Proceedings of

Algebra and Computation 2013

Tokyo Metropolitan University

December 17-19, 2013

Edited by AC2013 Proceedings Committee

Organizers

Hirofumi Tsumura (Tokyo Metropolitan Univ.)
Shigenori Uchiyama (Tokyo Metropolitan Univ.)
Katsushi Waki (Yamagata Univ.)
Takuya Ikuta (Kobe Gakuin Univ.)
Yukihiro Uchida (Tokyo Metropolitan Univ.)

第 10 回「代数学と計算」研究集会 (AC2013)

標記の研究集会を下記の要領で開催いたしますので, ご案内申し上げます.

主催者

津村 博文 (首都大学東京)
内山 成憲 (首都大学東京)
脇 克志 (山形大学)
生田 卓也 (神戸学院大学)
内田 幸寛 (首都大学東京)

記

日時：2013 年 12 月 17 日 (火) – 19 日 (木)
場所：首都大学東京 11 号館 204 大教室

[プログラム]
Dec. 17（Tue.）

10:20 - 10:25: Opening

10:30 - 11:00: 小松尚夫 (弘前大学)

"Balancing with binomial coefficients"

11:00 - 11:30: O.Khadir(University of Hassan II Mohammedia-Casablanca), 小松尚夫 (弘前大学)

"On the modular equation $3^x \equiv b$ [p] when p is prime"

11:40 - 12:00: 森川良三 (長崎大学・名誉教授)

"ある整数の集合を二つの部分集合の直和に分解すること"

14:00 - 14:50: [特別講演] 横田佳之 (首都大学東京)

"二重対数関数と結び目不変量"

15:00 - 15:30: 竹森翔 (京都大学)

"Sage での degree 2 のジーゲル保型形式の計算について"

15:30 - 15:50: 筒石奈央 (津田塾大学)

"至る所 good reduction をもつ代数体上の楕円曲線の決定方法とその計算"

16:00 - 16:50: [特別講演] 河原林健一 (国立情報学研究所)

"巨大グラフの解析とアルゴリズム"

Dec. 18（Wed.）

10:00 - 10:30: 籾原幸二 (熊本大学)
"Skew Hadamard difference set の非同値性の問題について"

10:30 - 11:00: 佐々木義卓 (大阪体育大学), 大野泰生 (近畿大学)
"多重 Euler 数の諸性質について"

11:10 - 11:40: 平野康之 (鳴門教育大学), 隅山孝夫 (愛知工業大学)
"正整数上へのある作用の繰り返しの振る舞い"

13:30 - 14:20: [特別講演] 野崎寛 (愛知教育大学)
"有向グラフの複素球面埋め込みに関するアルゴリズム"

14:35 - 15:05: 平尾将剛 (東京女子大学), 澤正憲 (名古屋大学)
"有限既約鏡映群による最適実験計画の分類について"

15:05 - 15:30: 林怡伶 (名古屋大学), 三嶋美和子 (岐阜大学), 佐藤潤也 (名古屋大学), 神保雅一 (名古屋大学)
"可逆元の位数と等差衝突回避符号への応用"

15:45 - 16:05: 山田紘頌 (東京理科大学), 宮本暢子 (東京理科大学)
"Baer subplane による直交配列の構成"

16:05 - 16:35: 澤正憲 (名古屋大学)
"Ellison の誤り – Waring 問題"

16:45 - 17:15: 須田庄 (愛知教育大学), 野崎寛 (愛知教育大学)
"Weighing matrix に関連したアソシエーションスキームについて"

Dec. 19（Thu.）

10:00 - 10:30: 横山俊一 (九州大学)
“Magma による多変数多項式の終結式計算の高速化について”

10:40 - 11:10: 原瀬晋 (東京工業大学), 大堀龍一 (東京大学)
“拡張可能性を有する低 WAFOM 点集合の探索”

13:30 - 14:20: [特別講演] 木村巌 (富山大学)
“モジュラー形式の計算”

14:30 - 15:00: 谷口哲也 (学習院大学)
“「総当たり GCD」の高速計算について”

15:00 - 15:30: 安田貴徳 (九州先端科学技術研究所), 高木剛 (九州大学), 櫻井幸一 (九州大学/九州先端科学技術研究所)
“数体上の楕円曲線のペアリングに適した還元”

15:40 - 16:00: 宮脇朗 (大阪大学), 綾野孝則 (大阪大学), 鈴木譲 (大阪大学)
“Super-elliptic 曲線を用いたペアリングに基づく暗号にむけて-原澤-鈴木によるヤコビ多様体の表現-”

16:00 - 16:20: 早坂健一郎 (九州大学), 青木和麻呂 (NTT セキュアプラットフォーム研究所), 小林鉄太郎 (NTT セキュアプラットフォーム研究所), 高木剛 (九州大学)
“拡大体 $GF(p^n)$ 上の数体篩法における 3 次元 Lattice Sieve の構成”

16:20 - 16:40: 高橋龍介 (岡山大学), 野上保之 (岡山大学)
“拡大体における巡回ベクトル乗算アルゴリズムとその部分体への効率的な適用”

16:40 - 16:50: Closing

Sageでの degree 2のジーゲル保型形式の計算について

竹森 翔

Abstract

In this paper, we introduce a package of Sage [7] for the calculation of Siegel modular forms of degree 2.

1 Introduction

Sage [7] is a free and open software for various areas of mathematics. With Sage, we can compute many number theoretical objects including modular forms of one variable i.e. elliptic modular forms. But we cannot compute modular forms of several variables such as Siegel modular forms with built-in functions of Sage. The author wrote a package [8] for Siegel modular forms of degree two. In this paper, we introduce the package by computing Hecke eigenforms. This paper does not contain any new mathematical results.

2 Definitions

In this section, we recall the definition and related topics of Siegel modular forms.

2.1 Definition of Siegel modular forms of degree n

Let n be a positive integer and define the Siegel modular group of degree n by

$$\Gamma_n := \left\{ g \in \mathrm{GL}_{2n}(\mathbb{Z}) \;\middle|\; {}^t g w_n g = w_n \right\}.$$

Here $w_n = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$. Note that $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$. Define Siegel upper half space $\mathfrak{H}_n$ by

$$\mathfrak{H}_n := \left\{ Z = X + iY \;\middle|\; X,\ Y \in \mathrm{Sym}_n(\mathbb{R}),\ Y \text{ is positive definite} \right\}.$$

For a non-negative integer k, let $M_k(\Gamma_n)$ the the set of holomorphic functions F on $\mathfrak{H}_n$ satisfying the following condition:

$$F((AZ+B)(CZ+D)^{-1}) = \det(CZ+D)^k F(Z), \quad \forall \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n.$$

If $n = 1$, we add the cusp condition. We call an element of $M_k(\Gamma_n)$ a Siegel modular form of degree n and weight k (and level 1). If $n = 1$, $M_k(\Gamma_1)$ is equal to the space of elliptic modular forms of weight k. It is known that $M_k(\Gamma_n)$ is a finite dimensional vector space over $\mathbb{C}$.

2.2 Fourier expansion of Siegel modular forms of degree two

Let $F \in M_k(\Gamma_2)$ be a Siegel modular form of degree 2. We put $Z = \begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix} \in \mathfrak{H}_2$. Then F has the following Fourier expansion:

$$F\left(\begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix}\right) = \sum_{\substack{n,\, r,\, m \in \mathbb{Z} \\ n,\, m,\, 4nm - r^2 \geq 0}} a((n,r,m), F)\mathbf{e}(n\tau + rz + m\omega),$$

where $\mathbf{e}(z) = \mathrm{e}(2\pi i z)$ for $z \in \mathbb{C}$. With the notation above, we define the Siegel operator $\Phi : M_k(\Gamma_2) \to M_k(\Gamma_1)$ by

$$\Phi(F) := \sum_{n=0}^{\infty} a((n,0,0), F)\mathbf{e}(nz).$$

We define the space of cusp forms $S_k(\Gamma_2)$ of degree 2 by

$$S_k(\Gamma_2) := \ker \Phi \subseteq M_m(\Gamma_2).$$

2.3 Hecke polynomials

Let $n = 1$ or 2. For $m \in \mathbb{Z}_{\geq 1}$, let $T(m) \in \mathrm{End}_{\mathbb{C}}(M_k(\Gamma_n))$ the mth Hecke operator. We omit the definition of $T(m)$. See [1] for the definition. For a prime p and $F \in M_k(\Gamma_n)$, define a polynomial $Q_p^{(n)}(F;X)$ as follows.

1. If $n = 1$, then we define
$$Q_p^{(1)}(F;X) = 1 - \lambda(p)X + p^{k-1}X^2.$$
2. If $n = 2$, then we define
$$Q_p^{(2)}(F;X) = 1 - \lambda(p)X + \left(\lambda(p)^2 - \lambda(p^2) - p^{2k-4}\right)X^2 - \lambda(p)p^{2k-3}X^3 + p^{4k-6}X^4.$$

Remark 1. $Q_p^{(n)}(F;p^{-s})^{-1}$ is the Euler factor of spinor L-function of F.

3 Structure theorem for the ring of Siegel modular forms of degree 2

In this section, we recall the structure theorem for the ring of Siegel modular forms of degree 2 proved by Igusa [3]. The structure theorem and the explicit formula for Siegel Eisenstein series of degree 2 enable us to compute Siegel modular forms of degree 2 explicitly.

Let
$$M(\Gamma_2) = \bigoplus_{k \in \mathbb{Z}_{\geq 0}} M_k(\Gamma_2)$$
be the ring of Siegel modular forms of degree 2. Put
$$x_{10} := E_4E_6 - E_{10},$$
$$x_{12} := 3^2 \cdot 7^2E_4^3 + 2 \cdot 5^3E_6^2 - 691E_{12},$$
where E_k is the Siegel-Eisenstein series of degree 2 and weight k. Then x_{10} and x_{12} are Siegel cusp forms of weight 10 and 12 respectively. For $k = 10,\ 12$, we put
$$X_k := \frac{1}{a((1,1,1),x_k)}x_k.$$

The following theorem was proved by Igusa [3].

Theorem 1. *1. There exists a weight* 35 *cusp form* X_{35} *(we normalize* X_{35} *so that* $a((2,-1,3),X_{35})=1$*).*

2. E_4, E_6, X_{10}, X_{12} *and* X_{35} *generate* $M(\Gamma_2)$ *as a* $\mathbb{C}$*-algebra.*

3. E_4, E_6, X_{10} *and* X_{12} *are algebraically independent over* $\mathbb{C}$*.*

The Fourier coefficients of Siegel-Eisenstein series of degree 2 was known by Kaufhold [4]. Aoki and Ibukiyama [2] proved that cusp form X_{35} of weight 35 can be written by a polynomial of Siegel-Eisenstein and its differentials. Thus the generators of the ring $M(\Gamma_2)$ can be written by the polynomials of Siegel-Eisenstein series of degree 2 and its differentials. Therefore we can compute the Fourier coefficients of an element of $M(\Gamma_2)$ explicitly.

4 Computation of elliptic modular forms

In this section, we compute Hecke polynomial of elliptic cusp forms by using built-in functions of Sage.

```
R.<x> = PolynomialRing(QQ, 1, order='neglex')
def euler_factor_of_l(f, p):
   wt = f.weight()
   return 1 - f[p]/f[1]*x + p^(wt-1)*x^2
wts_of_one_dim = \
   [k for k in range(12, 30)
       if CuspForms(1, k).dimension() == 1]
```

In the code above, we compute $Q_p^{(1)}(f;X)$ for $p=2$ and $f \in S_k(\Gamma_1)$ with $\dim S_k(\Gamma_1)=1$. The function **euler_factor_of_l** takes an eigenform and a prime p and returns $Q_p^{(1)}(f;X)$. **wts_of_one_dim** is the list of the positive integers k such that $12 \leq k < 30$ and $\dim S_k(\Gamma_1)=1$.

```
euler_factor_at_2 = {}
for k in wts_of_one_dim:
    f = CuspForms(1, k).basis()[0]
    euler_factor_at_2[k] = euler_factor_of_l(f, 2)
```

The python's dictionary **euler_factor_at_2** is a dictionary such that $k \mapsto Q_2^{(1)}(f_k;X)$, which value is as follows:

```
sage: euler_factor_at_2
{12: 1 + 24*x + 2048*x^2,
 16: 1 - 216*x + 32768*x^2,
 18: 1 + 528*x + 131072*x^2,
 20: 1 - 456*x + 524288*x^2,
 22: 1 + 288*x + 2097152*x^2,
 26: 1 + 48*x + 33554432*x^2}
```

For example the $Q_2^{(1)}(\Delta; X) = 1+24X+2048X^2$, where Δ is the Ramanujan's delta.

5 Computation of Siegel modular forms in Sage

In this section, we compute Siegel modular forms of degree 2 by using the package [8]. The following code has been tested under Sage 6.11 and "degree2" (revision 706bfe).

5.1 Computation of generators of $M(\Gamma_2)$

The generator X_{10} can be obtained by the function **x10_with_prec(prec)**. Here the argument **prec** is a positive integer and this function computes the Fourier coefficients of X_{10} for

$$\left\{(n,r,m) \;\middle|\; 0 \leq n, m \leq \mathbf{prec},\ 4nm - r^2 \geq 0\right\}.$$

X_{12} and X_{35} can be obtained by the function **x12_with_prec(prec)** and **x35_with_prec(prec)**. Siegel-Eisenstein series E_k can be obtained by the function **eisenstein_series_degree2(k, prec)**. Here are examples.

```
from degree2.all import *

prec = 4
# The cusp forms of weight 10 and 12.
X10 = x10_with_prec(prec)
X12 = x12_with_prec(prec)
```

```
# Fourier coefficient of X10 at (1, 1, 1).
X10[(1, 1, 1)] # => 1
# Fourier coefficient of X10 at (3, 5, 4).
X10[(3, 5, 4)] # => 2736
```

5.2 Computation of Hecke polynomials

We define the following space:

$$N_k(\Gamma_2) = \{F \in M_k(\Gamma_2) | a((0,0,0), F) = 0\},$$

Then we have

$$M_k(\Gamma_2) = \mathbb{C}E_k \oplus N_k(\Gamma_2),$$

as Hecke modules. Since Fourier coefficients of Siegel-Eisenstein series E_k is known, we calculate $Q_p^{(2)}(F; X)$ for $p = 2$, $F \in M_k(\Gamma_2)$ and a small weight k.

In our package, we can create the space $N_k(\Gamma_2)$ by the function **KlingenEisensteinAndCuspForms**. To obtain an eigenform of weight 12, we compute the characteristic polynomial of $T^{(2)}(2)$ on $N_{12}(\Gamma_2)$.

```
sage: N12 = KlingenEisensteinAndCuspForms(12, 5)
sage: N12.hecke_matrix(2).charpoly().factor()
(x - 2784) * (x + 24600)
sage: G12 = N12.eigenform_with_eigenvalue_t2(-24600)
sage: F12 = G12 * G12[(1, 0, 0)]^(-1)
```

Here **G12** is an eigenform of $N_{12}(\Gamma_2)$ whose eigenvalue of $T^{(2)}(2)$ is equal to -24600 and **F12** is a constant multiple of **G12** whose Fourier coefficient at $(1, 0, 0)$ is 1. We compute the image of **G12** under the Siegel operator $\Phi : M_{12}(\Gamma_2) \to M_{12}(\Gamma_1)$.

```
sage: F12.phi_operator()
{1: 1, 2: -24, 3: 252, 4: -1472, 5: 4830}
delta = CuspForms(1, 12).basis()[0]
q - 24*q^2 + 252*q^3 - 1472*q^4 + 4830*q^5 + O(q^6)
```

So we have $\Phi(F_{12}) = \Delta$, where Δ is the Ramanujan's delta. We can compute the polynomial $Q_p^{(2)}(F_{12}; X)$ for $p = 2$ as follows.

```
sage: F12.euler_factor_of_spinor_l(2).factor()
(1 + 24*x + 2048*x^2) * (1 + 24576*x + 2147483648*x^2)
```

The first factor is equal to $Q_2^{(1)}(\Delta; x)$ and the second factor is equal to $Q_2^{(1)}(\Delta; 2^{10}x)$. Here is an another example.

```
sage: N16 = KlingenEisensteinAndCuspForms(16, 4)
sage: F16 = N16.eigenform_with_eigenvalue_t2(3539160)
sage: F16.euler_factor_of_spinor_l(2).factor()
(1 - 3538944*x + 8796093022208*x^2) * (1 - 216*x + 32768*x^2)
```

Here **F16** is an eigenform of $N_{16}(\Gamma_2)$ whose eigenvalue of $T^{(2)}(2)$ is equal to 3539160. By the result of the previous section, we see that the polynomial $Q^{(2)}(F_{16}; X)$ is equal to $Q^{(1)}(f_{16}; X)Q^{(1)}(f_{16}; 2^{14}X)$, where $f_{16} \in S_{16}(\Gamma_1)$ is the normalized eigenform.

The examples above can be explained by the following theorem:

Theorem 2 (Klingen [5], Maass [6])**.** *There exists a $\mathbb{C}$-linear injective map $E : S_k(\Gamma_1) \hookrightarrow N_k(\Gamma_2)$ such that $\Phi \circ E = \mathrm{id}$. For an eigenform $f \in S_k(\Gamma_1)$, $E(f)$ is also an eigenform and we have*

$$Q_p^{(2)}(E(f); X) = Q_p^{(1)}(f; X)Q_p^{(1)}(f; p^{k-2}X),$$

for all prime p.

Remark 2. Here we state the special case of the theorem. More general statements were proved by Klingen [5] and Zharkovskaya [9].

Sho Takemori
Department of Mathematics,
Kyoto University
Kitashirakawa-Oiwake-Cho, Sakyo-Ku,
Kyoto, 606-8502, Japan
E-mail: takemori@math.kyoto-u.ac.jp

References

[1] A. N. Andrianov and V. G. Zhuravlev, *Modular forms and Hecke operators*, no. 145, American Mathematical Soc., 1995.

[2] H. Aoki and T. Ibukiyama, *Simple graded rings of Siegel modular forms, differential operators and Borcherds products*, International Journal of Mathematics **16** (2005), no. 03, 249–279.

[3] J. Igusa, *On siegel modular forms of genus two*, American Journal of Mathematics (1962), 175–200.

[4] G. Kaufhold, *Dirichletsche Reihe mit Funktionalgleichung in der Theorie der Modulfunktion 2. Grades*, Mathematische Annalen **137** (1959), no. 5, 454–476.

[5] H. Klingen, *Zum Darstellungssatz für Siegelsche Modulformen*, Mathematische Zeitschrift **102** (1967), no. 1, 30–43.

[6] H. Maass, *Die Primzahlen in der Theorie der Siegelschen Modulfunktionen*, Mathematische Annalen **124** (1951), no. 1, 87–122.

[7] W. A. Stein et al., *Sage Mathematics Software (Version 6.1.1)*, The Sage Development Team, 2014, `http://www.sagemath.org`.

[8] S. Takemori, *degree2*, `https://github.com/stakemori/degree2`.

[9] N. A. Zharkovskaya, *The Siegel operator and Hecke operators*, Functional analysis and its applications **8** (1974), no. 2, 113–120.

Skew Hadamard difference set の非同値性の問題について

熊本大学教育学部　　籾原　幸二*
Koji Momihara
Faculty of Education, Kumamoto University

概 要

この論文では, difference set の同値性の新たな不変量 (素数を法とする三重交差数) を導入し, Feng-Xiang [9] が与えた Skew Hamadard difference set の構成法が Paley difference set と非同値なものを無限個与えることを示す.

キーワード: skew Hamadard difference set; Paley difference set; 三重交差数

1　導入

この論文では, 基本可換群上のある difference set の非同値性の問題を扱う. 証明を行わない箇所もあるので, 詳細は論文 [14] を参照していただきたい.

可換群 G の部分集合 D に対し, $\{x-y \,|\, x,y \in D, x \neq y\}$ という多重集合が G の単位元以外の元を一定数回 (λ 回) 被覆するとき, D を difference set と呼ぶ. 特に, D が $D \cup -D \cup \{0\} = G$ かつ $D \cap -D = \emptyset$ を満たすとき, D は skew Hadamard であると呼ぶ. このとき, 明らかに $|D| = (|G|-1)/2$, $\lambda = (|G|-3)/4$ であり, $|G| \equiv 3 \pmod 4$ でなければならない. (もちろん, difference set の概念は非可換な群へ定義を拡張することはできるが, 本研究では可換な場合のみを扱う.) 例えば, $q \equiv 3 \pmod 4$ なる素数べき q に対し, $\mathbb{F}_q$ の非零平方元からなる集合は skew Hadamard difference set を成し, Paley difference set(または平方剰余差集合) と呼ばれている.

今, 興味があるのは skew Hadmard difference set の非同値性についてである. ここで, G の二つの部分集合 D_1, D_2 が以下を満たすとき, 同値であると呼ぶ.

$$\exists \alpha \in Aut(G), \exists x \in G \text{ s.t. } \alpha(D_1) = D_2 + x.$$

skew Hadamard difference set に関する以下の二つの予想が知られている.

予想 1.1. *(i) G が可換であるとき, G は基本可換群である.*

[1] 〒 860-8555, 熊本県熊本市黒髪 2-40-1, 熊本大学教育学部数学科, Email: momihara@educ.kumamoto-u.ac.jp
この研究は, 科学研究費補助金 (若手 (B) 25800093 および基盤 (C) 24540013) の補助を受けています.

(ii) 基本可換群上の *skew Hadamard difference set* はすべて *Paley difference set* と同値である.

一つ目の予想に関しては, 一般的には未解決であるものの, 部分的にではあるが結果がある. 例えば, G は p 群でなければならないとか, $|G| = p^3, p^5$ の場合には予想は正しいといった結果が知られている. 詳細は, [3] を参照してほしい. 二つ目の予想については, つい最近反例が挙がってしまい, 反証された. Ding-Yuan [7] は標数 3 の有限体上で, skew Hadamard difference set の構成法を与え, そのうちのいくつかが Paley difference set と非同値であることを計算機を使って示した. この論文の後, 私が知る限り 10 本以上の skew Hadamard difference set の新たな構成法に関する論文が提出された [1, 2, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17]. 特に, Muzychuk [15] は, $\mathbb{F}_{q^3}$ 上で Paley difference set と非同値なものを無限個与えたという点で, 非常に大きな結果であると思われる. 実は, この論文以外に skew Hadamard difference set の非同値性を理論的に取り扱っている論文はなく, 全て計算機によって非同値性のチェックが行われている. また, Muzychuk の結果も彼の与えた difference set の構成法に非常に依存しており, そういった意味では非同値性に関する一般論は乏しいといってよいだろう.

一般の difference set D の非同値性の問題は比較的進んでいると思われる. 既存の同値性の不変量としては,

- D から得られる対称デザイン $Dev(D)$ の (全) 自己同型群やその位数
- 三重交差数の集合 $\{|D \cap (D+x) \cap (D+y)| : x, y \in G\}$
- $Dev(D)$ の生起行列の p-rank
- $Dev(D)$ の生起行列のスミス標準形

が挙げられる. 上記二つの不変量の計算は一般には困難であって, それらが求まったような結果は非常に少ない. (Paley difference set から得られるデザインの全自己同型群は決定している.) 下の二つに関しては, 例えば, Singer パラメータの difference set の非同値性の証明に利用され, 非常に多くのことが知られている. 詳しいことは, 論文 [5] 等を参照していただきたい. skew Hadamard difference set の非同値性の問題の困難な点は, D が skew Hadamard のとき, これらの計算可能な不変量 (下の二つの不変量) が構造に依存せずにパラメータのみによって決定してしまい, 不変量として役に立たないという点である. よって, 計算が困難な不変量か, 計算は可能だが役に立たない不変量かの二種類となってしまい, 手詰まりであったと考えられる. 本論文では, その中間をとるような新しい不変量を定義して, 議論を行う.

また, この論文で取り扱う skew Hadamard difference set は以下のような性質を満たすとする: p を素数とし, f を正整数, $q = p^f$, N を $q-1$ を割る正整数とする. γ を $\mathbb{F}_q$ の原始根とし, $C_i^{(N,q)} = \gamma^i\langle\gamma^N\rangle$, $0 \le i \le N-1$ とおく. $D = \bigcup_{i\in I} C_i^{(N,q)}$ を $\mathbb{F}_q$ 上の skew Hadamard difference set とし, 更には, ある正整数 d で $D' = \bigcup_{i\in I} C_i^{(N,q^d)}$ もまた skew Hadamard difference set になるようなものを取り扱う. 例えば, Paley difference set は, $N = 2$, $q = p$, $f = 1$, d は任意の奇数として, この性質を満たしている.

この性質を持つ skew Hadamard difference set は Feng-Xiang [9] で見つかっている.

定理 1.2. ([9, 定理 3.2]) $p_1 \equiv 7 \pmod 8$ を素数, $N = 2p_1^m$, $p \equiv 3 \pmod 4$ とし, $f := \mathrm{ord}_N(p) = \phi(N)/2$ と仮定する. s を任意の奇数とし, I を

$$\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}$$

を満たす $\mathbb{Z}/N\mathbb{Z}$ の任意の部分集合とする. ここで, $D = \bigcup_{i\in I} C_i^{(N,q)} \subseteq \mathbb{F}_q = \mathbb{F}_{p^{fs}}$ とすると, D は $\mathbb{F}_q$ 上 *skew Hadamard difference set* となる.

この結果の一般化については, 論文 [14] を参照していただきたい. 今後, この difference set を Feng-Xiang difference set とよぶことにする. 更には, $\omega = \gamma^{(q^t-1)/(q-1)}$ とおいて, $D = \bigcup_{i\in I} C_i^{(N,q)} = \bigcup_{i\in I} \omega^i\langle\omega^N\rangle$ が Feng-Xiang difference set ならば, $D' = \bigcup_{i\in I} C_i^{(N,q^t)} = \bigcup_{i\in I} \gamma^i\langle\gamma^N\rangle$ もそうである. D' を D の $\mathbb{F}_{q^t}$ へのリフトという. また, 集合 $\bigcup_{i\in I} \omega^{ti}\langle\omega^N\rangle$ を $D^{(t)}$ で表記する. $\gcd(t, N) = 1$ の場合には, $D^{(t)}$ も Feng-Xiang difference set である.

このようなリフトもまた difference set となるような性質をもつ構成法は, [9] および [14] 以外知られていないが, Paley difference set も持つ性質で非常に多くの skew difference set を構成できる. この論文では, この Feng-Xiang difference set と Paley difference set との非同値性について議論する. この論文での議論はリフトの性質をもつどんな difference set の非同値性の問題に対しても有効であることに注意したい.

2 指標に関する準備

p を素数, f を正整数 , $q = p^f$ とおく. ψ を $\mathbb{F}_q$ の標準的な加法的指標, χ_N で $\mathbb{F}_q$ の位数 N の乗法的指標を表記する.

以下の結果はよく知られている.

定理 2.1. ([11, 定理 5.39, 5.41]) χ を $\mathbb{F}_q$ の位数 N の自明でない乗法的指標, $f \in \mathbb{F}_q[x]$ をモニック多項式で N べきでないものとする. d を $f(x) = 0$ の $\mathbb{F}_q$ の分解体での根の数とし, $d \geq 2$ とする. このとき, $w_1, \ldots, w_{d-1} \in \mathbb{C}$ が存在し, 任意の t に対し,

$$\sum_{x\in\mathbb{F}_{q^t}} \chi'(f(x)) = -w_1^t - \cdots - w_{d-1}^t \tag{2.1}$$

となる. ここで, χ' は χ の $\mathbb{F}_{q^t}$ へのリフトとする. 特に,

$$\left|\sum_{x\in\mathbb{F}_{q^t}} \chi'(f(x))\right| \leq (d-1)\sqrt{q^t} \tag{2.2}$$

が成立する.

今, $d = 3$ とする. Warning の公式 [11, 定理 1.76] より, $w_1^t + w_2^t$ は以下のように書ける.

$$w_1^t + w_2^t = \sum_{j=0}^{\lfloor t/2\rfloor} (-1)^j \frac{t}{t-j}\binom{t-j}{j}(w_1+w_2)^{t-2j}(w_1w_2)^j. \tag{2.3}$$

ここで, $(w_1+w_2)^{t-2j}(w_1w_2)^j$ の各係数は整数である. また, [11] の定理 5.39 の証明部分にもあるように, $w_1w_2, w_1+w_2 \in \mathbb{Z}[\zeta_N]$ を満たしている. よって, t が素数の場合には, $\mathbb{Z}[\zeta_N]$ で

$$w_1^t + w_2^t \equiv (w_1+w_2)^t \pmod{t}$$

が成立する.

では標数 p を法としたときはどうだろうか? 以下の結果を証明なしで与えることにする. この結果は, 次の章で用いる.

命題 2.2. χ を $\mathbb{F}_q$ の位数 $N > 1$ の乗法的指標, $a \in \mathbb{F}_p^* \setminus \{1\}$ と $i_1, i_2, i_3 \not\equiv 0 \pmod{N}$ に対し, $f(x) = x^{i_1}(x+1)^{i_2}(x+a)^{i_3} \in \mathbb{F}_q[x]$ とおく. ここで, $\chi^{i_2i_3}$ が非自明のとき, p が $J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3})$ を割ると仮定する. このとき, 任意の奇数 t に対し,

$$\sum_{x \in \mathbb{F}_{q^t}} \chi'(f(x)) \equiv \left(\sum_{x \in \mathbb{F}_q} \chi(f(x)) \right)^t \pmod{p}$$

が成立する. ここで, χ' は, χ の $\mathbb{F}_{q^t}$ へのリフト, $J(\chi^i, \chi^j)$ はヤコビ和 $\sum_{x \in \mathbb{F}_q^* \setminus \{1\}} \chi^i(x)\chi^j(1-x)$ を表す.

注意 2.3. q および N を定理 *1.2* の条件を満たすものとする. よく知られているように, ヤコビ和はガウス和を用いて $J(\chi^i, \chi^j) = G(\chi^i)G(\chi^j)/G(\chi^i\chi^j)$ と書ける *[4]*. よって,

$$J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}) = \frac{G(\chi^{i_2})G(\chi^{i_3})}{G(\chi^{i_2i_3})} \cdot \frac{G(\chi^{i_1})G(\chi^{i_2i_3})}{G(\chi^{i_1i_2i_3})} = \frac{G(\chi^{i_1})G(\chi^{i_2})G(\chi^{i_3})}{G(\chi^{i_1i_2i_3})}$$

を得る. 論文 *[18]* において, この場合 *($s=1$ の場合)* のガウス和の値は完全に決定していて, 任意の $0 \le t \le m-1$ に対し,

$$\begin{aligned} G(\chi^{p_1^t}) &= (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{-p}, \\ G(\chi^{2p_1^t}) &= p^{\frac{f-p_1^t h}{2}} \left(\frac{b + c\sqrt{-p_1}}{2} \right)^{p_1^t}, \\ G(\chi^{p_1^m}) &= (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{-p} \end{aligned}$$

となる. ここで, h は $\mathbb{Q}(\sqrt{-p_1})$ の類数, b と c は $4p^h = b^2 + p_1c^2$ と $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$ で決まる整数とする. 今, i_1, i_2, i_3 が奇数で $\chi^{i_2i_3}$ が非自明とする. このとき, $\chi^{i_1i_2i_3}$ は非自明であることに注意して,

$$J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}) = \left((-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{-p} \right)^{2s} \equiv 0 \pmod{p},$$

となり, 命題 *2.2* の条件を満たす.

3 素数を法とする三重交差数

この章では, まず, difference set の同値性の新たな不変量を導入する. $D \subseteq \mathbb{F}_q$ を skew Hadamard difference set とし, ω を $\mathbb{F}_q$ の原始根とする. $a \in \mathbb{F}_p^* \setminus \{1\}$ に対し, 以下の特殊な三重交差数を

$$T_{\omega^\ell, a}(D) := |D \cap (D - \omega^\ell) \cap (D - a\omega^\ell)|$$

とおく. $\{T_{\omega^\ell,a}(D)\,|\,0\le\ell\le q-2\}$ は difference set の同値性の不変量となる. 事実, D' と D が同値である (つまり $\sigma\in\mathrm{Aut}(\mathbb{F}_q,+)$ と $x\in\mathbb{F}_q$ が存在して, $\sigma(D)=D'+x$ が成立) とすると,

$$\begin{aligned}\{T_{\omega^\ell,a}(D)\,|\,0\le\ell\le q-2\}&=\{|\sigma(D\cap(D-\omega^\ell)\cap(D-a\omega^\ell))|:0\le\ell\le q-2\}\\&=\{|\sigma(D)\cap(\sigma(D)-\sigma(\omega^\ell))\cap(\sigma(D)-a\sigma(\omega^\ell))|:0\le\ell\le q-2\}\\&=\{|D'\cap(D'-\omega^\ell)\cap(D'-a\omega^\ell)|:0\le\ell\le q-2\}\end{aligned}$$

となって,

$$\{T_{\omega^\ell,a}(D)\,|\,0\le\ell\le q-2\}=\{T_{\omega^\ell,a}(D')\,|\,0\le\ell\le q-2\}$$

が言える.

注意 3.1. *D を Paley difference set とすると, 任意の $0\le\ell\le(q-3)/2$ に対し, $T_{1,a}(D)=T_{\omega^{2\ell},a}(D)$ および $T_{\omega,a}(D)=T_{\omega^{2\ell+1},a}(D)$ が成立するので, $|\{T_{\omega^\ell,a}(D)\,|\,0\le\ell\le q-2\}|\le 2$ は明らか. よって, skew Hadamard difference set D' が $|\{T_{\omega^\ell,a}(D')\,|\,0\le\ell\le q-2\}|\ge 3$ を満たせば, D' は D と非同値である. さてここで, 新たな同値性の不変量として, $\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le q-2\}$ を考える. ここで t は素数とする. $\{T_{\omega^\ell,a}(D)\,|\,0\le\ell\le q-2\}$ が不変量であったので, $\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le q-2\}$ も明らかに不変量である. また, Paley difference set D に対しては,*

$$|\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le q-2\}|=|\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le 1\}|\le 2,$$

Feng-Xiang skew Hadamard difference set D に対しては

$$|\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le q-2\}|=|\{T_{\omega^\ell,a}(D)\,(\mathrm{mod}\ t)\,|\,0\le\ell\le N-1\}|\le N$$

に注意されたい.

D を Feng-Xiang skew Hadamard difference set とする. χ_N を $\chi_N(\omega)=\zeta_N$ なる $\mathbb{F}_q$ の位数 N の乗法的指標とし, η_p を $\mathbb{F}_p$ の位数 2 の乗法的指標とする. $\chi_N|_{\mathbb{F}_p}=\eta_p$ に注意する. 集合 $D=\bigcup_{i\in I}C_i^{(N,q)}$ の $\mathbb{F}_q^*$ における特性関数は

$$f(x)=\frac{1}{N}\sum_{h\in I}\sum_{i=0}^{N-1}\zeta_N^{-ih}\chi_N^i(x)$$

で与えられるので,

$$\begin{aligned}&N^3\cdot T_{\omega^\ell,a}(D)\\&=\sum_{x\in\mathbb{F}_q\setminus\{0,-1,-a\}}\sum_{h_1,h_2,h_3\in I}\Big(\sum_{i_1=0}^{N-1}\zeta_N^{-i_1h_1}\chi_N^{i_1}(x)\Big)\Big(\sum_{i_2=0}^{N-1}\zeta_N^{-i_2h_2}\chi_N^{i_2}(x+\omega^\ell)\Big)\Big(\sum_{i_3=0}^{N-1}\zeta_N^{-i_3h_3}\chi_N^{i_3}(x+a\omega^\ell)\Big)\end{aligned}$$

を得る. 展開し整理すると,

$$\begin{aligned}N^3\cdot T_{\omega^\ell,a}(D)=&\sum_{i_1,i_2,i_3\in A}S_{i_1,i_2,i_3}(\omega^\ell,I)+(q-3)M^3+3MN^2\frac{q-3}{4}-3M^3(q-1)\\&-M(\eta_p(a)+\eta_p(-a+1)+\eta_p(a^2-a))p_1^{2m}\end{aligned}\tag{3.1}$$

が得られる. ここで, $M = N/2$, $A = \{2j+1 \,|\, 0 \le j \le (q-3)/2\}$,

$$S_{i_1,i_2,i_3}(\omega^\ell, I) = \sum_{h_1,h_2,h_3 \in I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x)\chi_N^{i_2}(x+1)\chi_N^{i_3}(x+a)$$

とおく. (計算の詳細は, [14] を参考にしていただきたい.) ここで, 値

$$(q-3)M^3 + 3MN^2\frac{q-3}{4} - 3M^3(q-1) - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2-a))p_1^{2m}$$

は ℓ に依存しないので, N と互いに疎な奇素数 t に対し,

$$\begin{aligned} |\{T_{\omega^\ell,a}(D) \pmod t \,|\, 0 \le \ell \le q-2\}| &= |\{N^3 \cdot T_{\omega^\ell,a}(D) \pmod t \,|\, 0 \le \ell \le q-2\}| \\ &= |\{\sum_{i_1,i_2,i_3 \in A} S_{i_1,i_2,i_3}(\omega^\ell, I) \pmod t \,|\, 0 \le \ell \le q-2\}| \end{aligned}$$

となる.

3.1 拡大次数 t を法とする三重交差数

以下の結果が, 本論文の主定理の一つである.

定理 3.2. *t を $\gcd(t, p_1) = 1$ なる奇素数, $D = \bigcup_{i \in I} C_i^{(N,q)}$ を Feng-Xiang skew Hadamard difference set, D' を D の $\mathbb{F}_{q^t}$ へのリフトとする. このとき,*

$$|\{T_{\omega^\ell,a}(D^{(t^{-1})}) \pmod t \,|\, 0 \le \ell \le N-1\}| = u$$

ならば

$$|\{T_{\gamma^\ell,a}(D') \pmod t \,|\, 0 \le \ell \le N-1\}| = u$$

が成り立つ. ここで, ω と γ は $\mathbb{F}_q$ と $\mathbb{F}_{q^t}$ の原始根である.

証明: 一般性を失うことなく, $\omega = \gamma^{(q^t-1)/(q-1)}$ とおける. χ_N を $\chi_N(\omega) = \zeta_N$ なる $\mathbb{F}_q$ の位数 N の乗法的指標とし, χ'_N を χ_N の $\mathbb{F}_{q^t}$ へのリフトとする.

$$S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) = \sum_{h_1,h_2,h_3 \in I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \sum_{x \in \mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a)$$

と定めると, 式 (3.1) より,

$$\begin{aligned} N^3 \cdot T_{\gamma^\ell,a}(D') = \sum_{i_1,i_2,i_3 \in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) + (q^t-3)M^3 + 3MN^2\frac{q^t-3}{4} - 3M^3(q^t-1) \\ - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2-a))p_1^{2m} \end{aligned}$$

を得る. また, 定理 2.1 の式 (2.1) より, $w_1, w_2 \in \mathbb{C}$ が存在し,

$$\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x)\chi_N^{i_2}(x+1)\chi_N^{i_3}(x+a) = -w_1 - w_2$$

かつ

$$\sum_{x\in\mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a) = -w_1^t - w_2^t$$

と書ける. ここで, t は $\gcd(t,N)=1$ を満たすので,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a) &= -w_1^t - w_2^t \\ &\equiv (-w_1-w_2)^t \pmod t \\ &\equiv \Bigg(\sum_{x\in\mathbb{F}_q} \chi_N^{i_1}(x)\chi_N^{i_2}(x+1)\chi_N^{i_3}(x+a)\Bigg)^t \pmod t \\ &\equiv \sum_{x\in\mathbb{F}_q} \chi_N^{ti_1}(x)\chi_N^{ti_2}(x+1)\chi_N^{ti_3}(x+a) \pmod t\end{aligned}$$

を得る. よって,

$$\begin{aligned}S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) &\equiv \sum_{h_1,h_2,h_3\in I} \zeta_N^{-ti_1(t^{-1}h_1)-ti_2(t^{-1}h_2)-ti_3(t^{-1}h_3)+(\ell\cdot t^{-1})(ti_1+ti_2+ti_3)} \\ &\qquad \cdot \sum_{x\in\mathbb{F}_q} \chi_N^{ti_1}(x)\chi_N^{ti_2}(x+1)\chi_N^{ti_3}(x+a) \pmod t \\ &= S_{ti_1,ti_2,ti_3}(\omega^{t^{-1}\ell}, t^{-1}I)\end{aligned}$$

となり,

$$\begin{aligned}&\Bigg\{ \sum_{i_1,i_2,i_3\in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) \,|\, 0\le \ell \le N-1 \Bigg\} \\ \equiv &\Bigg\{ \sum_{i_1,i_2,i_3\in A} S_{ti_1,ti_2,ti_3}(\omega^{t^{-1}\ell}, t^{-1}I) \,|\, 0\le \ell \le N-1 \Bigg\} \pmod t \\ \equiv &\Bigg\{ \sum_{i_1,i_2,i_3\in A} S_{i_1,i_2,i_3}(\omega^{\ell}, t^{-1}I) \,|\, 0\le \ell \le N-1 \Bigg\} \pmod t \qquad (3.2)\end{aligned}$$

が得られる. 仮定より,

$$\Bigg| \Bigg\{ \sum_{i_1,i_2,i_3\in A} S_{i_1,i_2,i_3}(\omega^{\ell}, t^{-1}I) \pmod t \,|\, 0\le \ell \le N-1 \Bigg\} \Bigg| = u$$

であったので,

$$\Bigg| \Bigg\{ \sum_{i_1,i_2,i_3\in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) \pmod t \,|\, 0\le \ell \le N-1 \Bigg\} \Bigg| = u$$

となり, $|\{T_{\gamma^\ell,a}(D') \pmod t \,|\, 0\le \ell\le N-1\}| = u$ が導かれる. □

注意 3.3. (i) $D=\bigcup_{i\in I} C_i^{(N,q)}$ を定理 3.2 の skew Hadamard difference set とし,

$$\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,|\, 0\le \ell \le N-1\}$$

の濃度を $u(\geq 3)$ とする. それらの元を $a_1 < a_2 < \cdots < a_u$ とし,

$$v = \min\{a_{j+2} - a_j \,|\, 1 \leq j \leq u-2\}$$

と置こう. $t > v$ をみたすとき, D' を D の $\mathbb{F}_{q^t}$ へのリフトとする. このとき,

$$\left|\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\}\right| \geq 3$$

が満たされるので, 定理 3.2 より, $|\{T_{\gamma^\ell,a}(D') \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\}| \geq 3$ が導かれる. (より大雑把に, $t > a_u - a_1$ としてもよい.)

(ii) 二つの Feng-Xiang skew Hadamard difference sets $D_1, D_2 \subseteq \mathbb{F}_q$ に対し,

$$\{T_{\omega^\ell,a}(D_1^{(t^{-1})}) \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\} \neq \{T_{\omega^\ell,a}(D_2^{(t^{-1})}) \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\}$$

とすると, 定理 3.2 の証明から D_1, D_2 の $\mathbb{F}_{q^t}$ へのリフト D_1', D_2' も

$$\{T_{\gamma^\ell,a}(D_1') \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\} \neq \{T_{\gamma^\ell,a}(D_2') \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\}$$

を満たし, D_1' と D_2' も非同値となる.

系 3.4. *$D = \bigcup_{i\in I} C_i^{(N,q)}$ を Feng-Xiang skew Hadamard difference set とし, $t > 4N^3\sqrt{q}$ なる任意の奇素数 t に対し, D' を D の $\mathbb{F}_{q^t}$ へのリフトとする. このとき,*

$$|\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,|\, 0 \leq i \leq N-1\}| = u$$

ならば

$$|\{T_{\gamma^\ell,a}(D') \,(\mathrm{mod}\ t) \,|\, 0 \leq \ell \leq N-1\}| = u$$

が成立する.

証明: $|\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,|\, 0 \leq i \leq N-1\}| = u$ と仮定する. 注意 3.3 (i) より, $a_u - a_1 \leq 4N^3\sqrt{q}$ を示せば十分である. 式 (3.1) より,

$$a_u - a_1 \leq \frac{2}{N^3} \max\left\{\left|\sum_{i_1,i_2,i_3\in A} S_{i_1,i_2,i_3}(\omega^\ell, t^{-1}I)\right| : 0 \leq \ell \leq N-1\right\}$$

となる. よって, $|\sum_{i_1,i_2,i_3\in A} S_{i_1,i_2,i_3}(\omega^\ell, t^{-1}I)|$ の値の限界式を得ることを考える. 定理 2.1 の式 (2.2) より,

$$\begin{aligned}
&\left|\sum_{i_1,i_2,i_3\in A} S_{i_1,i_2,i_3}(\omega^\ell, t^{-1}I)\right| \\
&\leq \sum_{i_1,i_2,i_3\in A} \sum_{h_1,h_2,h_3\in t^{-1}I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \left|\sum_{x\in\mathbb{F}_q} \chi_N^{i_1}(x)\chi_N^{i_2}(x+1)\chi_N^{i_3}(x+a)\right| \\
&\leq |A|^3|I|^3\sqrt{q} = 2N^6\sqrt{q}.
\end{aligned}$$

よって,

$$a_u - a_1 \le \frac{2}{N^3} \max\left\{ \left| \sum_{i_1,i_2,i_3 \in A} S_{i_1,i_2,i_3}(\omega^\ell, t^{-1}I) \right| : 0 \le \ell \le N-1 \right\} \le 4N^3\sqrt{q}$$

が得られる. □

系 3.4 は十分大きな奇素数 t に対し, Feng-Xiang skew Hadamard difference set $D \subseteq \mathbb{F}_q$ が, $|\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,|\, 0 \le \ell \le N-1\}| \ge 3$ を満たせば, D の $\mathbb{F}_{q^t}$ へのリフト D' もまた Paley difference set と非同値であることを意味している.

例 3.5. $p = 11$, $N = 2p_1 = 14$, $f = 3$, $I = \langle p \rangle \cup -2\langle p \rangle \cup \{0\} \pmod N$ とする. このとき, $I \pmod{p_1} = \mathbb{Z}/p_1\mathbb{Z}$ と定理 *1.2* の条件を満たすので, $D = \bigcup_{i\in I} C_i^{(N,p^f)} = \bigcup_{i\in I} \omega^i \langle \omega^N \rangle$ は *Feng-Xiang skew Hadamard difference set* である. ここで, ω は $\mathbb{F}_{p^f}$ の原始根とする. 今, $a = 3$ として, $T_{\omega^\ell,a}(D^{(t^{-1})})$, $0 \le \ell \le N-1$ を考える. 計算機によって, $1 \le t < N$ かつ $\gcd(t, p_1) = 1$ なる任意の奇素数 t に対し,

$$\{T_{\omega^\ell,a}(D^{(t^{-1})}) \,|\, 0 \le \ell \le N-1\} = \{147, 158, 164, 167, 173, 184\}$$

がチェックできる. *(これは, D が Paley difference set と非同値であることを意味する.)*

一方で, $\gcd(t, p_1) = 1$ なる任意の奇素数 t に対し,

$$\left| \{T_{\omega^\ell,a}(D^{(t^{-1})}) \pmod t \,|\, 0 \le \ell \le N-1\} \right| \ge 3$$

が成立するので, 定理 *3.2* より, D の $\mathbb{F}_{p^{ft}}$ へのリフト D' は

$$\left| \{T_{\gamma^\ell,a}(D') \pmod t \,|\, 0 \le \ell \le N-1\} \right| \ge 3$$

を満たす. ここで, γ は $\mathbb{F}_{p^{ft}}$ の原始根とする. よって, D' も *Paley difference set* と非同値である. さらに, 定理 *3.2* を再帰的に繰り返すと, 任意の $h \ge 1$ に対し, D の $\mathbb{F}_{p^{ft^h}}$ へのリフトもまた *Paley difference set* と非同値になる. このようにして, 被覆される 50 以下の拡大次数 t^h は以下のようになる*:* $t^h = 3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49$.

3.2 標数 p を法とする三重交差数

定理 3.2 において, 素数 t は奇素数に限られていたために, 必然的に拡大次数も素数 (または素数べき) に限られてしまった. 以下の結果は t として任意の奇数を取ることを許すことができる.

定理 3.6. t を任意の奇数とし, t の p 進展開 $t = \sum_{h=0}^{r} x_h p^h$ *(*$0 \le x_h \le p-1$*)* を考え, $e(t) = \sum_{h=0}^{r} x_h$ とおく. このとき, $1 \le t' \le p-2$ なる t' で $t' = e(e(\cdots e(t) \cdots))$ となる奇数が一つきまる. $D = \bigcup_{i\in I} C_i^{(N,q)}$ を *Feng-Xiang skew Hadamard difference set* とし, D' と D'' を $\mathbb{F}_{q^t}$ と $\mathbb{F}_{q^{t'}}$ へのリフトとする. このとき,

$$|\{T_{\beta^\ell,a}(D'') \pmod p \,|\, 0 \le \ell \le N-1\}| = u$$

であれば,

$$|\{T_{\gamma^\ell,a}(D') \pmod p \,|\, 0 \le \ell \le N-1\}| = u$$

が成立する. ここで, β と γ はそれぞれ $\mathbb{F}_{q^{t'}}$ と $\mathbb{F}_{q^t}$ の原始根とする.

証明: ω を $\mathbb{F}_q$ の原始根とする. 一般性を失うことなく, $\omega = \beta^{(q^{t'}-1)/(q-1)} = \gamma^{(q^t-1)/(q-1)}$ と置ける. χ_N を $\mathbb{F}_q$ の位数 N の乗法的指標で $\chi_N(\omega) = \zeta_N$ なるものとし, χ'_N と χ''_N を χ_N の $\mathbb{F}_{q^t}$ と $\mathbb{F}_{q^{t'}}$ へのリフトとする. ここで,

$$S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) = \sum_{h_1,h_2,h_3 \in I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \sum_{x\in\mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a)$$

と定めておくと, 式 (3.1) より,

$$\begin{aligned} N^3 \cdot T_{\gamma^\ell,a}(D') = \sum_{i_1,i_2,i_3\in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) + (q^t-3)M^3 + 3MN^2\frac{q^t-3}{4} - 3M^3(q^t-1) \\ - M(\eta_p(a)+\eta_p(-a+1)+\eta_p(a^2-a))p_1^{2m} \end{aligned}$$

を得る. また, 定理 2.1 の式 (2.1) より, $w_1, w_2 \in \mathbb{C}$ が存在して,

$$\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x)\chi^{i_2}_N(x+1)\chi^{i_3}_N(x+a) = -w_1 - w_2,$$

$$\sum_{x\in\mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a) = -w_1^t - w_2^t,$$

$$\sum_{x\in\mathbb{F}_{q^{t'}}} \chi''^{i_1}_N(x)\chi''^{i_2}_N(x+1)\chi''^{i_3}_N(x+a) = -w_1^{t'} - w_2^{t'}$$

の三つが成立する. また, 命題 2.2 より,

$$\begin{aligned} \sum_{x\in\mathbb{F}_{q^t}} \chi'^{i_1}_N(x)\chi'^{i_2}_N(x+1)\chi'^{i_3}_N(x+a) &\equiv \Big(\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x)\chi^{i_2}_N(x+1)\chi^{i_3}_N(x+a)\Big)^t \pmod p \\ &= \prod_{h=0}^{r}\Big(\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x)\chi^{i_2}_N(x+1)\chi^{i_3}_N(x+a)\Big)^{x_hp^h} \\ &\equiv \prod_{h=0}^{r}\Big(\sum_{x\in\mathbb{F}_q} \chi^{p^hi_1}_N(x)\chi^{p^hi_2}_N(x+1)\chi^{p^hi_3}_N(x+a)\Big)^{x_h} \pmod p \\ &= \prod_{h=0}^{r}\Big(\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x^{p^h})\chi^{i_2}_N(x^{p^h}+1)\chi^{i_3}_N(x^{p^h}+a)\Big)^{x_h} \\ &= \prod_{h=0}^{r}\Big(\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x)\chi^{i_2}_N(x+1)\chi^{i_3}_N(x+a)\Big)^{x_h} \\ &= \Big(\sum_{x\in\mathbb{F}_q} \chi^{i_1}_N(x)\chi^{i_2}_N(x+1)\chi^{i_3}_N(x+a)\Big)^{e(t)}. \end{aligned}$$

これを繰り返せば,

$$\sum_{x\in\mathbb{F}_{q^t}} {\chi'}_N^{i_1}(x){\chi'}_N^{i_2}(x+1){\chi'}_N^{i_3}(x+a) \equiv \left(\sum_{x\in\mathbb{F}_q} \chi_N^{i_1}(x)\chi_N^{i_2}(x+1)\chi_N^{i_3}(x+a)\right)^{t'} \pmod p$$
$$\equiv \sum_{x\in\mathbb{F}_{q^{t'}}} {\chi''}_N^{i_1}(x){\chi''}_N^{i_2}(x+1){\chi''}_N^{i_3}(x+a) \pmod p$$

となり

$$\begin{aligned}
&S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I)\\
&= \sum_{h_1,h_2,h_3\in I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \sum_{x\in\mathbb{F}_{q^t}} {\chi'}_N^{i_1}(x){\chi'}_N^{i_2}(x+1){\chi'}_N^{i_3}(x+a)\\
&\equiv \sum_{h_1,h_2,h_3\in I} \zeta_N^{-i_1h_1-i_2h_2-i_3h_3+\ell(i_1+i_2+i_3)} \sum_{x\in\mathbb{F}_{q^{t'}}} {\chi''}_N^{i_1}(x){\chi''}_N^{i_2}(x+1){\chi''}_N^{i_3}(x+a) \pmod p\\
&= S^{(t')}_{i_1,i_2,i_3}(\beta^\ell, I)
\end{aligned}$$

が得られる. したがって,

$$\left\{\sum_{i_1,i_2,i_3\in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) \,|\, 0\le \ell\le N-1\right\} \equiv \left\{\sum_{i_1,i_2,i_3\in A} S^{(t')}_{i_1,i_2,i_3}(\beta^\ell, I) \,|\, 0\le \ell\le N-1\right\} \pmod p \tag{3.3}$$

を得る. ゆえに, 仮定から,

$$\left|\left\{\sum_{i_1,i_2,i_3\in A} S^{(t')}_{i_1,i_2,i_3}(\beta^\ell, I) \pmod p \,|\, 0\le \ell\le N-1\right\}\right| = u$$

であり, 式 (3.3) より

$$\left|\left\{\sum_{i_1,i_2,i_3\in A} S^{(t)}_{i_1,i_2,i_3}(\gamma^\ell, I) \pmod p \,|\, 0\le \ell\le N-1\right\}\right| = u$$

を得る. つまりは, $|\{T_{\gamma^\ell,a}(D') \pmod p \,|\, 0\le\ell\le N-1\}| = u$ を得る. □

定理 3.6 は, $1\le t'\le p-2$ なる任意の奇数 t に対し, Feng-Xiang skew Hadamard difference set $D\subseteq\mathbb{F}_q$ の $\mathbb{F}_{q^{t'}}$ へのリフト D'' が

$$|\{T_{\beta^\ell,a}(D'') \pmod p \,|\, 0\le\ell\le N-1\}| \ge 3$$

を満たすことをチェックさえしておけば, 任意の奇数 t に対し, D の $\mathbb{F}_{q^t}$ へのリフトが Paley difference set と非同値になることを意味している.

例 3.7. *p, N, f, a, I は例 3.5 の表記を用いることとする. このとき, $D=\bigcup_{i\in I} C_i^{(N,q)}$ は*

$$\{T_{\omega^\ell,a}(D) \,|\, 0\le\ell\le N-1\} = \{147, 158, 164, 167, 173, 184\}$$

を満たし,

$$\left|\{T_{\omega^\ell,a}(D) \pmod p \,|\, 0 \le \ell \le N-1\}\right| \ge 3$$

が成り立つ. 定理 *3.6* より, $e(e(\cdots e(t)\cdots)) = 1$ なる任意の奇数 t に対し, D の $\mathbb{F}_{p^{ft}}$ へのリフト D' は

$$\left|\{T_{\gamma^\ell,a}(D') \pmod p \,|\, 0 \le \ell \le N-1\}\right| \ge 3$$

を満たすので, D' は *Paley difference set* と非同値である. このとき定理 *3.6* によって被覆される 50 以下の拡大次数 t は $t = 11, 21, 31, 41$ となり, 特に $t = 21$ は定理 *3.2* では被覆できないことに注意しておく.

4 最後に

この論文では, Feng-Xiang skew Hadamard difference set のリフトが Paley difference set と非同値であるための条件についての定理を二つ与えた. 例として, Feng-Xiang difference set $D = \bigcup_{i\in\langle 11\rangle\cup -2\langle 11\rangle\cup\{0\}} C_i^{(14,11^3)}$ に対し, 無限個の t が存在して, D の $\mathbb{F}_{11^{3t}}$ へのリフトが Paley difference set と非同値となることをみた. $p_1 = 7$(つまり $f = 3$) と固定した際の p が小さな場合のそのほかの例については表 1 に与えることにする. (この表では, ω は $\mathbb{F}_{p^f}$ の原始根, $n_t := |\{T_{\omega^\ell,3}(D^{(t^{-1})}) \pmod t \,|\, 0 \le \ell \le N-1\}|$, t は $p_1 = 7$ と互いに疎な奇素数とする.) 各 $p \in \{11, 23, 67, 79, 107\}$ に対し, 表の I に対する Feng-Xiang skew Hadamard difference set $D = \bigcup_{i\in I} C_i^{(N,p^f)}$ およびそれらの $\mathbb{F}_{p^{ft}}$ へのリフトは Paley difference set と非同値である. ここで, t は十分大きくとっておく. さらに, 注意 3.3 (ii) より, 表の Feng-Xiang skew Hadamard difference set のリフトも互いに非同値であることがわかる.

参考文献

[1] Y. Q. Chen, T. Feng, Paley type group schemes from cyclotomic classes and Arasu-Dillon-Player difference sets, arXiv:1210.2801.

[2] Y. Q. Chen, J. Polhill, Paley type group schemes and planar Dembowski-Ostrom polynomials, *Discr. Math.,* **311** (2011), 1349–1364.

[3] Y. Q. Chen, Q. Xiang, S. K. Sehgal, An exponent bound on skew Hadamard abelian difference sets, *Des. Codes Cryptogr.,* **4** (1994), 313–317.

[4] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.

[5] P. Ó. Catháin, Inequivalence of difference sets: On a remark of Baumert, *Elect. J. Combin.*, **20** (2013), #P38.

[6] C. Ding, A. Pott, Q. Wang, Skew Hadamard difference sets from Dickson polynomials of order 7, arXiv:1305.1831.

表 1: Feng-Xiang skew Hadamard difference set と それらの三重交差数の例

(p,f,N)	添え字集合 I	$\{T_{\omega^\ell,3}(D^{(t^{-1})}) \mid 0 \le \ell \le N-1\}$	奇素数 t に対する n_t
$(11,3,14)$	$\{0,1,2,3,4,5,6\}$	$\{159,162,164,167,169,172\}$	$n_5=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,3,4,6,12\}$	$\{157,160,165,166,171,174\}$	$n_3=2$ and $n_t \ge 3$ for any other t
	$\{0,1,6,9,10,11,12\}$	$\{147,158,164,167,173,184\}$	$n_t \ge 3$ for any t
	$\{0,1,2,4,6,10,12\}$	$\{163,164,167,168\}$	$n_t \ge 3$ for any $t \ge 3$
$(11,3,2)$	$\{0\}$ (Paley)	$\{157,174\}$	$n_{17}=1$ and $n_t=2$ for any other t
$(23,3,14)$	$\{0,1,2,3,4,5,6\}$	$\{1497,1498,1503,1515,$ $1525,1537,1542,1543\}$	$n_3=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,3,4,6,12\}$	$\{1498,1503,1508,1514,$ $1526,1532,1537,1542\}$	$n_t \ge 3$ for any t
	$\{0,1,6,9,10,11,12\}$	$\{1481,1509,1514,1526,1531,1559\}$	$n_5=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,4,6,10,12\}$	$\{1508,1514,1526,1532\}$	$n_3=1$ and $n_t \ge 3$ for any t
$(23,3,2)$	$\{0\}$ (Paley)	$\{1520\}$	$n_t=1$ for any t
$(67,3,14)$	$\{0,1,2,3,4,5,6\}$	$\{37457,37519,37525,37587,$ $37602,37664,37670,37732\}$	$n_t \ge 3$ for any t
	$\{0,1,2,3,4,6,12\}$	$\{37453,37523,37587,37591,$ $37598,37602,37666,37736\}$	$n_t \ge 3$ for any t
	$\{0,1,6,9,10,11,12\}$	$\{37526,37587,37594,37595,37602,37663\}$	$n_t \ge 3$ for any t
	$\{0,1,2,4,6,10,12\}$	$\{37543,37559,37630,37646\}$	$n_3,n_{29}=2$ and $n_t \ge 3$ for any other t
$(67,3,2)$	$\{0\}$ (Paley)	$\{37502,37687\}$	$n_t=2$ for any t
$(79,3,14)$	$\{0,1,2,3,4,5,6\}$	$\{61470,61575,61607,61623,$ $61636,61652,61684,61789\}$	$n_t \ge 3$ for any t
	$\{0,1,2,3,4,6,12\}$	$\{61398,61535,61549,61552,$ $61707,61710,61724,61861\}$	$n_t \ge 3$ for any t
	$\{0,1,6,9,10,11,12\}$	$\{61513,61533,61546,61713,61726,61746\}$	$n_3,n_5=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,4,6,10,12\}$	$\{61434,61511,61748,61825\}$	$n_7,n_{11},n_{157}=2$ $n_t \ge 3$ for any other t
$(79,3,2)$	$\{0\}$ (Paley)	$\{61519,61740\}$	$n_t=2$ for any t
$(107,3,14)$	$\{0,1,2,3,4,5,6\}$	$\{152751,152895,152976,153021,$ $153238,153283,153364,153508\}$	$n_3=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,3,4,6,12\}$	$\{152969,153065,153092,$ $153167,153194,153290\}$	$n_3=1$ and $n_t \ge 3$ for any other t
	$\{0,1,6,9,10,11,12\}$	$\{152643,153040,153102,$ $153157,153219,153616\}$	$n_3=2$ and $n_t \ge 3$ for any other t
	$\{0,1,2,4,6,10,12\}$	$\{153028,153103,153156,153231\}$	$n_3,n_5=2$ and $n_t \ge 3$ for any other t
$(107,3,2)$	$\{0\}$ (Paley)	$\{152977,153282\}$	$n_t=2$ for any t

[7] C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory, Ser. A*, **113** (2006), 1526–1535.

[8] C. Ding, Z. Wang, Q. Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in PG$(3,3^{2h+1})$, *J. Combin. Theory, Ser. A*, **114** (2007), 867–887.

[9] T. Feng, Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory, Ser. A*, **119** (2012), 245–256.

[10] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, *Combinatorica*, to apear.

[11] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.

[12] K. Momihara, Cyclotomic strongly regular graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, *Europ. J. Combin.*, **34** (2013), 706–723.

[13] K. Momihara, Skew Hadamard difference sets from cyclotomic strongly regular graphs, *SIAM J. Discr. Math.*, **27** (2013), pp. 1112–1122.

[14] K. Momihara, Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime, *Elect. J. Combin.*, **20** (2013), #P35.

[15] M. E. Muzychuk, On skew Hadamard difference sets, arXiv:1012.2089.

[16] G. B. Weng, L. Hu, Some results on skew Hadamard difference sets, *Des. Codes Cryptogr.,* **50** (2009), 93–105.

[17] G. B. Weng, W. S. Qiu, Z. Wang, Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.,* **44** (2007), 49–62.

[18] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, **53** (2010), 2525–2542.

多重 Euler 数とその L 関数

佐々木 義卓
大阪体育大学体育学部
ysasaki@ouhs.ac.jp

大野泰生
近畿大学理工学部
ohno@math.kindai.ac.jp

概要

1997 年, 金子により Bernoulli 数を拡張した多重 Bernoulli 数が導入された. ここで議論する多重 Euler 数は, 古典的な Euler 数の母関数を多重 Bernoulli 数と同様の方法で拡張するものである. 本稿では多重 Euler 数の導入法, 数値データ, 2 重 Euler 数の符号決定, 多重 Euler 数の組合せ論的解釈, さらに数論的性質について述べる.

1 序

1997 年, 金子 [4] によって Bernoulli 数を拡張した**多重 Bernoulli 数**が導入された. 多重 Bernoulli 数 $\mathbb{B}_n^{(k)}$ はポリログ

$$\mathrm{Li}_k(x) := \sum_{n=1}^{\infty} \frac{x^n}{n^k} \qquad (|x| < 1, k \in \mathbb{Z})$$

を用いて

$$\frac{\mathrm{Li}_k(1-e^{-t})}{1-e^{-t}} = \sum_{n=0}^{\infty} \frac{\mathbb{B}_n^{(k)}}{n!} t^n \tag{1.1}$$

で定義される. $k = 1$ のとき $\mathrm{Li}_1(1-e^{-t}) = t$ より, Bernoulli 数 (ただし, $B_1 = 1/2$) の母関数であることが容易に理解できる.

Bernoulli 数と同様, 多重 Bernoulli 数もゼータ関数と結びつけて議論することが自然かつ肝要である. 荒川・金子 [1] は, 多重 Bernoulli 数をその特殊値にもつゼータ関数 (**荒川・金子のゼータ関数**) を与えた. このゼータ関数は非常に綺麗な構造を持っており, 後述する**多重ゼータ関数**との関係は, 奇跡としか言いようのない調和のとれた変形から導かれる. また, 多重 Bernoulli 数は双対的性質 $\mathbb{B}_n^{(-m)} = \mathbb{B}_m^{(-n)}$ ([4]) や組合せ論的解釈 ([3], [5], [11]) など, 多様な性質を併せ持つ. 例えば, Brewbaker [3] により, 負のインデックスの多重 Bernoulli 数はロンサム行列 (後述) の個数と一致することが示されている.

では, 何故この拡張法がこれだけ良い性質を併せ持つのであろうか. それを理解するには

もっと大きな枠組みで観察・議論することが重要である. これが多重 Euler 数を導入・研究する動機である. Euler 数は Bernoulli 数の親戚であり, 互いに数論的にも重要な意味を持つものである. それらの多重版を見比べることで, この拡張法の本質に迫ろうとする訳である. 次節では, 多重 Euler 数の導入法について解説し, その後の節において多重 Euler 数の符号決定や組合せ論的解釈などの研究結果について簡潔に述べる. 詳しくは, [6], [7], [8] を参照されたい.

2 多重 Euler 数

Euler 数 E_n は

$$\frac{1}{\cosh t} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n$$

で定義される. 左辺が偶関数であることから, n が奇数のとき $E_n = 0$ であることがわかる. また Euler 数は, 導手 4 の Dirichlet 指標の一般 Bernoulli 数でもあり, その L 関数は,

$$L(s) := \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} \frac{1}{e^t + e^{-t}}\, dt \tag{2.1}$$

で与えられる. この L 関数は $\mathbb{C}$ 上に整関数として解析接続され, 非負整数 n に対して, $L(-n) = E_n/2$ を満たす. 多重 Euler 数は, この性質に着目して導入したものである. すなわち, 荒川・金子のゼータ関数が多重 Bernoulli 数をその特殊値に持つことから, 上記 L 関数 (2.1) を荒川・金子のゼータ関数の構成法に倣って拡張し, その特殊値を通して多重 Euler 数を導入するわけである. まず, 多重 Euler 数の定義を述べる.

定義 2.1（多重 Euler 数） 多重 Euler 数 $E_n^{(k)}$ を次で定義する:

$$\frac{\mathrm{Li}_k(1 - e^{-4t})}{4t \cosh t} = \sum_{n=0}^{\infty} \frac{E_n^{(k)}}{n!} t^n. \tag{2.2}$$

多重 Euler 数の具体的な数値については, 表 1, 表 2 を参照されたい.

次の小節で, この拡張の元となった荒川・金子のゼータ関数の構成法について述べる.

2.1 荒川・金子のゼータ関数

荒川・金子のゼータ関数は

$$\xi_k(s) := \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} \frac{\mathrm{Li}_k(1 - e^{-t})}{e^t - 1}\, dt \qquad (k \geq 1)$$

表 1　$E_n^{(k)}$ $(1 \le k \le 8)$

$n\backslash k$	1	2	3	4	5
0	1	1	1	1	1
1	0	-1	$-\frac{3}{2}$	$-\frac{7}{4}$	$-\frac{15}{8}$
2	-1	$-\frac{1}{9}$	$\frac{41}{27}$	$\frac{221}{81}$	$\frac{842}{243}$
3	0	3	$\frac{7}{6}$	$-\frac{85}{36}$	$-\frac{145}{27}$
4	5	$-\frac{51}{25}$	$-\frac{3493}{375}$	$-\frac{31079}{5625}$	$\frac{251513}{84375}$
5	0	-25	$\frac{521}{90}$	$\frac{77071}{2700}$	$\frac{1726751}{81000}$
6	-61	$\frac{33221}{735}$	$\frac{8169601}{77175}$	$-\frac{41535229}{8103375}$	$-\frac{71715452684}{850854375}$
7	0	427	$-\frac{18313}{70}$	$-\frac{19160833}{44100}$	$-\frac{25259027}{514500}$
8	1385	$-\frac{1288391}{945}$	$-\frac{70339397}{33075}$	$\frac{33076559267}{31255875}$	$\frac{16895967725821}{9845600625}$
9	0	-12465	$\frac{11557561}{1050}$	$\frac{748381847}{73500}$	$-\frac{480568115197}{138915000}$
10	-50521	$\frac{252042789}{4235}$	$\frac{986047910537}{14674275}$	$-\frac{3065162516767009}{50846362875}$	$-\frac{8422942412191735762}{176182647361875}$

$n\backslash k$	6	7	8
0	1	1	1
1	$-\frac{31}{16}$	$-\frac{63}{32}$	$-\frac{127}{64}$
2	$\frac{5653}{1458}$	$\frac{35849}{8748}$	$\frac{221143}{52488}$
3	$-\frac{19139}{2592}$	$-\frac{266987}{31104}$	$-\frac{3453965}{373248}$
4	$\frac{13750789}{1265625}$	$\frac{1249362593}{75937500}$	$\frac{90758304241}{4556250000}$
5	$-\frac{308497}{1215000}$	$-\frac{3164224553}{145800000}$	$-\frac{328669347761}{8748000000}$
6	$-\frac{13363728130853}{178679418750}$	$-\frac{358429898641663}{18761338968750}$	$\frac{640308924888841241}{15759524733750000}$
7	$\frac{920793920551}{3889620000}$	$\frac{135001198394803}{544546800000}$	$\frac{72052924489405981}{686128968000000}$
8	$\frac{1285878287869223}{3101364196875}$	$-\frac{1215868617178437277}{1953859444031250}$	$-\frac{194401273048198680 3179}{2461862899479375000}$
9	$-\frac{567231622233841}{87516450000}$	$-\frac{61763666069504519}{27567681750000}$	$\frac{102907638651697550227}{69470558010000000}$
10	$\frac{10712366827341728785543}{1220945746217793750}$	$\frac{19777980839671353553424462 3}{8461154021289310687500}$	$\frac{29912308962457844466511790 6339}{29317898683767461532187500}$

で定義される ([1]). これは Riemann ゼータ関数の積分表示

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} \frac{1}{e^t - 1}\, dt \tag{2.3}$$

に注意すれば, その拡張であることが容易に理解できる. 実際 $k = 1$ のときは $\xi_1(s) = s\zeta(s+1)$ となる. 上述の通り, 多重 Euler 数は荒川・金子のゼータ関数の拡張法に倣って,

表 2　$E_n^{(k)}$ $(-8 \le k \le 0)$

$n\backslash k$	0	-1	-2	-3	-4
0	1	1	1	1	1
1	2	6	14	30	62
2	$\frac{13}{3}$	$\frac{109}{3}$	$\frac{493}{3}$	$\frac{1837}{3}$	$\frac{6253}{3}$
3	10	222	1798	10710	55030
4	$\frac{121}{5}$	$\frac{6841}{5}$	$\frac{95161}{5}$	$\frac{865081}{5}$	$\frac{6396601}{5}$
5	$\frac{182}{3}$	8502	$\frac{594554}{3}$	2670350	$\frac{82690442}{3}$
6	$\frac{1093}{7}$	$\frac{372709}{7}$	$\frac{14331493}{7}$	$\frac{280592677}{7}$	$\frac{3958958053}{7}$
7	410	335886	21078134	591278790	11230160870
8	$\frac{9841}{9}$	$\frac{19200241}{9}$	$\frac{1951326961}{9}$	$\frac{77624198641}{9}$	$\frac{1961872865521}{9}$
9	$\frac{14762}{5}$	$\frac{68177406}{5}$	$\frac{11157142694}{5}$	124916013054	$\frac{20819816118422}{5}$
10	$\frac{88573}{11}$	$\frac{964249309}{11}$	$\frac{252966361693}{11}$	$\frac{19811958812317}{11}$	$\frac{864960182738653}{11}$

$n\backslash k$	-5	-6	-7	-8
0	1	1	1	1
1	126	254	510	1022
2	$\frac{20269}{3}$	$\frac{63853}{3}$	$\frac{197677}{3}$	$\frac{605293}{3}$
3	260022	1166518	5058870	21440950
4	$\frac{41968441}{5}$	$\frac{255205561}{5}$	$\frac{1474388281}{5}$	$\frac{8217391801}{5}$
5	243487342	$\frac{5836302794}{3}$	14509820910	$\frac{309069453002}{3}$
6	$\frac{46088370469}{7}$	$\frac{473519630053}{7}$	$\frac{4461656417317}{7}$	$\frac{39487415403493}{7}$
7	169602610086	2205417795494	25836997580070	280515914328230
8	$\frac{37978754131441}{9}$	$\frac{617481161118961}{9}$	$\frac{8884959409517041}{9}$	$\frac{116896719524014321}{9}$
9	$\frac{511780950202326}{5}$	$\frac{10304271705550934}{5}$	36070508475019230	$\frac{2847626348007626582}{5}$
10	$\frac{26796243596416669}{11}$	$\frac{662962530489535453}{11}$	$\frac{14004154117362681757}{11}$	$\frac{263272861026817782493}{11}$

その特質全てを踏襲するように L 関数 (2.1) を拡張し, その特殊値で定義する. ここで着目する荒川・金子のゼータ関数の諸性質は以下の通りである:

定理 2.2（荒川・金子 [1]）

1. 任意の $k \ge 1$ に対して, $\xi_k(s)$ は, $\mathbb{C}$ 上整関数として解析接続される.

2. 任意の非負整数 n に対して,

$$\xi_k(-n) = \sum_{l=0}^{n} (-1)^l \binom{n}{l} \mathbb{B}_l^{(k)} = (-1)^n C_n^{(k)}.$$

3. $\Re s > 1$ に対して,

$$\begin{aligned}\xi_k(s) =& (-1)^{k-1} \left\{ \sum_{j=1}^{k-1} \zeta(\underbrace{1, \ldots, 1, \overset{j\text{-th}}{\overset{\downarrow}{2}}, 1, \ldots, 1}_{k-1}, s) + s\zeta(\underbrace{1, \ldots, 1}_{k-1}, s+1) \right\} \\ &+ \sum_{j=0}^{k-2} (-1)^j \zeta(k-j)\zeta(\underbrace{1, \ldots, 1}_{j}, s).\end{aligned}$$

ここで, $C_n^{(k)}$ は変種の多重 Bernoulli 数であり,

$$\frac{\mathrm{Li}_k(1-e^{-t})}{e^t - 1} = \sum_{n=0}^{\infty} \frac{C_n^{(k)}}{n!} t^n \tag{2.4}$$

で定義される. これは古典的な Bernoulli 数の定義が 2 通りあることに起因するものであり, 上記の多重 Bernoulli 数は $B_1 = -1/2$ ととるタイプの拡張にあたる. また,

$$\zeta(s_1, \ldots, s_n) := \sum_{0 < m_1 < \cdots < m_n} \frac{1}{m_1^{s_1} \cdots m_n^{s_n}}$$

は多重ゼータ関数であり, $\Re s_j \geq 1$ $(j = 1, \ldots, n-1)$ および $\Re s_n > 1$ に対して絶対収束する.

我々の目的において, 最も重要な性質は, 上定理の 3 番目の性質である. この公式は, 次にあげる被積分関数の性質から導かれるものであり、多重 Euler 数の導入においても重要な役割を担う:

- $1 - e^{-t}$ は $\mathrm{Li}_1(x)$ の逆関数 $(\mathrm{Li}_1(1-e^{-t}) = t)$
- $\dfrac{d}{dt}\mathrm{Li}_k(1-e^{-t}) = \dfrac{\mathrm{Li}_{k-1}(1-e^{-t})}{e^t - 1}$ (右辺は荒川・金子のゼータ関数の被積分関数)

これは Riemann ゼータ関数の積分表示の被積分関数と, ポリログ $\mathrm{Li}_k(x)$ との相性の良さを示唆するものである. すなわち, 荒川・金子のゼータ関数の拡張法とは, L 関数の被積分関数と相性の良いポリログのアナロジーが構成できればよいわけである. 次がその構成法である.

荒川・金子のゼータ関数の構成法 ([9]) L 関数が, ある関数 G の Mellin 変換

$$L(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} t^{s-1} G(t)\, dt$$

で与えられたとき,

$$L_k(s) := \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} G(t) P_k(\varphi(t))\, dt \qquad (k \geq 1)$$

を考える. ここで $\varphi(t)$ は, 適当な実数 C を用いて $G(t) = C\varphi'(t)/\varphi(t)$ をみたす関数で, $P_1(x)$ は $\varphi(t)$ の逆関数 ($P_1(\varphi(t)) = t$). $P_k(x)$ は, $P_k(x) = \int_0^x (P_{k-1}(x)/x)\, dx$ $(k \geq 2)$ で構成される関数である.

この構成法を L 関数 (2.1) に適用すると, 拡張された L 関数

$$L_k(s) = \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} \frac{\mathrm{Li}_k(1 - e^{-4t})}{4(e^t + e^{-t})}\, dt \qquad (k \geq 1) \tag{2.5}$$

が得られ, さらに定理 2.2 と同様の性質を持つことを示すことが出来る. 多重 Euler 数はこの L 関数の被積分関数を母関数とするものであり, また非正整数点での特殊値である. この L 関数の諸性質については, [10] を参照されたい.

注意 2.3 L 関数 (2.1) の被積分関数に, 上記拡張法をそのまま適用するのは難しい (微分方程式を解いて, その解の逆関数を計算しなければならないので). ここでは, (2.1) を

$$L(s) = \frac{1}{\Gamma(s)} \sum_{a=1}^{4} \chi_{-4}(a) \int_0^\infty t^{s-1} \frac{e^{(4-a)t}}{e^{4t} - 1}\, dt$$

(χ_{-4} は導手 4 の Dirichlet 指標で

$$\chi_{-4}(n) = \begin{cases} 1 & n \equiv 1 \pmod 4, \\ -1 & n \equiv 3 \pmod 4, \\ 0 & n \equiv 0, 2 \pmod 4 \end{cases}$$

として整数全体に拡張したもの) と書いて, 被積分関数の指標に関する和が影響しない $1/(e^{4t} - 1)$ を $G(t)$ として上記の拡張法を適用することで, $L_k(s)$ を導入する.

2.2 多重 Euler 数の明示公式

母関数 (2.2) で定義した多重 Euler 数 $E_n^{(k)}$ はどれほど扱い易いものだろうか. ここでは, 多重 Euler 数の性質を理解するための基本的道具立てとなる 2 つの明示公式について述べる.

まず 1 つ目の明示公式は, 多重 Bernoulli 数を用いて記述するものである. したがって, この明示公式は多重 Euler 数と多重 Bernoulli 数の性質の差異を議論するとき, 或は多重 Bernoulli 数の性質を多重 Euler 数の解析に応用するときに有用なものと言える:

定理 2.4（大野・佐々木 [6]） 任意の非負整数 n および整数 k に対して, 次が成立つ:

$$(n+1)E_n^{(k)} = \frac{1}{2}\sum_{m=0}^{n+1}\binom{n+1}{m}\mathbb{B}_{n-m+1}^{(k)}4^{n-m+1}((-1)^m-(-3)^m). \tag{2.6}$$

もう 1 つの明示公式は, 多重 Euler 数を古典的な Euler 数を用いて記述するものである. したがって, この明示公式を用いれば, 多重 Euler 数が Euler 数の情報をどれだけ踏襲しているか読み取ることもできる.

定理 2.5（[6]） 任意の非負整数 n および整数 k に対して, 次が成立つ:

$$(n+1)E_n^{(k)} = \sum_{m=0}^{n}\binom{n+1}{m}4^{n-m}C_{n-m}^{(k-1)}E_m. \tag{2.7}$$

ここで $C_n^{(k)}$ は変種の多重 Bernoulli 数 (2.4) である.

3 2 重 Euler 数の符号決定と Euler 数の組合せ論的性質

古典的な Bernoulli 数と Euler 数は, その符号が完全に決定されている. 同様に多重版の符号も決定できることが望まれるが, 実際はかなり複雑である. ここでは符号を完全に決定できた 2 重 Euler 数について述べる.

定理 2.5 より, 奇数番目の 2 重 Euler 数は,

$$E_{2l-1}^{(2)} = (1-2l)E_{2l-2}. \tag{3.1}$$

となり, 完全に古典的な Euler 数で記述できることが分かる. さらに, $(-1)^nE_{2n} > 0$ より, 奇数番目の 2 重 Euler 数の符号が決定される:

系 3.1 任意の正整数 n に対して, 次が成り立つ:

$$(-1)^nE_{2n-1}^{(2)} > 0. \tag{3.2}$$

一方, 偶数番目の 2 重 Euler 数の符号を決定するのは難しい. なぜなら, 明示公式 (2.7) より,

$$(-1)^{n-1}E_{2n}^{(2)} = \sum_{m=0}^{n-1}\binom{2n}{2m}\frac{4^{2(n-m)}|B_{2(n-m)}|}{2(n-m)+1}|E_{2m}| - |E_{2n}| \tag{3.3}$$

を得るが, 右辺が正であることを示すには, Euler 数や Bernoulli 数の増大度を詳しく知る必要がある. Euler 数等の漸近公式は知られているが, それらは複雑であり, 我々の問題には適

さない. この問題を解決するために, Euler 数の帰納的関係

$$|E_{2n}| = -\sum_{j=0}^{n-1} \binom{2n}{2j} (-1)^{n+j} |E_{2j}| \tag{3.4}$$

と次の Euler 数の計算アルゴリズムに着目する.

アルゴリズム 3.2（Euler 数の計算アルゴリズム） 数列 $a_{n,m}$ を, 初期値 $a_{0,0} = 1$, $a_{0,m} = 0$ $(m > 0)$ として次で定義する:

$$a_{n,0} = a_{n-1,1}, \quad a_{n,m} = m a_{n-1,m-1} + (m+1) a_{n-1,m+1} \ (n > 0).$$

そのとき, $a_{2n,0} = (-1)^{2n} E_{2n} (= |E_{2n}|)$ が成り立つ.

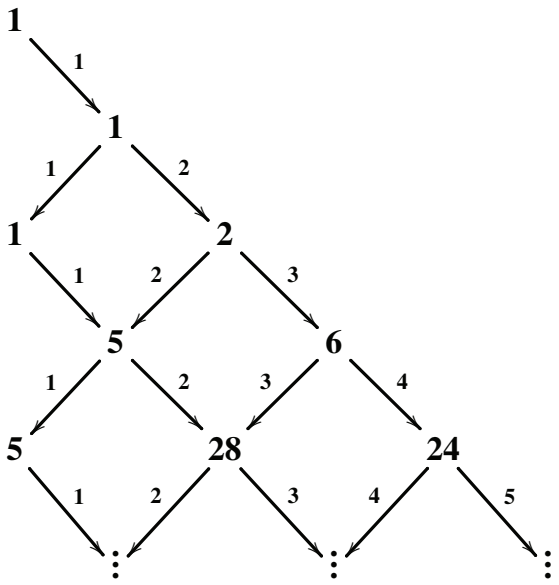

図 1 Euler 数の計算アルゴリズム

アルゴリズムの様子を図示したのが図 1 である. 矢印上の数字は, その矢印方向に進むとその数字倍されることを意味し, 矢印が合流するところの数字は, 各矢印からくる寄与の和が記されている.

図 1 を観察すると, Euler 数 $|E_{2n}|$ は $a_{0,0}$ から $a_{2n,0}$ までの最短経路に対する寄与の総和として与えられることが分かる. 例えば $a_{4,0} = 5 (= |E_4|)$ は, $a_{0,0} = 1$ からジグザグに降りてくる経路 (寄与は $1 \cdot 1 \cdot 1 \cdot 1 = 1$) と, 最初に右斜め下に 2 つ進み, 次に左斜め下に 2 つ進む経路 (寄与は $1 \cdot 2 \cdot 2 \cdot 1 = 4$) に対する寄与の総和となっている. 一般に, $a_{2n,0}$ には最初に右斜め下に n 進み, 次に左斜め下に n 進む経路の寄与が含まれているので,

$$|E_{2n}| \geq n!^2$$

という評価が成り立つ. これは決してよい評価とは言えないが, Euler 数の情報を $n!$ という非常に扱いやす形に変換できるという利点がある.

同様のアルゴリズムと評価が, タンジェント数 $T_n := (2^{2n}-1)2^{2n}|B_{2n}|/(2n)$ に対しても成り立つ. すなわち,

$$\frac{4^{2n}|B_{2n}|}{2n+1} > \frac{T_n}{2} \geq \frac{n!(n-1)!}{2}. \tag{3.5}$$

この評価と (3.4) を組み合わせることで次を得る:

定理 3.3（[6]） 任意の正整数 $n \geq 2$ に対して, 次が成り立つ:

$$(-1)^{n-1}E_{2n}^{(2)} > 0. \tag{3.6}$$

注意 3.4 $n = 0, 1$ のときは $(-1)^{n-1}E_{2n}^{(2)} < 0$ となり, 定理 3.3 の不等式は成り立たない. これは, $n = 1$ と $n = 2$ の間で符号の反転現象が起きているためである. 数値実験では, 一般の多重 Euler 数においては, このような現象が不規則に (我々がまだその規則性を理解できていないだけかもしれない) 現れることが確認できる.

4 組合せ論的解釈

ここでは, 多重 Bernoulli 数と多重 Euler 数の組合せ論的解釈について議論する. まず, 多重 Bernoulli 数の組合せ論的解釈について述べる.

4.1 多重 Bernoulli 数とロンサム行列

ロンサム行列とは, 成分が 0 か 1 の行列で, その行和・列和によって一意的に再構成可能な行列のことである (図 2, 3 参照). Brewbaker [3] は, サイズ $m \times n$ のロンサム行列の個数が, 多重 Bernoulli 数 $\mathbb{B}_n^{(-m)}$ と一致することを示した. すなわち,

$$\mathbb{B}_n^{(-m)} = \#\{A \in M(m, n; \{0, 1\}) \mid A : \text{ロンサム行列}\}$$

が成り立つ. ここで, 多重 Bernoulli 数の双対性 $\mathbb{B}_n^{(-m)} = \mathbb{B}_m^{(-n)}$ は, ロンサム行列においては行列の転置に対応していることに注意されたい.

$$\begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix} \begin{matrix} \mathbf{2} \\ \mathbf{1} \end{matrix}$$
$$\begin{matrix} \mathbf{1} & \mathbf{2} & \mathbf{0} \end{matrix}$$

図 2 ロンサム行列の例

$$\begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix} \begin{matrix} \mathbf{1} \\ \mathbf{1} \end{matrix} \qquad \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{matrix} \mathbf{1} \\ \mathbf{1} \end{matrix}$$
$$\begin{matrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \end{matrix} \qquad \begin{matrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \end{matrix}$$

図 3 ロンサム行列でない例

4.2 多重 Euler 数の組合せ論的解釈

まず, 負のインデックスの多重 Euler 数の明示公式を述べることから始める. 負のインデックスの場合, 多重 Euler 数は定理 2.4, 2.5 よりもさらに簡潔な形で書くことができる. 特に, インデックス $k = 0, -1$ の場合は本節の主役となるため, ここに特記しておく.

定理 4.1（[6]） 任意の正整数 n に対して, 次が成り立つ:

$$nE_{n-1}^{(0)} = \frac{3^n - 1}{2}, \qquad nE_{n-1}^{(-1)} = \frac{7^n - 5^n}{2}.$$

定理 4.1 が示す数列がどのような意味を持つのかを調べてみると, 次のような対象物と結びつくことがわかった.

事実 4.2 数列 $nE_{n-1}^{(0)} = (3^n - 1)/2$ は, n 次元超立方体の異なる 2 頂点の組で与えられる線分で, 平行でないものの個数と一致する.

事実 4.3 数列 $nE_{n-1}^{(-1)} = (7^n - 5^n)/2$ は, $\underbrace{5 \times \cdots \times 5}_{n}$ n 次元格子内の 5 点が共線となる組合せの数と一致する[*1].

上記の幾何学的イメージについては, 図 4, 5 を参照されたい. これらは多重 Euler 数の組合せ論的解釈の萌芽であって, 多重 Euler 数を数論的な枠組みで扱うには不十分すぎることを示唆するものと言えよう. しかしながら, 上記は数値的に一致しているだけであり, 多重 Euler 数自体に, 対応する組合せ論的な背景があるかどうかはまだ分かっていない. 今後の進展が待たれるところである.

さて, 一般に負のインデックスの多重 Euler 数全体に組合せ論的な意味付けを期待するのであれば, それらはすべて正の整数でなければならない. しかしながら, 明示公式 (2.6) からは, 整数であることは容易に分かるが, 正であることを理解するのは難しい. 多重 Bernoulli 数のときは, (2.6) のような明示公式の代わりに, Stirling 数を用いた新たな明示公式を与えることで正値性を示しているので, 多重 Euler 数でもそのような明示公式が必要である. それが次の定理であって, 多重 Euler 数の正値性を示すばかりでなく, インデックスに関する帰納的関係も与えるものとなっている:

[*1] [2] によれば, これは $n \leq 9$ に対してのみ証明されていて, 一般には予想だそうだが, 2011 年 12 月に RIMS で講演した際に山本修司氏から一般に証明できることをご指摘頂いた.

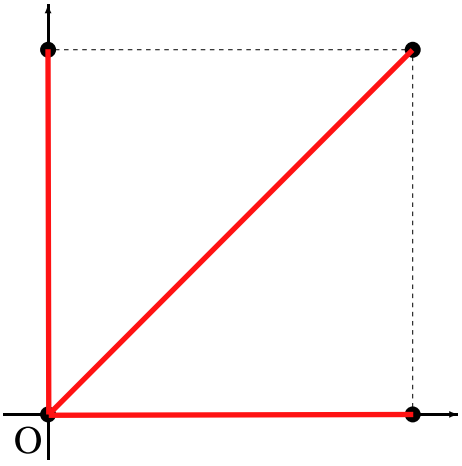

図 4　2 次元超立方体の 2 頂点を結ぶ平行でない線分

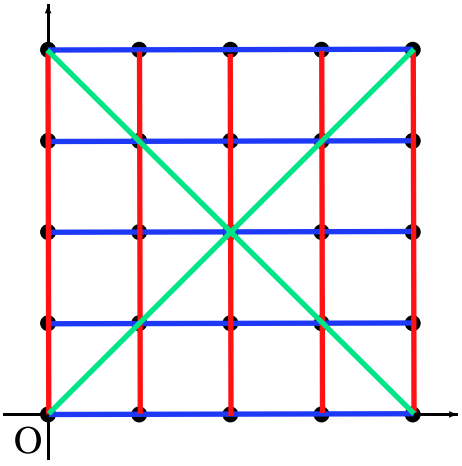

図 5　5×5 2 次元格子内の 5 点が共線

定理 4.4（[6]）　任意の非負整数 k, $n(>0)$ に対して,

$$nE_{n-1}^{(-k)} = \sum_{j=0}^{\min(k,n-1)} j!^2 \left(\sum_{m=1}^{n-j} \binom{n}{m} m E_{m-1}^{(0)} \left\{ {n-m \atop j} \right\} 4^{n-m} \right) \left\{ {k+1 \atop j+1} \right\},$$

ここで $\left\{ {k \atop l} \right\}$ は第 2 種 Stirling 数である.

特に, 定理 4.4 で $k = 1$ のときは次のように書くことができる:

系 4.5　任意の正整数 n に対して,

$$nE_{n-1}^{(-1)} = \sum_{m=1}^{n} \binom{n}{m} m E_{m-1}^{(0)} 4^{n-m}.$$

系 4.5 の観点からすると, 我々は $nE_{n-1}^{(0)}$ と $nE_{n-1}^{(-1)}$ の組合せ論的解釈が同質である理由を自然に理解することができる. 一方, $k \geq 2$ に対しては, 系 4.5 のように綺麗にはならない. これは, もし一般に多重 Euler 数が組合せ論的解釈を持つならば, $k \geq 2$ に対応する組合せ論的背景は, $k = 0, 1$ の時と比べてはるかに複雑なものであるということを示唆しているのかもしれない.

5 負のインデックスの多重 Euler 数の数論的性質

前節で見たように, 負のインデックスの多重 Euler 数 $(n+1)E_n^{(-k)}(=\widetilde{E}_n^{(-k)})$ は整数であり, 一般に有理数である正のインデックスと比べると, 扱い易い対象と言える. ここでは, 整数論の観点から負のインデックスの多重 Euler 数の性質を多数紹介する.

5.1 Parity result

負のインデックスの多重 Euler 数の偶奇は完全に決定でき, その規則性は次のように記述される.

定理 5.1（parity result [7]） 非負整数 k, n に対して, 次が成り立つ：

$$(n+1)E_n^{(-k)} \equiv \begin{cases} 0 \pmod 2 & (n：奇数), \\ 1 \pmod 2 & (n：偶数). \end{cases}$$

注意 5.2 上定理より, n が奇数のときは多重 Euler 数は偶数である. この事実から多重 Euler 数の 2-order に自然と興味を抱くが, 数値実験から任意の奇数 n に対して $\mathrm{ord}_2\, \widetilde{E}_n^{(-k)} \stackrel{?}{=} 1$ が期待される. この観察は [6] で部分的に解決されている.

5.2 n 進的周期性

多重 Euler 数の p-order の評価, あるいは $\bmod p$ の合同式は整数論において非常に興味深い研究である. まず, 多重 Euler 数の合同式について述べる. 素数番目の多重 Euler 数について, 次を得る：

定理 5.3 任意の奇素数 p および非負整数 k に対して,

$$pE_{p-1}^{(-k)} \equiv 1 \pmod p. \tag{5.1}$$

上定理は素数番目の多重 Euler 数の p-order だけでなく, $E_{p-1}^{(-k)}$ が真に有理数であることも示している. なぜなら, $\widetilde{E}_n^{(-k)} = (n+1)E_n^{(-k)}$ は (2.6) より整数であり, したがって $E_n^{(-k)}$ の分母は高々 $(n+1)$ である. より一般には次が成り立ち, その帰結として $E_n^{(-k)}$ の整数性もわかる.

定理 5.4 奇素数 p とする. 正の奇数 n および $k \equiv p-2 \pmod{p-1}$ を満たす非負整数 k に対して,

$$(n+1)E_n^{(-k)} \equiv 0 \pmod p.$$

表 3　$\widetilde{E}_n^{(-k)}(=(n+1)E_n^{(-k)})$ $(0 \le k \le 7)$

$n\backslash k$	0	1	2	3	4
0	1	1	1	1	1
1	4	12	28	60	124
2	13	109	493	1837	6253
3	40	888	7192	42840	220120
4	121	6841	95161	865081	6396601
5	364	51012	1189108	16022100	165380884
6	1093	372709	14331493	280592677	3958958053
7	3280	2687088	168625072	4730230320	89841286960
8	9841	19200241	1951326961	77624198641	1961872865521
9	29524	136354812	22314285388	1249160130540	41639632236844
10	88573	964249309	252966361693	19811958812317	864960182738653

$n\backslash k$	5	6	7
0	1	1	1
1	252	508	1020
2	20269	63853	197677
3	1040088	4666072	20235480
4	41968441	255205561	1474388281
5	1460924052	11672605588	87058925460
6	46088370469	473519630053	4461656417317
7	1356820880688	17643342363952	206695980640560
8	37978754131441	617481161118961	8884959409517041
9	1023561900404652	20608543411101868	360705084750192300
10	26796243596416669	662962530489535453	14004154117362681757

系 5.5　p_j $(j=1,\dots,\nu)$ を相異なる素数とし, 正整数 k を $k \equiv p_j - 2 \pmod{p_j - 1}$ $(j=1,\dots,\nu)$ を満たすものとする. そのとき, 任意の奇数 n に対して,

$$(n+1)E_n^{(-k)} \equiv 0 \pmod{p_1 \cdots p_\nu}.$$

注意 5.6　系 5.5 で $n+1 = p_1 \cdots p_\nu$ のとき, 多重 Euler 数 $E_n^{(-k)}$ は整数であることがわかる. 例えば, k が奇数のとき, $E_5^{(-k)}$ は整数であり, $k \equiv 3 \pmod 4$ のとき, $E_9^{(-k)}$, $E_{29}^{(-k)}$ は

整数である. また, 表 2 から $E_{2^s-1}^{(-k)} \in \mathbb{Z}$ $(s \in \mathbb{Z}_{>0})$ を推測できるが, これは [6] で示されている.

最後に, 多重 Euler 数 $(n+1)E_n^{(-k)}$ の一の位の周期性について述べる. その周期性は表 3 を観察すれば容易に確認でき, 次のように定式化される:

定理 5.7 n, n', k, k' を $n \equiv n', k \equiv k' \pmod 4$ を満たす正整数とする. そのとき,

$$(n+1)E_n^{(-k)} \equiv (n'+1)E_{n'}^{(-k')} \pmod{10}.$$

謝辞

講演の機会を与えて下さった世話人の先生方に感謝申し上げます.

参考文献

[1] T. Arakawa and M. Kaneko, *Multiple zeta values, poly-Bernoulli numbers, and related zeta functions*, Nagoya Math. J. **153** (1999), 189–209.
[2] P. Barry, *Sequence number* A081200 *in On-line Encyclopedia of Integer Sequences*, http://oeis.org/A081200.
[3] C. Brewbaker, *Lonesum* $(0,1)$*-matrices and poly-Bernoulli numbers of negative index*, Master's thesis, Iowa State University, 2005.
[4] M. Kaneko, *Poly-Bernoulli numbers*, J. Th. Nombre Bordeaux **9** (1997), 199–206.
[5] S. Launois, *Rank t $\mathscr{H}$-primes in quantum matrices*, Comm. Algebra **33** (2005), 837–854.
[6] Y. Ohno and Y. Sasaki, *On poly-Euler numbers*, preprint.
[7] Y. Ohno and Y. Sasaki, *On the parity of poly-Euler numbers*, RIMS Kōkyūroku Bessatsu, **B32** (2012), 271–278.
[8] Y. Ohno and Y. Sasaki, *Periodicity on poly-Euler numbers and Vandiver type congruence for Euler numbers*, RIMS Kōkyūroku Bessatsu, **B42** (2013), .
[9] Y. Sasaki, *On generalized poly-Bernoulli numbers and related L-functions*, J. Number Theory **132** (2012), 156–170.
[10] 佐々木義卓, 多重 Euler 数の諸性質と付随する L 関数について, 第 4 回多重ゼータ研究集会報告集, 2011, pp. 1-8.
[11] M. Shikata, *Lonesum matrices and poly-Bernoulli numbers*, Kyoto Sangyo University essays. Natural science series, **40** (2011), 1–12.

正整数上へのある作用の繰り返しの振る舞い

鳴門教育大学大学院学校教育研究科　平野 康之
愛知工業大学基礎教育センター　隅山孝夫

1. はじめに

$f : \mathbf{N} \to \mathbf{N}$ を，n が偶数のとき $f(n) = n/2$, n が奇数のとき $f(n) = 3n+1$ により定義する。**コラッツ予想**とは,「任意の自然数 n に対して，$V(n) = \{f^k(n) \mid k = 0, 1, 2, \cdots\}$ は 1 を含む。」という主張である。コンピュータを用いた計算により、3×2^{53} までには反例がないことが確かめられている。コラッツ予想及びその一般化についてはコンピュータを用いた計算が行なわれているが，多くの場合，発散についての情報が殆んど無い。今回は，3n + 1 の代わりに n を変数とするいくつかの関数を考えた場合に，循環や発散などの振る舞いについて論じる。

より一般的に述べると，関数 $f : \mathbf{N} \to \mathbf{N}$ に対して，$V_f(n) = \{f^k(n) \mid k = 0, 1, 2, \cdots\}$ とおく。各自然数 n に対して $V_f(n)$ が有限集合になるか，無限集合になるか，そして，もし，有限集合になるときはどのような有限集合になるか，を問題にしたい。この問題は繊細であり，現時点では余りわからないので，我々は極端な場合のみ扱うことにする。

2. 一次関数

$f : \mathbf{N} \to \mathbf{N}$ を $f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 3n+1 & \text{if } n \text{ is odd} \end{cases}$ により定義する。先ほど述べたように，コラッツ予想とは,「任意の自然数 n に対して，$V(n) = \{f^t(n) \mid t = 0, 1, 2, \cdots\}$ は 1 を含む。」という主張である。

そこでまず，上の関数 f の一般化を考えよう。p, q を自然数とし，$p > 1$ とする。$f_{p,q,r}$ を，$p|n$ のとき $f(n) = \dfrac{n}{p}$, そして p が n を整除しないとき $f(n) = p[\dfrac{qn}{p} + r]$ と定義する。ここで [ ] はガウス記号を表す。

例 1. コラッツ予想に現れる関数は $f_{2,3,1}$ である。実際，n が偶数でなければ，0 以上の整数 k があり，$n = 2k + 1$ と書けるので，
$2[\frac{3n}{2} + 1] = 2[3k + \frac{3}{2} + 1] = 2(3k + 2) = 6k + 4 = 2(2k + 1) = 3n + 1$ となる。

例 2. $f = f_{3,2,1}$ を考える。このとき，$f(n) = \begin{cases} k & \text{if } n = 3k \\ 6k+3 & \text{if } n = 3k+1 \\ 6k+6 & \text{if } n = 3k+2. \end{cases}$
任意の自然数 n に対して，$V(n) = \{f^m(n) \mid m = 0, 1, 2, \cdots\}$ が 1 か 2 を含むことを示そう。これを n に関する帰納法で示そう。

$n = 3k$ ならば $f(n) = k < n$.

$n = 3k + 1$ かつ $k \geq 1$ ならば $f^2(n) = 2k + 1 < 3k + 1 = n$.

$n = 3k + 2$ かつ $k \geq 1$ ならば $f^2(n) = 2k + 2 < 3k + 2 = n$.

よって $n = 2$ の場合だけ確かめればよい。この場合，$2 \to 6 \to 2$ とループになるので，$1 \notin V(2), 2 \in V(2)$ となる。以上から $V(n)$ は 1 か 2 を含むことがわかる。

例 3. $f = f_{3,4,1}$ を考える。このとき，$f(n) = \begin{cases} k & \text{if } n = 3k \\ 3(4k+2) & \text{if } n = 3k+1 \\ 3(4k+3) & \text{if } n = 3k+2. \end{cases}$
である。$7 \to 10 \to 14 \to 19 \to 26 \to 35 \to 47 \to 63 \to 21 \to 7$ となり，loop になる。50 以下の数を考えると，2, 3, 6, 9, 13, 18, 21, 27, 39, は 1 に到達する。その他の数は 7 に到達する。

予想 1. 任意の自然数 n に対して，$V_{3,4,1}(n) = \{f^m_{3,4,1}(n) \mid m = 0, 1, 2, \cdots\}$ は 1 か 7 を含む。

定理 1. $f = f_{p,q,r}$ とおくとき，$q < p$ ならば，任意の n に対して，$V_{p,q,r}(n) = \{f^t(n) \mid t = 0, 1, 2, \cdots\}$ は有限集合である。

証明. n は $n = pk + i$ $(0 \leq i \leq p - 1)$ の形に書ける。
もし $\frac{r-1}{p-q} < k$ であれば $i = 0$ のとき $f(n) = k < n$ である。$0 < i \leq p - 1$ のとき，$f^2(n) = [\frac{q}{p}(pk + i) + r] = [qk + \frac{q}{p}i + r] \leq qk + i - 1 + r < pk + i = n$. 最後の不等式は $r - 1 < (p - q)k$ から従う。従って，ある $m > 0$ に対して，$\frac{r-1}{p-q} < [\frac{f^m(n)}{p}]$ であれば $f^{m+1}(n) = f(f^m(n)) < n$ または $f^{m+2}(n) = f^2(f^m(n)) < n$ となる。従って，1 から n の各 i に対して，$\frac{r-1}{p-q} < [\frac{f^m(i)}{p}]$ となる m があれば，最初の m を m_i とし，無ければ $m_i = 0$ とおけば，$V_{p,q,r}(n)$ は $\{1, 2, \cdots, n\} \cup \{f^{m_i}(i) \mid i = 1, 2, \cdots, n\} \cup \{f^{m_i+1}(i) \mid i = 1, 2, \cdots, n\}$ に含まれる。

例 4. コラッツの問題を少し変えて，

$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 5n+1 & \text{if } n \text{ is odd} \end{cases}$
とすると，1 に到達しない数がある。例えば，次のようなループがある：
$13 \to 66 \to 33 \to 166 \to 83 \to 416 \to 208 \to 104 \to 52 \to 26 \to 13$

m を正の奇数とする。$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ n+m & \text{if } n \text{ is odd} \end{cases}$ と定義する。

定理 2. 任意の k に対して，$f^{2k}(n) < n + 2m$ が成り立つ。従って，$V_f(n) = \{f^t(n) \mid t = 0, 1, 2, \cdots\}$ は有限集合である。

証明. n を奇数とすると，$f(n) = n+m$, よって，$f^2(n) = \dfrac{n+m}{2} < n + 2m$. n が偶数のとき，$f(n) = n/2$ となり，$n/2$ が偶数ならば $f^2(n) = n/4 < n + 2m$, $n/2$ が奇数ならば $f^2(n) = n/2 + m < n + 2m$ となる。k に関する帰納法により，$f^{2k}(n) < n + 2m$ と仮定する。$f^{2k}(n)$ が偶数ならば，$f^{2k+1}(n) = f^{2k}(n)/2 < n/2 + m$ となるので，$f^{2k+2}(n) < n/2 + m + m = n/2 + 2m < n + 2m$ となる。$f^{2k}(n)$ が奇数のとき，$f^{2k+1}(n) = f^{2k}(n) + m < n + 2m + m$ となる。このとき，$f^{2k}(n) + m$ は偶数より，$f^{2k+2}(n) = \dfrac{f^2k(n) + m}{2} < \dfrac{n}{2} + \dfrac{3}{2}m < n + 2m$ となる。

3. 二次関数

f が一次関数の場合は，コンピュータを用いた計算である自然数 n に対して $\lim_{m\to\infty} f^m(n) = \infty$ となることが予測されるが，多くの場合，証明することは困難である。しかし，一般の f を考えると，このようなことが証明できる場合がある。mod 8 で考えると，奇数は 1，3，5，7 であるので，まず，次の表を考えよう：

n	0	1	2	3	4	5	6	7
$n^2+1 \pmod 8$	1	2	5	2	1	2	5	2
$3n^2+1 \pmod 8$	1	4	5	4	1	4	5	4
$5n^2+1 \pmod 8$	1	6	5	6	1	6	5	6
$7n^2+1 \pmod 8$	1	0	5	0	1	0	5	0

(1) $f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ n^2+1 & \text{if } n \text{ is odd} \end{cases}$
と定義すると，n が奇数であれば，$n = 2k+1$ と置くことができるので，
$f(n) = (2k+1)^2 + 1 = 2(2k^2 + 2k + 1)$.
上の表から $2k^2 + 2k + 1$ は常に奇数であるので，$n > 1$ ならば，
$f^3(n) = \dfrac{n^2+1}{2} > n$
となる。よって，$n > 1$ が奇数ならば $\mathrm{im}_{m\to\infty} f^m(n) = \infty$ となる。

(2) $f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 3n^2+1 & \text{if } n \text{ is odd} \end{cases}$
と定義すると，n が奇数であれば，$n = 2k+1$ と置くことができるので，

$f(n) = 3(2k+1)^2 + 1 = 4(3k^2+3k+1)$.

上の表から $3k^2+3k+1$ は常に奇数であるので,

$f^3(n) = \dfrac{3n^2+1}{4} > n$

となる。よって，n が奇数ならば $\mathrm{im}_{m\to\infty} f^m(n) = \infty$ となる。

(3) $f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 5n^2+1 & \text{if } n \text{ is odd} \end{cases}$

と定義すると，n が奇数であれば，$f^2(n) = \dfrac{5n^2+1}{2}$ は奇数となり,

また，$g^2(n) = \dfrac{5n^2+1}{2} > n$ となる。よって，n が奇数ならば $\mathrm{im}_{m\to\infty} f^m(n) = \infty$ となる。

(4) $f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 7n^2+1 & \text{if } n \text{ is odd} \end{cases}$

と定義すると，上の表からは，$n > 1$ が奇数のとき $\lim_{m\to\infty} f^m(n) = \infty$ となるかどうかはわからない。そこで，mod 16，mod 32，等々，一般に n を大きくして，mod 2^n で考えればいいのであるが，そうすると考えなければならない奇数も 7 以外に沢山増えてくる。

予想 2. $7n^2+1 \equiv -(n^2-1) \pmod 8$ であるので，$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ n^2-1 & \text{if } n \text{ is odd} \end{cases}$ を考えてみる。このとき，無数の奇数 n に対して，$\lim_{m\to\infty} f^m(n) = \infty$ となる。特に，$\lim_{m\to\infty} f^m(13) = \infty$ となる。

問題. a, b, c を定数とし，$g(n) = an^2+bn+c$ とおく。$f : \mathbf{N} \to \mathbf{N}$ を

$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ \mathrm{g(n)} & \text{if } n \text{ is odd} \end{cases}$ と定義する。

(1) 与えられた $a,\ b,\ C$ に対して，$V(n) = \{f^k(n) \mid k = 0, 1, 2, \cdots\}$ が無限集合になるような n を決定せよ。

(2) $1 < n$ が奇数ならば $\lim_{m\to\infty} f^m(n) = \infty$ となるような g はどのようなものか。

4. 指数関数

この節では指数関数について考える。特に，$g(n) = e^{2^n \log 3} - 1 = 3^{2^n} - 1$ について考える。

例 5. [1, p.86] の補題 21.12 によると自然数 n に対して，$3^{2^n} - 1 = 1 + 2^{n+2}k$, $(k, 2) = 1$ となる。そこで，$f : \mathbf{N} \to \mathbf{N}$ を

$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 3^{2^n} - 1 & \text{if } n \text{ is odd} \end{cases}$ と定義する。このとき，$1 < n$ が奇数ならば

$f^{n+3}(n) = \dfrac{3^{2^n}-1}{2^{n+2}}$ は奇数であり，$f^{n+3}(n) > n$ となる。よって，n が奇数ならば $\lim_{m\to\infty} f^m(n) = \infty$ となる。ちなみに，$f(1) = 8,\ f^4(1) = 1,\ f^m(2^m) = 1$ である。

例 6. 自明な例として， $f : \mathbf{N} \to \mathbf{N}$ を
$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 2^n & \text{if } n \text{ is odd} \end{cases}$ と定義すると任意の自然数 n に対して，$V_f(n)$ は有限集合である。

問題. $g(n)$ を指数関数から作られる関数とする。$f : \mathbf{N} \to \mathbf{N}$ を
$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ \mathrm{g(n)} & \text{if } n \text{ is odd} \end{cases}$ と定義する。このとき，$1 < n$ が奇数ならば $\lim_{m\to\infty} f^m(n) = \infty$ となるような g はどのようなものか。

予想 2 に対する参考データ. データの読み方は，End は 1 で終わる場合。Out of Range は，計算途中で３００桁を超えた場合。

a = 3 End	a = 49 Out of Range	a = 95 Out of Range
a = 5 End	a = 51 Out of Range	a = 97 Out of Range
a = 7 End	a = 53 Out of Range	a = 99 Out of Range
a = 9 End	a = 55 Out of Range	a = 101 Out of Range
a = 11 End	a = 57 Out of Range	a = 103 Out of Range
a = 13 Out of Range	a = 59 Out of Range	a = 105 Out of Range
a = 15 End	a = 61 Out of Range	a = 107 Out of Range
a = 17 End	a = 63 End	a = 109 Out of Range
a = 19 Out of Range	a = 65 End	a = 111 Out of Range
a = 21 Out of Range	a = 67 Out of Range	a = 113 Out of Range
a = 23 End	a = 69 Out of Range	a = 115 Out of Range
a = 25 Out of Range	a = 71 Out of Range	a = 117 Out of Range
a = 27 Out of Range	a = 73 Out of Range	a = 119 Out of Range
a = 29 Out of Range	a = 75 Out of Range	a = 121 Out of Range
a = 31 End	a = 77 Out of Range	a = 123 Out of Range
a = 33 End	a = 79 Out of Range	a = 125 Out of Range
a = 35 Out of Range	a = 81 Out of Range	a = 127 End
a = 37 Out of Range	a = 83 Out of Range	a = 129 End
a = 39 Out of Range	a = 85 Out of Range	a = 131 Out of Range
a = 41 Out of Range	a = 87 Out of Range	a = 133 Out of Range
a = 43 Out of Range	a = 89 Out of Range	a = 135 Out of Range
a = 45 Out of Range	a = 91 Out of Range	a = 137 Out of Range
a = 47 Out of Range	a = 93 Out of Range	a = 139 Out of Range

a = 141 Out of Range
a = 143 Out of Range
a = 145 Out of Range
a = 147 Out of Range
a = 149 Out of Range
a = 151 Out of Range
a = 153 Out of Range
a = 155 Out of Range
a = 157 Out of Range
a = 159 Out of Range
a = 161 Out of Range
a = 163 Out of Range
a = 165 Out of Range
a = 167 Out of Range
a = 169 Out of Range
a = 171 Out of Range
a = 173 Out of Range
a = 175 Out of Range
a = 177 Out of Range
a = 179 Out of Range
a = 181 End
a = 183 Out of Range
a = 185 Out of Range
a = 187 Out of Range
a = 189 Out of Range
a = 191 Out of Range
a = 193 Out of Range
a = 195 Out of Range
a = 197 Out of Range
a = 199 Out of Range
a = 201 Out of Range
a = 203 Out of Range
a = 205 Out of Range
a = 207 Out of Range
a = 209 Out of Range
a = 211 Out of Range
a = 213 Out of Range
a = 215 Out of Range
a = 217 Out of Range

References

[1] 永尾 汎: 代数学 (新数学講座 4), 朝倉書店 (1983)
[2] 三室 智明, 西村 滋人, 平松 豊一:コラッツ予想について, http://www.media.hosei.ac.jp/bulletin/vol16-25.pdfni
[3] 大平麗子, 山下倫範.: Collatz 問題の一般化について, yamashita-lab.net/open/p-col.pdf
[4] Richard K. Guy(Ed.), 一松信 監訳: 数論における未解決問題集（シュプリンガー・フェアラーク東京，1983）.
[5] Jeffrey C. Lagarias : The 3x + 1 Problem and its Generalizations, Amer. Math. Monthly 92(1985), 3-23. http://www.cecm.sfu.ca/organics/papers/lagarias/

有向グラフの複素球面埋め込みに関するアルゴリズム

野崎寛
愛知教育大学数学教育講座
hnozaki@auecc.aichi-edu.ac.jp

1 はじめに

本原稿は，2013 年 12 月に行われた第 10 回「代数学と計算」研究集会において，同題にて著者により行われた講演の内容に関する報告集である。本原稿を執筆するにあたり，招待していただいた，生田卓也（神戸学院大学）様を初めとする，主催者，実行委員の方々に，この場を借りて，改めて感謝申し上げたい。

本原稿では，著者が講演を行ったものから，特に複素球面上の 3-code に焦点をしぼり紹介したい．ここで，複素球面上の有限集合で，異なる 2 点間における複素内積の集合の濃度が s のときに，その集合を複素 s-code と呼ぶことにしている．つまり，X を d 次元複素球面 $\Omega(d)$ の有限集合としたとき，

$$A(X) = \{\langle x, y\rangle \mid x, y \in X, x \neq y\}$$

の濃度が s のときに，X を複素 s-code と呼ぶ．特に，$A(X)$ は虚数を含むと仮定する．もし，$A(X)$ の成分が実数のみで構成されている場合は，X は実球面に実現できる．任意の $\alpha \in A(X)$ に対して，その複素共役 $\overline{\alpha}$ もまた，$A(X)$ の元でなければならないことから，X が 3-code であるならば，虚数 α, 実数 β が存在して，$A(X) = \{\alpha, \overline{\alpha}, \beta\}$ と表わされることが分かる．ここで，辺集合を $E = \{(x, y) \mid \langle x, y\rangle = \alpha, x \in X, y \in X\}$ とすることで，3-code X に自然に有向グラフ (X, E) の構造を入れることが出来る．本原稿で問題としたいのは，勝手な有向グラフを与えたときに，そのグラフ構造を持つ 3-code を，どのように構成することが出来るかということである．

有向グラフと 3-code の関係は，すでに知られている実空間上での無向グラフと 2-距離集合の関係から動機を得ている．ユークリッド空間 $\mathbb{R}^n$ 上の有限集合 X で，互いに異なる 2 点間のユークリッド距離の集合の濃度が s であるとき，X を s-距離集合と呼ぶ．2-距離集合は明らかに無向グラフの構造を持っている．与えられた無向グラフから，そのグラフ構造を持つ 2-距離集合の構成法については，[2] により与えられており，極小な次元の埋め込みが高々2 種類であることが分かっている．後に，その極小次元が，隣接行列の固有空間のパラメータにより記述できることを，Roy [5] が示している．[2] において，元の個数が最大である距離集合が 7 次元以下で分類されている．ここで，これらの理論を関係の個数が 3 である彩色グラフと，3 距離集合の間で考えたいが，現在のところ上手くいっていない．s 彩色グラフの s-距離集合としての埋め込みは，s-距離集合の分類問題における，最も重要な問題のひとつである．

代数的組合せ論の立場からは，Delsarte–Goethals–Seidel [1] により，距離集合とデザイン，アソシエーションスキームの密接な関係が明らかにされ，距離集合の視点から，デザイン，アソシエーションスキームの特徴づけや，構成問題へのアプローチが期待される．また，Roy–Suda [6] により，[1] の理論の複素球面版が与えられており，全てが上手く行く訳ではないようだが，実球面における諸定理の複素球面版が求められてきている．

2　無向グラフの 2 距離集合としての埋め込み

本節では，無向グラフの 2 距離集合としての埋め込みにおける諸定理を紹介する．ここでの結果を用いて有向グラフの 3-code としての埋め込みを次の節で考えることになる．特に，無向グラフの極小次元への埋め込みが，いつ球面にのるのかが重要になってくる．

Roy [5] は極小次元を隣接行列 A の固有空間の情報で記述することに成功した．それを紹介するために，記号をいくつか用意する．τ_i を i 番目に小さい A の異なる固有値であるとし，m_i を τ_i の重複度とする．E_i を τ_i の固有空間とし，P_i を E_i への直交射影行列とする．β_i を τ_i の主角 (main angle) とする．つまり，

$$\beta_i = \frac{1}{\sqrt{n}}||P_i j||,$$

とする．ここで，$j = (1, \ldots, 1)^T$, $||x|| = \sqrt{x^T x}$ であるとする．このとき

次が成立する．

Theorem 2.1 (Roy [5])**.** 無向グラフ G の *2* 距離集合としての埋め込みの極小次元を d とする．また極小次元の埋め込みの距離の集合を $\{1, c\}(0 \leq c < 1)$ とする．そのとき次が成立する．

(1) $\beta_1 = 0$ ならば，$c = \tau_1/(\tau_1 + 1)$, $d = n - m_1 - 1$.

(2) $\beta_1 \neq 0$ かつ $m_1 > 1$ ならば，$c = \tau_1/(\tau_1 + 1)$, $d = n - m_1$.

(3) $\beta_2 = 0$, $m_1 = 1$, $\tau_2 < -1$ かつ $\beta_1^2/(\tau_2 - \tau_1) = \sum_{i \geq 3} \beta_i^2/(\tau_i - \tau_2)$ ならば，$c = \tau_2/(\tau_2 + 1)$, $d = n - m_2 - 2$.

(4) $\beta_2 = 0$, $m_1 = 1$, $\tau_2 < -1$ かつ $\beta_1^2/(\tau_2 - \tau_1) > \sum_{i \geq 3} \beta_i^2/(\tau_i - \tau_2)$ ならば，$c = \tau_2/(\tau_2 + 1)$, $d = n - m_2 - 1$.

(5) 上記以外であれば，$d = n - 2$.

上の条件 (i) を満たすグラフを Type (i) と呼ぶことにする $(1 \leq i \leq 5)$. 無向グラフの極小次元埋め込みが，いつ球面に乗るかは，この Type により判別が可能である．

Theorem 2.2 (野崎–篠原 [3])**.** (1) *Type (1), (2), (4)* の無向グラフの極小次元埋め込みは *1* つの球面に乗る．

(2) *Type (3), (5)* の無向グラフの極小次元埋め込みは *1* つの球面に乗らない．

(3) 極小次元でない埋め込みは *1* つの球面に乗る．

3 節では，球面に乗る埋め込みを必要とするので，主に Type (1), (2), (4) のグラフを扱うことになる．極小次元でない埋め込みは，今回の議論においては，重要な役割を果たさない．

3 最大 3-code の分類アルゴリズム

この節では，元の個数が最大の 3-code を分類するアルゴリズムの概要を紹介する．与えられた有向グラフに対して，3-code としての極小次元埋め込みを与えることが理想であったが，それに達することは出来なかった．しかし，最大な 3-code を分類するために必要であろうグラフの極小

次元を与えることには成功し，結果として 3 次元以下の最大 3-code を分類することができた．

まず，3-code と球面 2 距離集合との関係を述べたい．次に定義される複素球面 $\Omega(d)$ から実球面 $\mathbb{R}^d$ への自然な写像 $\phi : \Omega(d) \to S^{2d-1}$ を準備する．

$$\phi : (a_1 + b_1\sqrt{-1}, \ldots, a_d + b_d\sqrt{-1})^T \mapsto (a_1, b_1, \ldots, a_d, b_d)^T.$$

このとき，

$$\phi(x)^T\phi(y) = \mathrm{Re}(x^*y),$$

が成り立つ．つまり複素内積の実部が，像の実内積となっている．これを 3-code X で考えると，$A(X) = \{a \pm b\sqrt{-1}, c\}$ であるとすれば，$A(\phi(X)) = \{a, c\}$ となるため，$\phi(X)$ は球面 2 距離集合となる．特に H を X のグラム行列とすれば，それを実部 M と虚部 A に分けた

$$H = M + \sqrt{-1}A$$

を考えれば，M は $\phi(X)$ のグラム行列であることが分かる．

H を半正定値行列であるとしたとき，H, M, A の関係において次の定理が重要である．

Theorem 3.1 (野崎–須田 [4]). $\mathcal{E}_0'$ を M の固有値 0 における固有空間，$\mathcal{E}_0$ を $\sqrt{-1}A$ の固有値 0 における固有空間とする．そのとき，

$$\mathcal{E}_0' \subset \mathcal{E}_0$$

が成立する．

Theorem 3.2 (野崎–須田 [4]).

$$2\mathrm{Rank}(H) \geq \mathrm{Rank}(M)$$

が成立する．

A を有向グラフ G の隣接行列であるとする．G' を隣接行列 $B = A + A^T$ の無向グラフであるとする．ここで，G' は G の辺の向きを無くした無向グラフであることに注意する．$\overline{B}$ を G' の補グラフの隣接行列であるとする．G の埋め込みのグラム行列 H は適当に定数倍することにより，ある実数 a, c を用いて，

$$H(a, c) := \underbrace{-(\xi B + \overline{B}) + aJ}_{G' \text{ の埋め込み}} + c\sqrt{-1}(A - A^T).$$

と表すことが出来る．ここで，$\xi B+\overline{B}$ は，G' の埋め込みの距離行列であることに注意する．Theorem 3.2 より，

$$2\mathrm{Rank}(H(a,c)) \geq \mathrm{Rank}(-(\xi B+\overline{B})+aJ)$$

が成り立つから，H の階数，つまり埋め込みの次元を小さくしようとすれば，G' の埋め込みの次元も小さくする必要がある．ここで，G' の埋め込みとして，極小次元埋め込みを採用することにすると，距離の値である ξ は一意的に定まる．特に，その埋め込みが球面にあることに注意すれば，Theorem 2.1 より，ξ は B の固有値により定められる．実際に極小でない G' の埋め込みが最大 3-code を与え得ないことは，十分に大きな 3-code を得ることで分かる．ここで，ひとつのパラメータ ξ が決まり，残り 2 つのパラメータ a, c を $H(a,c)$ が半正定値行列かつ，階数が出来るだけ小さくなるように設定したい．

G' の極小次元埋め込みは球面でなければならないから，G' は Type (1), (2), (4) のいずれかでなければならないことが分かる．まず，Type (1), (2), (4) の無向グラフ G' を与え，G' の辺集合に向きを与え，有向グラフ G を得ることを考える．辺に向きを与えるとき役に立つのが，Theorem 3.1 である．つまり，G の隣接行列 A は次の等式を満たさなければならない．

$$\mathcal{E}'_0 = \mathrm{Null}(-(\xi B+\overline{B})+aJ) \subset \mathrm{Null}(A-A^T).$$

ここで，$\mathrm{Null}(M)$ は行列 M の固有値 0 に対する固有空間を意味する．$\mathcal{E}'_0$ は Type ごとに計算することができ，次のようになる．

$$\begin{aligned}
&\mathcal{E}'_0 = E_1 && G' \text{ が Type (1) のとき,}\\
&\mathcal{E}'_0 = E_1 \cap j^{\perp} && G' \text{ が Type (2) のとき,}\\
&\mathcal{E}'_0 = E_2 && G' \text{ が Type (4) のとき.}
\end{aligned}$$

$\mathcal{E}'_0$ への直交射影行列 P'_0 と $A-A^T$ が直交することから，$A-A^T$ の列ベクトルの候補を，かなり絞ることが出来る．今回のアルゴリズムでは，このステップでの計算量をかなり削減できた部分が大きかった．また，$\mathcal{E}'_0 \subset j^{\perp}$ であることに注意すれば，

$$\mathrm{Null}(-(\xi B+\overline{B})+aJ) = \mathrm{Null}(-(\xi B+\overline{B}))$$

であることが分かるので，A の候補を a に依らずに決めることが出来る．

実際には，c を決めてから，a を決めることになる．そのときに有用なのが次の補題になる．

Lemma 3.3. H をエルミート行列とし，$P = I - \frac{1}{n}J$ とする．$\tau_{k_1} < \tau_{k_2} < \cdots < \tau_{k_r}$ を H の主固有値 *(main eigenvalue:* 主格が正である固有値*)* とする．H を半正定値行列でないとする．そのとき次が同値である．

(1) ある $a > 0$ が存在して，$H + aJ$ が半正定値行列になる．

(2) $\tau_{k_2} > 0$, $\sum_{i=1}^{r} \beta_{k_i}^2/\tau_{k_i} < 0$, かつ PHP が半正定値行列となる．

さらに *(1)* が成り立つならば，$a \geq -1/(\sum_{i=1}^{r} \beta_{k_i}^2/\tau_{k_i})$ が成り立つ．

$H(a,c)$ が半正定値行列となるためには，Lemma 3.3 の (2) の条件を満たす様な，c がまず取ってこれなければならないことが分かる．もし，(2) を満たす様な c が取れないとすると，$H(a,c)$ の階数を小さくすることは出来ず，G の埋め込み可能な次元は，G' の埋め込み可能な次元と等しくなってしまうことが証明できる．また (2) を満たす様な c が取れるとすると，その中でも $H(a,c)$ の階数を最小にする，c が唯一定まり，G の埋め込み可能な次元は，G' の埋め込み可能な次元より真に小さくなることが分かる．(2) を満たす c が取れる場合，取れない場合，いずれの場合においても，G の埋め込み可能な次元の最小値は与えることが出来ることに注意されたい．c が決まれば，自動的に a が定まることになる．

以上まとめると，非常に大雑把でテクニカルな部分は省略しているが，$\Omega(d)$ 上の最大 3-code を与えるアルゴリズムは次のようになる．目的は，

$$H(a,c) := -(\xi B + \overline{B}) + aJ + c\sqrt{-1}(A - A^T)$$

が半正定値で，階数が最小となるように，ξ, a, c を与えることである．

(1) Types (1), (2), (4) の無向グラフ G' で極小次元が $2d$ 以下であるものを分類する（分類方法は [2] で与えられている）．

(2) G' の極小次元埋め込みを与える距離 ξ を固定する．

(3) $\mathcal{E}_0' \subset \mathrm{Null}(A - A^T)$ となるように，G' の辺に向き付けを行い，有向グラフ G を得る．

(4) Lemma 3.3(2) を満たす c が存在するか確認する．

- 存在するならば，その中でも良い a, c を選ぶことができ $\mathrm{Rep}(G) < \mathrm{Rep}(G')$ となる（Rep は極小埋め込みの次元を意味する）．
- 存在しないならば $\mathrm{Rep}(G) = \mathrm{Rep}(G')$ となる．

実際に，最も時間が必要になってくるのは，ステップ (1) である．それは，次元 $2d$ 以下の 2 距離集合を分類することを意味しているが，$2d \leq 7$ でしか分類に成功していない [2]．それは計算機の性能が追いついていないというだけの理由である．したがって，最大 3-code の分類は $d \leq 3$ でしか今のところ行えない．以下に最大 3-code の元の個数と，その非同型（ユニタリ変換で移りあわない）な集合の個数を表にまとめる．

d	1	2	3
$\lvert X\rvert$	4	8	9
#	1	1	35

最後にそれぞれの構造についての考察を与える．$d = 1$ のとき，最大 3-コードは正方形の頂点集合．$d = 2$ のとき，Y をサイズ 4 の歪アダマール行列（一意的）の極小埋め込みとし，$Y \cup (-Y)$ が最大 3-コード．$d = 1, 2$ のときは Fisher 型の上界を達成している．$d = 3$ のとき，最大 3-コードの 1 つは，サイズ 3 の正則トーナメントを 3 つ disjoint union させたもの，残りの 34 個は 6 次元最大実 2-距離集合の部分構造から得られる．

参考文献

[1] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), no. 3, 363–388.

[2] S.J. Einhorn and I.J. Schoenberg, On euclidean sets having only two distances between points. I. II. *Nederl. Akad. Wetensch. Proc. Ser. A* 69=*Indag. Math.* 28 (1966), 479–488, 489–504.

[3] H. Nozaki and M. Shinohara, A geometrical characterization of strongly regular graphs, *Linear Algebra Appl.* 437 (2012) 2587–2600.

[4] H. Nozaki and S. Suda Complex spherical codes with small degree, preprint.

[5] A. Roy, Minimal Euclidean representation of graphs, *Discrete math.* 310 (2010), 727–733.

[6] A. Roy and S. Suda, Complex spherical designs and codes, to appear in *J. Combin. Des.*

Characterizing optimum designs in terms of finite irreducible reflection groups

東京女子大学・現代教養学部　　平尾　将剛*
名古屋大学大学院・情報科学研究科　　澤　正憲

1　最適計画

実験計画法とは，統計的データ解析を行なう上で実験対象の特徴を的確に捉えた観測値を得るための方法の一つである．特に本稿ではデータ観測を行う実験領域を n 次元単位球 $B^n = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\| \quad 1\}$ に限定し，以下で与える多項式回帰モデルを考えることにする．

$\mathcal{P}_t(B^n)$ を高々t 次の多項式空間を B^n に制限した空間，$N = \dim(\mathcal{P}_t(B^n)) = \binom{n+t}{t}$ とおき，$f_1, f_2, \ldots, f_N$ を $\mathcal{P}_t(B^n)$ のある基底とする．このとき，我々の扱うモデルは

$$Y(\boldsymbol{x}) = \boldsymbol{\theta}\boldsymbol{f}'(\boldsymbol{x}) + \epsilon(\boldsymbol{x}) \tag{1.1}$$

である．ここで $\boldsymbol{f} = (f_1, f_2, \ldots, f_N)$ を基底を並べたベクトル, $\boldsymbol{\theta} = (\theta_1, \theta_2, \ldots, \theta_N)$ を未知パラメータを並べたベクトルとする．さらに $\epsilon(\boldsymbol{x})$ を観測誤差とし，$\boldsymbol{x}, \boldsymbol{y} \in B^n, \boldsymbol{x} \neq \boldsymbol{y}$ に対して $\epsilon(\boldsymbol{x}), \epsilon(\boldsymbol{y})$ は独立な確率変数で期待値 $E[\epsilon(\boldsymbol{x})] = 0$，分散 $V[\epsilon(\boldsymbol{x})] = \sigma^2 > 0$ を満たすとする．

我々の目的は観測地点 $\boldsymbol{x}$ とその応答 $Y(\boldsymbol{x})$ の関係を上手く表すことである．そのために B^n 上のどこでどれだけ観測すれば未知パラメータ $\boldsymbol{\theta}$ をうまく推定できるかを計画する必要がある．ここで数学的には B^n 上の確率測度 ξ を計画 (**design**) と定義する．例えば，離散測度 $\xi(\boldsymbol{x}) = m^{-1}\sum_{i=1}^{m} \delta_{\boldsymbol{x}_i}(\boldsymbol{x})$ は m 個の各観測点 $\boldsymbol{x}_i$ において等数回データをとる計画と解釈することができる[1]．このように我々が B^n 上の確率測度 ξ を計画と呼ぶ場合，ξ の台を観測地点，その台における重み係数を総実験回数に対する各地点での実験回数の割合と見なす．本稿では特に応用上重要な離散測度としての計画に焦点を当てる．

さて，実験の観測結果から (1.1) のパラメータを推定するためには，**情報行列**

$$\mathbf{M}(\xi) = \int_{\boldsymbol{x} \in B^n} \boldsymbol{f}(\boldsymbol{x})'\boldsymbol{f}(\boldsymbol{x}) d\xi(\boldsymbol{x})$$

[1]〒 167-8585 東京都杉並区善福寺 2-6-1 東京女子大学現代教養学部数理科学科
e-mail: hirao@lab.twcu.ac.jp

[1] $\delta_{\boldsymbol{x}_i}$ は点 $\boldsymbol{x}_i$ における Dirac 測度とする．

が重要となる．未知パラメータ $\boldsymbol{\theta}$ の最小二乗推定量 $\hat{\boldsymbol{\theta}}$，及びその分散・共分散行列 $V[\hat{\boldsymbol{\theta}}]$ は[2]，情報行列の逆行列 $\mathbf{M}^{-1}(\xi)$ に比例するからである．$\boldsymbol{\theta}$ が**推定可能**であるためには，$\mathbf{M}(\xi)$ が正定値行列となる ξ に制限する必要がある．また，このとき多項式空間 $\mathcal{P}_t(B^n)$ 上の双一次形式

$$\langle f, g\rangle_\xi = \int_{\boldsymbol{x}\in B^n} f(\boldsymbol{x})g(\boldsymbol{x})d\xi(\boldsymbol{x})$$

は自然に内積を定める．本稿では Neumaier and Seidel (1992) の流儀に従い，このような ξ を ***t* 次の計画**と呼ぶことにする．

先述したように最小二乗推定量の分散・共分散行列 $V[\hat{\boldsymbol{\theta}}]$ は情報行列の逆行列に比例する．このことは計画を適切に選ぶことによって，未知パラメータの推定精度を上げることが可能であることを意味している．そこで我々はそのような意味でのある統計的基準を満たす計画を構成することを考えたい．幾つもの統計的最適性基準があるが，ここでは情報行列の逆行列を最小化する **D 最適性基準**を採用することにする．以降，単に**最適計画** (**optimal design**) と言えば，この D 最適性基準を満たす計画を指すこととする．

最適計画の存在及び構成法に関する先行研究としては，Farrell et al (1967), Ga ke and Heiligers (1995), Pukelsheim (2006) などが顕著な成果として挙げられる．しかしながら，これらのほとんどが 2 次回帰モデルの場合に対応しており, もし何らかの要請から 3 次以上の多項式回帰モデルが必要な場合にはこれらは適応できない．そこで 3 次回帰モデルに対する D 最適計画に関して，Hirao et al (2014) では B 型 Weyl 群を用いた構成法を与えた．本稿では Hirao et al (2014) における構成法の一般化として，その他の有限既約鏡映群 $F_4, H_3, H_4, E_6, E_7, E_8$ の群軌道から得られる最適計画を考察する．

定理 1.1 (主定理)**.** 有限既約鏡映群 $G = F_4, H_3, H_4, E_6, E_7, E_8$ に対して，3 次以上の G 不変最適計画が存在する．特に $G = H_3, E_8$ では，それぞれ 6 次，5 次の G 不変最適計画が存在する．

本稿では 3 節において，ある軌道の取り方に着目した最適計画の最大次数，及び幾つかの例の提示にだけ止める．これらの詳細な分類結果については Sawa and Hirao (2014) を参照されたい．

2 最適計画の構成法

2.1 Euclid 空間上のデザイン

単位球 B^n 上の t 次の最適計画は，最大半径を 1 とするある $(t+1)/2$ 重同心球面上に配置されることが，Karlin and Studden (1966); Neumaier and Seidel (1992) 等によって知られている[3]. このことから t 次の最適計画を構成することは，ある $(t+1)/2$ 重同心球面上の $2t$-デザイン (

[2]簡単のために先にとりあげた $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m\} \subset \mathbb{R}^n$ 上の一様な離散測度 $\xi(\boldsymbol{x}) = m^{-1}\sum_{i=1}^m \delta_{\boldsymbol{x}_i}(\boldsymbol{x})$ を考えると．$\hat{\boldsymbol{\theta}}$ の分散・共分散行列は

$$V(\hat{\boldsymbol{\theta}}) = \frac{\sigma^2}{m}\mathbf{M}^{-1}(\xi).$$

[3]ここで $(t+1)/2$ が半整数の場合，$1/2$ は原点に対応する．

ある $(t+1)/2$ 重同心球面上の積分に対する $2t$ 次の cubature 公式) を構成することと同値であることも分かる．ここで以下に Euclid 空間上のデザインの定義を紹介することにする．

X を $\mathbb{R}^n$ の有限部分集合，w を X 上の正値重み関数とする．X の動径集合を $\{\|\boldsymbol{x}\| \mid \boldsymbol{x} \in X\} = \{r_1, \ldots, r_p\}$, $r_1 > \quad > r_p$, とし，$X_i = X \cap S_{r_i}$, $W_i = \sum_{\boldsymbol{x} \in X_i} w(\boldsymbol{x})$, 及び $S = \cup_{i=1}^{p} S_{r_i}$ とする．

定義 2.1. (X, w) を重み付き有限集合であるとする．任意の $f \in \mathcal{P}_{2t}(\mathbb{R}^n)$ に対して，

$$\sum_{i=1}^{p} \frac{W_i}{|S_{r_i}|} \int_{\boldsymbol{x} \in S_{r_i}} f(\boldsymbol{x}) d\rho_{r_i}(\boldsymbol{x}) = \sum_{\boldsymbol{x} \in X} w(\boldsymbol{x}) f(\boldsymbol{x}) \tag{2.1}$$

が成り立つとき，(X, w) を p 重同心球面 S 上の $2t$-デザインという．

t 次の最適計画を構成したい場合，上述した Karlin and Studden (1966) の結果を用い，情報行列 $\mathbf{M}(\xi)$ が最大となる各同心球面の半径 r_i, 及びその同心球面上の重み W_i を一意に決定することができる[4]．そこで我々の問題は高々$2t$ 次の多項式に対して，(2.1) を常に満たす重み付き有限集合 (X, w) を見つけることである．しかしながら，高々$2t$ 次の多項式全てに対し (2.1) が成り立っているかを判定するのは time-consuming な作業である．そこで計算量を劇的に減らす Sobolev の定理を次に紹介する．

2.2 Sobolev の定理

我々は最適性条件から決定される $(t+1)/2$ 重同心球面上の $2t$-デザインを既約鏡映群の軌道から得られる点配置を基に構成したい．先ず始めに G を n 次直交群 $O(\mathbb{R}^n)$ の部分群とし，一般的な主張を幾つか述べる．このとき，$f \in \mathcal{P}_t(\mathbb{R}^n)$ に対して，$\gamma \in G$ の f への作用を次で定める．

$$(\gamma f)(\boldsymbol{x}) = f(\boldsymbol{x}^{\gamma^{-1}}), \quad \forall \boldsymbol{x} \in \mathbb{R}^n.$$

任意の $\gamma \in G$ に対して $\gamma f = f$ を満たす多項式を G **不変** (G-invariant) であるという．$\mathcal{P}_t(\mathbb{R}^n)$, $\mathrm{Harm}_t(\mathbb{R}^n)$ の G 不変多項式からなる部分空間をそれぞれ $\mathcal{P}_t(\mathbb{R}^n)^G, \mathrm{Harm}_t(\mathbb{R}^n)^G$ と表すとする．

多重同心球面上のデザイン (X, w) が条件 (i), (ii) を満たすとき，G 不変と呼ぶことにする．

(i) X は G-軌道 $\boldsymbol{x}_1^G, \boldsymbol{x}_2^G, \ldots, \boldsymbol{x}_M^G$ の和集合で表される．

(ii) 各軌道 $\boldsymbol{x}_i^G$ 及び $\boldsymbol{y}, \boldsymbol{y}' \in \boldsymbol{x}_i^G$ に対して， $w(\boldsymbol{y}) = w(\boldsymbol{y}')$.

次の Sobolev の定理，及び，多重同心球面上のデザインに対して拡張 (Nozaki and Sawa, 2012) が成り立つ．

定理 2.2 (Sobolev (1962))**.** G を $O(\mathbb{R}^n)$ の部分群とする．このとき，次は同値である．

(i) 球面上の t-デザイン (X, w) が G 不変である．

[4] 3 節において具体例を幾つか提示する際に，必要な最適値 r_i, W_i についてはのみ紹介する．具体的な最適値 r_i, W_i の満たす関係式については，例えば，Neumaier and Seidel (1992); Hirao et al (2014) を参照して欲しい．

(ii) 任意の $1 \quad l \quad t$, $\phi \in \mathrm{Harm}_l(\mathbb{R}^n)^G$ に対して, $\sum_{\boldsymbol{x}\in X} w(\boldsymbol{x})\phi(\boldsymbol{x}) = 0$.

定理 2.3 (Nozaki and Sawa (2012)). G を $O(\mathbb{R}^n)$ の部分群, $X = \cup_{k=1}^{M} r_k \boldsymbol{x}_k^G$ とする. ただし, $\boldsymbol{x}_k \in S_1$, $r_k > 0$ とする. このとき次は同値である.

(i) (X, w) は Euclid 空間上の G 不変 t-デザインである.

(ii) 任意の $1 \quad l \quad t, 0 \quad j \quad \lfloor \frac{t-l}{2} \rfloor$, $\varphi \in \mathrm{Harm}_l(\mathbb{R}^n)^G$ に対して, $\sum_{\boldsymbol{x}\in X} w(\boldsymbol{x})\|\boldsymbol{x}\|^{2j}\varphi(\boldsymbol{x}) = 0$.

これらの結果から $2t$-デザインを構成する際には, 多項式全てではなく, その G 不変調和多項式に関連した一部のみを調べれば良く, これは実際の計算の上で非常に有用である.

3 構成例

この節では G を既約鏡映群 $F_4, H_3, H_4, E_6, E_7, E_8$ とする. 我々は t 次の最適計画 (最適性条件から得られるある $(t+1)/2$ 同心球面上の $2t$-デザイン) を群軌道を用いて構成するために軌道の始点を決めなければならないが, ここでは既存の B 型 Weyl 群を用いた構成法 (Hirao et al, 2014) を一般化し, **corner vector** を群軌道の始点とすることにする.

ここで $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$ が G の corner vector であるとは, G の基本ルート $\alpha_1, \alpha_2, \ldots, \alpha_n$ に対して, $\|\boldsymbol{v}_i\| = 1$, 及び

$$\boldsymbol{v}_i \perp \alpha_j \Longleftrightarrow i \neq j,$$

を満たすベクトルであるとする[5].

corner vector の取り方について重複がない場合における G 不変最適計画の最大次数は以下のように決定される.

定理 3.1. *Corner vector* の取り方について重複がない場合における単位球上の G 不変最適計画に対する最大次数は以下の通りである.

(i) $G = F_4, H_3, E_6, E_7$ の場合 : 最大次数は 3;

(ii) $G = E_8$ の場合 : 最大次数は 5;

(iii) $G = H_4$ の場合 : 最大次数は 6.

以下に定理 3.1 で挙げた最大次数を達成する G 不変最適計画の例をそれぞれ幾つか紹介する. ここで $R_i = r_i^2$ とし, J_i は $X \cap S_{r_i}$ に対応する corner vector を表す index set, w_i は corner vector v_i に対応した重みとする.

F_4 不変最適計画. (2.1) に対応した最適値は, $W_1 = 0.850308$, $W_2 = 0.149692$, $R_1 = 1$, $R_2 = 0.313408$. このとき,

[5] 各既約鏡映群 G に対する基本ルート, 及び corner vector 等の詳細については, Nozaki and Sawa (2014); Sawa and Hirao (2014) を参照されたい.

1. $J_1 = \{1,2\},\ J_2 = \{3,4\}$:

$$w_1 = 0.0354295 \quad 4w_2, \quad w_3 = \quad 0.321934 + 32.484w_2,$$
$$w_4 = 1.29397 \quad 129.936w_2, \quad 0.00226244 < w_2 \quad 0.00885737.$$

2. $J_1 = \{2,4\},\ J_2 = \{1,3\}$:

$$w_1 = 0.00623717 \quad 4w_3, \quad w_2 = 0.00792843 + 0.0307844w_3,$$
$$w_4 = 0.00371576 \quad 0.123138w_3, \quad 0 \quad w_3 \quad 0.00155929.$$

3. $J_1 = \{2,3\},\ J_2 = \{1,4\}$:

$$w_1 = \quad (\quad 0.00623717 + w_4), \quad w_2 = 0.069265(0.0608198 + w_4),$$
$$w_3 = \quad 0.069265(\quad 0.0670569 + w_4), \quad 0 \quad w_4 \quad 0.00623717.$$

H_3 **不変最適計画.** (2.1) に対応した最適値は，$W_1 = 0.791993,\ W_2 = 0.208007,\ R_1 = 1,\ R_2 = 0.296255.$ このとき，

1. $J_1 = \{1,2\},\ J_2 = \{3\}$:

$$w_1 = 0.0159049, \quad w_2 = 0.0200378, \quad w_3 = 0.0104003.$$

2. $J_1 = \{1,3\},\ J_2 = \{2\}$:

$$w_1 = 0.0236618, \quad w_2 = 0.00693356, \quad w_3 = 0.0254026.$$

H_4 **不変最適計画.** (2.1) に対応した最適値は，$W_1 = 0.644994,\ W_2 = 0.269306,\ W_3 = 0.0809367,\ W_4 = 0.00476298,\ R_1 = 1,\ R_2 = 0.693266,\ R3 = 0.290845,\ R_4 = 0.$ このとき，

1. $J_1 = \{1,2\},\ J_2 = \{4\},\ J_3 = \{3\}$:

$$w_1 = 0.000645503,\ w_2 = 0.000788242,\ w_3 = 0.0000674472,\ w_4 = 0.000448843.$$

2. $J_1 = \{1,3\},\ J_2 = \{4\},\ J_3 = \{2\}$:

$$w_1 = 0.00119579,\ w_2 = 0.000112412\ w_3 = 0.000417916,\ w_4 = 0.000448843.$$

3. $J_1 = \{1,3\},\ J_2 = \{2\},\ J_3 = \{4\}$:

$$w_1 = 0.00115801,\ w_2 = 0.000374036,\ w_3 = 0.000421694,\ w_4 = 0.000134894.$$

E_6 **不変最適計画.** (2.1) に対応した最適値は，$W_1 = 0.912086,\ W_2 = 0.087914,\ R_1 = 1,\ R_2 = 0.331571.$ このとき，

1. $J_1 = \{1, 4, 6\},\ J_2 = \{2, 3, 5\}$:

$$\begin{aligned} w_1 &= \quad 0.0000634021 \quad 0.118238w_5 + 3.00413w_6, \\ w_2 &= 0.0674463 + 2.00468w_5 \quad 40.5069w_6, \\ w_3 &= \quad 0.0201118 \quad 0.638903w_5 + 12.1521w_6, \\ w_4 &= 0.00423055 + 0.0147797w_5 \quad 0.708850w_6. \end{aligned}$$

ここで (i) $0 \quad w_5 < 0.00325607,\ 0.00165501 + 0.0525757w_5 \quad w_6 \quad 0.00166506 + 0.0494898w_5$, もしくは (ii) $w_5 = 0.00325607, w_6 = 0.0018262$.

2. $J_1 = \{2, 5, 6\},\ J_2 = \{1, 3, 4\}$:

$$\begin{aligned} w_1 &= \quad 0.033644 + 0.498833w_4 + 20.2062w_6, \\ w_2 &= 0.003733 + 0.007373w_4 \quad 0.410208w_6, \\ w_3 &= 0.001384 \quad 0.318706w_4 \quad 0.757732w_6, \\ w_5 &= 0.003915 \quad 0.058981w_4 + 0.614996w_6, \end{aligned}$$

ここで (i) $0 \quad w_4 < 0.000407,\ 0.001665 \quad 0.024687w_4 \quad w_6 \quad 0.001826 \quad 0.420606w_4$, もしくは (ii) $w_4 = 0.000407, w_6 = 0.001655$.

3. $J_1 = \{2, 4, 5\},\ J_2 = \{1, 3, 6\}$:

$$\begin{aligned} w_1 &= 0.0612494 + 0.969697w_6 \quad 24.2407w_5, \\ w_2 &= 0.000913902 \quad 0.0189573w_6 + 0.720215w_5, \\ w_3 &= \quad 0.00217475 \quad 0.136364w_6 + 0.909027w_5, \\ w_4 &= 0.00330872 + 0.0189573w_6 \quad 0.845215w_5. \end{aligned}$$

ここで (i) $0 \quad w_6 < 0.00122103,\ 0.00239239 + 0.15001w_6 \quad w_5 \quad 0.00252672 + 0.0400028w_6$. もしくは (ii) $w_6 = 0.00122103, w_5 = 0.00257556$.

E_7 不変最適計画. (2.1) に対応した最適値は, $W_1 = 0.929562,\ W_2 = 0.070438,\ R_1 = 1,\ R_2 = 0.336856$. このとき,

1. $J_1 = \{4, 5, 6, 7\},\ J_2 = \{1, 2, 3\}$:

$$\begin{aligned} w_1 &= 0.000559032 \quad 16w_2 \quad 80w_3, \\ w_4 &= 0.0001923 + 0.0261807w_2 + 0.163629w_3 + 0.071347w_6 \quad 0.22465w_7, \\ w_5 &= 0.000203981 \quad 0.13963w_2 \quad 0.872689w_3 \quad 0.454592w_6 + 0.436226w_7. \end{aligned}$$

ここで w_2, w_3, w_6, w_7 は $0 \quad w_1, \ldots, w_7 < 1$ を満たす正の実数.

2. $J_1 = \{3, 5, 6, 7\},\ J_2 = \{1, 2, 4\}$:

$$\begin{aligned} w_1 &= 0.000559032 \quad 16w_2 \quad 32w_4, \\ w_3 &= 0.0000561515 + 0.00764476w_2 + 0.0232401w_4 + 0.0208333w_6 \quad 0.0655977w_7, \\ w_5 &= 0.000480892 \quad 0.10193w_2 \quad 0.309867w_4 \quad 0.351852w_6 + 0.112731w_7. \end{aligned}$$

ここで w_2, w_4, w_6, w_7 は $0 \quad w_1, \ldots, w_7 < 1$ を満たす正の実数.

3. $J_1 = \{3, 4, 6, 7\},\ J_2 = \{1, 2, 5\}$:

$$w_1 = 0.000559032 \quad 16w_2 \quad 6w_5,$$
$$w_3 = \quad 0.0000413628 + 0.0283139w_2 + 0.0238899w_5 + 0.0921811w_6 \quad 0.088457w_7,$$
$$w_4 = 0.000333953 \quad 0.0707848w_2 \quad 0.0597247w_5 \quad 0.244342w_6 + 0.0782853w_7.$$

ここで w_2, w_5, w_6, w_7 は $0 \quad w_1, \ldots, w_7 < 1$ を満たす正の実数.

E_8 不変最適計画. (2.1) に対応した最適値は, $W_1 = 0.834316,\ W_2 = 0.153639,\ W_3 = 0.0120447,\ R_1 = 1,\ R_2 = 0.620885,\ R_3 = 0.180194$. このとき,

1. $J_1 = \{1, 7\},\ J_2 = \{2, 6\},\ J_3 = \{3\}$:

$$w_1 = 0.000340924, \quad w_2 = 1.02686 \quad 10^{-6}, \quad w_3 = 1.72448 \quad 10^{-8},$$
$$w_6 = 9.15974 \quad 10^{-6}, \quad w_7 = 0.000511382.$$

2. $J_1 = \{1, 6\},\ J_2 = \{2, 7\},\ J_3 = \{5\}$:

$$w_1 = 0.000159098, \quad w_2 = 1.74907 \quad 10^{-6}, \quad w_5 = 1.37958 \quad 10^{-7},$$
$$w_6 = 0.0000767076, \quad w_7 = 0.0000484746.$$

3. $J_1 = \{1, 7\},\ J_2 = \{2, 6\},\ J_3 = \{4\}$:

$$w_1 = 0.000340923, \quad w_2 = 1.02703 \quad 10^{-6}, \quad w_4 = 3.44896 \quad 10^{-8},$$
$$w_6 = 9.15794 \quad 10^{-6}, \quad w_7 = 0.000511382.$$

4 補遺

1. Hirao and Sawa (2014) において A 型, 及び D 型 Weyl 群を用いて構成される最適計画についても分類済である. 特に A 型 Weyl 群を用いて構成される最適計画はどのように corner vector を選んでも最大次数は 2 にしかならない. しかしながら, この場合, 構成される最適計画は重み係数が有理数となる **exact design** となっている. これは応用上も非常に有用である.

2. 本稿では最適性基準として D 最適性基準を採用したが, より一般的な Φ_p 最適性基準 (D 最適性基準は Φ_0 最適性基準と同値) に対しても適用可能である. Hirao and Sawa (2014) においては, この他にも幾つかの最適性基準に対して最適計画が構成可能であることを注意している.

3. より高次の最適計画を構成するためには, 群の選び方, 及び, 軌道の始点の選び方等, まだ改善されるべき点が多い. 何らかの統計的意味付けをした上でこれらの分類を行う必要がある.

参考文献

Farrell RH, Kiefer J, Walbran A (1967) Optimum multivariate designs. In: Proceedings of the Berkeley Symposium, vol 1, pp 113–138

Ga ke N, Heiligers B (1995) Optimal and robust invariant designs for cubic multiple regression. Metrika 42:29–48

Hirao M, Sawa M (2014) Characterizing optimum designs in terms of finite irreducible reflection groups. II. In preparation

Hirao M, Sawa M, Jimbo M (2014) Constructions of Φ_p-optimal rotatable designs on the ball. To appear in Sankhyâ Series A

Karlin S, Studden WJ (1966) Tchebyche systems: With applications in analysis and statistics. John Wiley & Sons, New York-London-Sydney

Neumaier A, Seidel JJ (1992) Measures of strength $2e$ and optimal designs of degree e. Sankhyâ Series A 54:299–309

Nozaki H, Sawa M (2012) Note on cubature formulae and designs obtained from group orbits. Canadian Journal of Mathematics 64:1359–1377

Nozaki H, Sawa M (2014) Remarks on Hilbert identities, isometric embedding, and invariant cubature. To appear in St Petersburg Mathematical Journal

Pukelsheim F (2006) Optimal design of experiments. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA

Sawa M, Hirao M (2014) Characterizing optimum designs in terms of finite irreducible reflection groups. I. In preparation

Sobolev SL (1962) Cubature formulas on the sphere which are invariant under transformations of finite rotation groups. Doklady Akademii Nauk SSSR 146:310–313

Baer subplaneによる直交配列の構成

山田 紘頌 [1] and 宮本 暢子 [2]

[1] 東京理科大学 理工学研究科
[2] 東京理科大学 理工学部

1 はじめに

直交配列 $\mathrm{OA}_\lambda(N,k,s,t)$ とは, $N\times k$ 行列であって, その成分が s 個の要素からなり, 行列のどの t 列を取り出しても, その行に全ての t-順列がちょうど一定数 (λ 回) ずつ現れるもののことをいいます. ここで, t を強さ, N を行数, k を列数, s を水準数, λ をインデックスといいます. 直交配列はデザイン理論の基礎, 応用両面において非常に重要な組合せ構造であるために, その存在条件の解明や構成法の研究は組合せ論における重要な問題となっています. 特に, 多様な水準数に対してより大きい強さを持ち, より小さい行数, より大きい列数を持つ直交配列の構成法を得ることが求められています. しかし, 与えられた強さ t, 列数 k, 水準数 s に対して, いくらでも行数 N を小さくできるわけではなく, 次の Rao の限界式を満たさなければならないことがわかっています.

定理 1.1 (Rao の限界式) 強さ t, 制約数 k, 位数 s, インデックス λ の直交配列 $\mathrm{OA}_\lambda(t,k,s)$ について, その行数 N の下限が以下で与えられる.

$$N=\lambda s^t \geq 1+\begin{cases} \sum_{i=1}^{\frac{t}{2}}\binom{k}{i}(s-1)^i & (t:even)\\ \sum_{i=1}^{\frac{t}{2}}\binom{k}{i}(s-1)^i+\frac{k-1}{(t-1)/2}(s-1)^{\frac{t+1}{2}} & (t:odd)\end{cases}$$

直交配列の構成問題は, 水準数が素数ベキの場合についてはよく研究がなされ多くの構成法が知られているのですが, 水準数が素数ベキでない場合の状況についてはあまりわかっていません. (筆者の知る限り, Bush [2], Fuji-Hara and Kamimura [4], および Colbourn et al.[3] などによる結果があります.)

定理 1.2 (Bush [2]) 直交配列 $\mathrm{OA}_{\lambda_1}(N_1,k_1,s_1,t)$ および $\mathrm{OA}_{\lambda_2}(N_2,k_2,s_2,t)$ が存在すれば, 直交配列 $\mathrm{OA}_{\lambda_1\lambda_2}(N_1N_2,\min(k_1,k_2),s_1s_2,t)$ が存在する.

特に Bush による方法は強力で, ほとんどの水準数に対して直交配列を得ることが出来ます. しかしながら, この定理の主張を見ればわかるように, 水準数を非素数ベキに出来る代償として, 行数は増加し (N_1N_2), 列数は小さく ($\min(k_1,k_2)$) なってしまいます. この Bush の構成法のように, 直交配列を構成するために別の直交配列の存在を仮定するような構成法を再帰的構成法といいます. Fuji-Hara and Kamimura [4] は, Baer subplane とよばれる有限幾何上の構造を用いて, 直接的に非素数ベキ水準数を持つ直交配列を構成する方法を提案しました.

本稿では, ある射影変換群の部分群の作用を用いて, Fuji-Hara らの構成した直交配列よりも行数の小さい直交配列が得られたことを報告します. さらに, この直交配列には, Bush の方法では構成できないものが含まれることを計算機によって確かめました.

2 Fuji-Hara and Kamimura による直交配列の構成

ここでは, Fuji-Hara and Kamimura[4] の構成法を紹介します.

定理 2.1 (Fuji-Hara and Kamimura [4, Theorem 3.3]) 任意の素数べキ q に対して, 次のパラメタの (分割可能[1]) 巡回的[2] 直交配列が存在する.

$$\mathrm{OA}_{q^2(q^2-1)}\Big(q^4(q-1)^3(q+1)/3, q^2+q+1, q^2-q, 2\Big). \tag{2.1}$$

Fuji-Hara らの方法は, transversal design と呼ばれる直交配列と完全に等価な組合せ構造 (group divisible design の一種) を構成するものです. transversal design は次のように定義されます.

定義 2.2 (transversal design) 点集合 $\mathcal{P}$ の分割 $\mathcal{C}$ を伴う結合構造を $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ とする. $\mathcal{B}$ は点集合 $\mathcal{P}$ の k-部分集合 (これをブロックと呼ぶ) N 個からなり, この k をブロックサイズ, N をブロック数という. $\mathcal{C}$ は点集合 $\mathcal{P}$ の s-部分集合への分割であり, $\mathcal{C}$ の要素のことをクラスという. この結合構造 $\mathcal{D}$ が次の 2 つの性質を満たすとき, $\mathcal{D}$ を強さ t の transversal design という.

1. 任意の類 $C \in \mathcal{C}$ と任意のブロック $B \in \mathcal{B}$ の共有点がちょうど 1 点である.
2. 異なる類から取り出した t 点を含むブロックの数が一定数 λ である. この λ を会合数と呼ぶ.

この transversal design を t-$(k, s; \lambda)$-TD とかく. (特に, 本稿では $t = 2$ の場合のみを扱う.) $t = 2$ の場合 $(k, s; \lambda)$-TD とかくことにする.

直交配列と transversal design のパラメータの対応は表 1 の通りです.

表 1: 直交配列と transversal design のパラメタの対応

直交配列	transversal design
実験回数 (行数, runs) N	ブロックの数 N
制約数 (列数, constraint) k	ブロックサイズ = クラスの数 k
水準数 (order, number of symbols) s	クラスサイズ s
インデックス (index) λ	会合数 (covalency) λ

Fuji-Hara らは Baer subplane を用いて, 次のように transversal design を構成しました. ここで, Baer subplane とは, $\mathrm{PG}(2, q^2)$ 上の, 位数 q の射影平面と同型な部分結合構造です.

定理 2.3 (Fuji-Hara and Kamimura [4, Theorem 3.3]) $\mathcal{P} = \mathrm{PG}(2, q^2)$ 上の Baer subplane を $\mathcal{P}_0 = (\mathcal{P}_0, \mathcal{L}_0)$ とする. このとき,

$$\begin{aligned}
&\mathcal{V} := \mathcal{P} \backslash \mathcal{P}_0, \\
&\mathcal{B} := (\mathcal{P}_0 \text{と交わらない全ての Baer subplane の集合}), \\
&\mathcal{C} := \{(l \backslash \mathcal{P}_0) \mid l \in \mathcal{L}_0\},
\end{aligned}$$

と定めると (図 1), 結合構造 $(\mathcal{V}, \mathcal{B}, \mathcal{C})$ は $(q^2+q+1, q^2-q; q^2(q^2-1))$-TD であり, つまり式 (2.1) の直交配列と等価な構造である.

[1] この直交配列が分割可能であることは Fuji-Hara らによって予想されていましたが, Ueberberg [6] の成果の帰結として, 今回予想の正しさが証明されました. このことから, Fuji-Hara らの直交配列は 1 列増やすことが可能です.(Hedayat et al.[5, Corollary 6.18] 参照)

[2] 直交配列が巡回的であるとは, ある行の任意の巡回シフトがまた直交配列の行になっているものをいいます.

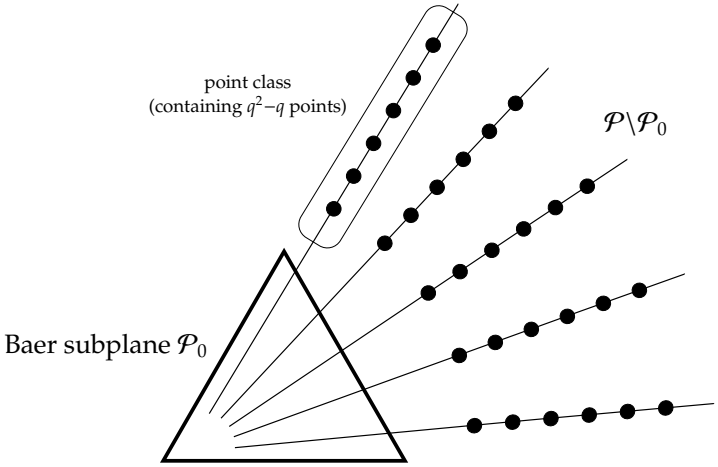

図 1: Baer subplane から構成される transversal design の点と類

Baer subplane は様々な組合せ論的性質を持つことが知られていますが, 特に次の Bose の結果は重要です.

定理 2.4 (Bose et al. [1, Theorem 2.1]) PG$(2,q^2)$ 上の 2 つの Baer subplane $\mathcal{P}_i,\mathcal{P}_j$ の共有点の個数と共有する直線の個数は一致する. つまり,

$$\forall i,j,\ |\mathcal{P}_i\cap\mathcal{P}_j| = |\mathcal{L}_i\cap\mathcal{L}_j|$$

(2 つの Baer subplane $\mathcal{P}_i,\mathcal{P}_j$ が直線 l を共有するとは, $l\in\mathcal{L}_i\cap\mathcal{L}_j$ すなわち $|\mathcal{P}_1\cap l| = |\mathcal{P}_2\cap l| = q+1$ であるときをいう. 必ずしも $\mathcal{P}_1\cap l = \mathcal{P}_2\cap l$ である必要はない.)

系 2.5 $\mathcal{P}_0,\mathcal{P}_1$ を, $\mathcal{P}=$ PG$(2,q^2)$ 上の互いに交わらない (点を共有しない)Baer subplane とする. このとき, $\mathcal{P}_0$ の任意の直線と $\mathcal{P}_1$ の交わりはちょうど 1 点である.

系 2.5 より, ある Baer subplane $\mathcal{P}_0$ を固定し, その直線 (上の点) をクラスと定めておけば, $\mathcal{P}_0$ と交わらない全ての Baer subplane は transversal design の 1 番目の条件を満たすことがわかります. 後は 2 番目の条件を満たすように Baer subplane を選ぶことが出来れば, クラスサイズ q^2-q の transversal design すなわち水準数 q^2-q の直交配列を構成することが出来ます.

3 主結果, 非素数べキ水準数直交配列の構成

点集合とクラスの設定は Fuji-Hara らの方法と同じで, 選択するブロックを少なくした transversal design を構成できれば, 列数, 水準数などは変えずに, より小さい行数の直交配列を構成できることになります. 今回, 射影変換群のある部分群による Baer subplane の軌道を用いて, そのような transversal design が得られることを示しました.

定理 3.1 (Yamada and Miyamoto, 2014) 任意の素数べキ q に対して, 次のパラメタの巡回的直交配列が存在する.

$$\mathrm{OA}_{q(q+1)}\Big(q^3(q-1)^2(q+1), q^2+q+1, q^2-q, 2\Big). \tag{3.1}$$

さらに, $q \bmod 3 \equiv 2$ のとき, 次のパラメタの巡回的直交配列が存在する.

$$\mathrm{OA}_{q(q+1)/3}\Big(q^3(q-1)^2(q+1)/3, q^2+q+1, q^2-q, 2\Big). \tag{3.2}$$

定理 3.2 (Yamada and Miyamoto, 2014) $\mathrm{PG}(2,q^2) = (\mathcal{P},\mathcal{L})$ 上の 2 つの交わらない Baer subplane を $\mathcal{P}_0 = (\mathcal{P}_0,\mathcal{L}_0), \mathcal{P}_1 = (\mathcal{P}_1,\mathcal{L}_1)$ とし, $\mathcal{P}_0$ 上の 1 点を $O \in \mathcal{P}_0$ とする. さらに, 射影変換群の部分群 Γ を次のように定める.

$$\Gamma = \{g \in \mathrm{PGL}(3,q^2) \mid g(\mathcal{P}_0) = \mathcal{P}_0, g(O) = O\}$$

結合構造 $\mathcal{D} = (\mathcal{V},\mathcal{B},\mathcal{I})$ を次のように定めるとき, これは強さ 2 の transversal deisgn である.

$$\begin{aligned}
\mathcal{V} &:= \mathcal{P}\backslash\mathcal{P}_0, \\
\mathcal{B} &:= \{g(\mathcal{P}_1) \mid g \in \Gamma\}, \\
\mathcal{C} &:= \{(l\backslash\mathcal{P}_0) \mid l \in \mathcal{L}_0\}.
\end{aligned}$$

条件の詳細は省略しますが, ブロック数 $|\mathcal{B}|$ は初期ブロック $\mathcal{P}_1$ の選び方によって 2 通りの値をとり, それぞれ直交配列 (3.1), (3.2) に対応します. Fuji-Hara らの直交配列とあわせて, 定理 3.1 の具体的なパラメタを表 2 および 3 に示します. ($*$ のついた値は直交配列 (3.2) のものです.)

表 2: 先行研究, Theorem 3.2 の場合の直交配列の各パラメタ

構成法	N	k	s	λ
[4, Theorem 3.3]	$q^4(q-1)^3(q+1)/3$	q^2+q+1	$q(q-1)$	$q^2(q^2-1)/3$
Theorem 3.2	$q^3(q-1)^2(q+1)$	q^2+q+1	$q(q-1)$	$q(q+1)$
Theorem 3.2*	$q^3(q-1)^2(q+1)/3$	q^2+q+1	$q(q-1)$	$q(q+1)/3$

表 3: 先行研究, Theorem 3.2 の場合の直交配列の各パラメタの具体例

q	N, [4]	N, Th.3.2	λ, [4]	λ, Th.3.2	k	s
2	16	8	2	1	7	2
3	864	432	24	12	13	6
4	11520	2880	80	20	21	12
5	80000	*4000	200	*10	31	20
7	1382976	98784	784	56	57	42
8	4214784	*75264	1344	*24	73	56

特に, 直交配列 (3.2) の系列には Bush [2] の方法 (定理 1.2) では構成できないものが含まれることは簡単に確認できます. 具体的には, 直交配列 $\mathrm{OA}_{\lambda_1}(N_1,k_1,s_1,t)$ および $\mathrm{OA}_{\lambda_2}(N_2,k_2,s_2,t)$ を Bush の方法で合成して直交配列 $\mathrm{OA}_{\lambda_1\lambda_2}(N_1N_2, \min(k_1,k_2), s_1s_2, t)$ が構成できたとすると,

1. $N_1N_2 = N$, $s_1s_2 = s$,

2. $s_1^2 \mid N_1$, $s_2^2 \mid N_2$,

3. $N_1 > k$, $N_2 > k$,

の 3 つの条件が満たされる必要がありますが, 今回構成した直交配列 (3.2) に対してこれらの条件を満たす直交配列の組は Rao の限界式の観点から存在しない, ということを確かめることが出来ます。実際に, $q < 10^7$ までの全ての直交配列 (3.2) が Bush の方法では構成できないことを計算機によって確認しました.

4 今後の課題と展望

今回構成した直交配列は, Rao の限界式の観点からはあまり良い直交配列であるとは言えません. 例えば $q = 3$ の場合には定理 3.2 は 432 行の直交配列を与えますが, Rao の限界式の観点からは, (同じ水準数かつ同じ列数なら)72 行の直交配列があり得ます.

しかし, 素数ベキ水準数の場合の直交配列で Rao の限界式を達成するものは筆者の知る限り存在しませんので, 非素数ベキ水準数直交配列に対しては Rao の限界式よりも適切な限界式があるのではないかと思われます[3]. このような非素数ベキ水準数直交配列のための限界式の研究を含め, 今回構成した直交配列よりもより行数の小さい直交配列が存在するかどうかを検証したいと思います.

2014 年 3 月現在の計算機実験結果では, 定理 3.2 より小さい直交配列は見つかっていません. しかし, $q = 3$ の場合に, 108 行の行列でどの 2 列を見ても全ての順序対が 2 回, 3 回ないし 4 回出現する行列 (i 回出現する順序対の数は, 選んだ 2 列によらず一定 ($i = 2, 3, 4$)) が見つかっています.

また, 本稿で詳しくは扱いませんでしたが, 定理 3.2 の証明は Ueberberg[6, 7, 8] の結果を用いて組合せ論的な手法で行いました. 可能ならば, 射影変換群のみに着目して, 代数的な別証明を与えたいと考えています.

謝辞

今回このような伝統ある研究集会にて発表の機会を下さいました主催者ならびに実行委員会の先生方に, 厚く御礼申し上げます.

参考文献

[1] R.C. Bose, J.W. Freeman, and D.G. Glynn. *On the intersection of two Baer subplanes in a finite projective plane.* Utilitas Math, 1980.

[2] K.A. Bush. *A Generalization of a Theorem due to MacNeish.* The Annals of Mathematical Statistics, 23(2): pp.293-295, June 1952.

[3] C.J. Colbourn, D.L. Kreher, J.P. McSorley, and D.R. Stinson. *Orthogonal arrays of strength three from regular 3-wise balanced designs.* Journal of Statistical Planning and Inference, 100(2): pp.191-195, February 2002.

[3] $\lambda = 1$ の場合に対しては, Hedayat et al.[5, Research Problem 3.10] においても非素数ベキ水準数直交配列の構成法と限界式について, 研究課題として言及されています.

[4] R. Fuji-Hara and S. Kamimura. *Orthogonal arrays from Baer subplanes.* Utilitas Math,43: pp.65-70, 1993.

[5] A.S. Hedayat, N.J.A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications (Springer Series in Statistics).* Springer, 1999 edition, 1999.

[6] J. Ueberber. *Projective planes and dihedral groups.* Discrete Mathematics, 174(1-3): pp.337-345, September 1997.

[7] J. Ueberberg. *Frobenius collineations in finite projective planes.* Bulletin of the Belgian Mathematical Society Simon, 3(March 1996): pp.473-492, 1997.

[8] J. Ueberberg. *A Class of Partial Linear Spaces Related to* $\mathrm{PGL}_3(q^2)$. European Journal of Combinatorics, 18(1): pp.103-115, 1997.

Weighing matirxに関連したアソシエーションスキームについて

須田庄 (愛知教育大学) 野崎寛 (愛知教育大学)

1 序

Hadamard 行列の一般化である Weighing matrix について, 本報告集では Hadamard 行列とアソシエーションスキームの関係性を weighing 行列へ拡張することを目標とする . また MUB の一般化として, mutually unbiased weighing matrices についても同様のことを考察する. 本研究は愛知教育大の野崎寛氏との共同研究に基づく. 本文で省略された証明は [3] を参照ください。

2 Weighing matrix

W を成分を $0, \pm 1$ とする d 次の正方行列とする. W が重さ k の weighing matrix であるとは, $WW^T = kI$ を満たすこととする. ここで, I は単位行列とする. 定義から明らかなように $k = d$ となる weighing matrix は位数 d の Hadamard matrix に一致する.

まず, Hadamard matrix とアソシエーションスキームの関連性について述べる. 位数 d の Hadamard matrix H から d 次元の実球面 S^{d-1} 上の有限集合 X を以下のようにして作る. $X_0 = \{\pm e_1, \ldots, \pm e_d\}$, $X_1 = \{\pm \frac{1}{\sqrt{d}} h_1, \ldots, \pm \frac{1}{\sqrt{d}} h_d\}$ (e_i は第 i 成分が 1 の単位ベクトル, h_i は H の第 i 行とする) とし, $X = X_0 \cup X_1$ とおく. このとき X の内積集合 $A(X) := \{\langle x, y\rangle \mid x, y \in X, x \neq y\}$ は $A(X) = \{\pm \frac{1}{\sqrt{d}}, 0, -1\}$ で与えられる. $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = \frac{1}{\sqrt{d}}, \alpha_3 = \frac{-1}{\sqrt{d}}, \alpha_4 = 0$ とおく. このとき,

$$R_i = \{(x, y) \in X \times X \mid \langle x, y\rangle = \alpha_i\} \qquad (i = 0, 1, \ldots, 4)$$

とおくことで $(X, \{R_i\}_{i=0}^4)$ はアソシエーションスキームになる.

しかし Weighing matrix に対して同様の方法ではアソシエーションスキームにはならないことが容易にわかる. これは, Hadamard matrix に対しては X_0 と X_1 の間に 0 の二点が現れないのに対し, weighing matrix に対してはそうではないことに由来する. 従って, 重さ k の weighing matrix W に対して, $X_1 = \{\pm \frac{1}{\sqrt{k}} w_1, \ldots, \pm \frac{1}{\sqrt{k}} w_d\}$ (w_i は W の第 i 行) とし, $X = X_0 \cup X_1$ に対し $A(X) = \{\pm \frac{1}{\sqrt{k}}, 0, -1\}$ であるので. $\beta_0 = 1, \beta_1 = -1, \beta_2 = \frac{1}{\sqrt{k}}, \beta_3 =$

$\frac{-1}{\sqrt{k}}, \beta_4 = 0$ とおく. このとき,

$$R_i = \{(x,y) \in X \times X \mid \langle x,y \rangle = \beta_i\} \qquad (i = 0,1,2,3)$$
$$R_4 = \{(x,y) \in X \times X : \langle x,y \rangle = 0, x \in X_i, y \in X_j \text{ for } i \neq j\},$$
$$R_5 = \{(x,y) \in X \times X : \langle x,y \rangle = 0, x,y \in X_i \text{ for } i = 1,2\}.$$

のように, 内積 0 から定まる二項関係を分割することが自然である. しかし, このような二項関係を考えても次のような W は X 上にアソシエーションスキームを定めない :

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & -1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 \end{pmatrix}.$$

ではどのような W に対してはアソシエーションスキームを定めるかについては次のような特徴づけが得られた. 定理の証明には球面上のデザインの理論が用いられる.

Theorem 2.1. *W を重さ k で d 次の weighing matrix (ただし, $k < d$) とし, X, R_i は上記のように定義する. このとき次の二条件は同値である :*

(i) $(X, \{R_i\}_{i=0}^5)$ はアソシエーションスキームである,

(ii) W は *balanced generalized weighing matrix* である.

ここで位数 d, 重さ k の weighing matrix W が balanced generalized weighing matrix であるとは次の条件をみたすことである: 任意の相異なる $i, j \in \{1, \ldots, d\}$ に対して, 多重集合として $\{W_{ik}W_{jk}^{-1} \mid 1 \leq k \leq d, W_{ik} \neq 0 \neq W_{jk}\} = \frac{\lambda}{2}\{1,-1\}$ $(\lambda = \frac{k(k-1)}{d})$ が成り立つ. さらに $(ii) \Rightarrow (i)$ についてはアーベル群上の balanced generalized weighing matrix に次のように拡張される. $M : G \to \mathrm{Mat}_{|G|}(\mathbb{C})$ を群 G の置換表現とし B_g を次の式で定める :

$$W = \sum_{i=0}^{n-1} g_i B_{g_i}.$$

M_g, B_g $(g \in G)$ から $(0,1)$-行列を次のように定める：

$$A_i = \begin{pmatrix} M_{g_i} \otimes I_d & 0 \\ 0 & M_{g_i} \otimes I_d \end{pmatrix} \quad (0 \le i \le n-1),$$

$$A_n = \begin{pmatrix} J_n \otimes (J_d - I_d) & 0 \\ 0 & J_n \otimes (J_d - I_d) \end{pmatrix},$$

$$A_{n+1+i} = \begin{pmatrix} 0 & \sum_{j=0}^{n-1} M_{g_j} \otimes B_{g_i g_j} \\ \sum_{j=0}^{n-1} M_{g_j} \otimes B^T_{g_i g_j^{-1}} & 0 \end{pmatrix} \quad (0 \le i \le n-1),$$

$$A_{2n+1} = \begin{pmatrix} 0 & J_n \otimes (J_d - \sum_{h=0}^{n-1} B_{g_h}) \\ J_n \otimes (J_d - \sum_{h=0}^{n-1} B^T_{g_h}) & 0 \end{pmatrix}.$$

このとき次の定理が成り立つ.

Theorem 2.2. *(i)* $k = d$ のとき $\{A_i\}_{i=0}^{2n}$ はアソシエーションスキームをなす.

(ii) $k < d$ のとき $\{A_i\}_{i=0}^{2n+1}$ はアソシエーションスキームをなす.

3 Mutually quasi-unbiased weighing matrices

まず mutually quasi-unbiased weighing matrices の定義を与える. 位数 d, 重さ k の weighing matrices $W_1, \ldots, W_f$ が mutually quasi-unbiased weighing matrices(MQUWM) であるとは, ある実数 l, a が存在して $\frac{1}{\sqrt{a}} H_1 H_2^T$ が重さ l の weighing matrix になることする. このとき (d,k,l,a) を MQUWM のパラメータという.

パラメータ (d,d,d,d) である MQUWM は MUB と一致し, パラメータ (d,k,k,k) である MQUWM は Holzmann, Kharaghani, Orrick [2] によって定義された mutually unbiased weighing matrices と一致する.

MUWM に関する基本的な問題は位数 d, 重さ k の mutually unbiased weighing matrices $W_1, \ldots, W_f$ の個数 f に関する上限を決定することである. MQUWM に関する主結果は次の二つである.

Theorem 3.1. $\{W_1, \ldots, W_f\}$ をパラメータ $(d,d,d/2,2d)$ の *mutually quasi-unbiased weighing matrices* とする. このとき

$$f \le d$$

が成り立つ. また等号成立する例が $d = 2^{2t+1}$ のときに存在する.

Theorem 3.2. $\{W_1, \ldots, W_f\}$ をパラメータ $(d,2,4,1)$ の *mutually quasi-unbiased weighing matrices* とする. このとき

$$f \le d - 1$$

が成り立つ. また等号成立する例が存在するのは d が偶数が必要十分である.

参考文献

[1] D. Best, H. Kharaghani, and H. Ramp, Mutually Unbiased Weighing Matrices, Des. Codes Cryptogr. DOI 10.1007/s10623-014-9944-6.

[2] W. H. Holzmann, H. Kharaghani and W. Orrick, On the real unbiased Hadamard matrices, Combinatorics and graphs, 243–250, Contemp. Math. 531, Amer. Math. Soc., Providence, RI, 2010.

[3] H. Nozaki and S. Suda, Weighing matrices and spherical codes preprint.

Magma による多変数多項式の終結式計算の高速化について

Computing resultant matrix of general multivariate polynomials and its determinant using Magma

横山 俊一[1]（Shun'ichi Yokoyama）
九州大学大学院 数理学研究院[2] / JST CREST

概要 計算機代数システム Magma における多変数多項式の終結式計算に関して, 現行のビルトイン関数に比べ（Magma のユーザー言語のみを用いて）数百倍の高速化を行った. 本稿は講演の補足という位置付けでテクニカルな部分を中心に解説する. 講演内容そのものに関しては [3] を参照頂きたい.

1 主結果

まず必要最低限の事項を復習する. 2 つの多項式 $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ を用意し, それぞれの係数を用いてシルベスター行列

$$Syl_x(f,g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & \\ & a_m & a_{m-1} & \cdots & a_0 & \\ & & \ddots & \ddots & \ddots & \ddots \\ & & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & \cdots & b_0 & & \\ & b_n & b_{n-1} & \cdots & \cdots & b_0 & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & b_n & b_{n-1} & \cdots & \cdots & b_0 \end{pmatrix}$$

を考える. この $(m+n)$ 次正方行列の行列式 $|Syl_x(f,g)|$ を, f と g の x に関する**終結式**（resultant）と呼び $Res_x(f,g)$ と書く. Magma [1] のビルトイン関数は, この行列式をそのまま計算して出力している. 更にマニュアルの一部を抜粋すると

> `Resultant:` Resultants are computed using asymptotically-fast modular and evaluation/interpolation algorithms [2]. Options are provided for Monte Carlo-style stopping on stability, which greatly speeds up the computation (since the bounds are usually very much worse than the required lifting level).

とある. Magma はソースコード非公開となっているので, 行列式を計算するための補間法アルゴリズムとして何を採用しているのか, そしてそれが「良く」プログラミングされているかは確認出来ない. 但しこの時点で, 低速化する理由は

1. シルベスター行列をそのまま利用したことにより行列のサイズが落ちない,
2. 上記の補間法の実装に問題があるかもしれない,

という（少なくとも）2 つの原因が推察出来る. そこで行列式を計算する関数を調べると

> `Determinant:` Efficient elimination and minor expansion algorithm for multivariate polynomial rings with many variables.

[1] s-yokoyama@math.kyushu-u.ac.jp
[2] 講演当時（2013 年 12 月）は九州大学マス・フォア・インダストリ研究所所属.

とあり, 小行列式展開法と或る種の消去法が採用されている. 実はよく調べると, この消去法は分母項が現れない Gauss 消去法（FFGE）であることも分かる. この 2 つの実装に関しては Magma は優れており, 他の数式処理システムと比べても高速である. そこで今回は, シルベスター行列の表現をまず次数の小さい行列**（関孝和-Bézout 行列）**に置き換える操作を行い, 行列式の計算は素直にビルトイン関数を採用するという手法をとる. 更にそれでも次数の高い行列式を計算しなければならない時を考慮し, 新たに Berkowitz の手法を Magma で実装した. このあたりの解説は拙文 [3] を参照頂きたい.

以上の成果物を用いて, 一般係数 n 次多項式（$7 \leq n \leq 11$）の判別式（正確にはその終結式部分の）計算のベンチマークを行った. 一般係数 n 次多項式の計算を行うためには, 変数 x と係数 $a_0, \cdots, a_n$ の計 $(n+2)$ 変数の多変数多項式を取り扱うことになる. 全ての計算は Magma ver. 2.18-5 on Windows 7 64bit / Intel Core i7-2630QM 3.30GHz / 8GB Memory の環境で行った. 計算に際し, 並列化処理や特別なライブラリの導入等は一切行っていない.

Deg	#Terms	Built-in (sec)	Type BR (sec)	**Type SR** (sec)
7	1103	2.387	0.047	**0.026**
8	5247	15.460	0.281	**0.047**
9	26059	204.174	3.120	**0.390**
10	133881	3201.349	46.207	**3.994**
11	706799	$\geq$ 15hrs	907.372	**48.064**

Magma の従来実装に比べて, 数百倍の高速化が実現されている. 成果物本体は

`http://www2.math.kyushu-u.ac.jp/~s-yokoyama/Resultant.html`

に公開している. 例えば $n = 9$ の場合を Type SR で計算する場合は以下のコマンドを実行すればよい. 1 行目の load は絶対パスで指定する.

```
> load "<directory>/resultant.m";
> _<x,a0,a1,a2,a3,a4,a5,a6,a7,a8,a9>:=PolynomialRing(Rationals(),11);
> f:=a9*x^9+a8*x^8+a7*x^7+a6*x^6+a5*x^5+a4*x^4+a3*x^3+a2*x^2+a1*x+a0;
> g:=Derivative(f,x);
> time SR:=SekiResultant(f,g,x);
```

タイミングデータが不要であれば `time` は省略してよい. Berkowitz 法の実装を使用する場合は, load の指定を

```
> load "<directory>/resultant-berkowitz.m";
```

として

```
> time BR:=BerkowitzResultant(f,g,x);
```

とする. ビルトイン関数 `MR:=Resultant(f,g,x);` と同じ返り値になっているかを確認したければ

```
> MR eq SR;
```

などとすればよい. 言うまでも無いことであるが, 計算結果を格納する `SR` や `BR` は好きな名前を指定できる.

2 コードに関する補足

2.1 シルベスター行列表現を関孝和-Bézout 行列表現に書き換える Magma 版のプログラムに関する注意

```
> seki_res:=function(A,B,W)

> > M:=Degree(A,W);
> > N:=Degree(B,W);

> > if M ge N then
> > > L:=M;
> > > S:=N;
> > > end if;
> > if M lt N then
> > > L:=N;
> > > S:=M;
> > > T:=A;
> > > A:=B;
> > > B:=T;
> > > end if;

> > MAT:=Matrix(L,L,[Parent(W)!0: i in [1..L^2]]);

> > for I in [0..L-S-1] do
> > > for J in [0..S] do
> > > > MAT[I+1][J+I+1]:=Coefficient(B,W,J);
> > > > end for;
> > > end for;

> > B:=W^(L-S)*B;

> > srem:=function(f,W,L)
> > > X,Y:=CoefficientsAndMonomials(f);
> > > U:=#X;
> > > I:=[i : i in [1..U] | Degree(Y[i],W) lt L];
> > > xx:=&+[X[j]*Y[j] : j in I];
> > > return xx;
> > > end function;

> > F:=srem(A,W,L);
> > G:=srem(B,W,L);
> > H:=Coefficient(A,W,L)*G-Coefficient(B,W,L)*F;
> > for J in [0..L-1] do
> > > MAT[2*L-S-L+1][J+1]:=Coefficient(H,W,J);
> > > end for;
> > for I in [L-1..L-S+1 by -1] do
> > > H:=W*srem(H,W,L-1)+Coefficient(A,W,I)*G-Coefficient(B,W,I)*F;
> > > for J in [0..L-1] do
> > > > MAT[2*L-S-I+1][J+1]:=Coefficient(H,W,J);
> > > > end for;
> > > end for;

> > return MAT;
> > end function;
```

まず中盤に出てくる `MAT:=Matrix(L,L,[Parent(W)!0:i in [1..L^2]]);` について補足する. 一般に行列のリストを格納する際, C 言語などではインデックスは 0 から始まるのに対し, Magma は 1 から始まる. 即ち m 行 n 列成分は C 言語では `MAT[M-1][N-1]`, Magma は `MAT[M][N]` である. 更にその後の `Parent(W)!` は要注意である. ここで `W` はグローバル変数であるが, 補助関数を定義している部分（`seki_res` の内部）ではその情報は引き継がれない. 従って `W` の情報を引用するために入力として用いている. 関数 `Parent` は入力の属するカテゴリを表すので, ここでは変数 `W` を含む多変数多項式環を表す. よって `Parent(W)!0` と書いたら「0 は変数 `W` を含む多変数多項式環の元と見なす」という意味となる.

関数 `srem` は今回新しく実装した関数である. これは同名の Risa/Asir のビルトイン関数から来ている. Risa/Asir には `sdiv` という関数もあり, 多変数多項式の除算が最後まで実行出来る場合に商（div）および剰余（rem）を求める. この 2 つを合わせた `sqr` も存在する. これは関孝和-Bézout 行列の生成に用いる. 実は Magma には `sdiv` に相当する関数 `div` が存在するので, 安直に Magma で `srem` を `A-(A div B)*B` とすれば良い（`A` を `B` で割った余りとなる）ように見えるが, 実はエラーが出てしまう. その原因は `div` の内部構造であり, 多変数多項式が入力として与えられた場合に限り `div` は `ExactQuotient` という関数と同一となる. これは名前の通り `rem=0` の場合（割り切れる場合）のみ動作するため, 今回の目的は達成出来ない. しかし今回のパッケージにおいては `B=W^L`（単項式の冪）の場合のみ実現すれば良いので, 各 term を並べて係数と単項式部分の tuple のリストと見なし, `W^L` で割り切れない部分, 即ち `W^i`（`i<L`）の部分を抜いて再度和をとることで除算を計算している.

2.2 小行列式展開法に現れる for ループの実装に関する注意

```
> for(K=L;K>J;K--)
> > for(B2=B1;B2>=Q[K];B2--)
> > > U=U+CT[B2][V]
> > B1=B2-1
> > V=V-1
```

上は Risa/Asir における小行列式展開法の実装の一部である. この 2 重の for ループを Magma に実装することを試みる際, この文法のままでは Magma に実装することは出来ない. これは非常に初歩的な（しかし陥り易い）事柄である. 具体的には次の 2 点である：

1. Magma では `[K=2;K=5;K++]` というリスト（即ち `[2,3,4,5]`）は `[2..5]` と与える. 逆に `[K=5;K=2;K--]`（即ち `[5,4,3,2]`）は `[5..2 by -1]` と与える[3]. 減少列を与える場合に `by -1` が抜けているとエラーを返すので注意が必要である.

2. 2 重目の for ループを抜けた直後の 4 行目, `B2` には `B2=Q[K]-1` が格納されている. 一方 Magma の仕様では, 3 行目で保持されていた `B2` の情報は for ループを抜けたことにより 4 行目で忘却されてしまう. これにより, 4 行目の `B2` は未定義変数としてエラーを返す. これは 1 重目の for ループ以前に与えられていたリストの元 `Q[*]` を直接利用することで回避出来る.

[3]公開当初（2013 年 9 月）は異なる記法を用いていたが, この記法の方がより高速であることを内田幸寛氏（首都大学東京）よりご教示頂いた. 現在公開している最新版（2014 年 1 月）ではこちらを採用している. この場を借りて氏に深謝したい.

結論として, この部分は次のようにプログラムすればよい.

```
> for K in [L..J+1 by -1] do
> > for B2 in [B1..Q[K+1] by -1] do
> > > U:=U+CT[B2+1][V+1];
> > B1:=Q[K+1]-2;
> > V:=V-1;
```

3 Magma に関する補足 - Intel AVX サポート開始

2013 年 6 月 26 日, Magma 2.19-7 より Magma は Intel64(AMD64)/Linux 上での Intel AVX サポート開始を正式に発表した：

> From V2.19-7 onwards, for the Intel64/Linux version an executable is available which supports Intel AVX instructions. This is applicable to most Intel processors released since 2012 (including the Sandy Bridge, Ivy Bridge and Haswell architectures) with a Linux version which is suitably new (Kernel version 2.6.30 or later and GLIBC_2.7 or later). The AVX version runs significantly faster than the standard Intel64 version for several types of computation.（リリースノートより抜粋）

AVX とは SIMD 演算の（拡張）命令セットのことである. 原理的には Magma の高速化に貢献しているということになっているが, 実際に Intel Hyper-Threading Technology (HTT) 等の恩恵を十分に活かし切る実装を行っているかは疑問点も多い. この周辺の精査に早急に取り掛かり, 近日何らかの形で報告予定である. なお AVX に関する情報として, 最新リリース AVX-512 がアナウンスされている. また 2013 年 6 月に発売された Intel の最新マイクロアーキテクチャ Haswell には AVX の改良版 AVX2 が搭載されている. AVX2 では, AVX で行われた浮動小数点演算許容レジスタの 2 倍化（256bit）が整数演算にも行われている.

数学的に関連する情報としては, Magma 2.20 より導入された Faugère の F4 アルゴリズムの実装が挙げられる. これにより Gröbner 基底計算の高速化が実現されたという報告が出ている. 詳細は “A Dense Variant of the F4 Groebner Basis Algorithm”：

`http://magma.maths.usyd.edu.au/users/allan/densef4/`

を参照されたい. 詳細なベンチマーク結果も公開されている.

謝辞

今回このような素晴らしい講演の機会を頂き有難うございました. 本研究集会「第 10 回『代数学と計算』」（AC2013）の世話人の皆様に心より御礼申し上げます. また本稿の成果は木村欣司氏（京都大学情報学研究科）の協力によるものです. 重ねて感謝致します.

最後に, 本成果物は現在も改良・最適化中です. お気付きの点, コメント・アドバイス等お寄せ頂けましたら幸甚です. 宜しくお願い申し上げます.

参考文献

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation, **24** (1997), 235-265.

[2] K. O. Geddes, S. R. Czapor and G. Labahn, *Algorithms for Computer Algebra*, Springer (1992).

[3] 横山俊一, 数式処理における数学と世界最速への挑戦：終結式の計算を例に, 北海道大学数学講究録, **160** (2014), 43-49.

Shun'ichi Yokoyama
Faculty of Mathematics, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail Address: s-yokoyama@math.kyushu-u.ac.jp