathcal{I}[\cdot] = \int_a^b \cdot w(t) dt$ を考える. このとき x_i, y_i に関する不定方程式系

$$\sum_{i=1}^m x_i y_i^j = \int_a^b t^j w(t) dt, \quad j = 0, 1, \dots, n, \quad (1)$$

は有理解をもつか?

不定方程式系 (1) が有理解 x_i, y_i をもつことと, 有理点 y_i と有理ウェイト x_i からなる次数 n の求積公式¹ が存在することは等価である. 求積公式の点集合のサイズ m を下から評価する Stroud 型不等式と同様の議論から ([15] 等参照), $n \leq 2m - 1$ となることがわかる. この不等式においてタイトな場合 ($n = 2m - 1$ の場合), 各点 y_i は w に関する m 次直交多項式 $\Phi_m(x)$ の零点になり, この逆も成り立つ. 一般に, m 個の点からなる次数 $2m - k$ の求積公式の点は階数 $k - 1$ の準直交多項式 $\Phi_m(x) + b_1 \Phi_{m-1}(x) + \dots + b_{k-1} \Phi_{m-k+1}(x)$ の零点になり, この逆も成り立つ [13]. この事実は特に $k = 2$ のときは Riesz [11] の古典的な結果に等しくなる. なお本稿での準直交多項式の定義は [17] に基づいているが, いくつかの文献 ([14] 等) では階数の定義が少々異なるので注意が必要である.

筆者の知る限り問題1は Hausdorff [5] まで遡る. Hausdorff はガウス積分 $\frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} dx$ を考えて, $n = m - 1$ の場合に不定方程式系 (1) が有理解をもつことを示した. Hausdorff のモチベーションはワーリング問題の Hilbert [6] による解の簡略化にあった. Hausdorff の仕事はその重要性に反してワーリング問題関連のほとんどの文献で見落とされてきたが, 2006 年の Nestarenko の論文 [9] で業界的に再認識されるようになった. なお本稿の主眼からは逸れるが, (1) 式の実解は古典的な有限次元バナッハ空間の等長埋め込みやユークリッドデザインの構成にも応用されるため, 組合せ論的な視点からも重要である [9, 10].

Schur [12] によるエルミート多項式の \mathbb{Q} 上既約性の証明から, $n = 2m - 1$ のときには不定方程式系 (1) は有理解をもたない. そこで筆者ら [19] は, $n = 2m - 2$ の場合に次の非存在定理を示した:

事実1 ([19]). 自然数 $r \equiv 2, 3, 4, 5, 6 \pmod{8}$ について,

$$\sum_{i=1}^{r+1} x_i y_i^k = a_k, \quad k = 0, 1, \dots, 2r. \quad (2)$$

を満たす有理数 x_i, y_i は存在しない.

組合せ論的には, 事実1は有理点・有理ウェイトの almost tight Gaussian $2r$ -design [1] の非存在に言及している.

この他に興味深いのは区間 $(-1, 1)$ 上の定数関数 $w \equiv 1$ の場合である. これに対応する有理的多項式はルジャンドル多項式である. エルミート多項式と異なり, ルジャ

¹

$$\int_a^b f(t) w(t) dt = \sum_{i=1}^m x_i f(y_i), \quad f \in \text{Pol}_n(a, b)$$

の形の積分近似公式を次数 n の求積公式と呼び, y_i を点 (ノード), x_i をウェイトという. 組合せ論的には次数 n の求積公式の点配置は区間 (a, b) 上の n -デザインである.

ンドル多項式の \mathbb{Q} 上既約性の判定問題は未解決である。しかし, Holt の古典的な結果 [7] からルジャンドル多項式が有理的な一次式で分解されないことはわかっているの
で, $n = 2m - 1$ のときには (1) は有理解をもたない。かくしてエルミート多項式の場合と同様に almost tight なケースが自然に興味の対象になる。

また坂内-坂内-伊藤 [2, 問題 2] では区間 $(-1, 1)$ 上で一般の重み関数 w について問題 1 が提起されている。

そこで本研究の目的はこれらの状況を問題 1 の枠組みで統一的に扱うことであり, これまでに関連する結果として次を得ている:

定理 2 ([18]) . $m \geq 3$ を整数, $n = 2m - 2$ とする。このとき不定方程式系 (1) は (有理的多項式のクラスの選び方に依らず) 高々有限個しか有理解をもたない。

定理 2 の証明の概略を述べる。まず解析学の基本的な事実である

$$K_{m-1}(x, y) = \frac{k_{m-1}}{k_m} \cdot \frac{\Phi_m(x)\Phi_{m-1}(y) - \Phi_{m-1}(x)\Phi_m(y)}{x - y}$$

に注目する (Christoffel-Darboux 公式, [16] 等参照)。ここで k_m は有理的多項式 Φ_m の主係数である。 $n = 2m - 2$ のとき, 上の準直交多項式の零点に関するくだりから, 方程式系 (1) の有理解 y_i はある 1 階の準直交多項式 $\Phi_m(x) + c\Phi_{m-1}(x)$ の零点にならなければならない。すると Christoffel-Darboux 公式から, 異なる零点 y_i, y_j を用いて曲線 C_{m-1} 上の有理点 (y_i, y_j) を構成することができる。定理 1 より C_{m-1} 上の有理点の個数は高々有限個なのだから, (1) 式の有理解の個数も高々有限個になる。

エルミート多項式, ラゲール多項式 (一般ラゲール多項式の特例), ルジャンドル多項式 (ヤコビ多項式の特例) について定理 2 の結果を改良することができる:

定理 3 ([18]) . $m \geq 3$ を整数, $n = 2m - 2$ とする。このとき次の w と (a, b) に対して不定方程式系 (1) は有理解をもたない:

- (1) $w(t) = e^{-t^2}/\sqrt{\pi}$, $(a, b) = (-\infty, \infty)$;
- (2) $w(t) \equiv 1/2$, $(a, b) = [-1, 1]$;
- (3) $w(t) = e^{-t}$, $(a, b) = (0, \infty)$.

一連の結果の証明にはニュートン多角形とベルトラン仮説を用いる。これらの手法は, 原理的には上記以外の重み関数 w にも適用可能なのだが, 一般ラゲール多項式やヤコビ多項式の係数は上の三つのケースとは比べものにならないくらい繁雑であり, 多くの場合, ニュートン多角形に関する付値の計算でおよそ手詰まりになる。論文 [19] では (1 階の) 準エルミート多項式の判別式の明示公式を与えることで事実 1 を証明した。同様の手法を, 準ヤコビ, 準ラゲール多項式についても試みたが, 計算の繁雑さからやはり手詰まりになる。

問題 1 への他のアプローチとして, カーネル多項式 K_r の付値を直接計算することで曲線 C_r 上の有理点を分類する方法もある。たとえば (1 階の) 準ルジャンドル多項式 $\Phi_3(x) + c\Phi_2(x)$ の場合には 2 進付値の計算によって C_2 上に有理点がないとわかる。し

かし，同じ準ヤコビ多項式系列であっても，たとえば第2種の準チェビシェフ多項式の場合には事情が大きく異なる．実際，この場合には曲線 $K_2(x, y) = 0$ の方程式は

$$32x^2y^2 - 8x^2 + 8xy - 8y^2 + 4 = 0$$

となり，有理点 $(1/2, -1/2), (-1/2, 1/2)$ を含むことが容易にわかる．上の曲線の方程式を Tate のアルゴリズム（例えば [20] 等参照）などで適当な楕円曲線に変形した後，Mordell 群を計算すると， C_2 上の有理点が $(1/2, -1/2), (-1/2, 1/2)$ に限られることが結論される．このように C_2 上の有理点の分類から準チェビシェフ多項式の零点の有理性を直ちに判定することはできないのである．幸い，いまの例では $\pm 1/2$ が第2種準チェビシェフ多項式の零点にならないことを具体計算で確かめられるが，一般の準ヤコビ多項式になると曲線 C_r の分類だけでは足りないのかもしれない²．

最後に不定方程式 (1) の求解問題に関する肯定的な結果に触れておく．既に述べたように Hausdorff は $n = m - 1$ の場合に (1) が有理解をもつことを示した．次の結果は $n = m$ の場合にも方程式系 (1) が有理解をもつことを示している：

定理 4 ([18])．任意の自然数 m について，

$$\sum_{i=1}^m x_i y_i^j = \int_a^b t^j w(t) dt, \quad j = 0, 1, \dots, m.$$

を満たす有理数 x_i, y_i が存在する．

$m + 1 \leq n \leq 2m - 3$ の場合には問題 1 にまったく手をつけていない．

謝辞．本研究報告は，一昨年に篠原雅史先生（滋賀大学），野崎寛先生（愛教大）らに口頭発表の機会をいただいた同シンポジウムでの報告内容の継続研究である．一昨年，昨年と私事で講演時間帯の調整や報告集執筆の辞退など，世話人の先生方には随分とご迷惑をおかけしてしまった．それにも関わらず本研究集会でも再び講演の機会をくださった谷口哲至（広島工業大学）をはじめとする世話人の皆様，そして一昨年，昨年の世話人の皆様に心から謝意を申し上げたい．

参考文献

- [1] E. BANNAI, E. BANNAI. *Tight Gaussian 4-designs*. J. Algebr. Comb. **22** (2005), 22–39.
- [2] 坂内英一，坂内悦子，伊藤達郎. 代数的組合せ論入門．共立出版，2016．
- [3] S. BOCHNER. *Über Sturm-Liouvillesche Polynomsysteme*. Math. Z. **29** (1929), 730–736.
- [4] G. FALTINGS. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73** (1983), 349–366.
- [5] F. HAUSDORFF. *Zur Hilbertschen Lösung des Waringschen Problems*. Math. Ann. **67** (1909), 301–305.

²問題 1 への応用的な側面に限らず，有理的多項式から誘導される曲線 C_r 上の有理点の分類はそれ自身興味深い問題である．これは筆者が 2015 年に九州工業大学で開催された 13th Workshop on Combinatorics and Algebra でプレゼンテーションをした際に，坂内英一先生と伊藤達郎先生から提示していただいた問題でもあり，今後も折に触れて進展させたい．

- [6] D. HILBERT. *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n -ter Potenzen (Waringsches Problem)*. Math. Ann. **67** (1909), 281–300.
- [7] J. B. HOLT. *On the irreducibility of Legendre's polynomials*. Proc. London Math. Soc. **11** (1912), 351–356.
- [8] P. LESKY. *Die Charakterisierung der klassischen orthogonalen Polynome durch Sturm-Liouvillesche Differentialgleichungen*. Arch. Rat. Mech. Anal., **10** (1962), 341–351.
- [9] Y. V. NESTERENKO. *On Waring's problem (elementary methods)*. (Russian) Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **322** (2005), Trudy po Teorii Chisel, 149–175, 254; translation in J. Math. Sci. (N. Y.) **137** (2006), 4699–4715.
- [10] H. NOZAKI, M. SAWA. *Remarks on Hilbert identities, isometric embeddings, and invariant cubature*. St. Petersburg Math. J., **25** (2014), 615–646.
- [11] M. RIESZ. *Sur le problème des moments, III*. Ark. Math. Fys., **17** (1923), 1–52.
- [12] I. SCHUR. *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II*. Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., **14** (1929), 370–391.
- [13] J. SHOHAT. *On mechanical quadratures, in particular, with positive coefficients*. Trans. Amer. Math. Soc., **42** (1937), 461–496.
- [14] J. A. SHOHAT, J. D. TAMARKIN. *The Problem of Moments*, American Mathematical Society Mathematical Surveys and Monographs, I, American Mathematical Society, Providence, 1970.
- [15] A. H. STROUD. *Approximate Calculation of Multiple Integrals*. Prentice-Hall, Englewood Cliffs, N.J., 1971.
- [16] G. SZEGŐ. *Orthogonal Polynomials (4th ed.)*. American Mathematical Society Colloquium Publications, vol. 23, American Mathematical Society, Providence, 1975.
- [17] Y. XU. *A characterization of positive quadrature formulae*. Math. Comp., **62** (1994), 703–718.
- [18] M. SAWA, Y. UCHIDA. *Algebraic-geometric aspects of the kernel polynomials of classical quasi-orthogonal polynomials*. Submitted.
- [19] M. SAWA, Y. UCHIDA. *Discriminants of classical quasi-orthogonal polynomials with their application to Diophantine equations*. To appear in Jour. Math. Soc. Japan.
- [20] L. C. WASHINGTON. *Elliptic Curves: Number Theory and Cryptography*, 2nd edition, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Boca Raton, 2008.

On the closed subset generated by a regular relation

吉川 昌慶 (兵庫教育大学)

1 序

アソシエーション・スキームの正則な relation s ($s^*ss = \{s\}$ を満たす relation) に対して, s^*s は $n_{s^*s} = n_s$ を満たし, さらに閉部分集合となることが知られている. こうして, 正則な relation の valency n_s は, 元のアソシエーション・スキームの位数を割ることが分かる. 一方, relation s が正則ならば, その strong girth $\text{sg}(s)$ は有限であり,

$$a_{s^{n_1}} = \begin{cases} n_s^{n-1} & (\text{sg}(s) \mid n \text{ のとき}), \\ 0 & (\text{それ以外の場合}) \end{cases}$$

を満たす. こうして, 正則な relation の strong girth は, 有限群の元の位数と似た特徴をもつ. 実際, 任意の thin relation s は正則であるが, その strong girth は, s で生成される巡回群の位数に一致する. 有限群の元の位数は, よく知られているように, 元の群の位数を割るが, 正則な relation の strong girth は元のアソシエーション・スキームの位数を割るだろうかという問題が考えられる.

本稿では, 正則な relation s で生成される閉部分集合 $\langle s \rangle$, 上記の閉部分集合 s^*s , s の strong girth $\text{sg}(s)$ の関係を考察することにより, 任意の正則な relation の strong girth は元のアソシエーション・スキームの位数を割ることを紹介する.

また, 閉部分集合 $\langle s \rangle$ の構造の研究の応用として, 正則アソシエーション・スキームに対して Burnside の定理が成り立つことを紹介する. ここで得られる Burnside の定理は, 「正則アソシエーション・スキーム S において, χ を重複度 m_χ が 2 以上の既約指標とすると, $\chi(\sigma_s) = 0$ となる S の relation s が必ず存在する」であり, 有限群の指標理論における Burnside の定理よりも強い主張が成り立つ (有限群を考えた場合は, $m_\chi = \chi(1)$ であるので, 有限群の場合における主張は変わらない).

2 準備

アソシエーション・スキームの定義などは, Zieschang [4] による.

(X, S) もしくは単に S をアソシエーション・スキームとし, σ_s を $s \in S$ の隣接行列とする. また, a_{stu} を交叉数とし, n_s を $s \in S$ の valency とする. S の任意の部分集合 T に対して, $n_T := \sum_{t \in T} n_t$ と定義する. $\mathbb{C}S$ を S の複素数体上の隣接代数とし, その既約指標全体の集合を $\text{Irr}(S)$ とする.

$O^\theta(S)$ を S の thin residue とする. $S//O^\theta(S)$ は thin なアソシエーション・スキーム, すなわち本質的に有限群である, ことが知られている.

$\Gamma_X : \mathbb{C}S \rightarrow M_{|X|}(\mathbb{C}), \sigma_s \mapsto \sigma_s$ を $\mathbb{C}S$ の標準表現といい, その対応する指標を χ_X とかき, 標準指標という. $\chi_X = \sum_{\chi \in \text{Irr}(S)} m_\chi \chi$ と表されるとき, m_χ を既約指標 χ の重複度という.

交叉数 a_{stu} に対して、次のような記述による省略を許すことにする。

$$\sigma_s^\ell = \sum_{u \in S} a_{s^\ell u} \sigma_u$$

3 正則アソシエーション・スキーム

正則アソシエーション・スキームの詳しい議論は、[3]にある。

$s \in S$ が次の同値な条件

1. $s^* s s = \{s\}$
2. $\sigma_{s^*} \sigma_s \sigma_s = n_s^2 \sigma_s$
3. $a_{s^* s s} = n_s^2$

の一つを満たすとき、正則な relation であるという。すべての relation が正則であるようなアソシエーション・スキームは正則であると呼ばれる。

注意 1. 有限群 G をアソシエーション・スキームと見なしたとき、 $g \in G$ に対して、 g^* は g^{-1} に相当するので、 $g^* g g = \{g\}$ を満たす。したがって、有限群は正則アソシエーション・スキームである。

有限群の元の位数に対応する 2 つの概念を定義する。 $1 \neq s \in S$ に対して、 s の girth $g(s)$ を

$$g(s) := \min\{e \in \mathbb{N} \setminus \{1\} \mid a_{s^e 1} \neq 0\}$$

で定義する。明らかに、任意の relation $s \in S$ に対して、 $g(s) < \infty$ である。また、 s の strong girth $sg(s)$ を

$$sg(s) := \min\{e \in \mathbb{N} \setminus \{1\} \mid a_{s^e 1} = n_s^{e-1}\},$$

もしそのような e が存在しないときは、 $sg(s) = \infty$ と定義する。 $1 \in S$ に対しては、 $g(1) = sg(1) = 1$ と定義する。定義から、 $g(s) \leq sg(s)$ が成り立つことが分かる。実際には、 $sg(s) < \infty$ ならば、 $g(s) = sg(s)$ が成り立つ。特に、定理 2 で紹介するように、relation s が正則ならば、 $sg(s) < \infty$ であり、 $g(s) = sg(s)$ が成り立つ。

任意の relation $s \in S$ に対して、 $sg(s) < \infty$ であるとき、 S の exponent $\exp(S)$ を

$$\exp(S) := \text{l.c.m}\{sg(s) \mid s \in S\}$$

で定義する（ただし、l.c.m は最小公倍数を意味する）。そうでないときは、 $\exp(S) = \infty$ と定義する。上記にあるように、 S が正則アソシエーション・スキームならば、任意の $s \in S$ に対して $sg(s) < \infty$ なので、 S の exponent $\exp(S)$ は有限である。

アソシエーション・スキームの正則な relation は、次の特徴を有する。

定理 2. $s \in S$ が正則な relation であるとき、次を満たす。

1. $g(s) = sg(s) < \infty$,
2. $s^* s = s s^*$,
3. $s^* s$ は、 $n_{s^* s} = n_s$ を満たす S の閉部分集合、

4. $t \geq 2$ に対して,

$$a_{s^t} = \begin{cases} n_s^{t-1} & \text{sg}(s) \mid t \text{ であるとき,} \\ 0 & \text{そうでないとき.} \end{cases}$$

特に 1 番目と 4 番目の性質から, 正則な relation の $\text{sg}(s)$ (もしくは $g(s)$) は, 有限群の元の位数に対応する概念の候補と考えられる.

4 1 つの正則な relation で生成される閉部分集合の構造

アソシエーション・スキームの 1 つの正則な relation によって生成される閉部分集合 $\langle s \rangle$ を考える. 組合せ論的な議論は行わないので, 閉部分集合とそれに付随する部分アソシエーション・スキームを区別しないで議論する. 正則な relation s に対して, 閉部分集合 s^*s が与えられる. この閉部分集合は, $n_s \mid n_S$ であることの証明にも使われるが, $\langle s \rangle$ の構造にも重要な役割を果たす.

定理 3. $s \in S$ が正則であるとき, $s^*s = O^\theta(\langle s \rangle)$ である.

こうして, 剰余スキーム $\langle s \rangle // (s^*s)$ は complex product に関して有限群をなすことがわかる. さらに, 詳しく次が成り立つ.

定理 4. $s \in S$ が正則であるとき, $\langle s \rangle // (s^*s)$ は位数 $\text{sg}(s)$ の巡回群 $C_{\text{sg}(s)}$ に同型である.

この定理から, $n_{\langle s \rangle} = \text{sg}(s) \cdot n_{s^*s} = \text{sg}(s) \cdot n_s$ が得られるので, 任意の正則な relation s に対して, $\text{sg}(s) \mid n_S$ が分かる. 従って, 正則アソシエーション・スキーム S に対して, $\exp(S) \mid n_S$ が成り立つことが分かる.

この節の残りで, 一元生成正則アソシエーション・スキーム $S = \langle s \rangle$ の指標について考察する. S の relation はすべて正則であることが仮定されていることに注意する. このとき, $R = s^*s$ とおくと, 上の定理より, $S//R \cong C_{\text{sg}(s)}$ が成り立つ. さらに, 次の 2 つの集合の要素の間に 1 対 1 対応があることが分かる.

$$T := \{t \in S \mid \langle t \rangle = S\}, \quad \bar{T} := \{t^R \in S//R \mid \langle t^R \rangle = S//R\}$$

K を位数 n_s のランク 2 のアソシエーション・スキームとする. このとき, 自然な単射準同型 $\mathbb{C}(K \wr S//R) \rightarrow \mathbb{C}S$ がある. ここで, $K \wr S//R$ は, K と $S//R$ の wreath product を意味する. こうして, $\mathbb{C}S$ の任意の表現は, $\mathbb{C}(K \wr C_{\text{sg}(s)})$ の表現として考えることができる. Hanaki-Hirotsuka の論文 [1] からこの wreath product $K \wr C_{\text{sg}(s)}$ の既約指標は具体的に分かっていて, 次の定理が得られる.

定理 5. $S = \langle s \rangle$ を一元生成正則アソシエーション・スキームとし, $R = s^*s$ とする. $T = \{t \in S \mid \langle t \rangle = S\}$ とする. このとき, $\mathbb{C}S$ の任意の (既約でなくてもよい) 指標 χ に対して, 任意の $t \in T$ に対して $\chi(\sigma_t) = n_t \bar{\chi}(\sigma_{t^R})$ を満たす $\mathbb{C}S//R \cong \mathbb{C}C_{\text{sg}(s)}$ の指標 $\bar{\chi}$ が存在する.

5 Burnside の定理の正則アソシエーション・スキームへの拡張

Isaacs [2] において, 有限群の Burnside の定理の証明には, 次の補題が用いられている.

補題 6. [2, Lemma 3.14] G を巡回群とし, χ を G の (既約でなくてもよい) 指標とする. $T = \{g \in G \mid$

$\langle g \rangle = G$ とする. 任意の $g \in G$ に対して, $\chi(g) \neq 0$ と仮定すると

$$\sum_{t \in T} |\chi(t)|^2 \geq |T|$$

が成り立つ.

前節の定理 5 を用いることにより, この補題を一元生成正則アソシエーション・スキームに拡張することができる.

補題 7. S を一元生成正則アソシエーション・スキームとし, χ を $\mathbb{C}S$ の (既約でなくてもよい) 指標とする. $T = \{t \in S \mid \langle t \rangle = S\}$ とする. 任意の $t \in T$ に対して, $\chi(\sigma_t) \neq 0$ と仮定すると,

$$\sum_{t \in T} \frac{\chi(\sigma_t)\chi(\sigma_{t^*})}{n_t} \geq n_T$$

が成り立つ.

この補題を用いれば, Isaacs [2] の Burnside の定理の証明 [2, Theorem 3.15] とほぼ同様に, 正則アソシエーション・スキームに対する Burnside の定理が示される.

定理 8. S を正則アソシエーション・スキームとし, $\chi \in \text{Irr}(S)$ を重複度 m_χ が 2 以上の既約指標とする. このとき, $\chi(\sigma_s) = 0$ となる S の relation s が必ず存在する.

参考文献

- [1] A. Hanaki and K. Hirotsuka, Irreducible Representations of Wreath Products of Association Schemes, J. Algebraic Combin. **18**, 47-52 (2003).
- [2] I. M. Isaacs: “Character Theory of Finite Groups”, Dover (1994).
- [3] M. Yoshikawa, On association schemes of finite exponent, European J. Combin. **51**, 433-442 (2016).
- [4] P. -H. Zieschang: “Theory of Association schemes. Springer Monographs in Mathematics”, Berlin-Heidelberg-New York (2005)