第 37 回代数的組合せ論シンポジウム報告集

2021 年 6 月 14 日－ 16 日
オンライン開催

まえがき

この報告集は 2021 年 6 月 14 日から 16 日にわたり、オンラインで行われた「第 37 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 85 名の参加者がありました。講演者の皆様をはじめ、ご参加いただいた皆様、この集会の開催にご協力いただいた皆様に深く感謝いたします。

世話人：
宗政 昭弘　（東北大）
徳重 典英　（琉球大）
島倉 裕樹　（東北大）
野崎 寛　（愛教大）
三枝崎 剛　（早大）

第 37 回代数的組合せ論シンポジウム

標記の研究集会を下記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）
徳重 典英 （琉球大）
島倉 裕樹 （東北大）
野崎 寛 （愛教大）
三枝崎 剛 （早大）

日程：2021 年 6 月 14 日 (月) ∼16 日 (水)
会場：Zoom を用いたオンライン開催

プログラム

6 月 14 日 (月)

9:30–10:10 石川雅雄（岡山大学）
Hankel type hyperpfaffians and the Selberg integrals
10:20–11:00 吉野聖人（東北大学）
Maximality of Seidel matrices and switching roots of graphs
11:10–11:50 中空大幸（神戸学院大学）
符号と格子に対する Assmus-Mattson 型の定理について
12:00–13:00 自由討論
13:20–14:00 谷口哲至（広島工業大学）
整化可能な整格子
14:10–15:00 見村万佐人（東北大学）
数体の素元星座定理 I
15:20–16:10 関真一朗（青山学院大学）
数体の素元星座定理 II
16:20–17:20 自由討論

6 月 15 日 (火)

9:30–10:10 新屋良磨（秋田大学）
原子語予想に対する密度的アプローチ
10:20–11:00 齋藤正顕（工学院大学）
正則グラフにおける non-backtracking cycle の個数の誤差項
11:10–11:50 佐久間雅（山形大学）
Pebble Exchange on Graphs and Graph Automorphism
12:00–13:00 自由討論
13:20–14:00 栗原大武（北九州工業高等専門学校）
有限群から得られる等質カンドルについて
14:10–15:00 松下尚弘（琉球大学）
Kneser グラフと共通の Kronecker 二重被覆を持つグラフについて
15:20–16:10 岸本大祐（京都大学）
Tverberg's theorem for cell complexes
16:20–17:20 自由討論

6 月 16 日 (水)

9:30–10:10　篠原雅史（滋賀大学）
ユークリッド空間における距離集合の分類問題について

10:20–11:00　入江佑樹（東北大学）
base-p Sprague-Grundy 型定理: マヤゲームと一般化対称群の表現

11:10–11:50　Hyungrok Jo（筑波大学）
Iterative construction of Cayley-type Ramanujan graphs and its cryptographic application

12:00–13:00　自由討論

目　次

Hankel type hyperpfaffians and the Selberg integrals

Masao ISHIKAWA*

岡山大学自然科学研究科
mi@math.okayama-u.ac.jp

2020 Mathematics Subject Classification : Primary 05A30 Secondary 33C50, 05A10, 33D50.

Keywords : Hankel Pfaffian, Selberg integral, moments of orthogonal polynomials, Narayana polynomials of Coxeter groups.

概要

講演の中では, パフィアンを計算する動機づけをのべるのに時間を割いたが, ここでは超パフィアンの等式を中心に述べることにする. 超パフィアンを扱うので式や証明が複雑になるが, セルバーグ積分がたいへん一般的な形の積分なので, それをフルに応用することを考えると超パフィアンまで拡張する必要がある. 主な結果がパフィアンの和公式の超パフィアン版であり, その応用として de Bruijn の 2 つの公式を超パフィアンに拡張する. de Bruijn の公式は 2 つあるが, 2 番目の方を応用するとパフィアン (さらに超パフィアン) の値を積分に帰着させることができる. 直交多項式については, いろいろなことが知られているので, その結果を使っていろいろなパフィアンを計算できることを最後の節で示す. q-類似についても面白い結果が得られるが紙面の都合上省略する. 詳細は Masao ISHIKAWA and Jiang ZENG, "Hankel hyperpfaffian calculations and Selberg integrals", arXiv:2008.09776 を見て欲しい.

1 Introduction

数え上げ組合せ論に現れる対象は平面分割など, その個数や母関数などが lattice path method 等を使って行列式で表されることが多い. 例えば Mills-Robbins-Rumsey [12] は回転対称かつ歪自己補完 (cyclically symmetric transpose complement) な平面分割の個

* Partially supported by JSPS KAKENHI Grant Numbers JP20K03558, 21K03202.

数が

$$\det\left(\binom{i+j}{2i-j}\right)_{0\le i,j\le n-1}.$$

で表せることを示した. 彼らは, この行列式の評価を Andrews の結果 [2] に帰着させたが, 一般的に行列式の評価は決して易しい問題ではない. Gessel-Xin [**?**] は, この行列式を Henkel 行列式に帰着させる方法を提示し, その他にも母関数を使って, Henkel 行列式に帰着できる行列式の研究を行った. Hankel 行列式の長所は, 直交多項式の古典論との関係を使って値を評価できる点である.

一方で, 数え上げ組合せ論に現れる対象には, Pfaffian で個数や母関数を計算できる例も多い. この研究の動機は, このような Pfaffian を同様に Hankel 型に帰着して評価できるかということである. この場合に Pfaffian に Hankel 型というものは, もともとないので, ここで Hankel 型というものを定義するが, 必ずしも, これが正しい定義かどうかわからない. もう少し広い範疇の Pfaffian に適用できる可能性もある. ここでは, 我々が Hankel 型と呼ぶ Pfaffian を定義し, その Pfaffian の計算がセルバーグ積分に帰着することを使って計算を行う. セルバーグ積分 [14] は一般に

$$\begin{aligned} S_n(\alpha,\beta,\gamma) &= \int_{[0,1]^n} \prod_{i=1}^{n} t_i^{\alpha-1}(1-t_i)^{\beta-1} \prod_{1\le i<j\le n} |t_i-t_j|^{2\gamma}\, d\boldsymbol{t} \\ &= \prod_{j=1}^{n} \frac{\Gamma(\alpha+(j-1)\gamma)\,\Gamma(\beta+(j-1)\gamma)\,\Gamma(j\gamma+1)}{\Gamma(\alpha+\beta+(n+j-2)\gamma)\,\Gamma(\gamma+1)}. \end{aligned} \tag{1.1}$$

の形をしている. また, 青本先生による拡張 [1]

$$\begin{aligned} &\int_{[0,1]^n} e_k(\boldsymbol{t}) \prod_{i=1}^{n} t_i^{\alpha-1}(1-t_i)^{\beta-1} \prod_{1\le i<j\le n} |t_i-t_j|^{2\gamma}\, d\boldsymbol{t} \\ &= \binom{n}{k} S_n(\alpha,\beta,\gamma) \prod_{j=1}^{k} \frac{\alpha+(n-j)\gamma}{\alpha+\beta+(2n-j-1)\gamma}, \end{aligned} \tag{1.2}$$

もある. ここで $e_k(\boldsymbol{t}) = e_k(t_1,\dots,t_n)$ は基本対称式で $\sum_{k=0}^{n} e_k(\boldsymbol{t})y^k = \prod_{i=1}^{n}(1+t_iy)$ によって定義される. この中で [6] の中の予想を解決するのみでなく, 拡張された問題を解決する. セルバーグ積分に帰着される過程で, その機能をフルに使うには普通のパフィアンではなく, 超パフィアン (huperpfaffian) を考えた方が良いことがわかる. そこで議論が, かなり一般論になるが次の節は超パフィアンの枠組みで議論を展開する. Luque-Thibon [9, 10, 11] による先行研究もある.

2　超行列式と超パフィアン

この節の目的は, 超行列式と超パフィアンを導入して, パフィアンの和公式 [7, Theorem 1], [8, Theorem 3.2] を超パフィアンに拡張することである.

正整数 n に対して $[n]=\{1,2,\dots,n\}$ と書く. 集合 S に対して S の r-元部分集合全体の集合を $\binom{S}{r}$ と書く. l, n を正整数とし S を ln-元集合とすうとき. $\binom{S}{l,\dots,l}$ (下の行は l が n 個) によって $1\le j\le n$ に対して $S_j\in\binom{S}{l}$ であり, かつ $S_1\cup\cdots\cup S_n=S$ (disjpint union) であるような n-個の組 $(S_1,\dots,S_n)$ 全体を表す.

正整数 n に対して $\mathfrak{S}_n$ を文字 $[n]$ 上の対称群とする. 対称群 $\mathfrak{S}_n$ の元を表すのに, $\sigma=(\sigma(1),\dots,\sigma(n))$ のような 1 行表示を用いる. $\sigma\in\mathfrak{S}_{ln}$ に対して, σ を長さが l の n 個のブロックに分割して書くことが便利なことが多い. すなわち $1\le k\le n$ に対して $\boldsymbol{\sigma}_k=(\sigma((k-1)l+1),\dots,\sigma(kl))$ とおき, $\sigma=(\boldsymbol{\sigma}_1,\dots,\boldsymbol{\sigma}_n)$ の形をしているとする. 各ブロック $\boldsymbol{\sigma}_k$ $(1\le k\le n)$ の中の文字が単調増加であるようなブロックの集まり $\sigma=(\boldsymbol{\sigma}_1,\dots,\boldsymbol{\sigma}_n)$ の形をした置換全体のなす $\mathfrak{S}_{ln}$ の部分集合を $\mathfrak{S}_{ln}(l,\dots,l)$ (l は n 回) によって表す. すなわち, $\mathfrak{S}_{ln}(l,\dots,l)$ は

$$\left\{\sigma=(\sigma(1),\dots,\sigma(ln))\in\mathfrak{S}_{ln}\,\middle|\,\sigma((j-1)l+1)<\cdots<\sigma(jl)\text{ for }1\le j\le n\right\}$$

とする. 今後 $I\in\binom{S}{l,\dots,l}$ を $\sigma\in\mathfrak{S}_{ln}(l,\dots,l)$ と同一視して, 対応する σ の符号 $\operatorname{sgn}\sigma$ を表すのに $\operatorname{sgn}I$ と書く. 例えば $l=n=2$ で $S=\{1,3,5,7\}$ のとき, $\binom{S}{2,2}$ は 6 個の元 $(\{1,3\},\{5,7\})$, $(\{1,5\},\{3,7\})$, $(\{1,7\},\{3,5\})$, $(\{3,5\},\{1,7\})$, $(\{3,7\},\{1,5\})$, $(\{5,7\},\{1,3\})$ からなる. それぞれの符号は, この順に $+$, $-$, $+$, $+$, $-$, $+$ である.

m を偶数, n を正整数とする. n 次の m-次元テンソルとは $A=(A(i_1,\dots,i_m))_{1\le i_1,\dots,i_m\le n}$ とは写像 $A:[n]^m\to F$, $(i_1,\dots,i_m)\mapsto A(i_1,\dots,i_m)$ のこととする. ここで F は標数 0 の体としておく. また, A の第 $(i_1,\dots,i_{m-1})$ 行を $(A(i_1,\dots,i_{m-1},1),\dots,A(i_1,\dots,i_{m-1},n))$ とする. A の **超行列式 (hyperdeterminant)** $\det^{[m]}A$ を

$$\begin{aligned}\det{}^{[m]}A&=\frac{1}{n!}\sum_{\sigma_1,\dots,\sigma_m\in\mathfrak{S}_n}\operatorname{sgn}(\sigma_1\cdots\sigma_m)\prod_{i=1}^{n}A(\sigma_1(i),\sigma_2(i),\dots,\sigma_m(i))\\&=\sum_{\sigma_1,\dots,\sigma_{m-1}\in\mathfrak{S}_n}\operatorname{sgn}(\sigma_1\cdots\sigma_{m-1})\prod_{i=1}^{n}A(\sigma_1(i),\dots,\sigma_{m-1}(i),i).\end{aligned}\tag{2.1}$$

によって定義する. 行列のときに, 添字の動く範囲を制限することによって部分行列を得たように, ここでは n 次の m-次元テンソルの部分テンソルの概念を準備する. $[n]$ の部分集合の m-個の組 $(I^{(1)},\dots,I^{(m)})$ を準備しよう. すなわち $I^{(1)},\dots,I^{(m)}\in\binom{[n]}{r}$ とする. このとき

$$A_{I^{(1)},\cdots,I^{(m)}}=(A(i^{(1)},\dots,i^{(m)}))_{i^{(1)}\in I^{(1)},\dots,i^{(m)}\in I^{(m)}}.$$

を, 添字を $(I^{(1)},\dots,I^{(m)})$ に制限して得られる部分テンソルとする. また, 超行列式 $\det^{[m]}A_{I^{(1)},\cdots,I^{(m)}}$ を A の $(I^{(1)},\cdots,I^{(m)})$-**小超行列式 (minor)** といい, $a_{I^{(1)},\cdots,I^{(m)}}$ と書くことにする. 次の補題は, 超行列式のラプラス展開と言えるものである. もう少し一般的な形でも述べることができるが, この形が 定理 2.3 の証明で重要である.

補題 2.1. l, m, n, N を正整数で $ln \le N$ を満たすとする. $A = (A(i_1,\dots,i_m))_{1\le i_1,\dots,i_m\le N}$ を N 次の m-次元テンソルとする. $I = \{i_1,\dots,i_{ln}\} \in \binom{N}{ln}$ を長さ l のブロックに分けて $I = (I_1,\dots,I_n)$ と書く. すなわち, $I_j = \{i_{(j-1)l+1},\dots,i_{jl}\}$ $(1 \le j \le n)$ である. このとき

$$\det{}^{[m]}A_{[ln],\dots,[ln],I} = \sum_{I^{(1)},\dots,I^{(m-1)}\in\binom{[ln]}{l,\dots,l}} \operatorname{sgn} I^{(1)}\cdots\operatorname{sgn} I^{(m-1)} \prod_{j=1}^{n} \det{}^{[m]}A_{I_j^{(1)},\dots,I_j^{(m-1)},I_j}, \tag{2.2}$$

が成り立つ. ここで $1 \le j \le n$, $1 \le k \le m-1$ に対して $I^{(k)} = (I_1^{(k)},\dots,I_n^{(k)})$ $(I_j^{(k)} \in \binom{[ln]}{l})$ のようにブロックで表した表現である.

Barvinok [3] が最初に超パフィアン (hyperpfaffian) を定義した. 普通のパフィアンは歪対称行列に対してマッチングを使って定義される. すなわち, 行列が $B = (B(i,j))_{i,j\in[2n]}$ 歪対称とは $B(j,i) = -B(i,j)$ 満たすことであるが, この条件から $B(i,i) = 0$ であり, 歪対称行列は写像 $\mathscr{B} : \binom{[2n]}{2} \to F$, $\{i,j\} \mapsto \mathscr{B}(\{i,j\}) = B(i,j)$ $(i<j)$ と看做すことができる. Barvinok の超パフィアンは偶数 l に対して, $\mathscr{B} : \binom{[ln]}{l} \to F$, $\mathscr{B}(\{i_1,\dots,i_l\}) = B(i_1,\dots,i_l)$ $(i_1 < \cdots < i_l)$ というテンソルに対してであったが, ここではもう少し拡張して次のような状況を考える.

l, m, n を正整数とし, l は偶数とする. 写像 $\mathscr{B} : \binom{[ln]}{l}^m \to F$, $(I^{(1)},\dots,I^{(m)}) \mapsto \mathscr{B}(I^{(1)},\dots,I^{(m)})$ を

$$\mathscr{B} = \left(\mathscr{B}(I^{(1)},\dots,I^{(m)})\right)_{I^{(1)},\dots,I^{(m)}\in\binom{[ln]}{l}},$$

と書く. このとき **超パフィアン (hyperpfaffian)** $\mathrm{Pf}^{[l,m]}(\mathscr{B})$ を

$$\mathrm{Pf}^{[l,m]}(\mathscr{B}) = \frac{1}{n!} \sum_{I^{(1)},\dots,I^{(m)}\in\binom{[ln]}{l,\dots,l}} \operatorname{sgn}(I^{(1)})\cdots\operatorname{sgn}(I^{(m)}) \prod_{j=1}^{n} \mathscr{B}\left(I_j^{(1)},\dots,I_j^{(m)}\right), \tag{2.3}$$

によって定義する. ここで, $I^{(k)} = (I_1^{(k)},\dots,I_n^{(k)})$ with $I_j^{(k)} \in \binom{[ln]}{l}$ $(1 \le j \le n,\ 1 \le k \le m)$ とする. 超パフィアン $\mathrm{Pf}^{[l,m]}\left(\mathscr{B}(I_1,\dots,I_m)\right)_{I_1,\dots,I_m\in\binom{[ln]}{l}}$ を短く $\mathrm{Pf}^{[l,m]}(\mathscr{B})$ とも書く. $l=2$, $m=1$ のときは, 普通のパフィアンになる.

前述の超行列式と同様に, 添字の動く範囲を制限することにより, 部分超パフィアンを考えることが必要になる. 考え方は単純であるが, notation が長くなる. $\mathscr{B} = (\mathscr{B}(I_1, \dots, I_m))_{I_1,\dots,I_m \in \binom{[ln]}{l}}$ ln 次 m-次元配列とし, r を $1 \le r \le n$ であるような正整数とする. $1 \le k \le m$ に対して $S^{(k)} \in \binom{[ln]}{lr}$ であるような m 個の組 $(S^{(1)}, \dots, S^{(m)})$ に対して $\mathscr{B}_{S^{(1)},\cdots,S^{(m)}}$ によって, 添字を制限した lr 次の m-次元 l-ブロック配列

$$(\mathscr{B}(I_1, \dots, I_m))_{I_1 \in \binom{S^{(1)}}{l}, \dots, I_m \in \binom{S^{(m)}}{l}}$$

を表す. その超パフィアン

$$\mathrm{Pf}^{[l,m]}(\mathscr{B}_{S^{(1)},\cdots,S^{(m)}}) = \frac{1}{r!} \sum_{I^{(1)} \in \binom{S^{(1)}}{l,\dots,l}, \dots, I^{(m)} \in \binom{S^{(m)}}{l,\dots,l}} \prod_{k=1}^{m} \mathrm{sgn}(I^{(k)}) \prod_{j=1}^{r} \mathscr{B}\left(I_j^{(1)}, \cdots, I_j^{(m)}\right), \tag{2.4}$$

を $\mathscr{B}$ の **部分超パフィアン (subhyperpfaffian)** と呼ぶ. ここで和の中の記号は $I^{(k)} = (I_1^{(k)}, \dots, I_r^{(k)})$ という意味である.

証明は述べないが, 次の和は普通のパフィアンでは良く知られた結果を超パフィアンに拡張したものであり, de Bruijn 型の公式を証明するのに本質的に使う. 記号として, 次のものを使う. 正の整数 λ に対して $D_l(\lambda) = \{l(\lambda-1)+1, l(\lambda-1)+2, \dots, l(\lambda-1)+l\}$ と置き, $1 \le \lambda_1 < \cdots < \lambda_n \le N$ に対して $D_l(\lambda_1, \dots, \lambda_n) = D_l(\lambda_1) \cup \cdots \cup D_l(\lambda_n)$ と書く. $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n) \in \binom{[N]}{n}$ に対して短く $D_l(\boldsymbol{\lambda})$ と書く.

補題 2.2. l, m, n, N が正整数で l は偶数, $n \le N$ とする. lN 次の m-次元 l-ブロック配列 $\mathscr{B} = (\mathscr{B}(I^{(1)}, \cdots, I^{(m)}))_{I^{(1)},\cdots,I^{(m)} \in \binom{lN}{l}}$ を

$$\mathscr{B}(I^{(1)}, \cdots, I^{(m)}) = \begin{cases} 1 & \text{if } I^{(k)} = D_l(\lambda^{(k)}) \text{ for some } \lambda^{(k)} \in [N] \ (1 \le k \le m), \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

とする. このとき $S^{(1)}, \dots, S^{(m)} \in \binom{[lN]}{ln}$ に対して

$$\mathrm{Pf}^{[l,m]}(\mathscr{B}_{S^{(1)},\dots,S^{(m)}}) = \begin{cases} 1 & \text{if } S^{(k)} = D_l(\boldsymbol{\lambda}^{(k)}) \text{ for some } \boldsymbol{\lambda}^{(k)} \in \binom{[N]}{n} \ (1 \le k \le m), \\ 0 & \text{otherwise.} \end{cases} \tag{2.6}$$

となる.

例えば, $l = 2$, $m = 1$ のとき, $\mathscr{B}$ は

$$\mathscr{B}(I) = \begin{cases} 1 & \text{if } I = \{2\lambda-1, 2\lambda\} \text{ for } 1 \le \lambda \le N, \\ 0 & \text{otherwise.} \end{cases}$$

によって定義される配列 (歪対称行列) で, $S \in \binom{[2N]}{2n}$ が $S = \{2\lambda_1 - 1, 2\lambda_1\} \cup \cdots \cup \{2\lambda_n - 1, 2\lambda_n\}$ $(1 \leq \lambda_1 < \cdots < \lambda_n \leq N)$ の形のとき $\mathrm{Pf}(\mathscr{B}_S)$ の値が 1 で, それ以外のとき 0 になる.

次の定理はパフィアンの和公式 ([7, 8]) と呼ばれるものの超パフィアン版であり, de Brijn の定理の超パフィアン版をすべてこれを使って証明する.

定理 2.3. l, m, n, N, r を正整数とし, l が偶数で $ln \leq N$ とする. $1 \leq \nu \leq r$ なる整数 ν に対して $H(\nu) = (H(\nu)(i_1, \ldots, i_m))_{1 \leq i_1, \ldots, i_{m-1} \leq ln,\, 1 \leq i_m \leq N}$ が, サイズが $(ln, \ldots, ln, N)$ である m-次元で, $\mathscr{B} = (\mathscr{B}(I^{(1)}, \ldots, I^{(r)}))_{I^{(1)}, \cdots, I^{(r)} \in \binom{[N]}{l}}$ をサイズが N の r-次元 l-ブロック配列とする. このとき

$$\sum_{S^{(1)}, \ldots, S^{(r)} \in \binom{[N]}{ln}} \mathrm{Pf}^{[l,r]}(\mathscr{B}_{S^{(1)}, \ldots, S^{(r)}}) \prod_{\nu=1}^{r} \det{}^{[m]} H(\nu)_{[ln], \ldots, [ln], S^{(\nu)}} = \mathrm{Pf}^{[l,(m-1)r]}(Q), \tag{2.7}$$

が成り立つ. ここで, 右辺の配列

$$Q = (Q(I^{(1,1)}, \ldots, I^{(1,m-1)}, \ldots, I^{(r,1)}, \ldots, I^{(r,m-1)}))_{I^{(1,1)}, \ldots, I^{(r,m-1)} \in \binom{[ln]}{l}}$$

はサイズが ln の $(m-1)r$-次元 l-ブロック配列であり

$$\begin{aligned} &Q(I^{(1,1)}, \ldots, I^{(1,m-1)}, \ldots, I^{(r,1)}, \ldots, I^{(r,m-1)}) \\ &= \sum_{K^{(1)}, \ldots, K^{(r)} \in \binom{[N]}{l}} \mathscr{B}(K^{(1)}, \ldots, K^{(r)}) \prod_{\nu=1}^{r} \det{}^{[m]}(H(\nu)_{I^{(\nu,1)}, \ldots, I^{(\nu,m-1)}, K^{(\nu)}}) \end{aligned} \tag{2.8}$$

によって定義される.

定理 2.3 において $m = 2$ と置けば, 超行列式は普通の行列式なので次の系を得る.:

系 2.4. l, n, N, r が正の整数で l は偶数, $ln \leq N$ とする. $1 \leq \nu \leq r$ に対して $H(\nu) = (h_{ij}(\nu))_{1 \leq i \leq ln, 1 \leq j \leq N}$ を $ln \times N$ 矩形行列とし, $\mathscr{B} = (\mathscr{B}(I^{(1)}, \cdots, I^{(r)}))_{I^{(1)}, \cdots, I^{(r)} \in \binom{[N]}{l}}$ をサイズが N の r-次元 l-ブロック配列とする. このとき

$$\sum_{S^{(1)}, \ldots, S^{(r)} \in \binom{[N]}{ln}} \mathrm{Pf}^{[l,r]}(\mathscr{B}_{S^{(1)}, \ldots, S^{(r)}}) \prod_{\nu=1}^{r} \det H(\nu)_{[ln], S^{(\nu)}} = \mathrm{Pf}^{[l,r]}(Q), \tag{2.9}$$

が成り立つ. ここで $Q = (Q(I^{(1)}, \ldots, I^{(r)}))_{I^{(1)}, \ldots, I^{(r)} \in \binom{[ln]}{l}}$ is はサイズが ln の r-次元 l-ブロック配列で, その成分は

$$Q(I^{(1)}, \ldots, I^{(r)}) = \sum_{K^{(1)}, \ldots, K^{(r)} \in \binom{[N]}{l}} \mathscr{B}(K^{(1)}, \ldots, K^{(r)}) \prod_{\nu=1}^{r} \det(H(\nu)_{I^{(s)}, K^{(s)}}) \tag{2.10}$$

によって定義される.

3　超パフィアンに関する De Bruijn の公式

De Bruijn は次の 2 つの主要なパフィアンの公式, [4, (4,7)] と [4, (7.3)] を得た. この節では, その超パフィアンへの一般化を考える. まず, [4, (4,7)] 式は次のようなものである. $s(x,y)$ を $s(x,y)=-s(y,x)$ をみたす関数とし, $S=S(x_1,\dots,x_n)$ $(1\le i,j\le n)$ を (i,j) 成分が $s_{ij}=s(x_i,x_j)$ である歪対称行列とする. このとき

$$\int\cdots\int_{a\le x_1<\cdots<x_n\le b}\mathrm{Pf}(S(x_1,\dots,x_n))\det(\phi_i(x_j))_{1\le i,j\le n}dx_1\cdots d_n=\mathrm{Pf}(A_s)\quad(3.1)$$

が成り立つ. ここで A_s は (i,j) 成分が

$$a_{ij}=\int_a^b\int_a^b\psi_i(x)\psi_j(y)s(x,y)\,dxdy\qquad(3.2)$$

で定義される n 次の歪対称行列である.

もう 1 つの公式 [4, (7.3)] は次のようなものである. $\phi_1,\dots,\phi_{2n},\psi_1,\dots,\psi_{2n}$ を x の関数とし $(\phi_i(x_j)|\psi_i(x_j))_{i\in[2n],j\in[n]}$ が, 第 i $(i\in[2n])$ 行が

$$\begin{pmatrix}\phi_i(x_1) & \psi_i(x_1) & \dots & \phi_i(x_n) & \psi_i(x_n)\end{pmatrix}$$

を表す行列とする. このとき

$$\begin{aligned}&\int_{0\le x_1<\cdots<x_n\le\alpha}\det(\phi_i(x_j)|\psi_i(x_j))_{i\in[2n],j\in[n]}dx_1\cdots dx_n\\&\qquad=\mathrm{Pf}\left(\int_0^\alpha\begin{vmatrix}\phi_{i_1}(x)&\psi_{i_1}(x)\\\phi_{i_2}(x)&\psi_{i_2}(x)\end{vmatrix}dx\right)_{i_1,i_2\in[2n]}\end{aligned}\qquad(3.3)$$

が成り立つ. 特に, 後者の (3.3) のタイプの式を, ここでは使うが, 一般のセルバーグ積分にも使えるように超パフィアンに拡張する. また, q-アナログを扱うためにジャクソン積分の枠組みで述べる.

$f(x)$ が区間 $[0,\alpha]$ 上の関数のとき, ジャクソン積分は

$$\int_0^\alpha f(x)\,d_qx(1-q)\alpha\sum_{n=0}^\infty f(\alpha q^n)q^n$$

によって定義する. ここでは $|q|<1$ とする. また $[0,\alpha]$ 上の重み関数を w として $d_q\omega(x)=w(x)d_qx$ と書く. さらに多重積分を

$$\begin{aligned}&\int_{0\le x_1<\cdots<x_n\le\alpha}f(x_1,\dots,x_n)d_q\omega(x_1)\cdots\omega(x_n)\\&=(1-q)^n\alpha^n\sum_{0\le i_1<\cdots<i_n}f(\alpha q^{i_n},\dots,\alpha q^{i_1})w(\alpha q^{i_1})\cdots w(\alpha q^{i_n})q^{i_1+\cdots+i_n}.\end{aligned}$$

によって定義する. このとき, De Bruijn の 1 つ目の等式 (3.1) の超パフィアン版は次のものである. 証明は, 定理 2.3 を使う.

定理 3.1. l, m, n, r を正整数とし, l は偶数と仮定する. $i_1,\dots,i_{m-1}\in[ln]$, $1\le\nu\le r$ に対して, $\phi^{(\nu)}_{i_1,\dots,i_{m-1}}(y)$ を $[0,\alpha]$ 上の関数とする. $\boldsymbol{y}^{(\nu)}=(y_1^{(\nu)},\dots,y_l^{(\nu)})\in[0,\alpha]^l$ $(1\le\nu\le r)$ とし $f(\boldsymbol{y}^{(1)},\dots,\boldsymbol{y}^{(r)})$ を $\boldsymbol{y}^{(1)},\dots,\boldsymbol{y}^{(r)}$ の関数とするとき,

$$\int_{0\le x_1^{(1)}<\cdots<x_{ln}^{(1)}\le\alpha}\cdots\int_{0\le x_1^{(r)}<\cdots<x_{ln}^{(r)}\le a}\mathrm{Pf}^{[l,r]}\left(f(\boldsymbol{x}^{(1)}_{I^{(1)}},\dots,\boldsymbol{x}^{(r)}_{I^{(r)}})\right)_{I^{(1)},\dots,I^{(r)}\in\binom{[ln]}{l}}$$
$$\times\prod_{\nu=1}^{r}\det{}^{[m]}\left(\phi^{(\nu)}_{j_1,\dots,j_{m-1}}(x^{(\nu)}_{j_m})\right)_{1\le j_1,\dots,j_m\le ln}d_q\omega(\boldsymbol{x}^{(s)})=\mathrm{Pf}^{[l,(m-1)r]}(Q)\,,\quad(3.4)$$

が成り立つ. ここで $I^{(1,1)},\dots,I^{(1,m-1)},\dots,I^{(r,1)},\dots,I^{(r,m-1)}\in\binom{[ln]}{l}$ に対して

$$Q(I^{(1,1)},\dots,I^{(1,m-1)},\dots,I^{(r,1)},\dots,I^{(r,m-1)})=\int_{0\le x_1^{(1)}<\cdots<x_l^{(1)}\le\alpha}\cdots\int_{0\le x_1^{(r)}<\cdots<x_l^{(r)}\le\alpha}$$
$$f(\boldsymbol{x}^{(1)},\dots,\boldsymbol{x}^{(r)})\prod_{\nu=1}^{r}\det{}^{[m]}(\phi^{(\nu)}_{i^{(\nu,1)},\cdots,i^{(\nu,m-1)}}(x^{(\nu)}_{i_m}))_{i^{(\nu,1)}\in I^{(\nu,1)},\dots,i^{(\nu,m-1)}\in I^{(\nu,m-1)},i_m\in[l]}$$
$$\times\prod_{\nu=1}^{r}d_q\omega(x_1^{(\nu)})\cdots d_q\omega(x_l^{(\nu)})\quad(3.5)$$

ここで $\boldsymbol{x}^{(\nu)}=(x_1^{(\nu)},\dots,x_{ln}^{(\nu)})$ のとき $I^{(\nu)}=\{i_1^{(\nu)},\dots,i_l^{(\nu)}\}\in\binom{[ln]}{l}$ $(1\le\nu\le r)$ に対して $\boldsymbol{x}^{(\nu)}_{I^{(\nu)}}=(x^{(\nu)}_{i_1^{(\nu)}},\dots,x^{(\nu)}_{i_l^{(\nu)}})$ と書く. また $\boldsymbol{x}^{(\nu)}$ は $(x_1^{(\nu)},\dots,x_l^{(\nu)})$ を表す.

De Bruijn の 2 番目の等式 (3.3) の超パフィアンへの一般化は次のようになる. ここでは, 主に, こちらの式を使う. Luque-Thibon による [9, (96)] の式は, この定理の特別な場合である.

定理 3.2. l, m, n, r を正整数とし, l を偶数と仮定する. $\boldsymbol{i}'=(i_1,\dots,i_{m-1})\in[ln]^{m-1}$ $(\nu\in[r],\,k\in[l])$ に対して $\phi^{(\nu,k)}_{\boldsymbol{i}'}(x)=\phi^{(\nu,k)}_{i_1,\dots,i_{m-1}}(x)$ を $[0,\alpha]$ 上の関数とする. このとき

$$\int_{0\le x_1^{(1)}<\cdots<x_n^{(1)}\le\alpha}\cdots\int_{0\le x_1^{(r)}<\cdots<x_n^{(r)}\le\alpha}\prod_{\nu=1}^{r}\det{}^{[m]}\left(\phi^{(\nu,1)}_{\boldsymbol{i}'}(x_j^{(\nu)})\middle|\cdots\middle|\phi^{(\nu,l)}_{\boldsymbol{i}'}(x_j^{(\nu)})\right)_{\boldsymbol{i}'\in[ln]^{m-1},\,j\in[n]}$$
$$\times\prod_{\nu=1}^{r}d_q\omega(\boldsymbol{x}^{(\nu)})=\mathrm{Pf}^{[l,(m-1)r]}(Q)\,,\quad(3.6)$$

このとき $d_q\omega(\boldsymbol{x}^{(\nu)})=d_q\omega(x_1^{(\nu)})\cdots d_q\omega(x_n^{(\nu)})$ であり Q は $I^{(1,1)},\dots,I^{(r,m-1)}\in\binom{[ln]}{l}$

に対して

$$Q(I^{(1,1)},\dots,I^{(1,m-1)},\dots,I^{(r,1)},\dots,I^{(r,m-1)})$$
$$=\int_{[0,\alpha]^r}\prod_{\nu=1}^{r}\det{}^{[m]}\left(\phi^{(\nu,k)}_{i^{(\nu,1)},\dots,i^{(\nu,m-1)}}(x^{(\nu)})\right)_{i^{(\nu,1)}\in I^{(\nu,1)},\dots,i^{(\nu,m-1)}\in I^{(\nu,m-1)},k\in[l]}d_q\omega(x^{(\nu)}) \tag{3.7}$$

によって定義される. ここで $\left(\phi^{(\nu,1)}_{\boldsymbol{i}'}(y_j)\middle|\cdots\middle|\phi^{(\nu,l)}_{\boldsymbol{i}'}(y_j)\right)_{\boldsymbol{i}'\in[ln]^{m-1},\,j\in[n]}$ は $\boldsymbol{i}'$ 行が

$$\left(\phi^{(\nu,1)}_{\boldsymbol{i}'}(y_1),\cdots,\phi^{(\nu,l)}_{\boldsymbol{i}'}(y_1),\dots,\phi^{(\nu,1)}_{\boldsymbol{i}'}(y_n),\cdots,\phi^{(\nu,l)}_{\boldsymbol{i}'}(y_n)\right).$$

によって定義される ln 次の m-次元テンソルである.

ここからは, この 2 番目の de Bruijn 型の等式 (3.2) の応用である. [5] の中で使われた記号

$$\Delta^1_k(\boldsymbol{x})=\Delta^1_k(x_1,\dots,x_n)=\prod_{i<j}\prod_{\nu=0}^{k-1}(x_j-q^{\nu}x_i)(x_j-q^{-\nu}x_i) \tag{3.8}$$

を使おう. また $(q)_k=(q;q)_k=\prod_{i=1}^{k}(1-q^i)$ という記号を使う.

系 3.3. l, n を正整数とし, l を偶数とする. また t を整数とし, $\mu_i=\int_0^{\alpha}x^i d_q\omega(x)$ を測度 ω の 第 i 番目のモーメントとする. このとき

$$\mathrm{Pf}^{[l,1]}\Big(\prod_{1\le j<k\le l}(q^{i_j-1}-q^{i_k-1})\cdot\mu_{\sum_{k=1}^{l}i_k+t-l}\Big)_{1\le i_1<i_2<\cdots<i_l\le ln}$$
$$=q^{n\binom{l}{3}+l\binom{l}{2}\binom{n}{2}}\prod_{k=1}^{l}(q)_{k-1}^{n}\int_{0\le x_1<\cdots<x_n\le\alpha}\prod_{i=1}^{n}x_i^{t+\binom{l}{2}}\prod_{1\le i<j\le n}(x_j-x_i)^{-l}\prod_{k=1}^{l}\Delta^1_k(\boldsymbol{x})\,d_q\omega(\boldsymbol{x}), \tag{3.9}$$

が成り立つ. ここで $d_q\omega(\boldsymbol{x})=d_q\omega(x_1)\cdots d_q\omega(x_n)$ とする.

この系 3.3 で $q\to 1$ とすると, 次の系を得る. 我々は, この系の右辺に現れる積分をセルバーグ-青本型の積分に帰着する方法を考える.

系 3.4. l, n は正整数で l は偶数, t を整数とする. $d\psi(x)=\psi'(x)dx$ を区間 $[0,\alpha]$ 上の測度とし, $\mu_i=\int_0^{\alpha}x^i d\psi(x)$ を測度 ψ の第 i 番目のモーメントとする. このとき

$$\mathrm{Pf}^{[l,1]}\Big(\prod_{1\le j<k\le l}(i_k-i_j)\cdot\mu_{\sum_{k=1}^{l}i_k-l+t}\Big)_{1\le i_1<\cdots<i_l\le ln}$$
$$=\frac{\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\int_{[0,\alpha]^n}\prod_i x_i^{t+\binom{l}{2}}\prod_{i<j}(x_j-x_i)^{l^2}\,d\psi(\boldsymbol{x}) \tag{3.10}$$

が成り立つ.

この系を応用した結果が, 次の節である.

4 モツキン数, デラノイ数, シュレーダー数とナラヤナ多項式

この節の目標は [6, Conjecture 6.2] で述べられたモツキン数, デラノイ数, シュレーダー数に関する予想を, もっと一般的な形で証明することである. そのために系 3.4 を使う. 一般化するために, A, B, D 型のコクセター群のナラヤナ多項式を定義する.

A, B, D 型の **ナラヤナ数 (Narayana numbers)** は, それぞれ

$$N_k(A_n)=\frac{1}{n}\binom{n}{k}\binom{n}{k-1},\quad N_k(B_n)=\binom{n}{k}^2,\quad N_k(D_n)=\binom{n}{k}\left\{\binom{n-1}{k}+\binom{n-2}{k-2}\right\}$$

によって定義される ([13, pp. 277–278] 参照). $X=A,B,D$ に対して, それぞれの型の **ナラヤナ多項式 (Narayana polynomials)** $N(X_n,a)$ $(n\geq 0)$ は

$$N(X_n,a)=\sum_{k=0}^{n}N_k(X_n)a^k \tag{4.1}$$

によって定義される. ここで, のちの便宜上 $N(A_0,a)=(D_0,a)=1$, $N(D_1,a)=\frac{a+1}{2}$ とおくことにする. また ${}_2F_1(a,b;c;x)=\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{n!(c)_n}x^n$ をガウスの超幾何級数とする. ここで $(x)_n=\frac{\Gamma(x+n)}{\Gamma(x)}$ は**ポッホハマー記号 (Pochhammer symbol)** とする. 大事なのは, 次の点である.

注 4.1. n を非負整数とし, $\omega=\frac{-1\pm\sqrt{-3}}{2}$ を 1 の原始 3 乗根とする. このとき, 次の特殊化が知られている. $n\geq 0$ に対して $\mathrm{Cat}(n)=N(A_n,1)=\frac{1}{2n+1}\binom{2n+1}{n}$ はカタラン数 (Catalan numbers), $\mathrm{Sch}(n)=N(A_n,2)=\sum_{k=0}^{n}\binom{n+k}{2k}\mathrm{Cat}(k)$ はシュレーダー数 (large Schröder numbers), $\mathrm{CBC}(n)=N(B_n,1)=\binom{2n}{n}$ は中央二項係数 (central binomial coefficients), $\mathrm{Del}(n)=N(B_n,2)=\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}$ はデラノイ数 (central Delannoy numbers) と呼ばれる. $n\geq 1$ に対する数列 $N(D_n,1)=(3n-2)\mathrm{Cat}(n-1)$ は名前を持たないが, 組合せ論のいろいろな場面で現れる. さらに $\mathrm{Mot}(n)=(-1)^n\omega^{n+2}N\left(A_{n+1},\omega\right)=\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{2k}\mathrm{Cat}(k)$ $(n\geq 0)$ はモツキン数 (Motzkin numbers), and $\mathrm{CTC}(n)=(-1)^n\omega^nN\left(B_n,\omega\right)$ $(n\geq 0)$ は中央三項係数 (central trinomial coefficient) と呼ばれ, $(1+x+x^2)^n$ の x^n の係数である. 最後に $\mathrm{Mot}^D(n)=(-1)^n\omega^nN\left(D_n,\omega\right)={}_2F_1\left(\frac{1-n}{2},1-\frac{n}{2};1;4\right)+(n-2){}_2F_1\left(1-\frac{n}{2},\frac{3}{2}-\frac{n}{2};2;4\right)$ $(n\geq 2)$ は D 型のモツキン数 (Motzkin number for Coxeter type D) と呼ばれる.

ここでは, 系 3.4 とセル—バーグ-青本の公式 (1.1), (1.2) の応用として得られる公式を述べる.

まず, 次のように置く:

$$\Phi_n(r,s,m)=\prod_{j=1}^{n}\frac{\binom{2m(j-1)+2r}{m(j-1)+r}\binom{2m(j-1)+2s}{m(j-1)+s}}{\binom{2m(j-1)+r+s}{m(j-1)+r}}\prod_{j=2}^{n}\frac{\binom{mj}{m}}{\binom{m(2j-3)+r+s}{m(j-1)}}. \tag{4.2}$$

このとき, この節の結果の最も一般的な形 (超パフィアンの場合) は次の定理である.

定理 4.2. l, n を正整数とし, l は偶数とする. r を $r\geq-\binom{l}{2}$ である整数とし, a を複素数とする. このとき, 次の等式が成り立つ.

$$\begin{aligned}&\mathrm{Pf}^{[l,1]}\Big(\prod_{1\leq j<k\leq l}(i_k-i_j)\cdot N\left(A_{|I|+r-l},a\right)\Big)_{I\in\binom{[ln]}{l}}\\&=\begin{cases}\frac{\prod_{k=1}^{l}\{(k-1)!\}^n}{2^n n!}\cdot\Phi_n\left(r+\binom{l}{2},1,\frac{l^2}{2}\right) & \text{if } a=1,\\ \frac{a^{n+\frac{l^2}{2}\binom{n}{2}}\prod_{k=1}^{l}\{(k-1)!\}^n}{2^n n!}\Phi_n\left(1,1,\frac{l^2}{2}\right) & \text{if } r=1-\binom{l}{2},\\ \frac{2^n a^{\frac{3}{2}n+\frac{l^2}{2}\binom{n}{2}}\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\Phi_n\left(1,1,\frac{l^2}{2}\right)\sum_{k=0}^{n}\binom{n}{k}B_a^{n-k}\prod_{j=1}^{k}\frac{\frac{3}{2}+\frac{l^2}{2}(n-j)}{3+\frac{l^2}{2}(2n-j-1)} & \text{if } r=2-\binom{l}{2},\end{cases}\end{aligned} \tag{4.3}$$

ここで $B_a=\frac{(\sqrt{a}-1)^2}{4\sqrt{a}}$ とする.

$$\begin{aligned}&\mathrm{Pf}^{[l,1]}\Big(\prod_{1\leq j<k\leq l}(i_k-i_j)\cdot N\left(B_{|I|+r-l},a\right)\Big)_{I\in\binom{[ln]}{l}}\\&=\begin{cases}\frac{\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\cdot\Phi_n\left(r+\binom{l}{2},0,\frac{l^2}{2}\right) & \text{if } a=1,\\ \frac{a^{\frac{l^2}{2}\binom{n}{2}}\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\Phi_n\left(0,0,\frac{l^2}{2}\right) & \text{if } r=-\binom{l}{2},\\ \frac{2^{2n}a^{\frac{n}{2}+\frac{l^2}{2}\binom{n}{2}}\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\Phi_n\left(0,0,\frac{l^2}{2}\right)\sum_{k=0}^{n}\binom{n}{k}B_a^{n-k}\prod_{j=1}^{k}\frac{\frac{1}{2}+\frac{l^2}{2}(n-j)}{1+\frac{l^2}{2}(2n-j-1)} & \text{if } r=1-\binom{l}{2}.\end{cases}\end{aligned} \tag{4.4}$$

$$\begin{aligned}&\mathrm{Pf}^{[l,1]}\Big(\prod_{1\leq j<k\leq l}(i_k-i_j)\cdot N(D_{|I|+r-l},a)\Big)_{I\in\binom{[ln]}{l}}\\&=\begin{cases}\frac{2^{2n}\prod_{k=1}^{l}\{(k-1)!\}^n}{n!}\Phi_n\left(r+\binom{l}{2}-1,0,\frac{l^2}{2}\right)\sum_{k=0}^{n}\binom{n}{k}\left(-\frac{1}{4}\right)^{n-k}\prod_{j=1}^{k}\frac{r+\binom{l}{2}-\frac{1}{2}+\frac{l^2}{2}(n-j)}{r+\binom{l}{2}+\frac{l^2}{2}(2n-j-1)} & \text{if } a=1,\\ \frac{2^{2n}\omega^{n+\frac{l^2}{2}\binom{n}{2}}\prod_{k=1}^{n}\{(k-1)!\}^n}{n!}\Phi_n\left(1,0,\frac{l^2}{2}\right)\sum_{k=0}^{n}\binom{n}{k}\left(-\frac{5}{8}\right)^{n-k}\prod_{j=1}^{k}\frac{\frac{3}{2}+\frac{l^2}{2}(n-j)}{2+\frac{l^2}{2}(2n-j-1)} & \text{if } a=\omega \text{ and } r=2-\binom{l}{2}.\end{cases}\end{aligned} \tag{4.5}$$

ここでは, 右辺において $\sqrt{a}$ の適当な分枝を選ぶ必要がある.

これらの一般の超パフィアンの等式で $l=2$ とおくと [6] の中で述べられた次の等式の証明が得られるだけでなく, いろいろな等式が得られる.

系 4.3. $n \geq 1$ を整数とするとき, 次の等式が成り立つ:

$$\operatorname{Pf}\Big((j-i)\operatorname{Mot}(i+j-3)\Big)_{1\leq i,j\leq 2n} = \prod_{k=0}^{n-1}(4k+1), \tag{4.6}$$

$$\operatorname{Pf}\Big((j-i)\operatorname{Del}(i+j-3)\Big)_{1\leq i,j\leq 2n} = 2^{n^2-1}(2n-1)\prod_{k=1}^{n-1}(4k-1), \tag{4.7}$$

$$\operatorname{Pf}\Big((j-i)\operatorname{Sch}(i+j-2)\Big)_{1\leq i,j\leq 2n} = 2^{n^2}\prod_{k=0}^{n-1}(4k+1). \tag{4.8}$$

定理 4.2 と注 4.1 から導かれる等式として, パフィアンだけに絞ってみても, 次のような等式が青本の拡張から得られる:

$$\operatorname{Pf}\Big((j-i)\operatorname{Mot}(i+j-2)\Big)_{1\leq i,j\leq 2n} = 2^{2n}\prod_{k=0}^{n-1}(4k+1)\left|\sum_{k=0}^{n}\binom{n}{k}\left(-\frac{1}{4}\right)^{n-k}\prod_{j=1}^{k}\frac{\frac{3}{2}+2(n-j)}{3+2(2n-j-1)}\right|,$$

$$\operatorname{Pf}\Big((j-i)\operatorname{Del}(i+j-2)\Big)_{1\leq i,j\leq 2n}$$
$$= 2^{n\left(n+\frac{5}{2}\right)-1}(2n-1)\prod_{k=1}^{n-1}(4k-1)\left|\sum_{k=0}^{n}\binom{n}{k}\left(\frac{3\sqrt{2}-4}{8}\right)^{n-k}\prod_{j=1}^{k}\frac{\frac{1}{2}+2(n-j)}{1+2(2n-j-1)}\right|,$$

$$\operatorname{Pf}\Big((j-i)\operatorname{Sch}(i+j-1)\Big)_{1\leq i,j\leq 2n}$$
$$= 2^{n\left(n+\frac{5}{2}n\right)}\prod_{k=0}^{n-1}(4k+1)\left|\sum_{k=0}^{n}\binom{n}{k}\left(\frac{3\sqrt{2}-4}{8}\right)^{n-k}\prod_{j=1}^{k}\frac{\frac{3}{2}+2(n-j)}{3+2(2n-j-1)}\right|.$$

さらに, 定理 4.2 において $a=1$ とおくと, とおくと次のような等式が, 上記の範囲をみたす r について成り立つ:

$$\operatorname{Pf}\left((j-i)\operatorname{Cat}(i+j+r-2)\right)_{1\leq i,j\leq n} = \prod_{j=0}^{n-1}\frac{(4j+2)!(4j+2r+1)!}{(4j+r)!(4j+r+2)!},$$

$$\operatorname{Pf}\left((j-i)\operatorname{CBC}(i+j+r-2)\right)_{1\leq i,j\leq n} = 2^n\prod_{j=0}^{n-1}\frac{(4j)!(4j+2r+1)!(2j+1)}{(4j+r-1)!(4j+r)!(2j+r)},$$

$$\operatorname{Pf}\left((j-i)\{3(i+j+r)-8\}\operatorname{Cat}(i+j+r-3)\right)_{1\leq i,j\leq n}$$
$$= 2^{3n}\prod_{j=0}^{n-1}\frac{(4j)!(4j+2r-1)!(2j+1)}{(4j+r)!(4j+r-2)!(2j+r-1)}\left|\sum_{k=0}^{n}\binom{n}{k}\left(-\frac{1}{4}\right)^{n-k}\prod_{j=1}^{k}\frac{r+\frac{1}{2}+2(n-j)}{r-1+2(2n-j)}\right|.$$

参考文献

[1] K. Aomoto, "On the complex Selberg integral", *The Q. J. Math.* **38** (1987), 385–399.

[2] G.E. Andrews, "Plane partitions (III): The weak Macdonald conjecture", *Invent. Math.* **53** (1979), 193–225.

[3] A. I. Barvinok, "New algorithms for linear k-matroid intersection and matroid k-parity problems", *J. Mathematical Programming*, **69** (1995), 449–470. *J. Combin. Theory Ser. A* , **144** (2016), 80–138.

[4] N. G. de Bruijn. "On some multiple integrals involving determinants", *J. Indian Math. Soc.*, **19** (1955), 133–151.

[5] L. Habsieger, Une q-intégrale de Selberg et Askey, *SIAM J. Math. Anal.* **19** (1988), no. 6, 1475 – 1489

[6] M. Ishikawa, H. Tagawa and J. Zeng, "Pfaffian decomposition and a Pfaffian analogue of q-Catalan Hankel determinants", *J. Combin. Theory Ser. A*, **120** (2013), 1263–1284.

[7] M. Ishikawa and M. Wakayama, "Minor summation formula of Pfaffians", *Linear and Multilinear Alg.* **39** (1995), 285-305

[8] M. Ishikawa and M. Wakayama, "Applications of minor summation formula, III: Plücker relations, lattice paths and Pfaffian identities", *J. Combin. Theory Ser. A.*, **113** (2006), 113–155.

[9] J. Luque and J. Thibon, "Pfaffian and Hafnian identities in shuffle algebras", *Advances in Applied Mathematics* **29** (2002), 620–646.

[10] J. Luque and J. Thibon, "Hankel hyperdeterminants and Selberg integrals", *J. Phys. A: Math. Gen.* **36** (2003), 5267–5292.

[11] J. Luque and J. Thibon, "Hyperdeterminantal calculations of Selberg's and Aomoto's integrals", *Molecular Physics* **102** (2004), 1351–1359.

[12] W.H. Mills, David P. Robbins, and Howard Rumsey, Jr., "Enumeration of a Symmetry Class of Plane Partitions", *Discrete Math.*, **67** (1987) 43 – 55.

[13] T. K. Petersen, *Eulerian Numbers*, Birkhäuser Advanced Texts Basler Lehrbücher (2015).

[14] A. Selberg, "Remarks on a multiple integral", *Norsk Mat. Tidsskr.* **26** (1944), 71–78.

Maximality of Seidel matrices and switching roots of graphs

吉野 聖人（東北大学情報科学研究科）

1　はじめに

本稿は 2021 年 6 月 14 日に行った講演の内容に加筆したものである．内容は，Meng-Yue Cao 氏（北京師範大学），Jack. H. Koolen 氏（中国科学技術大学），宗政昭弘氏（東北大学）との共同研究 [1] に基づく．

等角直線族とは互いに成す角が一定であるような原点を通る直線の集合である．例えば、図 1 は角度 $\pi/3$ の等角直線族の例である．正整数 d に対して，d 次元ユークリッド空間内の角度 $\arccos(\alpha)$ の等角直線族の最大濃度を $N_\alpha(d)$ で表す．さらに，d 次元ユークリッド空間内の等角直線族の最大濃度を $N(d)$ で表す．定義から明らかに $N(d) = \max_{\alpha>0} N_\alpha(d)$ が成り立つ．この $N(d)$ を決定する問題は 1940 年代 [4] にまで遡り，現時点では 17 次元までは $N(d)$ の値が決定されている [3, Table 1].

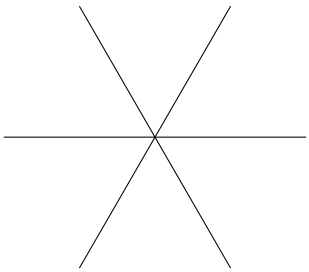


図 1: 2 次元ユークリッド空間内の角度 $\pi/3$ の等角直線族のひとつ

等角直線族の**階数（*rank*）**とは，その等角直線族を等長埋め込み可能なユークリッド空間の最小次元である．例えば，図 1 の等角直線族は 2 次元以上のユークリッド空間で実現可能であるが，1 次元では実現できないため階数は 2 である．正整数 r に対して，階数 r かつ角度 $\arccos(\alpha)$ の等角直線族の最大濃度を $N^*_\alpha(r)$ で表す．さらに，階数 r の等角直線族の最大濃度を $N^*(r)$ で表す．このとき，$N_\alpha(d) = \max_{r\le d} N^*_\alpha(r)$ という関係がある．

次元の代わりに階数を考えることで等角直線族はより詳細に観察される．実際に，表 1 では $N^*(d)$ と $N(d)$ の値が異なる次元がある．特に興味深いのは，$d = 7, 8, \ldots, 14$

d	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$N^*(d)$	6	10	16	28	14	18	18	20	22	26	28	36	40	48
$N^*_{1/3}(d)$	6	10	16	28	14	16	18	20	22	24	26	28	30	32
$N(d)$	6	10	16	28	28	28	28	28	28	28	28	36	40	48

表 1: $N^*(d)$, $N_{1/3}(d)$，$N(d)$ の値

のとき $N(d) = 28$ にも関わらず，$d = 8, 9, \ldots, 13$ のとき $N^*(d) < 28$ となることである．言い換えると，8 次元から 13 次元の間はできるだけ濃度の大きい等角直線族を作ろうとすると，それは 7 次元に収まってしまうということである．この現象は $N^*_{1/3}(d)$ が $d = 8$ の時に急に減少することに起因する．なお $N^*(9) = N^*_{1/\sqrt{17}}(9)$ かつ，$d = 13, \ldots, 17$ のとき $N^*(d) = N^*_{1/5}(d)$ である．

Lemmens 氏と Seidel 氏 [5] は pillar method を導入して $N_{1/3}$ の全ての値を決定した．そこから，$d \neq 8, \ldots, 14$ のときの $N^*_{1/3}(d)$ の値は直ちに判明する．その後，$d \in \{8, \ldots, 11\}$ に対して，$N^*_{1/3}(d) < 28 = N^*_{1/3}(7)$ が示されている [2, Theorem 4]．さらに Lin 氏と Yu 氏は $N^*_{1/3}(8) = 14$ [6, Proposition 5.2] を示し，階数 8 で共通角度 $\arccos(1/3)$，濃度 14 の等角直線族は一意であることも示している [6, Remark on p. 14].

共同研究の結果（定理 2）として，ルート格子を利用して $N^*_{1/3}(d)$ を決定し，それを与える等角直線族の分類を得た．本稿では主にその証明の概要を紹介する．証明をみることで，先に述べた $N^*_{1/3}$ の急な減少が E 型のルート格子が最大で 8 次元までしか存在しないことに起因していることが分かる．さらに，E_8 ルート格子から得られる等角直線族が持つ性質を一般化し，absolute bound（i.e., $N(d) \leq d(d+1)/2$）を達成する等角直線族はその性質を満たす（定理 3）ことも紹介する．

2 準備

対角成分が 0 で非対角成分が ± 1 である対称行列は ***Seidel* 行列**と呼ばれる．2 つの Seidel 行列 S と S' が**スイッチング同値**であるとは，ある ± 1 対角行列 D と置換行列 P が存在して $S = (PD)S'(PD)^\top$ が成り立つことである．

グラフ Γ に対して Seidel 行列 $S(\Gamma)$ を $S(\Gamma) := J - I - 2A(\Gamma)$ によって定める．ただし，$A(\Gamma)$ はグラフ Γ の隣接行列を表し，J は成分が全て 1 の行列を表す．また，2 つのグラフ Γ と Δ に対して，$S(\Gamma)$ と $S(\Delta)$ がスイッチング同値であるとき，2 つのグラ

フは**スイッチング同値**であるという．グラフ Γ とスイッチング同値なグラフ全体を $[\Gamma]$ で表す.

スイッチング同値をグラフの言葉で説明する．グラフ Γ の頂点集合 V の部分集合 U をとる．このとき，グラフ $\Gamma^U = (V, E^U)$ を次で定める．

$$x \sim y \text{ in } G^U \text{ if } \begin{cases} x \sim y \text{ in } G \text{ かつ } x, y \in U, \\ x \sim y \text{ in } G \text{ かつ } x, y \in V \setminus U, \\ x \not\sim y \text{ in } G \text{ かつ } x \in U,\ y \in V \setminus U. \end{cases}$$

グラフ Γ と Γ^U はスイッチング同値になり，逆に Γ とスイッチング同値なグラフ Δ に対して U を適当に選ぶと Δ と Γ^U は同型になる.

最大固有値 λ である位数 n の Seidel 行列 S に対して，$r := \mathrm{rank}(\lambda I - S)$ とおく．このとき，$I - S/\lambda$ は半正値であるからある単位ベクトル $x_1, \ldots, x_n \in \mathbb{R}^r$ が存在して

$$(I - S/\lambda)_{i,j} = (x_i, x_j)$$

を満たす．そのため，$\{\mathbb{R}x_1, \ldots, \mathbb{R}x_n\}$ は階数 r かつ角度 $\arccos(1/\lambda)$ の等角直線族である．逆にこの等角直線族からスイッチング同値を除いて元の Seidel 行列は復元される．よって以降は等角直線族の代わりに Seidel 行列を主に扱う.

3　極大性，強極大性の定義と主定理

対称行列 M の最大固有値を $\lambda_{\max}(M)$ で表す．一般に行列 M を首座小行列に含む対称行列 M' に対して $\lambda_{\max}(M) \leq \lambda_{\max}(M')$ が成り立つ.

定義 1. 行列 S を Seidel 行列とする．次の条件 (1) から (3) を満たす Seidel 行列 S' が存在しないとき，S は**極大** (*maximal*) であるという．また，次の条件 (1) と (2) を満たす Seidel 行列 S' が存在しないとき，S は**強極大** (*strongly maximal*) であるという.

(1) S は S' の首座小行列.

(2) $\lambda_{\max}(S) = \lambda_{\max}(S')$.

(3) $\mathrm{rank}(\lambda_{\max}(S)I - S) = \mathrm{rank}(\lambda_{\max}(S')I - S')$.

さらに，G をグラフとするとき，$S(G)$ が極大ならば G も**極大**であるという．同様に $S(G)$ が強極大であるならば G も**強極大**であるという.

Lin 氏と Yu 氏 [7] は極大な Seidel 行列に対応する等角直線族は *saturated* であると呼んでいる．

第一の主定理を述べる前に基本的なグラフを記号を確認する．頂点数 n の完全グラフは K_n で表し，完全二部グラフは $K_{n,m}$ で表す．グラフ G のライングラフは $L(G)$ と書く．2 つのグラフ $G_1 = (V_1, E_1)$ と $G_2 = (V_2, E_2)$ に対し，$G_1 + G_2$ はグラフ $(V_1 \sqcup V_2, E_1 \sqcup E_2)$ を表す．

定理 2 ([1, Theorem 3.1])**.** 位数 n のグラフ G をとる．Seidel 行列 $S(G)$ の最大固有値は 3 と仮定し，その重複度を m とおく．このとき，$S(G)$ が極大ならば G は以下のいずれかとスイッチング同値である．

(1) $L(K_5)$，$L(K_{2,4})$ （$n - m = 5$）．

(2) $L(K_6) + K_1$，$L(K_{2,5})$ （$n - m = 6$）．

(3) $L(K_8)$ （$n - m = 7$）．

(4) $L(K_{2,n-m-1})$ （$n - m = 3, 4$ または $n - m \geq 8$）．

特に $S(G)$ が強極大ならば，G は $L(K_8)$ と同型である．

この系として表 1 の $N^*_{1/3}$ の値が決定される．またこの定理において強極大性が示された $L(K_8)$ は absolute bound $N(d) \leq d(d+1)/2$ で等号を達成する．この事実の逆の主張である次の定理も共同研究の結果として得られた．

定理 3 ([1, Theorem 5.5])**.** 頂点数 n のグラフ G をとる．Seidel 行列 $S(G)$ の最大固有値の重複度を m とし $r := n - m$ とおく．このとき，$n = r(r+1)/2$ ならば G は強極大である．

この定理において $n = r(r+1)/2$ は $S(G)$ に対応する等角直線族が absolute bound で等号を達成することに対応する．一般に，与えられたユークリッド空間内で濃度の大きい等角直線族を得たいのであった．そこで absolute bound を達成する等角直線族に直線を付け加えることで別次元の濃度の大きい等角直線族を得ようとするのは自然な発想である．しかし，この定理の主張はこのような方法で新しい等角直線族が得られないことを意味する．

4　スイッチングルート

主定理の証明の前に，重要な役割を果たすスイッチングルートと必要な定理を与えておく．スイッチングルートを考えることで，Seidel 行列，隣接行列，ルート格子の間にある対応を見ることができる．

定義 4. グラフ $G=(V,E)$ の Seidel 行列の最大固有値を $2\theta-1$ とする．ベクトル $\alpha^{(x)}$ （$x\in V$）を

$$(\alpha^{(x)},\alpha^{(y)})=(A(G)+\theta I)_{x,y}\quad(x,y\in V).$$

を満たすようにとる．このとき，ベクトル r が**スイッチングルート**であるとは次の 2 つの条件を満たすことである．

(1) $(\mathsf{r},\mathsf{r})=2$.

(2) 任意の $x\in V$ に対して $(\mathsf{r},\alpha^{(x)})=1$.

スイッチングルートという名前の理由を説明する．頂点集合 V の部分集合 U をとる．ベクトル $\beta^{(x)}$ を次のように定める．

$$\beta^{(x)}:=\begin{cases}\alpha^{(x)} & (v\in V\setminus U)\\ \mathsf{r}-\alpha^{(x)} & (v\in U).\end{cases}$$

このとき

$$(\beta^{(x)},\beta^{(y)})=(A(G^U)+\theta I)_{x,y}\quad(x,y\in V)$$

が成り立つ．このようにスイッチングルートはスイッチングに関連している．

定義 5. 正の実数 θ とグラフ G をとる．行列 $B_\theta(G)$ を

$$B_\theta(G):=\begin{pmatrix}A(G)+\theta I & j\\ j^T & 2\end{pmatrix}$$

で定める．ただし，j は成分が全て 1 のベクトルとする．

この定義のもと

$$\begin{pmatrix}I & -\frac{1}{t}j\\ 0 & 1\end{pmatrix}B_\theta(G)\begin{pmatrix}I & 0\\ -\frac{1}{2}j^\top & 1\end{pmatrix}=\begin{pmatrix}A(G)+\theta I-\frac{1}{2}J & 0\\ 0 & 2\end{pmatrix}.$$

が成り立つので次の定理が従う．ただしグラフ G に対して，その**錐**は $\tilde{G}$ で表され，G に新しい点を追加してその点と G の全ての点を結んでできるグラフとして定義される．

定理 6. 任意のグラフ G に対して以下は同値である．

(1) Seidel 行列 $S(G)$ の最大固有値は 3 以下である．

(2) 錐 $\tilde{G}$ の隣接行列 $A(\tilde{G})$ の最小固有値は -2 以上である．

いずれかが成り立つ場合，$\mathrm{rank}(3I-S(G))+1=\mathrm{rank}(A(\tilde{G})+2I)$ が成り立つ．

5　定理 2 の証明

本セクションでは定理 3 の証明を与える．簡単な補題の証明は省略しているので，より詳細な議論は [1] を参照されたい．証明を見ることによって，定理 2 内の $L(K_5)$, $L(K_6)+K_1$, $L(K_8)$ が E 型ルート格子に由来し，その他の $L(K_{2,n-m-1})$ は D 型ルート格子に由来することが分かる．最大固有値 3 の Seidel 行列を考えることは角度 $\arccos(1/3)$ の等角直線族を考えることに等しかったので，$N^*_{1/3}$ の値の変化をルート格子を通じて理解することができる．

まずはルート格子について説明しておく．長さが $\sqrt{2}$ のベクトルを**ルート**といい，ルートで生成される整格子を**ルート格子**と呼ぶ．

定義 7. グラフ G の錐 $\tilde{G}$ の隣接行列 $A(\tilde{G})$ の最小固有値が -2 以上であるとする．このとき，$A(\tilde{G})+2I$ をグラム行列にもつベクトルたちで生成される格子を $\Lambda(G)$ で表す．

定理 6 から直ちに次が従う．

補題 8. グラフ G の Seidel 行列 $S(G)$ の最大固有値は 3 以下であるとする．このとき $\operatorname{rank}(3I - S(G)) + 1 = \operatorname{rank}\Lambda(G)$ が成り立つ．

この定義において $\Lambda(G)$ はルート格子になり，特に G が連結グラフのとき $\Lambda(G)$ は既約ルート格子になる．また，上記の補題によってそのルート格子の階数もわかる．よく知られるように，既約ルート格子は次のように分類される．

$$
\begin{aligned}
\mathsf{A}_n &:= \{\mathsf{v} \in \mathbb{Z}^{n+1} \mid (\mathsf{v},\mathsf{j}) = 0\} \quad (n \in \mathbb{Z}_{\geq 1}),\\
\mathsf{D}_n &:= \{\mathsf{v} \in \mathbb{Z}^{n} \mid (\mathsf{v},\mathsf{j}) \in 2\mathbb{Z}\} \quad (n \in \mathbb{Z}_{\geq 4}),\\
\mathsf{E}_8 &:= \mathsf{D}_8 \sqcup (\mathsf{j}/2 + \mathsf{D}_8)\,,\\
\mathsf{E}_7 &:= \{\mathsf{v} \in \mathsf{E}_8 \mid (\mathsf{v}, \mathsf{e}_1 - \mathsf{e}_2) = 0\},\\
\mathsf{E}_6 &:= \{\mathsf{v} \in \mathsf{E}_8 \mid (\mathsf{v}, \mathsf{e}_1 - \mathsf{e}_2) = (\mathsf{v}, \mathsf{e}_2 - \mathsf{e}_3) = 0\}.
\end{aligned}
$$

ただし，e_i は第 i 成分が 1 で他の成分は 0 であるベクトルとする．ルート格子 D_n $(n \in \mathbb{Z}_{\geq 4})$ は D 型，E_n $(n = 6, 7, 8)$ は E 型であるという．

定義 9. 既約ルート格子 L をとり，**スイッチングクラス** $[\mathsf{L}]$ を $[L]$ で定義する．ここで，グラフ L は以下の方法で定める．まず L に含まれるルート r を任意にとる．次に $(\mathsf{r},\mathsf{v}) = 1$ を満たすルート v 全体からなる集合を N とおく. 集合 N の濃度 $|N|/2$ の部分集合 $X \subset N$ を $\mathsf{u} = \mathsf{r} - \mathsf{v}$ なるルート u，v を含まないようにとる．グラフ L は $A(L)+2I$ が X のグラム行列と一致するようにとる．

この定義において，異なるルート $\mathsf{u} \in X$ と $\mathsf{v} \in X$ は $(\mathsf{u}, \mathsf{v}) \in \{0, 1\}$ を満たすため，グラフ L の存在は保証される．さらに，r はグラフ L のスイッチングルートであるから $[L]$ は X の選び方に依存しない．一般に既約ルート格子の自己同型群はそのルートに推移的に作用する．そのため r の選び方に関係なく $[\mathsf{L}]$ は定義され，well-defined である．

簡単に次の補題が確かめられる．

補題 10. (1) $[\mathsf{A}_n] = [K_{n-1}] \quad (n \in \mathbb{Z}_{\geq 1})$.

(2) $[\mathsf{D}_n] = [L(K_{2,n-2})] \quad (n \in \mathbb{Z}_{\geq 4})$.

(3) $[\mathsf{E}_8] = [L(K_8)]$, $[\mathsf{E}_7] = [L(K_6) + K_1]$, $[\mathsf{E}_6] = [L(K_5)]$.

スイッチングクラス $[\mathsf{D}_n]$ $(n \geq 4)$ と $[\mathsf{E}_n]$ $(n = 6, 7, 8)$ に含まれるグラフの Seidel 行列の最大固有値は 3 である．またスイッチングクラス $[\mathsf{A}_n]$ $(n \geq 1)$ に含まれるグラフの Seidel 行列の最大固有値は 1 である．

また定義から次が分かる．

補題 11. グラフ G の Seidel 行列の最大固有値は 3 以下であるとする．このとき，あるグラフ $L \in [\Lambda(G)]$ が存在して，L は G を誘導部分グラフに含む．特に $\Lambda(L) = \Lambda(G)$ が成り立つ.

この補題は与えられたユークリッド空間に存在する角度 $\arccos(1/3)$ の等角直線族に対して，それを含む形で D 型または E 型の既約ルート格子に由来する等角直線族が存在することを保証している．そのため，次の補題でそのようなルート格子由来の等角直線族の関係を調べる．そしてその関係はルート格子の包含関係に帰着されることが分かる．

補題 12. D 型か E 型の既約ルート格子 L をとる．グラフ $L \in [\mathsf{L}]$ が $\mathsf{L} = \Lambda(L)$ を満たすとする．このとき，L が極大 (resp. 強極大) であることの必要十分条件は条件 (1) と (2) (resp. 条件 (1)) を満たす D 型か E 型の既約ルート格子 M が存在しないことである．

(1) M は L を同型を除いて真に包含する．

(2) M と L の階数が一致する．

Proof. 補題 10 より $S(L)$ の最大固有値は 3 である. グラフ L を誘導部分グラフに含むグラフ H が存在し，その Seidel 行列 $S(H)$ の最大固有値が 3 であったと仮定する．補題 11 を $G := H$ とおいて適用し，$\mathsf{M} := \Lambda(H)$ とすると, グラフ H を誘導部分グラフに含むグラフ $M \in [\mathsf{M}]$ が $\mathsf{M} = \Lambda(M)$ を満たすようにとれる．このとき，$S(M)$ の最大固

有値は $S(L)$ の最大固有値以上である．一方で，補題 10 より $S(M)$ の最大固有値は 3 以下であるから，ちょうど 3 に一致することが分かる．特に，M は D 型か E 型のルート格子となることもわかる．一般性を失わず，M は L を部分集合として含むとして良い．また，$\mathsf{L} = \Lambda(L)$ かつ $\mathsf{M} = \Lambda(M)$ に注意すると $L = M$ と $\mathsf{L} = \mathsf{M}$ は同値であると分かる．これによって，グラフ L が強極大になるための所望の必要十分条件が得られた．

最後に, Lemma 8 によって

$$\operatorname{rank}(3I - S(L)) + 1 = \operatorname{rank}\mathsf{L} \quad \text{かつ} \quad \operatorname{rank}(3I - S(M)) + 1 = \operatorname{rank}\mathsf{M}$$

を得る．そして，条件 (2) は $\operatorname{rank}(3I - S(L)) = \operatorname{rank}(3I - S(M))$ と同値であると分かる. これによって，グラフ L が極大になる所望の必要十分条件が得られた． □

一応，これまでの補題を組み合わせて定理 2 の証明を完了させておく．

（定理 *2* の証明）. 極大な G グラフをとり，その Seidel 行列 $S(G)$ の最大固有値は 3 であると仮定する．補題 11 を適用し，$\mathsf{L} := \Lambda(G)$ とおくことで, G を誘導部分グラフに含むグラフ $L \in [\mathsf{L}]$ で $\mathsf{L} = \Lambda(L)$ なるものを得る. さらに補題 10 によって $S(L)$ の最大固有値は 3 であり，$\Lambda(G)$ は D 型か E 型であることが分かる．また

$$\operatorname{rank}(3I - S(L)) + 1 = \operatorname{rank}\Lambda(L) = \operatorname{rank}\mathsf{L} = \operatorname{rank}\Lambda(G) = \operatorname{rank}(3I - S(G)) + 1,$$

が補題 8 より従い, 極大なグラフ G は L に一致することが分かる. 一方で，以下の関係はよく知られている．

$$\mathsf{D}_4 \subset \mathsf{D}_5 \subset \cdots, \mathsf{E}_6 \subset \mathsf{E}_7 \subset \mathsf{E}_8,$$
$$\mathsf{D}_6 \not\subset \mathsf{E}_6, \mathsf{D}_7 \not\subset \mathsf{E}_7, \mathsf{D}_8 \subset \mathsf{E}_8,$$
$$\mathsf{E}_n \not\subset \mathsf{D}_{n'} \text{ for } n \text{ and } n'.$$

そのため，補題 12 によって直ちに定理が導かれる． □

本稿で紹介した手法で角度 $\arccos(1/5)$ の等角直線族を調べようとすると，いわゆる 3-格子（= 長さ $\sqrt{3}$ のベクトルで生成される整格子）を調べることに帰着される．しかし，ルート格子と異なり 3-格子はほとんど調べられておらず，現時点では本稿の手法では $N_{1/5}$ の値の決定などをすることなどはできていない．

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

[1] Meng-Yue Cao, Jack H. Koolen, Akihiro Munemasa, and Kiyoto Yoshino. Maximality of Seidel matrices and switching roots of graphs. *Graphs and Combinatorics*, pages 1–17, 2021.

[2] Alexey Glazyrin and Wei-Hsuan Yu. Upper bounds for s-distance sets and equiangular lines. *Adv. Math.*, 330:810–833, 2018.

[3] Gary R. W. Greaves, Jeven Syatriadi, and Pavlo Yatsyna. Equiangular lines in euclidean spaces: dimensions 17 and 18. *arXiv:2104.04330*, 2021.

[4] J. Haantjes. Equilateral point-sets in elliptic two- and three-dimensional spaces. *Nieuw Arch. Wiskunde*, 22:355–362, 1948.

[5] P.W.H. Lemmens and J.J. Seidel. Equiangular lines. *J. Algebra*, 24(3):494–512, 1973.

[6] Yen-Chi Roger Lin and Wei-Hsuan Yu. Equiangular lines and the Lemmens-Seidel conjecture. *Discrete Math.*, 343(2):1–18, 2020.

[7] Yen-chi Roger Lin and Wei-Hsuan Yu. Saturated configuration and new large construction of equiangular lines. *Linear Algebra Appl.*, 588:272–281, 2020.

「符号と格子に対する Assmus–Mattson 型の定理について」

中空　大幸　（神戸学院大学）

1　序文

本稿は東北大学の宗政先生と早稲田大学の三枝崎先生との共同研究 [11] に基づいている。

C を $\mathbb{F}_q$ 上の $[n,k,d]$ code とし，$C^\perp$ を C の dual code とする。$C = C^\perp$ のとき，C は self-dual と呼ばれる。本稿では $C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\}$ を C の shell と呼ぶ。

X を v 個の点集合とし，$\mathcal{B}$ は X の k 点の部分集合の族 (ブロックの集合) で，性質として任意の t 個の点は丁度 λ 個のブロックに含まれるとする。このとき，$(X,\mathcal{B})$ を combinatorial t-(v,k,λ)design と呼ぶ。

符号と combinatorial t-design の関係において次の Assmus–Mattson の定理が重要である。

Theorem 1.1 (Assmus–Mattson [1])**.** *Let C be an $[n,k,d]$ linear code over $\mathbb{F}_q$ and $C^\perp$ be the dual $[n,n-k,d^\perp]$ code. Let t be an integer less than d. Let v_0 be the largest integer satisfying $v_0 - \lfloor \frac{v_0+q-2}{q-1} \rfloor < d$, and w_0 be the largest integer satisfying $w_0 - \lfloor \frac{w_0+q-2}{q-1} \rfloor < d^\perp$, where, if $q = 2$, we take $v_0 = w_0 = n$. Let $C^\perp$ have at most $d-t$ non-zero weights less than or equal to $n-t$. Then, for each weight v with $d \le v \le v_0$, C_v is a combinatorial t-design, and for each weight w with $d^\perp \le w \le \min\{n-t, w_0\}$, $C_w^\perp$ is a combinatorial t-design.*

ある linear code C の shell C_w が Assmus–Mattson の定理によって combinatorial t-design $(t > 0)$ となるならば，C を Assmus–Mattson の定理を適用可能な符号と呼ぶ。Assmus–Mattson の定理を適用可能な符号の例には extremal self-dual code という重要なクラスの符号が知られている。

C を長さ n の Type II (binary doubly even self-dual) code とし，$\min(C)$ を C の最小ハミング重さとする。すると，次の限界式が知られている。

$$\min(C) \le 4\left\lfloor \frac{n}{24} \right\rfloor + 4. \tag{1.1}$$

C の最小ハミング重さが (1.1) の等号を満たすとき，C は extremal と呼ばれる。

C を長さ n の extremal Type II code としたとき，Assmus–Mattson の定理が適用できて，$\forall w$ に対して C_w が combinatorial

$$\begin{cases} \text{5-design} & (n \equiv 0 \pmod{24}), \\ \text{3-design} & (n \equiv 8 \pmod{24}), \\ \text{1-design} & (n \equiv 16 \pmod{24}). \end{cases}$$

である。

C を長さ n の Type III または IV (ternary or quaternary self-dual) code とする。次の最小ハミング重さに関する限界式が知られている。

$$\min(C) \leq \begin{cases} 3\left\lfloor \frac{n}{12} \right\rfloor + 3 & \text{if } C \text{ is Type III}, \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 2 & \text{if } C \text{ is Type IV}. \end{cases} \tag{1.2}$$

Type II と同様に C の最小ハミング重さが (1.2) の等号を満たすとき，C は extremal と呼ばれ，repeated block を認めると $\forall w$ に対して C_w が combinatorial

$$\begin{cases} \text{5-design} & (n \equiv 0 \pmod{12}), \\ \text{3-design} & (n \equiv 4 \pmod{12}), \\ \text{1-design} & (n \equiv 8 \pmod{12}), \quad \text{if } C \text{ is Type III}, \end{cases}$$

$$\begin{cases} \text{5-design} & (n \equiv 0 \pmod{6}), \\ \text{3-design} & (n \equiv 2 \pmod{6}), \\ \text{1-design} & (n \equiv 4 \pmod{6}), \quad \text{if } C \text{ is Type IV}. \end{cases}$$

である。

Assmus–Mattson の定理にある v_0 および w_0 の範囲は simple design を扱う場合の条件である。もっと正確には，C_w が simple combinatorial t-design の各ブロックを定数回繰り返したデザイン (n-repeated of simple combinatorial t-design と呼ぶ) となる条件である。

$$w_0 - \left\lfloor \frac{w_0 + q - 2}{q - 1} \right\rfloor < d. \tag{1.3}$$

w_0 が不等式 (1.3) を満たす最大の整数とする。$\forall w \leq w_0$ に対して，C が extremal Type III code (extremal Type IV code) ならば C_w が 2-repeated (3-repeated) of simple combinatorial t-design である。

2 格子と spherical t-design

$L \subset \mathbb{R}^n$ をランク n の格子とする。L の双対格子は

$$L^\sharp := \{y \in \mathbb{R}^n \mid (y, x) \in \mathbb{Z},\ \forall x \in L\}.$$

で定義される。ここで，(,) は通常内積である。

- L が整格子である。 $\Longleftrightarrow$ 任意の $x, y \in L$ に対して，$(x, y) \in \mathbb{Z}$
- 整格子 L が偶格子である。$\Longleftrightarrow$ 任意の $x \in L$ に対して，$(x, x) \in 2\mathbb{Z}$
- 整格子 L がユニモジュラーである。 $\Longleftrightarrow L^\sharp = L$

$\mathbb{R}^n$ の単位球面を

$$S^{n-1} = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 = 1\}$$

とする。$X \subset S^{n-1}$ が球面 S^{n-1} 上の spherical t-design であるとは,

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \frac{1}{|S^{n-1}|}\int_{S^{n-1}} f(x)d\sigma(x),$$

がすべての多項式 $f(x) = f(x_1, \ldots, x_n)$ が $\deg(f) \leq t$ に対して成り立つことと定義する。

符号と同様に格子 L に対して，$L_\ell := \{x \in L \mid (x, x) = \ell\}$ を L の shell と呼ぶ。L をランク n の Type II (even unimodular) lattice とし，$\min(L)$ を L の最小ノルムとする。すると，次の限界式が知られている。

$$\min(L) \leq 2\left\lfloor \frac{n}{24} \right\rfloor + 2. \tag{2.1}$$

L の最小ハミング重さが (2.1) の等号を満たすとき，L は extremal と呼ばれる。格子と spherical t-design においても次のような Assmus–Mattson 型の定理が存在する。

Theorem 2.1 ([15]). *Let L be an extremal Type II lattice of rank n. If $L_{2m} \neq \phi$, then L_{2m} is a spherical*

$$\begin{cases} 11\text{-}design & (n \equiv 0 \pmod{24}), \\ 7\text{-}design & (n \equiv 8 \pmod{24}), \\ 3\text{-}design & (n \equiv 16 \pmod{24}). \end{cases}$$

例えば，$(E_8)_{2m}$ は spherical 7-design である。そして，次の Ramanujan τ 函数との関係がある。

Theorem 2.2 ([15]). *$(E_8)_{2m}$ is a spherical 8-design if and only if $\tau(m) = 0$, where*

$$q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=0}^{\infty}\tau(m)q^m.$$

すると，有名な Lehmer 予想が関係している。

Conjecture 2.3 ([10]). For all m,

$$\tau(m) \neq 0.$$

一般に，格子 L の shell L_{2m} について次のような定義を与えることができる。

$$\delta(L) := \max\{t \in \mathbb{N} \mid \forall w, L_{2m} \text{ is a spherical } t\text{-design}\}$$
$$s(L) := \max\{t \in \mathbb{N} \mid \exists w, \text{ s.t. } L_{2m} \text{ is a spherical } t\text{-design}\}$$

レーマー予想の解決は「$\delta(E_8) < s(E_8)$ となる場合はどこで起こり得るか ?」という問題の解決と同値であるといえる。

符号と combinatorial t-design においても同様に次のように定義を与えることができて,

$$\delta(C) := \max\{t \in \mathbb{N} \mid \forall w, D_w \text{ is a combinatorial } t\text{-design}\}$$
$$s(C) := \max\{t \in \mathbb{N} \mid \exists w, \text{ s.t. } D_w \text{ is a combinatorial } t\text{-design}\}$$

「$\delta(C) < s(C)$ となる場合はどこで起こり得るか ?」という問いはレーマー型の問題として，本研究ならびに一連の研究 [12, 13, 14] で取り組んできた。

3　主定理とその強力版

3.1　主定理

本研究の主定理は次である。

Theorem 3.1. (1) *Let C be a Type II $[24m, 12m, 4m]$ code. Then every shell of C is a combinatorial 1-design.*

(2) *Let C be a Type III $[12m, 6m, 3m]$ code. Then for $\ell \leq 6m-3$, C_ℓ is a combinatorial 1-design.*

(3) *Let C be a Type IV $[6m, 3m, 2m]$ code. Then for $\ell \leq 3m-1$, C_ℓ is a combinatorial 1-design.*

(4) *Let L be a Type II lattice of rank $24m$ with minimum norm $2m$. Then every shell of L supports a spherical 3-design.*

Theore 3.1(1)–(3) 符号と (4) 格子は near-extremal と呼ばれる。
near-extremal code は次の長さ n に対して存在しないこと [8] が知られている。

$$\begin{array}{ll} \text{Type II:} & n = 24i\ (i \geq 315),\ 24i+8\ (i \geq 320),\ 24i+16\ (i \geq 325), \\ \text{Type III:} & n = 12i\ (i \geq 147),\ 12i+4\ (i \geq 150),\ 12i+8\ (i \geq 154), \\ \text{Type IV:} & n = 6i\ (i \geq 38),\ 6i+2\ (i \geq 41),\ 6i+4\ (i \geq 43). \end{array}$$

near-extremal code は Assmus–Mattson の定理を適用可能な符号ではない。例えば，C を Type II [24,12,4] code とする。C の weight の分布は $0, 4, 8, 12, 16, 20, 24$ である。Assmus–Mattson の定理の条件から $4 - t \geq 5$ より，自然数 t を取ることができない。よって，C は Assmus–Mattson の定理を適用可能な符号ではないことが分かる。

Theorem 3.1(2) $\ell \leq 6m-3$ と (3) $\ell \leq 3m-1$ の ℓ の範囲は (1.3) から得られる simple design(の repeated) となる条件である。オリジナルの論文 [11] では simple design となる形にしたが，repeated block を認めて ℓ の範囲を除く形でも成り立つことを追記しておく。

Theorem 3.1(1) と (4) は宗政先生と Venkov によって最初に証明された (未出版)。その証明はモジュラー形式が使われた方法であるが，我々の論文 [11] における Theore 3.1(1) の証明は異なっている。Delsarte 理論 [3] を基にした Bachoc[2] の手法 Harmonic weight enumerator を用いて Theore 3.1(1)–(3) を証明している。

Theore 3.1(1)–(3) から，次のような self-dual code の weight enumerator の制限を得る。

Corollary 3.2. (1) *Let C be a Type II code of length $24m$ with minimum weight $4m$. Then the coefficient of $x^{24m-4m}y^{4m}$ in the weight enumerator of C is divisible by 6.*

(2) *Let C be a Type III code of length $12m$ with minimum weight $3m$. Then the coefficient of $x^{12m-3m}y^{3m}$ in the weight enumerator of C is divisible by 4.*

(3) *Let C be a Type IV code of length $6m$ with minimum weight $2m$. Then the coefficient of $x^{6m-2m}y^{2m}$ in the weight enumerator of C is divisible by 3.*

3.2 主定理の強力版

Theorem 3.1 は符号 (格子) のすべての shell が 1-design (3-design) という主張であるが, 次の定理のように少し強い主張のできる符号と格子がある。これは前述のレーマー型の問題「$\delta(C) < s(C)$ となる場合はどこで起こり得るか ?」に付随する。

Theorem 3.3. (1) *Let C be a Type II $[96, 48, 16]$ code. Then C_{20} (also C_{76}) is a combinatorial 2-design.*

(2) *Let L be a Type II lattice of rank 240 with minimum norm 20. Then L_{22} supports a spherical 5-design.*

一方で, Type II $[96, 48, 16]$ code の shell である combinatorial t-design の t の上限を次の定理で与える。ここで, $\mathcal{L} = \{\ell \in \mathbb{Z} \mid 16 \le \ell \le 80,\ \ell \equiv 0 \pmod 4\}$ とする。

Theorem 3.4. *Let C be a Type II code of length 96 with minimum weight 16, and let $\ell \in \mathcal{L}$. Assume that C_ℓ is a combinatorial t-design. Then the following statements hold:*

(1) *If $t = 2$ and $\ell \neq 20, 76$, then every shell of C is a combinatorial 2-design.*

(2) *If $t \ge 3$ and $\ell \neq 20, 48, 76$, then every shell of C is a Type II $[96, 48, 16]$ code.*

(3) *We have*

$$t \le \begin{cases} 7 & \text{if } \ell = 48, \\ 5 & \text{if } \ell = 20, 76. \\ 4 & \text{otherwise.} \end{cases}$$

C を Type II $[96, 48, 16]$ code とすると, Theorem 3.1(1), Theorem 3.3(1), Theorem 3.4 より,

$$1 \le \delta(C) \le 4,\ 2 \le s(C) \le 7$$

を得る。次の節で Type II $[96, 48, 16]$ code の実例で combinatorial t-design の t の値を調べる。

3.3 長さ 96 の near-extremal Type II code

この節では C を Type II $[96, 48, 16]$ code とする。[5] において, C の weight enumerator $W_C(x, y)$ が次のように決定された。

$$\begin{aligned} & W_C(x, y) \qquad (3.1) \\ & = 1 + (-28086 + a)y^{16} + (3666432 - 16a)y^{20} \\ & + (366474560 + 120a)y^{24} + (18658567680 - 560a)y^{28} \\ & + (422018863695 + 1820a)y^{32} + (4552989336064 - 4368a)y^{36} \\ & + (24292464652992 + 8008a)y^{40} + (65727332943360 - 11440a)y^{44} \\ & + (91447307757260 + 12870a)y^{48} + \cdots, \end{aligned}$$

そこで,

$$28086 < a \leq 229152 \tag{3.2}$$

である。C の知られている例は次の通りである。

Example 3.5. (a) Feit [6]: $a = 37722$.

(b) Dougherty, Gulliver and Harada [5]: $a \in \{37584, 37500, 37524, 37596\}$.

(c) Dontcheva [4]: $a \in \{36918, 37884, 37332\}$.

(d) Harada, Kiermaier, Wassermann and Yorgova [9]: $a = 37194$.

(e) Gulliver and Harada [7]: there are 639 values of a.

a の値は全部で 648 個であるが，符号は同値類を除いて 4565 個の例が知られている。Example 3.5 の知られているすべての符号 C に対して，Magma を用いて計算した結果

$$\delta(C) = 1 < 2 = s(C)$$

である。もっと正確に述べると，各 $\ell \in \mathcal{L}$ に対して，C_ℓ が combinatorial t-design となる最大の整数 t を $t_\ell(C)$ とすると,

$$t_\ell(C) = \begin{cases} 2 & \text{if } \ell \in \{20, 76\}, \\ 1 & \text{if } \ell \in \mathcal{L} \setminus \{20, 76\}. \end{cases}$$

である。

参考文献

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

[2] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999), no. 1-3, 11-28.

[3] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.* **34** (1978), no. 1, 157-166.

[4] R. Dontcheva, Doubly-even self-dual code of length 96, *IEEE Trans. Inform. Theory* **48** (2002), 557–561.

[5] S.T. Dougherty, T.A. Gulliver and M. Harada, Extremal binary self-dual codes, *IEEE Trans. Inform. Theory* **43** (1997), 2036–2047.

[6] W. Feit, A self-dual even $(96, 48, 16)$ code, *IEEE Trans. Inform. Theory* **20** (1974), 136–138.

[7] T.A. Gulliver and M. Harada, On extremal double circulant self-dual codes of lengths 90-96, *Applicable Algebra in Eng. Communi. Comput.* First online (2019), 1–13.

[8] S. Han and J.-L. Kim, The nonexistence of near-extremal formally self-dual codes. *Des. Codes Cryptogr.* **51** (2009), no. 1, 69–77.

[9] M. Harada, M. Kiermaier, A. Wassermann and R. Yorgova, New binary singly even self-dual codes, *IEEE Trans. Inform. Theory* **56** (2010), 1612–1617.

[10] D. H. Lehmer, The vanishing of Ramanujan's $\tau(n)$, *Duke Math. J.* **14** (1947), 429–433.

[11] T. Miezaki, A. Munemasa and H. Nakasora, A note on Assmus–Mattson type theorems, *Des. Codes Cryptogr.*, **89** (2021), 843-858.

[12] T. Miezaki and H. Nakasora, An upper bound of the value of t of the support t-designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, **79** (2016), 37-46.

[13] T. Miezaki and H. Nakasora, The support designs of the triply even binary codes of length 48, *J. Combin. Designs*, **27** (2019), 673-681.

[14] T. Miezaki and H. Nakasora, Strengthening of the Assmus–Mattson theorem for some dual codes, arXiv:2004.03396.(2020)

[15] B. B. Venkov, Even unimodular extremal lattices (Russian), *Algebraic geometry and its applications. Trudy Mat. Inst. Steklov.* **165** (1984), 43–48; translation in *Proc. Steklov Inst. Math.* **165** (1985) 47–52.

整化可能な整格子

谷口 哲至 (広島工業大学)

1 はじめに

格子 (lattice) の元同士の内積が全て整数であるものを，整格子 (integral lattice) と呼ぶ。一般に，整格子は標準格子 (standard lattice) の部分格子とはならないが，スカラー $\sqrt{s}$ 倍して標準格子 ($\cong \mathbb{Z}^n$) の部分格子とする整化を考える。与えられた格子がそうなるなら，s-整化可能であるいう。

一方，先行する研究で，root 格子と呼ばれる整格子を用いて最小固有値が -2 以上のグラフを分類する研究がある。

定理 1.1. 最小固有値が -2 以上のグラフについて以下の一つが成立する*:*

(i) a line graph of a bipartite graph rep. by root system A_n

(ii) a generalized line graph rep. by root system D_n

(iii) a graph rep. by root system E_8

これによれば，そのようなグラフはルート系の A, D, E-型で分類される。A, D-型整格子は標準格子の部分格子であるが，E-型整格子は標準格子の部分格子ではない。しかし，E-型整格子はスカラー $\sqrt{2}$ 倍して標準格子の部分格子となるので，2-整化可能である。そこで，一般に最小固有値が λ 以上である場合に，グラフから整格子を作るとき，s をどのようにとれば整化可能となるかは自然な興味である。

また，ライングラフの最小固有値が -2 以上であることは良く知られている。これにより，最小固有値によるグラフの階層構造を知ろうという問題が自然と生じるのだが，(良く知られている) ライングラフの構成法では最小固有値が -2 よりも小さいグラフを構成する事はできない。そこで R. Woo と A. Neumaier [6] は，グラフの「辺」を「点」で置き換えるという単純な作業であるライングラフの構成法を高度に一般化し，最小固有値が -2 よりも小さいグラフの構成法を定式化した。[6] では，最小固有値 $-1-\sqrt{2}$ 以上のグラフが分類されている。それには (9 種類の) ホフマングラフと呼ばれる特別なグラフ達の和の概念が用いられており，そこにホフマングラフの既約性と共にルート系との関わりも生じる。そこで，最小固有値が $-\frac{3}{\sqrt{2}}$ 以上の辺符号グラフから作られる整格子について，宗政昭弘氏，吉野聖人氏[1]、らと共同で研究を進める。

[1]東北大学大学院 情報科学研究科

2　ホフマングラフ

定義 2.1. 条件 (i)、(ii) を満たすグラフ $H=(V,E)$ とラベリング $\mu: V \to \{f,s\}$ とのペア $\mathfrak{H}=(H,\mu)$ をホフマングラフという:

(i) ラベル f の総ての頂点は、少なくとも一つラベル s の頂点と隣接する;

(ii) ラベルが f の頂点は互いに非隣接である。

ラベル s の頂点を **slim 頂点**と呼び、それらから成る $\mathfrak{h}$ の頂点集合を $V^s(\mathfrak{h})$ で表す。また、ラベル f の頂点を **fat 頂点**と呼び、それらから成る $\mathfrak{h}$ の頂点集合を $V^f(\mathfrak{h})$ で表す。また、どの slim 頂点も、ある fat 頂点と隣接するとき、$\mathfrak{h}$ を fat-ホフマングラフと呼ぶ。更に、ホフマングラフの固有値を次で与える [6]:

定義 2.2. A を次の様なホフマングラフ $\mathfrak{h}$ の隣接行列とする:

$$A=\begin{pmatrix} A_s & C \\ C^T & O \end{pmatrix}$$

但し、A_s は slim 頂点の隣接関係を表し、C は slim 頂点と fat 頂点の隣接関係を表す。ここで、実対称行列 $B(\mathfrak{h})=A_s-CC^T$ の固有値を $\mathfrak{h}$ の固有値と呼ぶ。

定理 2.3 (Hoffman [4])**.** $\mathfrak{h}$ をホフマングラフとする。更に Γ^n を、各 *fat* 頂点 f を *slim n-clique* $K(f)$ で置き換え、f の総ての隣接点と $K(f)$ の総ての頂点を互いに辺で結ぶことで $\mathfrak{h}$ から得られるグラフとする。このとき、以下二式が成り立つ*:*

$$\lambda_{\min}(\Gamma^n) \geq \lambda_{\min}(\mathfrak{h}) \tag{1}$$

$$\lim_{n\to\infty} \lambda_{\min}(\Gamma^n) = \lambda_{\min}(\mathfrak{h}) \tag{2}$$

特に、任意の $\epsilon>0$ に対し、Γ^n を誘導部分グラフとして含む総ての *slim* グラフ Δ が

$$\lambda_{\min}(\Delta) \leq \lambda_{\min}(\mathfrak{h})+\epsilon.$$

を満たすように、自然数 n をとれる。

定理 2.3 から、ホフマングラフとはグラフの最小固有値における極限構造であり、Woo 氏、Neumaier 氏 [6] らは上手く導入したと言えよう。

2.1　ホフマングラフの和

定義 2.4. $\mathfrak{h}$ をホフマングラフとし、$\mathfrak{h}^1$、$\mathfrak{h}^2(\neq\emptyset)$ を $\mathfrak{h}$ の二つの誘導部分グラフとする。以下の条件を満たすとき、$\mathfrak{h}$ は $\mathfrak{h}^1$ と $\mathfrak{h}^2$ の和であると言い、$\mathfrak{h}=\mathfrak{h}^1\uplus\mathfrak{h}^2$ で書き表す:

(i) $V(\mathfrak{h})=V(\mathfrak{h}^1)\cup V(\mathfrak{h}^2)$;

(ii) $V^s(\mathfrak{h}) = V^s(\mathfrak{h}^1) \cup V^s(\mathfrak{h}^2)$,
$V^s(\mathfrak{h}^1) \cap V^s(\mathfrak{h}^2) = \emptyset$;

(iii) $x \in V^s(\mathfrak{h}^i)$, $y \in V^f(\mathfrak{h})$, $\{x, y\} \in E(\mathfrak{h}) \Longrightarrow y \in V^f(\mathfrak{h}^i)$;

(iv) $x \in V^s(\mathfrak{h}^1)$, $y \in V^s(\mathfrak{h}^2) \Longrightarrow |N^f_{\mathfrak{h}}(x, y)| \leq 1 \wedge (|N^f_{\mathfrak{h}}(x, y)| = 1 \Longleftrightarrow \{x, y\} \in E(\mathfrak{h}))$.

$\mathfrak{h}$ がホフマングラフ $\mathfrak{h}^1$、$\mathfrak{h}^2(\neq \emptyset)$ で $\mathfrak{h} = \mathfrak{h}^1 \uplus \mathfrak{h}^2$ と表されるなら、$\mathfrak{h}$ は分解可能であるという。非連結なホフマングラフは明らかに分解可能である。

これより、ホフマングラフの既約性の概念が生じる。これまでに得た成果の 1 つを紹介する。

定理 2.5 ([5])**.** $\mathfrak{h}$ を分解出来ない *fat*-ホフマングラフで、$V^s = V^s(\mathfrak{h})$、最小固有値が -3 以上とする。このとき、総ての *slim* 頂点は高々3 個の *fat* と隣接する。更に、以下の主張が成立する*:*

(i) $\exists x \in V^s\ (|N^f_{\mathfrak{h}}(x)| = 3) \Longrightarrow \mathfrak{h} \cong \mathfrak{h}^{(3)}$

(ii) $\forall x \in V^s\ (|N^f_{\mathfrak{h}}(x)| \leq 2) \wedge \exists x \in V^s\ (|N^f_{\mathfrak{h}}(x)| = 2) \Longrightarrow \exists n \geq 0$ $(\Lambda^{\mathrm{red}}(\mathfrak{h}, 3) \simeq \mathbb{Z}^n)$

(iii) $\forall x \in V^s\ (|N^f_{\mathfrak{h}}(x)| = 1) \Longrightarrow \Lambda^{\mathrm{red}}(\mathfrak{h}, 3)$*:* 既約ルート格子*.*

但し、$\mathfrak{h}^{(3)}$ は *slim* 頂点が 1 つで、3 つの *fat* 頂点をその隣接点に持つホフマングラフである。

2.2 ホフマングラフの表現

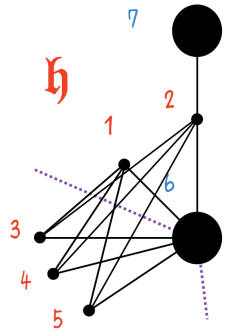
グラフの最小固有値を考える時に、よく知られた構造（ルート格子等）上で議論を展開する為に、Woo 氏、Neumaier 氏 [6] らはホフマングラフの表現を導入した。

定義 2.6. ホフマングラフ $\mathfrak{h}$ と正の整数 n に対し、以下を満たす写像 $\phi : V(\mathfrak{h}) \to \mathbf{R}^n$ をノルム m の表現と呼ぶ:

$$(\phi(x), \phi(y)) = \begin{cases} m & \text{if } x, y \in V_s(\mathfrak{h}) \text{ and } x = y; \\ 1 & \text{if } x, y \in V_f(\mathfrak{h}) \text{ and } x = y; \\ 1 & \text{if } \{x, y\} \in E(\mathfrak{h}); \\ 0 & \text{その他.} \end{cases}$$

$\{\phi(x) \mid x \in V(\mathfrak{h})\}$ で生成される格子を $\Lambda(\mathfrak{h}, m)$ で表す。

Example 2.7. 右の表は，左のホフマングラフ $\mathfrak{h}$ についての表現の例を表している。



	ϕ(1)	ϕ(2)	ϕ(3)	ϕ(4)	ϕ(5)	ϕ(6)	ϕ(7)
6	1	1	1	1	1	1	0
7	0	1	0	0	0	0	1
	-1	1	0	0	0	0	0
	1	0	0	0	0	0	0
	0	0	1	-1	0	0	0
	0	0	1	0	-1	0	0
	0	0	0	1	-1	0	0

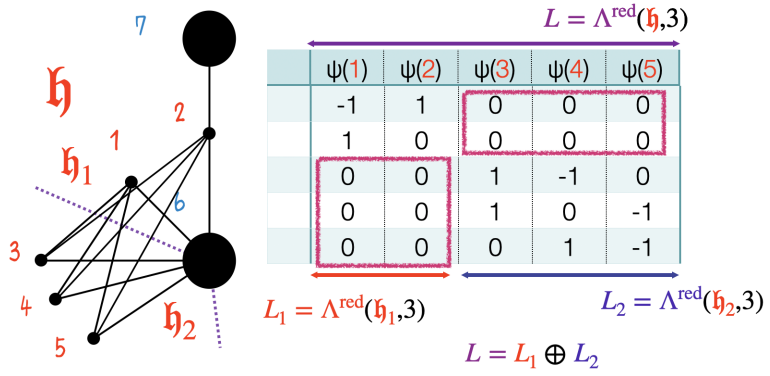
定義 2.8. ホフマングラフ $\mathfrak{h}$ と正の整数 n に対し、以下を満たす写像 $\psi : V^s(\mathfrak{h}) \to \mathbf{R}^n$ をノルム m の被約表現と呼ぶ:

$$(\psi(x),\psi(y)) = \begin{cases} m - |N^f_{\mathfrak{h}}(x)| & \text{if } x = y; \\ 1 - |N^f_{\mathfrak{h}}(x,y)| & \text{if } \{x,y\} \in E(\mathfrak{h}); \\ -|N^f_{\mathfrak{h}}(x,y)| & \text{その他.} \end{cases}$$

但し、$N^f_{\mathfrak{h}}(x)$ は x と隣接する fat 頂点の集合を表し、$N^f_{\mathfrak{h}}(x,y)$ は x,y の両方に隣接する fat 頂点の集合を表す。更に、$\{\psi(x) \mid x \in V_s(\mathfrak{h})\}$ で生成される格子を $\Lambda^{\mathrm{red}}(\mathfrak{h},m)$ で表す。

これで最小固有値が -2 を下回った時にも、ルート格子の理論を用いる事が出来るようになった。

Example 2.9. 右の表は，左のホフマングラフ $\mathfrak{h}$ についての被約表現の例を表している。$\mathfrak{h}$ は Example2.7 と同じグラフであり，fat 頂点 $6,7$ についての項目 $\phi(6),\phi(7)$ を除き，更に，fat 頂点に対応する行を取り除くことで，この表が得られる。また，$\mathfrak{h}$ が $\mathfrak{h} = \mathfrak{h}_1 \oplus \mathfrak{h}_2$ と分割されているので，$\psi(1),\psi(2)$ で張られる格子 $\Lambda^{\mathrm{red}}(\mathfrak{h}_1,3)$ と $\psi(1),\psi(2)$ で張られる格子 $\Lambda^{\mathrm{red}}(\mathfrak{h}_2,3)$ は直交している。



3　整格子

有限集合 U に対し，格子 Λ を次の様に定義する。

$$\Lambda = \langle U \rangle_{\mathbb{Z}} := \quad \left\{ \sum_{u \in U} a_u u \,\middle|\, a_u \in \mathbb{Z} \text{ for all } u \right\} \tag{3}$$

すべてのベクトルの組 $u, v \in \Lambda$ について，内積 (u, v) が整数のとき，格子 Λ は整格子と呼ばれる。

次に，グラフから整格子を作ることを考える。G をグラフとし，$B := A(G) - \lfloor \lambda_{\min}(G) \rfloor$ とする。このとき，正方行列 B は半正定値なので，$B = N^{\top} N$ と分解できる。このとき，G から生成される格子を $\Lambda = \Lambda(G) := \langle N \rangle_{\mathbb{Z}}$ で与える。隣接行列の成分は整数であることから，格子 Λ のすべてのベクトルの組 $u, v \in \Lambda$ について，内積 (u, v) は整数なので，グラフから作られた格子 Λ は整格子になる。

また，正の整数 n に対し，整格子 Λ が二乗ノルム n のベクトルたちからなる部分集合 $S = \{u \,|\, (u, u) = n\} \subset \Lambda$ で生成されるとき（すなわち $\Lambda = \langle S \rangle_{\mathbb{Z}}$），$\Lambda$ を n-格子と呼ぶ。$n = 2$ のとき，Λ は root 格子である。

Example 3.1. グラフ G の最小固有値が $-3 \leq \lambda_{\min} < -2$ のとき，$\Lambda(G)$ は 3-格子である。一方，ホフマングラフ $\mathfrak{h}$ の最小固有値が $\lambda_{\min} \geq -3$ のとき，$\Lambda(\mathfrak{h}, 3)$ は 3-格子である。

整格子 Λ について，$\sqrt{s}\Lambda$ が標準格子 $\mathbb{Z}^n$ の部分格子と同型であるとき，整格子 Λ は s-整化可能であるという。

Example 3.2. 定理 1.1 によれば，E-型 root 系によって表されるグラフがある。例えば E_6 のディンキン図形を表すグラフ (E_6 と書くようにしよう) がそれである。$\Lambda(E_6)$ は 2-格子である。しかし，1-整化可能ではない。$E_6 (\subset E_8)$ の基底の成分表示はよく知られており，直ちに確認することができる。それによれば，2-整化可能であることも直ちにわかる。

4　ホフマングラフの一般化

有向辺と無向辺を持つ，頂点・辺重み付きグラフ $\mathfrak{h} = (V, E, \mu, w)$ が次の性質を満たすとき，$\mathfrak{h}$ を一般ホフマン混合グラフと呼ぶ:

(i) (V, E) は混合グラフ（有向辺と無向辺を持つ）である。

(ii) $\mu : V \to [0, \infty)$ について，$\mu^{-1}((0, \infty))$ は独立集合である。

(iii) $w : E \to \mathbf{C}$ は，非辺 $\gamma\delta \notin E$ について $w(\gamma, \delta) = 0$ であり，辺 $\gamma\delta \in E$ について $w(\gamma, \delta) = \overline{w(\gamma, \delta)}$ であり，

$\mu(v) = 0$ のとき，v を slim 頂点と呼び，$\mu(v) \neq 0$ のとき，v を fat 頂点と呼ぶ。また，一般隣接行列 $A = A(\mathfrak{h})$ を次で与える:

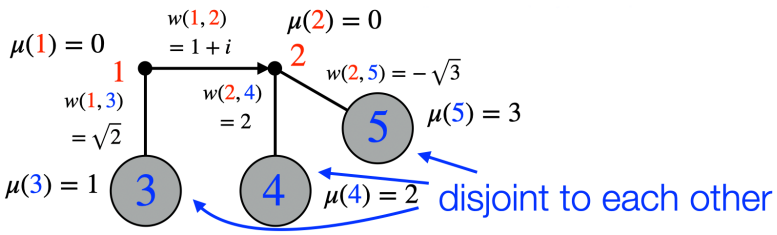
$$A_{\gamma,\delta} = \begin{cases} w(\gamma, \delta) & \text{if } \gamma\delta \in E(\mathfrak{h}), \\ 0 & \text{otherwise.} \end{cases}$$

一般ホフマングラフ $\mathfrak{h} = (V, E, \mu, w)$ について，

$$A(\mathfrak{h}) = \begin{pmatrix} A_s & L \\ L^* & O \end{pmatrix}$$

と表せる。ただし，L^* は L の複素共役転置行列，O は零行列を表す。また，$D = D(\mathfrak{h}) := (\mu(f_i))_{ii}$ $(f_i \in V_f)$ とする。このとき，$B(\mathfrak{h}) := A_s - LD^{-1}L^*$ の最小固有値を，一般ホフマングラフ $\mathfrak{h}$ の最小固有値と呼ぶ。

Example 4.1. 赤の数字は slim 頂点を表し，青の数字は fat 頂点を表す。



このグラフについての一般隣接行列は，

$$A = \begin{pmatrix} 0 & 1+i & \sqrt{2} & 0 & 0 \\ 1-i & 0 & 0 & 2 & -\sqrt{3} \\ \sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & -\sqrt{3} & 0 & 0 & 0 \end{pmatrix}$$

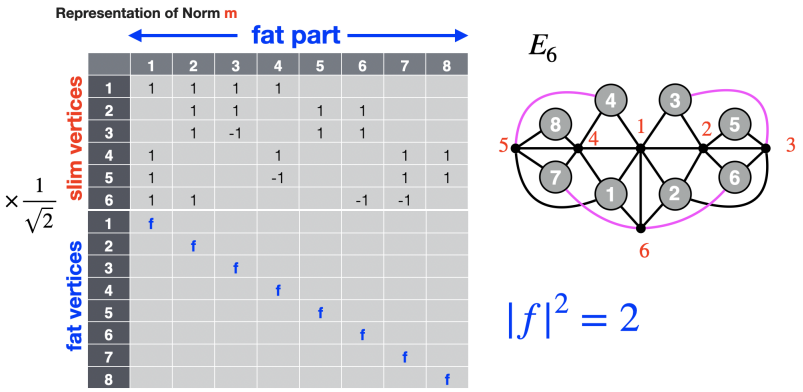
である。また，

$$\begin{aligned} B(\mathfrak{h}) &= \begin{pmatrix} 0 & 1+i \\ 1-i & 0 \end{pmatrix} - \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 2 & -\sqrt{3} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}^{-1} \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 2 \\ 0 & -\sqrt{3} \end{pmatrix} \\ &= \begin{pmatrix} -2 & 1+i \\ 1-i & -3 \end{pmatrix} \end{aligned}$$

なので，$\lambda_{\min}(\mathfrak{h}) = -4$ を得る。

Example 4.2. $w(E) = \{-1, 0, 1\}$ のときは辺符号グラフであり，$w(E) = \{0, 1, i, -i\}$ のとき，一般隣接行列は mixed graph (有向辺と無向辺を持つグラフ) の Hermitian 行列になる。

Example 4.3. E_6 のディンキン図形が，下図のような一般ホフマングラフの部分であることが確かめられる。



次のように，一般ホフマングラフでも定理 2.3 のような結果が得られる。

定理 4.4 (Hoffman's limit theorem)**.** $\mathfrak{h} = (V, E, \mu, w)$ を一般ホフマングラフとする。また，$\mathfrak{h}$ のすべての *fat* 頂点を，重み $\mu(f)$ の辺をもつ t 個の *slim* 頂点からなる完全グラフ K_t で置き換え，それを $\mathfrak{h}^t$ とする。このとき，$\lim_{t\to\infty} \lambda_{\min}(\mathfrak{h}^t) = \lambda_{\min}(\mathfrak{h})$ である。

4.1 一般ホフマングラフの表現

定義 4.5. m を正の実数とする。ホフマングラフ $\mathfrak{h} = (V, E, \mu, w)$ と正の整数 n に対し、以下を満たす写像 $\phi : V(\mathfrak{h}) \to \mathbf{R}^n$ をノルム m の表現と呼ぶ:

$$(\phi(\gamma), \phi(\delta)) = \begin{cases} m & \text{if } \gamma = \delta \in \mu^{-1}(0), \\ \mu(\gamma) & \text{if } \gamma = \delta \notin \mu^{-1}(0), \\ w(\gamma, \delta) & \text{if } \gamma\delta \in E(\mathfrak{h}); \\ 0 & \text{その他.} \end{cases}$$

$\{\phi(x) \mid x \in V(\mathfrak{h})\}$ で生成される格子を $\Lambda(\mathfrak{h}, m)$ で表す。

一般ホフマングラフは次の定理にあるように，[6] の定理 4.2 と同じような性質をもつ。

定理 4.6. $\mathfrak{h} = (V, E, \mu, w)$ を一般ホフマングラフとする。また，$V^f = \{f_1, \ldots, f_n\}$ で，

$$A(\mathfrak{h}) = \begin{pmatrix} A_s & L \\ L^* & O \end{pmatrix}, \quad D = (\mu(f_i))_{ii}$$

とする。このとき，以下は同値である。

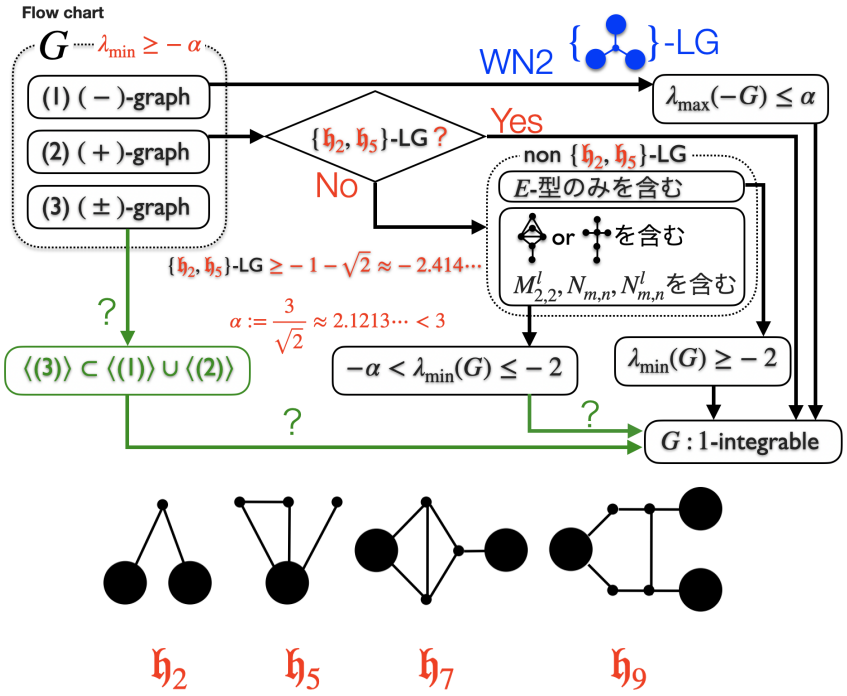
(i) $\lambda_{\min}(\mathfrak{h}) \geq -m$

(ii) $\mathfrak{h}$ はノルム m の表現をもつ

(iii) $A_s - LD^{-1}L^* + mI$ は半正定値行列である

5　最後に

現在，最小固有値が $-\frac{3}{\sqrt{2}}$ 以上のホフマングラフについて研究を進めている。



E-型のグラフから 3-格子を作るとき，研究集会で発表した整化性について一部例外が見つかった。上図の「E-型のみを含む → G : 1-integrable」の部分である。最小固有値が -2 以上の場合をもっとしっかり調べる必要がある。

参考文献

[1] A. J. Hoffman, *On graphs whose least eigenvalue exceeds* $-1-\sqrt{2}$, Linear Algebra Appl. 16 (1977), 153–165.

[2] H. J. Jang, J. Koolen, A. Munemasa and T. Taniguchi, *On fat Hoffman graphs with smallest eigenvalue at least* -3, Ars Mathematica Contemporanea, 7:105–121, 2014.

[3] R. Woo and A. Neumaier, *On graphs whose smallest eigenvalue is at least* $-1-\sqrt{2}$, Linear Algebra Appl. 226-228 (1995), 577–591.

数体の素元星座定理 I

見村万佐人（東北大学大学院理学研究科）
MIMURA, Masato
Mathematical Institute, Tohoku University

概要

本稿は，甲斐亘氏（東北大学大学院理学研究科），宗政昭弘氏（東北大学大学院情報科学研究科），関真一朗氏（青山学院大学理工学部），吉野聖人氏（東北大学大学院情報科学研究科）との共同研究 [KMM$^+$20] についてその結果や研究の背景を概説したものである．主定理は定理 3.1，その応用は先んじて定理 2.1，定理 2.3 で述べられる．主定理の証明に用いられる主要な道具に関しては，本報告集の関真一朗氏による「数体の素元星座定理 II」[関 21] を参照されたい．

本稿では $\mathbb{N} = \{1, 2, \dots, \}$ とし，$k \in \mathbb{N}$ に対し $[k] = \{1, 2, \dots, k\}$ とおく．$\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}$ を（有理）素数全体のなす集合とする．有限集合 A の濃度を $\#A$ で表わすことにする；A が無限集合のときは単に $\#A = \infty$ と書くことにする．

1 “星座定理”とは？

[KMM$^+$20] の主結果は，有名な「Green–Tao」の定理の一般の数体（有理数体の有限次拡大）への拡張である．[KMM$^+$20] の結果群に関して述べる前に，その動機付けとなる Green–Tao の定理の主張をここで与える．Green–Tao の定理は非退化等差数列の存在に関する定理であるが，[KMM$^+$20] のような多次元化を見据えて “星座定理” という枠組みで読み替えておく．

「Green–Tao の定理」にはいくつかのバージョンがあるが，ここで与えるものは「上漸近密度版」と呼ばれるものである．一般に $n \in \mathbb{N}$ に対し，$\mathbb{Z}^n$ の空でない部分集合 X と X の部分集合 A に対し，A の X に対する相対上漸近密度 $\overline{d}_X(A)$ を

$$\overline{d}_X(A) = \limsup_{M \to \infty} \frac{\#(A \cap [-M, M]^n)}{\#(X \cap [-M, M]^n)}$$

と定義する．特に，$\mathcal{P} \subseteq \mathbb{Z}$ であるので，$n = 1$ として $A \subseteq \mathcal{P}$ の相対上漸近密度 $\overline{d}_{\mathcal{P}}(A)$ が定義される．

定理 1.1 (Green–Tao の定理（上漸近密度版），[GT08])．$A \subseteq \mathcal{P}$ を $\overline{d}_{\mathcal{P}}(A) > 0$ なる集合とする．このとき，任意の $k \in \mathbb{N}$ に対し，A は k 項からなる非退化等差数列を含む．

ここで，「k 項からなる非退化等差数列」とはある $a \in \mathbb{Z}$, $d \in \mathbb{N}$ を用いて $\{a, a + l, a + 2l, \dots, a + (k-1)l\}$ と書ける形の $\mathbb{Z}$ の部分集合を指すこととする；$0 \notin \mathbb{N}$ であることに注意せ

よ．この定理を“多次元化”するために，「星座」と呼ばれる概念を定義する．

定義 **1.2** (星座)．$\mathcal{Z}$ を有限ランクの自由 $\mathbb{Z}$-加群とする．S を $\mathcal{Z}$ の空でない有限部分集合とする．このとき，S を形状とする星座（constellation with the shape S）$\mathcal{S}$ とは，$\alpha \in \mathcal{Z}, l \in \mathbb{N}$ を用いて

$$\mathcal{S} = \alpha + lS$$

と書ける集合を指す．

S を形状とする星座を「S-星座」(S-constellation）と以下略記する．上の定義において，$\mathcal{Z}$ のランクを n とおくと適切な基底のもとで $\mathcal{Z} \simeq \mathbb{Z}^n$ である．基底を一つ選んでこの同一視のもとで最初から $\mathcal{Z} = \mathbb{Z}^n$ と思ってもよいが，後に $\mathcal{Z}$ の例として数体 K の整数環 $\mathcal{O}_K$ のような一般には“標準的”な基底が決まるわけではないものを扱うため，上のような定式化をしている．

$\mathcal{Z} = \mathbb{Z}$ のとき，$\{a, a+l, a+2l, \ldots, a+(k-1)l\} = (a-l) + l[k]$ である．従って，「k 項からなる非退化等差数列」は定義 1.2 の言葉を用いると「$[k]$-星座」と読み替えることができる．定理 1.1 は以下の主張と同値である．（補足 1.4 も見よ．）

定理 **1.3** (定理 1.1 の“（1 次元）星座定理”への読み替え)．$A \subseteq \mathcal{P}$ を $\overline{d}_{\mathcal{P}}(A) > 0$ なる集合とする．このとき，任意の空でない有限集合 $S \subseteq \mathbb{Z}$ に対し，A は S-星座を含む．

定理 1.3 の主張は，有限ランク自由 $\mathbb{Z}$-加群 $\mathcal{Z}$ の特定の部分集合 A が「任意の空でない有限集合 $S \subseteq \mathcal{Z}$ に対し，A は S-星座を含む」，という形をしている．この形の定理，ないし，さらに S-星座に条件を追加したものの存在を保証する定理を，本稿では星座定理（constellation theorem）と呼ぶことにする．

補足 1.4. 定理 1.3 から定理 1.1 の導出は易しい．逆の導出では，任意の空でない有限集合 $S \subseteq \mathbb{Z}$ に対しある $a \in \mathbb{Z}$ とある $k \in \mathbb{N}$ が存在し，$S \subseteq a + [k]$ とできることに注意せよ．

補足 1.5. 定理 1.1 において，A から有限部分集合を取り除いてできる集合 A' は $\overline{d}_{\mathcal{P}}(A') = \overline{d}_{\mathcal{P}}(A)$ を満たすことに注意しよう．このため，定理 1.1 の仮定を満たす A は，任意の $k \in \mathbb{N}$ に対し k 項からなる非退化等差数列を互いに非交和（disjoint）であるように無数に含むこともわかる．

補足 1.6. 特に $\overline{d}_{\mathcal{P}}(\mathcal{P}) = 1 > 0$ である．これと補足 1.5 より，任意の $k \in \mathbb{N}$ に対し，$\mathcal{P}$ は k 項からなる非退化等差数列を互いに非交和（disjoint）であるように無数に含むことがわかる．この主張がいわゆる “Green–Tao の定理” として広く知られているものであろう．

Dirichlet の算術級数定理（の枠組みでの素数定理の拡張）より，$a \in \mathbb{N}, b$ を a と互いに素な整数とするとき，$\bmod a$ で b と合同な素数全体の集合 $P(a,b)$ は

$$\overline{d}_{\mathcal{P}}(P(a,b)) = \frac{1}{\varphi(a)} > 0$$

を満たす．ここで，φ は Euler のトーシェント関数である．この $P(a,b)$ は定理 1.1, 定理 1.3 を適用できる A の典型例である．

2　主定理の応用：2 元 2 次形式での素数表現星座定理

[KMM+20] の主定理は数体の整数環の素元に関する星座定理であるが，いきなり「数体の整数環の素元」と言われても今一つ親しみが持てない，という読者（筆者が以前はそうであった）もおられるであろう．主定理を述べる前に，本節では主定理の応用である「2 元 2 次形式での素数表現に関する星座定理」について説明する．この定理は “通常の素数”（つまり，有理素数）に関する定理である．

整数係数の 2 元 2 次形式（以下，単に “2 元 2 次形式” と書くことにする）を一つとってこよう．本稿では，

$$F_1(x,y) = x^2 - 79y^2$$

という具体的な 2 次形式について考えることにしよう．F_1 は写像 $\mathbb{Z}^2 \to \mathbb{Z}$ とみなせるが，$F_1^{-1}(\mathcal{P})$ という $\mathbb{Z}^2$ の部分集合に注目しよう．$(x,y) \in F_1^{-1}(\mathcal{P})$ であることは，$F_1(x,y) \in \mathcal{P}$ であることを意味する．一般に 2 元 2 次形式 F に対し $F(\mathbb{Z}^2) \cap \mathcal{P}$，つまり，形式 F が表現できる素数全体の集合については古くから数論の研究対象であった．この集合は $\mathcal{P}$ の部分集合で，(F が後で述べる定理 2.3 の仮定を満たすときは）定理 1.3 が適用できうるものである．ここでは 1 次元の星座定理の “多次元化” ということで，「どのような素数が形式 F で表現できるか？」ではなく「どのような整数の組 (x,y) が形式 F によって素数に写るか？」を考えている．上の形式 F_1 では，例えば $F_1(9,1) = 2 \in \mathcal{P}$，$F_1(28,3) = 73 \in \mathcal{P}$，$F_1(55,6) = 181 \in \mathcal{P}$ なので，$(9,1), (28,3), (55,6) \in F_1^{-1}(\mathcal{P})$ である．このとき，[KMM+20] の結果群の具体例として，以下が成立する．

定理 2.1 ([KMM+20, Theorem C] の具体例)**.** 上の 2 元 2 次形式 F_1（$F_1(x,y) = x^2 - 79y^2$）に対し，$A \subseteq F_1^{-1}(\mathcal{P}) \subseteq \mathbb{Z}^2$ が $\overline{d}_{F_1^{-1}(\mathcal{P})}(A) > 0$ を満たすとする．このとき，任意の空でない有限集合 $S \subseteq \mathbb{Z}^2$ に対し，次の 2 条件をともに満たす S-星座 $\mathcal{S}$ が存在する．

(1) $\mathcal{S} \subseteq A$ である．
(2) F_1 の $\mathcal{S}$ への制限 $F_1|_{\mathcal{S}} \colon \mathcal{S} \to \mathbb{Z}$ は単射である．

(2) は，「F_1 によって表現される素数が，$\mathcal{S}$ 上ですべて異なる」ことを意味している．

定理 2.1 のような 2 元 2 次形式による素数表現星座定理は，F_1 と異なる形式で我々の結果より以前に知られているような例がある．それは Tao [Tao06] による「Gauss 素数星座定理」の系として得られる以下の結果である．

定理 2.2 ([Tao06] の系)**.** 次の 2 元 2 次形式

$$F_2(x,y) = x^2 + y^2$$

に対し，$A \subseteq F_2^{-1}(\mathcal{P})$ が $\overline{d}_{F_2^{-1}(\mathcal{P})}(A) > 0$ を満たすとする．このとき，任意の空でない有限集合 $S \subseteq \mathbb{Z}^2$ に対し，次の 2 条件をともに満たす S-星座 $\mathcal{S}$ が存在する．

(1) $\mathcal{S} \subseteq A$ である．
(2) F_2 の $\mathcal{S}$ への制限 $F_2\,|_{\mathcal{S}} \colon \mathcal{S} \to \mathbb{Z}$ は単射である．

定理 2.1 と定理 2.2 の見かけはそっくりであるが，定理 2.1 の証明には定理 2.2 の証明には現れなかった大きな困難が 2 つ生じる．実際，上で述べたように定理 2.2 は Tao の論文 [Tao06] の結果から直接従う結果であるが，定理 2.1 の証明は我々の結果 [KMM+20] を待たなければいけなかった．以下の 2 つの “大きな困難” については，4 節でさらに論を進める．

(a)（1 つ目の困難） Fermat 以来よく知られているように，F_2 が表現できる素数，つまり，$F_2(\mathbb{Z}^2) \cap \mathcal{P}$ の元，には $\bmod 4$ による特徴づけがある：$p \in F_2(\mathbb{Z}^2) \cap \mathcal{P}$ であることは，$p = 2$ または p が $\bmod 4$ で 1 と合同であることと同値である．他方，一般の 2 元 2 次形式 F では，F が表現できる素数の mod による特徴づけができないことが知られている．（背後に非類体論的現象がある．）

(b)（2 つ目の困難） 形式 F_2 において $p \in \mathcal{P}$ の逆像 $F_2^{-1}(\{p\})$ は高々 8 元集合であることが知られている．（もし $(x, y) \in F_2^{-1}(\{p\})$ であるならば，$F_2^{-1}(\{p\}) = \{(\pm x, \pm y), (\pm y, \pm x)\}$ である．ここで $\pm$ は好きにとってよい．）従って，$A \subseteq F_2^{-1}(\mathcal{P})$ が $\overline{d}_{F_2^{-1}(\mathcal{P})}(A) > 0$ を満たすとき，適切に部分集合 $A' \subseteq A$ をとると

$$\overline{d}_{F_2^{-1}(\mathcal{P})}(A') \geq \frac{1}{8}\overline{d}_{F_2^{-1}(\mathcal{P})}(A)$$

を満たすようにできる；特にこの A' は $\overline{d}_{F_2^{-1}(\mathcal{P})}(A') > 0$ を満たす．A の代わりに A' に定理 2.2 を適用することで，(2) の単射性を容易に担保できる．

他方，形式 F_1 においては線型変換

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 80 & 711 \\ 9 & 80 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

が形式 F_1 を保つ．つまり，

$$F_1(80x + 711y, 9x + 80y) = F_1(x, y)$$

を満たす．（興味がある読者は確認されたい．）上の線型変換（とその逆変換）の繰り返しによる $\mathbb{Z}$-作用での $(0, 0)$ 以外の元の軌道は無限集合である．そのため，定理 2.1 (2) の単射性の証明には，定理 2.2 (2) の証明の際には現れなかった “大きな困難” が生じる．

さて，今までの記述から，「[KMM+20] では，どんな（整数係数）2 元 2 次形式に対して素数表現星座定理を得たのか？」が気になった読者もおられるのではないかと思われる．もっともナイーブには，“$F(x, y) = ax^2 + bxy + cy^2$，$a, b, c \in \mathbb{Z}$，なる任意の（整数係数）2 元 2 次形式での定理” を望みたくなるが，これが不可能であることは容易にわかる．実際，素数表現星座定理の成立には，次の 3 種類の “自明な制約” がある．

- （原始性）形式 $F(x.y) = ax^2 + bxy + cy^2$ において，a, b, c の最大公約数が 1 であるとき F は原始的（primitive）であるという．F が非原始的であるとき，$F(\mathbb{Z}^2) \cap \mathcal{P}$ は有限集合となり，素数表現星座定理は望むべくもない．

- （非退化性）例えば形式 $F(x,y)=3x^2+13xy+10y^2$ は，$F(x,y)=(3x-2y)(x+5y)$ のように 2 変数多項式環 $\mathbb{Z}[x,y]$ の元として 1 次式の積に分解されてしまう．このような形式でも $F(\mathbb{Z}^2)\cap\mathcal{P}$ は有限集合となり，素数表現星座定理は望むべくもない．$F(x,y)=ax^2+bxy+cy^2$ において，その判別式 $D_F=b^2-4ac$ が完全平方数でないことが，$F(x,y)$ が零形式でなく，かつ，$\mathbb{Z}$-係数の 1 次式の積に分解されないことの必要十分条件を与える．これを満たすとき，F は非退化（non-degenerate）であるという．
- （負定値でないこと）例えば形式 $F(x,y)=-x^2-79y^2$ は負定値である，つまり，任意の $(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}$ に対し $F(x,y)<0$ を満たす．このような形式では $F(\mathbb{Z}^2)\cap\mathcal{P}$ は空集合となり，素数表現星座定理は望むべくもない．

我々の結論は，“2 元 2 次形式での素数表現星座定理の制約” は，上の 3 つに限るというものである．正確な主張を以下で述べる．

定理 **2.3** (2 元 2 次形式での素数表現星座定理, [KMM$^+$20, Theorem C])．$F(x,y)=ax^2+bxy+cy^2$, $a,b,c\in\mathbb{Z}$, を 2 元 2 次形式とする．F が次の 3 条件を全て満たすとする．

- F は原始的である：つまり，a,b,c の最大公約数が 1 である．
- F は非退化である：つまり，F の判別式 $D_F=b^2-4ac$ は完全平方数でない．
- F は負定値ではない：上の 2 条件のもとで，これは「$a>0$ または $c>0$ である」ことと同値である．

$A\subseteq F^{-1}(\mathcal{P})$ が $\overline{d}_{F^{-1}(\mathcal{P})}(A)>0$ を満たすとする．このとき，任意の空でない有限集合 $S\subseteq\mathbb{Z}^2$ に対し，次の 2 条件をともに満たす S-星座 $\mathcal{S}$ が存在する．

(1) $\mathcal{S}\subseteq A$ である．
(2) F の $\mathcal{S}$ への制限 $F|_{\mathcal{S}}\colon\mathcal{S}\to\mathbb{Z}$ は単射である．

3　主定理：数体の素元星座定理

本節で，いよいよ [KMM$^+$20] の主定理である「数体の素元星座定理」について述べる．一般論を述べる前に，まず定理 2.1 を例に，その背景にある数論的対象を明らかにしていく．定理 2.1 の 2 元 2 次形式 $F_1(x,y)=x^2-79y^2$ を思い出そう．F_1 は $\mathbb{Z}$-係数では既約であるが，係数の範囲を拡大すれば

$$F_1(x,y)=(x+\sqrt{79}y)(x-\sqrt{79}y)$$

と分解される．これは数体を有理数体 $\mathbb{Q}$ から実 2 次体 $\mathbb{Q}(\sqrt{79})$ に拡大していることと対応する．数体 $\mathbb{Q}(\sqrt{79})$ の整数環 $\mathcal{O}_{\mathbb{Q}(\sqrt{79})}$ は $\mathcal{O}_{\mathbb{Q}(\sqrt{79})}=\mathbb{Z}[\sqrt{79}]$ である．これはランクが 2 の自由 $\mathbb{Z}$-加群であり，その基底として $(1,\sqrt{79})$ がとれる．（順番も込みで基底を取っているので $\{1,\sqrt{79}\}$ と書いていない：$\mathbb{Z}^2$ の元と区別されたい．）このときのノルム形式（norm form），つまり，

$$\mathbb{Z}^2\to\mathbb{Z}[\sqrt{79}]\to\mathbb{Z};\quad (x,y)\mapsto\alpha=x+y\sqrt{79}\mapsto N_{\mathbb{Q}(\sqrt{79})/\mathbb{Q}}(\alpha)=\alpha\overline{\alpha}$$

が形式 F_1 の “数論的な正体” である．ここで $\alpha = x + y\sqrt{79} \in \mathbb{Z}[\sqrt{79}]$ $(x, y \in \mathbb{Z})$ に対し，$\overline{\alpha}$ はその共役，つまり $\overline{\alpha} = x - y\sqrt{79}$ を意味する．以上では色々なものの定義を説明しなかったが，以下で一般の設定で定義を紹介しておく．

K を数体（number field），つまり，有理数体 $\mathbb{Q}$ の有限次拡大とし，その拡大次数 $[K : \mathbb{Q}]$ を n とおく．K の整数環（the ring of integers）とは，K の元で $\mathbb{Z}$-係数のモニック多項式の根となるもの全体のなす集合である；これは環となり，ランクが n の自由 $\mathbb{Z}$-加群の構造をもつ．$\mathcal{O}_K$ の自由 $\mathbb{Z}$-加群としての基底 $\boldsymbol{\omega} = (\omega_1, \omega_2, \ldots, \omega_n)$ を K の整基底（integral basis）という．K の複素数体 $\mathbb{C}$ への体の埋め込みはちょうど n 個ある；これらを $\sigma_1, \sigma_2, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ とおく．このとき，ノルム写像 $N_{K/\mathbb{Q}}$ は

$$N_{K/\mathbb{Q}} \colon \mathcal{O}_K \to \mathbb{Z}; \quad \alpha \mapsto \prod_{i \in [n]} \sigma_i(\alpha)$$

で定義される．（$N_{K/\mathbb{Q}}$ の終域を $\mathbb{Z}$ と取れることが知られている．）$\alpha \in \mathcal{O}_K \setminus \{0\}$ に対し，そのノルム（norm）の絶対値 $|N_{K/\mathbb{Q}}(\alpha)|$ は単項イデアル $\alpha\mathcal{O}_K$ のイデアルノルム（ideal norm）$\mathbf{N}(\alpha\mathcal{O}_K)$ と一致することが知られている．ここで $\mathfrak{a}$ を $\mathcal{O}_K$ の非零イデアルとするとき，そのイデアルノルムは

$$\mathbf{N}(\mathfrak{a}) = \#\left(\mathcal{O}_K/\mathfrak{a}\right)$$

で定義される．（これが有限値であることが知られている．）$\pi \in \mathcal{O}_K$ が $\mathcal{O}_K$ の素元（prime element）であるとは，単項イデアル $\pi\mathcal{O}_K$ が非零な素イデアルであることをいう．数体 K に対し，$\mathcal{O}_K$ の素元全体のなす集合を $\mathcal{P}_K$ と本稿ではおくことにする．

イデアルノルム $\mathbf{N}(\pi\mathcal{O}_K)$ が（有理）素数であるような元 π は特に $\pi \in \mathcal{P}_K$ を満たす（素元である）ことが示せる．（正確には，このような π は次数が 1 の素元と呼ばれる．）こうして，$F_1(x, y) = x^2 - 79y^2$ での素数表現星座定理は，粗い意味で（次数が 1 の素元を考えていること，ノルムの符号，定理 2.1 (2) の単射性の条件，の 3 つを棚に上げれば）「実 2 次体 $\mathbb{Q}(\sqrt{79})$ の整数環 $\mathbb{Z}[\sqrt{79}]$ の素元に関する星座定理」と読み替えることができる．

以上の設定のもとで，[KMM+20] の主定理「数体の素元星座定理」（の上漸近密度版）を述べる．ここで，有限ランクの自由 $\mathbb{Z}$-加群 $\mathcal{Z}$ とその基底 $\mathbf{v}$ に対し，相対上漸近密度を以下のように定義する．$\|\cdot\|_{\infty,\mathbf{v}}$ を $\mathcal{Z}$ 上の $\mathbf{v}$ に関する ℓ_∞-長さ（ℓ_∞-length）とする：これは，$\mathcal{Z}$ の元を基底 $\mathbf{v}$ で成分表示した際の成分の絶対値の最大値のことと定義する．空でない集合 $X \subseteq \mathcal{Z}$ と X の部分集合 A に対し，A の X に対する，基底 $\mathbf{v}$ に関する相対上漸近密度 $\overline{d}_{X,\mathbf{v}}(A)$ を

$$\overline{d}_{X,\mathbf{v}}(A) = \limsup_{M \to \infty} \frac{\#(A \cap \{\alpha \in \mathcal{Z} : \|\alpha\|_{\infty,\mathbf{v}} \leq M\})}{\#(X \cap \{\alpha \in \mathcal{Z} : \|\alpha\|_{\infty,\mathbf{v}} \leq M\})}$$

で定める．$\overline{d}_{X,\mathbf{v}}(A)$ の値自体は $\mathcal{Z}$ の基底 $\mathbf{v}$ の取り方に一般には依存する；しかし，$\overline{d}_{X,\mathbf{v}}(A) > 0$ であるかどうかは $\mathbf{v}$ の取り方に依らないことが容易に確認できる．数体 K の整基底 $\boldsymbol{\omega}$ を取るとき，$\boldsymbol{\omega}$ は整数環 $\mathcal{O}_K$ の自由 $\mathbb{Z}$-加群としての基底であった．また，定理 2.3 (2) の単射性に粗方（完全ではないが）対応する条件として，単数群の作用を考える．$\mathcal{O}_K$ の乗法での可逆元全体のなす群を $\mathcal{O}_K^\times$ と書き，K の単数群（the group of units）という．乗法による作用

$$\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}; \quad \eta \cdot \alpha = \eta\alpha$$

はイデアルノルムを保つ作用で，$\mathcal{P}_K$ を保つ．$\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ が同伴（associate）であるとは，これらが上の $\mathcal{O}_K^\times$-作用で同じ軌道に属することをいう．

定理 3.1 (数体の素元星座定理：上漸近密度版, [KMM+20, Theorem A, Theorem 1.4 も見よ．]). K を数体，$\boldsymbol{\omega}$ を整基底とし，$\mathcal{O}_K$ を K の整数環とする．$\mathcal{O}_K$ の素元全体の集合 $\mathcal{P}_K$ の部分集合 A が $\overline{d}_{\mathcal{P}_K,\boldsymbol{\omega}}(A) > 0$ を満たすとする．このとき，任意の空でない有限集合 $S \subseteq \mathcal{O}_K$ に対し，次の 2 条件をともに満たす S-星座 $\mathcal{S}$ が存在する．

(1) $\mathcal{S} \subseteq A$ である．
(2) $\mathcal{S}$ に属する相異なる 2 元は同伴でない．

補足 3.2. 定理 3.1 から定理 2.3 を導出しようと思うと，K が 2 次体のときに更なる一般化を行なう必要がある．古くから知られた一般論として，非原始的で非退化な（整数係数）2 元 2 次形式が 2 次体 K とその整環（order）$\mathcal{O}$，$\mathcal{O}$ の可逆分数イデアル（invertible fractional ideal）$\mathfrak{c}$，$\mathfrak{c}$ の $\mathbb{Z}$-加群としての基底 (γ_1, γ_2)，符号 $\epsilon \in \{\pm 1\}$ の組 $(K, \mathcal{O}, \mathfrak{c}, (\gamma_1, \gamma_2), \epsilon)$ で決まることが分かっている；このことは [KMM+20, Theorem 10.3 と Appendix A] でも振り返っている．定理 3.1 は数体の整環 $\mathcal{O}$ とその可逆分数イデアル $\mathfrak{c}$ の組 $(\mathcal{O}, \mathfrak{c})$ の設定に拡張することができ，これが K が 2 次体のときに定理 2.3 の導出に用いられる．整環やその可逆分数イデアルに関しては本稿では詳細は述べない：$(\mathcal{O}, \mathfrak{c}) = (\mathcal{O}_K, \mathcal{O}_K)$ のときが定理 3.1 の主張である．

補足 3.3. 補足 3.2 で述べたように，定理 3.1 は数体 K の整環 $\mathcal{O}$ とその可逆分数イデアル $\mathfrak{c}$ の組 $(\mathcal{O}, \mathfrak{c})$ の設定に拡張できる．この設定で $\mathfrak{c}$ の $\mathbb{Z}$-加群としての基底 $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ を一つ決めることでノルム形式

$$\mathbb{Z}^n \to \mathfrak{c} \to \mathbb{Z}; \quad (x_1, \cdots, x_n) \mapsto \alpha = \sum_{i \in [n]} x_i \gamma_i \mapsto \frac{N_{K/\mathbb{Q}}(\alpha)}{\mathbf{N}(\mathfrak{c})}$$

を適切な定式化のもとで定義できる．ここで n は K の $\mathbb{Q}$ 上の拡大次数である．定理 2.3 を適切な形で，この意味での一般のノルム形式の枠組みに一般化できる．詳細が気になる読者は [KMM+20, Theorem 10.36] を参照されたい．

4 主証明について：戦略と 2 つの “大きな困難”

本稿の最後に，定理 3.1 の証明について大まかに説明する．定理 2.2 は Tao の定理の系であると 2 節で述べていた．正確には，定理 3.1 で $K = \mathbb{Q}(\sqrt{-1})$ のときの主張を Tao は [Tao06] で示しており，3 節で説明した読み替えによって定理 2.2 をこれから導出できる．$K = \mathbb{Q}$ のときが Grenn–Tao の定理 [GT08]（本稿の 定理 1.3）である．このように，[KMM+20] の主定理 3.1 は先行研究の，任意の数体への一般化と解釈することができる．星座定理の証明における基本的な戦略と，任意の数体への一般化の際に生じた 2 つの “大きな困難” について述べる．

まず，（本来はもっと前の章で述べるべきだったが）星座定理の源流は以下の Furstenberg–Katznelson [FK78] による「多次元 **Szemerédi** の定理（Multi-dimensional Szemerédi Theo-

rem)」である：この定理で $n=1$ のときが，有名な Szemerédi の定理 [Sze75] である．

定理 4.1 (多次元 Szemerédi の定理 [FK78])．$n \in \mathbb{N}$ とする．$A \subseteq \mathbb{Z}^n$ が $\overline{d}_{\mathbb{Z}^n}(A) > 0$ を満たすとする．このとき，任意の空でない有限集合 $S \subseteq \mathbb{Z}^n$ に対し，A は S-星座を含む．

定理 4.1 は「密 (dense)」，つまり，$\overline{d}_{\mathbb{Z}^n}(A) > 0$ の設定で発動する．これを「疎 (sparse)」，つまり，$\overline{d}_{\mathbb{Z}^n}(A) = 0$ のときでも特定の A に対し拡張しようという試みが数多く行なわれ，Green–Tao の定理はその中での金字塔と言うべき結果である．もっとも挑戦的な問いは，“A の（$[-M,M]^n$ で区切って $M \to \infty$ としたときの）数え上げが十分なオーダーをもっていさえすれば，それだけで定理 4.1 の結論が成り立つのではないか？” というものである．近年の目覚ましい発展として，$n=1$ で $S=[3]$（つまり，S-星座として 3 項からなる非退化等差数列を考える）ときに Bloom–Sisask [BS20] によって次の結果が得られた．

定理 4.2 ([BS20] の系)．$A \subseteq \mathbb{Z}$ が

$$\limsup_{M\to\infty} \frac{\#(A \cap [-M,M])}{M(\log M)^{-1}} > 0$$

を満たすとする．このとき，A は 3 項からなる非退化等差数列を含む．

素数定理より，$\mathcal{P}$ に対する相対上漸近密度が正な部分集合 $A \subseteq \mathcal{P}$ は定理 4.2 の数え上げ条件を満たす．従って，$k=3$ のとき定理 1.1 は，[BS20] が示された現在となっては素数に関する（素数定理よりも）深い性質は一切用いることなく，数え上げ条件のみから導出される．

このように，我々の主定理 3.1 も将来的には A の $\|\cdot\|_{\infty,\boldsymbol{\omega}}$ を尺度とする数え上げ条件のみから導出できる可能性もある．しかし，現状では定理 4.2 の証明は $n \geq 2$，ないし $n=1$ でも $S=[k]$ が $k \geq 4$ の場合には拡張が大変困難であると考えられている．以上のことを踏まえると，我々の定理 3.1 の証明の戦略は以下 (I)，(II) の 2 つの柱からなると解釈することもできる．

(I) 数え上げ（counting）：仮定を満たす A は，数え上げ条件

$$\limsup_{M\to\infty} \frac{\#(A \cap \{\alpha \in \mathcal{O}_K : \|\alpha\|_{\infty,\boldsymbol{\omega}} \leq M\})}{M^n(\log M)^{-1}} > 0$$

を満たす．

(II) 劣擬ランダム性（subpseudorandomness）：A は “よく適合する擬ランダム測度が存在する集合” の部分集合である．

(I) の数え上げは，数論（素数定理の数体への拡張）によって保証できる：2 つの “大きな困難” のところでより詳細を述べる．(II) の “劣擬ランダム性” の正確な定式化には多くの準備が必要となる：[KMM+20, Definition 8.3] で定義される集合族 $\mathrm{S}\Psi_{\log}(\mathcal{O}_K)$ の元が “劣擬ランダム” な集合 $A \subseteq \mathcal{O}_K$ である．擬ランダム性は「重みつきハイパーグラフ（weighted hypergraph）」ついて先行研究で定義され（本報告集の関真一朗さんの文書 [関 21, 定義 3.2] も見よ），これを “拡大解釈” することで今回の設定で $\mathcal{O}_K \simeq \mathbb{Z}^n$ 上の重みに関しても定式化できる：[関 21, 定義 4.1]．(I), (II) からの星座定理の導出には，組合せ論の大道具を用いる．それが相対ハイパーグラフ

除去補題（Relative Hypergraph Removal Lemma）[CFZ15] など：主張は [関 21, 定理 3.3] を見よ，である．我々の論文 [KMM$^+$20] では，一連の組合せ論による星座定理” の導出をパッケージ化した．その成果として，「相対多次元 **Szemerédi** の定理（Relative Multi-dimensinal Szemerédi Theorem)」([KMM$^+$20, Theorem 5.4]：[関 21, 定理 4.3] も見よ）や “$A \subseteq \mathcal{O}_K$ に関する主張”（[KMM$^+$20, Theorem 8.21]）を得ている．以上のように，「(II) の正確な定式化」，および，「(I) と (II) からの星座定理の導出」は，かなり技術的なものになる．本稿では上記の大まかな戦略のみを述べ，詳細は本報告集での関さんの文書 [関 21] に譲ることとする．

本稿の最後に，我々の主定理 3.1 の証明における (I), (II) の確認に伴う 2 つの “大きな困難” について述べる：これらの困難の克服が，$K = \mathbb{Q}$（[**GT08**]），$K = \mathbb{Q}(\sqrt{-1})$（[**Tao06**]）の先行研究と比較しての新規性となる．2 節で，$F_2(x, y) = x^2 + y^2$ と比較して，$F_1(x, y) = x^2 - 79y^2$ や一般の（定理 2.3 の条件を満たす）2 元 2 次形式での素数表現星座定理の攻略上の 2 つの “大きな困難” (a), (b) について述べた．3 節での読み替えにより，これらの背後には付随する数体 K の数論的な性質がある．(a) と関係するのが，数体 K の類数（class number）h_K である．これは数体のイデアル類群 Cl_K と呼ばれる有限群の位数であり，h_K が 1 であるかそうでないかは整数環 $\mathcal{O}_K$ の構造に大きな違いをもたらす．例えば，$\mathcal{O}_K$ が一意分解整域（UFD）であること（本質的には，素元分解が可能であること）と $h_K = 1$ であることは同値である．(b) はまさしく，単数群 $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{79})}$ の無限性に起因している：(b) の説明で出てきた線型変換は，$(x, y) \mapsto x + y\sqrt{79}$ の対応のもとで $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{79})} \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ の自由部分の生成元 $80 + 9\sqrt{79}$ の掛け算に由来している．また，$h_{\mathbb{Q}(\sqrt{79})} = 3 > 1$ である．以上のように，主定理 3.1 における 2 つの大きな困難とは

- 「類数」による困難（$h_K > 1$）；
- 「単数群」による困難（$\#(\mathcal{O}_K^\times) = \infty$）

である．先行研究での $K = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-1})$ ではどちらも $h_K = 1$ かつ $\#(\mathcal{O}_K^\times) < \infty$ で，これらの困難はともに現れない．2021 年現在 $h_K = 1$ となる数体 K が無限個存在するかは未解決問題とされており，また，Dirichlet の単数定理より $\#(\mathcal{O}_K^\times) < \infty$ となることと $K = \mathbb{Q}$ または K が虚 2 次体であることは同値である．さらに，Baker–Heegner–Stark の定理より，虚 2 次体で類数が 1 である K はちょうど 9 個である．特に，$h_K = 1$ かつ $\#(\mathcal{O}_K^\times) < \infty$ を満たす数体 K は 10 個のみである．上記の 2 つの困難は我々が乗り越えなければいけない壁であった．

我々の研究 [KMM$^+$20] でのこれら 2 つの大きな困難の克服の概略は以下である．まず「類数」による困難は，元ではなく $\mathcal{O}_K$ の非零イデアルを考えることで行なった．$\mathcal{O}_K$ は素イデアル分解の存在と一意性は（K の類数によらず）成り立つ．[GT08] や [Tao06] では戦略の (II) （“劣擬ランダム性”）と関係する擬ランダム測度は $\mathcal{O}_K$ の元を用いて構成されていた．我々はこの擬ランダム測度の構成を一般の数体に拡張する際に，設定を全てイデアルに移行させることで行なった．詳細は [KMM$^+$20, Section 6] を参照されたい．戦略の (I)（元の数え上げ）の際も，数論的な立場からは「元の数え上げ（element counting)」よりも「イデアルの数え上げ（ideal counting)」の方が自然と思える：素イデアルのイデアルノルム $\mathbf{N}$ を尺度とする数え上げの結果として，**Chebotarev** の密度定理が著名である．しかし，戦略 (I) で実際に必要なのは「元の数

え上げ」なので，「イデアルの数え上げ」を「元の数え上げ」に何とかして移行する必要がある．この際に気を付けないといけないことは以下の二つである．

- 単数群が掛け算により $\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}$ と作用していたことを 3 節で述べた．この作用は，$\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ に対し，単項イデアルの相等 $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$ は α と β が同じ $\mathcal{O}_K^\times$-軌道に属する（つまり，同伴である）ことと同値である．従って，$\#(\mathcal{O}_K^\times) = \infty$ のとき，1 つの単項（非零）素イデアルに対応する素元は無限個存在してしまい，そのままでは「元の数え上げ」ができない．
- 元 $\alpha \in \mathcal{O}_K \setminus \{0\}$ には整基底 $\boldsymbol{\omega}$ に関する ℓ_∞-長さ $\|\alpha\|_{\infty,\boldsymbol{\omega}}$ とイデアルノルム $\mathbf{N}(\alpha\mathcal{O}_K)$ の 2 つの尺度がある．「イデアルの数え上げ」には後者が用いられるが，「元の数え上げ」で考えるべき尺度は前者である．$[K : \mathbb{Q}] = n$ とおくと，よい状況では $\|\alpha\|_{\infty,\boldsymbol{\omega}}^n$ と $\mathbf{N}(\alpha\mathcal{O}_K)$ は近い．しかし，$\#(\mathcal{O}_K^\times) = \infty$ のときは，上記の単数群作用により $\mathbf{N}(\alpha\mathcal{O}_K)$ を変えずに $\|\alpha\|_{\infty,\boldsymbol{\omega}}$ をいくらでも大きくできる．

我々はこれらの問題を，Minkowski 埋め込みを用いた「数の幾何（the geometry of numbers）」により解決した．特に後者では，“$\mathbf{N}(\alpha\mathcal{O}_K)$ と $\|\alpha\|_{\infty,\boldsymbol{\omega}}^n$ が近い” ような $\mathcal{O}_K^\times \curvearrowright \mathcal{O}_K \setminus \{0\}$ の基本領域を取ることができることを示した．このような集合を，**NLC**（Norm-Length-compatible）であると呼んでいる：詳細は [KMM$^+$20, Section 4, Section 8] を参照されたい．

参考文献

[BS20] Thomas F. Bloom and Olof Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, preprint, arXiv:2007.03528 (2020).

[CFZ15] David Conlon, Jacob Fox, and Yufei Zhao, *A relative Szemerédi theorem*, Geom. Funct. Anal. **25** (2015), no. 3, 733–762.

[FK78] H. Furstenberg and Y. Katznelson, *An ergodic Szemerédi theorem for commuting transformations*, J. Analyse Math. **34** (1978), 275–291 (1979).

[GT08] Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547.

[KMM$^+$20] Wataru Kai, Masato Mimura, Akihiro Munemasa, Shin ichiro Seki, and Kiyoto Yoshino, *Constellations in prime elements of number fields*, preprint:2012.15669v1 (2020).

[Sze75] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245. MR 369312

[Tao06] Terence Tao, *The Gaussian primes contain arbitrarily shaped constellations*, J. Anal. Math. **99** (2006), 109–176.

[関 21] 関真一朗, 数体の素元星座定理 *II,* 本「第 37 回代数的組合せ論シンポジウム報告集」, 2021.

数体の素元星座定理II

関 真一朗 （青山学院大学）

1 はじめに

筆者は第 37 回代数的組合せ論シンポジウムにおいて見村万佐人さんと [KMMSY] の研究成果に関する連続講演を行った (見村さんが I で筆者が II). この原稿は筆者が行った講演に基づく報告記事である.

Szemerédi は組合せ論と整数論に関する深い結果を有名な論文 [Sz1] で証明し, Szemerédi の定理ではカバーできなかった素数の場合を Green と Tao が証明した [GT]. 今回の研究はこれらの仕事の多次元版に関係する. Szemerédi の定理の多次元版は Furstenberg と Katznelson が証明した次の定理である.

定理 1.1 (多次元 Szemerédi の定理 [FK])**.** d を正整数とする. 上漸近密度が正であるような $\mathbb{Z}^d$ の部分集合は $\mathbb{Z}^d$ に対する任意の形状の星座を含む.

次数 d の数体の整数環は $\mathbb{Z}$ 加群としては $\mathbb{Z}^d$ と同型であるが, 素元全体の集合に対しては多次元 Szemerédi の定理を適用できない. 東北大学の研究チーム (Kai–Mimura–Munemasa–Seki–Yoshino) による共同研究により, 以下のように Green–Tao の定理が拡張された (筆者は当時東北大学に所属していた).

定理 1.2 (数体の素元星座定理 [KMMSY])**.** K を数体とし, $\mathcal{O}_K$ を K の整数環とする. このとき, $\mathcal{O}_K$ の素元全体の集合 $\mathcal{P}_K$ は $\mathcal{O}_K$ に対する任意の形状の星座を含む.

定理 1.1 の最初の証明はエルゴード理論によるものであったが, その後組合せ論的な証明が模索され, Solymosi [So] の着想に遡ることができるハイパーグラフ除去補題を使った証明が得られるに至った [G2, RSTT]. 定理 1.2 を証明する際には (幾分エルゴード理論的であった Green–Tao の証明とは異なる) この流れを相対化したもの (Tao [T2] および Conlon–Fox–Zhao [CFZ] による相対ハイパーグラフ除去補題と, それから導出される相対多次元 Szemerédi の定理) が用いられる. 相対多次元 Szemerédi の定理を応用して定理 1.2 を導く部分が数論的には大事であるが, 組合せ論の研究集会における得難い講演機会を頂けたので, 強力な組合せ論的ツールであるハイパーグラフ除去補題およびその相対化を以下の節で簡単にまとめたい. なお, 相対多次元 Szemerédi の定理の定式化は数種類知られており, 本稿では [KMMSY] による定式化を紹介する.

2　ハイパーグラフ除去補題

r を正整数とする. 有限集合 V に対して, $\binom{V}{r}$ を $\binom{V}{r} \coloneqq \{e \in \mathfrak{P}(V) : \#e = r\}$ で定義する ($\mathfrak{P}$ で冪集合を表す). このとき, V と $\binom{V}{r}$ の部分集合 $E \subset \binom{V}{r}$ の組 (V, E) のことを r ハイパーグラフとよぶ. 次がハイパーグラフ除去補題である.

定理 2.1 (ハイパーグラフ除去補題)**.** 正整数 k と正の実数 $\varepsilon > 0$ に対して $\delta = \delta_{\mathrm{HR}}(k, \varepsilon) > 0$ が存在して以下が成立する. H を頂点数 k の r ハイパーグラフとし ($r \in [k] \coloneqq \{1, 2, \ldots, k\}$), r ハイパーグラフ G を任意に考えて, その頂点数を n とおく. もし G が高々 δn^k 個しか H と同型な部分ハイパーグラフを含まなければ, 高々 εn^r 個の辺を除去することによって H と同型な部分ハイパーグラフを含まないような G の部分ハイパーグラフを得ることができる.

k, r を $r \in [k]$ を満たすような正整数とする. このとき, k 頂点完全 r ハイパーグラフ $K_k^{(r)} = (V, E)$ を $V = [k]$, $E = \binom{[k]}{r}$ によって定める. また, $K_k^{(2)} = K_k$ と略記する (k 頂点完全グラフ).

Ruzsa–Szemerédi [RuSz] が $H = K_3$ の場合を証明し, 今では三角形除去補題とよばれている (Ruzsa–Szemerédi が元々このような形で定式化していたわけではなく若干弱い version を示しており, このような名称で呼ばれるようになったのも 21 世紀に入ってからのようである). 証明は Szemerédi の有名な正則化補題 [Sz2] が鍵となるが, ハイパーグラフへ拡張することは容易でなく, その後の一般化に至るまでの歴史を簡単に述べると次のようになる (論文に実際に載っている定理の定式化はやはり異なったり若干弱くなっているが, H として何を扱ったに注目して紹介する. 定理 2.1 と同じ形で除去補題が登場したのは Alon 達の論文 [ADLRY](完全グラフの場合) や Füredi の論文 [F](一般のグラフの場合) であり, 定理 2.1 の形の一般のハイパーグラフ除去補題を問題にしたのは Rödl–Skokan [RoSk3] によれば Füredi とのことである).

Erdős–Frankl–Rödl [EFR] は完全グラフの除去補題を証明し, 完全 r ハイパーグラフについても同様のことが成り立つかという問題を提出した. その後, Füredi [F] が 1994 年に一般のグラフに対する除去補題を証明し, 世紀をまたいでハイパーグラフの時代に突入する. Frankl–Rödl [FR] は 2002 年に $K_4^{(3)}$ 除去補題を証明することによって長さ 4 の等差数列の場合の Szemerédi の定理を導出することに成功した. また, Erdős–Frankl–Rödl の「問題」を「予想」に格上げし, その予想から Szemerédi の定理を導出することができることを確認している. 実際は多次元 Szemerédi の定理まで導出することができるのであるが, それには Solymosi の慧眼が必要であった. なお, Gowers [G1] が Frankl–Rödl の定理の別証明を与えている. 続いて, Nagle–Rödl [NR] が一般の 3 ハイパーグラフの場合を証明し, Rödl–Skokan [RoSk2] が $K_5^{(4)}$ の場合を証明した. このような歴史を経て, 最終的にハイパーグラフ除去補題に到達したのが, Gowers [G2] および Nagle–Rödl–Schacht–Skokan [RoSk1, RoSk3, NRS, RoSc1, RoSc2] である. 論文毎に定理の記述や version が異なるが (Gowers [G2] および Nagle–Rödl–Skokan [NRS] では $K_{r+1}^{(r)}$ の場合が証明されており, 多次元 Szemrédi の定理を導出するにはこの場合で十分である), 定理 2.1 の形は [RoSk3, RoSc1] に現れる.

Tao [T1] は以下の形でハイパーグラフ除去補題の証明を短くまとめており, 次節の相対化はこの version を元に行われる. (J, E) が r ハイパーグラフで各 $j \in J$ に対して V_j が空

でない有限集合であるとき, $V=((J,E);(V_j)_{j\in J})$ を r ハイパーグラフ系とよぶ. J の部分集合 e に対して $V_e\coloneqq\prod_{j\in e}V_j$ と略記する.

定理 2.2. 正整数 k と正の実数 $\varepsilon>0$ に対して $\delta=\delta_{\mathrm{SHR}}(k,\varepsilon)>0$ が存在して以下が成立する. $((J,E);(V_j)_{j\in J})$ を $\#J=k$ であるような r ハイパーグラフ系 $(r\in[k])$ として, 各 $e\in E$ 毎に $E_e\subset V_e$ を考える. もし

$$\mathbb{E}\left(\prod_{e\in E}\mathbf{1}_{E_e\times V_{J\setminus e}}\;\middle|\;V_J\right)\leq\delta \tag{1}$$

が満たされるならば, ある $(E'_e)_{e\in E}\in\prod_{e\in E}\mathfrak{P}(V_e)$ が存在して,

$$\bigcap_{e\in E}(E'_e\times V_{J\setminus e})=\varnothing \tag{2}$$

かつ

$$\forall e\in E,\quad\mathbb{E}\left(\mathbf{1}_{E_e\setminus E'_e}\;\middle|\;V_e\right)\leq\varepsilon \tag{3}$$

が成り立つ.

ここで, $\varnothing\neq A\subset X$, $\#X<\infty$, $f\colon X\to\mathbb{R}$ に対して, $\mathbb{E}(f\mid A)=\frac{1}{\#A}\sum_{x\in A}f(x)$ であり, $\mathbf{1}_\bullet$ は指示関数を表す. 定理 2.2 から定理 2.1 を導出することができる.

3 相対ハイパーグラフ除去補題

定義 3.1. $V=((J,E);(V_j)_{j\in J})$ を r ハイパーグラフ系とする. g が V 上の重み付きハイパーグラフであるとは, g が関数 $g_e\colon V_e\to\mathbb{R}_{\geq0}$ の組 $g=(g_e)_{e\in E}$ であるときにいう.

g,g' を V 上の重み付きハイパーグラフとする. 任意の $e\in E$ に対して各点で $g_e\leq g'_e$ が成り立つとき, $g\leq g'$ と表す.

有限集合 e に対して, $\omega\in\{0,1\}^e$ が $\omega=(\omega_j)_{j\in e}$ と成分表示され, 各 $j\in e$ に対して $x_j^{(0)}$ および $x_j^{(1)}$ が定まっているとき, 記号 $x_e^{(\omega)}$ で $(x_j^{(\omega_j)})_{j\in e}$ を略記しているものと約束する. また, $(0)_{j\in e},(1)_{j\in e}\in\{0,1\}^e$ をそれぞれ $0,1$ と表すこととし, 従って今の記法から $x_e^{(0)}=(x_j^{(0)})_{j\in e}$, $x_e^{(1)}=(x_j^{(1)})_{j\in e}$ を意味しているということになる.

定義 3.2. $\rho>0$ を正の実数, $V=((J,E);(V_j)_{j\in J})$ を r ハイパーグラフ系 $(r\in\mathbb{Z}_{>0})$, $\nu=(\nu_e)_{e\in E}$ を V 上の重み付きハイパーグラフとする. また, $\mathrm{D}(E)\coloneqq\bigcup_{e\in E}\{0,1\}^e$ とおく. このとき, ν が ρ 擬ランダムであるとは, 任意の $(n_\omega)_{\omega\in\mathrm{D}(E)}\in\{0,1\}^{\mathrm{D}(E)}$ に対して

$$\left|\mathbb{E}\left(\prod_{e\in E}\prod_{\omega\in\{0,1\}^e}\nu_e(x_e^{(\omega)})^{n_\omega}\;\middle|\;(x_J^{(0)},x_J^{(1)})\in V_J\times V_J\right)-1\right|\leq\rho \tag{4}$$

が成り立つときにいう.

定理 2.2 は次のように一般化される.

定理 3.3 (相対ハイパーグラフ除去補題)**.** 正整数 k および正の実数 $\varepsilon > 0$ に対して $\delta = \delta_{\mathrm{RHR}}(k,\varepsilon) > 0$ および $\rho = \rho_{\mathrm{RHR}}(k,\varepsilon) > 0$ が存在して以下が成立する. $V = ((J,E);(V_j)_{j\in J})$ を $\#J = k$ であるような r ハイパーグラフ系 ($r \in [k]$) とする. ν を ρ 擬ランダムな V 上の重み付きハイパーグラフとし, g を $g \le \nu$ を満たすような V 上の重み付きハイパーグラフとする. もし

$$\mathbb{E}\left(\prod_{e\in E} g_e(x_e) \;\middle|\; x \in V_J\right) \le \delta \tag{5}$$

が満たされるならば, ある $(E'_e)_{e\in E} \in \prod_{e\in E} \mathfrak{P}(V_e)$ が存在して,

$$\bigcap_{e\in E} (E'_e \times V_{J\setminus e}) = \varnothing$$

かつ

$$\forall e \in E, \quad \mathbb{E}\left(g_e \cdot \mathbf{1}_{V_e\setminus E'_e} \mid V_e\right) \le \varepsilon \tag{6}$$

が成り立つ.

$\pi_e \colon V_J \to V_e$ を自然な全射とするとき, $x \in V_J$ に対して $x_e = \pi_e(x)$ と略記している. ν として $\nu_e = \mathbf{1}_{V_e}$ で定まるものを考えると自明に ρ 擬ランダムとなり, その場合が定理 2.2 と同値であることが確認される. この定理のプロトタイプを証明したのは Tao [T2] であり, 条件を緩めてこの version にしたのが Conlon–Fox–Zhao [CFZ] である (上の記述はオリジナルとは若干異なる定式化にはなっている). 証明には定理 2.2 を用いるが, 非自明な ν を構成することによって疎な集合に対する星座定理を証明できるようになる.

4 相対多次元 Szemerédi の定理

定義 4.1. d を正整数とし, S を 0 を含むような $\mathbb{Z}^d$ の有限部分集合とする. $r := \#S - 1 \ge 1$ とし, $S = \{s_1,\dots,s_r\} \cup \{0\}$ と元に名前を付けておく. $D_{r+1} := \bigcup_{i\in[r+1]} \{0,1\}^{[r+1]\setminus\{i\}}$ とおく. 各 $\omega \in \mathrm{D}_{r+1}$ に対して, $\mathbb{Z}$ 線形写像 $\psi_S^{(\omega)} \colon \mathbb{Z}^{2r+2} \to \mathbb{Z}^d$ を次のように定める: $i \in [r]$ で $\omega = (\omega_j)_{j\in[r+1]\setminus\{i\}} \in \{0,1\}^{[r+1]\setminus\{i\}}$ のときは

$$\psi_S^{(\omega)}(a_1^{(0)},\dots,a_{r+1}^{(0)},a_1^{(1)},\dots,a_{r+1}^{(1)}) := \left(\sum_{j\in[r]\setminus\{i\}} (s_j - s_i) a_j^{(\omega_j)}\right) + s_i a_{r+1}^{(\omega_{r+1})}$$

と定義し, $\omega = (\omega_i)_{i\in[r]}$ のときは

$$\psi_S^{(\omega)}(a_1^{(0)},\dots,a_{r+1}^{(0)},a_1^{(1)},\dots,a_{r+1}^{(1)}) := \sum_{j\in[r]} s_j a_j^{(\omega_j)}$$

と定義する. ρ を $0 < \rho < 1$ を満たす実数, N を正整数とする. このとき, 写像 $\lambda \colon \mathbb{Z}^d \to \mathbb{R}_{\ge 0}$ が (ρ,N,S)-擬ランダム測度であるとは, 元の個数が N 以上であるような整数の区間の直積として表される任意の $L \subset \mathbb{Z}^{r+1}$ および任意の $\Omega \subset \mathrm{D}_{r+1}$ に対して

$$\left|\mathbb{E}\left(\prod_{\omega\in\Omega} \lambda\circ\psi_S^{(\omega)} \;\middle|\; L\times L\right) - 1\right| \le \rho$$

が成り立つときにいう.

定義 4.2. d を正整数, S を $\mathbb{Z}^d$ の有限部分集合とする. $0 \in S$ および $S = -S$ が成り立っており, 更に S が $\mathbb{Z}^d$ を $\mathbb{Z}$ 加群として生成するとき, S を標準形状とよぶ.

$\mathbb{Z}^d$ の任意の有限部分集合に対してそれを含むような標準形状が存在するため, 任意の形状の星座の存在を証明したい場合には標準形状のみを扱えば十分であることに注意する.

定理 4.3 (相対多次元セメレディの定理)**.** d を正整数とし, $S \subset \mathbb{Z}^d$ を標準形状とし, $r \coloneqq \#S - 1 \geq d$ とおく. このとき, 任意の正の実数 $\delta > 0$ に対して正の実数 $\rho = \rho_{\mathrm{RMST}}(S, \delta)$ および $\gamma = \gamma_{\mathrm{RMST}}(S, \delta)$ が存在して以下が成立する. N を正整数, $\lambda\colon \mathbb{Z}^d \to \mathbb{R}_{\geq 0}$ を (ρ, N, S)-擬ランダム測度とする. 集合 $A \subset [-N, N]^d$ は次の 2 条件を満たすと仮定する:

1. (重み付き密度条件) $\mathbb{E}(\lambda \cdot \mathbf{1}_A \mid [-N, N]^d) \geq \delta$,
2. (Smallness 条件) $\mathbb{E}(\lambda^{r+1} \cdot \mathbf{1}_A \mid [-N, N]^d) \leq \gamma N$.

このとき, A は S 星座を含む.

自明な擬ランダム測度 $\lambda = \mathbf{1}_{\mathbb{Z}^d}$ に対してこの定理を適用すると, いわゆる「有限版」の多次元 Szemerédi の定理となり, 特に定理 1.1 が従う.

Solymosi の手法を応用することによって, 相対ハイパーグラフ除去補題から相対多次元 Szemerédi の定理を導出することができる. 定理 4.3 の λ と A に対して定理 3.3 の ν と g をどのように構成すればよいかをここに述べておこう.

$\mathbb{Z}$ 加群の全射準同型写像 $\phi_S\colon \mathbb{Z}^r \twoheadrightarrow \mathbb{Z}^d$ を各 $i \in [r]$ に対して $\phi_S(\epsilon_i) = s_i$ として定める ($(\epsilon_i)_{i\in[r]}$ は標準基底). このとき, S から定まる正整数 U が存在し, 任意の $a \in [-N, N]^d$ に対して

$$(2N+1)^{r-d} \leq \#(\phi_S^{-1}(a) \cap [-UN, UN]^r) \leq (2UN+1)^{r-d}$$

が成り立つ. 各 $j \in [r]$ に対し, V_j を $V_j \coloneqq \{H_j(a) : a \in [-UN, UN]\}$ と定義し, V_{r+1} を $V_{r+1} \coloneqq \{H_{r+1}(a) : a \in [-rUN, rUN]\}$ と定義する. ここで, $j \in [r]$ のときは $H_j(a) \coloneqq \{(x_i)_{i\in[r]} \in \mathbb{Z}^r : x_j = a\}$, $j = r+1$ のときは $H_{r+1}(a) \coloneqq \left\{(x_i)_{i\in[r]} \in \mathbb{Z}^r : \sum_{i\in[r]} x_i = a\right\}$ である. そうして, $V \coloneqq (K_{r+1}^{(r)}; (V_j)_{j\in[r+1]})$ と r ハイパーグラフ系を定める.

$i \in [r+1]$ 毎に $e_i \coloneqq [r+1] \setminus \{i\} \in \binom{[r+1]}{r}$ とおく. 超平面の組 $(H_j)_{j\in e_i} \in V_{e_i}$ をとるとき, 定義から $\bigcap_{j\in e_i} H_j$ は 1 点集合であることがわかる. この 1 点を取り出す写像を $T_i\colon V_{e_i} \to \mathbb{Z}^r$ と表すことにする. 写像 $\nu_{e_i}\colon V_{e_i} \to \mathbb{R}_{\geq 0}$ を合成

$$\nu_{e_i}\colon V_{e_i} \xrightarrow{T_i} \mathbb{Z}^r \xrightarrow{\phi_S} \mathbb{Z}^d \xrightarrow{\lambda} \mathbb{R}_{\geq 0}$$

によって定義する. こうして, V 上の重み付きハイパーグラフ $\nu = \nu(\lambda, N, S)$ が $\nu \coloneqq (\nu_{e_i})_{i\in[r+1]}$ によって構成できた. このとき, 次が証明される.

命題 4.4. λ が $0 < \rho < 1$ に対して (ρ, N, S)-擬ランダム測度であれば, V 上の重み付きハイパーグラフ ν は ρ 擬ランダムである.

次に, V 上の重み付きハイパーグラフ $g = (g_{e_i})_{i\in[r+1]}$ で $g \leq \nu$ を満たすようなものを, 各 $i \in [r+1]$ に対して $E_{e_i} \coloneqq (\phi_S \circ T_i)^{-1}(A)$ とし, $g_{e_i} \coloneqq \nu_{e_i} \cdot \mathbf{1}_{E_{e_i}}$ とすることで定める. こうして定まった g と ν に対して相対ハイパーグラフ除去補題を適用することによって相対多次元 Szemerédi の定理が導出される.

5　擬ランダム測度の構成

定理 1.2 は相対多次元 Szemerédi の定理を応用することによって証明されるが, 実際に擬ランダム測度を構成することは容易ではなく, Goldston–Yıldırım 型漸近公式と呼んでいる解析的整数論的な定理から最終的な帰結を得るまでには W-trick や鳩の巣原理に基づく counting の議論を組み込む必要がある. 論文 [KMMSY] では幾つかの種類の星座定理を導出することもあり, これらの議論をあらかじめ行いパッケージ化した定理を証明した. それを簡易化したものを次に記載する.

定理 5.1. K を次数 d の数体とし, $\mathbb{Z}$ 加群としての同型写像 $\mathcal{O}_K \xrightarrow{\sim} \mathbb{Z}^d$ を 1 つとって固定し, 同一視する. 集合 $A \subset \mathcal{O}_K$ に対して以下の性質が満たされていると仮定する: 任意の標準形状 $S \subset \mathcal{O}_K$ に対して $D_1, D_2 > 0$, $0 < \varepsilon < 1$ が存在して以下が成立する. 任意の $\rho > 0$ に対して或る $M_0 \in \mathbb{Z}_{>0}$ が存在して, 任意の $M \in \mathbb{Z}_{\geq M_0}$ に対して $W \leq M^{\varepsilon}$ を満たすような $W \in \mathbb{Z}_{>0}$ および写像 $\lambda\colon \mathcal{O}_K \to \mathbb{R}_{\geq 0}$ が存在して

1. W と互いに素な任意の $b \in \mathcal{O}_K$ に対して写像 $\mathcal{O}_K \to \mathbb{R}_{\geq 0}$; $\beta \mapsto \frac{\varphi_K(W)}{W^d} \cdot \lambda(W\beta + b)$ は $(\rho, \left\lceil \frac{M}{W} \right\rceil, S)$-疑ランダム測度であり ($\varphi_K$ は totient 関数),
2. ある $T \subset A \cap \mathcal{O}_K(M)$ が存在して $\#T \leq M^{\varepsilon n}$ であり, 任意の $\alpha \in (A \cap \mathcal{O}_K(M)) \setminus T$ に対して α は W と互いに素であり, $D_1 \cdot \log M \leq \lambda(\alpha) \leq D_2 \cdot \log M$ が成り立つ ($\mathcal{O}_K(M)$ は固定した同型によって $([-M, M] \cap \mathbb{Z})^d$ に対応する $\mathcal{O}_K$ の部分集合).

その上で,

$$\limsup_{M \to \infty} \frac{\#(A \cap \mathcal{O}_K(M))}{M^d (\log M)^{-1}} > 0$$

が満たされれば, A は $\mathcal{O}_K$ に対する任意の形状の星座を含む

さて, このややこしく見える条件を素元の集合 $\mathcal{P}_K$ が満たすことから定理 1.2 が得られるのであるが, 定理 5.1 における $\lambda\colon \mathcal{O}_K \to \mathbb{R}_{\geq 0}$ は

$$\lambda(\alpha) = \frac{\kappa \cdot \Lambda_{R,\chi}(\alpha)^2}{c_\chi \log R}$$

という形で選ばれる (κ は類数公式に由来する正定数, χ は或る滑らかな関数で c_χ はそれに付随する正定数, $R = M^{\frac{1}{17 \# S \cdot 2^{\# S - 1}}}$, $\Lambda_{R,\chi}$ は von Mangoldt 関数の変形版).

謝辞

講演の機会を与えて下さった宗政昭弘先生（東北大学）, 徳重典英先生（琉球大学）, 島倉裕樹先生（東北大学）, 野崎寛先生（愛知教育大学）, 三枝崎剛先生（早稲田大学）に心より感謝申し上げます.

参考文献

[ADLRY] N. Alon, R. A. Duke, H. Lefmann, V. Rödl, R. Yuster, *The algorithmic aspects of the regularity lemma*, J. Algorithms **16** (1994), 80–109.

[CFZ] D. Conlon, J. Fox, Y. Zhao, *A relative Szemerédi theorem*, Geom. Funct. Anal. **25** (2015), 733–762.

[EFR] P. Erdős, P. Frankl, V. Rödl, *The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent*, Graphs Combin. **2** (1986), 113–121.

[F] Z. Füredi, *Extremal hypergraphs and combinatorial geometry*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994), 1343–1352, Birkhäuser, Basel, 1995.

[FK] H. Furstenberg, Y. Katznelson, *An ergodic Szemerédi theorem for commuting transformations*, J. Analyse Math. **34** (1978), 275–291.

[FR] P. Frankl, V. Rödl, *Extremal problems on set systems*, Random Structures Algorithms **20** (2002), 131–164.

[G1] W.T. Gowers, *Quasirandomness, counting and regularity for* 3*-uniform hypergraphs*, Combin. Probab. Comput. **15** (2006), 143–184.

[G2] W. T. Gowers, *Hypergraph regularity and the multidimensional Szemerédi theorem*, Ann. of Math. **166** (2007), 897–946.

[GT] B. J. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. **167** (2008), 481–547.

[KMMSY] W. Kai, M. Mimura, A. Munemasa, S. Seki, K. Yoshino, *Constellations in prime elements of number fields*, preprint, arXiv:2012.15669.

[NR] B. Nagle, V. Rödl, *Regularity properties for triple systems*, Random Structures Algorithms **23** (2003), 264–332.

[NRS] B. Nagle, V. Rödl, M. Schacht, *The counting lemma for regular* k*-uniform hypergraphs*, Random Structures Algorithms **28** (2006), 113–179.

[RoSc1] V. Rödl, M. Schacht, *Regular partitions of hypergraphs: regularity lemmas*, Combin. Probab. Comput. **16** (2007), 833–885.

[RoSc2] V. Rödl, M. Schacht, *Regular partitions of hypergraphs: counting lemmas*, Combin. Probab. Comput. **16** (2007), 887–901.

[RoSk1] V. Rödl, J. Skokan, *Applications of the regularity lemma for k-uniform hypergraphs*, Random Structures Algorithms **25** (2004), 1–42.

[RoSk2] V. Rödl, J. Skokan, *Counting subgraphs in quasi-random 4-uniform hypergraphs*, Random Structures Algorithms **26** (2005), 160–203.

[RoSk3] V. Rödl, J. Skokan, *Applications of the regularity lemma for uniform hypergraphs*, Random Structures Algorithms **28** (2006), 180–194.

[RuSz] I. Z. Ruzsa, E. Szemerédi, *Triple systems with no six points carrying three triangles*, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, 939–945.

[RSTT] V. Rödl, M. Schacht, E. Tengan, N. Tokushige, *Density theorems and extremal hypergraph problems*, Israel J. Math. **152** (2006), 371–380.

[So] J. Solymosi, *Note on a generalization of Roth's theorem*, Discrete and Computational Geometry, 825–827, Algorithms Combin., **25**, Springer, Berlin, 2003.

[Sz1] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

[Sz2] E. Szemerédi, *Regular partitions of graphs*, Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), 399–401, Colloq. Internat. CNRS, 260, CNRS, Paris, 1978.

[T1] T. Tao, *A variant of the hypergraph removal lemma*, J. Combin. Theory Ser. A **113** (2006), 1257–1280.

[T2] T. Tao, *The Gaussian primes contain arbitrarily shaped constellations*, J. Anal. Math. **99** (2006), 109–176.

原始語予想に対する密度的アプローチ

新屋良磨

秋田大学
ryoma@math.akita-u.ac.jp

1　はじめに

原始語とは「自身より短い語の繰り返し」では表されない語 (文字の有限列) のことである (正確な定義は次節にて行う)．任意の語はある原始語の繰り返しとして一意に分解することができ，そういった意味で原始語は語の世界における素数のような対象であり，定義は単純であるが非常に奥深い性質を持っている．

形式言語理論においては「ある語の集合 (言語) が特定の言語族に属するかどうか?」といった種類の問題がしばしば興味の対象となる．ここでは「特定の言語族」とは計算論的あるいは代数的な特徴づけを持った言語族が主な興味の対象とされ，典型的な例としては Chomsky の階層における正規言語 (regular languages)，文脈自由言語 (context-free languages)，文脈依存言語 (context-sensitive languages) などの族が挙げられる．

本稿では

原始語全体の集合は文脈自由言語ではない

という原始語予想 (Dömösi-Horváth-Ito 1991 [2]∼) に対する著者のアプローチを紹介する．

2　正規言語と文脈自由言語

A を空でない有限集合とし，その元を文字と呼ぶ．A 上の文字の有限列（すなわち語）全体の集合を A^* で表し，長さが 0 の空列（空語）を ε で表す．

形式言語理論においては任意の語の集合 $L \subseteq A^*$ を言語と呼ぶ．言語は非可算無限個存在するが，その中でも特に方程式によって定義される言語が形式言語理論においては歴史的に良く研究されてきた．方程式によって定義される言語の例を見てみよう．

$$X = aX + Y \qquad Y = bY + \{\varepsilon\} \tag{1}$$

上の方程式では大文字 X, Y はそれぞれ言語を表す変数を，小文字 a, b はアルファベット $A = \{a, b\}$ の元 (すなわち文字) を，$+$ は集合和を，ε は長さ 0 の語 (空語) をそれぞれ表している．この方程式の読み方はこうである：

- $X = aX + Y$ は「X の元 w に対して左から a をつなげた語 aw も X の元になる」「Y の元は X の元でもある」
- $Y = bY + \{\varepsilon\}$ は「Y の元 w に対して左から b をくっつけた語 bw も Y の元になる」「ε は Y の元である」

をそれぞれ表している．これらの規則に従って X と Y それぞれに属すると言い切れるもの全体がすなわち X と Y の表している言語となる．方程式 (1) について，例えば $\varepsilon \in Y$ から $b\varepsilon = b \in Y$ が，また $b \in Y$ から $b \in X$ や $ab \in X$ などが成り立つことがわかる．要は方程式は言語の帰納的定義を与えており，方程式の解とは最小不動点を意味している．方程式 (1) の変数 X が表している言語を $L(X)$ と表すことにしよう．少し考えると $L(X)$ は「a が最初にいくつか続いた後，b がいくつか続くような語」全体の集合を表していることがわかるだろう：$L(X) = \{\varepsilon, a, b, aa, ab, bb, aaa, aab, \ldots\}$.

形式言語理論においては，一般の方程式というよりは，ある種の単純な方程式で記述できる言語クラスが主要な対象となる．その中でも特に深く研究されてきたのが**正規言語**と**文脈自由言語**である．

正規言語とは次の制約を満たす単純な方程式の解として表現できる言語のことを言う：

(1) 方程式の各等式の左辺は単独の変数.
(2) 各等式の右辺は wX(w は語で X は変数) という形の項と語の有限集合の有限和.

この制約を満たす方程式は XY のような 2 次以上の項を右辺に含まず，また wX のように右辺の変数を含む項は係数となる語 w(空語であっても良い) が必ず変数の左側に出現する．この制限 (1)–(2) を満たす方程式は**右線形方程式**と呼ばれる．例えば (1) の方程式は $X = aX + Y, Y = bY + \varepsilon$ と制約 (1)–(2) を満たしているため右線形であり，よってその解 $L(X) = \{\varepsilon, a, b, aa, ab, bb, aaa, aab, \ldots\}$. は正規言語である．一方，

$$P = aPa + bPb + \varepsilon + a + b \tag{2}$$

という 1 変数方程式は線形な方程式であるが，aPa という制約 (2) を満たしていない項を含むため右線形ではない．この方程式 (2) の解 $L(P)$ は回文，すなわち $abba$ のような「左から読んでも右から読んでも同じ語」全体の集合であることは容易に見て取れるだろう．

文脈自由言語とは制約 (1) を満たす方程式で記述できる言語のことを言う．すなわち等式の左辺が単独の変数であれば良く，右辺には何の制約もなく高次の項が出てきても良い (もちろん，有限和である必要はある)．例えば

$$Z = aZb + Z^2 + \varepsilon \tag{3}$$

の解は文脈自由言語である．この方程式は制約 (2) を 2 つの意味で破っている：右辺の aZb は b が変数 Z の右側に出現しており，$Z^2 = ZZ$ のような 2 次の項も含んでいる．方程式 (3) について，a を開きカッコ‘「’ で b を閉じカッコ‘」’ だと思おう．すると方程式 (3) から Z に属すと帰納的に示せる語は $abab$ (「」「」) や $aabb$(「「」」) のように「カッコの整合性が取れている語」しかない．例えば，方程式 (3) から $Z \supseteq aZb, Z \supseteq Z^2, Z \supseteq \{\varepsilon\}$ という 3 つの包含関係が得られるが，これを用いると

$$Z \supseteq ZZ \supseteq aZbZ \supseteq a\varepsilon bZ \supseteq a\varepsilon baZb \supseteq a\varepsilon ba\varepsilon b \tag{4}$$

という包含列が得られ，$a\varepsilon ba\varepsilon b = abab \in L(Z)$ であることが確かめられる．語の長さに対する帰納法で，逆側の包含も成り立つこと，すなわち解は「カッコの整合性が取れている語」全体の集合となることが示せる：$L(Z) = \{\varepsilon, ab, aabb, abab, aaabbb, aababb, \ldots\}$.

3　原始語と原始語予想

A^+ で空語以外の語全体の集合 $A^+ = A^* \setminus \{\varepsilon\}$ を表す．空語でない語 $w \in A^+$ が**原始語**であるとは，w よりも真に短い語の繰り返しとして w が表現できないことを言う：$u^n = w \Rightarrow u = w\,(n = 1)$．$A$ が 2 つ以上の文字を含む場合に，原始語全体の集合 $\mathrm{Q} = \{w \in A^+ \mid w \text{ は原始語 }\}$ が文脈自由言語ではない，というのが原始語予想である [2]．実は原始語予想は文字の種類が 2 文字だけ $A = \{a, b\}$ の場合に限定しても一般性を失わない．そのため以降は常に 2 文字上の原始語全体の集合

$$\mathrm{Q} = \{w \in \{a, b\}^+ \mid w \text{ は原始語 }\}$$

について考える．

簡単な考察から，語 w の長さがある素数 p となる場合は，$w = a^p$ や $w = b^p$ のように 1 文字の p 回の繰り返し (よって原始語ではない) であるか，それ以外は必ず原始語であることがわかる．有限集合 X の濃度を $\#(X)$ で表すことにする．言語 L について

$$F_L(n) = \#(L \cap A^n)$$

と定義すると，原始語の集合 Q について

$$F_{\mathrm{Q}}(n) \begin{cases} = 0 \text{ if } n = 0 \\ = 2 \text{ if } n = 1 \\ = 2^n - 2 \text{ if } n \text{ is prime} \\ < 2^n - 2 \text{ otherwise.} \end{cases}$$

が成り立つことが上記の考察から容易にわかる．すなわち Q は素数の情報を含んだ言語であり，そのような複雑な言語が「方程式で定義できる (=文脈自由である)」ほど単純であることはないだろう，というのが密度予想の 1 つの正当化である．原始語予想についてはこれまで様々なアプローチが試みられてきたが，それらはことごとく「上手く行きそうにはない」という否定的な結果が得られている．詳細は Dömösi-Ito による原始語予想のモノグラフを参照せよ [3]．

実は，Q が正規言語でないことは簡単に示すことができる．というのも，

1. 正規言語の補集合もまた正規言語である．
2. Q の補集合 $\overline{\mathrm{Q}}$（すなわち非原始語全体の集合）は「小さい」言語である．
3. 与えられた「小さい」言語が正規言語でないことは，多くの場合ポンピング補題と呼ばれる正規言語の必要条件を述べた補題を使って非正規性を示すことができる．実際，$\overline{\mathrm{Q}}$ が非正規であることもポンピング補題を用いて示すことができる．

という 3 つの事実から成り立つ．ここで「小さい」というのは次節で正式に定義される（密度が 0）が，ポンピング補題の言明やそれを用いた Q の非正規性の証明はモノグラフ [3] を参照せよ．しかし，このアプローチは文脈自由言語においては上手くいかない．というのも，ポンピング補題は文脈自由言語においても存在するが，文脈自由言語の補集合は一般に文脈自由言語にならないためである．よって，Q の補集合が文脈自由言語でないことは実際にポンピング補題によって示すことができるが，そこから Q 自体も文脈自由言語でないということが帰結できないのである．

4 密度と可測性

言語 $L \subseteq A^*$ の密度 $\delta_A(L)$ は

$$\delta_A(L) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \frac{\#\left(L \cap A^i\right)}{\#\left(A^i\right)} \tag{5}$$

で定まる 0 以上 1 以下の実数値である．定義 (5) 中の分数は長さ i で L に属する語の割合を表しており，その平均値の極限を取っているため密度は言語 L の「大きさ」とみなすことができる．例えば aA^* は「a で始まる語」全体の集合であるが，先頭の文字が a である確率も b である確率も等しいため $\delta_A(aA^*) = 1/\#\left(A\right)$ となる．言語によっては密度が定まらない ((5) が収束しない) ものもあるが，正規言語であれば必ず有理数に収束することが知られている [1].

前節で Q が「大きい」ということを述べたが，これは密度を用いて以下のように定式化することができる．証明も難しくないので説明しよう．

Theorem 1 ([4]). Q の密度は 1.

Proof. Q の補集合 $\overline{\mathrm{Q}}$ の密度が 0 になることを示せば良い．長さが $n \geq 1$ の語 $w \in A^+$ が非原始語であるとは，ある v と $m \geq 2$ が存在して $w = v^m$ となることであった．この場合 m は n の真の約数である必要があり，そのため m のあり得る組み合わせは高々$2\sqrt{n}$ 通りである．また，$|v| \leq n/2$ であることも容易にわかるため，v のあり得る組み合わせは高々$2^{n/2+1}$ 通りしかない ($A = \{a, b\}$ の場合を考えていることに注意)．よって各 $n \geq 1$ に対して $\#\left(\overline{Q} \cap A^n\right)$ の大雑把な見積もりとして $\#\left(\overline{Q} \cap A^n\right) \leq 2\sqrt{n} \cdot 2^{n/2+1}$ が得られる．すると長さ n の $\overline{Q}$ の要素の割合は

$$\frac{\#\left(\overline{Q} \cap A^n\right)}{2^n} \leq \frac{2\sqrt{n} \cdot 2^{n/2+1}}{2^n} \leq \frac{2\sqrt{n}}{2^{n/2-1}}$$

となり，これは $n \to \infty$ で 0 に収束する．よってその平均を取った $\delta_A(\overline{\mathrm{Q}})$ も 0 となる． □

可測性はこの密度を応用した概念である．言語 $L \subseteq A^*$ に対してその**正規下密度** $\underline{\mu}_A(L)$ と**正規上密度** $\overline{\mu}_A(L)$ をそれぞれ

$$\underline{\mu}_A(L) = \sup\{\delta_A(K) \mid K \text{ は正規言語かつ } K \subseteq L\}$$
$$\overline{\mu}_A(L) = \inf\{\delta_A(K) \mid K \text{ は正規言語かつ } K \supseteq L\}$$

と定義する．L が正規言語によって**可測**であるとは，$\underline{\mu}_A(L) = \overline{\mu}_A(L)$ が成り立つことを言う．直感的には $\underline{\mu}_A(L), \overline{\mu}_A(L)$ はそれぞれ正規言語によって L を内側・外側から**近似**したときの最大・最小の密度を表しており，L が正規言語によって可測であるとは，正規言語でいくらでも近似できる程度に「単純な形」をしていることを意味する．μ_A は加法的測度ではあるが可算加法性は満たさない．例えば $\sum_{w\in A^*} \mu_A(\{w\}) = 0 \neq 1 = \mu_A(\bigcup_{w\in A^*}\{w\}) = \mu_A(A^*)$ が成り立つ (任意の有限集合 $L \subseteq A^*$ は正規言語でありかつ $\delta_A(L) = 0$ が成り立つため)．そのため測度論で通常扱う可算加法測度とは毛色がことなるが，ここで定義した可測性はカラテ

オドリ拡張でも特徴付けを与えることができ [5]，その意味で測度論的に自然な概念と言える．

言語 L が密度を持つ場合は定義より明らかに $\underline{\mu}_A(L) \leq \delta_A(L) \leq \overline{\mu}_A(L)$ が成り立つが，この差分 $\overline{\mu}_A(L) - \underline{\mu}_A(L)$ を L の**ギャップ**と呼ぶことにしよう．L のギャップが 0 とは可測ということであり，逆にギャップが 1 というのは L が強い意味で非可測ということを意味している．すなわちギャップは言語の「形の複雑さ」を表す実数値と思ってよい．

著者は [4] で

1. Q の密度が 1 である (定理 1) 一方，
2. 任意の $L \subseteq \mathrm{Q}$ なる正規言語 L の密度が 0 になる

ということを示した．(1) と (2) から Q のギャップが 1 になることがわかる．すなわち Q は非常に「複雑な形」をしており，正規言語によって下から全く近似ができず，強い意味で非可測なのである．前述したとおり (1) は素朴に示せるが，(2) の証明は統語モノイドの解析 (特に半群論の基本的な結果である **Green の定理**を用いる) に基づいている．

著者はもともとギャップが 1 になる文脈自由言語は存在しない (よって原始語予想は正しい) と考え可測性という概念を導入した．実際，多くの複雑な文脈自由言語が可測であることが示せたが，ギャップが 1 になる文脈自由言語が存在することもわかった [4]．そのため正規言語による可測性では原始語予想を解決するには至らなかったが，より一般的な言語クラスによる可測性を考えればまだ可能性があるかもしれない．例えば上密度と下密度の言語の動く範囲を文脈自由言語全体にすれば，文脈自由言語による可測性が自然に得られる．任意の密度 1 な文脈自由言語は定義より文脈自由言語によって可測であるが，果たして Q は文脈自由言語によって可測であろうか？これはまだ未解決であり，今後の研究課題である．

References

1. Berstel, J.: Sur la densité asymptotique de langages formels, *International Colloquium on Automata, Languages and Programming (ICALP, 1972)*, France, North-Holland, 1973, pp. 345–358.
2. Dömösi, P., Horváth, S., and Ito, M.: On the connection between formal languages and primitive words, 1991, pp. 59–67.
3. Domosi, P., Horváth, S., and Ito, M.: *Context-Free Languages and Primitive Words*, World Scientific Publishing Company Pte Limited, 2014.
4. Sin'ya, R.: Asymptotic Approximation by Regular Languages, Proceedings of the 47th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'21), 2021, pp. 74–88.
5. Sin'ya, R.: Carathéodory Extensions of Subclasses of Regular Languages, Proceedings of the 25th International Conference on Developments in Language Theory (DLT'21), 2021, pp. 355–367.

正則グラフにおける non-backtracking cycle の個数の誤差項

齋藤　正顕　(工学院大学　教育推進機構)*

概　　要

$(q+1)$-正則グラフの長さ m の non-backtracking cycle の個数 N_m について, 絶対値が $2\sqrt{q}$ 未満の (隣接行列の) 固有値が寄与している項 t_m を考える (ここでは N_m の誤差項とよぶ). 本研究では, データ t_m $(m=1,2,\dots)$ の分布について調べ, そのモーメント母関数を与えた. また, これを応用して, 正則グラフの増大列がある条件をみたすとき, $t_m/\sqrt{n}$ (n は絶対値が $2\sqrt{q}$ 未満の固有値の個数) の極限分布が正規分布となることを示した.

1. Non-backtracking cycle の個数

$G=(V,E)$ を有限単純[1]連結グラフとし, V をその頂点集合, E を辺集合とする. G の隣接する 2 つの頂点 $v,w\in V$ に対し, $vw=wv\in E$ を v, w を端点とする (無向) 辺とし, v を始点, w を終点とする有向辺を (v,w) と表す. $e:=(v,w)$ の逆向きの有向辺を $\overline{e}:=(w,v)$ とする. $D(G):=\{(v,w),(w,v)\mid vw\in E\}$ を有向辺の全体とする. G の有向辺 $e\in D(G)$ に対し, a の始点と終点をそれぞれ $o(e)$, $t(e)$ とおく. G の長さ m の路 (path) $C=e_1\cdots e_m$ とは $e_1,\dots e_m\in D(G)$ かつ $t(e_i)=o(e_{i+1})$ $(i=1,\dots,m-1)$ のときをいう. とくに, $t(e_m)=o(e_1)$ のとき, C は閉路 (closed path) あるいはサイクル (cycle) といわれる. 本稿では, グラフ G のサイクル $C=e_1\cdots e_m$ が以下の条件を満たすとき, non-backtracking cycle とよぶ:

- $e_{i+1}\neq\overline{e}_i$, $(i=1,\dots,m-1)$. つまり, C には後戻りがない.
- $e_1\neq\overline{e}_m$. つまり C の最初の辺が最後の辺の逆になっていない.

自然数 m に対し, N_m を G の長さ m の non-backtracking cycle の個数とする. N_m の母関数

$$Z_G(u)=\exp\left(\sum_{m\geq1}\frac{N_m}{m}u^m\right)$$

はグラフ G の伊原ゼータ関数 [4] とよばれ, とくに G が $(q+1)$-正則グラフのときは,

$$Z_G(u)=\frac{1}{(1-u^2)^{(q-1)n/2}\det(I_n-Au+qu^2)}.$$

(伊原の公式) が成り立つ. ここに, A は G の隣接行列である. 以降, 本稿では G は $(q+1)$-正則グラフを仮定する.

本研究は科研費 (基盤研究 (C) :19K03608) の助成を受けたものである. また本研究は, 長谷川武博氏 (滋賀大学), 西郷甲矢人氏 (長浜バイオ大学), 杉山真吾氏 (日本大学), 谷口哲也氏 (金沢工業大学) との共同研究に基づく.

* e-mail: saito.seiken@cc.kogakuin.ac.jp

[1] 本稿では簡単のため単純グラフを仮定するが, 単純でないグラフについても同様の結果が成り立つ.

2. 正則グラフの跡公式と隣接行列の固有値の分布

N_m は G の隣接行列 A の固有値と以下の等式で結びついている.

Proposition 1 (G. Ahumada '87[1], R. Brooks '91[2], P. Mnëv '07 [6]) G を n 頂点からなる $(q+1)$-正則グラフとし, A をその隣接行列とするとき,

$$\sum_{\lambda\in \mathrm{Spec}(A)} e^{\lambda t} = n\,\frac{q+1}{2\pi}\int_{-2\sqrt{q}}^{2\sqrt{q}} \frac{\sqrt{4q-x^2}}{(q+1)^2-x^2}\cdot e^{xt}\,dx + \sum_{m\geq 1} N_m\, q^{-m/2}\, I_m(2\sqrt{q}t) \qquad (1)$$

が成り立つ. ここで, $\mathrm{Spec}(A)$ は A の固有値の重複度も含めた multiset, $I_m(t)$ は第 1 種変形ベッセル関数とする:

$$I_m(t) := \sum_{\ell\geq 0} \frac{(t/2)^{m+2\ell}}{\Gamma(\ell+1)\Gamma(\ell+m+1)}.$$

Example 1 図 1 のような 10 頂点の 3-正則グラフについて跡公式を確認してみる. N_m を求めるために, 伊原の公式からゼータ関数を計算し, その対数微分をとる.

$$\begin{aligned}\frac{1}{Z_G} &= \left(1-u^2\right)^4\left(1+4\,u^2-4\,u^3+6\,u^4-24\,u^5-4\,u^6-76\,u^7-23\,u^8-152\,u^9\right.\\ &\qquad \left.-16\,u^{10}-192\,u^{11}+96\,u^{12}-128\,u^{13}+256\,u^{14}+256\,u^{16}\right),\\ \sum_{m\geq 1} N_m u^m &= u\frac{Z_G'}{Z_G}\\ &= 12\,u^3+16\,u^4+40\,u^5+96\,u^6+140\,u^7+208\,u^8+552\,u^9+1120\,u^{10}+\cdots.\end{aligned}$$

数式処理ソフト Maple で A の固有値を求めると, 跡公式の左辺は

$$\sum_{\lambda\in \mathrm{Spec}(A)} e^{\lambda} = 30.97135041\ldots.$$

である. 一方, 右辺を I_{10} の項まで計算すると

$$\begin{aligned}&10\cdot\frac{3}{2\pi}\int_{-2\sqrt{2}}^{2\sqrt{2}}\frac{\sqrt{8-x^2}}{9-x^2}\cdot e^x\,dx + \frac{12}{2^{3/2}}I_3(2\sqrt{2}) + \frac{16}{2^{4/2}}I_4(2\sqrt{2}) + \cdots + \frac{1120}{2^{10/2}}I_{10}(2\sqrt{2})\\ &= 30.97128542\ldots.\end{aligned}$$

となる. 有限で打ち切らなければ左辺と一致しそうだということが実感できる.

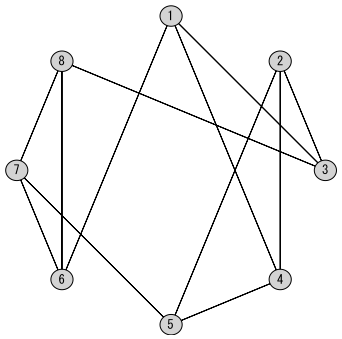


図 1: 10 頂点の 3-正則グラフ

跡公式から正則木に収束するような正則グラフの無限列の固有値の分布に関する次の結果がいえる:

Proposition 2 (B. D. McKay [5]) 有限 $(q+1)$-正則グラフの無限列 $\{G_n\}_{n\geq 1}$ が $(q+1)$-正則木 T_{q+1} に収束するとする. つまり, $G_n \to T_{q+1}$ $(n\to\infty)$ とする. A_n を G_n の隣接行列とする. このとき,

$$\lim_{n\to\infty}\frac{1}{n}\sum_{\lambda\in \mathrm{Spec}(A)} f(\lambda) = \frac{q+1}{2\pi}\int_{-2\sqrt{q}}^{2\sqrt{q}} \frac{\sqrt{4q-x^2}}{(q+1)^2-x^2}\cdot f(x)\,dx$$

が成り立つ. ここで, $f(x)$ は $[-q-1, q+1]$ 上の連続関数とする.

上記の結果は, G_n の隣接行列の固有値の極限分布が Kesten-McKay 分布とよばれる分布であることを述べている. つまり巨大な $(q+1)$-正則グラフの固有値の分布は Kesten-McKay に近い形状をしている. 図 2 はその例である.

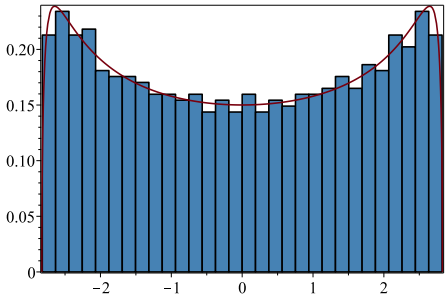


図 2: 1000 頂点, 3-正則 Ramanujan グラフの固有値の分布

Kesten-McKay 分布は次式によって台が $[-2,2]$ の確率密度関数に書きかえると, 異なるパラメータ q の分布の形状が比較しやすい. とくに $q+1=2$ のときは逆正弦則, $q+1=\infty$ のときは Wigner の半円則とよばれる.

$$\frac{q+1}{2\pi}\int_{-2\sqrt{q}}^{2\sqrt{q}} \frac{\sqrt{4q-x^2}}{(q+1)^2-x^2}\cdot f(x)\,dx = \frac{q(q+1)}{2\pi}\int_{-2}^{2} \frac{\sqrt{4-y^2}}{(q+1)^2-qy^2}\cdot f(\sqrt{q}y)\,dy.$$

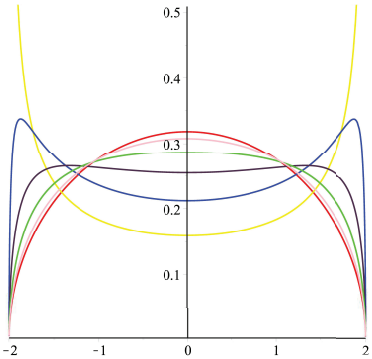


図 3: Kesten-McKay 分布の比較 $(q+1=2,3,5,10,30,\infty)$

3. Non-backtracking cycle の個数の誤差項

$(q+1)$-正則グラフ G に対し, N_m は A の固有値よって次のように表される ([3]).

$$N_m = 2q^{m/2} \sum_{\lambda \in \mathrm{Spec}(A)} T_m\left(\frac{\lambda}{2\sqrt{q}}\right) + ne_m(q-1).$$

ここで, T_m は第1種チェビシェフ多項式 (つまり $T_m(\cos\theta) = \cos m\theta$) とし, e_m は m が偶数のときは 1, それ以外のときは 0 と定義する. このとき, N_m について, 絶対値が $2\sqrt{q}$ より小さい A の固有値の寄与を t_m で表す.

$$t_m := \frac{1}{2q^{m/2}}\{N_m - 2q^{m/2} \sum_{\substack{l \in \sigma(A) \\ |\lambda| \geq 2\sqrt{q}}} T_m\left(\frac{\lambda}{2\sqrt{q}}\right) m_\lambda - n(q-1)e_m\}$$

$$= \sum_{i=1}^{l} T_m\left(\frac{\lambda_i}{2\sqrt{q}}\right) m_{\lambda_i} = \sum_{i=1}^{l} m_{\lambda_i} \cos m\theta_i.$$

ここで, $\sigma(A)$ は G の隣接行列 A の相異なる固有値全体の集合, $\{\lambda_1, \ldots, \lambda_l\} := \{\lambda \in \sigma(A) \mid |\lambda| < 2\sqrt{q}\}$, m_λ は A の固有値 λ の重複度とする.

特に, G が $|\lambda| = 2\sqrt{q}$ なる固有値 λ をもたない $(q+1)$-正則 Ramanujan グラフのときは,

$$t_m = \frac{1}{2q^{m/2}}\{N_m - n(q-1)e_m\}$$

である.

我々は, N_m の（主要部でないという意味での）“誤差項” t_m の分布について調べた.

Example 2 (数値実験と統計的分析) 以下のような 18 頂点の 3-正則グラフについて t_m $(m \leq 10000)$ の分布は図のようなヒストグラムになる (階級の個数=30).

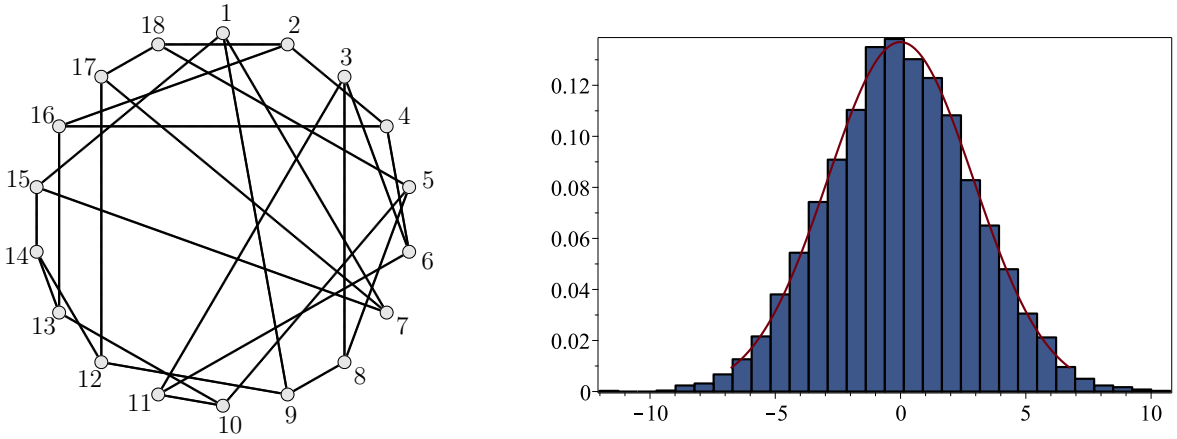


図 4: t_m $(m \leq 10000)$ の分布と $N(\mu, \sigma^2)$

データ $(t_m)_{1 \leq m \leq 10^4}$ の平均は $\mu = -0.00049429...$, 標準偏差は $\sigma = 2.9134...$ である. 帰無仮説「H_0: t_m は正規分布 $N(\mu, \sigma^2)$ に従う」のもとで適合度検定 (自由度 29 の χ^2-検定) をすると, p-値 $= 0.43020... > \alpha = 0.05$ (有意水準) である. よって帰無仮説は棄却されず採択される.

t_m の分布が正規分布に従うように見えることは, 中心極限定理の観点から解釈できる.

$$X_1 := (T_m\left(\frac{\lambda_1}{2\sqrt{q}}\right))_m, \quad \ldots, \quad X_l := (T_m\left(\frac{\lambda_l}{2\sqrt{q}}\right))_m$$

とおくと $(t_m)_m = X_1 + \cdots + X_l$ である. G_n を正則木 T_{q+1} に収束する $(q+1)$-正則グラフの無限列とする.

- $n \to \infty$ のとき, 正則グラフの固有値の極限分布は Kesten-McKay 分布だから, $X_1, \ldots, X_l$ は同じ分布 (逆正弦則) に従う.
- 重複度 m_λ が「全て 1」 で $X_1, \ldots, X_l$ が確率変数として「独立ならば」中心極限定理より $\dfrac{t_m}{\sqrt{l}}$ の極限分布は正規分布である.

実際には, G がループを持たないとき, 全ての固有値の和は 0 だから $X_1, \ldots, X_l$ の間にも代数的な関係がある (独立ではない). よって厳密には, 中心極限定理を使うことはできない.

Theorem 1 (主結果 1: グラフの増大列における $\frac{t_m}{\sqrt{n_\nu}}$ の極限分布) $(G_\nu)_{\nu \in \mathbf{Z}_{\geq 1}}$ を $(q+1)$-正則グラフの列とし, A_ν を G_ν の隣接行列とする.

$$\begin{aligned} \{\lambda_1, \ldots, \lambda_{l_\nu}\} &:= \{\lambda \in \sigma(A_\nu) \mid |\lambda| < 2\sqrt{q}\}, \\ \theta_i &:= \arccos \tfrac{\lambda_i}{2\sqrt{q}} \in (0, \pi) \quad (i = 1, \ldots, l_\nu), \\ n_\nu &:= |\{\lambda \in \mathrm{Spec}(A_\nu) \mid |\lambda| < 2\sqrt{q}\}| \end{aligned}$$

とおく. 以下を仮定する. $\lim_{\nu \to \infty} n_\nu = \infty$ かつ

$$(*)_\nu \qquad \text{各 } \nu \text{ について } \tfrac{\theta_1}{2\pi}, \ \ldots, \ \tfrac{\theta_{l_\nu}}{2\pi} \text{ は } \mathbf{Q} \text{ 上 1 次独立.}$$

このとき, $\frac{1}{\sqrt{n_\nu}} t_m$ $(m \in \mathbf{Z}_{\geq 1})$ の極限分布は平均が 0, 分散が $1/2$ の正規分布 $N(0, 1/2)$ である.

Theorem 1 は, 後述の Corollary 1 から得られる. 中心極限定理の観点から, Example 2 のグラフについて, データの和 $X_1 + \cdots + X_k$ の分布を k をいろいろと変えて観察する.

Example 3 (18 頂点の 3-正則 Ramanujan グラフ) Example 2 の 3-正則 Ramanujan グラフについて, 非自明な固有値を大きさの順に $\lambda_1 > \cdots > \lambda_{17}$ とする. データ $\sum_{j=1}^{k} T_m\left(\frac{\lambda_j}{2\sqrt{q}}\right)$ $(m \leq 10000)$ の分布を $k = 1, \ldots, 5$ について (上段左から順に) 図示したものが図 3 の 5 つのヒストグラムである. また, 曲線はデータの平均 μ と標準偏差 σ で与えられる正規分布 $N(\mu, \sigma^2)$ である. $k = 1, 2, 3, 4$ のときは有意水準 5%の適合度検定で, 帰無仮説が棄却されるが, $k = 5$ になると採択される.

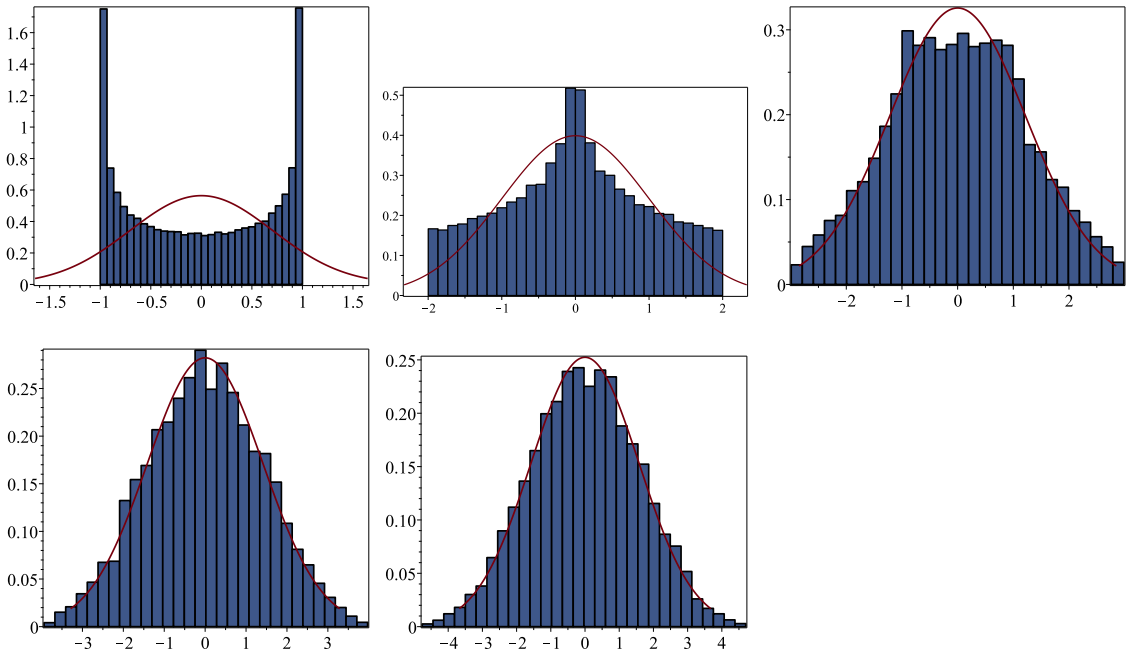


図 5: $\sum_{j=1}^{k} T_m\left(\frac{\lambda_j}{2\sqrt{q}}\right)$ $(m \leq 10000)$ の分布 $(k = 1, 2, 3, 4, 5)$

上記 Example 3 は以下の Theorem 2 の例である:

Theorem 2 (主結果 2: t_m の分布は逆正弦則の畳み込み) G を $(q+1)$-正則グラフとし, $\{\lambda_1, \ldots, \lambda_l\} := \{\lambda \in \sigma(A) \mid |\lambda| < 2\sqrt{q}\}$, $\theta_i := \arccos \frac{\lambda_i}{2\sqrt{q}} \in (0, \pi)$ $(i = 1, \ldots, l)$ とおく. t_m の d 次モーメントを M_d, モーメント母関数を $\varphi(x) := \sum_{d=0}^{\infty} \frac{M_d}{d!} x^d$ とすると,

$$\varphi(x) = \sum_{\substack{k_1, \ldots, k_l \in \mathbf{Z} \\ \sum_{h=1}^{l} k_h \theta_h \in 2\pi\mathbf{Z}}} \prod_{h=1}^{l} I_{k_h}(m_{\lambda_h} x). \tag{2}$$

Corollary 1

$$(*) \quad \frac{\theta_1}{2\pi}, \ \ldots, \ \frac{\theta_l}{2\pi} \text{ が } \mathbf{Q} \text{ 上 1 次独立ならば,}$$

$$\varphi(x) = \prod_{k=1}^{l} I_0(m_{\lambda_k} x).$$

謝辞

代数的組合せ論シンポジウムにて発表の機会を与えていただいた世話人の方々並びに関係者の方々に深く御礼申し上げます.

参考文献

[1] G. Ahumada, Fonctions périodiques et formule des traces de Selberg sur les arbres, C. R. Acad. Sci. Parris Ser. I 305, no. 16 (1987), 709–712.

[2] R. Brooks, The spectral geometry of k-regular graphs. J. Anal. Math. 57 (1991), 120–151.

[3] T. Hasegawa, T. Komatsu, N. Konno, H. Saigo, S. Saito, I. Sato and S. Sugiyama, The limit theorem with respect to the matrices on non-backtracking paths of a graph, arXiv:2005.09341v2 [math.CO], Sun, 22 Aug 2021.

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

[5] B. D. McKay, The expected eigenvalue distribution of a large regular graph, Linear Algebra Appl. 40 (1981), 203–216.

[6] A. Mnëv, Discrete path integral approach to the Selberg trace formula for regular graphs, Comm. in Math. Phys., 274 (2007), no.1, 233–241.

有限群から得られる等質カンドルについて

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 *
kurihara@kct.ac.jp†

1　序

今回の講演および報告集の内容は東谷 章弘氏（大阪大学）との共同研究に基づくものである。

カンドルの概念は元々 Joyce [4] によって結び目理論の文脈から導入された。集合 Q と Q 上の二項演算 $*\colon Q\times Q\to Q$ の組 $(Q,*)$ が**カンドル**とは以下の条件を満たすことである：

(Q1) $x*x=x$ for $\forall x\in Q$;

(Q2) for $\forall x,y\in Q$, $\exists! z\in Q$ such that $z*y=x$;

(Q3) for $\forall x,y,z\in Q$, $(x*y)*z=(x*z)*(y*z)$.

上記の 3 つの公理は結び目理論における Reidemeister 変形にそれぞれ対応する。一方でこの公理を対称空間論の類似としてとらえなおすこともできる。$(Q,*)$ をカンドルとするとき、$x\in Q$ における**点対称** $s_x:Q\to Q$ を $s_x(y)=y*x$ により定める。すると (Q1)∼(Q3) は以下のように言い直すことができる：

(Q1') $s_x(x)=x$ for $\forall x\in Q$;

(Q2') for $\forall x\in Q$, s_x は Q 上の全単射写像;

(Q3') $s_x\circ s_y=s_{s_x(y)}\circ s_x$ for $\forall x,y\in Q$.

対称空間は (Q1')∼(Q3') を満たすことが知られているので、対称空間はカンドルである (cf. [4])。対称空間論の立場からのカンドルの研究も多く

*2021 年 10 月 1 日からの所属は山口大学大学院創成科学研究科
†2021 年 10 月 1 日からのメールアドレスは kurihara-hiro@yamaguchi-u.ac.jp

あり (例えば [3, 5, 8] など)、これらの研究では特に**等質カンドル**が主な研究対象である。等質カンドルの定義や性質は 3 節で扱う。

カンドルは特別な二項演算をもつ集合であり、同じ二項演算をもつ群と似た性質もあればそうでない場合もある。この報告集では、特に群に “近い” 性質をもつ一般化 Alexander カンドルについて、様々な性質を調べた結果を記載する。一般化 Alexander カンドルは群 G と G の自己同型写像 ψ の組 (G, ψ) から得られる (定義は 3.2 節で与える)。一般化 Alexander カンドルについての大きな問題として、問 3.3 が考えられる。この問いに関して、一般化 Alexander カンドルの様々な不変量を考えることで部分的な解決を与えた。特に Higashitani–Kurihara [2] において、群が対称群の場合に問 3.3 の部分的な解決を与えた。さらに [2] の後続の共同研究として、新たな不変量を導入して、より多くの群に対して、問 3.3 の部分的な解決を与えた。

この報告集の内容は 4 節までが [2] の内容である。そして 5 節で最近得られた内容を紹介する。

2　準備

以降では、カンドルの演算 $*$ の代わりに点対称の記号 s を用いて、カンドルを (Q, s) のように表す。また点対称 s を省略して、カンドルを単に Q と書くこともある。

2.1　カンドルの定義や性質

(Q, s) と (Q', s') をカンドルとする。写像 $f : Q \to Q'$ が以下の条件を満たすとき、f を**カンドル準同型写像**と呼ぶ：

$$f \circ s_x = s'_{f(x)} \circ f \quad \text{for any } x \in Q.$$

さらにカンドル準同型 f が全単射であるとき、f を**カンドル同型写像**と呼ぶ。もし Q と Q' の間にカンドル同型写像が存在するとき、Q と Q' は**カンドル同型**であるといい、$Q \cong_{\mathrm{qu}} Q'$ で表す。$\mathrm{Aut}(Q, s)$ (もしくは単に $\mathrm{Aut}(Q)$) を (Q, s) 上のカンドル自己同型写像の集合とし、これを (Q, s) の**カンドル自己同型群**と呼ぶ。カンドルの公理 (Q3') から $s_x \in \mathrm{Aut}(Q)$ であることがわかる。$\mathrm{Inn}(Q, s)$ (もしくは単に $\mathrm{Inn}(Q)$) を $\{s_x : x \in Q\}$ で生成される $\mathrm{Aut}(Q)$ の部分群とし、これを (Q, s) の**カンドル内部自己同型群**と呼ぶ。

2.2 群の記号の準備

G を単位元 e をもつ群とする。$\mathrm{Aut}(G)$ を G の自己同型群とする。2 つの群 G, G' が同型のとき、$G \cong_{\mathrm{gr}} G'$ で表す。

$g, h \in G$ に対して、$g^h = hgh^{-1}$ と書くことにする。$\mathrm{Inn}(G)$ を G の内部自己同型群とする。$\psi \in \mathrm{Aut}(G)$ が**外部自己同型写像**とは、$\psi \notin \mathrm{Inn}(G)$ であることとする。

$\psi \in \mathrm{Aut}(G)$ に対して、

$$\mathrm{Fix}(\psi, G) = \{g \in G : \psi(g) = g\}$$

とおく。なお、$\mathrm{Fix}(\psi, G)$ は G の部分群であり、ψ が内部自己同型、つまり $\psi = (\cdot)^g$ と書けるときには、$\mathrm{Fix}((\cdot)^g, G)$ は g の中心化群 $C_G(g)$ と一致する。

3 等質カンドル

3.1 等質カンドルとカンドル三つ組

Q をカンドルとする。Q に $\mathrm{Aut}(Q)$ が推移的に作用するとき、Q を**等質**であるという。

定義 3.1 ([3, Definition 3.1])**.** G を群として、K を G の部分群とする。また $\psi \in \mathrm{Aut}(G)$ とする。これらが $K \subset \mathrm{Fix}(\psi, G)$ を満たすとき、三つ組 (G, K, ψ) をカンドル三つ組と呼ぶ。

等質カンドル (Q, s) からカンドル三つ組を得ることができる。$G = \mathrm{Aut}(Q, s)$ とし、$x \in Q$ を一つ固定して $K = \{f \in \mathrm{Aut}(Q, s) : f(x) = x\}$ とおく。さらに $\psi : G \to G$ を $f \mapsto s_x \circ f \circ s_x^{-1}$ で定めると、(G, K, ψ) はカンドル三つ組になる。上記の証明は例えば [3, Proposition 3.3] などを参考にしていただきたい。

逆にカンドル三つ組 (G, K, ψ) から以下のようにして等質カンドルを得ることができる：$G/K = \{[g] : g \in G\}$ を G の K による左剰余空間を表すことにして、G/K 上に点対称を

$$s_{[g]}([h]) := [g\psi(g^{-1}h)] \quad ([g], [h] \in G/K)$$

によって定めるとこれは well-defined であり、カンドルの公理を満たす。さらにこのカンドル $(G/K, s)$ は等質である。上記の証明は例えば [3, Proposition 3.2] などを参考にしていただきたい。今後このカンドルを $Q(G, K, \psi)$ で表すことにする。

3.2 一般化 Alexander カンドル

カンドル三つ組の K を $\{e\}$ として取ると、どのような G と ψ に対しても、$(G, \{e\}, \psi)$ は必ずカンドル三つ組になる。これから得られる等質カンドルは $Q = G$ であり、点対称は

$$s_g(h) = g\psi(g^{-1}h) \quad \text{for any } g, h \in G$$

となる。このカンドルを**一般化** *Alexander* **カンドル**と呼び、$Q(G, \psi)$ で表す。なお G がアーベル群のとき、Alexander カンドルと呼ばれている。

等質カンドルの研究には、以下の命題から一般化 Alexander カンドルを調べることが重要であると思われる。

命題 3.2 (Higashitani–K. [2])**.** $\psi, \psi' \in \mathrm{Aut}(G)$ とし、$K = \mathrm{Fix}(\psi, G)$、$K' = \mathrm{Fix}(\psi', G)$ とする。もし $Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ ならば、$Q(G, K, \psi) \cong_{\mathrm{qu}} Q(G, K', \psi')$ である。

証明は [2] を参考にされたい。

有限群 G に対して、$\mathcal{Q}(G)$ を $Q(G, \psi)$ の同型類の集合とする。つまり、

$$\mathcal{Q}(G) := \{Q(G, \psi) : \psi \in \mathrm{Aut}(G)\}/\cong_{\mathrm{qu}}$$

とする。以下の問題がこの報告集の主題である。

問題 3.3. 与えられた G に対して、$\mathcal{Q}(G)$ を決定せよ。

以下の命題は $\mathcal{Q}(G)$ を大雑把に把握するのに役に立つ。

命題 3.4 (Higashitani–K. [2])**.** $\psi, \psi' \in \mathrm{Aut}(G)$ は共役とする。つまり $\psi' = \tau \circ \psi \circ \tau^{-1}$ となる $\tau \in \mathrm{Aut}(G)$ が存在すると仮定する。このとき、$Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ が成り立つ。

したがって $\mathcal{Q}(G)$ は $\mathrm{Aut}(G)$ の共役類の集合と同じになるかということが気になる。しかし、そうはならない例が存在する。C_n を位数 n の巡回群とする。Nelson [7] は $\mathcal{Q}(C_n)$ を決定した。以下で $\mathcal{Q}(C_n)$ について説明する。まず $\mathrm{Aut}(C_n) \cong_{\mathrm{gr}} U(C_n)$ であることが知られている。ただし、$U(C_n) = \{x \in C_n : x \text{ is coprime to } n\}$ であり、$a \in U(C_n)$ に対して、$x \mapsto ax$ によって C_n 上に自己同型が定まる。この a に関する Alexander カンドルを $Q(C_n, a)$ で表す。$N(n, a) = \frac{n}{\gcd(n, 1-a)}$ とおくとき、$Q(C_n, a) \cong_{\mathrm{qu}} Q(C_n, b)$ の必要十分条件は $N(n, a) = N(n, b)$ かつ $a \equiv b \pmod{N(n, a)}$ である。つまり、$\mathcal{Q}(C_n)$ は完全に特徴づけられている。

例えば、$Q(C_9, 4) \cong_{\mathrm{qu}} Q(C_9, 7)$ である。一方で、$U(C_n)$ は可換群だから、$U(C_n)$ の共役類は $U(C_n)$ 自身である。したがって、この例は $\mathrm{Aut}(C_n)$ の共役類と $\mathcal{Q}(C_n)$ は一対一に対応しないことを示している。

問題 3.3 の解決に向けて、等質カンドルや、その中でも $Q(G,\psi)$ の不変量をいくつか紹介する。この節では G は有限群を表すものとする。

命題 3.4 の再掲といくつかの不変量を以下で紹介する。

定理 3.5 (Higashitani–K. [2])**.** $\psi,\psi' \in \mathrm{Aut}(G)$ とし、$Q = Q(G,\psi)$, $Q' = Q(G,\psi')$ とする。

(*a*) ψ と ψ' が共役とする。このとき、$Q \cong_{\mathrm{qu}} Q'$ が成り立つ。

(*b*) もし $Q \cong_{\mathrm{qu}} Q'$ ならば以下が成り立つ。

- $\mathrm{ord}_{\mathrm{Aut}(G)}\,\psi = \mathrm{ord}_{\mathrm{Aut}(G)}\,\psi'$*;*
- $[G : \mathrm{Fix}(\psi, G)] = [G : \mathrm{Fix}(\psi', G)]$, *i.e.,* $|\,\mathrm{Fix}(\psi, G)| = |\,\mathrm{Fix}(\psi', G)|$*;*
- $\mathrm{Inn}(Q) \cong_{\mathrm{gr}} \mathrm{Inn}(Q')$*;*
- $Q(G,\psi^i) \cong_{\mathrm{qu}} Q(G,\psi'^i)$ *for any* $i \in \mathbb{Z}_{>0}$*.*

4　対称群の場合

$\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) を $\{1,\dots,n\}$ 上の対称群 (resp. 交代群) とする。ここでは、$\mathfrak{S}_n$ に対しての問題 3.3 を考える。

以降では、$\mathfrak{S}_n$ の自己同型が内部自己同型 $\psi = (\cdot)^\pi$ のとき、$Q(\mathfrak{S}_n, (\cdot)^\pi) = Q(\pi)$ のように省略する。

4.1　対称群特有の不変量

ここでは群が対称群であるときに得られる一般化 Alexander カンドルの不変量を与える。すべての証明は [2] を参考にしていただきたい。$m = \mathrm{ord}(Q(\pi)) = \mathrm{ord}_{\mathfrak{S}_n}(\pi)$ とおく。

補題 4.1. $n \geq 5$ とする。このとき、

$$\mathrm{Inn}(Q(\pi)) \cong_{\mathrm{gr}} \mathfrak{A}_n \rtimes_\varphi C_m$$

が成り立つ。ただし上記の半直積は $\varphi : C_m \to \mathrm{Aut}(\mathfrak{A}_n)$, $\bar{i} \mapsto (\cdot)^{\pi^i}$ によって定まるものである。つまり具体的な積は

$$(g,\bar{i}) \cdot (h,\bar{j}) = (g\pi^i h \pi^{-i}, \overline{i+j})$$

である。さらにこの半直積について次が成り立つ。

(*a*) π が偶置換ならば、$\mathfrak{A}_n \rtimes_\varphi C_m \cong_{\mathrm{gr}} \mathfrak{A}_n \times C_m$ である。

(*b*) π 奇置換ならば、$\mathfrak{A}_n \rtimes_\varphi C_m \ncong_{\mathrm{gr}} \mathfrak{A}_n \times C_m$ である。

特にこのことから、$Q(\pi) \cong_{\mathrm{qu}} Q(\pi')$ ならば、π と π' は同符号になる。

次に $\mathfrak{S}_n$ の両側コセットに関する $Q(\pi)$ の不変量を与える。$K = \mathrm{Fix}((\cdot)^\pi, \mathfrak{S}_n)$、つまり $K = C_{\mathfrak{S}_n}(\pi)$ とおき、

$$K_{\mathrm{alt}} = K \cap \mathfrak{A}_n$$

とする。同様に $K' = C_{\mathfrak{S}_n}(\pi')$ とおき、$K'_{\mathrm{alt}} = K' \cap \mathfrak{A}_n$ とおく。

補題 4.2. $Q(\pi) \cong_{\mathrm{qu}} Q(\pi')$ であれば、$|K_{\mathrm{alt}} \setminus \mathfrak{S}_n / K| = |K'_{\mathrm{alt}} \setminus \mathfrak{S}_n / K'|$ である。

4.2 $\mathrm{Aut}(\mathfrak{S}_6)$ の構造とカンドル

ここでは $\mathrm{Aut}(\mathfrak{S}_6)$ の共役類の構造を与える。以下の事実は Lam–Leep [6] に詳しく記載されている。まず有名な事実として、$\mathfrak{S}_6$ は外部自己同型写像をもつ。さらに $\mathrm{Aut}(\mathfrak{S}_6) \cong_{\mathrm{gr}} \mathrm{Inn}(\mathfrak{S}_6) \rtimes C_2$ が成り立つ。ここでは具体的な外部自己同型写像を与えて $\mathrm{Aut}(\mathfrak{S}_6)$ の構造を与える。外部自己同型 $\xi : \mathfrak{S}_6 \to \mathfrak{S}_6$ を以下の $\mathfrak{S}_6$ の生成系の行き先を与えることで定義する。

$$\begin{aligned}
&(1\ 2) \mapsto (1\ 2)(3\ 4)(5\ 6),\\
&(2\ 3) \mapsto (1\ 6)(2\ 4)(3\ 5),\\
&(3\ 4) \mapsto (1\ 2)(3\ 6)(4\ 5),\\
&(4\ 5) \mapsto (1\ 6)(2\ 5)(3\ 4),\\
&(5\ 6) \mapsto (1\ 2)(3\ 5)(4\ 6).
\end{aligned}$$

このとき $\mathrm{ord}(\xi) = 2$ である。

$\mathrm{Aut}(\mathfrak{S}_6)$ の任意の元 ψ は、$g \in \mathfrak{S}_6$ と $\varepsilon \in \{0, 1\}$ を用いて、$\psi = (\cdot)^g \circ \xi^\varepsilon$ の形で表すことができる。このことより $\mathrm{Aut}(\mathfrak{S}_6)$ を定める半直積は

$$((\cdot)^{g_1} \circ \xi^{\varepsilon_1}) \circ ((\cdot)^{g_2} \circ \xi^{\varepsilon_2}) = (\cdot)^{g_1 \cdot \xi^{\varepsilon_1}(g_2)} \circ \xi^{\varepsilon_1 + \varepsilon_2}$$

によって定まる。

型 λ に対して、$\mathcal{I}_\lambda$ を以下のように定める：

$$\mathcal{I}_\lambda := \{(\cdot)^\pi \in \mathrm{Inn}(\mathfrak{S}_6) : \pi \text{ の型は } \lambda\}.$$

このとき、任意の外部自己同型 ψ に対して、

$$\psi^2 \in \mathcal{I}_{(5,1)} \cup \mathcal{I}_{(4,2)} \cup \mathcal{I}_{(2^2,1^2)} \cup \mathcal{I}_{(1^6)}$$

であることが知られている。$\lambda=(5,1),(2^2,1^2),(1^6)$ に対して、$\mathcal{O}_\lambda$ を $\psi^2\in\mathcal{I}_\lambda$ となる外部自己同型 ψ の集合とし、また、

$$\mathcal{O}^{\mathrm{E}}_{(4,2)}:=\{(\cdot)^g\circ\xi:((\cdot)^g\circ\xi)^2\in\mathcal{I}_{(4,2)}\text{ and }g\text{ is even}\},\text{ and}$$
$$\mathcal{O}^{\mathrm{O}}_{(4,2)}:=\{(\cdot)^g\circ\xi:((\cdot)^g\circ\xi)^2\in\mathcal{I}_{(4,2)}\text{ and }g\text{ is odd}\}$$

とする。このとき $\mathrm{Aut}(\mathfrak{S}_6)$ の共役類は以下の 13 個であることが知られている (cf. [6]):

$$\begin{aligned}\mathrm{Inn}(\mathfrak{S}_6):\ &\mathcal{I}_{(6)}\cup\mathcal{I}_{(3,2,1)},\ \mathcal{I}_{(5,1)},\ \mathcal{I}_{(4,2)},\ \mathcal{I}_{(4,1,1)},\ \mathcal{I}_{(3,3)}\cup\mathcal{I}_{(3,1^3)},\\ &\mathcal{I}_{(2^3)}\cup\mathcal{I}_{(2,1^4)},\ \mathcal{I}_{(2,2,1,1)},\ \mathcal{I}_{(1^6)};\\ \mathrm{Aut}(\mathfrak{S}_6)\setminus\mathrm{Inn}(\mathfrak{S}_6):\ &\mathcal{O}_{(5,1)},\ \mathcal{O}^{\mathrm{E}}_{(4,2)},\ \mathcal{O}^{\mathrm{O}}_{(4,2)},\ \mathcal{O}_{(2^2,1^2)},\ \mathcal{O}_{(1^6)}.\end{aligned}$$

$\mathcal{Q}(\mathfrak{S}_6)$ の決定に向けて、$\mathrm{Inn}(Q(\mathfrak{S}_6,\psi))$ の構造に注目する。特に $\psi\in\mathcal{O}^{\mathrm{E}}_{(4,2)}$ と $\psi\in\mathcal{O}^{\mathrm{O}}_{(4,2)}$ の差異を見ていく。

$$\eta_0:=(\cdot)^{(2\,5\,6\,4\,3)}\circ\xi,\qquad \eta_1:=(\cdot)^{(1\,5\,6\,4)}\circ\xi$$

とおく。すると簡単な計算から $\eta_0\in\mathcal{O}^{\mathrm{E}}_{(4,2)}$, $\eta_1\in\mathcal{O}^{\mathrm{O}}_{(4,2)}$ であることがわかる。また $k=0,1$ に対して、$Q_k:=Q(\mathfrak{S}_6,\eta_k)$ とおく。

補題 4.3. $\mathrm{Inn}(Q_k)\cong_{\mathrm{gr}}\mathfrak{A}_6\rtimes_{\varphi_k}C_8$ が成り立つ。ただし上記の半直積は $\varphi_k\colon C_8\to\mathrm{Aut}(\mathfrak{A}_6)$, $\overline{i}\mapsto\eta_k^i$ により定められるもの、つまり

$$(g,\overline{i})\cdot(h,\overline{j}):=(g\eta_k^i(h),\overline{i+j})$$

という積である。

さらに次の命題から $\mathfrak{A}_6\rtimes_{\varphi_0}C_8$ と $\mathfrak{A}_6\rtimes_{\varphi_1}C_8$ は群として非同型であることがわかる。

命題 4.4. 次が成り立つ。

(*a*) $\mathfrak{A}_6\rtimes_{\varphi_0}C_8$ 内の $((1\,2\,3\,4\,5),\overline{0})$ に関する中心化群の位数は *40* である。

(*b*) $\mathfrak{A}_6\rtimes_{\varphi_1}C_8$ については、位数 *40* の中心化群をもたない。

したがって、$\mathfrak{A}_6\rtimes_{\varphi_0}C_8\not\cong_{\mathrm{gr}}\mathfrak{A}_6\rtimes_{\varphi_1}C_8$ であるから、とくに $Q_0\not\cong_{\mathrm{qu}}Q_1$ である。

4.3 $\mathcal{Q}(\mathfrak{S}_n)$ の構造決定に向けて

$n = 1$ のときは $\mathfrak{S}_1 = \{e\}$、$n = 2$ のときは $\mathfrak{S}_2 = C_2$ なので、これらの場合の $\mathcal{Q}(\mathfrak{S}_n)$ の構造は容易にわかる。ここでは、$n \geq 3$ である $\mathfrak{S}_n$ に対しての問題 3.3 について、以下の戦略で各共役類ごとに区別をしていく。

(i) 共役類ごとに $\mathrm{ord}(\psi)$ と $|\mathrm{Fix}(\psi, \mathfrak{S}_n)|$ の組の計算をする。そして共役類ごとに値が異なっているかどうか確かめる。(もし $\psi = (\cdot)^\pi$ ならば、$\mathrm{ord}(\psi) = \mathrm{ord}(\pi)$, $\mathrm{Fix}(\psi, \mathfrak{S}_n) = C_{\mathfrak{S}_n}(\pi)$ であることに注意)

(ii) 戦略 (i) で区別できない場合は $\mathrm{Inn}(Q(\mathfrak{S}_n, \psi))$ と $\mathrm{Inn}(Q(\mathfrak{S}_n, \psi'))$ の構造を比較する。($\psi = (\cdot)^\pi$ かつ $\psi' = (\cdot)^{\pi'}$ の場合は、補題 4.1 より π と π' の符号の比較をすればよい)

(iii) 戦略 (i), (ii) で区別できない場合は、自然数 i について、$Q(\mathfrak{S}_n, \psi^i)$ と $Q(\mathfrak{S}_n, \pi'^i)$ の比較を戦略 (i), (ii) に則り行う。

(iv) 戦略 (i), (ii), (iii) で区別できない場合は、補題 4.2 を適応する。つまり、$|K_{\mathrm{alt}} \setminus \mathfrak{S}_n / K|$ と $|K'_{\mathrm{alt}} \setminus \mathfrak{S}_n / K'|$ の比較を行う。

$\underline{n = 3, 4, 5}$

$n = 3, 4, 5$ については戦略 (i) だけで区別できる。つまり、$\mathrm{Aut}(\mathfrak{S}_n) \cong_{\mathrm{gr}} \mathfrak{S}_n$ の共役類ごとに $\mathrm{ord}(\pi)$ と $|C_{\mathfrak{S}_n}(\pi)|$ の組が異なるので、異なる共役類に対する $Q(\pi)$ と $Q(\pi')$ は非同型である。具体的な $\mathrm{ord}(\pi)$ と $|C_{\mathfrak{S}_n}(\pi)|$ の組は表 1, 2, 3 にある。

Shape of π	(3)	$(2,1)$	$(1,1,1)$
$\mathrm{ord}(\pi)$	3	2	1
$\lvert C_{\mathfrak{S}_3}(\pi)\rvert$	3	2	6

表 1: Conjugacy classes for $\mathfrak{S}_3$ and the invariants

Shape of π	(4)	$(3,1)$	$(2,2)$	$(2,1,1)$	$(1,1,1,1)$
$\mathrm{ord}(\pi)$	4	3	2	2	1
$\lvert C_{\mathfrak{S}_4}(\pi)\rvert$	4	3	8	4	24

表 2: Conjugacy classes for $\mathfrak{S}_4$ and the invariants

Shape of π	(5)	$(4,1)$	$(3,2)$	$(3,1,1)$	$(2,2,1)$	$(2,1,1,1)$	$(1,1,1,1,1)$
$\mathrm{ord}(\pi)$	5	4	6	3	2	2	1
$\lvert C_{\mathfrak{S}_5}(\pi)\rvert$	5	4	6	6	8	12	120

表 3: Conjugacy classes for $\mathfrak{S}_5$ and the invariants

$\underline{n=6}$

表 4, 5 より、$\mathcal{O}^{\mathrm{E}}_{(4,2)}$ and $\mathcal{O}^{\mathrm{O}}_{(4,2)}$ 以外については、戦略 (i), (ii) で区別可能である。また $\mathcal{O}^{\mathrm{E}}_{(4,2)}$ と $\mathcal{O}^{\mathrm{O}}_{(4,2)}$ については、命題 4.4 より区別可能である。

Conjugacy classes	$\mathcal{I}_{(6)} \cup \mathcal{I}_{(3,2,1)}$	$\mathcal{I}_{(5,1)}$	$\mathcal{I}_{(4,2)}$	$\mathcal{I}_{(4,1,1)}$	$\mathcal{I}_{(3,3)} \cup \mathcal{I}_{(3,1^3)}$	$\mathcal{I}_{(2^3)} \cup \mathcal{I}_{(2,1^4)}$	$\mathcal{I}_{(2,2,1,1)}$	$\mathcal{I}_{(1^6)}$
$\mathrm{ord}(\pi)$	6	5	4	4	3	2	2	1
$\lvert \mathrm{Fix}((\cdot)^\pi, \mathfrak{S}_6)\rvert$	6	5	8	8	18	48	16	6!
Parity of π			even	odd				

表 4: Conjugacy classes for $\mathrm{Inn}(\mathfrak{S}_6)$ and the invariants

Conjugacy classes	$\mathcal{O}_{(5,1)}$	$\mathcal{O}^{\mathrm{E}}_{(4,2)}$	$\mathcal{O}^{\mathrm{O}}_{(4,2)}$	$\mathcal{O}_{(2^2,1^2)}$	$\mathcal{O}_{(1^6)}$
$\mathrm{ord}(\psi)$	10	8	8	4	2
$\lvert \mathrm{Fix}(\psi, \mathfrak{S}_6)\rvert$	5	4	4	4	20

表 5: Conjugacy classes for $\mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Inn}(\mathfrak{S}_6)$ and the invariants

$\underline{n=7}$

表 6 より、戦略 (i), (ii) で区別可能である。

Shape of π	(7)	$(6,1)$	$(5,2)$	$(4,3)$	$(5,1^2)$	$(4,2,1)$	$(3^2,1)$	$(3,2^2)$
$\mathrm{ord}(\pi)$	7	6	10	12	5	4	3	6
$\lvert C_{\mathfrak{S}_7}(\pi)\rvert$	7	6	10	12	10	8	18	24

Shape of π	$(4,1^3)$	$(3,2,1^2)$	$(2^3,1)$	$(2^2,1^3)$	$(3,1^4)$	$(2,1^5)$	(1^7)
$\mathrm{ord}(\pi)$	4	6	2	2	3	2	1
$\lvert C_{\mathfrak{S}_7}(\pi)\rvert$	24	12	48	48	72	240	7!
Parity			odd	even			

表 6: Conjugacy classes for $\mathfrak{S}_7$ and the invariants

$\underline{n=8}$

表 7 より、$(3^2,2)$ と $(3,2,1^3)$ 以外は戦略 (i), (ii) で区別可能である。$(3^2,2)$ と $(3,2,1^3)$ については、戦略 (iii) で区別可能である。$\pi_1 \in \mathfrak{S}_8$ (resp. $\pi_2 \in \mathfrak{S}_8$) を型 $(3^2,2)$ (resp. $(3,2,1^3)$) をもつ置換とする。このとき、π_1^2 (resp. π_2^2) の型は $(3^2,1^2)$ (resp. $(3,1^5)$) であるので、再び表 7 よりこれらは区別可能である。

Shape of π	(8)	$(7,1)$	$(6,2)$	$(6,1^2)$	$(5,3)$	(4^2)	$(4,2^2)$	$(5,2,1)$
$\mathrm{ord}(\pi)$	8	7	6	6	15	4	4	10
$\lvert C_{\mathfrak{S}_8}(\pi)\rvert$	8	7	12	12	15	32	32	36
Parity			even	odd		even	odd	

Shape of π	$(4,3,1)$	$(3^2,2)$	$(3,2,1^3)$	(2^4)	$(5,1^3)$	$(4,2,1^2)$	$(3^2,1^2)$
$\mathrm{ord}(\pi)$	12	6	6	2	5	4	3
$\lvert C_{\mathfrak{S}_8}(\pi)\rvert$	10	36	36	384	30	16	36
Parity		odd	odd				

Shape of π	$(3,2^2,1)$	$(4,1^4)$	$(2^3,1^2)$	$(3,1^5)$	$(2^2,1^4)$	$(2,1^6)$	(1^8)
$\mathrm{ord}(\pi)$	6	4	2	3	2	2	1
$\lvert C_{\mathfrak{S}_8}(\pi)\rvert$	24	96	24	360	96	1440	8!

表 7: Conjugacy classes for $\mathfrak{S}_8$ and the invariants

$\underline{n = 9, 11, 12, 16, 19, 20, 23, 28}$

これらの場合は、$n = 8$ のときと同様にして、戦略 (i), (ii), (iii) を用いれば区別可能である。

$\underline{n = 10}$

$(4,2^3)$ と $(4,2,1^4)$ 以外は戦略 (i), (ii), (iii) を用いれば区別可能である。$(4,2^3)$ と $(4,2,1^4)$ については、戦略 (iv) で区別可能である。$\pi_1 \in \mathfrak{S}_{10}$ (resp. $\pi_2 \in \mathfrak{S}_{10}$) を型 $(4,2^3)$ (resp. $(4,2,1^4)$) をもつ置換とする。このとき、`GAP` [1] を用いると、

$$|C_{\mathfrak{S}_{10}}(\pi_1) \cap \mathfrak{A}_{10} \setminus \mathfrak{S}_{10} / C_{\mathfrak{S}_{10}}(\pi_1)| = 240; \text{ and}$$
$$|C_{\mathfrak{S}_{10}}(\pi_2) \cap \mathfrak{A}_{10} \setminus \mathfrak{S}_{10} / C_{\mathfrak{S}_{10}}(\pi_2)| = 291.$$

であることがわかり、区別可能である。

$\underline{n = 13, 14, 17, 18, 21, 22, 24, 25, 26, 27, 29, 30}$

これらの場合は、$n = 10$ のときと同様にして、戦略 (i), (ii), (iii), (iv) を用いれば区別可能である。

$\underline{n = 15}$

$(9, 3^2)$ と $(9, 3, 1^3)$ 以外は戦略 (i), (ii), (iii), (iv) を用いれば区別可能である。$(9, 3^2)$ と $(9, 3, 1^3)$ については、戦略 (i), (ii), (iii), (iv) のどれを用いても区別ができない。

以上のことをまとめると以下の結果となる。

定理 4.5. $n \in \{3, 4, \ldots, 30\} \setminus \{15\}$ のとき、$\mathcal{Q}(\mathfrak{S}_n)$ と $\mathrm{Aut}(\mathfrak{S}_n)$ の共役類集合の間に一対一対応がある。特に、$n \in \{3, 4, \ldots, 30\} \setminus \{6, 15\}$ のときは、$\mathcal{Q}(\mathfrak{S}_n)$ と $\mathfrak{S}_n$ の共役類集合の間に一対一対応がある。

5 最近得られたこと

G を有限群とし、$\psi \in \mathrm{Aut}(G)$ を恒等写像でないものとする。また $Q = Q(G, \psi)$ とする。このとき、P_Q を $\mathrm{Inn}(Q)$ による e の軌道とする。つまり、

$$P_Q = \{x \in G : \exists a_1, \ldots, a_p \in G \text{ s.t. } x = s_{a_p} \circ \cdots \circ s_{a_1}(e)\}$$

とする。

定理 5.1. P_Q について以下が成り立つ。

(*a*) P_Q は Q の部分カンドルになる。

(*b*) $\psi|_{P_Q}$ は P_Q 上のカンドル自己同型写像である。

(*c*) P_Q は G の正規部分群である。

定理 5.2. $\psi, \psi' \in \mathrm{Aut}(G)$ に対して、$Q = Q(G, \psi)$, $Q' = Q(G, \psi')$ とおく。また $P = P_Q$, $P' = P_{Q'}$ とおく。$Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ を仮定し、$f : Q(G, \psi) \to Q(G, \psi')$ を $f(e) = e$ であるようなカンドル同型写像とする（このような f は必ず存在する）と次が成り立つ。

(*a*) $f|_P$ は P と P' の間のカンドル同型写像である。したがって $P \cong_{\mathrm{qu}} P'$ である。

(*b*) $f|_P$ は P と P' の間の群同型写像である。したがって $P \cong_{\mathrm{gr}} P'$ である。

(*c*) $\psi' \circ f|_P = f|_P \circ \psi$ が成り立つ。

系 5.3. G が有限単純群のとき、$\mathcal{Q}(G)$ と $\mathrm{Aut}(G)$ の共役類集合の間に一対一対応がある。

Proof. まず $\psi = \mathrm{Id}_G$ の場合は、$Q(G, \mathrm{Id}_G)$ は自明カンドルであり、$\psi \neq \mathrm{Id}_G$ ならば $Q(G, \psi)$ は自明カンドルにならない。したがって $\psi, \psi' \in \mathrm{Aut}(G)$ は $\psi, \psi' \neq \mathrm{Id}_G$ を仮定する。今 $Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ を仮定する。G が正規部分群なので、定理 5.1 (c) より $P = P' = G$ である。定理 5.2 (b) より $f \in \mathrm{Aut}(G)$ であり、定理 5.2 (c) より $\psi' \circ f = f \circ \psi$ を得る。これは ψ と ψ' が共役であることを意味する。 □

この結果を用いれば、定理 4.5 は一般の n の場合に拡張される。

系 5.4. $n \geq 3$ のとき、$\mathcal{Q}(\mathfrak{S}_n)$ と $\mathrm{Aut}(\mathfrak{S}_n)$ の共役類集合の間に一対一対応がある。

Proof. $n = 3, 4$ のときは定理 4.5 で示されているので、$n \geq 5$ を仮定する。$\psi, \psi' \neq \mathrm{Id}$ である $\psi, \psi' \in \mathrm{Aut}(\mathfrak{S}_n)$ に対して、$Q = Q(\mathfrak{S}_n, \psi)$, $Q' = Q(\mathfrak{S}_n, \psi')$ として、P と P' について考える。$\mathfrak{S}_n$ の非自明な正規部分群は $\mathfrak{A}_n$ しかないので、P と P' は $\mathfrak{A}_n$ になる。今 $Q \cong_{\mathrm{qu}} Q'$ を仮定する。定理 5.2 (a) より $Q(\mathfrak{A}_n, \psi|_{\mathfrak{A}_n})$ と $Q(\mathfrak{A}_n, \psi'|_{\mathfrak{A}_n})$ はカンドル同型であり、$\mathfrak{A}_n$ は有限単純群より系 5.3 から $\psi|_{\mathfrak{A}_n}$ と $\psi'|_{\mathfrak{A}_n}$ は共役である。これから ψ と ψ' が共役であることを得る。 □

参考文献

[1] GAP, https://www.gap-system.org/

[2] A. Higashitani and H. Kurihara, Homogeneous quandles arising from automorphisms of symmetric groups. *arXiv preprint* arXiv:2005.12057. https://arxiv.org/abs/2005.12057

[3] Y. Ishihara and H. Tamaru, Flat connected finite quandles. *Proc. Amer. Math. Soc.* **144** (2016), no. 11, 4959–4971. https://doi.org/10.1090/proc/13095

[4] D. Joyce, A classifying invariant of knots, the knot quandle. *J. Pure Appl. Algebra* **23** (1982), no. 1, 37–65. https://doi.org/10.1016/0022-4049(82)90077-9

[5] S. Kamada, H. Tamaru, and K. Wada, On classification of quandles of cyclic type. *Tokyo J. Math.* **39** (2016), no. 1, 157–171. https://doi.org/10.3836/tjm/1459367262

[6] T. Y. Lam and D. B. Leep, Combinatorial structure on the automorphism group of S_6. *Exposition. Math.* **11** (1993), no. 4, 289–308.

[7] S. Nelson, Classification of finite Alexander quandles. In *Proceedings of the Spring Topology and Dynamical Systems Conference.* 2003, 245–258

[8] L. Vendramin, Doubly transitive groups and cyclic quandles. *J. Math. Soc. Japan* **69** (2017), no. 3, 1051–1057. https://doi.org/10.2969/jmsj/06931051

Kneser グラフと共通の Kronecker 被覆を持つグラフについて

概要

Kronecker 被覆とは，グラフ G に対して標準的な方法で定義される二重被覆で， Kronecker 積を用いて $K_2 \times G$ と書かれる．一般には $K_2 \times G \cong K_2 \times H$ であっても $G \cong H$ であるとは限らない．本稿では [15] において示した，$K_2 \times K(n,k) = K_2 \times G$ を満たす単純グラフ G の分類と，それらの自己同型群と彩色数の決定について紹介する．

本稿の構成について述べる．第一節で基本的な用語と Kronecker 被覆の背景について説明し，第二節で主定理を述べる．第三節では主定理の一部，すなわち $K_2 \times K(n,k) \cong K_2 \times G$ を満たす単純グラフ G の分類と自己同型群の決定について述べ，第四節において Lovász の近傍複体と Kronecker 被覆との関係を用いて，$K_2 \times K(n,k) \cong K_2 \times G$ を満たす単純グラフの彩色数を決定する．

1　イントロダクション

本稿で**グラフ**とは次の二つを満たす組 $G = (V(G), E(G))$ のことであるとする：

(1) $V(G)$ は有限集合である．
(2) $E(G) \subset V(G) \times V(G)$ であって，$(v,w) \in E(G)$ ならば $(w,v) \in E(G)$ を満たす．

したがって本稿で扱うグラフは多重辺を許さない有限無向グラフである．特に $v \in V(G)$ で $(v,v) \in E(G)$ となるものが存在しないとき，G を**単純グラフ**という．

グラフ G と H に対し，**グラフ準同型**とは写像 $f\colon V(G) \to V(H)$ であって，$(f \times f)(E(G)) \subset E(H)$ を満たすものである．言い換えると $(v,w) \in E(G)$ ならば $(f(v), f(w)) \in E(H)$ が成立するものである．グラフ準同型に関しては，[5] や [3] などが詳しい．

n-頂点完全グラフを K_n で書く．すなわち $V(K_n) = [n] = \{1, \cdots, n\}$ とし，$E(K_n) = \{(i,j) \mid i,j \in [n],\ i \neq j\}$ で定まるグラフである．このときグラフ G の n-彩色とは，G から K_n へのグラフ準同型に他ならない．また G の彩色数とは，G の n-彩色が存在するような最小の n のことであり，$\chi(G)$ と表すことにする．

$v \in V(G)$ に対し，v の**近傍**あるいは**開近傍** $N_G(v)$ を

$$N_G(v) = \{w \in V(G) \mid (v,w) \in E(G)\}$$

により定める．G を特に明示する必要のないときは，単に $N(v)$ と書く．写像 $f\colon V(G) \to V(H)$ がグラフ準同型であることと，全ての $v \in V(G)$ に対して $f(N_G(v)) \subset N_H(f(v))$ が成立することは同値である．

定義 1.1. グラフ準同型 $p\colon G \to H$ が**被覆写像**であるとは，任意の $v \in V(G)$ に対し，写像 $p|_{N(v)}\colon N(v) \to N(p(v))$ が全単射になることをいう．

グラフの被覆写像については例えば [13] などが詳しい．

例 1.2. n-サイクルグラフ C_n $(n \geq 3)$ を

$$V(C_n) = \mathbb{Z}/n,\ E(C_n) = \{\{x, x \pm 1\} \mid x \in \mathbb{Z}/n\}$$

として定める．$n \geq 3$，$k \geq 1$ に対し，自然な射影 $\mathbb{Z}/kn \to \mathbb{Z}/n$ はグラフ準同型 $C_{kn} \to C_n$ を定めるが，これは被覆写像である．

このように被覆写像 $p\colon G \to H$ は，H が単純グラフである場合はトポロジーの意味での被覆写像（詳細は [4] の 1.3 節）と本質的には等しい．ただし H が単純でない場合には，以下のように幾何学的イメージとは若干異なる被覆写像がある．

例 1.3. グラフ $\mathbf{1}$ を $V(\mathbf{1}) = \{1\}$, $E(\mathbf{1}) = \{(1,1)\}$ とする．このとき全てのグラフ G に対して G から $\mathbf{1}$ への写像がただ一つだけ存在する．特に K_2 から $\mathbf{1}$ への写像を p とすると，p は被覆写像になる．

このように H が単純グラフでない場合は，$p\colon G \to H$ が被覆写像であることと，トポロジーの意味での被覆空間であることは必ずしも一致しない．しかしこのようなものも含めて考えておくと，後述の定理などで例外を作る必要がなく便利なので，例外視しないことにする．

続いて Kronecker 二重被覆について説明するために， Kronecker 積の定義を書いておく：

G と H をグラフとする．G と H の **Kronecker 積** $G \times H$ とは

$$V(G \times H) = V(G) \times V(H),$$

$$E(G \times H) = \{((v,w),(v',w')) \mid (v,v') \in E(G), (w,w') \in E(H)\}$$

で定義されるグラフのことである．なおこの $G \times H$ の名称は多くあり， tensor product（テンソル積），categorical product （圏論的積）， Kronecker product （ Kronecker 積）などの名称が主に使われる．テンソル積という用語の由来は $G \times H$ の隣接行列が G の隣接行列と H の隣接行列のテンソル積になるからである．圏論的積については，グラフの圏をグラフを対象としグラフ準同型を射とする圏を考えたとき，圏論的な意味での G と H の積が $G \times H$ に一致するからである．なお単純に積といった場合，別の概念を指すことも多いので，ここでは $G \times H$ のことを Kronecker 積ということにする．

Kronecker 積 $G \times H$ に対し，第一射影 $V(G) \times V(H) \to V(G)$ および第二射影 $V(G) \times V(H) \to V(H)$ はともにグラフ準同型 $G \times H \to G$ および $G \times H \to H$ を誘導する．

定義 1.4. G の Kronecker 被覆とは，第二射影 $p\colon K_2 \times G \to G$ のことである．

$p\colon K_2 \times G \to G$ は実際に被覆写像の公理（定義 1.1）を満たすので，被覆写像である．なお Kronecker 被覆にも様々な名称があり， canonical (bipartite) double などと呼ばれたりもする．

例 1.5. $K_2 \times C_{2n+1} \cong C_{4n+2}$，$K_2 \times C_{2m} \cong C_{2m} \sqcup C_{2m}$ が成立する（ただし $n \geq 1$, $m \geq 2$）．ここで $C_{2m} \sqcup C_{2m}$ は C_{2m} の二つのコピーの非交叉和である．

例 1.6. $K_2 \times K_4$ は立方体の辺と頂点からなるグラフである．

$K_2 \times G \cong K_2 \times H$ を満たすグラフ G と H は非常に似た性質を持つ．例えば頂点数や辺の個数は等しく，また次数列も等しい．最後の節で述べる近傍複体も一致する．しかし一般にはグラフ G と H に対し，$K_2 \times G \cong K_2 \times H$ であったとしても，$G \cong H$ であるとは限らない．

例 1.7. $K_2 \times (C_3 \sqcup C_3) \cong C_6 \sqcup C_6 \cong K_2 \times C_6$ となるが，$C_3 \sqcup C_3 \ncong C_6$.

例 1.8. より一般に，$K_2 \times K_2 \cong K_2 \sqcup K_2$ であることに注目すると，

$$K_2 \times (K_2 \times K_n) \cong (K_2 \times K_2) \times K_n \cong (K_2 \sqcup K_2) \times K_n \cong K_2 \times K_n \times (K_n \sqcup K_n)$$

が成立するが，$K_2 \times K_n \ncong K_n \sqcup K_n$ である．例 1.7 はこの例の $n = 3$ の場合に他ならない．

例 1.9. グラフ G と H に対し，G と H の**ジョイン** $G * H$ を

$$V(G * H) = V(G) \sqcup V(H),\ E(G * H) = E(G) \sqcup E(H) \cup \{(v, w), (w, v) \mid v \in V(G), w \in V(H)\}$$

と定める．グラフ G_1 と G_2 が $K_2 \times G_1 \cong K_2 \times G_2$ を満たすならば，任意のグラフ H に対し

$$K_2 \times (G_1 * H) \cong K_2 \times (G_2 * H)$$

を満たすことがわかる．これにより，例えば $G_1 = K_2 \times K_n$, $G_2 = K_n \sqcup K_n$, $H = K_m$ とすると，

$$K_2 \times (G_1 * H) \cong K_2 \times (G_2 * H)$$

となり，さらに $\chi(G_1 * H) = \chi(G_1) + \chi(H) = 2 + m$, $\chi(G_2 * H) = \chi(G_2) + \chi(H) = n + m$ となる．このように，共通の Kronecker 被覆を持つという条件は，彩色数には特に関係がないように思える．

このように $K_2 \times G \cong K_2 \times H$ が成立したとしても $G \ncong H$ となる例は多く存在するが，一般には以下の Lovász による古典的な定理が示すように，グラフ A によっては「$A \times G \cong A \times H$ が成立した場合 $G \cong H$」が成立するものは多く存在する：

定理 1.10 (Lovász's cancellation theorem [10])**.** A が二部グラフでないグラフ，G と H をグラフとする．このとき，$A \times G \cong A \times H$ が成立するならば $G \cong H$ が成立する．

そこで次のような問題を考えることは自然であろう．

問題 1.11 (Imrich-Pisanski [6])**.** X を二部グラフとする．このときグラフ G であって，$K_2 \times G \cong X$ を満たす単純グラフ G の同型類を全て求めよ．

この問題は X が超立方体 [2]，一般 Petersen グラフ [9] においてこの問題は解決される．本稿の目的の一つは，X が二部 Kneser グラフ $H(n, k)$（定義は次節参照）の場合に解決したことである．

2 主定理

ここでは本稿の主定理を述べる．正の整数 n, k で，$n \geq 2k$ を満たすものに対し，**Kneser グラフ** $K(n,k)$ を

$$V(n,k) = \binom{[n]}{k} = \{\sigma \subset [n] \mid \#\sigma = k\},$$

$$E(n,k) = \left\{(\sigma,\tau) \in \binom{[n]}{k} \times \binom{[n]}{k} \mid \sigma \cap \tau = \emptyset\right\}$$

により定める．ここで $K(n,1)$ は K_n に，$K(5,2)$ は Petersen グラフに同型である．

定義 2.1. 二部 Kneser グラフ $H(n,k)$ を $K(n,k)$ の Kronecker 二重被覆，すなわち $H(n,k) = K_2 \times K(n,k)$ により定める．

Imrich と Pisanski は Petersen グラフ $K(5,2)$ と共通の Kronecker 被覆を持つグラフ G で，$K(5,2)$ と同型でない単純グラフを構成している．本稿はそれを以下のように一般化した：

定理 2.2 (松下 [15])**.** n, k を正の整数で $n > 2k$ を満たすものとする．このとき Kronecker 被覆が $H(n,k)$ となる単純グラフはちょうど k 個

$$K(n,k) = G_0(n,k), G_1(n,k), \cdots, G_{k-1}(n,k)$$

ある．

これらに現れた $G_i(n,k)$ の自己同型群および彩色数を決定することができる．まず自己同型群に関して述べる．

2 つの群 Γ と Γ' を考える．$\mathrm{Aut}(\Gamma')$ により群 Γ' の自己同型群を表す．Γ の Γ' への（左）作用とは，群準同型 $\varphi\colon \Gamma \to \mathrm{Aut}(\Gamma')$ のことである．しばしば $\alpha \in \Gamma$ と $x \in \Gamma'$ に対し，$\varphi(\alpha)(x)$ のことを単に αx などと書く．

Γ' への Γ の作用 φ が与えられたとき，Γ と Γ' の**半直積** $\Gamma' \rtimes_\varphi \Gamma$ を以下のように定める．まず $\Gamma' \rtimes_\varphi \Gamma$ は集合としては Γ' と Γ の直積集合 $\Gamma' \times \Gamma$ に等しく，演算は

$$(x,\alpha)\cdot(y,\beta) = (x \cdot \varphi(\alpha)(y), \alpha\cdot\beta)$$

により定める．特に φ を明示する必要がない場合は単に $\Gamma' \rtimes \Gamma$ と書く．

S_i で i 次の対称群，すなわち $[i] = \{1, \cdots, i\}$ の置換全体を表し，$\mathbb{Z}_2$ で位数 2 の巡回群を表す．このとき $\mathbb{Z}_2$ の i 個の直積 $\mathbb{Z}_2^i$ に対し，S_i への作用を

$$\sigma(x_1, \cdots, x_i) = (x_{\sigma^{-1}(1)}, \cdots, x_{\sigma^{-1}(i)})$$

により定める．このとき $G_i(n,k)$ の自己同型群は以下のように表される．

定理 2.3 (松下 [15])**.** 正の整数 n, k で $n > 2k$ を満たすものに対し，$\mathrm{Aut}(G_i(n,k)) \cong (\mathbb{Z}_2^i \rtimes S_i) \times S_{n-2i}$ が成立する．

続いて彩色数について述べる．ここで Kneser グラフの彩色数は次のように既に知られている：

定理 2.4 (Lovász [11])**.** $\chi(K(n,k)) = n - 2k + 2$

注意 2.5. 写像 $c\colon V(K(n,k)) \to \{2k-1, 2k, \cdots, n-2k+2\}$ を

$$c(\sigma) = \max\left\{\sigma \cup \{2k-1\}\right\}$$

により定めると，$\sigma \cap \tau = \emptyset$ の場合に $c(\sigma) \neq c(\tau)$ が成立する．このことから $\chi(K(n,k)) \leq n - 2k + 2$ が成立する．

既に述べたように， Kronecker 被覆が等しいからと言って，彩色数も一致するというわけではない．しかし $G_i(n,k)$ については次の定理が成立する：

定理 2.6. 正の整数 n, k で $n > 2k$ となるものに対し，$\chi(G_i(n,k)) = \chi(K(n,k)) = n - 2k + 2$ が成立する．

3 バイグラフの圏

本節では定理 2.3 と定理 2.4 の証明の概略を述べる．

バイグラフ (bigraph) とは，グラフ X とグラフ準同型 $\varepsilon\colon X \to K_2$ の組 (X, ε) のことである．K_2 へのグラフ準同型が存在することから X は二部グラフである．しばしばバイグラフ (X, ε) の ε を省略して「X をバイグラフとする」などということもある．この場合，X に付随する 2-彩色を ε_X などと書くことにする．なおバイグラフ (bigraph) という用語は bipartite graph, すなわち二部グラフのことを指して使うこともある．我々の bigraph は単に二つからなる部集合の存在を課すだけでなく，二つからなる部集合が指定されている二部グラフであるとも言え，この用語は [1] などにある．

X と Y をバイグラフとする．このとき X から Y へのグラフ準同型 f が $\varepsilon_Y \circ f = \varepsilon_X$ が成立するとき，f は**偶 (even)** であるといい，全ての $x \in V(X)$ に対し $\varepsilon_Y(f(x)) \neq \varepsilon_X(x)$ が成立するとき，f は**奇 (odd)** であるという．

グラフ G の自己同型 f で $f^2 = \mathrm{id}_G$ を満たすものを**対合**という．

以上の用語を準備すると， Kronecker 被覆 $K_2 \times G$ には，以下の構造が付随していると考えられる：

- $K_2 \times G$ には標準的な 2-彩色，すなわち第一射影 $K_2 \times G \to K_2$ が存在する．これにより $K_2 \times G$ はバイグラフである．
- $K_2 \times G$ には，自然な対合 $(1, v) \leftrightarrow (2, v)$ で奇であるもの（**奇対合**）が存在する．

X をバイグラフとして α を X の奇対合とする．このとき商 X/α を

$$V(X/\alpha) = \left\{\{x, \alpha(x)\} \mid x \in V(X)\right\},$$

$$E(X/\alpha) = \{(\sigma, \tau) \mid (\sigma \times \tau) \cap E(X) \neq \emptyset\}$$

により定義する．これは α によって移り変わる辺や頂点を同一視して得られるグラフである．また商写像

$V(X) \to V(X/\alpha)$ によりグラフ準同型 $\pi\colon X \to X/\alpha$ が定義される．

注意 3.1. バイグラフ X は二部グラフだから単純であるが，その商 X/α は必ずしも単純ではない．ここで X/α が単純でないことと同値な条件は，$x \in V(X)$ で $(x, \alpha(x)) \in E(X)$ となるものが存在することである．

次のことはよく知られており，また簡単に示すこともできる（例えば [14] を参照）：

補題 3.2. X と Y をバイグラフ，α と β をそれぞれ X と Y の奇対合とする．グラフ準同型 $f\colon X \to Y$ で $\beta f = f\alpha$ を満たすものに対し，グラフ準同型 $\overline{f}\colon X/\alpha \to Y/\beta$ で図式

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ X/\alpha & \xrightarrow{\overline{f}} & Y/\beta \end{array}$$

を可換にするものがただ一つだけある．また f が同型ならば $\overline{f}$ も同型である．

補題 3.3. X と Y をバイグラフ，α と β をそれぞれ X と Y の奇対合とする．グラフ準同型 $g\colon X/\alpha \to Y/\beta$ に対し，偶なグラフ準同型 $\tilde{g}\colon X \to Y$ であって，$\beta \circ \tilde{g} = \tilde{g} \circ \alpha$ を満たすものがただ一つ存在する．g が同型ならば $\tilde{g}$ も同型である．

補題 3.4. X をバイグラフ，α をその奇対合とすると，自然な写像

$$X \xrightarrow{(\varepsilon_X, \pi)} K_2 \times (X/\alpha)$$

は同型である．

注意 3.5. 圏の言葉を用いると，次のように簡略化して表現することができる．グラフの圏とは，対象をグラフとし，射をグラフ準同型とする圏のこととし，$\mathcal{G}$ で表す．$\mathcal{G}_{/K_2}$ でバイグラフの圏，すなわち対象をバイグラフとし，射を偶なグラフ準同型とする圏とする．さらに圏 $\mathcal{G}^o_{/K_2}$ を次のように定める．対象は三つ組 (X, ε, α) であって，(X, ε) はバイグラフであり，α は (X, ε) の奇対合である．さらに二つの $\mathcal{G}^o_{/K_2}$ の対象 $(X, \varepsilon_X, \alpha_X)$ と $(Y, \varepsilon_Y, \alpha_Y)$ の間の射とは，偶なグラフ準同型 $f\colon X \to Y$ であって，$\alpha_Y \circ f = f \circ \alpha_X$ を満たすものとする．このとき Kronecker 二重被覆は $\mathcal{G}$ から $\mathcal{G}^o_{/K_2}$ への関手を満たすが，上の主張は Kronecker 被覆が与える関手

$$K_2 \times (-)\colon \mathcal{G} \to \mathcal{G}^o_{/K_2}$$

は， quasi-inverse を商 $(X, \varepsilon, \alpha) \mapsto X/\alpha$ とする圏同値であるということである（詳しくは [14] を参照せよ）．

これらの主張から次がしたがう：

系 3.6. X をバイグラフとし，α と β を X の奇対合とする．このとき以下は同値である：

(1) $X/\alpha \cong X/\beta$
(2) α と β は $\mathrm{Aut}(X)$ で共役である．すなわち $f \in \mathrm{Aut}(X)$ であって $f\alpha = \beta f$ を満たすものが存在する．
(3) 偶な $f \in \mathrm{Aut}(X)$ であって，$f\alpha = \beta f$ を満たすものが存在する．

Proof. (3) ⇒ (2) は明らか．(2) ⇒ (1) および (1) ⇒ (3) はそれぞれ補題 3.2 と補題 3.3 からわかる． □

系 3.7. (X, ε) をバイグラフ，α をその奇対合とすると，

$$\mathrm{Aut}(X/\alpha) \cong \{f \in \mathrm{Aut}(X) \mid f \text{ は偶で } \alpha \circ f = f \circ \alpha\}.$$

Proof. 右辺を Γ とする．$\mathrm{Aut}(X/\alpha) \to \Gamma$ は $f \in \mathrm{Aut}(X/\alpha)$ に対し補題 3.3 で構成されるリフト $\tilde{f}\colon X \to X$．$\Gamma \to \mathrm{Aut}(X/\alpha)$ は補題 3.2 が誘導するグラフ準同型 $X/\alpha \to X/\alpha$．これらの対応が逆になっていることは，補題 3.2 と補題 3.3 における一意性からわかる． □

それでは定理 2.3 と定理 2.4 の証明の概略を書く．まず Mirafzal による $H(n,k)$ の自己同型群について述べる．S_n は $[n]$ に作用するが，それにより同型 $S_n \xrightarrow{\cong} \mathrm{Aut}(K(n,k))$ が得られることが Erdős-Ko-Rado の定理からわかる．これを用いると，$H(n,k)$ の自己同型群は次のように書くことができる．

定理 3.8 (Mirafzal [16])**.** 自然な写像

$$\mathbb{Z}_2 \times S_n \xrightarrow{\cong} \mathrm{Aut}(K_2) \times \mathrm{Aut}(K(n,k)) \to \mathrm{Aut}(H(n,k))$$

は同型である．

$\mathbb{Z}_2$ の生成元を α_{K_2} とすると，$\mathrm{Aut}(H(n,k))$ の奇対合は位数 2 の元 $\beta \in S_n$ と α_{K_2} の対 $\alpha_{K_2} \times \beta$ と書くことができる．$\alpha_{K_2} \times \beta$ と $\alpha_{K_2} \times \beta'$ が $\mathbb{Z}_2 \times S_n$ で共役であることと，β と β' が S_n で共役であることは同値である．$0 \le i \le \lfloor n/2 \rfloor$ に対し β_i を

$$\beta_i = (1,2)(3,4)\cdots(2i-1, 2i)$$

と書かれる S_n の元とすると，$H(n,k)$ の奇対合は何らかの $\alpha_{K_2} \times \beta_i$ と共役であり，$i \neq j$ のとき $\alpha_{K_2} \times \beta_i$ と $\alpha_{K_2} \times \beta_j$ は共役でない．そこで

$$G_i(n,k) = H(n,k)/(\alpha_{K_2} \times \beta_i)$$

と置く．$i \ge k$ のとき，

$$(\alpha_{K_2} \times \beta_i)(1, \{1,3,5,\cdots 2k-1\}) = (2, \{2,4,6,\cdots,2k\}) \sim (1, \{1,3,5,\cdots,2k-1\})$$

が成立するので，注意 3.1 より $G_i(n,k)$ は単純でないが，一方で $i \le k$ の時に $G_i(n,k)$ は単純になる．これにより定理 2.3 が成立する．

また $\alpha_{K_2} \times \beta_i$ と可換な $\mathbb{Z}_2 \times S_n$ の元全体が $\mathrm{Aut}(G_i(n,k))$ に同型であるが，これは β_i と可換な S_n の元全体に同型である．それが $(\mathbb{Z}_2^i \rtimes S_i) \times S_{n-2i}$ に同型になることも単純計算によりわかる．これが定理 2.4 の証明の概略である．

4　定理 2.6 の証明

G をグラフとする．$v \in V(G)$ に対し，$N(v) = \{w \in V(G) \mid (v,w) \in E(G)\}$ のことを v の近傍というのであった（第 1 節参照）．

定義 4.1 (Lovász 1978)**.** グラフ G の近傍複体 $N(G)$ を底集合を $V(G)$ とし，単体のなす集合を

$$N(G) = \{\sigma \subset V(G) \mid \sigma \subset N(v) \text{ を満たす頂点 } v \in V(G) \text{ が存在する } \}$$

により定義する．

近傍複体のある位相的不変量が，彩色数と関係があることが知られている．その位相的不変量を定式化するため，まず記号として

$$D^n = \{(x_1, \cdots, x_n) \in \mathbb{R}^n \mid x_1^2 + \cdots + x_n^2 \leq 1\},$$
$$S^n = \{(x_0, \cdots, x_n) \in \mathbb{R}^{n+1} \mid x_0^2 + \cdots + x_n^2 = 1\}$$

と定義し，D^n を n 次元単位球体，S^n を n 次元単位球面と呼ぶことにする．ただし D^0 は一点空間，$S^{-1} = \emptyset$ とし，$n < 0$ のとき D^n や S^{n-1} は定義しないものとする．

定義 4.2. X を位相空間，n を整数とする．X が n-連結であるとは，$-1 \leq i$ かつ $i \leq n$ を満たす全ての整数 i と連続写像 $f\colon S^{i-1} \to X$ に対し，連続写像 $g\colon D^i \to X$ で $g|_{S^{i-1}} = f$ を満たすものが存在することをいう．

例 4.3. 位相空間の n-連結性のいくつかの性質をまとめておく（詳しくは [4]）．

$n \leq m$ とすると，m-連結な空間は n-連結でもある．$n \leq -2$ ならば全ての位相空間は n-連結である．(-1)-連結であることは，空でないことと同値である．0-連結であることは，弧状連結であるということと同値である．一般に $n \geq 1$ に対しては，n-連結であるということは，弧状連結でありかつ全ての $1 \leq i \leq n$ に対し i 次ホモトピー群 $\pi_i(X)$ が自明群になることと同値である．なおグラフの n-連結性とは特に関係はない．

Lovász は Kneser 予想の解決の中で，次の二つの定理を証明している：

定理 4.4 (Lovász [11])**.** $N(G)$ が n-連結ならば，$\chi(G) \geq n + 3$ である．

定理 4.5 (Lovász [11])**.** $N(K(n,k))$ は $(n - 2k - 1)$-連結である．

上の二つの定理から $\chi(K(n,k)) = n - 2k + 2$ がしたがう．

次の命題は $K_2 \times G$ と $N(G)$ の定義から簡単に示すことができる．例えば本質的に [1] にも書かれている：

命題 4.6. $K_2 \times G \cong K_2 \times H$ ならば $N(G) \cong N(H)$ である．

注意 4.7. 一般には $N(G) \cong N(H)$ であるからと言って，$K_2 \times G \cong K_2 \times H$ であるとは限らない．例えば G として 4 頂点からなる道のグラフ P_4，H として C_4 を考えると，$N(P_4) \cong N(C_4)$ だが $K_2 \times P_4 = P_4 \sqcup P_4 \ncong C_4 \sqcup C_4 \cong K_2 \times C_4$ となる．

ただし G と H が次の stiff という性質を満たしているとき，$N(G) \cong N(H)$ となることから $G \cong H$ が成立する．グラフ G が **stiff** であるとは，任意の相異なる G の 2 頂点 v と w に対し，$N(v) \not\subset N(w)$ が成立することをいう．G と H がともに stiff であり，さらに $N(G) \cong N(H)$ ならば $G \cong H$ が成立する．

これらの準備の下で，定理 2.6，すなわち $\chi(G_i(n,k)) = n - 2k + 2$ となることは次のように示される：

定理 *2.6* の証明. まず $K_2 \times G_i(n,k) \cong H(n,k) = K_2 \times K(n,k)$ であるから，命題 4.6 より $N(G_i(n,k)) \cong N(K(n,k))$ である．すなわち定理 4.5 より $N(G_i(n,k))$ は $(n-2k-1)$-連結であり，定理 4.4 より $\chi(G_i(n,k)) \geq n - 2k + 2$ となる．

次に $\chi(G_i(n,k)) \leq n - 2k + 2$ を示すために，$(n-2k+2)$-彩色を具体的に構成する．写像

$$f \colon V(H(n,k)) = \{1,2\} \times \binom{[n]}{k} \to \{2k-1, 2k, \cdots, n\}$$

を

$$f(i,\sigma) = \max\{\sigma \cup \{2k-1\}\}$$

により定義すると，$G_i(n,k)$ の構成から f は写像

$$\overline{f} \colon V(G_i(n,k)) \to \{2k-1, 2k, \cdots, n\}$$

を誘導し，さらに $(\sigma,\tau) \in E(G_i(n,k))$ ならば $\overline{f}(\sigma) \neq \overline{f}(\tau)$ を満たすことがわかる．すなわち $G_i(n,k)$ は $(n-2k+2)$-彩色を持ち，$\chi(G_i(n,k)) \leq n - 2k + 2$ が成立する． □

参考文献

[1] E. Boros, V. Gurvich, I. Zverovich: Neighborhood hypergraphs of bipartite graphs, *J. Graph Theor.* **58** (2008), 69-95.

[2] B. Brešar, W. Imrich, S. Klavžar, B. Zmazek: Hypercubes as direct products, *SIAM J. Discrete Math.* **18** (2005), 779-786.

[3] C. Godsil, G.F. Royle, Algebraic graph theory, Graduate texts in Mathematics Book 207, (2001).

[4] A. Hatcher, Algebraic Topology. (2000).

[5] P. Hell, J. Nešetřil, Graphs and Homomorphisms, Oxford lecture series in mathematics and its applications - 28 (2004).

[6] W. Imrich, T. Pisanski: Multiple Kronecker covering graphs, *Eur. J. Combin.* **29** (2008), 1116-1122.

[7] M. Kneser, Aufgabe 300, *Jahresber. Deutsch. Math.-Verein* **68** (1955) 27.

[8] D.N. Kozlov. Combinatorial algebraic topology. Springer, Berlin, Algorithms and Computation in Mathematics, Vol. 21. 2008.

[9] M. Krnc, T. Pisanski: Characterization of generalized Petersen graphs that are Kronecker covers, *Discrete Math. Theor.* **21** (2019)

[10] L. Lovász, On the cancellation law among finite relational structures, *Period. Math. Hungar.* **1** (1971) 145-156.

[11] L. Lovász, Kneser's conjecture, chromatic number, and homotopy, *J. Combin. Ser. A,* **25** (1978) 319-324.

[12] J. Matoušek, Using the Borsuk-Ulam theorem, Springer-Verlag, Berlin (2003).

[13] T. Matsushita, Fundamental groups of neighborhood complexes, *Journal of Mathematical Sciences, the University of Tokyo.* **24** (2017) 351-353.

[14] T. Matsushita, Neighborhood complexes and Kronecker double coverings, to appear in *Osaka J. Math.*

[15] T. Matsushita, Graphs whose Kronecker covers are bipartite Kneser graphs, *Discrete Math.* Volume 344, Issue 4, April 2021, 112264.

[16] S.M. Mirafzal: *The automorphism group of the bipartite Kneser graph,* Proc.: Math. Sci. **129** (2019), Article number 34.

TVERBERG'S THEOREM FOR CELL COMPLEXES

SHO HASUI, DAISUKE KISHIMOTO, MASAHIRO TAKEDA, AND MITSUNOBU TSUTAYA

Abstract. The topological Tverberg theorem states that given any continuous map $f\colon \Delta^{(d+1)(r-1)} \to \mathbb{R}^d$, there are pairwise disjoint faces $\sigma_1, \dots, \sigma_r$ of $\Delta^{(d+1)(r-1)}$ such that $f(\sigma_1) \cap \cdots \cap f(\sigma_r) \neq \emptyset$ whenever r is a prime power. We generalize this theorem to a continuous map from a certain CW complex into a Euclidean space.

1. Introduction

Let $d \geq 1$ and $r \geq 2$ be integers. Tverberg's theorem states that for any given $(d+1)(r-1)+1$ points in $\mathbb{R}^d$, there is a partition of points into r subsets whose convex hulls intersect. This theorem has been of great interest in combinatorics for more than 50 years. Clearly, Tverberg's theorem can be restated in terms of an affine map from a $(d+1)(r-1)$-simplex into $\mathbb{R}^d$. The topological Tverberg theorem replaces an affine map in Tverberg's theorem by a continuous maps: for any continuous map $f\colon \Delta^{(d+1)(r-1)} \to \mathbb{R}^d$, there are pairwise disjoint faces $\sigma_1, \dots, \sigma_r$ of the simplex $\Delta^{(d+1)(r-1)}$ such that

$$f(\sigma_1) \cap \cdots \cap f(\sigma_r) \neq \emptyset$$

whenever r is a prime power. This was first proved by Bárány, Shlosman and Szűcs [2] when r is a prime, and later by Özaydin [12] and Volovikov [13], independently, when r is a prime power. Remark that Frick [6] proved that the result does not hold unless we assume r is a prime power.

We will consider:

Problem 1.1. Can we replace a simplex in the topological Tverberg theorem by other CW complexes?

There was a relevant problem posed by Tverberg [7]: can we replace a simplex by a polytope in the topological Tverberg theorem? This is affirmatively solved because the boundary of any d-polytope is a refinement of the boundary of a d-simplex as proved by Grünbaum [8, p. 200]. So this is not an essential generalization of the topological Tverberg theorem. The problem was also studied by Bárány, Kalai and Meshulam[1] and Blagojević, Haase and Ziegler [3] for matroid complexes.

A *face* of a CW complex will mean a closed cell. For pairwise disjoint faces $\sigma_1, \dots, \sigma_k$ of a CW complex X, let $X(\sigma_1, \dots, \sigma_k)$ denote a subcomplex of X consisting of faces disjoint from $\sigma_1, \dots, \sigma_k$.

2010 *Mathematics Subject Classification.* 52A37, 55R80.

Key words and phrases. topological Tverberg theorem, discretized configuration space, homotopy colimit.

A space Y is called *n-acyclic* if Y is non-empty and $\widetilde{H}_*(Y) = 0$ for $* \leq n$, where $n \geq 0$. Clearly, n-connected spaces are n-acyclic. A non-empty space is called a (-1)-acyclic.

Definition 1.2. We say that a regular CW complex X is *r-complementary n-acyclic* if $X(\sigma_1, \dots, \sigma_k)$ is non-empty and $(n - \dim \sigma_1 - \cdots - \dim \sigma_k)$-acyclic for each pairwise disjoint faces $\sigma_1, \dots, \sigma_k$ with $\dim \sigma_1 + \cdots + \dim \sigma_k \leq n + 1$, where $k = 0, 1, \dots, r$.

Now we state the main theorem.

Theorem 1.3. *Let r be a prime power. If X is an $(r-1)$-complementary $(d(r-1)-1)$-acyclic regular CW complex, then for any continuous map $f\colon X \to \mathbb{R}^d$, there are pairwise disjoint faces $\sigma_1, \dots, \sigma_r$ of X such that*

$$f(\sigma_1) \cap \cdots \cap f(\sigma_r) \neq \emptyset.$$

We can easily see that every simplicial d-sphere is 1-complementary $(d-1)$-acyclic. Then we obtain a generalization of the topological Radon theorem, i.e. the topological Tverberg theorem for $r = 2$, which is interesting because neither convexity nor antipodality of a simplicial sphere is demanded.

Corollary 1.4. *Let X be a simplicial d-sphere. Then for any continuous map $f\colon X \to \mathbb{R}^d$ there are disjoint faces σ_1, σ_2 of X such that*

$$f(\sigma_1) \cap f(\sigma_2) \neq \emptyset.$$

Grünbaum and Sreedharan [9] gave a simplicial sphere which is not polytopal, the boundary of a polytope, and now most simplicial spheres in higher dimensions are known to be non-polytopal. Thus Corollary 1.4 does not follow from the topological Radon theorem, so Theorem 1.3 is a proper generalization of the topological Tverberg theorem.

Acknowledgement. The authors were partly supported by JSPS KAKENHI No. 18K13414 (Hasui), No. 17K05248 (Kishimoto), and No. 19K14535 (Tsutaya).

2. Proof of Theorem 1.3

2.1. **Topological method.** We will apply the so-called topological method in combinatorics. Let X be a regular CW complex. For a positive integers r, we define the discrete configuration space $\mathrm{Conf}_r(X)$ as a subcomplex of the direct product X^r consisting of faces $\sigma_1 \times \cdots \times \sigma_r$ of X^r, where $\sigma_1, \dots, \sigma_r$ are pairwise disjoint faces of X. Note that the canonical action of the symmetric group Σ_r on X^r restricts to $\mathrm{Conf}_r(X)$.

Let the symmetric group Σ_r act on $(\mathbb{R}^d)^r$ by permutation of $\mathbb{R}^d$. Then the fixed point set of this action is the diagonal set

$$\Delta = \{(x_1, \dots, x_r) \in (\mathbb{R}^d)^r \mid x_1 = \cdots = x_r\}.$$

Clearly, $(\mathbb{R}^d)^r - \Delta$ is homotopy equivalent to $S^{d(r-1)-1}$. The following lemma is immediate from the definition of $\mathrm{Conf}_r(X)$.

Lemma 2.1. *Let X be a regular CW complex. If there is a map $f\colon X \to \mathbb{R}^d$ such that $f(\sigma_1) \cap \cdots \cap f(\sigma_r) = \emptyset$ for every pairwise disjoint faces $\sigma_1, \ldots, \sigma_r$ of X, then there is a Σ_r-equivariant map*

$$\bar{f}\colon \mathrm{Conf}_r(X) \to (\mathbb{R}^d)^r - \Delta.$$

Let $r = p^n$ for a prime p. The action of $(\mathbb{Z}/p)^n$ on $(\mathbb{Z}/p)^n$ itself given by

$$(\mathbb{Z}/p)^n \times (\mathbb{Z}/p)^n \to (\mathbb{Z}/p)^n, \quad (x, y) \mapsto x + y$$

is faithful, so we get an embedding $(\mathbb{Z}/p)^n \to \Sigma_r$. In particular, we get actions of $(\mathbb{Z}/p)^n$ on $\mathrm{Conf}_r(X)$ and $(\mathbb{R}^d)^r$. The following Borsuk-Ulam type result is proved by Blagojević and Ziegler [4, Proof of Theorem 3.11] when Y is of the homotopy type of a $d(r-1)$-sphere. We can easily see that the proof of Blagojević and Ziegler works verbatim when Y is $(d(r-1)-1)$-acyclic.

Proposition 2.2. *If Y is a $(d(r-1)-1)$-acyclic $(\mathbb{Z}/p)^n$-space where $r = p^n$, then there is no $(\mathbb{Z}/p)^n$-equivariant map $Y \to (\mathbb{R}^d)^r - \Delta$.*

By Lemma 2.1 and Proposition 2.2, we get:

Corollary 2.3. *Let X be a regular CW complex such that $\mathrm{Conf}_r(X)$ is $(d(r-1)-1)$-acyclic. Then there are pairwise disjoint faces $\sigma_1, \ldots, \sigma_r$ of X such that*

$$f(\sigma_1) \cap \cdots \cap f(\sigma_r) \neq \emptyset.$$

Then for proving Theorem 1.3, it remains to show that $\mathrm{Conf}_r(X)$ is non-empty and n-acyclic whenever X is $(r-1)$-complementary n-acyclic. To this end, we describe $\mathrm{Conf}_r(X)$ as a homotopy colimit by modifying the description of $\mathrm{Conf}_r(\Delta^n)$ in [10, Theorem 15]. We will construct a spectral sequence computing the homology of a homotopy colimit from a poset, which is essentially the same as the Bousfield-Kan spectral sequence if the underlying poset is the face poset of a regular CW complex. Then we compute the acyclicity of $\mathrm{Conf}_r(X)$ by this spectral sequence.

2.2. **Homotopy colimit.** First, we recall from [14] the definition of the homotopy colimit of a functor from a poset. Let P be a poset and $F\colon P \to \mathbf{Top}$ be a functor, where we understand a poset P as a category such that $x \geq y$ in P is the unique morphism $x \to y$. Let $\Delta(P)$ denote the order complex of a poset P. For $x < y \in P$, let $\iota_{x,y}\colon \Delta(P_{\leq x}) \to \Delta(P_{\leq y})$ denote the inclusion. The homotopy colimit $\operatorname{hocolim} F$ is defined as the coequalizer of the maps

$$f, g\colon \coprod_{x<y\in P} \Delta(P_{\leq x}) \times F(y) \to \coprod_{x\in P} \Delta(P_{\leq x}) \times F(x)$$

where

$$f = \coprod_{x<y\in P} 1_{\Delta(P_{\leq x})} \times F(y > x) \quad \text{and} \quad g = \coprod_{x<y\in P} \iota_{x,y} \times 1_{F(y)}.$$

Next, we describe $\mathrm{Conf}_r(X)$ as a homotopy colimit. We will use the following property of regular CW complexes. See [11, Chapter III, Theorem 1.6] for the proof.

Lemma 2.4. *Let X be a regular CW complex and let P denote the face poset of X. Then there is a homeomorphism*

$$\Delta(P) \xrightarrow{\cong} X$$

which restricts to $\Delta(P_{\leq\sigma}) \xrightarrow{\cong} \sigma$ for each face σ of X.

Let X be a regular CW complex, and let P denote the face poset of X. For $\sigma < \tau \in P$, let

$$\theta_{\sigma,\tau}\colon \operatorname{Conf}_{r-1}(X(\tau)) \to \operatorname{Conf}_{r-1}(X(\sigma)) \quad \text{and} \quad \iota_{\sigma,\tau}\colon \sigma \to \tau$$

denote the inclusions. Then $\operatorname{Conf}_r(X)$ is given by the coequalizer of the two maps

$$f, g\colon \coprod_{\sigma<\tau\in P} \sigma \times \operatorname{Conf}_{r-1}(X(\tau)) \to \coprod_{\sigma\in P} \sigma \times \operatorname{Conf}_{r-1}(X(\sigma))$$

where

$$f = \coprod_{\sigma<\tau\in P} 1_\sigma \times \theta_{\sigma,\tau} \quad \text{and} \quad g = \coprod_{\sigma<\tau\in P} \iota_{\sigma,\tau} \times 1_{\operatorname{Conf}_{r-1}(X(\tau))}.$$

Define a functor $F\colon P \to \mathbf{Top}$ by

$$F(\sigma) = \operatorname{Conf}_{r-1}(X(\sigma)) \quad \text{and} \quad F(\sigma > \tau) = \theta_{\sigma,\tau}.$$

Then by Lemma 2.4 we get:

Proposition 2.5. $\operatorname{Conf}_r(X) = \operatorname{hocolim} F$.

We can construct the following spectral sequence, which is essentially the same as the Bousfield-Kan spectral sequence [5, XII 4.5].

Theorem 2.6. *Let $F\colon P \to \mathbf{Top}$ be a functor where P is the face poset of a regular CW complex. Then there is a spectral sequence*

$$E^1_{p,q} \cong \bigoplus_{\dim\sigma=p} H_q(F(\sigma)) \;\Rightarrow\; H_{p+q}(\operatorname{hocolim} F).$$

Applying the above spectral sequence, we get:

Lemma 2.7. *Let P be the face poset of a regular CW complex X, and let $F\colon P \to \mathbf{Top}$ be a functor. If $F(\sigma)$ is $(n - \dim\sigma)$-acyclic for each face $\sigma \in P$ of dimension $\leq n+1$, then there is an isomorphism for $* \leq n$*

$$H_*(\operatorname{hocolim} F) \cong H_*(X).$$

We calculate the acyclicity of $\operatorname{Conf}_r(X)$.

Proposition 2.8. *If X is an $(r-1)$-complementary n-acyclic regular CW complex, then $\operatorname{Conf}_r(X)$ is n-acyclic.*

Proof. We prove $\mathrm{Conf}_r(X)$ is n-acyclic by induction on r. For $r = 1$, $\mathrm{Conf}_1(X) = X$, which is n-acyclic by assumption. Assume that $\mathrm{Conf}_{r-1}(Y)$ is n-acyclic for any $(r-2)$-complementary n-acyclic space Y. Consider the functor F in Proposition 2.5. Then F is a functor from the face poset of X and

$$F(\sigma) = \mathrm{Conf}_{r-1}(X(\sigma))$$

for each face σ of X. Since $X(\sigma)$ is $(r-2)$-complementary $(n - \dim\sigma)$-acyclic for $\dim\sigma \leq n+1$, it follows from the induction assumption that $F(\sigma)$ is $(n-\dim\sigma)$-acyclic for $\dim\sigma \leq n+1$. Then by Lemmas 2.4, 2.7 and Proposition 2.5, $\mathrm{Conf}_r(X)$ is non-empty and there is an isomorphism

$$H_*(\mathrm{Conf}_r(X)) \cong H_*(X)$$

for $* \leq n$. Thus since X is n-acyclic, $\mathrm{Conf}_r(X)$ is n-acyclic, completing the proof. □

Now we are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Combine Corollary 2.3 and Proposition 2.8. □

3. Index of a free group action

Discretized configuration spaces are of particular interest, and they have a lot of applications in topology, geometric group theory, combinatorics, and applied mathematics. Here, we pose a possible future direction of the study of discretized configuration spaces along the line of the topological method.

Let G be a discrete group, and let $E_nG = \overbrace{G * \cdots * G}^{n+1}$. Then G acts freely on E_nG, and we let $B_nG = E_nG/G$. There are filtrations

$$E_1G \subset \cdots \subset E_nG \subset E_{n+1}G \subset \cdots \quad \text{and} \quad B_1G \subset \cdots \subset B_nG \subset B_{n+1}G \subset \cdots .$$

Let $EG = \bigcup_{n\geq 1} E_nG$ and $BG = \bigcup_{n\geq 1} B_nG$. Recall that the space BG is called the classifying space of G, and the principal bundle $G \to EG \to BG$ is called the universal G-bundle. Let X be a free G-complex. Then there is a pullback diagram

$$\begin{array}{ccc} X & \longrightarrow & EG \\ \downarrow & & \downarrow \\ X/G & \longrightarrow & BG \end{array}$$

such that the map $X/G \to BG$ is unique, up to homotopy. Then the map $X \to EG$ is unique, up to G-homotopy. We recall the index of a free G-action.

Definition 3.1. Let G be a finite group, and let X be a free G-complex. The *index* of X, denoted $\mathrm{ind}(X)$, is defined to be the least integer n such that the map $X \to EG$ factors through E_nG, up to G-homotopy.

The following properties of the index are fundamental.

Lemma 3.2. *Let G be a finite group, and let X, Y be free G-complexes.*

(1) *If there is a G-map $X \to Y$, then*

$$\mathrm{ind}(X) \leq \mathrm{ind}(Y).$$

(2) *There is an inequality*

$$\mathrm{acyc}(X) < \mathrm{ind}(X) \leq \mathrm{hodim}(X).$$

where $\mathrm{acyc}(X)$ *and* $\mathrm{hodim}(X)$ *denote the acyclicity and the homotopy dimension of X, respectively.*

The above lemma implies that the index of a free G-space is an invariant better than the acyclicity when we apply the topological method as in Section 2. Moreover, the index is of independent interest in topology and transformation group theory. So we pose:

Problem 3.3. Compute the index of $\mathrm{Conf}_r(X)$ acted upon freely by $\mathbb{Z}/r$ for r prime.

The index of a free G complex X is equal to the LS category of the map $X/G \to BG$. So we also pose the following problem, which is of particular interest in algebraic topology and applied topology.

Problem 3.4. Compute the LS category and the topological complexity of $\mathrm{Conf}_r(X)$

References

[1] I. Bárány, G. Kalai, and R. Meshulam, A Tverberg type theorem for matroids, A journey through discrete mathematics, 115-121, Springer, Cham, 2017.

[2] I. Bárány, S. B. Shlosman, and A. Szűcs, On a topological generalization of a theorem of Tverberg, J. London Math. Soc. (2) **23** (1981), no. 1, 158-164.

[3] P.V.M. Blagojević, A. Haase, and G.M. Ziegler, Tverberg-type theorems for matroids: a counterexample and a proof. Combinatorica **39** (2019), no. 3, 477-500.

[4] P.V.M. Blagojević and G.M. Ziegler, Beyond the Borsuk-Ulam theorem: The topological Tverberg story, A journey through discrete mathematics, 273-341, Springer, Cham, 2017.

[5] A.K. Bousfield and D.M. Kan, Homotopy Limits, Completions and Localizations, Lecture Notes in Mathematics **304**, Springer-Verlag, 1972.

[6] F. Frick, Counterexamples to the topological Tverberg conjecture, Oberwolfach Reports **12** (2015), no. 1, 318-321.

[7] P.M. Gruber and R. Schneider, Problems in geometric convexity, Contributions to geometry (Proc. Geom. Sympos., Siegen, 1978), Birkhäuser, Basel-Boston, Mass., 1979, pp. 255-278.

[8] B. Grünbaum, Convex Polytopes, Graduate Texts in Mathematics **221**, Springer-Verlag, New York, second edition, 2003.

[9] B. Grünbaum and V.P. Sreedharan, An enumeration of simplicial 4-polytopes with 8 vertices, J. Comb. Theory **2** (1967), 437-465.

[10] K. Iriye and D. Kishimoto, Hom complexes and hypergraph colorings, Topology Appl. **160** (2013), no. 12, 1333-1344.

[11] A.T. Lundell and S. Weingram, The Topology of CW Complexes, van Nostrand, New York, 1969.

[12] M. Özaydin, Equivariant maps for the symmetric group, 1987, Unpublished preprint, University of Winsconsin-Madison.

[13] A.Y. Volovikov, On a topological generalization of Tverberg's theorem (Russian), Mat. Zametki **59** (1996), no. 3, 454-456; English transl., Math. Notes **59** (1996), no. 3-4, 324-325.

[14] G. Ziegler and R. Živaljević, Homotopy types of subspace arrangements via diagrams of spaces, Math. Ann. **295** (1993) 527-548.

Department of Mathematical Sciences, Osaka Prefecture University, Sakai, 599-8531, Japan
Email address: s.hasui@ms.osakafu-u.ac.jp

Department of Mathematics, Kyoto University, Kyoto, 606-8502, Japan
Email address: kishi@math.kyoto-u.ac.jp

Department of Mathematics, Kyoto University, Kyoto, 606-8502, Japan
Email address: takeda.masahiro.87u@st.kyoto-u.ac.jp

Faculty of Mathematics, Kyushu University, Fukuoka 819-0395, Japan
Email address: tsutaya@math.kyushu-u.ac.jp

ユークリッド空間上の距離集合の分類問題について

–$\mathbb{R}^8$ 上の最良な 2-距離集合の一意性–

篠原雅史（滋賀大学教育学部）[1]

1　はじめに

$\mathbb{R}^d$ の有限部分集合 X に対し，X の相違なる 2 点間の距離がちょうど s 種類であるときに，X を s-距離集合という．つまり，

$$A(X) = \{d(x,y) \mid x,y \in X, x \neq y\}$$

と定め，$|A(X)| = s$ のとき，X を s-距離集合という．ここで，$d(x,y)$ は二点 x,y のユークリッド距離を表す．次元 d と距離の種類 s に対して，大きな頂点数を持つ s-距離集合 $X \subset \mathbb{R}^d$ を特徴付けたいというのが距離集合における主な研究目標である．ここで，相似変換で移りあう 2 つの距離集合を同型とし，同一視して考える．

$\mathbb{R}^d$ 上の s-距離集合の頂点数の最大値を $g_s(d)$ で表すことにする．また，その最大値を達成する s-距離集合を最良な s-距離集合という．

Kelly[6], Croft[4], Lisoněk[8] らにより次の Table 1 のように最大値が求められている．

d	1	2	3	4	5	6	7	8
$g_2(d)$	3	5	6	10	16	27	29	45
最良なものの個数	1	1	6	1	1	1	1	≥ 1

Table 1: 知られている最大値 $g_2(d)$ の値と最良なものの個数

$\mathbb{R}^d$ 上の s-距離集合の頂点数の上界について次の定理が知られている．

Theorem 1.1 (Bannai-Bannai-Stanton[1], Blokhuis[3])**.** $\mathbb{R}^d$ 上の s-距離集合 X に対し次が成り立つ．

$$|X| \leq \binom{d+s}{s}$$

$d = 1$ のときには等間隔に並んだ $s+1$ 点が，$s = 1$ のときには $\mathbb{R}^d$ 上の正単体の $d+1$ 点がそれぞれこの上界を満たす例となっている．一方，$d \geq 2$, $s \geq 2$ に対し，この上界を達成するもので知られているものは，Lisoněk により構成された $\mathbb{R}^8$ 上の 45 点 2-距離集合ただ 1 つのみである．本稿では $\mathbb{R}^8$ 上で 45 点 2-距離集合がこの 1 つに限られることを示す．なお，本研究は須田庄氏（防衛大），野崎寛氏（愛知教育大）との共同研究に基づいている．

2　Lisoněk の 2-距離集合

異なる実数 a, b と自然数 k に対し，座標の中に a が k 個，b が $n-k$ 個ある $\mathbb{R}^n$ の元全体の集合を $(a^k, b^{n-k})^P$ で表す．特に，$(a^k, b^{n-k})^P$ は $\binom{n}{k}$ 個の元を持つ．

一方，

$$J(n,s) := \{Y \subset \{1,2,\ldots,n\} \mid |Y| = s\}$$

[1]supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (C) 18K03396

とおくと，$(a^s, b^{n-s})^P$ と $J(n,s)$ の間の自然な 1 対 1 対応がある．本稿における幾つかの例に対し，この対応を意識して距離考えると計算しやすい．

ここで，$\mathbb{R}^9$ の 2 つの部分集合 X_1, X_2 を

$$X_1 = \left(1^1, 0^8\right)^P, \quad X_2 = \left(\left(-\frac{2}{3}\right)^2, \left(\frac{1}{3}\right)^7\right)^P$$

とする．このとき，$L_{45} = X_1 \cup X_2$ とすると $|L_{45}| = 9 + 36 = 45$ となる．また，L_{45} の各点は成分和が 1 となる $\mathbb{R}^9$ の超平面上にあるので，$\mathbb{R}^8$ の部分集合とみなせる．

ここで，先ほどの 1 対 1 対応を考えると，X_1, X_2 はそれぞれ,

$$X_1 = \{p_i \mid 1 \le i \le 9\}, \quad X_2 = \{p_{j,k} \mid 1 \le j < k \le 9\}$$

と表すことができる．このとき，$i \neq j$ に対し $d(p_i, p_j) = \sqrt{2}$ となる．また,

$$d(p_i, p_{j,k}) = \begin{cases} \sqrt{2} & (i \in \{j,k\}) \\ 2 & (i \notin \{j,k\}) \end{cases}, \quad d(q_{i,j}, q_{k,l}) = \begin{cases} 0 & (|\{i,j\} \cap \{k,l\}| = 2) \\ \sqrt{2} & (|\{i,j\} \cap \{k,l\}| = 1) \\ 2 & (|\{i,j\} \cap \{k,l\}| = 0) \end{cases}$$

より

$$A(L_{45}) = \{\sqrt{2}, 2\}$$

となるので，L_{45} は $\mathbb{R}^8$ 上の 45 点 2-距離集合となる．これが Lisoněk の 2-距離集合である．

Lisoněk の 2-距離集合は，$\mathbb{R}^d$ 上の s-距離集合の頂点数の上界 $\binom{d+s}{s}$ を達成する例となっているが，はじめに述べたように，これは非自明な例としてただ一つ知られているものである．Lisoněk の 2-距離集合にならって，Bannai-Sato-Shigezumi[2] や Nozaki-Shinohara[11] などにより，よい s-距離集合の構成が試みられてているが，Lisoněk の 2-距離集合の他に上界を達成するものがあるかは，興味を持たれている未解決問題である．

次の定理は，本稿の主結果である．

Theorem 2.1 (Nozaki-Shinohara-Suda)**.** $\mathbb{R}^8$ 上の 45 点 2-距離集合は L_{45} に限られる．

3 グラフと距離集合

$X = \{p_1, p_2, \ldots, p_n\} \subset \mathbb{R}^d$ に対し，X の 2 点間の距離を成分に持つ行列を

$$D_X = (d(p_i, p_j))_{1 \le i,j \le n}$$

で定め，X の距離行列という．また，距離行列 $D = (d_{i,j})_{1 \le i,j \le n}$ に対して,

$$C_D = \left(\frac{d_{i,n}^2 + d_{j,n}^2 - d_{i,j}^2}{2}\right)_{1 \le i,j \le n-1}$$

とする．

Theorem 3.1 ([9, 12])**.** M を対角成分が 0 で他の成分が非負であるような実対称行列とする．$M = D_X$ となる $X \subset \mathbb{R}^d$ が存在するための必要十分条件は C_M が半正定値で $\operatorname{rank} C_M \le d$ となることである．

Example 3.2. $d(p_1,p_2)=d(p_2,p_3)=d(p_3,p_4)=d(p_1,p_2)=1, d(p_1,p_3)=d(p_2,p_4)=\sqrt{\alpha}$ を満たす 4 点集合 $X=\{p_1,p_2,p_3,p_4\}$ について考える．

$$M=\begin{pmatrix} 0 & 1 & \sqrt{\alpha} & 1 \\ 1 & 0 & 1 & \sqrt{\alpha} \\ \sqrt{\alpha} & 1 & 0 & 1 \\ 1 & \sqrt{\alpha} & 1 & 0 \end{pmatrix}, \quad C=\frac{1}{2}\begin{pmatrix} 2 & \alpha & 2-\alpha \\ \alpha & 2\alpha & \alpha \\ 2-\alpha & \alpha & 2 \end{pmatrix}$$

より，

$$|C|=2\alpha^2(\alpha-2)$$

となる．

- $\alpha=0$ のとき，$\operatorname{rank} C=1$ となる．このとき，4 点がつぶれて 2 点 $p_1(=p_3)$, $p_2(=p_4)$ が $\mathbb{R}^1$ 上にある．
- $\alpha=2$ のとき，$\operatorname{rank} C=2$ となる．このとき，4 点が $\mathbb{R}^2$ 上で正方形となる．
- $0<\alpha<2$ のとき，X は $\mathbb{R}^3$ 上にある（α の変化に応じて，X が連続変形する）．

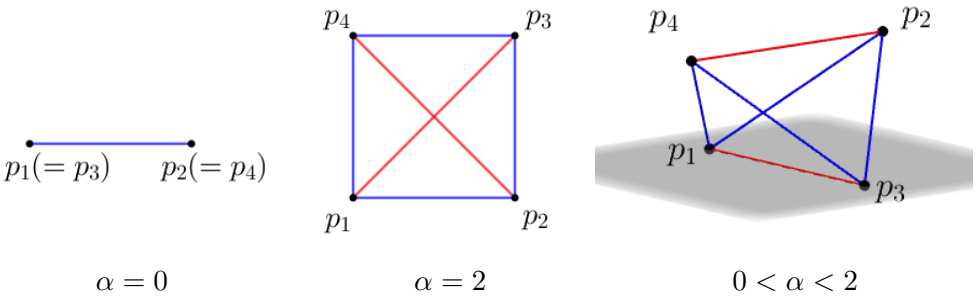


Figure 1: 距離行列とその実現

Theorem 3.1 より，距離行列が与えられたら，その距離行列を持つ点配置がどの次元に実現できるかを知ることができる．また，Example 3.2 のように，2-距離集合に対して 1 つの距離を 1 にすることで，グラフと距離の比 α が分かると距離行列が定まり，実現される次元が確定する．

2-距離集合を特徴づける際，次の Larman-Rogers-Seidel の定理は非常に効果的である．

Theorem 3.3 ([7, 9])**.** $X\subset\mathbb{R}^d$ を $2d+2$ 点以上の 2-距離集合とし，$A(X)=\{\alpha,\beta\}$ とする．このとき，ある整数 $k\le 1/2+\sqrt{d/2}$ が存在して，$\alpha^2/\beta^2=(k-1)/k$ となる．

特に，$d=8$ のとき $|X|\ge 18$ ならば，$\alpha^2/\beta^2=2$ となる．このことより，$\mathbb{R}^8$ 上の 45-点 2-距離集合を分類する際，グラフのみを動かして，どのような 45 頂点のグラフが $\mathbb{R}^8$ に実現できるかを考えればよいことが分かる．当然，45 頂点のグラフ全てに対してその判定を行う訳にはいかないので，何かしらの工夫が必要になってくる．次節以降でその詳細について考えていく．

4　ラムゼー数と 2-距離集合

ここでは，ラムゼー数を定義して，45 点 2-距離集合の構造をグラフ的観点からみてみる．$G=(V,E)$ を単純グラフとする．$W(\subset V)$ の任意の 2 頂点が隣接しているとき（resp. 隣接していないとき）

W をクリーク（resp. 独立集合）という．G のクリーク（resp. 独立集合）の頂点数の最大値を $\omega(G)$（resp. $\alpha(G)$）で表す．2 つの自然数 s,t に対し，任意の n 頂点のグラフが $\alpha(G) \geq s$ または $\omega(G) \geq t$ となるような n の最小値を $R(s,t)$ で表しラムゼー数とよばれる．ラムゼー数については，$R(3,m)$ については次の Table 4 のようになることが知られている．

m	3	4	5	6	7	8	9
R(3,m)	6	9	14	18	23	28	36

Table 2: ラムゼー数 $R(3,m)$ の値

Lemma 4.1. G を位数 45 の単純グラフとするとき，G は K_9 を含むか $K_{3,3,3}$ の全域部分グラフを含む．

Proof. 位数 45 グラフ $G=(V,E)$ が K_9 を含まないとして，G が $K_{3,3,3}$ の部分グラフを含むことを示す．G は K_9 を含まないので $R(3,9)=36<45$ より G の 3 点独立集合 W_1 が存在する．$G_1=(V_1,E_1)$ を $V\setminus W_1$ で誘導される G の部分グラフとする．G_1 は K_9 を含まないので $R(3,9)=36<42$ より G_1 の 3 点独立集合 W_2 が存在する．$G_2=(V_2,E_2)$ を $V_1\setminus W_2$ で誘導される G_1 の部分グラフとする．G_2 は K_9 を含まないので $R(3,9)=36<39$ より G_2 の 3 点独立集合 W_3 が存在する．このとき，$W_1\cup W_2\cup W_3$ で誘導される G の部分グラフは $K_{3,3,3}$ の部分グラフとなる． □

Larman-Rogers-Seidel の定理により，ここでの 2-距離集合 X は $A(X)=\{\sqrt{2},2\}$ としてよい．ここで，X に対応する単純グラフ $G(X)=(V,E)$ を次で定義し，X の表現グラフという．

$$\begin{cases} V=X \\ \{x,y\}\in E \Longleftrightarrow d(x,y)=\sqrt{2} \end{cases}$$

X の表現グラフに Lemma 4.1 を適用すると，$G(X)$ は K_9 を含むか $K_{3,3,3}$ の全域部分グラフを含む．このことを用いて分類を進めていく．ここで，L_{45} の 9 点部分集合で非同型なものがたくさんあることから，これらのグラフの中には 45 頂点まで増やせるグラフがたくさん含まれていることに注意する．

次節では $G(X)$ が K_9 を含む場合について考える．

5 正単体を含む 2-距離集合

Nozaki-Shinohara[11] は，$\mathbb{R}^d$ において，正単体を含む 2-距離集合の特徴付けを行った．特に，$\mathbb{R}^8$ 上の 2-距離集合 X で $|X|\geq 18(=2d+2)$ となるとき，次の捕題がなりたつ．

Lemma 5.1. $\mathbb{R}^9$ 上の超平面 $\pi:\{(x_1,x_2,\ldots,x_9)\in\mathbb{R}^9 \mid x_1+x_2+\cdots+x_9=1\}$ 上に正単体 $X_0=\left(1^1,0^8\right)^P$ を取り，π 上の 2-距離集合 X が X_0 を含むとする．$|X|\geq 18$ とするとき，次のいずれかが成り立つ．

(i) $A(X)=\{1,\sqrt{2}\}$ となり，

$$X\setminus X_0\subset\left(\left(-\frac{1}{3}\right)^1,\left(\frac{1}{6}\right)^8\right)^P\cup\left(\left(-\frac{1}{6}\right)^4,\left(\frac{1}{3}\right)^5\right)^P.$$

(ii) $A(X) = \{\sqrt{2}, 2\}$ となり，

$$X \setminus X_0 \subset \left(\left(-\frac{2}{3}\right)^2, \left(\frac{1}{3}\right)^7\right)^P \cup \left(\left(-\frac{1}{3}\right)^5, \left(\frac{2}{3}\right)^4\right)^P.$$

(i) のときは $|X| \leq 24$ となることが確認できるので，ここでは (ii) の場合について考える．(実際は，短い距離の K_9 が含まれることを確認すればよいのでこの部分を省略できる．)

捕題より，$X = X_0 \cup X_1 \cup X_2$ が 2-距離集合となるような

$$X_1 \subset \left(\left(-\frac{2}{3}\right)^2, \left(\frac{1}{3}\right)^7\right)^P, \quad X_2 \subset \left(\left(-\frac{1}{3}\right)^5, \left(\frac{2}{3}\right)^4\right)^P$$

で，$|X_1| + |X_2| = 36$ となるものを見つければよい．ここで，1 対 1 対応

$$X_1 \leftrightarrow \mathcal{F}_1 \subset J(9,2), \quad X_2 \leftrightarrow \mathcal{F}_2 \subset J(9,5)$$

を考える．$S \in \mathcal{F}_1$ と $T \in \mathcal{F}_2$ に対し，

$$\begin{cases} d(p_S, p_T) = \sqrt{2} \iff |S \cap T| = 2, \\ d(p_S, p_T) = 2 \iff |S \cap T| = 1 \end{cases}$$

となるので，$|S \cap T| \in \{1, 2\}$ となる必要がある．他の場合も同様にして，$|S \cap T|$ は次の Table 5 のようになる必要がある．ここで，青色は距離 $\sqrt{2}$, 赤色は距離 2 にそれぞれ対応している．

	$\mathcal{F}_0 = J(9,1)$	$\mathcal{F}_1 \subset J(9,2)$	$\mathcal{F}_2 \subset J(9,5)$
$\mathcal{F}_0$	0	0, 1	0, 1
$\mathcal{F}_1$		0, 1	1, 2
$\mathcal{F}_2$			3, 4

Table 3: X が 2-距離集合になるための $|S \cap T|$ の条件

上記の条件を満たす $\mathcal{F}_1, \mathcal{F}_2$ として次の 2 つの例がある．

Example 5.2.

(i) $|\mathcal{F}_1| = 36$, $|\mathcal{F}_2| = 0$ となる例．

$$\mathcal{F}_2 = J(9,2), \quad \mathcal{F}_3 = \emptyset.$$

(ii) $|\mathcal{F}_1| = 3 + 18 = 21$, $|\mathcal{F}_2| = 15$ となる例．

$$\mathcal{F}_2 = \{\{i,j\} \mid 1 \leq i < j \leq 3\} \cup \{\{i,j\} \mid 1 \leq i \leq 3, 4 \leq j \leq 9\},$$

$$\mathcal{F}_3 = \{\{1,2,3,i,j\} \mid 4 \leq i < j \leq 9\}.$$

計算機により，同値なものを除いて上の 2 つに限られることが確認できる．(i) については，明らかに Lisoněk の 2-距離集合 L_{45} に対応する．(ii) について，新しいものが出てくると嬉しかったのだが，残念ながら対応する $X = X_0 \cup X_1 \cup X_2$ は L_{45} と同型である．

以上より次の定理が成り立つ．

Theorem 5.3. 45 点からなる 2-距離集合 $X \subset \mathbb{R}^8$ が 9 頂点の正単体を含むとき，X は L_{45} と同型である．

6 計算

この節では，$X \subset \mathbb{R}^8$ を 45-点 2-距離集合で $A(X) = \{\sqrt{2}, 2\}$ として，$G(X)$ が $K_{3,3,3}$ の全域部分グラフを含む状況を考えていく．

位数 9 の単純グラフは 274668 個, $K_{3,3,3}$ の全域部分グラフは 62116 個，このうち 8 次元以下に実現可能なグラフは 2312 個となっている．この 2312 個からスタートして，45 頂点まで増やしていくことを考える．また，2312 個の内訳は，4 次元 1 個，5 次元 7 個，6 次元 124 個，7 次元 786 個，8 次元 1394 個となっている．

初めに，8 次元の 1394 個に対する手法を紹介する．9 点 2-距離集合 Y が $\dim(Y) = 8$ を満たし， $A(Y) = \{\sqrt{2}, 2\}$ であるとする．また，D を Y の距離行列とする．ここで，

$$\mathcal{L} = \{(x_1, x_2, \ldots, x_9) \mid x_i \in \{\sqrt{2}, 2\}\}$$

とする．このとき，Y に対応するグラフ $G^* = (V, E)$ を次で定義する．

$$V := \{\mathbf{v} \in \mathcal{L} \mid \mathrm{rank}(M_D(\mathbf{v})) = 8\}$$

ここで，

$$M_D(\mathbf{v}) := \left(\begin{array}{c|c} \mathrm{D} & {}^t\mathbf{v} \\ \hline \mathbf{v} & 0 \end{array}\right).$$

また，$\mathbf{v}, \mathbf{w} \in V$ に対し，$\mathrm{rank}(M_A(\mathbf{v}, \mathbf{w}; c)) = 8$ となる $c \in \{\sqrt{2}, 2\}$ が存在するとき，$\{\mathbf{v}, \mathbf{w}\} \in E$ とする．ここで，

$$M_D(\mathbf{v}, \mathbf{w}; c) := \left(\begin{array}{c|cc} \mathrm{D} & {}^t\mathbf{v} & {}^t\mathbf{w} \\ \hline \mathbf{v} & 0 & c \\ \mathbf{w} & c & 0 \end{array}\right).$$

$\mathbb{R}^8$ 上の 2-距離集合という条件を保ったまま，Y に 36 点足せるためには，$\omega(G^*(Y)) \geq 36$ となる必要がある（実際は必要十分）．1394 個のグラフに対応するものに対しては，この方法で全ての候補を列挙でき，全部で 57 個のグラフがあることが分かる．

次元 d が 7 以下のグラフに対しても，まずは次元が 8 になるまで次元を増やすような点を $8 - d$ 点足してから，つまり位数 $17 - d$ のグラフを作りそのクリーク数を計算することで全ての候補が列挙される．

rank	$1 \sim 3$	4	5	6	7	8
グラフの個数	0	1	7	124	786	1394
次元 8 にしたグラフの個数	0	812	3611	8832	3057	1394
$\omega(G^*) = 28 + r$ となるグラフ	0	268	1207	2792	1080	57

Table 4: 45 点まで成長できるグラフの個数

最後に 45 頂点まで成長させた 2-距離集合の表現グラフの同型判定を行う事で，全てのグラフが L_{45} と同型であることが確認できた．これにより我々の主結果が証明された．

7　おわりに

計算機の助けは必要になるが，ラムゼー型の定理や極値集合論的な議論を上手く用いる事により，$\mathbb{R}^8$ 上の最良な 2-距離集合は Lisoněk の 2-距離集合に限られることが証明された．ただ，その後の考察により，この計算が上手く実現可能な範囲に収まったのは，ラムゼー型の定理の恩恵というよりは，前の節の最後に少しだけ触れた，次元を 8 にするというところが鍵になったのではないかと思っている．もう少しこの部分を詳しくまとめておくと良いだろうが，今回はこの程度に留めておく．

References

[1] E. Bannai, E. Bannai and D. Stanton, An upper bound for the cardinality of an s-distance subset in real Euclidean space, II, *Combinatorica* **3** (1983), 147–152.

[2] E. Bannai, T. Sato and J. Shigezumi, Maximal m-distance sets containing the representation of the Johnson graph $J(n, m)$, *Discrete Math.* **312** (2012), 3283–3292.

[3] A. Blokhuis, *Few-distance sets*, Ph. D. thesis, Eindhoven Univ. of Technology (1983), (CWI Tract (7) 1984).

[4] H. T. Croft, 9-point and 7-point configuration in 3-space, *Proc. London. Math. Soc.* (3), **12** (1962), 400–424.

[5] S.J. Einhorn and I.J. Schoenberg, On euclidean sets having only two distances between points. I. II. *Nederl. Akad. Wetensch. Proc. Ser. A* 69=*Indag. Math.* 28 (1966), 479–488, 489–504.

[6] L. M. Kelly, Elementary Problems and Solutions. Isosceles n-points, *Amer. Math. Monthly*, **54** (1947), 227–229.

[7] D.G. Larman, C.A. Rogers and J.J. Seidel, On 2-distance sets in Euclidean space, *Bull. London Math. Soc.* **9** (1977), 261–267.

[8] P. Lisoněk, New maximal two-distance sets, *J. Combin. Theory, Ser. A* **77** (1997), 318–338.

[9] A. Neumaier, Distance matrices, dimension, and conference graphs, *Nederl. Akad. Wetensch. Indag. Math.***43** (1981), no. 4, 385–391.

[10] H. Nozaki, A generalization of Larman–Rogers–Seidel's theorem, *Discrete Math.* **311** (2011), 792–799.

[11] H. Nozaki and M. Shinohara, Maximal 2-distance sets containing the regular simplex, *Discrete Math.***437** (2020) 112071(10 pages).

[12] J. Schoenberg, Remarks to Maurice Frechet's article, *Ann. Math.***36** (1935) 724–732.

[13] A. Roy, Minimal Euclidean representation of graphs, *Discrete math.* 310 (2010), 727–733.

[14] F. Szöllősi and P.R.J. Östergård, Constructions of maximum few-distance sets in Euclidean spaces, *Electron. J. Combin.* **27** (1) (2020), #P1.23.

A base-p Sprague-Grundy type theorem: Maya game and representations of generalized symmetric groups

入江 佑樹（Yuki Irie）

東北大学 数理科学連携研究センター
Research Alliance Center for Mathematical Sciences, Tohoku University

組合せゲーム理論における古典的な結果である Sprague-Grundy の定理の p 進法における類似物をあたえる．さらにこの結果を用いてマヤゲームと一般化対称群の表現を結びつける．本稿は [8] の解説である．

1 序論

本稿の出発点は，佐藤幹雄による予想にある．1970 年代に佐藤は，表現とゲームの間には内部的なつながりがあると予想した [12–15]．その主な根拠は，対称群のフック公式とマヤゲームの Sprague-Grundy 関数（必勝法をあたえる関数）の公式の形が似ているなど，両者の間には様々な類似があったためである． 二つの間のつながりが [6] であたえられている．具体的には，対称群の表現の分岐に関する，p' 成分定理という定理が示され，この結果を使い，p 飽和マヤゲームというゲームの Sprague-Grundy 関数の公式が導かれた．すなわち，p' 成分定理によって対称群の表現とマヤゲームが結びつく．本研究の動機は，p' 成分定理を拡張し，表現とゲームのつながりを広げることにある．

まず元々の p' 成分定理を述べよう．ここでは結果を大まかに述べ，用語の説明は次節以降で行う．以下 p は素数とし，$\mathbb{N}$ は非負整数全体の集合を表す．分割と対応するヤング図形を同一視し，ヤング図形 Y に対して，ρ^Y で対応する対称群の（$\mathbb{C}$ 上の）既約表現を表す．$\psi^{(p)}(Y)$ を次で定義する:

$$\psi^{(p)}(Y) = \sum_{L\in\mathbb{N}} \overline{w}_L^{(p)}(Y) p^L.$$

ここで $w_L^{(p)}(Y)$ は Y の p^L-weight （長さが p^L で割り切れるフックの個数）であり，$\overline{w}_L^{(p)}(Y)$ は $w_L^{(p)}(Y)$ を p で割った余りを表す．例えば $p=2$ で $Y=$  の場合，フック長の多重集合は $\{1,1,1,2,3,3,4,5,6\}$ である．よって $w_0^{(2)}(Y)=9, w_1^{(2)}(Y)=3, w_2^{(2)}(Y)=1, w_L^{(2)}(Y)=0$ $(L\geqslant 3)$ であり，$\psi^{(2)}(Y)=1+2+2^2=7$ である．

定理 1.1 (p' 成分定理 [6])**.** 制限 $\rho^Y|_{\mathrm{Sym}(\psi^{(p)}(Y))}$ の既約成分には次数が p と素なものが存在する．

この定理を用いるとゲームに関する次の公式が導ける．

定理 1.2 ([6])**.** p 飽和マヤゲーム $\widetilde{\Gamma}$ の Sprague-Grundy 関数 $\mathrm{sg}_{\widetilde{\Gamma}}$ は $\psi^{(p)}$ に等しい． すなわち，Y が $\widetilde{\Gamma}$ の局面（ヤング図形と思える）のとき

$$\mathrm{sg}_{\widetilde{\Gamma}}(Y) = \psi^{(p)}(Y).$$

また局面 Y が full であることと表現 ρ^Y の次数が p と素なことは同値である．

以上が，[6] で得られた表現とゲームのつながりである．本稿の目的は，これらのつながりを一般化対称群 $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n)$ とマヤゲームの和へと拡張することにある．定理 1.1 と $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n)$ の表現について知られている結果（例えば [10, 11, 17] を参照）を使えば表現側は容易であり，次のようにできる．一般化対称群 $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n)$ の既約表現はヤング図形の k 組で添字付けできる． ヤング図形の k 組 $\boldsymbol{Y}=(Y^1,\dots,Y^k)$ に対して，$\rho^{\boldsymbol{Y}}$ で対応する $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n)$ の表現を表す．$\psi^{(p)}(\boldsymbol{Y})$ を次で定義する:

$$\psi^{(p)}(\boldsymbol{Y})=\sum_{L\in\mathbb{N}}\overline{w}_L^{(p)}(\boldsymbol{Y})p^L.$$

ここで $w_L^{(p)}(\boldsymbol{Y})=\sum_i w_L^{(p)}(Y^i)$ であり，$\overline{w}_L^{(p)}(\boldsymbol{Y})$ は $w_L^{(p)}(\boldsymbol{Y})$ を p で割った余りを表す．

定理 1.3 (p' 成分定理の拡張 [8])**.** 制限 $\rho^{\boldsymbol{Y}}|_{(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(\psi^{(p)}(\boldsymbol{Y}))}$ の既約成分には次数が p と素なものが存在する．

さて，元々の p' 成分定理ではここからゲームの公式を導くことができ，p 飽和マヤゲームの Sprague-Grundy 関数は $\psi^{(p)}(Y)$ で表せた．それでは拡張した p' 成分定理についても，対応するようなゲームがあるのだろうか？すなわち Sprague-Grundy 関数が $\psi^{(p)}(\boldsymbol{Y})$ で表せるゲームは存在するのだろうか？次の Sprague と Grundy による定理から，p が 2 の場合は，そのようなゲームを簡単に作ることができる．二つのゲーム Γ^1 と Γ^2 に対し，$\Gamma^1+\Gamma^2$ でその和（disjunctive sum）を表す．また $\oplus_p$ で p 進法で繰り上がりのない足し算（p ニム和）を表す．例えば $1\oplus_3 2=0$ であり，また $5\oplus_3 8=(2+3)\oplus_3(2+2\cdot 3)=1$ である．

定理 1.4 (Sprague [16], Grundy [5])**.** ゲーム Γ^1 と Γ^2 の和の Sprague-Grundy 関数はそれぞれの Sprague-Grundy 関数の 2 ニム和と等しい． すなわち A^1 と A^2 が Γ^1 と Γ^2 の局面のとき

$$\mathrm{sg}_{\Gamma^1+\Gamma^2}(A^1,A^2)=\mathrm{sg}_{\Gamma^1}(A^1)\oplus_2\mathrm{sg}_{\Gamma^2}(A^2).$$

定理 1.4 を使うと $p=2$ の場合は，対応するゲームが得られる．ヤング図形の k 組 $\boldsymbol{Y}$ に対して

$$\psi^{(p)}(\boldsymbol{Y})=\psi^{(p)}(Y^1)\oplus_p\cdots\oplus_p\psi^{(p)}(Y^k)$$

が成立することに注意する．定理 1.4 と定理 1.2 から次が従う．

系 1.5. $\widetilde{\Gamma}$ を 2 飽和マヤゲーム k 個の和とする．$\boldsymbol{Y}$ が $\widetilde{\Gamma}$ の局面（ヤング図形の k 組と思える）のとき

$$\mathrm{sg}_{\widetilde{\Gamma}}(\boldsymbol{Y})=\psi^{(2)}(Y^1)\oplus_2\cdots\oplus_2\psi^{(2)}(Y^k)=\psi^{(2)}(\boldsymbol{Y}).$$

もし Sprague-Grundy の定理の p 進法における類似物があれば，一般の p に対しても対応するゲームを構成できる．本稿では，p-calm subtraction ゲームという族を定義し，このゲームに対しては次のように Sprague-Grundy の定理の p 進法における類似が成立することを紹介する．

定理 1.6 ([8])**.** Γ^1 と Γ^2 を p-calm subtraction ゲームとする．このとき $\Gamma^1+\Gamma^2$ の p 飽和の Sprague-Grundy 関数はそれぞれの p 飽和の Sprague-Grundy 関数の p ニム和と等しい． すなわち A^1 と A^2 が Γ^1 と Γ^2 の局面のとき

$$\mathrm{sg}_{\widetilde{\Gamma^1+\Gamma^2}}(A^1,A^2)=\mathrm{sg}_{\widetilde{\Gamma^1}}(A^1)\oplus_p\mathrm{sg}_{\widetilde{\Gamma^2}}(A^2).$$

ここで $\widetilde{\Gamma}$ は Γ の p 飽和を表す．

p-calm subtraction ゲームの和も p-calm であることが証明でき，またマヤゲームは p-calm であるため，次の結果を得る[*1]．

系 1.7. $\widetilde{\Gamma}$ をマヤゲーム k 個の和の p 飽和とする．$\boldsymbol{Y}$ が $\widetilde{\Gamma}$ の局面のとき

$$\mathrm{sg}_{\widetilde{\Gamma}}(\boldsymbol{Y}) = \psi^{(p)}(Y^1) \oplus_p \cdots \oplus_p \psi^{(p)}(Y^k) = \psi^{(p)}(\boldsymbol{Y}).$$

また局面 $\boldsymbol{Y}$ が full であることと表現 $\rho^{\boldsymbol{Y}}$ の次数が p と素なことは同値である．

本稿の構成は次である．2 節にて subtraction ゲーム，ゲームの和，Sprague-Grundy 関数などの組合せゲーム理論に関する用語を定義する．3 節にて p 飽和と p-calm を紹介し，さらに，ゲームと表現の関係について述べる．

2 subtraction ゲーム

組合せゲーム理論において，不偏ゲームと呼ばれる族に含まれる，subtraction ゲームの周辺について基本事項を述べる．なお，組合せゲーム理論に関する文献として [1,3] 等がある．

本稿では次のように有向グラフでゲームを表す．Γ を有向グラフ $(\mathcal{P}_\Gamma, \mathcal{E}_\Gamma)$ とする．すなわち $\mathcal{P}_\Gamma$ は集合で $\mathcal{E}_\Gamma \subseteq \mathcal{P}_\Gamma^2$ である．本稿では Γ が **（不偏）ゲーム** であることを，各頂点 $A \in \mathcal{P}_\Gamma$ に対して，A から始まる最長 walk の長さ $\lg_\Gamma(A)$ が有限であることで定義する．例えば $(\{1,2,3,4\}, \{(1,2),(2,3),(1,4)\})$ はゲームであるが，$(\{1,2\}, \{(1,2),(2,1)\})$ は $(1,2,1,2,\ldots)$ という長さ無限の walk を持つためゲームではない．ゲーム Γ に対して $\mathcal{P}_\Gamma$ を **局面集合** と呼び，$(A,B) \in \mathcal{E}_\Gamma$ のとき B を A の **option** と呼ぶ．また A から B へのパスがあるとき B を A の **descendant** と呼び，特に $B \neq A$ のときは **proper descendant** と呼ぶ．

注 2.1. ゲーム Γ は次の二人対戦ゲームを表していると思うことができる．準備としてまず開始局面 $A \in \mathcal{P}_\Gamma$ を選ぶ．二人のプレイヤーは交互に現在の局面から，その option へ移動する．先に移動ができなくなった方が負けである． 例えば $\Gamma = (\{1,2,3,4\}, \{(1,2),(2,3),(1,4)\})$ で，開始局面を 1 とした場合で考えよう． 先手のプレイヤー P_1 は 2 か 4 に移動できる．もし 2 に移動した場合は，後手のプレイヤー P_2 は 3 に 移動することができ，P_1 は 3 からは移動できないため，P_2 の勝ちである．一方，P_1 が 1 から 4 に移動した場合は，P_2 が移動できないため，P_1 の勝ちである． このように有向グラフ Γ は二人対戦のゲームと思うことができる．

それでは subtraction ゲームを定義する．$\mathcal{P}_\Gamma$ を $\mathbb{N}^m$ の部分集合とし，$\mathscr{C}$ を $\mathbb{N}^m \backslash \{(0,\ldots,0)\}$ の部分集合とする．このとき **subtraction ゲーム** $\Gamma(\mathcal{P}_\Gamma, \mathscr{C})$ を局面集合が $\mathcal{P}_\Gamma$ で辺集合が

$$\{(A, A-C) \in \mathcal{P}_\Gamma^2 : C \in \mathscr{C}\}$$

のゲームとして定義する．

ここでは subtraction ゲームの例を三つあげる（後で述べるようにこれらは全て p-calm 性を満たす）．以下 $\mathbb{N}^m$ の元を大文字で表し，その i 成分を上に添字が付いた小文字で表す．例えば $A = (a^1, \ldots, a^m)$ である．

[*1] p'-成分定理 1.1 からゲームの公式をあたえる定理 1.2 を導いたように，拡張した p'-成分定理 1.3 から系 1.7 を導くのが話の流れとしては良く見える．が，系 1.7 を証明するには，元々の p'-成分定理 1.1 があれば十分である（系 1.7 は $m = 1$ の場合，すなわち定理 1.2 さえ示せれば，あとは定理 1.6 から直ちに従うため）．そのため本稿の本質（新しい部分）は，定理 1.3 よりも定理 1.6 にあり，今回の話は，対称群の表現とマヤゲームの関係と同様の関係が，一般化対称群の表現とマヤゲームの和の間にあることが定理 1.6 からわかる，というものになっている．

例 2.2. $\mathcal{P}=\mathbb{N}^m$ として

$$\mathscr{C}_1=\{C\in\mathbb{N}^m:\mathrm{wt}(C)=1\}$$

とする．ただし $\mathrm{wt}(C)$ は C の Hamming weight $\left|\{i\in\{1,\dots,m\}:c^i\neq 0\}\right|$ を表す．このとき $\Gamma(\mathcal{P},\mathscr{C}_1)$ を **Nim** と呼び，$\mathcal{N}_m$ で表す．例えば $m=2$ で，開始局面を $(1,1)$ とした場合で考えよう．先手のプレイヤー P_1 は $(1,0)$ と $(0,1)$ に移動でき，$(1,0)$ に移動したとすると，後手のプレイヤー P_2 は $(0,0)$ に移動でき，P_1 はこれ以上移動できないため，P_2 の勝ちである．

例 2.3. $\mathcal{M}_m=\Gamma(\mathbb{N}^m\backslash\{(0,\dots,0)\},\mathscr{C}_m^1)$ とする．$\mathcal{M}_m$ を **misère Nim** と呼ぶ．例えば $m=2$ で，開始局面を $(1,1)$ とした場合で考えよう．先手のプレイヤー P_1 は $(1,0)$ と $(0,1)$ に移動でき，$(1,0)$ に移動したとすると，後手のプレイヤー P_2 は $(0,0)$ に移動するしかないが，今 $(0,0)$ は局面集合から除いているため，P_2 は移動できず，P_1 の勝ちである．このように $\mathcal{M}_m$ は $(0,0)$ に移動してしまった方の負けというゲームと思える．通常の Nim では $(0,0)$ に移動した方が勝ちだったので，misère Nim は勝ち負けを逆にした Nim になっている．

例 2.4.

$$\mathcal{P}=\{A\in\mathbb{N}^m:a^i\neq a^j\ \text{ for }\ 1\leqslant i<j\leqslant m\}$$

とする．$\Gamma(\mathcal{P},\mathscr{C}_m^1)$ を **マヤゲーム（Welter ゲーム）** と呼び，$\mathcal{W}_m$ で表す．例えば $\mathcal{W}_2$ では $(1,2)$ の option は $(0,2)$ と $(1,0)$ である．マヤゲームは次のようにヤング図形を使ったゲームと思うこともできる．A をマヤゲームの局面 $(a^1,\dots,a^m)$ とする．必要ならば順番を入れ替えて $a^1>\cdots>a^m$ とする．このとき A に対応するヤング図形（分割）を $Y(A)=(a^1-m+1,a^2-m+2,\dots,a^m)$ で定義する．例えば $Y((3,6,4))=(4,3,3)=$  である．このようにマヤゲームの局面にヤング図形を対応させたとき，マヤゲームで局面 A からその option B に移動することは，ヤング図形 $Y(A)$ からフックを除くことに対応する．以上のようにしてマヤゲームはヤング図形のフックを抜くゲームと思うことができる．このとき，例えば最長 walk の長さ $\mathrm{lg}_{\mathcal{W}_m}(A)$ は $Y(A)$ の箱の数 $|Y(A)|$ に等しいことがわかる．

次にゲームの和を定義する．$i\in\{1,2\}$ に対して Γ^i をゲームとする．$\mathcal{P}^i=\mathcal{P}_{\Gamma^i}$ と $\mathcal{E}^i=\mathcal{E}_{\Gamma^i}$ とおく．このとき Γ^1 と Γ^2 の **和** $\Gamma^1+\Gamma^2$ を局面集合が $\mathcal{P}^1\times\mathcal{P}^2$ で辺集合が

$$\begin{aligned}&\{((A^1,A^2),(B^1,A^2)):(A^1,B^1)\in\mathcal{E}^1,\,A^2\in\mathcal{P}^2\}\\ \cup&\{((A^1,A^2),(A^1,B^2)):(A^2,B^2)\in\mathcal{E}^2,\,A^1\in\mathcal{P}^1\}\end{aligned}$$

であるゲームとして定義する．例えば

$$\mathcal{N}_m=\underbrace{\mathcal{N}_1+\cdots+\mathcal{N}_1}_{m}.$$

ここで subtraction ゲームの和も subtraction ゲームになることに注意しておく．

最後に Sprague-Grundy 関数について述べる．Γ をゲームとする．$A\in\mathcal{P}_\Gamma$ に対して，A の **Sprague-Grundy 数** $\mathrm{sg}_\Gamma(A)$ を次で再帰的に定義する:

$$\mathrm{sg}_\Gamma(A)=\mathrm{mex}\{\mathrm{sg}_\Gamma(B):(A,B)\in\mathcal{E}_\Gamma\}.$$

ただし $\mathrm{mex}\,S=\min\{\alpha\in\mathbb{N}:\alpha\notin S\}$ である．関数 $\mathrm{sg}_\Gamma\colon\mathcal{P}_\Gamma\to\mathbb{N}$ を Γ の **Sprague-Grundy 関数** と呼ぶ．簡単な帰納法より，A が開始局面であるとき，後手必勝である必要十分条件は $\mathrm{sg}_\Gamma(A)=0$ であることが示せる．1 節で述べた Sprague と Grundy の定理を再掲する．

定理 2.5 (Sprague [16], Grundy [5]). Γ^1 と Γ^2 がゲームのとき

$$\mathrm{sg}_{\Gamma^1+\Gamma^2} = \mathrm{sg}_{\Gamma^1} \oplus_2 \mathrm{sg}_{\Gamma^2}.$$

すなわち，A^i が Γ^i の局面のとき

$$\mathrm{sg}_{\Gamma^1+\Gamma^2}(A^1,A^2) = \mathrm{sg}_{\Gamma^1}(A^1) \oplus_2 \mathrm{sg}_{\Gamma_2}(A^2). \tag{1}$$

例 2.6. $\mathcal{N}_m = \mathcal{N}_1 + \cdots + \mathcal{N}_1$ だったので，定理 2.5 より A が $\mathcal{N}_m$ の局面のとき

$$\mathrm{sg}_{\mathcal{N}_m}(A) = a^1 \oplus_2 \cdots \oplus_2 a^m. \tag{2}$$

例えば $\mathrm{sg}_{\mathcal{N}_2}((1,1)) = 1 \oplus_2 1 = 0$ より $(1,1)$ は後手必勝の局面である．

定理 2.7 (Welter [18], 佐藤 [12–14]). A がマヤゲーム $\mathcal{W}_m$ の局面のとき

$$\begin{aligned} \mathrm{sg}_{\mathcal{W}_m}(A) &= a^1 \oplus_2 \cdots \oplus_2 a^m \oplus_2 \left(\bigoplus_{i<j}{}_2 \, 2^{\mathrm{ord}_2(a^i - a^j)+1} - 1 \right) \\ &= \psi^{(2)}(Y(A)) = \bigoplus_{h \in \mathscr{H}(Y(A))}{}_2 \, \mathfrak{N}^{(2)}(h). \end{aligned} \tag{3}$$

ただし，$\mathrm{ord}_2(a)$ は a の 2-adic order を表す．すなわち

$$\mathrm{ord}_2(a) = \begin{cases} \max\{L \in \mathbb{N} : 2^L \mid a\} & \text{if } a \neq 0, \\ \infty & \text{if } a = 0. \end{cases}$$

また $\mathscr{H}(Y(A))$ は $Y(A)$ のフック長の多重集合を表し，$\mathfrak{N}^{(2)}(h) = \sum_{L=0}^{\mathrm{ord}_2(h)} 2^L$ である．

例 2.8. A をマヤゲームの局面 $(7,5,3)$ とすると，定理 2.7 より

$$\begin{aligned} \mathrm{sg}_{\mathcal{W}_3}(A) &= 7 \oplus_2 5 \oplus_2 3 \oplus_2 (2^{\mathrm{ord}_2(7-5)+1} - 1) \oplus_2 (2^{\mathrm{ord}_2(7-3)+1} - 1) \oplus_2 (2^{\mathrm{ord}_2(5-3)+1} - 1) \\ &= 7 \oplus_2 5 \oplus_2 3 \oplus_2 3 \oplus_2 7 \oplus_2 3 = 6. \end{aligned}$$

また $Y(A) =$  であり，$Y(A)$ のフック長の多重集合は $\{1,1,1,2,3,3,3,4,5,5,6,7\}$ のため，

$$\begin{aligned} \mathrm{sg}_{\mathcal{W}_3}(A) &= \bigoplus_{h \in \mathscr{H}(Y(A))}{}_2 \, \mathfrak{N}^{(2)}(h) \\ &= \mathfrak{N}^{(2)}(1) \oplus_2 \mathfrak{N}^{(2)}(1) \oplus_2 \mathfrak{N}^{(2)}(1) \oplus_2 \mathfrak{N}^{(2)}(3) \oplus_2 \mathfrak{N}^{(2)}(3) \oplus_2 \mathfrak{N}^{(2)}(3) \\ &\quad \oplus_2 \mathfrak{N}^{(2)}(5) \oplus_2 \mathfrak{N}^{(2)}(5) \oplus_2 \mathfrak{N}^{(2)}(7) \\ &\quad \oplus_2 \mathfrak{N}^{(2)}(2) \oplus_2 \mathfrak{N}^{(2)}(6) \oplus_2 \mathfrak{N}^{(2)}(4) \\ &= 1 \oplus_2 1 \oplus_2 1 \oplus_2 1 \oplus_2 1 \oplus_2 1 \oplus_2 1 \oplus_2 1 \oplus_2 3 \oplus_2 3 \oplus_2 7 \\ &= 6. \end{aligned}$$

注 2.9. 以上のように Nim とマヤゲームについては Sprague-Grundy 関数の明示公式が知られている．しかし，これらのように明示公式が知られている例は珍しく，例えば misère Nim の Sprague-Grundy 関数の公式は知られていない．なお，misère Sprague-Grundy 関数と呼ばれるものがあり，この関数の明示公式は知られている [3].

注 2.10. ゲーム Γ とその局面 A に対して，A の Sprague-Grundy 数は A から始まる walk の最大長で上から抑えられる．すなわち

$$\mathrm{sg}_\Gamma(A) \leqslant \mathrm{lg}_\Gamma(A). \tag{4}$$

例えばマヤゲームの場合は，$\mathrm{lg}_{\mathcal{W}_m}(A) = |Y(A)|$ だったので $\mathrm{sg}_{\mathcal{W}_m}(A) \leqslant |Y(A)|$ である．局面 A がこの bound を達成するとき，すなわち $\mathrm{sg}_\Gamma(A) = \mathrm{lg}_\Gamma(A)$ となるとき，本稿では A を **full** と呼ぶことにしよう．次節で述べるように，（p 飽和マヤゲームの）full な局面は次数が p と素な表現に対応しており，この事実からゲームと表現が結びつく．

3 p-calm subtraction ゲーム

本節ではまず p 飽和を紹介する．そして p-calm subtraction ゲームを定義し，p-calm subtraction ゲームに対しては Sprague と Grundy の定理の p 進法における類似物が成立することを紹介する．また最後に p' 成分定理をゲームの言葉で言い換える．なお本節で述べるゲームに関する結果は，p が 2 以上の整数であれば，素数でなくても成立する．

3.1 p 飽和

前節で見たゲームは 2 進法と関係していた．本節で見るように p 飽和を使うと p 進法と関係するゲームを得ることができる．

$a \in \mathbb{N}$ に対して $\mathrm{ord}_p(a)$ で a の p-adic order を表す．すなわち

$$\mathrm{ord}_p(a) = \begin{cases} \max\{L \in \mathbb{N} : p^L \mid a\} & \text{if } a \neq 0, \\ \infty & \text{if } a = 0. \end{cases}$$

次の集合を定義する．

$$\mathscr{C}_m^{(p)} = \left\{ C \in \mathbb{N}^m \setminus \{(0,\dots,0)\} : \mathrm{ord}_p\Big(\sum_i c^i\Big) = \mathrm{mord}_p(C) \right\}.$$

ただし $\mathrm{mord}_p(C) = \min\{\mathrm{ord}_p(c^i) : 1 \leqslant i \leqslant m\}$．例えば

$$(1,0),(1,3) \in \mathscr{C}_2^{(3)}, \quad (1,2) \notin \mathscr{C}_2^{(3)}.$$

実際

$$\begin{aligned} &\mathrm{ord}_3(1+0) = 0 = \min\{\mathrm{ord}_3(1), \mathrm{ord}_3(0)\} = \min\{0, \infty\}, \\ &\mathrm{ord}_3(1+3) = 0 = \min\{\mathrm{ord}_3(1), \mathrm{ord}_3(3)\} = \min\{0, 1\}, \\ &\mathrm{ord}_3(1+2) = 1 > 0 = \min\{\mathrm{ord}_3(1), \mathrm{ord}_3(2)\} = \min\{0, 0\}. \end{aligned}$$

$\mathscr{C}_m^1 \subseteq \mathscr{C}_m^{(p)}$ であることに注意する（$\mathscr{C}_m^1$ は Hamming weight が 1 となる $\mathbb{N}^m$ の元全体であった）．$\Gamma = \Gamma(\mathcal{P}, \mathscr{C})$ と $\widetilde{\Gamma} = \Gamma(\mathcal{P}, \widetilde{\mathscr{C}})$ としよう．ゲーム $\widetilde{\Gamma}$ が Γ の p **飽和** であることを $\widetilde{\Gamma}$ が $\Gamma(\mathcal{P}, \mathscr{C} \cup \mathscr{C}_m^{(p)})$ と同じ Sprague-Grundy 関数を持つことで定義する．すなわち全ての $A \in \mathcal{P}$ に対して次が成立するとき p 飽和と呼ぶ:

$$\mathrm{sg}_{\widetilde{\Gamma}}(A) = \mathrm{sg}_{\Gamma(\mathcal{P}, \mathscr{C} \cup \mathscr{C}_m^{(p)})}(A). \tag{5}$$

明らかに $\Gamma(\mathcal{P}, \mathscr{C} \cup \mathscr{C}_m^{(p)})$ は Γ の p 飽和である．本稿では，次の条件を満たす subtraction ゲーム $\Gamma(\mathcal{P}, \mathscr{C})$ のみを考える．

$(*)$ $\quad \mathscr{C} \subseteq \mathscr{C}_m^{(p)}$.

もし Γ が $(*)$ を満たすならば $\widetilde{\Gamma}$ が Γ の p 飽和である必要十分条件は，$\mathrm{sg}_{\widetilde{\Gamma}} = \mathrm{sg}_{\Gamma(\mathcal{P},\mathscr{C}_m^{(p)})}$ である．条件 $(*)$ は和で閉じていることに注意する． すなわち，もし二つの subtraction ゲーム Γ^1 と Γ^2 が $(*)$ を満たすならば，$\Gamma^1+\Gamma^2$ も $(*)$ を満たす．

p 飽和を使うことにより，以下のように p 進法版のゲームが得られる場合がある．

例 3.1 ([6]). $\widetilde{\Gamma} = \Gamma(\mathbb{N}^2, \mathscr{C}_2^{(3)})$ とする．表 1 は $\widetilde{\Gamma}$ の一部の局面の Sprague-Grundy 数を表す．簡単に $\mathrm{sg}_{\widetilde{\Gamma}}(a,0) = \mathrm{sg}_{\widetilde{\Gamma}}(0,a) = a$ であることが確かめられる．$(1,1) \in \mathscr{C}_2^{(3)}$ のため， $(0,0)$ は $(1,1)$ の option である．よって $\mathrm{sg}_{\widetilde{\Gamma}}(1,1) = 2$．また，$(0,0)$ は $(1,2)$ の option でないため $\mathrm{sg}_{\widetilde{\Gamma}}(1,2) = 0$ がわかる．

	0	1	2	3
0	0	1	2	3
1	1	2	0	4
2	2	0	1	5
3	3	4	5	6

表 1　$\Gamma(\mathbb{N}^2, \mathscr{C}_2^{(3)})$ の Sprague-Grundy 数.

一般に $\widetilde{\Gamma}$ が Nim $\mathcal{N}_m$ の p 飽和で，A が $\widetilde{\Gamma}$ の局面ならば次が成立する（ここから Nim は自分自身の 2 飽和であることがわかる）．

$$\mathrm{sg}_{\widetilde{\Gamma}}(A) = a^1 \oplus_p \cdots \oplus_p a^m. \tag{6}$$

そのため p 飽和 Nim は p 進法版の Nim といえるゲームになっている．なお p 進法版の Nim は J. A. Flanigan の未出版論文 “Nim, Trim and Rim” にて Rim_p と呼ばれるゲームとして初めて発見された．Rim_p は（無限にある）p 飽和 Nim の一つになっている．

注 3.2. 上述のように Nim $\mathcal{N}_m$ は自分自身の 2 飽和である．これは $C \in \mathscr{C}_m^{(2)}$ に対して $(A, A-C)$ という辺を $\mathcal{N}_m$ に加えても，Sprague-Grundy 関数が変化しないことを意味する．なお，$\Gamma(\mathbb{N}^m, \mathscr{C})$ が $\mathcal{N}_m$ の 2 飽和である必要十分条件は，$\mathscr{C}_m^1 \subseteq \mathscr{C} \subseteq \mathscr{C}_m^{(2)}$ であることが知られている [2].

定理 3.3 ([7]). $\widetilde{\Gamma}$ を misère Nim $\mathcal{M}_m$ の p 飽和とする．A が $\widetilde{\Gamma}$ の局面のとき

$$\mathrm{sg}_{\widetilde{\Gamma}}(A) = a^1 \oplus_p \cdots \oplus_p a^m \oplus_p (p^{\mathrm{mord}_p(A)+1} - 1). \tag{7}$$

定理 3.4 ([6]). $\widetilde{\Gamma}$ をマヤゲーム $\mathcal{W}_m$ の p 飽和とする．A が $\widetilde{\Gamma}$ の局面のとき

$$\begin{aligned} \mathrm{sg}_{\widetilde{\Gamma}}(A) &= a^1 \oplus_p \cdots \oplus_p a^m \oplus_p \left(\bigoplus_{i<j}{}_p \; p^{\mathrm{ord}_p(a^i - a^j)+1} - 1 \right) \\ &= \psi^{(p)}(Y(A)) = \bigoplus_{h \in \mathscr{H}(Y(A))}{}_p \; \mathfrak{N}^{(p)}(h). \end{aligned} \tag{8}$$

ただし，$\mathfrak{N}^{(p)}(h) = \sum_{L=0}^{\mathrm{ord}_p(h)} p^L$． 特に $\mathcal{W}_m$ は自分自身の 2 飽和である．

例 3.5. $\widetilde{\Gamma}$ を $\mathcal{W}_3$ の 5 飽和とし，A を局面 $(7,5,3)$ とする．定理 3.4 より

$$\begin{aligned} \mathrm{sg}_{\widetilde{\Gamma}}(A) &= 7 \oplus_5 5 \oplus_5 3 \oplus_5 (5^{\mathrm{ord}_5(7-5)+1} - 1) \oplus_5 (5^{\mathrm{ord}_5(7-3)+1} - 1) \oplus_5 (5^{\mathrm{ord}_5(5-3)+1} - 1) \\ &= 7 \oplus_5 5 \oplus_5 3 \oplus_5 4 \oplus_5 4 \oplus_5 4 = 12. \end{aligned}$$

3.2 p-calm subtraction ゲーム

Γ を 条件 $(*)$ を満たす subtraction ゲームとする．すなわち $\mathscr{C} \subseteq \mathscr{C}_m^{(p)}$ となる $\mathscr{C}$ を使って $\Gamma = \Gamma(\mathcal{P}, \mathscr{C})$ と書けるとする．Γ が **p-calm** であることを，全ての局面 A とその proper descendant B に対して次が成立することで定義する．

$$\mathrm{sg}_{\widetilde{\Gamma}}(A) - \mathrm{sg}_{\widetilde{\Gamma}}(B) \equiv \sum_i a^i - b^i \pmod{p^{N+1}}.$$

ただし，$\widetilde{\Gamma}$ は Γ の p 飽和であり $N = \mathrm{mord}_p(A-B)$ である．本稿の主結果である，Sprague と Grundy の定理の p 進法における類似物を再掲する．

定理 3.6 ([8])**.** Γ^1 と Γ^2 を p-calm subtraction ゲームとする．このとき $\Gamma^1 + \Gamma^2$ も p-calm subtraction ゲームである．さらに，

$$\mathrm{sg}_{\widetilde{\Gamma^1+\Gamma^2}}(A^1, A^2) = \mathrm{sg}_{\widetilde{\Gamma^1}}(A^1) \oplus_p \mathrm{sg}_{\widetilde{\Gamma^2}}(A^2). \tag{9}$$

ただし $\widetilde{\Gamma}$ は Γ の p 飽和を表す．

例 3.7. 今までに紹介した，Nim と misère Nim とマヤゲームは全て p-calm である．

注 3.8. Γ^1 を $(*)$ を満たす subtraction ゲームとする．実は Γ^2 が Nim のとき，Γ^1 が 定理 3.6 の (9) を満たせば，Γ^1 は p-calm になることが示せる．すなわち，Γ^1 が Nim と (9) を満たす必要十分条件は，Γ^1 が p-calm であることである．一般に，Nim の代わりに Γ_2 として p-calm で $\mathrm{sg}_{\widetilde{\Gamma^2}} \colon \mathcal{P}_{\widetilde{\Gamma^2}} \to \mathbb{N}$ が全射となるものを考えても以上のことが成立する．

3.3 ゲームと表現

p' 成分定理のゲームの言葉による言い換えをあたえる．

まずは元々の p' 成分定理を言い換える．そのために対称群についてよく知られている事実からはじめる．ヤング図形 Y に対して ρ^Y で対応する対称群 $\mathrm{Sym}(n)$ の既約表現を表した．表現 ρ^Y の $\mathrm{Sym}(n-1)$ への制限は，分岐則により $\bigoplus f^Z$ と表せる． ここで Z は Y から長さ 1 のフック（1 個の箱）を除いて得られるヤング図形全体を走る．また f^Y で ρ^Y の次数を表すと，フック公式 [4] より

$$\deg f^Y = \frac{n!}{\prod_{h \in \mathscr{H}(Y)} h}.$$

さて，Macdonald [9] によって f^Y が p と素になる Y の特徴付けがあたえられている．また [6] において，Macdonald の特徴付けを用いると，f^Y が p と素であることと $\psi^{(p)}(Y) = |Y|$ が同値であることが観察された．ここで p 飽和マヤゲームの局面 A に対して次が成立したことを思い出そう:

$$\mathrm{sg}_{\widetilde{\Gamma}}(A) = \psi^{(p)}(Y(A)), \quad \mathrm{lg}_{\widetilde{\Gamma}}(A) = |Y(A)|.$$

また局面 A は $\mathrm{sg}_{\widetilde{\Gamma}}(A) = \mathrm{lg}_{\widetilde{\Gamma}}(A)$ のとき full と呼んだ．よって A が full であることと $f^{Y(A)}$ が p と素であることが同値である．以上より，p' 成分定理 1.1 は次のようにゲームの言葉で言い換えることができる．

命題 3.9 ([6])**.** p 飽和マヤゲームの局面 A に対して， full な descendant B で A と同じ Sprague-Grundy 数を持つものが存在する．

例 3.10. $p=2$ とし，$\widetilde{\Gamma}$ を 2 飽和マヤゲームとする（例えばマヤゲーム自身を取れば良い）．A を $\widetilde{\Gamma}$ の局面 $(6,4,2)$ とし，$Y=Y(A)=$  とする．1 節で見たように $\psi^{(2)}(Y)=7$ だったので，p' 成分定理より $\rho^Y|_{\mathrm{Sym}(7)}$ は奇数次数の既約成分を持つ．すなわち Y に含まれる 7 個の箱からなるヤング図形 Z で f^Z が奇数のものが存在する．実際，$Z=(3,2,2)=$  とすると，Z は Y に含まれる 7 個の箱からなるヤング図形であり

$$f^Z=\frac{7!}{1^2\cdot 2^2\cdot 3\cdot 4\cdot 5}=21$$

より，f^Z は奇数である．それでは，これらをゲームの側から見てみる．まず $\mathrm{sg}_{\widetilde{\Gamma}}(A)=\psi^{(2)}(Y)=7$．また Z に対応するのは局面 $B=(5,3,2)$ であり，B は full，すなわち，$\mathrm{sg}_{\widetilde{\Gamma}}(B)=\mathrm{lg}_{\widetilde{\Gamma}}(B)$ を満たす．実際，$\mathrm{lg}_{\widetilde{\Gamma}}(B)=|Z|=7$ かつ

$$\begin{aligned}\mathrm{sg}_{\widetilde{\Gamma}}(B)&=5\oplus_2 3\oplus_2 2\oplus_2(2^{\mathrm{ord}_2(5-3)+1}-1)\oplus_2(2^{\mathrm{ord}_2(5-2)+1}-1)\oplus_2(2^{\mathrm{ord}_2(3-2)+1}-1)\\&=5\oplus_2 3\oplus_2 2\oplus_2 3\oplus_2 1\oplus_2 1=7.\end{aligned}$$

よって B は A の full な descendant であり，かつ，A と同じ Sprague-Grundy 数を持つ．

注 3.11. 1 節で述べたように，p' 成分定理 1.1 を用いると，p 飽和マヤゲーム $\widetilde{\Gamma}$ の Sprague-Grundy 関数が $\psi^{(p)}$ と一致することが示せる．このことをもう少し詳しく述べる．要点は p' 成分定理によって，次のように証明を full な局面に帰着させる点にある．ただし，ここでは full な局面 A を $\psi^{(p)}(A)=\mathrm{lg}_{\widetilde{\Gamma}}(A)$ を満たすものとして定義する（$\mathrm{sg}_{\widetilde{\Gamma}}(A)=\psi^{(p)}(A)$ を示した後は，もちろん今までの定義と一致する）．まず full な局面 A に対しては $\mathrm{sg}_{\widetilde{\Gamma}}(A)=\psi^{(p)}(A)$ が比較的簡単に証明できる．また full でない局面 A に対しては，p' 成分定理 1.1 より，full な descendant B で $\psi^{(p)}(B)=\psi^{(p)}(A)$ を満たすものが存在する． ここで B は full なため $\mathrm{sg}_{\widetilde{\Gamma}}(B)=\psi^{(p)}(B)$ が成立し，このことから $\mathrm{sg}_{\widetilde{\Gamma}}(A)=\psi^{(p)}(A)$ を証明できる．

最後に，上と同様の方法で，拡張した p' 成分定理もゲームの言葉で言い換えられることを紹介する．ヤング図形の k 組 $\boldsymbol{Y}$ に対して $\rho^{\boldsymbol{Y}}$ で対応する対称群 $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n)$ の既約表現を表した．表現 $\rho^{\boldsymbol{Y}}$ の $(\mathbb{Z}/k\mathbb{Z})\wr\mathrm{Sym}(n-1)$ への制限は，分岐則により $\bigoplus f^{\boldsymbol{Z}}$ と表せる．ここで $\boldsymbol{Z}$ は $\boldsymbol{Y}$ から長さ 1 のフックを除いて得られるヤング図形の k 組全体を走る．また $f^{\boldsymbol{Y}}$ で $\rho^{\boldsymbol{Y}}$ の次数を表すと

$$\deg f^{\boldsymbol{Y}}=\frac{n!}{\prod_{h\in\mathscr{H}(\boldsymbol{Y})}h}.$$

例えば $\boldsymbol{Y}=((4,4,2),(2,1))=\left(\text{  },\text{  }\right)$ とすると図 1 に示すように $\mathscr{H}(\boldsymbol{Y})=\{1,1,1,1,2,2,2,3,3,4,5,5,6\}$．よって

$$f^{\left(\text{},\text{}\right)}=\frac{13!}{1^4\cdot 2^3\cdot 3^2\cdot 4\cdot 5^2\cdot 6}=144144.$$

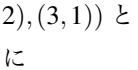
図 1　$((4,4,2),(2,1))$ と $((2,2,1),(2))$ のフック長.

Macdonald による次数が p と素な表現の特徴付けは一般化対称群へ直ちに拡張することができ [10]，対称群のときと同様に，$f^{\boldsymbol{Y}}$ が p と素である必要十分条件は $\psi^{(p)}(\boldsymbol{Y})=|\boldsymbol{Y}|$ が成立することである．ここでマヤゲームの和の p 飽和 $\widetilde{\Gamma}$ の局面 $\boldsymbol{A}$ に対して次が成り立つ:

$$\mathrm{sg}_{\widetilde{\Gamma}}(\boldsymbol{A})=\psi^{(p)}(\boldsymbol{Y}(\boldsymbol{A})),\quad \mathrm{lg}_{\widetilde{\Gamma}}(\boldsymbol{A})=|\boldsymbol{Y}(\boldsymbol{A})|.$$

ただし $\boldsymbol{Y}(\boldsymbol{A}) = (Y(A^1),\dots,Y(A^k))$ で $\boldsymbol{A} = (A^1,\dots,A^k)$ である．よって $\boldsymbol{A}$ が full であることと $f^{\boldsymbol{Y}(\boldsymbol{A})}$ が p と素であることが同値である．以上より，拡張した p' 成分定理 1.3 は次のようにゲームの言葉で言い換えることができる．

命題 3.12 ([8])**.** マヤゲームの和の p 飽和 $\widetilde{\Gamma}$ の局面 $\boldsymbol{A}$ に対して， full な descendant $\boldsymbol{B}$ で $\boldsymbol{A}$ と同じ Sprague-Grundy 数を持つものが存在する．

例 3.13. $p = 2$ とし，$\widetilde{\Gamma}$ をマヤゲームの和 $\mathcal{W}_3 + \mathcal{W}_2$ の 2 飽和とする（例えば $\mathcal{W}_3 + \mathcal{W}_2$ を取れば良い）．$\boldsymbol{A}$ を $\widetilde{\Gamma}$ の局面 $((6,5,2),(3,1))$ とし，$\boldsymbol{Y} = \boldsymbol{Y}(\boldsymbol{A}) = ((4,4,2),(2,1)) =$  とする．上で見たように $f^{\boldsymbol{Y}} = 144144$ である．さらに

$$\psi^{(2)}\left(\text{}\right) = \psi^{(2)}\left(\text{}\right) \oplus_2 \psi^{(2)}\left(\text{}\right) = 6 \oplus_2 1 = 7.$$

拡張した p' 成分定理より $\rho^{\boldsymbol{Y}}$ の $\mathrm{Sym}(7)$ への制限には奇数次数の既約成分が存在する．すなわち，$\boldsymbol{Y}$ に含まれるヤング図形のペア $\boldsymbol{Z}$ であり，計 7 個の箱からなり，$f^{\boldsymbol{Z}}$ が奇数のものがある．実際 $\boldsymbol{Z} = ((2,2,1),(2))$ とすると

$$f^{\left(\text{  }\right)} = \frac{7!}{1^3 \cdot 2^2 \cdot 3 \cdot 4} = 105.$$

以上をゲームの言葉で言い換える．まず $\mathrm{sg}_{\widetilde{\Gamma}}(\boldsymbol{A}) = \psi^{(2)}(\boldsymbol{Y}) = 7$．また，$\boldsymbol{Z}$ に対応する局面 $\boldsymbol{B}$ として $((4,3,1),(3,0))$ を取れば $\mathrm{lg}_{\widetilde{\Gamma}}(\boldsymbol{B}) = |\boldsymbol{Z}| = 7$ かつ

$$\mathrm{sg}_{\widetilde{\Gamma}}(\boldsymbol{B}) = \psi^{(2)}\left(\text{  }\right) \oplus_2 \psi^{(2)}\left(\text{  }\right) = 5 \oplus_2 2 = 7.$$

よって $\boldsymbol{B}$ は $\boldsymbol{A}$ の full な descendant であり，かつ，$\boldsymbol{A}$ と同じ Sprague-Grundy 数を持つ．

参考文献

[1] E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways for Your Mathematical Plays*, vol. 1, 2nd ed., A.K. Peters, Natick, MA, 2001.

[2] U. Blass, A. S. Fraenkel, and R. Guelman, How far can Nim in disguise be stretched?, *J. Combin. Theory Ser. A* **84(2)** (1998), 145–156.

[3] J. H. Conway, *On Numbers and Games*, 2nd ed., A.K. Peters, Natick, MA, 2001.

[4] J. S. Frame, G. de B. Robinson, and R. M. Thrall, The hook graphs of the symmetric group, *Canad. J. Math.* **6** (1954), 316–324.

[5] P. M. Grundy, Mathematics and games, *Eureka* **2** (1939), 6–8.

[6] Y. Irie, *p*-Saturations of Welter's game and the irreducible representations of symmetric groups, *J. Algebraic Combin.* **48** (2018), 247–287.

[7] Y. Irie. The Sprague-Grundy functions of saturations of misère Nim. *Electron. J. Combin.* **28(1)** (2021) #P1.58.

[8] Y. Irie. A base-*p* Sprague-Grundy type theorem for *p*-calm subtraction games: Welter's game and representations of generalized symmetric groups. To appear in *Integers* (The Elwyn Berlekamp, John Conway, and Richard Guy Memorial Volume).

[9] I. G. Macdonald, On the degrees of the irreducible representations of symmetric groups, *Bull. Lond. Math. Soc.* **3(2)** (1971), 189–192.

[10] J. B. Olsson, McKay numbers and heights of characters, *Math. Scand.* **38** (1976), 25–42.

[11] M. Osima, On the representations of the generalized symmetric group, *Math. J. Okayama Univ.* **4(1)** (1954), 39–56.

[12] 佐藤幹夫 (上野健爾 記). あるゲームについて. 第 12 回代数分科会シンポジューム報告集 (1968), 123–136.

[13] 佐藤幹夫 (榎本彦衛 記). Maya game について. 数学のあゆみ **15(1)** (1970), 73–84.

[14] 佐藤幹夫 (榎本彦衛 記). マヤ・ゲームの数学的理論. 数理解析研究所講究録 **98** (1970), 105–135.

[15] 佐藤幹夫 (梅田亨 記). 佐藤幹夫講義録 (1984 年度・1985 年度 1 学期). 数理解析レクチャー・ノート刊行会, 1989.

[16] R. P. Sprague, Über mathematische Kampfspiele, *Tohoku Math. J.* **41** (1935), 438–444.

[17] J. R. Stembridge, On the eigenvalues of representations of reflection groups and wreath products, *Pacific J. Math.* **140(2)** (1989), 353–396.

[18] C. P. Welter, The theory of a class of games on a sequence of squares, in terms of the advancing operation in a special group, *Indag. Math. (Proceedings)* **57** (1954), 194–200.

Iterative construction of Cayley-type Ramanujan graphs and its cryptographic application

Hyungrok Jo*
jo.hyungrok.gb@u.tsukuba.ac.jp

Abstract

It is an attempt to build a secure Cayley-based hash function by using combinatorial method to weave the existing Ramanujan graphs. This study is still going on with Noboru Kunihiro (University of Tsukuba) and Yoshinori Yamasaki (Ehime University).

1 Introduction

It has been developed the computational abilities of quantum computers in many aspects. Some experts assume that it could be realized the practical use of the large-scale quantum computer in approximately 15 to 30 years. These developments of quantum computer could derive the cryptanalysis to international standardized public key encryptions (PKE) or digital signature schemes (DS) using Shor's algorithm. In this context, NIST (National Institute of Standards and Technologies) suggested the standardizations of PQC (Post-Quantum Cryptography) which based on the mathematical hard problems with anti-quantum-attacks in 2016.

We are interested in building a cryptographic hash function based on expander graphs as a primitive of crypto-schemes in the era of PQC. In 2006, Charles, Goren, and Lauter[3] suggested cryptographic hash function based on two families of Ramanujan graphs as optimal structures of expander graphs. One of the families of Ramanujan graphs is constructed as Cayley graphs over finite fields with special generating sets, suggested by Lubotzky, Phillips and Sarnak in 1988. The other family of Ramanujan graph is represented by the relation between supersingular elliptic curves and their isogenies, suggested by Pizer in 1990. Variants of cryptographic hash functions based on Pizer's graph are still remained secure, it became one of main candidates in PQC standardization, named as Isogeny-based cryptography.

On the other hand, cryptographic hash functions based on LPS Ramanujan graphs are all broken so far. We are trying to build cryptographic hash functions with some tweaks of the existing Cayley-type Ramanujan graphs for mitigating insecurity of Cayley hash functions.

2 The families of LPS-type graphs

In this section, we describe how to construct the families of LPS-type graphs in [5]. First, we give the definition of a Cayley graph. Let G be a group and S a generating set, which is symmetric (i.e. $S = S^{-1}$) and does not contain the identity of G. A *Cayley graph* over G with respect to S is a $|S|$-regular graph with a vertex set V and an edge set E, where $V = G$ and E consists of $(g_1, g_2) \in G \times G$ such that $g_1 = g_2 s$ for some $s \in S$.

We recall basic facts and terminologies of quaternion algebras.

- F: a field (not of characteristic 2)

*University of Tsukuba, Faculty of Engineering, Information and Systems

- $F^\times$: the unit group of F
- $\mathcal{A} = \mathcal{A}_F(a,b) = \{\alpha = x + yi + zj + wk \,|\, x,y,z,w \in F\}$: quaternion algebra over F

For $\alpha = x + yi + zj + wk \in \mathcal{A}$,

- $\overline{\alpha} = x - yi - zj - wk$: conjugate
- $T(\alpha) = \alpha + \overline{\alpha} = 2x \in F$: reduced trace
- $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = x^2 - ay^2 - bz^2 + abw^2 \in F$: reduced norm

Throughout this report,

- $\mathbb{P}$: the set of all prime numbers
- For a prime $p \in \mathbb{P}$ and $d \in \mathbb{N}$, $\mathbb{F}_{p^d}$: the field of p^d elements
- $\left(\frac{\cdot}{\cdot}\right)$: the Kronecker symbol

Let us fix $q \in \mathbb{P} \setminus \{2\}$. When $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$, that is, $\sqrt{a}, \sqrt{-b} \in \mathbb{F}_q$, one has the following isomorphism.

Lemma 1. *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Then, the map* $\psi_q : \mathcal{A} \to \mathrm{M}_2(\mathbb{F}_q)$ *defined by*

$$\psi_q(x + yi + zj + wk) = \begin{bmatrix} x + y\sqrt{a} & \sqrt{-b}(z + w\sqrt{a}) \\ -\sqrt{-b}(z - w\sqrt{a}) & x - y\sqrt{a} \end{bmatrix}$$

is an isomorphism satisfying $\det(\psi_q(\alpha)) = N(\alpha)$ *and* $\psi_q(\overline{\alpha}) = \overline{\psi_q(\alpha)}$ *for* $\alpha \in \mathcal{A}$. *Here,* $\overline{\begin{bmatrix} s & t \\ u & v \end{bmatrix}} = \begin{bmatrix} v & -t \\ -u & s \end{bmatrix}$ *for* $\begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{M}_2(\mathbb{F}_q)$.

For a ring R, we denote by $R^\times$ the group of units of R. Let $\mathrm{GL}_2(\mathbb{F}_q) = \mathrm{M}_2(\mathbb{F}_q)^\times$ and $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in \mathrm{GL}_2(\mathbb{F}_q) \,|\, \det A = 1\}$. Moreover, let $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/Z(\mathrm{GL}_2(\mathbb{F}_q))$ and $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/Z(\mathrm{SL}_2(\mathbb{F}_q))$. Here, for a group G, we denote by $Z(G)$ the *center* of G. We can naturally see that $\mathrm{PSL}_2(\mathbb{F}_q)$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ of index 2 because now q is odd. Additionally, we remark that $|\mathrm{PGL}_2(\mathbb{F}_q)| = q(q^2-1)$ and $|\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{q(q^2-1)}{2}$. Since $\mathcal{A} \simeq \mathrm{M}_2(\mathbb{F}_q)$, we have $\mathcal{A}^\times \simeq \mathrm{GL}_2(\mathbb{F}_q)$ via (the restriction of) ψ_q and hence obtain the isomorphism $\beta_q : \mathcal{A}^\times/Z(\mathcal{A}^\times) \to \mathrm{PGL}_2(\mathbb{F}_q)$.

We need the following lemma later.

Lemma 2. *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Let* $\alpha \in \mathcal{A}$ *with* $N(\alpha) = p \in \mathbb{P} \setminus \{q\}$, *which implies that* $\alpha \in \mathcal{A}^\times$. *Then,* $\beta_q(\alpha\mathbb{F}_q^\times) \in \mathrm{PSL}_2(\mathbb{F}_q)$ *if and only if* $\left(\frac{p}{q}\right) = 1$.

Quaternion algebras over $\mathbb{Q}$

Let $a, b \in \mathbb{Z} \setminus \{0\}$. We consider $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a,b)$ a quaternion algebra over $\mathbb{Q}$.

A place v of $\mathbb{Q}$ is said to be *split* in $\mathcal{A}$ if $\mathcal{A}_v := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq \mathrm{M}_2(\mathbb{Q}_v)$, where $\mathbb{Q}_v$ is the v-adic completion of $\mathbb{Q}$ and is said to be *ramified* if $\mathcal{A}_v$ is a division algebra.

- $\mathrm{Ram}(\mathcal{A})$: the set of all places which are ramified in $\mathcal{A}$
- $\mathfrak{D}$, The product of all primes (= finite places) in $\mathrm{Ram}(\mathcal{A})$: *discriminant* of $\mathcal{A}$

From now on, we assume that $\mathcal{A}$ is definite, that is, the infinite place ∞ is ramified in $\mathcal{A}$, whence there are an odd number of primes which are ramified in $\mathcal{A}$. Notice that $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a, b)$ is definite if and only if $a < 0$ and $b < 0$.

- $\mathcal{I} \subset \mathcal{A}$, a free $\mathbb{Z}$-submodule of $\mathcal{A}$ of rank 4 : a lattice
- a lattice $\mathcal{O} \subset \mathcal{A}$ if it is a ring with unity : an order
- an order $\mathcal{O} \subset \mathcal{A}$ if it is not properly contained in any other order : maximal order

Notice that, if $\mathcal{O}$ is an order of $\mathcal{A}$, then $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is an order of $\mathcal{A}_p$ for $p \in \mathbb{P}$. Here, $\mathbb{Z}_p$ is the ring of p-adic integers.

Let $\mathcal{O}$ be an order of $\mathcal{A}$. We call a lattice $\mathcal{I}$ of $\mathcal{A}$ a *left* (resp. *right*) $\mathcal{O}$*-ideal* if $\mathcal{O}_L(\mathcal{I}) = \mathcal{O}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \mathcal{O}$), where $\mathcal{O}_L(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \alpha\mathcal{I} \subset \mathcal{I}\}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \mathcal{I}\alpha \subset \mathcal{I}\}$). We say that two left (resp. right) $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$ are equivalent if there exists $\alpha \in \mathcal{A}^{\times}$ such that $\mathcal{I} = \mathcal{J}\alpha$ (resp. $\mathcal{I} = \alpha\mathcal{J}$).

This is an equivalence relation. We denote by $\mathfrak{h}(\mathcal{O})$ the number of equivalence classes, which is shown to be finite, independent on left or right. We call $\mathfrak{h}(\mathcal{O})$ the *class number* of $\mathcal{O}$.

Now, it is necessary to recall Ibukiyama's construction of maximal orders of definite quaternion algebras over $\mathbb{Q}$ which is ramified at given primes.

Proposition 1. *Let r be an odd positive integer and $P_1, P_2, \ldots, P_r$ distinct prime numbers. Set $M = P_1P_2\cdots P_r$. Take a prime number Q such that $Q \equiv 3 \pmod 8$ and $(\frac{-Q}{P_i}) = -1$ for all i except for i with $P_i = 2$. Moreover, take an integer T such that $T^2 \equiv -M \pmod Q$. Then, $\mathcal{A}_{\mathbb{Q}}(-M, -Q)$ is a definite quaternion algebra which is ramified only at $\infty, P_1, P_2, \ldots, P_r$. Moreover, let*

$$\omega_1 = \frac{1+j}{2}, \quad \omega_2 = \frac{i+k}{2} \quad \text{and} \quad \omega_3 = \frac{Tj+k}{Q}.$$

Then, $\mathcal{O}_{-M,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ is a maximal order of $\mathcal{A}_{\mathbb{Q}}(-M, -Q)$.

In [5] a recipe for constructing LPS-type graphs is presented, and is shown below:

1. Fix a $p \in \mathbb{P}$.
2. Take $P \in \{2, 3, 5, 7, 13\}$ such that $P \neq p$.
3. We take a prime Q satisfying

   $$Q \equiv 3 \pmod 8, \left(\frac{-Q}{P}\right) = -1 \text{ unless } P = 2$$

   and an integer T satisfying $T^2 \equiv -P \pmod Q$. By Proposition 1, we have a definite quaternion algebra $\mathcal{A}_{\mathbb{Q}}(-P, -Q)$ (i.e., $i^2 = -P, j^2 = -Q, ij = -ji = k$) and its maximal order $\mathcal{O} = \mathcal{O}_{-P,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ with class number 1, where

   $$\omega_1 = \frac{1+j}{2}, \ \omega_2 = \frac{i+k}{2} \text{ and } \omega_3 = \frac{Tj+k}{Q}.$$

4. Find all elements in $\mathcal{O}^{\times} = \{\alpha \in \mathcal{O} \mid N(\alpha) = 1\}$.
5. Find all elements in $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}$. Moreover, seek a suitable complete representative of $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}/\mathcal{O}^{\times}$. Define S by the suitable complete representative. Then $|S|$ is exactly equal to $p + 1$, which follows by $\mathfrak{h} = 1$ condition.

6. Take a $q \in \mathbb{P} \setminus \{2\}$ satisfying $q \neq p$, $\left(\frac{-P}{q}\right) = \left(\frac{Q}{q}\right) = 1$ and $\left(\frac{p}{q}\right) = 1$.
7. Via the isomorphism ψ_q in Lemma 1 and using Lemma 2, we realize S as a subset of $\mathrm{PSL}_2(\mathbb{F}_q)$. Write S_{JSY} for the subset.
8. We have a Cayley graph $X_{P,Q}^{(p,q)} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S_{JSY})$.

3 Hash function

A *hash function* is a function that inputs a message as a bit string of arbitrary length and outputs (or compresses) a hash value as a bit string of fixed length. It should be efficient to hash, because of its primitivity. Such a function can be evaluated its security by certain properties, such as *collision resistant, second preimage resistant* and *preimage resistant*.

Let $n \in \mathbb{N}$ and let $H : \{0,1\}^* \to \{0,1\}^n$; $m \mapsto h = H(m)$, where $\{0,1\}^*$ is the set of bit strings of arbitrary length and $\{0,1\}^n$ is the set of bit strings of a fixed length n. The function H is said to be

- **Collision resistant** if it is *computationally infeasible* to find $m, m' \in \{0,1\}^*, m \neq m'$, such that $H(m) = H(m')$,
- **Second preimage resistant** if $m \in \{0,1\}^*$ is given, it is *computationally infeasible* to find $m' \in \{0,1\}^*$, $m \neq m'$, such that $H(m) = H(m')$,
- **Preimage resistant** if $h \in \{0,1\}^n$ is given, it is *computationally infeasible* to find $m \in \{0,1\}^*$ such that $h = H(m)$.

4 Cayley hash function

Let G be a non-commutative group and $S = \{s_0, \ldots, s_p\} \subset G$ be a generating set for the group G, symmetric and not having the identity. Charles, Goren and Lauter[3] described a definition of Cayley hash functions, by which the input to hash is used as directions for walking along a path of a graph, and the ending vertex is the output of the hash function.

A message m is given as a string $m_1 \cdots m_\ell$, where $m_i \in \{0, \ldots, p\}$. Then the resulting hashing value h of m will be obtained as a group product

$$h := H(m) = g_{ST} s_{m_1} s_{m_2} \cdots s_{m_\ell},$$

where g_{ST} is a fixed starting element in G. (We usually put g_{ST} as the identity in G.) To dispose a proper sequence of hashing bits inductively, we define a *choice function* π which assigns a next hashing bit with the bit of the message m and the previous hashing bit, while avoiding a back-tracking (i.e. ss^{-1} or $s^{-1}s$). We choose a function

$$\pi : \{0, \ldots, p\} \times S \to S \tag{1}$$

such that for any $s \in S$ the set $\pi(\{0, \ldots, p\} \times \{s\})$ is equal to $S \setminus \{s^{-1}\}$.

The security of Cayley hash functions lies on the hardness of solving *word problems* for group theory. Refer to [5] for more details.

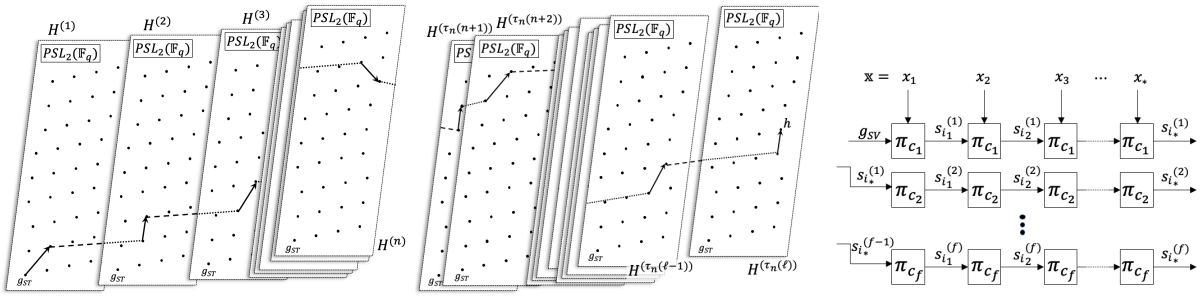


Figure 1: Cayley hash function-map.

5 Cayley hash function-map

In this section, we explain how to construct Cayley hash function-map which is presented in CSS2019 (Computer Security Symposium 2019).

By following the recipe in Section 2, we set up n numbers of LPS-type Ramanujan graphs (the case of $P = 13$) for constructing *Cayley hash function-map*. We construct n numbers of $X^{(p,q)}_{13,Q^{(i)}} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S^{(i)}_{JSY})$ for $i \in \{1, \ldots, n\}$.

1. Fix $p \in \mathbb{P}$, which determines the regularity $(p+1)$ of LPS-type Ramanujan graphs as mentioned in Section 2.
2. Choose n numbers of distinct $Q^{(i)} \in \mathbb{P}$ which satisfies $Q^{(i)} \equiv 3 \pmod 8$ and $\left(\frac{-Q^{(i)}}{P}\right) = -1$.
3. Fix $q \in \mathbb{P} \setminus \{2, p\}$ which satisfies $\left(\frac{-13}{q}\right) = \left(\frac{Q^{(i)}}{q}\right) = 1$ and $\left(\frac{p}{q}\right) = 1$ for all $i \in \{1, \ldots, n\}$.

Then we have the same group $\mathrm{PSL}_2(\mathbb{F}_q)$ of the size $\frac{q(q^2-1)}{2}$ and n numbers of corresponding generating sets $S^{(i)}_{JSY}$ for each $X^{(p,q)}_{13,Q^{(i)}}$.

Now we construct Cayley hash function-map H as $\{H^{(1)}, H^{(2)}, \ldots, H^{(n)}\}$ with corresponding individual consecutive choice function $\pi^{(1)}, \pi^{(2)}, \ldots, \pi^{(n)}$. We consider that a message m is given as a string $m_1 \cdots m_\ell$, where $m_i \in \{0, \ldots, p\}$ and $\ell > n$. Then the resulting hashing value h of m will be obtained as a group product

$$\begin{aligned} h &:= H(m) \\ &= H^{(\ell(n))}(H^{(\ell-1(n))}(\ldots, (H^{(1)}, g_{ST}), \ldots), m_{\ell-1}), m_\ell) \\ &= g_{ST} s_{m_1} s_{m_2} \cdots s_{m_\ell}, \end{aligned}$$

where g_{ST} is a fixed starting element as the identity in G. To dispose a proper sequence of hashing bits inductively, we define a *choice function* $\pi^{(i)}$ which assigns a next hashing bit with the bit of the message m from $S^{(i-1)}_{JSY}$ and the previous hashing bit from $S^{(i)}_{JSY}$, while avoiding a back-tracking (i.e. $s_{i-1}s_i^{-1}$ or $s_{i-1}^{-1}s_i$). We choose a function

$$\pi^{(i)} : \{0, \ldots, p\} \times S^{(i-1)}_{JSY} \to S^{(i)}_{JSY} \tag{2}$$

such that for any $s \in S^{(i-1)}_{JSY}$ the set $\pi^{(i)}(\{0, \ldots, p\} \times \{s\})$ is equal to $S^{(i)}_{JSY} \setminus \{s^{-1}\}$.

5.1 Expected vurnerability of Cayley hash function-map

In this report, it is omitted about a *lifting attack* which is the most powerful existing attack to Cayley hash function. Refer to [5] for more details.

For the purpose of mitigating insecure parts against a lifting attack, we simply weave the existing LPS-type graphs by only adjusting their parameters (size of graph, size of generating sets, etc). However, there are some natural questions for requirements of hash functions.

Q1. Is it mixing well if we do random walk on this new graph?

Q2. Is it guarantee that the new graph has a large girth?

For Q1., we expect that it is mixing well enough for using hash function. Since the new graph is also a regular graph, if we do random walk on the graph, it will derive uniform distribution. Besides, even if it is not known the specific expansion measurements, it should be mixing well because of the Ramanujan-ness of each graph.

For Q2., it is not known at all. It is less than the girth of the existing Ramanujan graphs. However, these arguments are also related to the Ramanujan-ness of the graphs. It seems to be better to find a way to weave each Ramanujan graph "well" without a loss of spectral goodness, instead of simply putting graphs together.

6 Possible approaches by combinatorial methods

For answering the Q2. in Subsection 5.1, we consider the zig-zag product in graphs. It is the method for taking two graphs X and Y and creating a larger graph whose spectral gap is controlled by the spectra of X and Y.

Let $X := (V_X, E_X)$ be a k_X-regular graph and $Y := (V_Y, E_Y)$ be a k_Y-regular graph such that $k_X = |Y|$. For each vertex $v \in V_X$, let $E_v = \{e \in E_X \mid v \text{ is an endpoint of } e\}$, and let $L_v : V_Y \to E_v$ be a bijection. We call L_v, the labeling at v. Moreover, $L = \{L_v \mid v \in V_Y\}$ is the labeling from Y to X.

We define a *zig-zag product* $X \otimes_Z Y$ with a labeling L if $(x_1, y_1), (x_2, y_2)$ in $X \otimes_Z Y$ then the multiplicity of the edge between them equals the number of ordered pairs $(z_1, z_2) \in E_Y \times E_Y$ such that y_1 is an endpoint of z_1, y_2 is an endpoint of z_2 and $L_{x_1}(z_1(y_1)) = L_{x_2}(z_2(y_2))$. Then, it is known that $X \otimes_Z Y$ is k_Y^2-regular graph with a labeling L.

Under certain circumstances, the zig-zag product of two Cayley graphs on two groups G and H equals a Cayley graph on the semi-direct product $G \rtimes H$. Then, it is also known that $\mathrm{Cay}(G, \Gamma) \otimes_Z \mathrm{Cay}(H, \Lambda) = \mathrm{Cay}(G \rtimes_\theta H, \Omega)$, where Ω is the multiset $\{\sigma_1 \gamma \sigma_2 \mid (\sigma_1, \sigma_2) \in \Lambda \times \Lambda\}$. Refer to [6] for more details.

From these facts, if we construct hash functions based on the zig-zag product of LPS-type Ramanujan graphs, we have less sparse graphs and it can be also represented by semi-direct product of Cayley graphs. In LPS-type case, the girth of graphs is larger than $2 \log_p q$. We expect to argue the girth of the zig-zag product of LPS-type Ramanujan graphs in a similar manner of LPS-type graphs.

It is necessary to study the specific way to construct hash functions based on the zig-zag product of graphs and their cryptographic properties.

Acknowledgements

I would like to thank all organizers of Symposium on Algebraic Combinatorics for giving me a valuable opportunity. This work was supported by JST CREST Grant Number JPMJCR14D6, Japan.

References

[1] Alon, N., Lubotzky, A., & Wigderson, A. (2001, October). Semi-direct product in groups and zig-zag product in graphs: connections and applications. In Proceedings 42nd IEEE Symposium on Foundations of Computer Science. IEEE., 630-637.

[2] Ben-Aroya, A., & Ta-Shma, A. (2011). A combinatorial construction of almost-Ramanujan graphs using the zig-zag product. SIAM Journal on Computing, 40(2), 267-290.

[3] Charles, D. X., Lauter, K. E., & Goren, E. Z. (2009). Cryptographic hash functions from expander graphs. Journal of CRYPTOLOGY, 22(1), 93-113.

[4] Hoory, S., Linial, N., & Wigderson, A. (2006). Expander graphs and their applications. Bulletin of the American Mathematical Society, 43(4), 439-561.

[5] Jo, H., Sugiyama, S., & Yamasaki, Y. (2021). Ramanujan Graphs for Post-Quantum Cryptography., International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, vol 33., 231-250.

[6] Krebs, M., & Shaheen, A. (2011). Expander families and Cayley graphs: a beginner's guide. Oxford University Press.

[7] Reingold, O., Vadhan, S., & Wigderson, A. (2000, November). Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In Proceedings 41st Annual Symposium on Foundations of Computer Science. IEEE., 3-13.

[8] Rozenman, E., Shalev, A., & Wigderson, A. (2006). Iterative construction of Cayley expander graphs. Theory OF Computing, 2(1), 91-120.