Proceedings of

Algebra and Computation 2007

Tokyo Metropolitan University

December 5-7, 2007

Edited by AC2007 Proceedings Committee

Organizers

Ken Nakamula (Tokyo Metropolitan Univ.)

Michio Ozeki (Yamagata Univ.)

Nobuki Takayama (Kobe Univ.)

Katsushi Waki (Yamagata Univ.)

Hirofumi Tsumura (Tokyo Metropolitan Univ.)

Shigenori Uchiyama (Tokyo Metropolitan Univ.)

プログラム [Program]

12 月 5 日（水）

9:20 - 9:30: Opening

9:30 - 10:00: 脇 克志 (山形大学)

“GAP による既約 Brauer 指標の計算”

“On calculation of Decomposition numbers by GAP”

10:10 - 10:50: 山田裕理 (一橋大学)

“Asir によるアフィン頂点作用素代数の計算”

“Computation of affine vertex operator algebras by Asir”

11:10 - 11:40: 生田 卓也 (神戸学院大学), 宗政 昭弘 (東北大学)

“GF(2^{20}) 上の新しい non-amorphous association sceheme”

“A new non-amorphous association sceheme on GF(2^{20})”

11:50 - 12:10: 堀口直之 (千葉大学)

“ある strongly regular graph の maximum clique and coclique design と再構成について”

“On the maximum clique and coclique designs and reconstructions of some strongly regular graphs”

14:00 - 14:50: [特別講演] Fidel Nemenzo (Univ. Philippines)

“Counting self-dual codes over finite rings”

15:10 - 15:40: 小関道夫 (山形大学・名誉教授)

“長さ６４の 2nd order Reed-Muller 符号の coset weight distribution の計算 (脇 克志氏との共同研究)”

“Computation of the coset weight distributions of second order Reed-Muller code of length 64 (A joint research with Prof. K. Waki)”

15:50 - 16:20: 宗政 昭弘 (東北大学)

“長さ２８の極値的３元自己双対符号の分類 (原田 昌晃氏および Boris Venkov 氏との共同研究)”

“Classification of ternary extremal self-dual codes of length 28 （joint work with Masaaki Harada and Boris Venkov）”

16:30 - 17:00: 藤田育嗣 (東北学院大学)

“ディオファンタスの 5 つ組は正則な 4 つ組を含む”

“Any Diophantine quintuple contains a regular Diophantine quadruple”

12 月 6 日（木）

10:00-10:20: 山口幸司, 仁木直人 (東京理科大学)

“統計への応用を考えた対称式の基底変換アルゴリズム”

“Base transformation algorithm of the symmetric polynomials for use in statistics”

10:30 - 11:00: 橋本竜太 (詫間電波高専)

“周期の長さが一定の循環連分数に付随する，基本単数の大きな実２次整環の判別式の例”

“Examples of discriminants of quadratic orders with large fundamental units attached to a fixed length of the period of continued fractions”

11:20 - 12:10: [特別講演] 駒野 雄一 (株式会社 東芝)

“公開鍵暗号技術と証明可能安全性”

“Public Key Cryptosystems and Provable Security”

14:00 - 14:40: 星明考 (早稲田大学)

“生成的多項式の同型問題への考察 (三宅克哉氏との共同研究)”

“Note on the field isomorphism problem of generic polynomials (joint work with K. Miyake)”

14:50 - 15:10: 田中覚, 西本啓一郎, 松井鉄史, 内山成憲, 中村憲 (首都大学東京)

“数論システム NZMATH 開発の現状と課題”

“Status and issues on development NZMATH”

15:20 - 15:50: 市来 信吾, 小椋 直樹, 小泉 賢洋, 西本 啓一郎, 田中 覚, 松井 鉄史, 内山 成憲, 中村 憲 (首都大学東京)

“すぐ使える数論システム NZMATH”

“A Brief Introduction to NZMATH”

16:10 - 17:00: [特別講演] 濱田 龍義 (福岡大学)

“数学ソフトウェアの森 KNOPPIX/Math”

“Forests of mathematical software, KNOPPIX/Math”

12 月 7 日 (金)

10:20 - 10:40: 森川良三 (首都大学東京)

“ワーリングタイプの問題を探求するための、いくつかの概念と方法”

“Some concepts and methods to investigate problems of Waring type.”

10:50 - 11:10: 小松尚夫 (弘前大学), Carsten Elsner(FHDW Hannover)

“三項関係式と整数列”

“Three term recurrence relations associated with integer sequences”

11:20 - 11:40: 金子昌信 (九州大学), 野呂正行 (神戸大学), 鶴巻健一 (日本オラクル (株))

“多重ゼータ値の生成する空間の次元予想について”

“On a conjecture for the dimension of the space of the multiple zeta values”

13:30 - 14:20: [特別講演] Andrej Dujella (Univ. Zagreb, CROATIA)

“Construction of high rank elliptic curves and related Diophantine problems”

14:40 - 15:10: 松井鉄史 (首都大学東京)

“計算量と数の超越性”

“Computational Complexity and Transcendence of Numbers”

15:20 - 15:50: 塩川宇賢, 立谷洋平 (慶應義塾大学)

“$\langle q, r\rangle$ 数系におけるパターン数列の性質について”

“Pattern sequences in $\langle q, r\rangle$-numaration sysytems”

16:00 - 16:30: 小松啓一 (早稲田大学), 福田隆 (日本大学)

“ウェーバーの類数問題に対する計算的アプローチ”

“A computational approach to Weber’s class number problem”

16:30 - 16:40: Closing

GAP による既約 Brauer 指標の計算

脇 克志

2007 年 12 月 4 日

研究に計算機をどう使う？

皆さんは、計算機を研究にどのように活用しているでしょうか？私の場合は、「準備段階の細かい計算を計算機でやっておくが、最終的な結果は、**計算機による結果の詳細には触れずに**論文にまとめる」形が多い気がします。ところが、たまに、論文に発表した最終結果より、**準備段階の計算**の方が自分にも、そして時には**他の人**にも**有用な場合**があったりします。困ったもので、一定の期間が過ぎると準備段階の計算は本人以外 (下手をすると本人さえ) 判読不可能になる場合がよくあります。そこで、雑多な計算しながら、出来るだけその結果を計算の経緯を含めて、自動的に TeX ソースにしてまとめてくれるプログラムを考えてみました。今回は、私が研究している有限群のモジュラー表現について紹介し、最後に、計算機を使った結果をお見せします。

1 有限群のモジュラー表現入門

1.1 通常表現とモジュラー表現

G を有限群、F をある体 として $GL(n,F)$ を F 上の n 次一般線形群 とします。このとき、G から $GL(n,F)$ への準同形写像 $R : G \to GL(n,F)$ を G の F–**表現**と呼び、n を R の次数と呼ぶことにします。F が複素数体のとき、R を**通常表現**と呼び、F が標数 $p > 0$ の有限体のとき、**モジュラー表現**と呼びます。また、G の元 x について、$o(x)$ は x の位数を表すことしにします。

1.2 表現の例

添字を付けて G の元を全て並べたものを $[x_1, x_2, \cdots, x_n]$ とします。表現 $FG : G \to GL(n,F)$ を

$$FG(x_k) = \{\alpha_{ij}^{(k)}\} \quad \alpha_{ij}^{(k)} := \begin{cases} 1 & x_i = x_k * x_j \\ 0 & x_i \neq x_k * x_j \end{cases}$$

で定義します。この FG を体 F 上の G の**正則表現**と呼びます。例えば 3 次巡回群 $G = \{1, x, x^2\}$ の場合、$[x_0, x_1, x_2] = [1, x, x^2]$ と置くと、$x_i = x_0 * x_i$, $x_i = x_1 * x_{i-1}$, $x_i = x_2 * x_{i+1}$ $(i = 0, 1, 2 \bmod 3)$ より $FG(x_0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, FG(x_1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, FG(x_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ となります。

1.3 既約と直既約

表現 R に対し、ある正則行列 P と表現 R_1, R_2 が存在して、$\forall x \in G, PR(x)P^{-1} = \begin{pmatrix} R_1(x) & * \\ 0 & R_2(x) \end{pmatrix}$ となるとき、$R \cong \begin{pmatrix} R_1 & * \\ 0 & R_2 \end{pmatrix}$ と書いて表現 R は、**既約でない**と呼びます。特に、$*$ の部分も常に 0 となる P が存在するとき、**直既約でない**と呼び、$R \cong R_1 \oplus R_2$ と書きます。正則表現 FG の直既約因子を**直既約射影表現**と呼びます。この非同型な直既約射影表現と非同型な既約表現の間に 1-1 の対応があり、その個数は一致します。以下では、非同型な既約通常表現の個数を $k(G)$、非同型な既約モジュラー表現の個数を $l(G)$ と表すことにします。

1.4 表現と指標

R が通常表現のとき、G 上の複素数値類関数 χ_R を $\chi_R(x) := TrR(x)$ $(x \in G, TrM$ は、正方行列 M の対角成分の総和) で定義して、 G の**通常指標**と呼びます。また、R がモジュラー表現でで F の標数が p であるとき、p–正則元全体の集合 $G_{p'} := \{x \in G \mid p \not| o(x)\}$ の元 x に対して、行列 $R(x)$ の固有値 $\{\varepsilon_1, \cdots, \varepsilon_s\} \subset F$ は、すべて、1 の $o(x)$ 乗根となりますが、この ε_i に対応する複素数の 1 の $o(x)$ 乗根を λ_i とすると、$G_{p'}$ 上の複素数値類関数 φ_R を $\varphi_R(x) := \lambda_1 + \cdots + \lambda_s$ で定義することが出来ます。この φ_R を G の Brauer 指標と呼びます。既約通常表現に対応する既約通常指標を集めた集合を $\mathrm{Irr}(G)$ で表し、既約モジュラー表現に対応する既約 Brauer 指標を集めた集合を $\mathrm{IBr}(G)$ で表します。

1.5 指標の例

指標の値は、表現行列の対角成分の和となり共役類ごとに決まります。6 次の交代群の既約通常指標は、

$Char.$	$1a$	$2a$	$3a$	$3b$	$4a$	$5a$	$5b$
χ_1	1	1	1	1	1	1	1
χ_{5a}	5	1	2	-1	-1	0	0
χ_{5b}	5	1	-1	2	-1	0	0
χ_{8a}	8	0	-1	-1	0	A	A^*
χ_{8b}	8	0	-1	-1	0	A^*	A
χ_9	9	1	0	0	1	-1	-1
χ_{10}	10	-2	1	1	0	0	0

$A = \frac{1+\sqrt{5}}{2}$

そして、3-既約 Brauer 指標は、

$Char.$	$1a$	$2a$	$3a$	$3b$	$4a$	$5a$	$5b$
φ_1	1	1	$*$	$*$	1	1	1
φ_{3a}	3	-1	$*$	$*$	1	A	A^*
φ_{3b}	3	-1	$*$	$*$	1	A^*	A
φ_4	4	0	$*$	$*$	-2	-1	-1
φ_9	9	1	$*$	$*$	1	-1	-1

$A = \frac{1+\sqrt{5}}{2}$

となります。

1.6 指標の比較

6 次の交代群の既約通常指標と既約 3-Brauer 指標を比べると、

$Char.$	$1a$	$2a$	$3a$	$3b$	$4a$	$5a$	$5b$
χ_1	1	1	1	1	1	1	1
χ_{5a}	5	1	2	-1	-1	0	0
χ_{5b}	5	1	-1	2	-1	0	0
χ_{8a}	8	0	-1	-1	0	A	A^*
χ_{8b}	8	0	-1	-1	0	A^*	A
χ_9	9	1	0	0	1	-1	-1
χ_{10}	10	-2	1	1	0	0	0
φ_1	1	1	$*$	$*$	1	1	1
φ_{3a}	3	-1	$*$	$*$	1	A	A^*
φ_{3b}	3	-1	$*$	$*$	1	A^*	A
φ_4	4	0	$*$	$*$	-2	-1	-1
φ_9	9	1	$*$	$*$	1	-1	-1

$A = \frac{1+\sqrt{5}}{2}$

$G_{3'}$ 上で、次の等式が成り立ちます。

- $\chi_1 = \varphi_1$,
- $\chi_{5a} = \chi_{5b} = \varphi_1 + \varphi_4$,
- $\chi_{8a} = \varphi_1 + \varphi_{3a} + \varphi_4$,
- $\chi_{8b} = \varphi_1 + \varphi_{3b} + \varphi_4$,
- $\chi_9 = \varphi_9$,
- $\chi_{10} = \varphi_{3a} + \varphi_{3b} + \varphi_4$

1.7 群 G の p -分解行列

$\{R_1, \cdots, R_{k(G)}\}$ を G の非同型な既約通常表現の集合とし、$\{S_1, \cdots, S_{l(G)}\}$ を G の非同型な既約 p -モジュラー表現の集合とします。このとき、$\chi_i := \chi_{R_i}$, $\varphi_j := \varphi_{S_i}$ とすると、χ_i は、$G_{p'}$ 上で、

$$\chi_i = \sum_{j=1}^{l(G)} d_{ij}\varphi_j \qquad d_{ij} : \text{非負の整数}$$

と表せます。この $\{d_{ij}\}_{1\leq i\leq k(G),\, 1\leq j\leq l(G)}$ を G の p **-分解定数**と呼びます。次のように分解定数は、行列の形で表され p **-分解行列**とも呼ばれます。

$Char.$	φ_1	φ_2	$\cdots$	$\varphi_{l(G)}$
χ_1	d_{11}	d_{12}	$\cdots$	$d_{1l(G)}$
χ_2	d_{21}	d_{22}	$\cdots$	$d_{2l(G)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\chi_{k(G)}$	$d_{k(G)1}$	$d_{k(G)2}$	$\cdots$	$d_{k(G)l(G)}$

1.6 の例から 3-分解行列は次のようになります。

$Char.$	φ_1	φ_{3a}	φ_{3b}	φ_4	φ_9
χ_1	1	0	0	0	0
χ_{5a}	1	0	0	1	0
χ_{5b}	1	0	0	1	0
χ_{8a}	1	1	0	1	0
χ_{8b}	1	0	1	1	0
χ_9	0	0	0	0	1
χ_{10}	0	1	1	1	0

1.8 3− 分解行列の列成分

次に、分解行列の列成分に注目します。1.7 の例で得られた分解行列の列成分を係数とする既約通常指標の和は直既約射影表現に対応する直既約射影指標となり、$\mathrm{IPr}(G) = \{\eta_1, \eta_{3a}, \eta_{3b}, \eta_4, \eta_9\}$ と書くことにします。つまり

- $\eta_1 := \chi_1 + \chi_{5a} + \chi_{5b} + \chi_{8a} + \chi_{8b}$,
- $\eta_{3a} := \chi_{8a} + \chi_{10}$, $\eta_{3b} := \chi_{8b} + \chi_{10}$,
- $\eta_4 := \chi_{5a} + \chi_{5b} + \chi_{8a} + \chi_{8b} + \chi_{10}$, $\eta_9 := \chi_9$.

となり、各指標の値は次の通りです。

$Char.$	$1a$	$2a$	$3a$	$3b$	$4a$	$5a$	$5b$
η_1	27	3	0	0	−1	2	2
η_{3a}	18	−2	0	0	0	A	A^*
η_{3b}	18	−2	0	0	0	A^*	A
η_4	36	0	0	0	−2	1	1
η_9	9	1	0	0	1	−1	−1

1.9 指標の内積

2 つの指標 χ_a, χ_b が与えられたとき、その内積を

$$\langle \chi_a, \chi_b \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_a(g)\chi_b(g^{-1})$$

で定義します。このとき、既約通常指標 χ_i, χ_j について、$\langle \chi_i, \chi_j \rangle = \delta_{ij}$ が成り立ちます。また、Brauer 指標で $G_{p'}$ 以外の元の値は 0 として内積を計算すると、既約 Brauer 指標 φ_i と直既約射影指標 η_j について、$\langle \varphi_i, \eta_j \rangle = \delta_{ij}$ が成り立ちます。また、直既約射影指標の定義 $\left(\eta_j = \sum_{i=1}^{k(G)} d_{ij}\chi_i \right)$ から $d_{ij} = \langle \chi_i, \eta_j \rangle$ で分解定数が得られます。

2 分解定数の計算

1.9 より、分解定数を求めるためには、直既約射影指標が得られれば良いことが分かりました。ではどうやって直既約射影指標を求めたら良いのでしょうか？

2.1 射影指標の作り方 (基本編)

まず、モジュラー表現論の一般論から得られる射影指標が持つ性質を紹介します。

- 位数 $|G|$ が p で割り切れないとき、**すべての**既約通常指標は**直既約射影指標**である。
- 位数 $|G|$ が最大 p^n で割り切れるとき、**次数が p^n で割り切れるすべての**既約通常指標は**直既約射影指標**である。
- 部分群 H の射影指標 ζ を G に**誘導した指標** ζ^G は**射影指標**となる。

- Brauer 指標 φ と**射影指標** η **とのテンサー積** $\eta \otimes \varphi$ は**射影指標**となる。
- 2 つの部分群 H_1, H_2 が位数が p の G で非共役な Sylow p-部分群を持てば、$I_{H_1}^G \otimes I_{H_2}^G$ は、**射影指標**となる。

以上のような性質を利用することで数多くの射影指標が計算できます。ここで問題になるのは、射影指標をどのように直既約射影指標の和に分解するかです。

2.2 FG のブロック分解

まずは、射影指標を大雑把に直和分解するためにブロックと言う考えを紹介します。正則表現 FG とその像 $FG(G)$ を同一視することで、$\langle FG \rangle_F$ を F-多元環と考えることが出来ます。このとき、この F-多元環のイデアルとしての直和分解 $\langle FG \rangle_F = A_1 \oplus \cdots \oplus A_s$ が得られますが、この A_i を G の $p-$ ブロックと呼びます。実は、正則表現 FG には、G の全ての F-表現が含まれるため上の直和分解で既約表現を分類することが出来ます。更にそのまま既約指標の分類にも使えます。つまり、既約モジュラー表現 R について、R がブロック A_i に所属するとき、既約 Brauer 指標 φ_R は、ブロック A_i に含まれると呼びます。$\mathrm{IBr}(A)$ で A に含まれる既約 Brauer 指標を表すことにします。

2.3 既約通常指標のブロック分解

次に既約通常指標のブロックによる分類を考えます。既約通常指標 $\chi_i = \sum_{j=1}^{l(G)} d_{ij}\varphi_j$ について $d_{ij} > 0$ となるすべての既約 Brauer 指標 φ_j はある 1 つのブロック A_k に属していることが知られています。このとき既約通常指標 χ_i は、ブロック A_k に含まれると呼びます。このことは、分解定数は、ブロック毎に求めれば十分であることを示しています。ただし、指標のブロック分解は、体 F の標数 p に依存して変化します。$\mathrm{Irr}(A)$ でブロック A に含まれる既約通常指標を、$\mathrm{IPr}(A)$ で A に含まれる直既約射影指標を表すことにします。しかし、このように F-表現に依存していては、具体的にブロック分解をするのは大変な作業になってしまいます。そこで F-表現を使わないで、既約通常指標をブロック分類する方法を紹介します。既約通常指標 χ, $x \in G$ について、指標 ω_χ を $\omega_\chi(x) := \frac{|G|\chi(x)}{|C_G(x)|\chi(1)}$ と定義します。このとき、「χ と χ' が同じ $p-$ ブロックに属する」$\Leftrightarrow$ 「任意の $p'-$ 元 x で、$\omega_\chi(x) \equiv \omega_{\chi'}(x) \bmod p$」が知らせています。この関係より指標 ω_χ を計算することで既約通常指標がブロック毎に分解できることが分かります。また、この事実より、G の位数が p で割り切れないときは、「すべての既約指標は異なるブロックに属する」ことになり、「各ブロックはただ 1 つの既約指標を含む」ことが分かります。

6 次の交代群についてこの指標を計算すると次の表の通りとなります。

$Char.$	$1a$	$2a$	$3a$	$3b$	$4a$	$5a$	$5b$
ω_{χ_1}	1	45	40	40	90	72	72
$\omega_{\chi_{5a}}$	1	9	16	-8	-18	0	0
$\omega_{\chi_{5b}}$	1	9	-8	16	-18	0	0
$\omega_{\chi_{8a}}$	1	0	-5	-5	0	$9A$	$9A^*$
$\omega_{\chi_{8b}}$	1	0	-5	-5	0	$9A^*$	$9A$
ω_{χ_9}	1	5	0	0	10	-8	-8
$\omega_{\chi_{10}}$	1	-9	4	4	0	0	0

$A = \frac{1+\sqrt{5}}{2}$

ここから 2 つのブロック b_0, b_1 があり、$\mathrm{Irr}(b_0) = \{\chi_1, \chi_{5a}, \chi_{5b}, \chi_{8a}, \chi_{8b}, \chi_{10}\}$ と $\mathrm{Irr}(b_1) = \{\chi_9\}$ に分かれることが分かります。また、次のように分解定数もきちんとブロック毎に分かれていることが見えて来ます。

Char.	φ_1	φ_{3a}	φ_{3b}	φ_4	φ_9
χ_1	1	0	0	0	0
χ_{5a}	1	0	0	1	0
χ_{5b}	1	0	0	1	0
χ_{8a}	1	1	0	1	0
χ_{8b}	1	0	1	1	0
χ_{10}	0	1	1	1	0
χ_9	0	0	0	0	1

次の章では、射影指標を更に分解して直既約であるかを判定するための定理を紹介します。

3 MOC-system について

今回のプログラムを作る上で、理論的な土台となった部分がこの MOC-system です。この system により半自動である程度細かい射影指標の直和分解が可能になりました。

MOC (MOdular Characters)[1] は、1993 年に、G. Hiss, C. Jansen, K. Lux, R. Parker によって開発された Brauer 指標を計算するプログラムの集合です。MOC では、 $\mathrm{Irr}(A)$, $\mathrm{IBr}(A)$, $\mathrm{IPr}(A)$ を $\mathbb{Z}$-基底とする格子を考えて、この格子で Basic Set や System of atom と呼ばれる別の $\mathbb{Z}$-基底を導入することで、射影指標の直既約判定などを可能にしています。オリジナルのプログラムは C 言語ですが、今回はこのプログラムを GAP 上に実装しました。

3.1 $\mathbb{Z}$-基底について

ブロック A について A に属する 3 つの指標の集合を、既約通常指標の集合 $\mathrm{Irr}(A) = \{\chi_1, \chi_2, \cdots, \chi_k\}$, 既約 Brauer 指標の集合 $\mathrm{IBr}(A) = \{\varphi_1, \varphi_2, \cdots, \varphi_l\}$, 直既約射影指標の集合 $\mathrm{IPr}(A) = \{\eta_1, \eta_2, \cdots, \eta_l\}$ とします。

このとき、 通常指標全体は、$\mathrm{Irr}(A)$ を $\mathbb{Z}$-基底とする $\mathbb{N}$ 格子 $\langle \mathrm{Irr}(A) \rangle_{\mathbb{N}}$ であり、Brauer 指標全体は、$\mathrm{IBr}(A)$ を $\mathbb{Z}$-基底とする $\mathbb{N}$ 格子 $\langle \mathrm{IBr}(A) \rangle_{\mathbb{N}}$ であり、射影指標全体は、 $\mathrm{IPr}(A)$ を $\mathbb{Z}$-基底とする $\mathbb{N}$ 格子 $\langle \mathrm{IPr}(A) \rangle_{\mathbb{N}}$ となります。

3.2 Basic Set

$\mathbb{Z}$ 格子 $\langle \mathrm{IBr}(A) \rangle_{\mathbb{Z}}$ の $\mathbb{Z}$-基底 $\mathrm{BS} = \{\phi_1, \cdots \phi_l\}$ が、$\mathbb{N}$ 格子 $\langle \mathrm{IBr}(A) \rangle_{\mathbb{N}}$ の部分集合となるとき、BS を既約 Brauer 指標の集合の Basic Set と呼ぶことにします。また、$\mathbb{Z}$ 格子 $\langle \mathrm{IPr}(A) \rangle_{\mathbb{Z}}$ の $\mathbb{Z}$-基底 $\mathrm{PS} = \{\zeta_1, \cdots \zeta_l\}$ が、$\mathbb{N}$ 格子 $\langle \mathrm{IPr}(A) \rangle_{\mathbb{N}}$ の部分集合となるとき、PS を直既約射影指標の集合の Basic Set と呼ぶことにします。

もちろん $\mathrm{IBr}(A) = \{\varphi_1, \cdots \varphi_l\}$, $\mathrm{IPr}(A) = \{\eta_1, \cdots \eta_l\}$ は、それぞれの Basic Set になります。

3.3 Basic Set の判定方法

定理： $\mathrm{BS} = \{\phi_1, \cdots \phi_l\}$, $\mathrm{PS} = \{\zeta_1, \cdots \zeta_l\}$ がそれぞれ $\mathbb{Z}$ 格子 $\langle \mathrm{IBr}(A)\rangle_{\mathbb{Z}}$ と $\langle \mathrm{IPr}(A)\rangle_{\mathbb{Z}}$ の $\mathbb{Z}$-基底とすると、$l \times l$-行列

$$U := \langle \mathrm{BS}, \mathrm{PS}\rangle = \begin{pmatrix} \langle \phi_1, \zeta_1\rangle & \langle \phi_1, \zeta_2\rangle & \cdots & \langle \phi_1, \zeta_l\rangle \\ \langle \phi_2, \zeta_1\rangle & \langle \phi_2, \zeta_2\rangle & \cdots & \langle \phi_2, \zeta_l\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \phi_l, \zeta_1\rangle & \langle \phi_l, \zeta_2\rangle & \cdots & \langle \phi_l, \zeta_l\rangle \end{pmatrix}$$

について、U^{-1} の成分が全て整数であることが BS, PS が、Basic Set となるための必要十分条件となります。特に行列 U が単位行列のとき、$\mathrm{BS} = \mathrm{IBr}(A)$, $\mathrm{PS} = \mathrm{IPr}(A)$ となります。

3.4 System of atom

$\mathbb{Z}$ 格子 $\langle \mathrm{IBr}(A)\rangle_{\mathbb{Z}}$ の $\mathbb{Z}$-基底 $\mathrm{BA} = \{\psi_1, \cdots \psi_l\}$ について、$\mathrm{IBr}(A)$ が $\langle \mathrm{BA}\rangle_{\mathbb{N}}$ に含まれるとき、BA を既約 Brauer 指標の集合の System of atom と呼ぶことにします。また、$\mathbb{Z}$ 格子 $\langle \mathrm{IPr}(A)\rangle_{\mathbb{Z}}$ の $\mathbb{Z}$-基底 $\mathrm{PA} = \{\gamma_1, \cdots \gamma_l\}$ について、$\mathrm{IPr}(A)$ が $\langle \mathrm{PA}\rangle_{\mathbb{N}}$ に含まれるとき、PA を直既約射影指標の集合の System of atom と呼ぶことにします。

今回も、$\mathrm{IBr}(A) = \{\varphi_1, \cdots \varphi_l\}$, $\mathrm{IPr}(A) = \{\eta_1, \cdots \eta_l\}$ は、それぞれの System of atom になります。特に、もし、$\eta \in \mathrm{PA} \cap \langle \mathrm{IPr}(A)\rangle_{\mathbb{N}}$ なら、$\eta \in \mathrm{IPr}(A)$ となります。

3.5 BS と PA を使った射影指標の直既約判定

ζ を射影指標とします。$\zeta = \sum_{i=1}^{l} n_i\gamma_i$ ($\gamma_i \in \mathrm{PA}$, $n_i > 0$) と表せたとき、$\zeta' = \sum_{i=1}^{l} n'_i\gamma_i$ ただし $(0 \leqq n'_i \leqq n_i)$ を ζ **の部分**と呼びます。

定理： ζ を射影指標とします。任意の ζ の部分 ζ' について、$\exists\varphi$：Brauer 指標、$\langle \zeta', \varphi\rangle_G < 0$ または、$\langle \zeta - \zeta', \varphi\rangle_G < 0$ なら、ζ は**直既約射影指標**となる。

以上の定理から射影指標の直既約性をある程度決めることが出来ます。今回作ってプログラムでは、この定理を利用して直既約射影指標をある程度自動的に計算しながらその結果を、TeX 形式で保存できるようにしています。

Appendix

以下に、実際に GAP を使った計算の様子とその結果としての TeX の出力をお見せします。ここでは、著者が修士学生の頃、結構苦労して求めた 6 次の交代群の 3-分解定数を GAP を使って全自動で求めて TeX の文章にまとめています。

```
GAP4, Version: 4.4.9 of 6-Nov-2006, i686-pc-linux-gnu-gcc
gap>  p:=3;;
gap>  MAX_mul:=20;;
gap>  ALL_MAXIMAL_SUBGROUP_CONTAIN_NORMALIZER:=false;;
gap> ###################################################################
gap>  Read("BrauerCT.gd");
```

```
This is BrauerCT.gd : Time-stamp: <07/12/02 22:28:42 waki>.
gap>  Read("BrauerCT2.gi");
This is BrauerCT.gi : Time-stamp: <07/12/03 17:21:30 waki>.
gap>  G:=AlternatingGroup(6);
Alt( [ 1 .. 6 ] )
gap>  mx:=MaximalSubgroupClassReps(G);
[ Group([ (1,2,3), (2,3,4), (1,2)(5,6) ]),
  Alt( [ 1 .. 5 ] ),
  Group([ (3,6)(4,5), (3,5)(4,6), (1,2)(3,5,4,6), (1,3,6)(2,4,5) ]),
  Group([ (2,3)(4,5), (2,3)(4,6), (1,2)(4,6), (1,4,3,6)(2,5) ]),
  PSL(2,5) ]
gap> List(mx,Size);
[ 24, 60, 24, 36, 60 ]
gap>  ct:=CharacterTable(G);
CharacterTable( Alt( [ 1 .. 6 ] ) )
gap>  ctH:=CharacterTable(mx[1]);;
gap>  ctK:=CharacterTable(mx[2]);;
gap>  ctL:=CharacterTable(mx[3]);;
gap>  ctM:=CharacterTable(mx[4]);;
gap>  ctX:=CharacterTable(mx[5]);;
gap>  nnG:=["G","A","\\chi","\\varphi"];;
gap>  nnH:=["H","B","\\theta","\\vartheta"];;
gap>  nnK:=["K","C","\\phi","\\psai"];;
gap>  nnL:=["L","D","\\zeta","\\eta"];;
gap>  nnM:=["M","E","\\xi","\\mu"];;
gap>  nnX:=["X","F","\\sigma","\\tau"];;
gap>  bAs:=SetBlocksInCharacterTable(ct,p,MAX_mul,nnG);;
gap>  bBs:=SetBlocksInCharacterTable(ctH,p,MAX_mul,nnH);;
gap>  bCs:=SetBlocksInCharacterTable(ctK,p,MAX_mul,nnK);;
gap>  bDs:=SetBlocksInCharacterTable(ctL,p,MAX_mul,nnL);;
gap>  bEs:=SetBlocksInCharacterTable(ctM,p,MAX_mul,nnM);;
gap>  bFs:=SetBlocksInCharacterTable(ctX,p,MAX_mul,nnX);;
gap> GetProjectiveCharacters(bAs,[bBs,bCs,bDs,bEs,bFs]);
gap> DisplayProjectiveCharactersInBlock(bAs[1],"P");
+++ Block A2a of defect 2 has 9 proj. characters. +++
 Irr:   1 2 3 4 5 7  : Indec. Flag
----+----+-+-+-+-+-+-:-------------
   1: [ . 1 1 1 1 1] :
   2: [ . 1 1 1 2 2] :
   3: [ . 1 1 2 1 2] :
   4: [ 1 1 1 2 2 2] :
   5: [ . 1 1 2 2 3] :
   6: [ 1 1 1 1 1 .] :
```

```
   7: [ . . . 1 1 2] :
   8: [ . . . 1 . 1] :
   9: [ . . . . 1 1] :
gap> DisplayCharactersId(bAs[1].P);
No. : Deg. :   Id.
----+------+------------------------------------------------------------
   1:    36: (T(P(6),2)).A2a
   2:    54: (T(P(6),4)).A2a
   3:    54: (T(P(6),5)).A2a
   4:    63: (T(P(6),6)).A2a
   5:    72: (T(P(6),7)).A2a
   6:    27: ((P(1))^G).A2a
   7:    36: ((P(4))^G).A2a
   8:    18: ((P(2))^G).A2a
   9:    18: ((P(3))^G).A2a
gap> DisplayProjectiveCharactersInBlock(bEs[1],"P");
+++ Block E2a of defect 2 has 20 proj. characters. +++
 Irr:   1 2 3 4 5 6  : Indec. Flag
----+----+-+-+-+-+-+-:-------------
   1: [ . 2 1 1 4 4] :
   2: [ . 2 2 2 6 6] :
   3: [ 1 2 2 2 7 7] :
   4: [ . 2 3 3 8 8] :
   5: [ 1 . . . 1 1] :
   6: [ 2 . 1 1 4 4] :
   7: [ 1 1 . 2 4 4] :
   8: [ 1 1 2 . 4 4] :
   9: [ 2 . 2 2 6 6] :
  10: [ 2 2 . 2 6 6] :
  11: [ 2 2 2 . 6 6] :
  12: [ 2 1 2 2 7 7] :
  13: [ 2 2 1 2 7 7] :
  14: [ 2 2 2 1 7 7] :
  15: [ 2 . 3 3 8 8] :
  16: [ 3 3 . 2 8 8] :
  17: [ 3 3 2 . 8 8] :
  18: [ . 1 . . 1 1] :
  19: [ . . 1 . 1 1] :
  20: [ . . . 1 1 1] :
gap> DisplayCharactersId(bEs[1].P);
No. : Deg. :   Id.
----+------+------------------------------------------------------------
   1:    36: (((T(P(6),2)).A2a)_M).E2a
```

```
   2:    54: (((T(P(6),4)).A2a)_M).E2a
   3:    63: (((T(P(6),6)).A2a)_M).E2a
   4:    72: (((T(P(6),7)).A2a)_M).E2a
   5:     9: ((P(6))_M).E2a
   6:    36: (T((((T(P(6),2)).A2a)_M).E2a,2)).E2a
   7:    36: (T((((T(P(6),2)).A2a)_M).E2a,3)).E2a
   8:    36: (T((((T(P(6),2)).A2a)_M).E2a,4)).E2a
   9:    54: (T((((T(P(6),4)).A2a)_M).E2a,2)).E2a
  10:    54: (T((((T(P(6),4)).A2a)_M).E2a,3)).E2a
  11:    54: (T((((T(P(6),4)).A2a)_M).E2a,4)).E2a
  12:    63: (T((((T(P(6),6)).A2a)_M).E2a,2)).E2a
  13:    63: (T((((T(P(6),6)).A2a)_M).E2a,3)).E2a
  14:    63: (T((((T(P(6),6)).A2a)_M).E2a,4)).E2a
  15:    72: (T((((T(P(6),7)).A2a)_M).E2a,2)).E2a
  16:    72: (T((((T(P(6),7)).A2a)_M).E2a,3)).E2a
  17:    72: (T((((T(P(6),7)).A2a)_M).E2a,4)).E2a
  18:     9: (T(((P(6))_M).E2a,2)).E2a
  19:     9: (T(((P(6))_M).E2a,3)).E2a
  20:     9: (T(((P(6))_M).E2a,4)).E2a
gap> TestPIM(bAs[1],MAX_mul);
3 th proj. char. in P is indec. because it is in PA.
4 th proj. char. in P is indec. because it is in PA.
gap> TestPIM(bEs[1],MAX_mul);
1 th proj. char. in P is indec. because it is in PA.
2 th proj. char. in P is indec. because it is in PA.
3 th proj. char. in P is indec. because it is in PA.
4 th proj. char. in P is indec. because it is in PA.
gap> DisplayProjectiveCharactersInBlock(bAs[1],"PS");
+++ Block A2a of defect 2 has 4 proj. characters. +++
 Irr:   1 2 3 4 5 7  : Indec. Flag
----+----+-+-+-+-+-+-:-------------
   1: [ 1 1 1 1 1 .] :
   2: [ . 1 1 1 1 1] :
   3: [ . . . 1 . 1] :  (*)
   4: [ . . . . 1 1] :  (*)
gap> DisplayProjectiveCharactersInBlock(bEs[1],"PS");
+++ Block E2a of defect 2 has 4 proj. characters. +++
 Irr:   1 2 3 4 5 6  : Indec. Flag
----+----+-+-+-+-+-+-:-------------
   1: [ 1 . . . 1 1] :  (*)
   2: [ . 1 . . 1 1] :  (*)
   3: [ . . 1 . 1 1] :  (*)
   4: [ . . . 1 1 1] :  (*)
```

```
gap> TryToSubstractIndecProjectiveCharacters(bAs[1],2,3,MAX_mul);
0
gap> WriteAllResultsByTeX(bAs,[bBs,bCs,bDs,bEs,bFs],"A6.tex");
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfGmod_3.tex
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfHmod_3.tex
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfKmod_3.tex
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfLmod_3.tex
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfMmod_3.tex
% This file is generated by WriteBlocksInCharacterTableByTeX.
FileName is DecOfXmod_3.tex
gap> Exec("platex A6.tex");
gap> Exec("xdvi A6.dvi &");
gap>
```

Decomposition numbers of G

3.6 Characteristic 3

There are 2 conjugacy classes of cyclic groups 3a and 3b of order 3 in G. The orders of centralizers of these cyclic groups are 9 and 9. In G, there are 1 blocks with defect 0, one block A_{1a} of defect 1, and one block A_{2a} of defect 2. The index of simple projective character is { 6 and 6}.

Lemma 1. *The block A_{2a} contains the following irreducible characters*

$$V_{A_{2a}} = {}^t[\quad \chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_7]$$

The next lemma is just obtained by GAP.

Lemma 2. *There are the following projective characters in A_{2a}.*

$$\begin{aligned}
(\widetilde{\theta_1}^G).A_{2a} &= [\ 1,\ 1,\ 1,\ 1,\ 1,\ 0].V_{A_{2a}} \\
(\widetilde{\chi_6} \otimes \chi_2).A_{2a} &= [\ 0,\ 1,\ 1,\ 1,\ 1,\ 1].V_{A_{2a}} \\
(\widetilde{\phi_2}^G).A_{2a} &= [\ 0,\ 0,\ 0,\ 1,\ 0,\ 1].V_{A_{2a}} \\
(\widetilde{\phi_3}^G).A_{2a} &= [\ 0,\ 0,\ 0,\ 0,\ 1,\ 1].V_{A_{2a}}
\end{aligned}$$

Theorem 3. *The decomposition matrix of A_{2a}. is the following.*

(1)					
	χ_1	1	0	0	0
	χ_2	1	1	0	0
	χ_3	1	1	0	0
	χ_4	1	1	1	0
	χ_5	1	1	0	1
	χ_7	0	1	1	1

Proof: This is immediate from lemma 2 □

Decomposition numbers of H

3.7 Characteristic 3

There are 1 conjugacy classes of cyclic groups 3a of order 3 in H. The order of centralizer of this cyclic group is 3. In H, there are 2 blocks with defect 0, and one block B_{1a} of defect 1. The indices of simple projective characters are { 4 and 5}.

Lemma 4. *The block B_{1a} contains the following irreducible characters*

$$V_{B_{1a}} = {}^t[\quad \theta_1, \theta_2, \theta_3]$$

The next lemma is just obtained by GAP.

Lemma 5. *There are the following projective characters in B_{1a}.*

$$\begin{aligned} \widetilde{\theta_1} &= [\quad 1, \quad 0, \quad 1].V_{B_{1a}} \\ \widetilde{\theta_2} &= [\quad 0, \quad 1, \quad 1].V_{B_{1a}} \end{aligned}$$

Theorem 6. *The decomposition matrix of B_{1a}. is the following.*

(1)			
	θ_1	1	0
	θ_2	0	1
	θ_3	1	1

Proof: This is immediate from lemma 5 □

Decomposition numbers of K

3.8 Characteristic 3

There are 1 conjugacy classes of cyclic groups 3a of order 3 in K. The order of centralizer of this cyclic group is 3. In K, there are 2 blocks with defect 0, and one block C_{1a} of defect 1. The indices of simple projective characters are { 2 and 3}.

Lemma 7. *The block C_{1a} contains the following irreducible characters*

$$V_{C_{1a}} = {}^t[\quad \phi_1, \phi_4, \phi_5]$$

The next lemma is just obtained by GAP.

Lemma 8. *There are the following projective characters in C_{1a}.*

$$\begin{aligned}\widetilde{\phi_1} &= [\ 1,\ 0,\ 1].V_{C_{1a}}\\ \widetilde{\phi_4} &= [\ 0,\ 1,\ 1].V_{C_{1a}}\end{aligned}$$

Theorem 9. *The decomposition matrix of C_{1a}. is the following.*

(1)

ϕ_1	1	0
ϕ_4	0	1
ϕ_5	1	1

Proof: This is immediate from lemma 8 □

Decomposition numbers of L

3.9 Characteristic 3

There are 1 conjugacy classes of cyclic groups 3a of order 3 in L. The order of centralizer of this cyclic group is 3. In L, there are 2 blocks with defect 0, and one block D_{1a} of defect 1. The indices of simple projective characters are { 4 and 5}.

Lemma 10. *The block D_{1a} contains the following irreducible characters*

$$V_{D_{1a}} = {}^t[\ \ \zeta_1, \zeta_2, \zeta_3]$$

The next lemma is just obtained by GAP.

Lemma 11. *There are the following projective characters in D_{1a}.*

$$\begin{aligned}\widetilde{\zeta_1} &= [\ 1,\ 0,\ 1].V_{D_{1a}}\\ \widetilde{\zeta_2} &= [\ 0,\ 1,\ 1].V_{D_{1a}}\end{aligned}$$

Theorem 12. *The decomposition matrix of D_{1a}. is the following.*

(1)

ζ_1	1	0
ζ_2	0	1
ζ_3	1	1

Proof: This is immediate from lemma 11 □

Decomposition numbers of M

3.10 Characteristic 3

There are 2 conjugacy classes of cyclic groups 3a and 3b of order 3 in M. The orders of centralizers of these cyclic groups are 9 and 9. In M, there are one block E_{1a} of defect 1, and one block E_{2a} of defect 2.

Lemma 13. *The block E_{2a} contains the following irreducible characters*

$$V_{E_{2a}} = {}^t[\ \ \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6]$$

The next lemma is just obtained by GAP.

Lemma 14. *There are the following projective characters in E_{2a}.*

$$\begin{aligned}(\widetilde{\chi_{6M}}).E_{2a} &= [\ 1,\ 0,\ 0,\ 0,\ 1,\ 1].V_{E_{2a}}\\ ((\widetilde{\chi_{6M}}).E_{2a}\otimes\xi_2).E_{2a} &= [\ 0,\ 1,\ 0,\ 0,\ 1,\ 1].V_{E_{2a}}\\ ((\widetilde{\chi_{6M}}).E_{2a}\otimes\xi_3).E_{2a} &= [\ 0,\ 0,\ 1,\ 0,\ 1,\ 1].V_{E_{2a}}\\ ((\widetilde{\chi_{6M}}).E_{2a}\otimes\xi_4).E_{2a} &= [\ 0,\ 0,\ 0,\ 1,\ 1,\ 1].V_{E_{2a}}\end{aligned}$$

Theorem 15. *The decomposition matrix of E_{2a}. is the following.*

(1)

ξ_1	1	0	0	0
ξ_2	0	1	0	0
ξ_3	0	0	1	0
ξ_4	0	0	0	1
ξ_5	1	1	1	1
ξ_6	1	1	1	1

Proof: This is immediate from lemma 14 □

Decomposition numbers of X

3.11 Characteristic 3

There are 1 conjugacy classes of cyclic groups 3a of order 3 in X. The order of centralizer of this cyclic group is 3. In X, there are 2 blocks with defect 0, and one block F_{1a} of defect 1. The indices of simple projective characters are { 2 and 3}.

Lemma 16. *The block F_{1a} contains the following irreducible characters*

$$V_{F_{1a}} = {}^t[\ \ \sigma_1, \sigma_4, \sigma_5]$$

The next lemma is just obtained by GAP.

Lemma 17. *There are the following projective characters in F_{1a}.*

$$\begin{aligned}\widetilde{\sigma_1} &= [\ 1,\ 0,\ 1].V_{F_{1a}}\\ \widetilde{\sigma_4} &= [\ 0,\ 1,\ 1].V_{F_{1a}}\end{aligned}$$

Theorem 18. *The decomposition matrix of F_{1a}. is the following.*

(1)

σ_1	1	0
σ_4	0	1
σ_5	1	1

Proof: This is immediate from lemma 17 □

参考文献

[1] http://www.math.rwth-aachen.de/~MOC/CoMoChaT/

Asirによるアフィン頂点作用素代数の計算

山田裕理
一橋大学大学院経済学研究科

1 はじめに

頂点作用素代数 (vertex operator algebra, VOA) の部分代数は、興味深い研究対象である．与えられた頂点作用素代数に対して、その部分代数の代表的な構成法として、次の 2 つがある．

1. 頂点作用素代数の有限位数の自己同型により固定されるベクトル全体は、部分代数になる．このような部分代数を、オービフォールドという．

2. ひとつの部分代数の commutant もまた、部分代数になる．これを、コセット構成法と呼ぶ．

実際、良く知られた頂点作用素代数から出発して、オービフォールドあるいはコセット構成法を考えることにより、様々な頂点作用素代数が構成されてきた．

本稿では、最も基本的な頂点作用素代数である $A_1^{(1)}$ 型アフィン頂点作用素代数をもとにして、コセット構成法により得られるある種の W-代数を考察する．最終的な目標は、この W-代数の既約加群を分類することであるが、ここでは、その準備として、特異ベクトルに関して得られた結果を紹介する．詳しいことは、Chongying Dong, Ching Hung Lam との共著論文 [3] を参照してください．なお、この研究の動機は [4, Chapter 14], [8] である．

頂点作用素代数の計算は複雑なため、計算機が必要になる場合がある．今回の計算では、計算機代数システム Asir を用いた．Asir による計算については、田辺顕一朗氏、横山和弘氏に様々な助言をいただいた。厚く御礼申し上げる次第である．

2 $\widehat{sl}_2$ のレベル ℓ Verma 加群 $V(\ell, 0)$

$\mathbb{C}$ 上のリー代数 sl_2 から始める．$[\cdot,\cdot]$ をブラケット積、$\langle\cdot,\cdot\rangle$ を正規化された Killing form、$\{h, e, f\}$ を sl_2 の Chevalley 基底とする．

$$\begin{gathered}[h,e] = 2e, \quad [h,f] = -2f, \quad [e,f] = h, \\ \langle h,h\rangle = 2, \quad \langle e,f\rangle = 1, \\ \langle h,e\rangle = \langle h,f\rangle = \langle e,e\rangle = \langle f,f\rangle = 0\end{gathered} \tag{2.1}$$

である．$A_1^{(1)}$ 型アフィンリー代数 $\widehat{sl}_2$ は、ベクトル空間として、

$$\widehat{sl}_2 = sl_2 \otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}C \tag{2.2}$$

で定義される．ここで、C は単なる記号である．$\widehat{sl}_2$ の標準的な基底として、

$$h \otimes t^n, \quad e \otimes t^n, \quad f \otimes t^n, \quad C \quad (n \in \mathbb{Z})$$

を考える．$\widehat{sl}_2$ におけるブラケット積は、

$$[a \otimes t^m, b \otimes t^n] = [a, b] \otimes t^{m+n} + m\langle a, b\rangle \delta_{m+n,0} C \tag{2.3}$$

(ただし $a, b \in \{h, e, f\},\ m, n \in \mathbb{Z}$)、および

$$[\widehat{sl}_2, C] = 0 \tag{2.4}$$

で与えられる．$\mathbb{C}C$ は、$\widehat{sl}_2$ の中心である．

$\ell \in \mathbb{C}$ をひとつ定める．$V(\ell, 0)$ を、$\widehat{sl}_2$ のレベル ℓ Verma 加群とする．$V(\ell, 0)$ は、$\widehat{sl}_2$ の加群として、真空ベクトル $\mathbf{1} \in V(\ell, 0)$ で生成される．$a \otimes t^n$ の $V(\ell, 0)$ への作用が引き起こす $V(\ell, 0)$ の線型作用素を、$a(n)$ で表すことにする．真空ベクトル $\mathbf{1}$ は、次の 2 つの性質をみたす.

(1) $a(n)\mathbf{1} = 0$; $n \geq 0$, $a \in \{h, e, f\}$.

(2) $C \cdot \mathbf{1} = \ell\mathbf{1}$; すなわち、$C$ は $\mathbf{1}$ に ℓ 倍として作用する.

線型作用素 $a(m)$ と $b(n)$ の交換関係、すなわち、$[f, g] = fg - gf;\ f, g \in \operatorname{End} V(\ell, 0)$ は、(2.3) により

$$[a(m), b(n)] = [a, b](m + n) + m\langle a, b\rangle \ell \delta_{m+n,0} \tag{2.5}$$

なので、(2.1) により

$$\begin{aligned}
[h(m), h(n)] &= m \cdot 2\ell\delta_{m+n,0}, \\
[h(m), e(n)] &= 2e(m + n), \\
[h(m), f(n)] &= -2f(m + n), \\
[e(m), f(n)] &= h(m + n) + m \cdot \ell\delta_{m+n,0}, \\
[e(m), e(n)] &= [f(m), f(n)] = 0
\end{aligned} \tag{2.6}$$

が成り立つ.

$V(\ell, 0)$ は、真空ベクトル $\mathbf{1}$ から、$h(m)$, $e(m)$, $f(m)$; $m < 0$ により自由に生成される．したがって、

$$\begin{gathered}
h(-i_1) \cdots h(-i_p) e(-j_1) \cdots e(-j_q) f(-m_1) \cdots f(-m_r)\mathbf{1}; \\
i_1 \geq \cdots \geq i_p \geq 1, \quad j_1 \geq \cdots \geq j_q \geq 1, \quad m_1 \geq \cdots \geq m_r \geq 1
\end{gathered} \tag{2.7}$$

は、$V(\ell,0)$ の標準的な基底になる．上の形のベクトルについて、そのウエイトを

$$i_1+\cdots+i_p+j_1+\cdots+j_q+m_1+\cdots+m_r$$

と定義する．なお、零ベクトルのウエイトは任意とする．

(2.7) の形のベクトルのうち、ウエイトが n のもの全部で張られる部分空間を $V(\ell,0)_{(n)}$ で表し、ウエイト n の部分空間と呼ぶ．$V(\ell,0)_{(n)}$ の次元の母関数は、

$$\begin{aligned}&\sum_{n=0}^{\infty}\bigl(\dim V(\ell,0)_{(n)}\bigr)q^n\\&\quad=\frac{1}{\prod_{i=1}^{\infty}(1-q^i)^3}\\&\quad=1+3q+9q^2+22q^3+51q^4+108q^5+221q^6\\&\qquad+429q^7+810q^8+1479q^9+\cdots\end{aligned}$$

である．これを、$V(\ell,0)$ の q-指標という．

$V(\ell,0)$ における計算の簡単な例を 2 つ紹介する．どちらも、(2.5) と真空ベクトル $\mathbf{1}$ の性質から、容易に計算できる．

$$\begin{aligned}a(0)b(-1)\mathbf{1}&=\bigl([a(0),b(-1)]+b(-1)a(0)\bigr)\mathbf{1}\\&=[a(0),b(-1)]\mathbf{1}\\&=[a,b](-1)\mathbf{1},\end{aligned}$$

$$\begin{aligned}a(1)b(-1)\mathbf{1}&=\bigl([a(1),b(-1)]+b(-1)a(1)\bigr)\mathbf{1}\\&=[a(1),b(-1)]\mathbf{1}\\&=\bigl([a,b](0)+\langle a,b\rangle\ell\bigr)\mathbf{1}\\&=\langle a,b\rangle\ell\mathbf{1}.\end{aligned}$$

3 $V(\ell,0)$ の VOA 構造

ベクトル $v\in V(\ell,0)$ に対して、頂点作用素と呼ばれる $V(\ell,0)$ の線型作用素の母関数

$$Y(v,x)=\sum_{n\in\mathbb{Z}}v_nx^{-n-1},\quad v_n\in\operatorname{End}V(\ell,0)$$

を、次のように定義する．ただし、x は形式的な変数である．$a^i\in\{h,e,f\}$ に対して、

$$\begin{aligned}&Y(a^1(-m_1)\cdots a^r(-m_r)\mathbf{1},x)\\&\quad=a^1(x)_{-m_1}a^2(x)_{-m_2}\cdots a^r(x)_{-m_r}1\\&\quad=a^1(x)_{-m_1}\bigl(a^2(x)_{-m_2}\cdots a^r(x)_{-m_r}1\bigr).\end{aligned}\tag{3.1}$$

1 は $V(\ell,0)$ の恒等変換を表す.

ここで用いられている記号の意味は、以下のとおりである.

$$a(x)=\sum_{n\in\mathbb{Z}}a(n)x^{-n-1}$$

について、

$$a(x)^-=\sum_{n<0}a(n)x^{-n-1},\qquad a(x)^+=\sum_{n\geq 0}a(n)x^{-n-1}$$

とおく.

$$:a(x)b(x):=a(x)^-b(x)+b(x)a(x)^+ \tag{3.2}$$

を、$a(x)$ と $b(x)$ の正規積と呼ぶ.

2つの無限和 $a(x),b(x)$ の積 $a(x)b(x)$ は、定義できない. しかし、任意に $v\in V(\ell,0)$ が与えられたとき、十分大きいすべての m に対して

$$a(m)v=0$$

となるので、どのような n についても、$:a(x)b(x):v$ の x^{-n-1} の係数は、$V(\ell,0)$ のベクトルの有限和として定まる. この意味で、$a(x)$ と $b(x)$ の正規積 $:a(x)b(x):$ は、$V(\ell,0)$ の線型作用素の母関数として定義できる.

一般に、$a^1(x),\dots,a^r(x)$ の正規積は、

$$\begin{aligned}&:a^1(x)a^2(x)\cdots a^r(x):\\&\quad=:a^1(x)\big(a^2(x)\cdots a^r(x)\big):\\&\quad=a^1(x)^-:a^2(x)\cdots a^r(x):+:a^2(x)\cdots a^r(x):a^1(x)^+\end{aligned} \tag{3.3}$$

として定義される.

$a(x)=\sum_{n\in\mathbb{Z}}a(n)x^{-n-1}$ の微分は、

$$\frac{d}{dx}a(x)=\sum_{n\in\mathbb{Z}}(-n-1)a(n)x^{-n-2}$$

である.

$a(x),b(x)$ および正の整数 m に対して、

$$a(x)_{-m}b(x)=\frac{1}{(m-1)!}:\Big(\big(\frac{d}{dx}\big)^{m-1}a(x)\Big)b(x):$$

とおく. 以上で、(3.1) の右辺に現れる記号の意味がわかった.

ここに出てきた記号について、いくつかの注意をする．x を変数とする母関数 $P(x)$ に対して、x の非負べきの項の部分 (すなわち正則部分) を $P(x)^-$ で表し、x の負べきの項の部分 (すなわち特異部分) を $P(x)^+$ で表す．微分について、

$$\big(\frac{d}{dx}P(x)\big)^{\pm} = \frac{d}{dx}(P(x)^{\pm})$$

が成り立つ．また、$b(x) = 1$; 恒等変換のとき、$a(x)_{-m}b(x)$ は、

$$a(x)_{-m}1 = \big(\frac{d}{dx}\big)^{m-1}a(x)$$

となる．特に、$a(x)_{-1}1 = a(x)$ である．

例として、$v = a(-1)b(-1)\mathbf{1}$ の場合に、$Y(v,x) = \sum_{n\in\mathbb{Z}} v_n x^{-n-1}$ の計算を示す．定義に従って計算すると、

$$\begin{aligned}
&Y(a(-1)b(-1)\mathbf{1},x)\\
&\quad = a(x)_{-1}b(x)_{-1}\mathbf{1}\\
&\quad = a(x)_{-1}b(x)\\
&\quad = {}^{\circ}_{\circ}a(x)b(x){}^{\circ}_{\circ}\\
&\quad = a(x)^-b(x) + b(x)a(x)^+\\
&\quad = \sum_{i<0}\sum_{j\in\mathbb{Z}} a(i)b(j)x^{-i-j-2} + \sum_{j\in\mathbb{Z}}\sum_{i\geq 0} b(j)a(i)x^{-i-j-2}
\end{aligned}$$

となる．これより、$Y(a(-1)b(-1)\mathbf{1},x)$ における x^{-n-1} の係数 $(a(-1)b(-1)\mathbf{1})_n$ は、

$$(a(-1)b(-1)\mathbf{1})_n = \sum_{i<0} a(i)b(n-i-1) + \sum_{i\geq 0} b(n-i-1)a(i)$$

であることがわかる．

$Y(v,x)$; $v \in V(\ell,0)$ は、Jacobi identity と呼ばれるある種の関係式をみたす．$V(\ell,0)$ と $Y(\,\cdot\,,x) : V(\ell,0) \to (\mathrm{End}\, V(\ell,0))[[x,x^{-1}]]$ に、真空ベクトル $\mathbf{1}$ を加えた組 $(V(\ell,0),Y,\mathbf{1})$ を、$A_1^{(1)}$ 型アフィン頂点代数 (vertex algebra) という．

頂点作用素代数の定義には、さらに共形元が必要である．そのために、$\ell \neq -2$ と仮定する．このとき、共形元 ω_{aff} は、

$$\omega_{\mathrm{aff}} = \frac{1}{2(\ell+2)}\Big(-h(-2)\mathbf{1} + \frac{1}{2}h(-1)^2\mathbf{1} + 2e(-1)f(-1)\mathbf{1}\Big)$$

で与えられる．その中心電荷は、$3\ell/(\ell+2)$ である．ω_{aff} も合わせて、$(V(\ell,0),Y,\mathbf{1},\omega_{\mathrm{aff}})$ は頂点作用素代数になる．これを、$A_1^{(1)}$ 型アフィン頂点作用素代数という ([6], [9, Section 6.2]).

ℓ が正の整数のとき、$V(\ell,0)$ は単純な頂点作用素代数ではなく、唯一つの自明でない極大イデアル $I(\ell,0)$ を持つ．剰余代数 $\mathcal{L}_{\widehat{sl}_2}(\ell,0)=V(\ell,0)/I(\ell,0)$ を、単純 $A_1^{(1)}$ 型アフィン頂点作用素代数という．$I(\ell,0)$ は、

$$e(-1)^{\ell+1}\mathbf{1}$$

で生成されることが知られている ([7]).

4 Asir による計算

$v,u\in V(\ell,0)$ と $n\in\mathbb{Z}$ について、v_nu を計算したい．前節で説明したように、与えられた v,u,n に対して v_nu を計算する具体的なアルゴリズムは、定義から直ちにわかる．しかし、必要となる計算は複雑であり、手計算で実行するのは現実的ではない．そこで、計算機代数システム Asir を用いて計算する．以下 $2\le\ell\in\mathbb{Z}$ をひとつ固定する．

アルゴリズムは明確に与えられているので、計算機で計算するためには、データをどのような形で扱うのかを考えればよい．ここでは、リストを用いて $V(\ell,0)$ のベクトルを表すことにする．リストによる表示として、次の 3 種類を扱う．

Expression in Asir

• terms without coefficients:
$h(m)\mathbf{1}\leftrightarrow$ `[[0,m]]`,
$e(m)\mathbf{1}\leftrightarrow$ `[[1,m]]`,
$f(m)\mathbf{1}\leftrightarrow$ `[[2,m]]`,

$a^1(m_1)\cdots a^r(m_r)\mathbf{1}\leftrightarrow$ `[[p1,m1]`, ... , `[pr,mr]]`,
where `pi` is `0`, `1`, or `2` according as $a^i=h,e,$ or f.

$\mathbf{1}\leftrightarrow$ `[]`; empty list.

例 $h(-2)\mathbf{1}\leftrightarrow$ `[[0,-2]]`, $h(-2)e(-1)\mathbf{1}\leftrightarrow$ `[[0,-2],[1,-1]]`.

• terms with coefficients: `[` term, coeff `]`;

例 $5h(-2)\mathbf{1}\leftrightarrow$ `[[[0,-2]],5]`,
$4h(-2)e(-1)\mathbf{1}\leftrightarrow$ `[[[0,-2],[1,-1]],4]`,
$3\mathbf{1}\leftrightarrow$ `[[],3]`.

• sum of terms with coefficients (each term is of the same weight):
`[[` term, coeff `]`, ... , `[` term, coeff `]]`;

例 $4h(-2)e(-1)\mathbf{1}+5e(-1)e(-1)f(-1)\mathbf{1}$

$\leftrightarrow$ `[[[[0,-2],[1,-1]],4],[[[1,-1],[1,-1],[2,-1]],5]]`.

また、$v_n u$ を計算する関数 `action(M,L,N)` を用意する.

Function `action(M,L,N)`

Input: `M`, `L`; lists of terms with coefficients, `N`; an integer.

Output: a list of terms with coefficients.

$v \leftrightarrow$ `M`, $u \leftrightarrow$ `L`, $n \leftrightarrow$ `N`,
$v_n u \leftrightarrow$ `action(M,L,N)`.

5 結果

頂点作用素代数 $V(\ell, 0)$ において、

$$\omega_\gamma = \frac{1}{4\ell} h(-1)^2 \mathbf{1}$$

は、中心電荷 1 のヴィラソロ元であり、ω_γ で生成される $V(\ell, 0)$ の部分代数 $\mathrm{Vir}(\omega_\gamma)$ は、中心電荷 1 のヴィラソロ頂点作用素代数になる. $\mathrm{Vir}(\omega_\gamma)$ の $V(\ell, 0)$ における commutant を $\widetilde{\mathcal{W}}$ とおく.

$$\widetilde{\mathcal{W}} = \{v \in V(\ell, 0) \mid (\omega_\gamma)_0 v = 0\}.$$

$\widetilde{\mathcal{W}}$ は、物理学では $W(2,3,4,5)$ と表される W-代数として知られている ([1], [2], [5]). その共形元は、

$$\begin{aligned}\omega &= \omega_{\mathrm{aff}} - \omega_\gamma \\ &= \frac{1}{2\ell(\ell+2)} \Big(- \ell h(-2)\mathbf{1} - h(-1)^2 \mathbf{1} + 2\ell e(-1) f(-1)\mathbf{1} \Big)\end{aligned}$$

で、中心電荷は $3\ell/(\ell+2) - 1 = 2(\ell-1)/(\ell+2)$ である.

$\widetilde{\mathcal{W}}$ は、頂点作用素代数として 1 個のウエイト 3 のベクトル

$$\begin{aligned}W^3 = {} & \ell^2 h(-3)\mathbf{1} + 3\ell h(-2)h(-1)\mathbf{1} + 2h(-1)^3\mathbf{1} \\ & - 6\ell h(-1)e(-1)f(-1)\mathbf{1} + 3\ell^2 e(-2)f(-1)\mathbf{1} - 3\ell^2 e(-1)f(-2)\mathbf{1}\end{aligned}$$

で生成される. しかし、作用素積展開を記述するためには、W^3 のほかに、ウエイトが 4 のベクトル W^4 とウエイトが 5 のベクトル W^5 も必要になる. W^3, W^4, W^5 は、共形元 ω に関する特異ベクトルとして、それぞれのウエイト部分空間において定数倍を除いて一意的に定まる. ちなみに、共形元 ω のウエイトは 2 であるが、$W(2,3,4,5)$

という記号は、ω, W^3, W^4, W^5 というウエイトが 2, 3, 4, 5 のベクトルを用いて記述されることを意味している．

作用素積展開、すなわち $W_n^iW^j$, $3 \le i \le j \le 5$, $0 \le n \le i+j-1$ を、ω, W^3, W^4, W^5 を用いて表すことは、頂点作用素代数 $\widetilde{\mathcal{W}}$ の性質を調べる上で、きわめて大切である．今回、Asir により計算することで、作用素積展開をすべて求めることができた．

$$L(n) = \omega_{n+1}, \quad W^i(n) = W^i_{i+n-1};\ i = 3, 4, 5$$

とおく．$W_1^3W^3$ について結果を書くと、次のようになる．

$$\begin{aligned} W_1^3W^3 = &-\big(162\ell^3(\ell-2)(\ell+2)(3\ell+4)/(16\ell+17)\big)\omega_{-3}\mathbf{1} \\ &+ \big(288\ell^3(\ell-2)(\ell+2)^2(3\ell+4)/(16\ell+17)\big)\omega_{-1}\omega \\ &+ \big(36\ell(2\ell+3)/(16\ell+17)\big)W^4. \end{aligned}$$

これからわかるように、$W_1^3W^3$ を記述するには W^4 が必要である．同様に、

$$\begin{aligned} W_1^3W^4 = &\big(1248\ell^2(\ell-3)(\ell+2)(2\ell+1)(2\ell+3)/(64\ell+107)\big)\omega_{-1}W^3 \\ &- \big(48\ell^2(\ell-3)(2\ell+1)(2\ell+3)(2\ell+7)/(64\ell+107)\big)W^3_{-3}\mathbf{1} \\ &- \big(12\ell(3\ell+4)(16\ell+17)/(64\ell+107)\big)W^5. \end{aligned}$$

となり、$W_1^3W^4$ を記述するのに W^5 が必要になることがわかる．

他の場合は省略するが、$W_n^iW^j$ がわかれば、線型作用素 $W^i(m)$ と $W^j(n)$ の交換関係 $[W^i(m), W^j(n)] = W^i(m)W^j(n) - W^j(n)W^i(m)$ がわかるので、$\widetilde{\mathcal{W}}$ における様々な計算が可能になる．たとえば、$\widetilde{\mathcal{W}}$ がベクトル空間として、

$$\begin{aligned} &L(-i_1)\cdots L(-i_p)W^3(-j_1)\cdots W^3(-j_q) \\ &\quad W^4(-m_1)\cdots W^4(-m_r)W^5(-n_1)\cdots W^5(-n_s)\mathbf{1}; \\ &\qquad i_1 \ge \cdots \ge i_p \ge 2, \quad j_1 \ge \cdots \ge j_q \ge 3, \\ &\qquad m_1 \ge \cdots \ge m_r \ge 4, \quad n_1 \ge \cdots \ge n_s \ge 5 \end{aligned} \tag{5.1}$$

で張られることも、作用素積展開からわかる．

(5.1) の形のベクトルを正規形と呼ぶことにする．ウエイト n の正規形のベクトルの個数を q^n の係数とする母関数は、

$$\begin{aligned} &\sum_{n=0}^{\infty}(\text{number of vecters of normal form of weight } n)q^n \\ &\quad = \prod_{r=2}^{5}\frac{1}{\prod_{i=r}^{\infty}(1-q^i)} \\ &\quad = 1 + q^2 + 2q^3 + 4q^4 + 6q^5 + 11q^6 + 16q^7 + 29q^8 + 44q^9 + \cdots \end{aligned}$$

である．一方、$\widetilde{\mathcal{W}}$ の q-指標は

$$\begin{aligned}&\sum_{n=0}^{\infty}(\dim \widetilde{\mathcal{W}}_{(n)})q^n\\ &\quad=\frac{\sum_{r=0}^{\infty}(-1)^r q^{r(r+1)/2}-q\sum_{r=0}^{\infty}(-1)^r q^{r(r+1)/2+r}}{\prod_{i=1}^{\infty}(1-q^i)^2}\\ &\quad=1+q^2+2q^3+4q^4+6q^5+11q^6+16q^7+27q^8+40q^9+\cdots\end{aligned}$$

であることが知られている ([1])．

これらの差は、

$$\begin{aligned}&\sum_{n=0}^{\infty}(\text{number of vecters of normal form of weight } n)q^n-\sum_{n=0}^{\infty}(\dim \widetilde{\mathcal{W}}_{(n)})q^n\\ &\quad=2q^8+4q^9+\cdots\end{aligned}$$

となるので、$\widetilde{\mathcal{W}}$ のウエイト 8、あるいはウエイト 9 の部分空間には、正規形のベクトルにそれぞれ 2 個、あるいは 4 個の自明でない独立な線型関係があることがわかる．

実は、自明でない線型関係は、$\widetilde{\mathcal{W}}$ の特異ベクトルと対応する．特に、$\widetilde{\mathcal{W}}$ にはウエイトが 7 以下の特異ベクトルは存在しない．一般に、頂点作用素代数の既約表現の分類などのために、特異ベクトルの情報はきわめて有用である．

最後に、今回得られた結果をまとめておく．

1. $\widetilde{\mathcal{W}}$ の作用素積展開、すなわち $W_n^i W^j$, $3\le i\le j\le 5$, $0\le n\le i+j-1$ を計算した．

2. $\widetilde{\mathcal{W}}$ のウエイトが 8 と 9 の特異ベクトルをすべて決定した．

注意 $\widetilde{\mathcal{W}}$ も、$V(\ell,0)$ と同様に単純な頂点作用素代数ではない．$V(\ell,0)$ の唯一つの極大イデアル $I(\ell,0)$ は $e(-1)^{\ell+1}\mathbf{1}$ で生成されるが、$e(-1)^{\ell+1}\mathbf{1}$ は $\widetilde{\mathcal{W}}$ には含まれない．しかし、

$$f(0)^{\ell+1}e(-1)^{\ell+1}\mathbf{1}$$

は、$\widetilde{\mathcal{W}}$ に含まれることが知られている ([3])．実は、$\widetilde{\mathcal{W}}$ の唯一つの極大イデアル $\widetilde{\mathcal{I}}$ は、このベクトルで生成されることが予想される．我々は、剰余代数 $\mathcal{W}=\widetilde{\mathcal{W}}/\widetilde{\mathcal{I}}$ に興味がある．$\ell=2,3,4$ の場合、$\mathcal{W}$ は良く知られている頂点作用素代数に同型である．$f(0)^{\ell+1}e(-1)^{\ell+1}\mathbf{1}$ のウエイトが ℓ に依存するため、一般の ℓ に対して計算機で計算することは困難である．一方、小さい ℓ が具体的に与えられている場合には、計算機が使える．実際、$\ell=5,6$ の場合について、Asir を用いて $\widetilde{\mathcal{I}}$ を計算することにより、$\mathcal{W}$ の既約表現を分類した ([3])．

参考文献

[1] R. Blumenhagen, W. Eholzer, A. Honecker, K. Hornfeck and R. Hübel, Coset realization of unifying W-algebras, *Internat. J. Modern Physics* **A 10** (1995), 2367–2430.

[2] A. Cappelli, L. S. Georgiev and I. T. Todorov, Parafermion Hall states from coset projections of abelian conformal theories, *Nuclear Physics* **B 599** (2001), 499–530.

[3] C. Dong, C.H. Lam and H. Yamada, W-algebras in lattice vertex operator algebras, preprint.

[4] C. Dong and J. Lepowsky, The algebraic structure of relative twisted vertex operators, *J. Pure and Applied Algebra* **110**(1996), 259–295.

[5] K. Hornfeck, W-algebras with set of primary fields of dimensions $(3, 4, 5)$ and $(3, 4, 5, 6)$, *Nuclear Physics* **B 407** (1993), 237–246.

[6] I. B. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Math. J.* **66** (1992), 123–168.

[7] V. G. Kac, *Infinite-dimensional Lie Algebras* 3rd ed., Cambridge University Press, Cambridge, 1990.

[8] C. H. Lam and H. Yamada, Decomposition of the lattice vertex operator algebra $V_{\sqrt{2}A_l}$, *J. Algebra* **272** (2004), 614–624.

[9] J. Lepowsky and H.-S Li, *Introduction to Vertex Operator Algebras and Their Representations*, Birkhäuser, Boston, 2004.

A New Example of Non-Amorphous Association Schemes on $\mathrm{GF}(2^{20})$

Takuya Ikuta
Faculty of Law, Kobe Gakuin University, Minatojima, Chuo-ku, Kobe, 650-8586 Japan
ikuta@law.kobegakuin.ac.jp

Akihiro Munemasa
Graduate School of Information Sciences, Tohoku University, Aramaki-Aza-Aoba, Aoba-ku, Sendai, 980-8579 Japan
munemasa@math.is.tohoku.ac.jp

Let X be a finite set with n elements, and R be a relation on X. Let $\Gamma = (X, R)$ be a graph with the vertex set X and the edge set R. For a graph $\Gamma = (X, R)$, the size of the set $\{y \in X \mid (x, y) \in R\}$ is called the valency $k(x)$ of $x \in X$. If this number $k(x)$ is independent of the choice of $x \in X$, $\Gamma = (X, R)$ is said to be regular of valency k.

Definition 1. $\Gamma = (X, R)$ is said to be a strongly regular graph of valency k if there exist constants $\lambda \geq 0$ and $\mu > 0$ such that every pair of adjacent (resp. non-adjacent) vertices has λ (resp. μ) common neighbours.

A connected regular graph has its valency as the Perron–Frobenius eigenvalue. We call all the other eigenvalues *nontrivial* eigenvalues of the graph. Strongly regular graphs are regular graphs with exactly two nontrivial eigenvalues.

Example 1. Let α be a primitive element of the finite field GF(16) of 16 elements. Let Γ be the graph with vertex set GF(16), where two vertices x, y are adjacent whenever $x - y \in \langle \alpha^3 \rangle$. Then Γ is a strongly regular graph with $(k, \lambda, \mu) = (5, 0, 2)$.

Example 2 (Brouwer–Wilson–Xiang, 1999). Let $q = p^s$ be a prime power, where p is a prime. Let e be a divisor of $q - 1$ such that $e \mid p^r + 1$ for some $r < s$ and $\frac{q-1}{e} \nmid p^r - 1$ for any $r < s$. Then $(\mathrm{GF}(q), \langle \alpha^e \rangle)$ is a strongly regular graph.

Definition 2. Let $\{R_i\}_{i=0}^d$ be a set of $d + 1$ relations on X. Let A_i be the adjacency matrix corresponding to R_i for $i = 0, \ldots, d$. $(X, \{R_i\}_{i=0}^d)$ is called an association scheme of class d on X if the following conditions are satisfied:

(i) $A_0 = I$,

(ii) $\sum_{i=0}^d A_i = J$ (all 1 matrix),

(iii) for all $i \in \{0, 1, \ldots, d\}$, ${}^t A_i = A_i$.

(iv) for all $i, j \in \{0, 1, \ldots, d\}$, $A_i A_j$ is expressed as

$$A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k,$$

where p_{ij}^k are nonnegative integers.

We call the algebra $\mathfrak{A} = \langle A_0, A_1, \ldots, A_d \rangle$ generated by $A_0, A_1, \ldots, A_d$ the Bose-Mesner algebra for $(X, \{R_i\}_{i=0}^d)$. Since $\mathfrak{A}$ is semi-simple, there exists uniquely the set $\{E_i\}_{i=0}^d$ of the primitive idempotents of $\mathfrak{A}$ with $E_0 = n^{-1}J$, that is, $\mathfrak{A}$ has two bases:

$$\mathfrak{A} = \langle A_0, A_1, \ldots, A_d \rangle = \langle E_0, E_1, \ldots, E_d \rangle.$$

We define the first eigenmatrix $P = (p_{i,j})_{\substack{0 \le i \le d \\ 0 \le j \le d}}$ and the second eigenmatrix $Q = (q_{i,j})_{\substack{0 \le i \le d \\ 0 \le j \le d}}$ of $(X, \{R_i\}_{i=0}^d)$ as follows:

$$\begin{aligned} (A_0, A_1, \ldots, A_d) &= (E_0, E_1, \ldots, E_d) \cdot P, \\ (E_0, E_1, \ldots, E_d) &= n^{-1}(A_0, A_1, \ldots, A_d) \cdot Q. \end{aligned}$$

The first eigenmatix P and the second eigenmatix Q have the following forms:

$$P = \left(\begin{array}{c|ccc} 1 & k_1 & \ldots & k_d \\ \hline 1 & & & \\ \vdots & & p_{i,j} & \\ 1 & & & \end{array}\right) \quad \text{and} \quad Q = \left(\begin{array}{c|ccc} 1 & m_1 & \ldots & m_d \\ \hline 1 & & & \\ \vdots & & q_{i,j} & \\ 1 & & & \end{array}\right),$$

where k_i is the valency of R_i and $m_i = \mathrm{rank} E_i$.

An associaiton scheme is called *pseudocyclic* if $m_1 = \ldots = m_d$.

Let $\{\Lambda_j\}_{j=0}^{d'}$ be a partition of $\{0, 1, \ldots, d\}$ with $\Lambda_0 = \{0\}$. We define $R_{\Lambda_j} = \bigcup_{\ell \in \Lambda_j} R_\ell$. If $(X, \{R_{\Lambda_j}\}_{j=0}^{d'})$ forms an association scheme, then we call $(X, \{R_{\Lambda_j}\}_{j=0}^{d'})$ a *fusion* scheme of $(X, \{R_i\}_{i=0}^d)$. If $(X, \{R_{\Lambda_j}\}_{j=0}^{d'})$ is an association scheme for any partition $\{\Lambda_j\}_{j=0}^{d'}$ of $\{0, 1, \ldots, d\}$ with $\Lambda_0 = \{0\}$, then $(X, \{R_i\}_{i=0}^d)$ is called *amorphous*.

There is a simple criterion in terms of P for a given partition $\{\Lambda_j\}_{j=0}^{d'}$ to give rise to a fusion scheme (due to Bannai [1], Muzychuk [9]): There exists a partition $\{\Delta_i\}_{i=0}^{d'}$ of $\{0, 1, \ldots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j)-block of the first eigenmatrix P has a constant row sum. The constant row sum turns out to be the (i, j) entry of the 1st eigenmatrix of the fusion scheme.

Example 3. Let q be a prime power and e be a divisor of $q-1$. Fix a primitive element α of the multiplicative group of the finite field $\mathrm{GF}(q)$. Then $\langle \alpha^e \rangle$ is a subgroup of index e and its cosets are $\alpha^i \langle \alpha^e \rangle$ $(0 \le i \le e-1)$. We define $R_0 = \{(x, x) | x \in \mathrm{GF}(q)\}$ and $R_i = \{(x, y) | x - y \in \alpha^i \langle \alpha^e \rangle, x, y \in \mathrm{GF}(q)\}$ $(1 \le i \le e)$. Then $(\mathrm{GF}(q), \{R_i\}_{i=0}^e)$ forms an association scheme and is called the *cyclotomic* scheme of class e on $\mathrm{GF}(q)$.

In Example 3, the first eigenmatrix P of the cyclotomic scheme $(\mathrm{GF}(q), \{R_i\}_{i=0}^{e})$ of class e on $\mathrm{GF}(q)$ is calculated by the Gaussian periods. Let α be a primitive element of $\mathrm{GF}(q)$, and let χ denote an additive character of $\mathrm{GF}(q)$. The Gaussian periods $\eta_0, \ldots, \eta_{e-1}$ are defined by

$$\eta_j = \sum_{\beta \in \langle \alpha^e \rangle} \chi(\alpha^j \beta).$$

The first eigenmatrix of the cyclotomic scheme $(\mathrm{GF}(q), \{R_i\}_{i=0}^{e})$ is given by the following:

$$P = \left(\begin{array}{c|ccc} 1 & f & \cdots & f \\ \hline 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{array}\right),$$

where $q = ef + 1$, and

$$P_0 = \begin{pmatrix} \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{e-1} \\ \eta_1 & \eta_2 & & \cdots & \eta_0 \\ \eta_2 & \vdots & & & \eta_1 \\ \vdots & \vdots & & & \vdots \\ \eta_{e-1} & \eta_0 & \eta_1 & \cdots & \eta_{e-2} \end{pmatrix}.$$

We call P_0 the *principal part* of the first eigenmatrix P.

The cyclotomic scheme $(\mathrm{GF}(q), \{R_i\}_{i=0}^{e})$ is a pseudocyclic association scheme.

The next lemma is immediate from the result of [7].

Theorem 1. *A pseudocyclic association scheme of class e is amorphous if and only if the principal part P_0 of the first eigenmatrix P is a linear combination of I and J, where I is the identity matrix of size e and J is the all 1 matrix of size e.*

Baumert, Mills and Ward [3] gave a necessary and sufficient condition for a cyclotomic scheme to be amorphous.

Theorem 2 (Baumert–Mills–Ward). *Let e be a divisor of $q-1$, where $q = p^s$ and p is a prime. Let $(\mathrm{GF}(q), \{R_i\}_{i=0}^{e})$ be the cyclotomic scheme of class e on $\mathrm{GF}(q)$. Then, P_0 is the linear combination of I and J if and only if $e \mid p^r + 1$ for some $r < s$.*

Theorem 2 can be restated as follows.

Theorem 3. *Let e be a divisor of $q-1$, where $q = p^s$ and p is a prime. Let α be a primitive element of $\mathrm{GF}(q)$. Then $(\mathrm{GF}(q), \{(x,y) \mid x - y \in \bigcup_{i \in \Lambda} \langle \alpha^e \rangle \alpha^i)\})$ is strongly regular for all $\emptyset \neq \Lambda \subsetneq \{1, \ldots, e\}$ if and only if $e \mid p^r + 1$ for some $r < s$ and $e \nmid p^r - 1$ for any $r < s$.*

Clearly, in an amorphous association scheme, every nontrivial relation is a strongly regular graph. A. V. Ivanov [8] conjectured the converse also holds.

Conjecture 1 (A. V. Ivanov, [8]). If, in an association scheme, the graph defined by its adjacency matrices are all strongly regular, then it is amorphous.

This conjecture was disproved by van Dam [5]. Since the counterexample given in [5] was an imprimitive association scheme, it remained as an unsolved problem to find a primitive non-amorphous association scheme in which every nontrivial relation is a strongly regular graph.

In order to put this example in a proper context, we consider an association scheme whose eigenmatrix has principal part P_0 given by the following:

$$P_0 = \begin{pmatrix} s_1 & r_2 & r_2 & r_2 \\ r_1 & r_2 & s_2 & s_2 \\ r_1 & s_2 & r_2 & s_2 \\ r_1 & s_2 & s_2 & r_2 \end{pmatrix}. \tag{1}$$

If such an association scheme exists, then each of its four adjacency matrices defines a strongly regular graph (provided it is connected), so it gives a counterexample to Ivanov's conjecture.

Theorem 4. *Let A_1, A_2, A_3, A_4 be the adjacency matrices of an association scheme whose eigenmatrix has principal part given by* (1)*. Assume that the valency of A_1 is the multiplicity of the eigenvalue r_1. Then the size is $(30r+4)^2$ and*

$$\begin{aligned} k_1 &= 12(6r+1)(10r+1) = 12k_2, \\ s_1 &= -4(6r+1), \\ r_1 &= 6r, \\ s_2 &= -7r-1, \\ r_2 &= 8r+1. \end{aligned}$$

If we want to construct an association scheme satisfying the conditions of Theorem 4 over a finite field $\mathrm{GF}(q)$, then $q = (30r+4)^2$, hence $q = 2^{8h+4}$ for some nonnegative integer h, and $r = \frac{2}{15}(2^{4h}-1)$. If $h = 0$, then we obtain

$$P_0 = \begin{pmatrix} -4 & 1 & 1 & 1 \\ 0 & 1 & -1 & -1 \\ 0 & -1 & 1 & -1 \\ 0 & -1 & -1 & 1 \end{pmatrix}.$$

In this association scheme, the three graphs defined by A_2, A_3, A_4 are disconnected, so it does not give a counterexample. The case $h = 1$ corresponds to the first (and the only previously known) counterexample given by van Dam [5]. It is constructed as follows:

Let α be a primitive element of $\mathrm{GF}(2^{12})$, and let H be the subgroup of the multiplicative group of $\mathrm{GF}(2^{12})$ of index 45. Let

$$H_j = \{(x,y) \mid x - y \in \langle \alpha^{45} \rangle \alpha^j\} \quad (j = 0, 1, \ldots, 44).$$

We find that

$$\begin{aligned} R_2 &= H_0 \cup H_5 \cup H_{10}, \\ R_3 &= H_{15} \cup H_{20} \cup H_{25}, \\ R_4 &= H_{30} \cup H_{35} \cup H_{40} \end{aligned}$$

are strongly regular graphs with nontrivial eigenvalues $17, -15$. This leads to a non-amorphous 4-class fusion scheme of the cyclotomic scheme of class 45 on $\mathrm{GF}(2^{12})$ with the following first eigenmatrix:

$$\begin{pmatrix} 1 & 3276 & 273 & 273 & 273 \\ 1 & -52 & 17 & 17 & 17 \\ 1 & 12 & -15 & -15 & 17 \\ 1 & 12 & -15 & 17 & -15 \\ 1 & 12 & 17 & -15 & -15 \end{pmatrix}.$$

We have found an example for $h = 2$, as follows.

Theorem 5 (Ikuta–Munemasa). *Let α be a primitive element of $\mathrm{GF}(2^{20})$, and let H be the subgroup of the multiplicative group of $\mathrm{GF}(2^{20})$ of index 75. Let*

$$H_j = \{(x, y) \mid x - y \in \langle \alpha^{75} \rangle \alpha^j\} \quad (j = 0, 1, \ldots, 74).$$

We find that

$$\begin{aligned} R_2 &= H_0 \cup H_3 \cup H_6 \cup H_9 \cup H_{12}, \\ R_3 &= H_{25} \cup H_{28} \cup H_{31} \cup H_{34} \cup H_{37}, \\ R_4 &= H_{50} \cup H_{53} \cup H_{56} \cup H_{59} \cup H_{62} \end{aligned}$$

are strongly regular graphs with nontrivial eigenvalues $273, -239$. The cyclotomic scheme of class 75 on $\mathrm{GF}(2^{20})$ has a non-amorphous fusion scheme of class 4 with the following first eigenmatrix :

$$\begin{pmatrix} 1 & 838860 & 69905 & 69905 & 69905 \\ 1 & -820 & 273 & 273 & 273 \\ 1 & 204 & -239 & -239 & 273 \\ 1 & 204 & -239 & 273 & -239 \\ 1 & 204 & 273 & -239 & -239 \end{pmatrix}.$$

We present a Magma program to verify Theorem 5.

```
q:=2^20;
e:=75;
f:=(q-1) div e;
Z:=Integers();
K<a>:=GF(q);
a^20+a^10+a^9+a^7+a^6+a^5+a^4+a+1 eq 0;
b:=a^e;
w:=-1;
chi:=function(a) return w^(Z!Trace(a)); end function;
g:=[ &+[ chi(a^j*b^i) : i in {0..f-1} ]
   : j in [0..e-1] ];
g eq
   [541,29,29,-67,29,221,-67,-3,29,-67,221,-3,-67,-3,-3,29,29,29,
   -67,29,221,-67,-3,29,-67,221,-3,-67,-3,-3,29,29,29,-67,29,-291,
   -67,-3,29,-67,221,-3,-67,-3,-3,29,29,29,-67,29,221,-67,-3,29,
```

```
   -67,-291,-3,-67,-3,-3,29,29,29,-67,29,-291,-67,-3,29,-67,-291,
   -3,-67,-3,-3];
e:=75;
Z:=Integers();
Ze:=Set(Integers(e));
P0:=function(i,j) return g[(Z!(i+j))+1]; end function;
R2:={Ze|0,3,6,9,12};
R3:={Ze|i+25:i in R2};
R4:={Ze|i+50:i in R2};
R1:=Ze diff (R2 join R3 join R4);
{ [ &+[ P0(i,j) : j in R1 ], &+[ P0(i,j) : j in R2 ],
    &+[ P0(i,j) : j in R3 ], &+[ P0(i,j) : j in R4 ] ]
    : i in Ze }
    eq
    {
    [ -820, 273, 273, 273 ],
    [ 204, 273, -239, -239 ],
    [ 204, -239, 273, -239 ],
    [ 204, -239, -239, 273 ]
};
```

References

[1] E. Bannai *Subschemes of some association schemes*, J. Algebra, **144** (1991), 167–188.

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

[3] L.D. Baumert, W.H. Mills and R.L. Ward, *Uniform cyclotomy*, J. Number Theory **14** (1982), 67–82.

[4] A.E. Brouwer, R.M. Wilson, and Q. Xiang, *Cyclotomy and strongly regular graphs*, J. Algbraic Combin. **10** (1999), 25–28.

[5] E. R. van Dam, *Strongly regular decompositions of the complete graph*, J. Algraic Combin. **17** (2003), 181–201.

[6] T. Ito, A. Munemasa, and M. Yamada, *Amorphous association schemes over the Galois rings of characteristic* 4, Europ. J. Combin., **12** (1991), 513–526.

[7] A.V. Ivanov *Amorphous cellular rings II*, Investigations in the algebraic theory of combinatorial objects, Vsesoyuz. Nauchno-Issled. Inst. Sistem. Issled., Moscow, (1985), 39–49 (in Russian).

[8] A.A. Ivanov and C.E. Praeger, *Problem session at ALCOM-91*, Europ. J. Combin. **15** (1994), 105–112.

[9] M.E. Muzychuk, *V-rings of permutation groups with invariant metric*, Ph.D. thesis, Kiev State University, 1987.

Computation of the coset weight distributions of second order Reed-Muller code of length 64 (A joint research with Prof. K. Waki) 長さ64の 2nd order Reed-Muller 符号の coset weight distribution の計算

Michio Ozeki and Katsushi Waki
Hirosaki, Aomori
and
Department of Mathematical Sciences
Faculty of Science
Yamagata University
1-4-12, Koshirakawa-chou, Yamagata
Japan
email addresses : ozeki.mitio@ruby.plala.or.jp
waki@sci.kj.yamagata-u.ac.jp

5 Dec. 2007

1 Introduction

1.1 Standard Definitions from Binary Codes and the Statements of the problem

Let $\mathbf{F}_2 = GF(2)$ be the field of 2 elements. Let $V = \mathbf{F}_2^n$ be the vector space of dimension n over $\mathbf{F}_2$. A linear $[n, k]$ code $\mathbf{C}$ is a vector subspace of V of dimension k. An element $\mathbf{x}$ in $\mathbf{C}$ is called a codeword of $\mathbf{C}$. In V , the inner product , which is denoted by $(\mathbf{x}, \mathbf{y})$ for $\mathbf{x}, \mathbf{y}$ in V, is defined as usual. Two codes $\mathbf{C}_1$ and $\mathbf{C}_2$ are said to be equivalent if and only if after a suitable change of coordinate positions of $\mathbf{C}_1$ all the codewords in both codes coincide. The dual code $\mathbf{C}^\perp$ of $\mathbf{C}$ is defined by

$$\mathbf{C}^\perp = \{\mathbf{u} \in V \mid (\mathbf{u}, \mathbf{v}) = \mathbf{0} \quad \forall \mathbf{v} \in \mathbf{C}\}.$$

The code $\mathbf{C}$ is called self-orthogonal if it satisfies $\mathbf{C} \subseteq \mathbf{C}^\perp$, and the code $\mathbf{C}$ is called self-dual if it satisfies $\mathbf{C} = \mathbf{C}^\perp$.

Let

$$\mathbf{x} = (x_1, x_2, \ldots, x_n)$$

be a vector in V , then the Hamming weight $wt(\mathbf{x})$ of the vector $\mathbf{x}$ is defined to be the number of i's such that $x_i \neq 0$. The Hamming distance d on V is also defined by $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. Let $\mathbf{C}$ be a code ,then the minimum distance d of the code $\mathbf{C}$ is defined by

$$\begin{aligned} d &= \mathrm{Min}_{\mathbf{x},\mathbf{y}\in\mathbf{C},\mathbf{x}\neq\mathbf{y}} d(\mathbf{x}, \mathbf{y}) \\ &= \mathrm{Min}_{\mathbf{x}\in\mathbf{C},\mathbf{x}\neq\mathbf{0}} wt(\mathbf{x}). \end{aligned}$$

Eelement $\mathbf{x}$ in $\mathbf{C}$ is called a codeword of $\mathbf{C}$.

A vector $\mathbf{v}$ in a coset U in $V/\mathbf{C}$ is a coset leader if $\mathbf{v}$ satisfies

$$wt(\mathbf{v}) \leq wt(\mathbf{z}) \text{ for all } \mathbf{z} \in U.$$

Then the covering radius of $\mathbf{C}$ is the weight of a coset leader of greatest weight.

$\mathbf{u} * \mathbf{v}$: the number of common 1's in the entries of the vectors $\mathbf{u}, \mathbf{v} \in V$

The inhomogeneous weight enumerator $W_{\mathbf{C}}(X)$ of a code $\mathbf{C}$ is defined by

$$\begin{aligned} W_{\mathbf{C}}(X) &= \sum_{\mathbf{v}\in\mathbf{C}} X^{wt(\mathbf{v})} \\ &= \sum_{r=0}^{n} a_r X^r, \end{aligned}$$

where a_r is the number of the codewords $\mathbf{v}$ of weight r in $\mathbf{C}$ The homgeneous weight enumerator of the code $\mathbf{C}$ is defined by :

$$W_{\mathbf{C}}(x, y) = \sum_{r=0}^{n} a_r x^{n-r} y^r.$$

A celebrated MacWilliams identity says :

Theorem 1 *Let $W_{\mathbf{C}}(X)$ be the weight enumerator of a binary code, then the following identity holds :*

$$W_{\mathbf{C}^\perp}(X) = \frac{1}{\mid \mathbf{C} \mid}(1 + X)^n W_{\mathbf{C}}(\frac{1 - X}{1 + X}).$$

The homogeneous version of the above theorem is

Theorem 2

$$W_{\mathbf{C}^\perp}(x, y) = \frac{1}{\mid \mathbf{C} \mid} W_{\mathbf{C}}(x + y, x - y) \tag{1}$$

The coset weight enumerator of a coset U in a code $\mathbf{C}$ is defined to be a polynomial in X given by

$$W_U(X) = \sum_{\mathbf{z}\in U} X^{wt(\mathbf{z})}.$$

2 Definition of Jacobi polynomials for Binary codes.

Jacobi polynomial $Jac(\mathbf{C}, \mathbf{v} \mid X, Z)$ for $\mathbf{C}$ with respect to $\mathbf{v} \in \mathbf{F}_2^n$ is defined by

$$Jac(\mathbf{C}, \mathbf{v} \mid X, Z) = \sum_{\mathbf{u} \in \mathbf{C}} X^{\mathbf{u}*\mathbf{u}} Z^{\mathbf{u}*\mathbf{v}}.$$

The homogeneous Jacobi polynomial is defined by

$$\begin{aligned} & Jac(\mathbf{C}, \mathbf{v}, x, y, u, v) \\ &= \sum_{\mathbf{u} \in \mathbf{C}} x^{n-wt(\mathbf{v})-wt(\mathbf{u})+\mathbf{u}*\mathbf{v}} y^{wt(\mathbf{u})-\mathbf{u}*\mathbf{v}} \\ & \cdot u^{wt(\mathbf{v})-\mathbf{u}*\mathbf{v}} v^{\mathbf{u}*\mathbf{v}}, \end{aligned}$$

, where x, y, u, v are algebraically independent variables over $\mathbb{C}$. The connection between inhomogeneous Jacobi and homogeneous Jacobi is described by

$$\begin{aligned} & Jac(\mathbf{C}, \mathbf{v}, x, y, u, v) \\ &= x^{n-wt(\mathbf{v})} u^{wt(\mathbf{v})} Jac_i(\mathbf{C}, \mathbf{v}, yx, xvyu), \end{aligned}$$

and

$$Jac_i(\mathbf{C}, \mathbf{v}, X, Z) = Jac(\mathbf{C}, \mathbf{v}, 1, X, 1, XZ).$$

One of our basic theorems is :

Theorem 3 *Let* $\mathbf{C}$ *be a binary code of length* n *and* $Jac(\mathbf{C}, \mathbf{v} \mid X, Z)$ *a Jacobi polynomial for the code* $\mathbf{C}$ *with any binary vector* $\mathbf{v} \in \mathbf{F}_2^n$*, then it holds that*

$$\begin{aligned} & Jac(\mathbf{C}^\perp, \mathbf{v} \mid X, Z) \\ &= \frac{1}{|\mathbf{C}|}(1+X)^n \left(\frac{1+XZ}{1+X}\right)^{wt(\mathbf{v})} \\ & \times Jac(\mathbf{C}, v \mid \frac{1-X}{1+X}, \frac{(1-XZ)(1+X)}{(1+XZ)(1-X)}). \end{aligned}$$

There is a homogeneous version of the above theorem :

Theorem 4 *Let* $\mathbf{C}$ *be a binary linear code of length* n*, then* $Jac(\mathbf{C}, \mathbf{v}, x, y, u, v)$ *satisfies*

$$\begin{aligned} & Jac(\mathbf{C}^\perp, \mathbf{v}, x, y, u, v) \\ &= \frac{1}{|\mathbf{C}|} Jac(\mathbf{C}, \mathbf{v}, x+y, x-y, u+v, u-v) \end{aligned} \tag{2}$$

2.1 Reed-Muller codes

Reed-Muller code $RM(r,m)$ is a class of binary linear codes of length 2^m of dimension $\sum_{k=0}^{r} \begin{pmatrix} m \\ k \end{pmatrix}$, where $1 \leq r \leq m$.
$R(r,m)$: r-th order Reed-Muller code of Length 2^m

We now give briefly the definition of Reed-Muller codes.

We denote by (1^n)(resp. (0^n)) the all one(resp. zero) vector of length n. We use the symbol $\mathbf{ab}$ to denote the concatenation of two vectors $\mathbf{a}$ and $\mathbf{b}$, and the symbol $\mathbf{a}^\ell$ to denote the concatenation of ℓ $\mathbf{a}$'s. For example, we see that

$$(1^3) = (111), \quad (1^2 0^2) = (1100) \text{and} (1010)^2 = (10101010)$$

and so on. We put

$$\begin{aligned} \mathbf{x}_0 &= (1^{2^m}), \\ \mathbf{x}_1 &= (0^{2^{m-1}} 1^{2^{m-1}}), \\ \mathbf{x}_2 &= ((0^{2^{m-2}} 1^{2^{m-2}})^2 \\ &\vdots \\ \mathbf{x}_m &= ((01))^{2^{m-1}}). \end{aligned}$$

If $\mathbf{x}$ and $\mathbf{y}$ are two vectors of the same length, then we denote by $\mathbf{xy}$ another vector of identical length obtained from the component-wise product of those two vectors. We call it the vector product of $\mathbf{x}$ and $\mathbf{y}$. Likewise we can define the vector product of arbitrary number of vectors of the same length.

The r-th order Reed-Muller code $R(r,m)$ of length 2^m is defined to be a binary linear code spanned by vectors

$$\prod_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_h \leq m} \mathbf{x}_{i_1} \mathbf{x}_{i_2} \cdots \mathbf{x}_{i_h}, \ \ h \leq r$$

and by $\mathbf{x}_0$.

We give an example. Let $m = 4$, then we see that

$$\begin{aligned} \mathbf{x}_0 &= (1111111111111111), \\ \mathbf{x}_1 &= (0000000011111111), \\ \mathbf{x}_2 &= (0000111100001111), \\ \mathbf{x}_3 &= (0011001100110011), \end{aligned}$$

and

$$\mathbf{x}_4 = (0101010101010101).$$

Further we see that

$$\begin{aligned} \mathbf{x}_1\mathbf{x}_2 &= (0000000000001111), \\ \mathbf{x}_1\mathbf{x}_3 &= (0000000000110011), \\ \mathbf{x}_1\mathbf{x}_4 &= (0000000001010101), \end{aligned}$$

$$\mathbf{x}_2\mathbf{x}_3 = (0000001100000011),$$

$$\mathbf{x}_2\mathbf{x}_4 = (0000010100000101),$$

and

$$\mathbf{x}_3\mathbf{x}_4 = (0001000100010001).$$

Thus the generator matrix of the first order Reed-Muller code of length $2^4 = 16$ $R(1,4)$ is given by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and the generator matrix of the second order Reed-Muller code of length $2^4 = 16$ $R(2,4)$ is given by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

3 Statement of the problems

Let $\mathbf{x}$ be a vector in V, then the Hamming sphere $S_t(\mathbf{x})$ of radius t with center $\mathbf{x}$ is defined by

$$S_t(\mathbf{x}) = \{\mathbf{y} \in V \mid d(\mathbf{y}, \mathbf{x}) \leq t\}.$$

The covering radius $t(\mathbf{C})$ of the code $\mathbf{C}$ is defined to be the smallest integer t such that the equation

$$V = \bigcup_{\mathbf{x} \in \mathbf{C}} S_t(\mathbf{x})$$

holds. The covering radius of a code $\mathbf{C}$ is also defined by another way.

Proposition 1 *It holds that*

$$t(\mathbf{C}) = \max_{\mathbf{u} \in \mathbf{F}_2^n} (\min_{\mathbf{z} \in \mathbf{u}+\mathbf{C}} wt(\mathbf{z})).$$

A more precise problem is that for a given code $\mathbf{C}$ determine all the coset weight enumerators (or equally the coset weight distributions) $W_U(X)$.

3.1 Krawtchouk polynomials

Krawtchouk polynomials are the sequence of polynomials $P_k(x)$ of degree n defined by

$$P_k(x) = \sum_{j=0}^{k} (-1)^j \begin{pmatrix} x \\ j \end{pmatrix} \begin{pmatrix} n-x \\ k-j \end{pmatrix} \quad 0 \le k \le n, \tag{3}$$

where x is a variable and we set

$$\begin{pmatrix} x \\ j \end{pmatrix} = \frac{x(x-1)\cdots(x-j+1)}{j!}, \quad j \ge 1 \quad \begin{pmatrix} x \\ 0 \end{pmatrix} = 1.$$

It is known that it holds that for any triple $i, j, u \in \{0, 1, \cdots, n\}$

$$P_i(u)P_j(u) = \sum_{k=0}^{n} p_{i,j}^{(k)} P_k(u).$$

Here the numbers $p_{i,j}^{(k)}$ are integers determined as follows. We put

$$D_i = \{\mathbf{a} \in \mathbb{F}_2^n \mid \ wt(\mathbf{a}) = i\},$$

then first for a fixed $\mathbf{c} \in D_k$ the number of pairs $\mathbf{a}$ and $\mathbf{b}$:

$$p_{i,j}^{(k)} = \#\{ < \mathbf{a}, \mathbf{b} > \mid \ \mathbf{a} \in D_i, \ \mathbf{b} \in D_j, \ \mathbf{a} + \mathbf{b} = \mathbf{c} \ \}$$

is proved to be independent of the choice of $\mathbf{c}$. As to the formula for $p_{i,j}^{(k)}$ one may refer MacWilliams and Sloane [19], Ch. 21 section 3. The formula reads

$$p_{i,j}^{(k)} = \begin{cases} \begin{pmatrix} k \\ \frac{i-j+k}{2} \end{pmatrix} \begin{pmatrix} n-k \\ \frac{i+j-k}{2} \end{pmatrix} \\ \qquad i+j \equiv k \pmod 2 \\ \\ 0 \\ \qquad i+j \equiv k+1 \pmod 2 \end{cases} \tag{4}$$

3.2 Distance Matrix

Let $\mathbf{C}$ be a binary linear [n,k] code. The $2^n \times (n+1)$ matrix $\mathbf{B} = (B_i(\mathbf{e}))_{\mathbf{e} \in \mathbb{F}_2^n, 0 \le i \le n}$, is called ,after Delsarte [8], the distance matrix for the code $\mathbf{C}$. Here the entries of $\mathbf{B}$ are defined by

$$B_i(\mathbf{e}) = \#\{ \ \mathbf{a} \in \mathbf{C} \mid d(\mathbf{a}, \mathbf{e}) = i \ \} \quad 0 \le i \le n.$$

More concretely we give

$$\mathbf{B} = \begin{pmatrix} B_0(\mathbf{e}_1) & B_1(\mathbf{e}_1) & B_2(\mathbf{e}_1) & \cdots & B_n(\mathbf{e}_1) \\ B_0(\mathbf{e}_2) & B_1(\mathbf{e}_2) & B_2(\mathbf{e}_2) & \cdots & B_n(\mathbf{e}_2) \\ \vdots & & & & \\ B_0(\mathbf{e}_m) & B_1(\mathbf{e}_m) & B_2(\mathbf{e}_m) & \cdots & B_n(\mathbf{e}_m) \\ \vdots & & & & \\ B_0(\mathbf{e}_{2^n}) & B_1(\mathbf{e}_{2^n}) & B_2(\mathbf{e}_{2^n}) & \cdots & B_n(\mathbf{e}_{2^n}) \end{pmatrix}.$$

Two formulas in [8] are very useful for our present work. The first one is

$$\sum_{\mathbf{e}\in\mathbb{F}_2^n} B_i(\mathbf{e})B_j(\mathbf{e}) = M\sum_{k=0}^{n} p_{i,j}^{(k)} A_k(\mathbf{C}). \tag{5}$$

Here $M = 2^r,\ r = dim\mathbf{C}$, and $A_k(\mathbf{C})$ is the number of codewords of weight k in the code $\mathbf{C}$. The above formula gives us vertical informations on $\mathbf{B}$. One may remark that

$$\begin{aligned} B_i(\mathbf{e}) &= \#\{\ \mathbf{a}\in\mathbf{C}\mid d(\mathbf{a},\mathbf{e}) = i\} \\ &= \#\{\ \mathbf{a}\in\mathbf{C}\mid wt(\mathbf{a}+\mathbf{e}) = i\} \\ &= \#\{\ \mathbf{b}\in\mathbf{e}+\mathbf{C}\mid wt(\mathbf{b}) = i\ \}, \end{aligned}$$

so that

$$B_0(\mathbf{e}), B_1(\mathbf{e}), \cdots, B_n(\mathbf{e})$$

is the coset weight distribution of the coset $\mathbf{e}+\mathbf{C}$. In other words the polynomial

$$\sum_{i=0}^{n} B_i(\mathbf{e})x^i$$

is the inhomogeneous coset weight enumeraror of the coset $\mathbf{e}+\mathbf{C}$, and the polynomial

$$\sum_{i=0}^{n} B_i(\mathbf{e})x^{n-i}y^i$$

is the homogeneous one.

3.3 A Modification of Distance Matrix

We remark that if two vectors $\mathbf{e}_1$ is congruent to $\mathbf{e}_2$ modulo $\mathbf{C}$ then it holds that $B_i(\mathbf{e}_1) = B_i(\mathbf{e}_2)$ for $0\le i\le n$, and so that we may rewrite the formula (5) into

$$\sum_{\mathbf{e}\in\mathbb{F}_2^n/\mathbf{C}} B_i(\mathbf{e})B_j(\mathbf{e}) = \sum_{k=0}^{n} p_{i,j}^{(k)} A_k(\mathbf{C}). \tag{6}$$

Accordingly we may use the shortened distance matrix $\mathbf{B}_S$:

$$\mathbf{B}_S = (B_i(\mathbf{e}))_{\mathbf{e}\in\mathbb{F}_2^n/\mathbf{C}, 0\le i\le n}$$

or more concretely

$$\mathbf{B}_S = \begin{pmatrix} B_0(\mathbf{e}_1) & B_1(\mathbf{e}_1) & B_2(\mathbf{e}_1) & \cdots & B_n(\mathbf{e}_1) \\ B_0(\mathbf{e}_2) & B_1(\mathbf{e}_2) & B_2(\mathbf{e}_2) & \cdots & B_n(\mathbf{e}_2) \\ \vdots & & & & \\ B_0(\mathbf{e}_m) & B_1(\mathbf{e}_m) & B_2(\mathbf{e}_m) & \cdots & B_n(\mathbf{e}_m) \\ \vdots & & & & \\ B_0(\mathbf{e}_t) & B_1(\mathbf{e}_t) & B_2(\mathbf{e}_t) & \cdots & B_n(\mathbf{e}_t) \end{pmatrix},$$

with $t = 2^{n-r}, r = \dim\mathbf{C}$.

4 Relation between Jacobi polynomials of codes and coset weight enumerator

We quote

Theorem 5 ([24]) *Let* $\mathbf{C}$ *be a binary linear code of length* n*. We take any vector* $\mathbf{v}$ *in* $\mathbf{F}_2^n$*. If* $\mathbf{v}+\mathbf{C}$ *is the coset in* $\mathbf{F}_2^n/\mathbf{C}$ *to which* $\mathbf{v}$ *belongs, then we have*

$$\begin{aligned} & W_{\mathbf{v}+\mathbf{C}}(X) \\ = \; & \psi(Jac(C,\mathbf{v} \mid X,Z)) \\ = \; & X^{wt(\mathbf{v})} Jac(C,\mathbf{v} \mid X,X^{-2}), \end{aligned}$$

where $Jac(C,\mathbf{v} \mid X,Z)$ *is the inhomogeneous Jacobi polynomial for the code* $\mathbf{C}$ *with respect to* $\mathbf{v}$*.*

Jacobi polynomials together with this theorem give us clearer insights for the horizontal information on the matrix $\mathbf{B}$ or $\mathbf{B}_S$.

$$\begin{array}{ccc} & \text{MacWilliams transform} & \\ Jac(C,\mathbf{v} \mid X,Z) & \longleftrightarrow & Jac(C^{\perp},\mathbf{v} \mid X,Z) \\ \downarrow \psi & & \downarrow \psi \\ W_{\mathbf{v}+\mathbf{C}}(X) & < -- > & W_{\mathbf{v}+\mathbf{C}^{\perp}}(X) \\ & \text{there is no algebraic correspondence such as MacWilliams transform} & \end{array}$$

5 A summary of known results

A table of the determination of the covering radius and the complete coset weight distribution

$r\backslash m$	3	4	5	6	7	8	9
1 1	$\rho=2$ **CWD**	$\rho=6$ **CWD**	$\rho=12$ **CWD**	$\rho=28$ **CWD**	$\rho=56$ $CWD hard$	$\rho=120$ $hard$	$240\le\rho\le244$ $hard$
2 2	$\rho=1$	$\rho=2$ **CWD**	$\rho=6$ **CWD**	$\rho=18$ $CWD\ p.$	$40\le\rho\le44$ $CWD\ hard$	$84\le\rho\le100$ $CWD\ hard$	$171\le\rho\le220$ $CWD\ hard$
3 3		$\rho=1$ **CWD**	$\rho=2$ **CWD**	$\rho=8$ $CWD\ p.$	$20\le\rho\le23$ $CWD\ hard$	$43\le\rho\le67$ $CWD\ hard$	$134\le\rho\le167$ $CWD\ hard$
4 4			$\rho=1$ **CWD**	$\rho=2$ $CWD\ p.$	$\rho=8$ $CWD\ p.$	$22\le\rho\le31$ $CWD\ hard$	$62\le\rho\le98$ $CWD\ hard$
5 5				$\rho=1$	$\rho=2$ $CWD\ p.$	$\rho=10$ $CWD\ hard$	$23\le\rho\le41$ $CWD\ hard$

$\rho = \rho(r, m)$: the covering radius of $R(r, m)$
CWD : Complete coset weight distribution is determined.
CWD p. : It is possible to determine the complete coset weight distribution
References : [1],[14],[15],[20],[22],[26],[29],[30].

6 Preliminary result

When we ask the computer algebra MAGMA in such a way that

```
> R2:=ReedMullerCode(3,6);
> CD:=CosetDistanceDistribution(R2);
> CD;
the answer of MAGMA is
[ <0, 1>, <1, 64>, <2, 2016>, <3, 41664>, <4, 313131>,
 <5, 1166592>, <6, 1768116>, <7, 888832>, <8, 13888> ]
```

The meaning of the above output is that in the third order Reed-Muller code of length $2^6 = 64$ the number of coset of weight 0 is 1, the number of the cosets of weight 1 is 64 and so on. But MAGMA (in my old version) does not answer the question such as

```
> R:=ReedMullerCode(2,6);
> CD:=CosetDistanceDistribution(R);
> CD;
```

When we want to know more concerning the coset distance distribution, we must explore some algebraic technics. This is our motivation of the previous sections.

7 How to reduce the runtime

7.1 Group theoretic process I

Our plan to determine the coset weight distributions of RM(2,6) is first to compute the Jacobi(-Ozeki) polynomials $Jac(\mathbf{v}, X, Z)$ for each reference vectors $\mathbf{v}$ of weight k. Among these vectors we select rigid vectors, and from these vectors we get coset weight enumerators of coset weight k. A naive idea to determine the coset weight enumerators of coset weight k is to use nested loops of depth k in the programs. The run time increases greatly as k grows . We give the estimates of runtime on our program below, some of which were tested in the actual programs.

Run time estimate for our programs.

k	run time (minutes)	days
$0 \leq k \leq 7$	tolerable	within a day
8	1840	1 day and 7 hours
9	11448	8 days
10	62968	43 days
11	309120	214 days
12	1365280	948 days
13	5461120	3792 days
14	19894080	13815 days
15	⋮	⋮
16	⋮	⋮
17	⋮	⋮
18	⋮	⋮

Therefore the naive approach to the computing seems to be unrealistic.

To save the runtime (and also my mathematical life time) we devised the following process.

We divide 64 coordinates into 16 blocks so that each block consists of 4 coordinates. The division is done in a natural order. Consider $G = Aut(RM(2,6))$ the group of automorphisms of the second order Reed-Muller code of length 64. G acts on the totality of the blocks. We remark that two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, which are connected by $\mathbf{v}_2 = \sigma(\mathbf{v}_1)$ with $\sigma \in Aut(RM(2,6)$, satisfy the identity

$$Jac(RM(2,6), \mathbf{v}_1, X, Z) = Jac(RM(2,6), \mathbf{v}_2, X, Z),$$

and therefore

$$W_{RM(2,6)+\mathbf{v}_1}(X) = W_{RM(2,6)+\mathbf{v}_1}(X).$$

Our strategy to reduce the runtime is to cutt off the repetition of the computation with the same outputs. When the weight of the reference vector $\mathbf{v}$ is 8, we look at the types of the distribution of non-zero coordinates of $\mathbf{v}$into the blocks. The result is

type	1^8	$2 \cdot 1^6$	$2^2 \cdot 1^4$	$2^3 \cdot 1^2$	2^4	$3 \cdot 1^5$	$3 \cdot 2 \cdot 1^3$	$3 \cdot 2^2 \cdot 1$
number of orbits	4	5	6	3	2	4	4	2

type	$3^2 \cdot 1^2$	$3^2 \cdot 2$	$4 \cdot 1^4$	$4 \cdot 2 \cdot 1^2$	$4 \cdot 2^2$	$4 \cdot 3 \cdot 1$	4^2
number of orbits	2	1	3	2	1	1	1

Here 1^8 means that non zero coordinates of a $\mathbf{v}$ of weight 8 are distributed into 8 different blocks, and so on. There are four orbits of type 1^8 under the action of G. Each orbit has a certain cardinality. For instance an orbit represented by the block distribution

```
[ 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0 ]
```

has the cardinality 30. This implies that we have only to examine only one case instead of doing 29 other cases with identical outputs. After all we have only to run 41 cases each of which needs small runtime (within 1 minute).

In the same way we make programs for other reference vectors of weights of from 9 upto 18.

However When the weights go to more than 12 the runtimes of some cases increase largely. To shorten the runtimes we devise another technical lemma, which will be described in the next subsection.

7.2 Group theoretic process II

In many types of block decomposition of the support vector of the reference vector it may contain more than three blocks that contain only one non-zero coordinate. For this case the runtime can be shortened by the following lemma.

Lemma 1 *It holds that (i) if the two reference vectors* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *have the same block decomposition with the additional condition that these two contains three (resp. two resp. one) blocks that contain only one non-zero coordinates, then there is an automorphism in* G *which send* $\mathbf{v}_1$ *to* $\mathbf{v}_2$.

By this lemma we can shorten the runtime to 1/64 (resp. 1/16, resp. 1/4) compared to original state. In other word we can cut the number of simple loops by three (resp. two, resp. one) in number. For instance consider the case

```
[ 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0 ]
```

we use 8 simple loops, and by the present lemma we may dispense with 3 simple loops. After these shortenings techniques we realize that the runtimes of finding cosets of weights from 8 upto 18 are largely reduced, and we give the runtimes in the table below.

coset weight	runtime
8	50 min.
9	120 min.
10	720 min.
11	1 day
12	3 days
13	5 days
14	2 weeks
15	2 weeks
16	2 weeks
17	6 days
18	1 week

8 How to verify the correctness of the computations

We may use the following three features of the distance matrix of the code $RM(2,6)$ as tests for the correctness of our computations. These features are also useful in finding unknown cosets of the code.

8.1 Combinatorial consideration

This is a simple fact that the totality of vectors of a fixed weight k equals the number $\begin{pmatrix} 64 \\ k \end{pmatrix}$. For instance the number of the vectors of weight 6 in all the cosets of of weight 6 of $RM(2,6)$ is $55996416+1166592+17498880+312480 = 74974368$ which equals the $\begin{pmatrix} 64 \\ 6 \end{pmatrix}$. (See a table in the section 9.)

8.2 Delsarte identities

This is an identity (6) in the section 3.3. Here we give two instances of using it. We note that for the case $\mathbf{C}$ =RM(2,6) the numbers $A_k(\mathbf{C})$, different from 0 in the section 3.2 are known to be

$$A_0 = A_{64} = 1, A_{16} = A_{48} = 2604, A_{24} = A_{40} = 291648, A_{28} = A_{36} = 888832, A_{32} = 1828134.$$

Also by computation of (4) we have

$$p_{6,6}^{(0)} = 74974368, p_{6,6}^{(16)} = 0, p_{6,6}^{(24)} = 0, \cdots$$

and

$$p_{6,10}^{(0)} = 0, p_{6,10}^{(16)} = 8008, p_{6,10}^{(24)} = 0, \cdots.$$

When $i = j = 6$, the right hand side of (6) is 74974368 and the lefthand side of (6) is, by a table the section 9, $55996416 + 1166592 + 17498880 + 312480 = 74974368$.
When $i = 6, j = 10$, the righthand side of (6) is $8008 \cdot 2604 = 20852832$ and the lefthand side of (6) is $1166592 + 17498880 + 7 \cdot 312480 = 20852832$ (See a table in Section 9.)

8.3 Partial coincidence

This phenomenon can be well described by the following

Proposition 2 *Suppose a binary linear code* $\mathbf{C}$ *is self-orthogonal. If the two reference vectors* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *(possibly of different weight) belong to the same coset* $\mathbf{v}_1 + \mathbf{C} = \mathbf{v}_2 + \mathbf{C}$*, then it holds that* $\mathbf{v}_1 + \mathbf{C}^\perp = \mathbf{v}_2 + \mathbf{C}^\perp$.

The proof is easy, and we leave it for the reader.

A class of codes such as $RM(r,m)$ $r \leq \frac{m-1}{2}$ are self-orthogonal, and therefore this proposition can be applied to them.

By this proposition each coset in $RM(2,6)$ can be naturally regarded as a coset in $RM(3,6)$. If we can detect which coset of various weights in $RM(2,6)$ corresponds to a coset of certain coset of coset weight ℓ in $RM(3,6)$, the number of the vectors of weight k in these cosets in $RM(2,6)$ should equal the number of the vectors of weight k in the cosets of weight ℓ.
Using the Table 1 in the section 9 we observe that the number of all the vectors of weight 8 of the cosets of various weights in $RM(2,6)$ that lead to the coset of weight 2 in $RM(3,6)$ is $2 \cdot 2499840 = 4999680$ while by Table 3 the number of the vectors of weight 8 in the coset of weight 2 in $RM(3,6)$ is $2480 \cdot 2016 = 4999680$.

9 Explicit results

We give some of our results by three tables. The final results should extend the table of the cosets of weights from 0 to 18. Therefore our present tables is a portion of the final state. Some explanations of the meanings in the tables. The leftmost of the tables indicates the weight of the coset. The next entry in the Tables 1 and 2 shows that the coset in $RM(2,6)$ should fall into the coset of the indicated weight type in $RM(3,6)$ in the sense of Proposition 2. Specifically "lead to 4_1" means that the coset in $RM(2,6)$ leads to the coset of weight 4 in $RM(3,6)$, which is presented first in the Table 3. Likewise others are explained. The first non-vanishing entry in the remaining entries of the row denotes the number of the coset leaders of the coset. After that the number of the vectors in that coset is presented together with the weight. "mul" means the number of the cosets with the identical coset weight distribution. We remark that we are not fully confident on the multiplicities of the cosets in the tables presented here, since we have not enought time to check all the tests in the previous section. The complete tables will appear elsewhere as a part of our research paper.

9.1 Tables

Table 1 Even weight cosets

coset wt	0	2	4	6	8	10	12	14	16	18	20	22	mul
coset wt	64	62	60	58	56	54	52	50	48	46	44	42	
0	1								2604				1
2		1						155	992	1457		39928	2016
4	lead to wt 4_1		1				7	112	552	1136	5669	37184	624960
4	lead to wt 4_2		1				35	0	720	1024	6033	35840	10416
6	lead to wt 6_1			1		0	6	75	340	1311	7566	37306	55996416
6	lead to wt 6_2			1		1	0	90	320	1306	7680	37071	1166592
6	lead to wt 4_1			1		1	12	58	328	1402	7580	36559	17498880
6	lead to wt 2			1		7	0	84	224	1884	6144	38669	312480
8	lead to wt 8				1	0	0	56	266	1400	8512	37216	31997952
8	lead to wt 6_1				1	0	1	50	276	1410	8461	37256	895942656
8	lead to wt 6_1				1	0	6	44	254	1484	8398	36976	2239856640
8	lead to wt 4_1				1	0	8	32	282	1440	8488	36864	209986560
8	lead to wt 6_2				1	0	12	32	242	1568	8284	36736	34997760
8	lead to wt 6_1				1	1	6	47	222	1563	8398	36501	559964160
8	lead to wt 4_1				1	2	8	38	266	1470	8360	36554	419973120
8	lead to wt 4_1				2	0	12	48	220	1584	8220	35904	13124160
8	lead to wt 4_2				2	0	24	0	420	1024	8888	35840	1093680
8	lead to wt 2				2	6	0	42	308	1778	6272	39934	2499840
8	lead to wt 0				8	0	0	0	784	0	14336	0	1395
10	lead to wt 6_1					1	0	27	264	1511	8768	37061	6719569920
10	lead to wt 4_1					1	0	39	208	1619	8704	36853	5039677440
10	lead to wt 6_1					1	1	31	238	1547	8813	36821	26878279680
10	lead to wt 6_1					1	2	33	224	1565	8826	36701	8959426560
10	lead to wt 8					1	3	27	234	1575	8775	36741	995491840
10	lead to wt 6_1					1	3	29	222	1593	8807	36621	26878279680
10	lead to wt 6_2					1	4	31	232	1547	8756	36821	1119928320
10	lead to wt 6_1					1	4	31	232	1547	8756	36821	6719569920
10	lead to wt 4_1					1	4	31	232	1547	8756	36821	8959426560
10	lead to wt 4_1					1	4	39	200	1619	8628	36853	1119928320
10	lead to wt 6_1					1	6	27	228	1575	8718	36741	26878279680
10	lead to wt 6_1					1	10	15	172	1787	8770	35861	335978496
10	lead to wt 6_1					2	4	34	224	1562	8692	36666	10079354880
10	lead to wt 4_1					2	8	22	224	1582	8808	36234	1259919360
10	lead to wt 4_1					2	8	38	224	1470	8808	36554	839946240
10	lead to wt 2					2	8	46	144	1862	7528	39594	52496640
10	lead to wt 6_1					3	6	29	212	1633	8590	36351	839946240
10	lead to wt 6_2					4	0	44	192	1628	8704	36116	52496640
10	lead to wt 4_1					4	4	28	280	1484	8372	37076	319979520
10	lead to wt 4_2					4	4	28	280	1484	8372	37076	9999360
10	lead to wt 4_1					4	4	44	216	1500	8756	36244	157489920
10	lead to wt 4_1					4	8	12	304	1468	8424	36884	69995520
10	lead to wt 2					6	0	106	32	1842	7680	38654	1749888

Table 2 Odd weight cosets

coset wt	1	3	5	7	9	11	13	15	17	19	21	mul
coset wt	63	61	59	57	55	53	51	49	47	45	43	
1	1							651	1953			64
3		1					35	360	1128	1081	14168	41664
5	lead to wt5		1			1	30	220	700	2686	16863	6999552
5	lead to wt3		1			7	28	168	808	2724	16621	624960
7	lead to wt1			1	7	0	0	196	588	4480	9856	89280
7	lead to wt 3			1	1	6	18	114	690	3290	17886	17498880
7	lead to wt 5			1	0	3	21	123	623	3449	17919	279982080
7	lead to wt5			1	0	1	15	155	591	3355	18293	55996416
7	lead to wt5			1	1	0	36	86	630	3652	17424	11665920
7	lead to wt 7			1	0	0	21	140	616	3325	18260	255983616
9	lead to wt7				1	0	3	126	594	3627	18876	995491840
9	lead to wt7				1	0	11	106	590	3715	18700	1791885312
9	lead to wt5				1	0	12	99	607	3708	18656	6719569920
9	lead to wt5				1	0	20	75	631	3732	18480	1119928320
9	lead to wt7				1	1	14	90	606	3762	18513	8959426560
9	lead to wt5				1	3	13	79	603	3889	18271	839946240
9	lead to wt5				1	3	13	95	603	3713	18447	4479713280
9	lead to wt3				1	3	17	67	687	3541	18799	279982080
9	lead to wt5				1	5	11	87	611	3783	18249	839946240
9	lead to wt5				2	2	18	90	594	3786	18106	629959680
9	lead to wt3				2	4	20	102	574	3588	18612	52496640
9	lead to wt3				3	5	7	105	749	3171	18425	39997440

Table 3 Cosets Reed-Muller code RM(3,6)

coset wt	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	mul
coset wt	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	
0	1								11160				1749888		22855680		1
1		1						1395		9765		328104		6421464		75876375	64
2			1				155		2480		65813		1573312		22901343		2016
3				1		15		420		12540		351249		6283679		76053456	41664
4					2		56		2100		71576		1566454		22829520		312480
4					16		0		3360		61440		1596848		22794240		651
5						6		298		13090		354510		6264276		76069196	1166592
6							32		2112		72352		1565952		22817472		1749888
6							64		1920		73024		1562112		22834560		18228
7								288		13216		354816		6263040		76059072	888832
8									2304		71680		1569792		22800384		13888

References

[1] E.R.Berlekamp and L.R. Welch, Weight Distributions of the Cosets of the (32,6) Reed-Muller Code, IEEE Trans. Inf. Th. Vol. 18 (1972) 203-207

[2] A.R. Calderbank and N.J.A. Sloane, IEEE Trans. Inf. Th. Vol. IT-33 (1987) 177-195

[3] G.D. Cohen, A.C. Lobstein and N.J.A. Sloane, On a cojecture concerning coverings of Hamming space, Proc. Int. Conf. Algebra, Algorithms and Codes, Toulouse, France, 1984 Lecture Notes in Computer Science No.228 79-89

[4] G.D.Cohen, Antoine C. Lobstein, and N.J.A. Sloane, Further Results on the Covering Radius of Codes, IEEE Trans. Inf. Th. Vol. 32 (1986) 680-694

[5] G.D. Cohen, M.G. Karpovsky, H.F. Mattson,Jr. and J.R. Schatz, Covering Radius– Survey and Recent Results, IEEE Trans. Inf. Th. Vol. IT-31 (1985) 328-343

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

[7] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Reports Supplements, No. 10 (1973)

[8] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Information and Control Vol.23, (1973) 407-438

[9] D. E. Downie and N.J.A. Sloane, IEEE Trans. Inf. Th. Vol. IT-31 (1985) 446-447

[10] R.L. Graham and N.J.A. Sloane, On the Covering Radius of Codes, IEEE Trans. Inf. Th. Vol. IT-31 (1985) 385-401

[11] T.Helleseth ,T. KØve, and J. Mykkeltveit, On the Covering Radius of Binary Codes, IEEE Trans. Inf. Th. Vol. 24 (1978) 627-628

[12] T.Helleseth and H.C.A. van Tilborg, A new class of Codes meeting the Griesmerbound, IEEE Trans. Inf. Th. Vol. 27 (1981) 548-555

[13] T.Helleseth, Further classifications of Codes meeting the Griesmer bound, IEEE Trans. Inf. Th. Vol. 30 (1984) 395-403

[14] Xiang-Dong Hou, Some Results on the Covering Radii of Reed-Muller Codes, IEEE Trans. Inf. Th. Vol. 39 (1993) 368-378

[15] Xiang-Dong Hou, Some inequalitiesabout the covering radius of Reed-Muller Codes, Designs, Codes and Cryptography, Vol. 2 (1992) 215-224

[16] H. Janwa, Some New Upper Bounds on the Covering Radius of Binary Linear Codes, IEEE Trans. Inf. Th. Vol. 35 (1989) 110-122

[17] J.G.Kalbfleisch, R.G. Stanton and J.D. Horton, On covering sets and error-correcting codes, J. Comb. Th. Vol. 11, (1971) 233-250

[18] M.Karpovsky, Weight Distribution of Translates, Covering Radius, and Perfect Codes Correcting Errors of Given Weights, IEEE Trans. Inf. Th. Vol. 27 (1981) 462-472

[19] F.J. MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes",North-Holl and, Amsterdam, 1977.

[20] A.M.McLoughlin, The covering radius of the $(m-3)$rd-order Reed-Muller codes and a lower bound on the $(m-4)$th-order Reed-Muller codes, SIAM J. Appl. Math., Vol. 37 (1979) 419-422

[21] A.M.McLoughlin, The Complexity of computing the covering radius of a code,IEEE Trans. Inf. Th. Vol. 30 (1984) 800-804

[22] J. Mykkeltveit, The covering radius of the (128,8) Reed-Muller code is 56, IEEE Trans. Inf. Th. Vol.IT-26 (1980) 359-362

[23] M. Ozeki, On the notion of Jacobi polynomilas for codes, Math. Proc. Cambridge Philos. Soc. **121** (1997), 15 – 30.

[24] M. Ozeki, Determination of covering radii and coset weight distributions of doubly even extremal binary self-dual codes of length 40 Theoretical Computer Science. Vol.235 (2000) 283-308

[25] M. Ozeki, Determination of covering radii and coset weight distributions of doubly even extremal binary self-dual codes of length 56, , IEEE Trans. Inf. Th., Vol.46 (2000)2359-2372

[26] N.J. Patterson and D.H. Wiedemann, The covering radius of the (2^{15},16) Reed-Muller code is at least 16276, IEEE Trans. Inf. Th. Vol.IT-29 (1983) 354-356

[27] V. Pless, An Introduction to the Theory of Error-Correcting Codes, Wiley Interscience, New York, 1982.

[28] O. Rothaus, On bent functions, J. Comb. Th. Ser.A, Vol. 20 (1976) 300-305

[29] J.R.Schatz, On the weight distributions of cosets of a linear code, Amer. Math. Month. vol. 87 , (1980) 548-551

[30] J.Schatz, The Second Order Reed-Muller Code of Length 64 Has Covering Radius 18, IEEE Trans. Inf. Th. Vol. 27 (1981) 529-530

[31] N.J.A. Sloane, A new approach to the covering radius of codes, J. Comb. Th. Ser.A Vol. 42, (1986) 61-86

[32] M.Sugino, Y. Ienaga, N. Tokura, and T. Kasami, Weight distribution of (128,64) Reed-Muller code, IEEE Trans. Inf. Th. Vol.IT-17 (1971) 627-628

[33] G.J.M. Van Wee, Improved sphere bounds on the covering radius of codes, IEEE Trans. Inf. Th. Vol. 34 (1988) 237-244

[34] G.J.M. van Wee, G.D. Cohen, and S.N. Litsyn, A note on Perfect multiple coverings of the Hamming Space, IEEE Trans. Inf. Th. Vol. 37 (1991) 678-682

[35] T. Verhoeff, An Updated Table of Minimum-Distance Bounds for Binary Linear Codes, IEEE Trans. Inf. Th. Vol. IT-33 (1987) 665-680

[36] J.H.Weber, C.de Vroedt, and D.E.Boecke, Bounds and constructions for binary codes of length less than 24 and asymmetric distance less than 6, IEEE Trans. Inf. Th. Vol. 34 (1988) 1321-1331

Classification of Ternary Extremal Self-Dual Codes of Length 28

Akihiro Munemasa
(joint work with Masaaki Harada and Boris Venkov [4])

Abstract

Using the classification of extremal unimodular lattices of rank 28 due to Bacher and Venkov, we classify ternary extremal self-dual codes of length 28. This is achieved by classifying 3-frames of each of these lattices up to isometry of the lattice. There are 38 such lattices, and four of them have no 3-frames. From the remaining 34 lattices, we obtain 6931 codes up to equivalence.

In this report, we document the MAGMA [2] program used to achieve this classification.

1 General purpose routines

The following function classfies a given set `Cs` up to the equivalence relation defined by a function `f` and extract a set of representatives.

```
uptoequivalence:=function(Cs,f)
   rem:=Cs;
   Css:={};
   while not IsEmpty(rem) do
      x:=Random(rem);
      Include(~Css,x);
      rem diff:={ y : y in rem | f(x,y) };
   end while;
   return Css;
end function;
```

2 Graph theory routines

Let `S` be a subset of vertices of a graph `Gamma` which is left invariant by a group of automorphisms `G`. The following function constructs the subgraph and the group of its automorphisms induced by the set `S` and the group `G`, respectively.

```
graphActionImage:=function(Gamma,S,G)
   m:=#S;
   VG:=VertexSet(Gamma);
   D:=sub< Gamma | S >;
   VD:=VertexSet(D);
   DinG:=[ Index(VG!(VD!i)) : i in [1..m] ];
   gen:=[ [ Position(DinG,DinG[x]^g) : x in [1..m] ]
      : g in Generators(G) ];
   return < D,sub< Sym(m) | gen > >;
end function;
```

Let `G` be a group of automorphisms of a graph `Gamma`, and let `k` be a positive integer. The following function constructs a set of representatives of cliques of size `k` in `Gamma`, up to the action of `G`.

```
allCliquesUpToG:=function(Gamma,G,k)
   V:=VertexSet(Gamma);
   if #V lt k then
         return {};
   elif #G eq 1 then
      return AllCliques(Gamma,k);
   else
      orbs:=[ { V | x : x in o } : o in Orbits(G) ];
      reps:=[ Random(o) : o in orbs ];
      if k eq 1 then
         return { { r } : r in reps };
      else
         M:=[1..#orbs];
         orbsU:=[ &join{ orbs[j] : j in {i..#orbs} } : i in M ];
         nbs:=[ Neighbours(reps[i]) meet orbsU[i] : i in M ];
         M1:=[ i : i in M | not IsEmpty(nbs[i]) ];
         reps:=[ reps[i] : i in M1 ];
         nbs:=[ nbs[i] : i in M1 ];
         N:=[1..#M1];
         stabs:=[ Stabilizer(G,Index(reps[i])) : i in N ];
         GG:=[ graphActionImage(Gamma,nbs[i],stabs[i]) : i in N ];
         C:=&join{ { { reps[i] } join { V!x : x in c }
            : c in $$(GG[i][1],GG[i][2],k-1) } : i in N };
         C:={ { Index(x) : x in c } : c in C };
         f:=func< C1,C2 | IsConjugate(G,C1,C2) >;
         C:=uptoequivalence(C,f);
         return { { V!x : x in c } : c in C };
      end if;
   end if;
end function;
```

3 Group Theory Routines

Let `G` be a group acting on a set Ω, and let `X` be a sequence of all the elements of Ω (for example, let `G` be a matrix group, and let `X` be a sequence of vectors which is left invariant under `G` as a set). The following function constructs the standard permutation group obtained from the action of `G` on Ω, where the ordering of the elements of Ω is specified by the sequence `X`.

```
actionImage:=function(G,X)
   n:=#X;
   S:=Sym(n);
   H:=sub< S | { S![ Position(X,X[i]^g) : i in [1..n] ]
      : g in Generators(G) } >;
   return H;
end function;
```

4 Lattice Routines

Let `L` be an integral lattice. The following function constructs the even sublattice of `L`.

```
EvenSublattice:=function(L)
     B:=Seqset(Basis(L));
     oB:={ b : b in B | IsOdd(Integers()!(b,b)) };
     if IsEmpty(oB) then
```

```
        return L;
     else
        o:=Random(oB);
        return sub< L | { b+o : b in oB } join
            (B diff oB) >;
    end if;
end function;
```

Let `L` be an odd unimodular lattice. The following function constructs the dual of the even sublattice of `L` and the set of shortest vectors (up to sign) of the shadow of `L`.

```
s3:=function(L)
   L0:=EvenSublattice(L);
   L0d:=Dual(L0:Rescale:=false);
   dq,f:=L0d/L0;
   reps:=[ x : x in dq | not L0d!(x @@ f) in L ];
   return L0d,&join[ { L0d | u
      : u in ShortestVectors(sub< L0d | L0,x @@ f >) }
      : x in reps ];
end function;
```

Let `B` be a basis of an integral lattice L, and let `f` be a 3-frame of L. The following function constructs a ternary code `C` such that L is isomorphic to the lattice `Lattice(C,"A")` and there exists an isomorphism which maps `f` to the standard 3-frame of `Lattice(C,"A")`.

```
LB2code:=function(B,f)
   V:=VectorSpace(GF(3),#B);
   return LinearCode< GF(3),#B
      | [ V![ GF(3)!(b,x) : x in f ] : b in B ] >;
end function;
```

5 Definitions

According to Bacher and Venkov [1], all the extremal odd unimodular lattices of rank 28 are obtained as a neighbour of the standard lattice. These are the unimodular lattices of rank 28 with minimum norm 3. Let `S` denote the standard lattice of rank 28:

```
S:=StandardLattice(28);
```

The following function constructs the neighbour of `S` with respect to a vector `v` of `S` and a positive integer `k`.

```
neighbourZk:=function(v,k)
   cmn:=Dual(ext< S | 1/k*v > : Rescale:=false);
   return ext< cmn | 1/k*v >;
end function;
```

The actual data are taken from [1].

```
vs:=[ S |
[1,2,4,5,7,8,9,57,11,12,13,14,15,16,17,18,19,20,21,22,24,25,27,28,29,30,32,33],
[1,3,4,5,6,7,8,58,10,11,12,13,14,15,17,18,19,20,21,22,23,24,27,29,30,31,32,33],
[1,3,4,5,6,7,8,9,10,12,14,16,17,18,86,20,21,22,23,24,25,26,27,28,29,30,31,32],
[1,2,5,6,8,9,10,12,13,14,15,16,17,18,19,47,21,22,23,24,25,27,28,29,30,31,32,33],
[68,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,24,26,28,30,32,33],
[1,2,3,4,5,6,7,8,9,10,11,12,80,14,82,16,17,18,19,20,25,26,27,29,30,31,32,33],
[1,2,3,4,5,6,7,8,9,10,11,12,14,15,16,18,20,21,22,23,24,25,26,94,28,29,32,33],
[1,2,3,4,7,8,9,10,11,12,13,14,15,45,17,18,19,20,21,22,23,24,25,26,27,28,29,30],
```

```
[1,2,3,4,5,61,7,8,9,10,12,13,14,15,16,18,19,20,21,22,24,25,26,27,29,30,31,33],
[1,2,3,4,5,6,60,9,10,11,12,13,14,15,16,17,19,20,21,23,24,25,26,27,28,31,32,33],
[1,2,3,4,76,6,7,8,9,10,11,12,13,14,15,16,17,18,19,21,22,24,25,27,29,31,33,34],
[1,65,3,4,5,6,7,8,9,10,11,12,13,14,15,18,19,20,21,22,23,24,26,27,28,29,30,31],
[66,2,3,4,5,6,7,8,9,10,11,12,13,14,16,17,18,19,20,21,23,24,25,26,27,29,31,33],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,22,26,27,30,32,33,34,106],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,16,17,18,19,20,21,22,24,27,28,32,33,34,106],
[1,2,3,4,5,6,7,8,9,10,11,12,13,15,17,18,20,22,23,91,25,26,27,28,29,30,31,33],
[1,2,3,71,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,24,25,26,27,28,29,30],
[1,2,3,71,5,6,7,8,9,10,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,28,33],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,19,20,22,24,25,26,29,30,33,34,106],
[1,2,3,4,5,6,7,59,9,10,11,12,13,14,15,18,20,21,23,24,25,26,27,28,29,30,31,32],
[1,2,3,4,5,6,7,8,9,10,11,12,13,15,16,18,19,21,23,24,25,28,29,30,105,33,35,36],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,19,20,23,26,27,99,29,30,31,33,34,35],
[1,75,3,4,5,6,7,8,9,10,11,12,13,14,15,17,18,22,23,24,26,27,28,30,104,34,35,36],
[1,2,3,4,5,6,7,8,10,11,13,16,17,18,20,21,23,24,48,47,27,29,30,31,32,33,35,36],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,19,20,22,25,27,29,30,31,33,35,109],
[1,77,3,4,5,6,7,8,9,10,11,12,13,14,16,17,21,23,24,25,26,27,29,31,33,45,35,39],
[1,4,5,6,12,14,15,16,17,18,20,23,24,26,27,28,29,37,38,46,48,50,51,56,58,59,69,93],
[1,2,3,4,5,6,7,8,9,89,11,12,13,15,16,17,21,104,26,27,29,30,31,33,34,36,37,39],
[1,2,3,4,5,6,7,8,9,10,11,12,13,14,17,18,19,21,22,23,25,26,27,28,33,107,35,36],
[1,2,3,4,5,6,9,10,11,12,13,16,19,20,23,27,29,33,34,40,41,49,51,52,58,59,92,97],
[1,5,7,8,12,15,16,17,18,19,21,23,27,30,32,33,39,40,42,43,44,47,48,49,52,53,55,56],
[1,2,3,4,5,6,7,65,9,10,11,12,13,14,17,18,20,21,22,26,27,29,30,31,33,34,35,36],
[1,116,4,5,6,7,12,16,17,19,20,21,23,24,27,28,29,30,33,34,35,37,42,45,46,48,49,55],
[1,4,5,6,17,19,21,22,23,24,28,29,30,165,33,161,40,43,53,59,61,62,65,71,76,83,93,95],
[1,3,4,108,7,10,12,16,19,20,21,23,27,28,29,30,33,34,35,37,38,39,40,43,47,48,49,54],
[1,2,4,7,8,9,102,13,14,15,16,18,22,25,26,28,30,31,32,36,41,44,49,50,51,52,53,56]
];

ks:=[67,67,67,67,67,67,67,61,67,67,71,67,67,71,71,67,67,67,71,67,73,71,
73,73,73,79,118,79,73,118,106,73,113,197,113,113];
```

6 Construction of a Graph

Lemma 1. *Let L be an extremal unimodular lattice of rank 28 having a 3-frame $u_1, \ldots, u_{28}$. Let L_0 be the even sublattice of the lattice L. If $u \in L_0^* \setminus L$, then*

$$u = \frac{1}{6} \sum_{i=1}^{28} \lambda_i u_i \tag{1}$$

for some odd integers $\lambda_1, \ldots, \lambda_{28}$.

Lemma 2. *Let C be an extremal ternary self-dual code of length 28. Let $u_1, \ldots, u_{28}$ be a 3-frame of $L = A_3(C)$ coming from C. Let L_0 be the even sublattice of the lattice L. Then L_0^* has minimum norm 3. Moreover, For any element $u \in L_0^* \setminus L$ of norm 3, there exists a unique $i_0 \in \{1, \ldots, 28\}$ such that*

$$|(u, u_i)| = \begin{cases} \frac{3}{2} & \text{if } i = i_0, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

For a lattice L, a vector u not necessarily in L, an integer m and a real number c, set

$$L_{m,c}(u) = \{v \mid v \in L,\ (v,v) = m,\ (u,v) = \pm c\}. \tag{2}$$

Lemma 3. *Let L be an extremal unimodular lattice of rank 28. Let S_3 be the set of elements of norm 3 in $L_0^* \setminus L$. Let u_1, u_2 be orthogonal elements of L of norm 3. If there exists a 3-frame containing u_1 and u_2, then*

$$\{u_1, u_2\} \not\subset L_{3,3/2}(u) \quad (\forall u \in S_3). \tag{3}$$

Proof. Immediate from Lemma 2. □

7 The Main Program

Set the number for the lattice to be considered, for example, set

```
Ln:=35;
```

for the 35th lattice of [1]. We first define the lattice `L`, and verify the basic properties.

```
L:=CoordinateLattice(neighbourZk(vs[Ln],ks[Ln]));
L3:={@ {x,-x} : x in ShortestVectors(L) @};
IsIntegral(L);
Determinant(L) eq 1;
Minimum(L) eq 3;
v:=1120;
#L3 eq v;
```

We construct the set `S3` of elements of norm 3 in $L_0^* \setminus L$. For each u in `S3`, we construct the set $L_{3,3/2}(u)$ defined in (2).

```
L0d,S3:=s3(L);
L3r:=[ L0d | Random(p) : p in L3 ];
L323us:={ { i : i in [1..v]
   | AbsoluteValue((u,L3r[i])) eq 3/2 } : u in S3 };
```

The function `adjL3` defined below, returns false if we can conclude that there exists no 3-frame containing both the i-th element and the j-th element of `L3`. It checks the orthogonality, and the condition (3).

```
adjL3:=function(i,j)
   return (Random(L3[i]),Random(L3[j])) eq 0
      and not exists(tt){ X : X in L323us | {i,j} subset X };
end function;
```

Then we define the graph `Gamma`, whose set of vertices is the set of 1120 pairs of the shortest vectors, and two vertices are adjacent whenever the function `adjL3` defined above returns the value `true`. It follows that the 3-frames are precisely the 28-cliques in the graph `Gamma`.

```
edges:=&join{
   { {i,j} : j in {i+1..v} | adjL3(i,j) } : i in {1..v-1} };
Gamma:=Graph< v | edges >;
```

For some lattices, there are too many 3-frames to enumerate. However, if we note that two 3-frames which are conjugate under the automorphism group of the lattice `L` lead to equivalent ternary codes, it suffices to find a set of representatives of 28-cliques of `Gamma` up to the action of the automorphism group of `L`. We compute this automorphism group. Note that the order of this automorphism group is given in [1], so we should make sure that the output agrees with [1].

```
AutL:=AutomorphismGroup(L);
print "#AutL=",#AutL;
```

Then we construct the permutation group induced by the action of `AutL` on `L3`. Note that `AutL` contains -1 which is in the kernel of the action on `L3`. Thus the order of the permutation group is half of `#AutL`.

```
G:=actionImage(AutL,L3);
#G eq (#AutL div 2);
```

It follows from the construction that `G` is a group of automorphisms of the graph `Gamma`. We now enumerate all 28-cliques of `Gamma` up to the action of `G` by our program. This computation may take up to a day, depending on the number of inequivalent cliques.

```
ac:=allCliquesUpToG(Gamma,G,28);
```

Finally, we convert each 28-clique to a 3-frame, and then to a ternary self-dual code.

```
B:=Basis(L);
frms:=[ [ Random(L3[Index(i)]) : i in c ] : c in ac ];
codes:=[ LB2code(B,f) : f in frms ];
&and{ IsSelfDual(C) : C in codes };
```

We save the result in a reloadable file.

```
outputfile:="L" cat IntegerToString(Ln) cat ".magma";
PrintFile(outputfile,"codes:=");
PrintFileMagma(outputfile,codes);
PrintFile(outputfile,";");
```

For the 35th lattice, it took 4327.199 seconds to perform all the computation documented in this report, on Sun Ultra 45 running Solaris 10 (64bit), MAGMA 2.14-11. The entire results are available from [3].

References

[1] R. Bacher and B. Venkov, Réseaux entiers unimodulaires sans racines en dimensions 27 et 28, Réseaux euclidiens, designs sphériques et formes modulaires, 212–267, Monogr. Enseign. Math., 37, Enseignement Math., Geneva, 2001.

[2] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[3] M. Harada and A. Munemasa, Database of Self-Dual Codes, Available online at `http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm`.

[4] M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, submitted.

Any Diophantine quintuple contains a regular Diophantine quadruple

Yasutsugu Fujita

1 Introduction

Diophantus raised the problem of finding a set of four (rational) numbers which has the property that the product of any two numbers in the set increased by one is a square, and found such a set $\{1/16, 33/16, 68/16, 105/16\}$ of four positive rational numbers. Fermat first found a set of four positive integers with the above property, which was $\{1, 3, 8, 120\}$. A set $\{a_1, \ldots, a_m\}$ of m distinct positive integers is called a Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all i, j with $1 \leq i < j \leq m$. In 1979, Arkin, Hoggatt and Strauss ([1]) found that for any Diophantine triple $\{a, b, c\}$, $\{a, b, c, d_+\}$ is a Diophantine quadruple, where $d_+ = a + b + c + 2abc + 2rst$ and $r = \sqrt{ab+1}$, $s = \sqrt{ac+1}$, $t = \sqrt{bc+1}$. Such a Diophantine quadruple is called regular. For a fixed Diophantine triple $\{a, b, c\}$, d_+ is the smallest among the d's such that $\{a, b, c, d\}$ is a Diophantine quadruple with $d > \max\{a, b, c\}$ (cf. [6, Proof of Lemma 6]). They also conjectured the following.

Conjecture 1.1. (cf. [1]) *All the Diophantine quadruples are regular.*

This immediately implies a folklore conjecture, which says that there does not exist a Diophantine quintuple. The first result supporting Conjecture 1.1 is due to Baker and Davenport ([2]), who showed that if $\{1, 3, 8, d\}$ is a Diophantine quadruple, then $d = 120$. Since 1990s, this result has been generalized in large part by Dujella and the following has been known.

Theorem 1.2. (cf. [5], [7], [8] and [4]) *Let $k \geq 2$ be an integer. If $\{k-1, k+1, c, d\}$ is a Diophantine quadruple with $c < d$, then $d = d_+$.*

In general, Dujella ([6]) showed that there does not exist a Diophantine sextuple and that there exist only finitely many Diophantine quintuples.

Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Then, it is not difficult to see that all the quadruples contained in the quintuple, other than $\{a, b, c, d\}$, are irregular (cf. [6, Proof of Corollary 1]). We assert that the remaining quadruple $\{a, b, c, d\}$ is always regular.

Theorem 1.3. *If $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$, then $d = d_+$.*

Theorem 1.3 immediately implies one of the above-mentioned results of Dujella.

Corollary 1.4. ([6, Theorem 2]) *There does not exist a Diophantine sextuple.*

In the following section, we give an outline of the proof of Theorem 1.3, where considering the cases $b \geq 2a$ and $b < 2a$ separately is strategically important.

2 Proof of Theorem 1.3

Suppose that $d > d_+$. First, look at the quadruple $\{a, b, c, d\}$. Then there exist integers x, y, z such that $ad + 1 = x^2$, $bd + 1 = y^2$, $cd + 1 = z^2$, from which eliminating d, we obtain the system of Diophantine equations

$$az^2 - cx^2 = a - c, \tag{2.1}$$
$$bz^2 - cy^2 = b - c. \tag{2.2}$$

Put $r = \sqrt{ab+1}$, $s = \sqrt{ac+1}$ and $t = \sqrt{bc+1}$.

Lemma 2.1. (cf. [6, Lemma 1]) *Let (z, x), (z, y) be positive solutions of* (2.1), (2.2), *respectively. Then there exist solutions (z_0, x_0) of* (2.1) *and (z_1, y_1) of* (2.2) *in the ranges $1 \leq x_0 < 0.76\sqrt[4]{ac}$, $1 \leq |z_0| < 0.269c$, $1 \leq y_1 < 0.723\sqrt[4]{bc}$, $1 \leq |z_1| < 0.148c$ such that*

$$z\sqrt{a} + x\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^m, \tag{2.3}$$
$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{a} + y_1\sqrt{c})(t + \sqrt{bc})^n \tag{2.4}$$

for some integers $m, n \geq 0$.

By (2.3) we may write $z = v_m$, where

$$v_0 = z_0,\ v_1 = sz_0 + cx_0,\ v_{m+2} = 2sv_{m+1} - v_m,$$

and by (2.4) we may write $z = w_n$, where

$$w_0 = z_1,\ w_1 = tz_1 + cy_1,\ w_{n+2} = 2tw_{n+1} - w_n.$$

By checking closely that $v_m \neq w_n$ for small m, n, we obtain the following gap principle.

Proposition 2.2. *Suppose that $\{a, b, c, d\}$ is an irregular Diophantine quadruple with $a < b < c < d$. Then, either $d > \max\{400a^5b^6, 100b^7\}$ or $d > 60b^8$. In case $b < 2a$, we have $d > 1400b^{12.5}$ unless $c = a + b + 2r$.*

Secondly, look at the quadruple $\{a, b, d, e\}$. Replace c, d in the above argument by d, e, respectively, and use the same symbols x, y, z, v_m, w_n as above (i.e., $ae + 1 = x^2$, $be + 1 = y^2$, $ce + 1 = z^2$, $z = v_m = w_n$). Then, considering the equation $v_m = w_n$ as $v_m \equiv w_n \pmod{d^2}$, we obtain lower bounds for n in terms of a, b and d (e.g, if $v_{2m+1} = w_{2n+1}$ has a solution with $m, n \geq 2$, then $n > \max\left\{0.586a^{-1/4}b^{-1/4}d^{1/4}, 0.816b^{-3/4}d^{1/4}\right\}$).

In order to get an upper bound for n, we need (a modification of) a theorem of Bennett ([3, Theorem 3.2]), which is based on Padé approximation method (cf. [10]).

Theorem 2.3. (cf. [3, Theorem 3.2], [9, Theorem]) *Let a, b and N be integers with $0 < a < b$, $b \geq 8$ and $N > 2.4a'a^2b^4(b-a)^2$, where $a' = \max\{b-a, a\}$. Then the numbers $\theta_1 = \sqrt{1+b/N}$ and $\theta_2 = \sqrt{1+a/N}$ satisfy*

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > (16.01a'b^2N)^{-1}q^{-\lambda} \tag{2.5}$$

for all integers p_1, p_2, q with $q > 0$, where

$$\lambda = 1 + \frac{\log(8.01a'b^2N)}{\log(3.37a^{-2}b^{-2}(b-a)^{-2}N^2)} < 2.$$

In view of Proposition 2.2, $N = abd$ satisfies the assumption in Theorem 2.3 (Note that we may assume that $b \geq 8$ because of Theorem 1.2). We apply Theorem 2.3 with $N = abd$, $p_1 = sbx$, $p_2 = tay$ and $q = abz$. From the system of Diophantine equations (2.1) and (2.2) with c replaced by d, it is easy to see that

$$\max\left\{\left|\theta_1 - \frac{sbx}{abz}\right|, \left|\theta_2 - \frac{tay}{abz}\right|\right\} < \frac{c}{2a}z^{-1},$$

which together with the inequality (2.5) yields an upper bound for z, and hence we get an upper bound for n in terms of a, b and d. Combined with the lower bounds for n, we obtain the following.

Proposition 2.4. *Suppose that $\{a, b, d, e\}$ is an irregular Diophantine quadruple with $a < b < d < e$.*

(1) *If $b \geq 2a$, then $d < \max\{100a^5b^6, 100b^7\}$ and $d < 20b^8$.*

(2) *If $b < 2a$, then $d < 100b^{12.5}$.*

If either $b \geq 2a$ or $c \neq a + b + 2r$, then Propositions 2.2 and 2.4 contradict each other. Hence, we may assume that $b < 2a$ and $c = a + b + 2r$. Now look at the quadruple $\{b, c, d, e\}$. Then, we can arrive at a contradiction again using Propositions 2.2 and 2.4 (with a, b replaced by b, c, respectively). This completes the proof of Theorem 1.3.

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. 17 (1979), 333–339.

[2] A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$*, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[3] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. 498 (1998), 173–199.

[4] Y. Bugeaud, A. Dujella and M. Mignotte, *On the family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$*, Glasgow Math. J. 49 (2007), 333–344.

[5] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen 51 (1997), 311–322.

[6] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214.

[7] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) 49 (1998), 291–306.

[8] Y. Fujita, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, J. Number Theory 128 (2008), 322–353.

[9] J. H. Rickert, *Simultaneous rational approximation and related Diophantine equations*, Math. Proc. Cambridge Philos. Soc. 11 (1993), 461–472.

[10] I. Wakabayashi, *On families of cubic Thue equations*, in Analytic Number Theory, C. Jia and K. Matsumoto (eds.), Developments in Mathematics Vol. 6, Kluwer Academic Publishers, 2002, 359–377.

統計への応用を考えた 対称式の基底変換アルゴリズム

山口 幸司* 仁木 直人†

1 序

1.1 はじめに

統計量の分布を求めることは，検定や推定の基礎であり，統計の分野における基本的なテーマである．しかし，統計量を表す式が簡単で，母集団が正規分布である場合などを除き，統計量分布を表す正確な式が求められることは希であり，ほとんどの場合は標本サイズなどに関する漸近展開（Edgeworth 展開など）による近似に頼らざるを得ない．しかし，高次の漸近展開をするためには，高次の統計量モーメントが必要であり，その導出には膨大な量の計算が必要である．特定の統計量と母集団の組み合わせに限っては，数式処理の利用によって，この問題を乗り越えられる [4] が，他の一般的な統計量に対して適用できるような，汎用的な方法ではない．

統計量モーメントの汎用的な導出方法としては，対称式が成すベクトル空間の基底変換による方法 [10] がある．統計量を表す式を Power Sum Product (PSP) の荷重和で表し，それを Augmented Symmetric Function (ASF) の荷重和に変換 （P2A 変換）し，その期待値を母集団モーメントで書くという手順で，統計量モーメントを導出することができる．しかし，この方法にも，P2A 変換途中において計算量・必要メモリが爆発的に増大し，中間膨張を引き起こすという問題がある．

そこで，P2A 変換における中間膨張を抑制するため，以下の 3 つのアルゴリズムを提案する．

- 変換途中において生成される不要な高次項の早期削除
- パーティション長を考慮した全順序による，ASF が生成される順序規則に即したソート
- ASF の重複度表現による，同類項生成の抑制

*東京理科大学 工学研究科 経営工学専攻 / 〒 102-0073 東京都千代田区九段北 1-14-6
†東京理科大学 工学部 / 〒 102-0073 東京都千代田区九段北 1-14-6

また，アルゴリズムを Gnu Common Lisp[2] 上に実現するとともに，統計分布論において実際に生じる計算に適用し，これらの対策による中間膨張抑制効果を検証する．

1.2 モーメント統計量分布の漸近展開

1.2.1 モーメント統計量

Edgeworth 展開が適用できる主要な統計量のほとんどは，標本モーメントの滑らかな関数で表せるモーメント統計量である，モーメント統計量の例として，以下のようなものがある．

$$\text{標本平均} \qquad \frac{1}{n}\sum_{i=1}^{n} x_i = m'_1 \tag{1}$$

$$\text{標本分散} \qquad \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \Big(\frac{1}{n}\sum_{i=1}^{n} x_i\Big)^2 = m'_2 - m'^2_1 \tag{2}$$

$$\text{標本歪度} \qquad \frac{m_3}{\sqrt{m_2^3}} \tag{3}$$

$$\text{標本尖度} \qquad \frac{m_4}{m_2^2} \tag{4}$$

ここに，x_i はそれぞれ独立に同一の母集団に従う確率変数，n はそのサンプルサイズであり，m'_r は原点周りの r 次標本モーメント，m_r は平均周りの r 次標本モーメントを表す．

モーメント統計量を標準化した確率変数 $X_n{=}\frac{\sqrt{n}(T_n-\theta)}{\sigma}$ のキュムラント κ_r は，以下の Cornish-Fisher assumption を満たすことが知られている．

$$\begin{aligned}
\kappa_1 &= n^{-\frac{1}{2}}\kappa_{1,1} + n^{-\frac{3}{2}}\kappa_{1,3} + n^{-\frac{5}{2}}\kappa_{1,5} + n^{-\frac{7}{2}}\kappa_{1,7} + \cdots \\
\kappa_2 &= 1 + n^{-1}\kappa_{2,2} + n^{-2}\kappa_{2,4} + n^{-3}\kappa_{2,6} + n^{-4}\kappa_{2,8} + \cdots \\
\kappa_r &= n^{-\frac{r-2}{2}}\kappa_{r,r-2} + n^{-\frac{r}{2}}\kappa_{r,r} + n^{-\frac{r+2}{2}}\kappa_{r,r+2} + \cdots \qquad (r \geq 3)
\end{aligned} \tag{5}$$

1.2.2 Edgeworth 展開

統計量分布の漸近展開において，最も有名なものに Edgeworth 展開がある．Edgeworth 展開は標本サイズ n に関する漸近展開である．母集団パラメータ θ を推定する統計量 $T_n{=}T(P_n)$ の Edgeworth 展開は，統計量を標準化した確率変数 X_n の統計量キュムラント κ_r を用いて，以下のように計算できる．

$$\begin{aligned}
F(x) \sim \Phi(x) - \phi(x)\Big[\Big\{\frac{1}{6}\kappa_3 H_2(x) + \kappa_1\Big\} + \Big\{\frac{1}{72}\kappa_3^2 H_5(x) \\
+\big(\frac{1}{6}\kappa_1\kappa_3 + \frac{1}{24}\kappa_4\big)H_3(x) + \big(\frac{1}{2}\kappa_1^2 + \frac{1}{2}(\kappa_2 - 1)\big)H_1(x)\Big\} + \cdots\Big]
\end{aligned} \tag{6}$$

$$\sim \Phi(x) - \phi(x)\Big[n^{-\frac{1}{2}}\Big\{\frac{1}{6}\kappa_{3,1}H_2(x) + \kappa_{1,1}\Big\} + n^{-1}\Big\{\frac{1}{72}\kappa_{3,1}^2 H_5(x) + \big(\frac{1}{6}\kappa_{1,1}\kappa_{3,1} + \frac{1}{24}\kappa_{4,2}\big)H_3(x) + \big(\frac{1}{2}\kappa_{1,1}^2 + \frac{1}{2}(\kappa_{2,2}-1)\big)H_1(x)\Big\}\Big] + O\Big(n^{-\frac{3}{2}}\Big) \tag{7}$$

$\Phi(x)$，$\phi(x)$ はそれぞれ標準正規分布の分布関数と密度関数であり，$H_j(x)$ は j 次 Hermite 多項式である．また，$\kappa_{r,s}$ は κ_r の $\frac{1}{\sqrt{n^s}}$ の係数である．

式 (5) より，X_n の r 次キュムラント $\kappa_r (r \geq 3)$ には，n の次数に関して $-\frac{r-2}{2}$ より低次の項が含まれないことがわかる．よって，Edgeworth 展開のオーダを $n^{-\frac{r}{2}}$ までとしたとき，r+2 次までのキュムラントが必要であることがわかる．

キュムラントとは，モーメントと同じく分布の特徴を表すパラメータであり，キュムラント母関数 $\log M(t)$ によって定義される．なお，$M(t)$ はモーメント母関数

$$M(t) = \mathrm{E}(e^{tX}) = \mathrm{E}\left(1 + tX + \frac{1}{2!}t^2X^2 + \frac{1}{3!}t^3X^3 + \cdots\right) \tag{8}$$

である．実際にキュムラントを求めるには，以下の変換公式が使える．

$$\begin{aligned}
\kappa_1 &= \lambda_1' \\
\kappa_2 &= \lambda_2' - \lambda_1'^2 = \lambda_2 \\
\kappa_3 &= \lambda_3' - 3\lambda_2'\lambda_1' + 2\lambda_1'^3 = \lambda_3 \\
\kappa_4 &= \lambda_4' - 4\lambda_3'\lambda_1' - 3\lambda_2'^2 + 12\lambda_2'\lambda_1'^2 - 6\lambda_1'^4 = \lambda_4 - 3\lambda_2^2 \\
&\vdots
\end{aligned} \tag{9}$$

なお，λ_r' は原点周りのモーメント，λ_r は平均周りのモーメントである．ここでも，r 次キュムラントには r より低次のモーメントしか含まれていないため，r 次キュムラントまでを求めるには r 次モーメントまでが必要であることがわかる．

式 (9) により，X_n のモーメントからキュムラントを求めることができ，それを用いて Edgeworth 展開をすることができる．しかし，より高次の Edgeworth 展開をするためには，高次の統計量モーメントが必要であり，その導出には膨大な量の計算が必要である．特定の統計量や母集団に限っては，数式処理の利用によって，この問題を乗り越えられるが，他の一般的な統計量に対して適用できるような，汎用的な方法ではない [7].

1.2.3 対称式を用いた統計量モーメントの導出

統計量モーメントの汎用的な導出方法としては，対称式が成すベクトル空間の基底変換による方法がある [10]．モーメント統計量は標本モーメントの

滑らかな関数で表せ，標本モーメント m'_r, m_r が対称式であるため，この方法が適用できる．

なお，標本歪度 (3) や標本尖度 (4) は対称関数ではあるが対称式ではないため，Taylor 展開により，対称式を係数とする漸近展開に展開する必要がある．例として尖度 $\frac{m_4}{m_2^2}$ は，補助的な確率変数

$$U = \frac{\sqrt{n}(m_2 - \mu_2)}{\mu_2}\ , \quad W = \frac{\sqrt{n}(m_4 - \mu_4)}{\mu_4} \tag{10}$$

を導入することで，Taylor 展開により，

$$\begin{aligned}\frac{m_4}{m_2^2} &= \frac{\mu_4}{\mu_2^2}\Big(1 + \frac{W}{\sqrt{n}}\Big)\Big(1 + \frac{U}{\sqrt{n}}\Big)^{-2} \\ &= \frac{\mu_4}{\mu_2^2}\big(1 + \frac{1}{\sqrt{n}}(W - 2U) + \frac{1}{n}(3U^2 - 2UW) + \cdots\big)\end{aligned} \tag{11}$$

のように $\frac{1}{\sqrt{n}}$ に関するべき級数に展開できる．$U^r W^s$ は対称多項式であるため，(11) は対称多項式であり，対称式の基底変換法が適用できる．

統計量モーメントの導出に用いる対称式は，Power Sum (PS) の積である Power Sum Product (PSP) と Augmented Symmetric Function (ASF) である．$x_1, x_2, \cdots, x_n$ を独立変数としたとき，PSP の定義は以下である．

$$\begin{aligned}p[r_1\ r_2\ \cdots\ r_l] &= p[r_1]p[r_2]\cdots p[r_l] \\ &= \sum_{i_1, i_2, \cdots, i_l} x_{i_1}^{r_1} x_{i_2}^{r_2} \cdots x_{i_l}^{r_l}\end{aligned} \tag{12}$$

ここで，$\sum_{i_1,i_2,\cdots,i_l} = \sum_{i_1}\sum_{i_2}\cdots\sum_{i_l}$ であり，以後暗黙のうちに 1 から n までをわたるものとする．また，対称式の引数部分 $[\boldsymbol{\pi}]$ の分割をパーティションと呼び，$|\boldsymbol{\pi}|$ をパーティションの長さと呼ぶことにする．なお，長さが 1 の PSP は PS と同義である．

PSP により，モーメント統計量をその荷重和で表すことができる．以下に標本分散 (2) の例を挙げる．

$$\frac{1}{n}\sum_i x_i^2 - \frac{1}{n^2}\Big(\sum_i x_i\Big)^2 = \frac{1}{n}p[2] - \frac{1}{n^2}p[1\ 1] \tag{13}$$

次に，ASF の定義は以下である．

$$a[r_1\ r_2\ \cdots\ r_l] = \sum_{i_1 \neq \cdots \neq i_l} x_{i_1}^{r_1} x_{i_2}^{r_2} \cdots x_{i_l}^{r_l} \tag{14}$$

ただし，$\sum_{i_1\neq\cdots\neq i_l} = \sum_{i_1}\sum_{i_2\neq i_1}\cdots\sum_{i_l\neq i_1,\cdots,i_{l-1}}$ である．ASF を用いる理由は，$x_1, x_2, \cdots, x_n$ がそれぞれ独立に同一の母集団分布に従う確率変数であるとき，その期待値が

$$\mathrm{E}\left(a[r_1\ r_2\ \cdots\ r_l]\right) = \prod_{i=1}^{l}(n{+}1{-}i)\mu'_{r_i} \tag{15}$$

のように，母集団の原点周りのモーメント μ'_r ときれいに対応していることにある．よって，PSP の荷重和で表した統計量を ASF の荷重和に変換（以後，P2A 変換と呼ぶ）し，母集団モーメントで表せば，統計量とそのべき乗の期待値である統計量モーメントが求められる．

1.2.4 対称式の基底変換法

P2A 変換の基礎となる公式 [10] は以下である．

$$p[r_1] = a[r_1] \tag{16}$$

$$\begin{aligned} a[r_1\ r_2\ \cdots\ r_l] \times p[s] = {} & a[r_1{+}s\ r_2\ \cdots\ r_l] + a[r_1\ r_2{+}s\ r_3\ \cdots\ r_l] \\ & + \cdots + a[r_1\ \cdots\ r_{l-1}\ r_l{+}s] + a[r_1\ \cdots\ r_l\ s] \end{aligned} \tag{17}$$

式 (16) より，PS はそのまま ASF である．以降，(17) のように ASF に PS を一つずつかけていくことで，P2A 変換をすることができる．

標本分散 V の 1 次モーメントと 2 次モーメントを例に，統計量モーメントを導出するまでの手順を以下に示す．

1. 統計量を PSP の荷重和で表す —(18)
2. P2A 変換を行う —(19)
3. 期待値を母集団モーメントで書く —(20)

$$V = \frac{1}{n}p[2] - \frac{1}{n^2}p[1\ 1] \tag{18}$$

$$= \frac{1}{n}a[2] - \frac{1}{n^2}a[2] - \frac{1}{n^2}a[1\ 1] \tag{19}$$

$$\mathrm{E}[V] = \frac{n-1}{n}\mu'_2 - \frac{n-1}{n}\mu'^2_1 \tag{20}$$

2 次以上の統計量モーメントは，(18) を累乗し，以降は手順 2. と手順 3. を同じようにすれば求められる．

$$\begin{aligned} V^2 &= \frac{1}{n^2}p[2\ 2] - \frac{2}{n^3}p[2\ 1\ 1] + \frac{1}{n^4}p[1\ 1\ 1\ 1] \\ &= \frac{1}{n^2}(a[4] + a[2\ 2]) - \frac{2}{n^3}(a[4] + 2a[3\ 1] + a[2\ 2] + a[2\ 1\ 1]) \\ &\quad + \frac{1}{n^4}(a[4] + 4a[3\ 1] + 3a[2\ 2] + 6a[2\ 1\ 1] + a[1\ 1\ 1\ 1]) \end{aligned} \tag{21}$$

$$\begin{aligned} \mathrm{E}[V^2] = {} & \frac{(n-1)^2}{n^3}\mu'_4 - \frac{4(n-1)^2}{n^3}\mu'_3\mu'_1 + \frac{(n-1)(n^2-2n+3)}{n^3}\mu'^2_2 \\ & - \frac{2(n-1)(n-2)(n-3)}{n^3}\mu'_2\mu'^2_1 + \frac{(n-1)(n-2)(n-3)}{n^3}\mu'^4_1 \end{aligned} \tag{22}$$

Table 1: P2A 変換後の ASF の項数

PSP のパーティションの長さ	P2A 変換後の ASF の項数
1	1
2	2
3	5
4	15
5	52
10	115975
20	5.17×10^{13}
30	8.47×10^{23}

P2A 変換による高次の統計量モーメント導出には，P2A 変換途中おいて計算量・必要メモリが爆発的に増大し，中間膨張を引き起こすという問題がある．P2A 変換前の PSP のパーティション長と，P2A 変換後の ASF の項数を Table 1 に示す.

Table 1 の ASF の項数は，P2A 変換途中に生成される ASF の同類項を全くまとめず，放っておいたまま変換したときの項数である．そのため，中間膨張を抑えるには，P2A 変換途中に ASF の同類項を度々まとめる必要がある．

また，P2A 変換後の ASF の荷重和には，最終的に Edgeworth 展開に使われない高次項が多く含まれている可能性がある．統計量の計算に頻出する P2A 変換を例に，まず変換過程を以下に示す.

$$\begin{aligned}\frac{1}{n^4}p[1\ 1\ 1\ 1] &= \frac{1}{n^4}(a[1]\times p[1\ 1\ 1]) \\ &= \frac{1}{n^4}(a[2]+a[1\ 1])\times p[1\ 1] \\ &= \frac{1}{n^4}(a[3]+3a[2\ 1]+a[1\ 1\ 1])\times p[1] \\ &= \frac{1}{n^4}(a[4]+4a[3\ 1]+3a[2\ 2]+6a[2\ 1\ 1]+a[1\ 1\ 1\ 1])\end{aligned} \tag{23}$$

式 (23) において，それぞれの ASF の期待値は，

$$\mathrm{E}(\frac{1}{n^4}a[4]) = \frac{n\mu_4'}{n^4}, \tag{24}$$

$$\mathrm{E}(\frac{1}{n^4}a[3\ 1]) = \frac{n(n-1)\mu_3'\mu_1'}{n^4} \tag{25}$$

$$\mathrm{E}(\frac{1}{n^4}a[2\ 2]) = \frac{n(n-1)\mu_2^2}{n^4} \tag{26}$$

$$\mathrm{E}(\frac{1}{n^4}a[2\ 1\ 1]) = \frac{n(n-1)(n-2)\mu_2\mu_1^2}{n^4} \tag{27}$$

$$\mathrm{E}(\frac{1}{n^4}a[1\ 1\ 1\ 1]) = \frac{n(n-1)(n-2)(n-3)\mu_1^4}{n^4} \tag{28}$$

となり，例として最終結果に必要な次数が n^{-1} であった場合，(24), (25), (26) はそれより高次であるため，最終的に不要な項であったということになる．さらに，(23) をさかのぼると，$a[3]$ からは $a[4]$, $a[3\ 1]$ しか生成されないため，その時点で $a[3]$ が不要であったということになる．

このように，Edgeworth 展開をある次数までと決め，それに必要な統計量モーメントを求める際に，不要な高次項を残したまま P2A 変換を続けると，それらが中間膨張の原因になる．そのため，P2A 変換途中で不要な高次項を順次削除していく必要がある．

2 中間膨張対策

2.1 不要な高次項の早期削除

P2A 変換途中に生成される不要な高次項が，中間膨張の原因になることが 1.2.4 節に示された．これを P2A 変換途中の早い段階で削除してやることで，中間膨張を抑制することができる．(23) について，以降不要な高次項にしかならない ASF を順次削除しながら変換すると，

$$\begin{aligned}
\frac{1}{n^4}p[1\ 1\ 1\ 1] &= \frac{1}{n^4}(a[1]\times p[1\ 1\ 1]) \\
&= \frac{1}{n^4}(a[2]+a[1\ 1])\times p[1\ 1] \\
&= \frac{1}{n^4}(\cancel{a[3]}+3a[2\ 1]+a[1\ 1\ 1])\times p[1] \\
&= \frac{1}{n^4}(\cancel{3a[3\ 1]}+\cancel{3a[2\ 2]}+6a[2\ 1\ 1]+a[1\ 1\ 1\ 1])
\end{aligned} \tag{29}$$

のように，引数であるパーティションの長さの短い ASF から削除すべきことがわかる．以後，パーティションの長さを “対称式の長さ” と呼ぶことにし，P2A 変換後に必要な ASF の長さの最小値（上記の例では 3）から，P2A 変換途中のある時点で削除すべき ASF の長さを以下のように決めることができる．

削除する ASF の長さ $<$ 変換後に必要な ASF の長さ$-$未変換の PSP の長さ (30)

実際の変換においては (30) により，不要な高次項の生成を予測し，不要な高次項を作らずに P2A 変換を進めていき，

$$\begin{aligned}
\frac{1}{n^4}p[1\ 1\ 1\ 1] &= \frac{1}{n^4}(a[1]\times p[1\ 1\ 1]) \\
&= \frac{1}{n^4}(a[2]+a[1\ 1])\times p[1\ 1]
\end{aligned}$$

$$= \frac{1}{n^4}(3a[2\ 1] + a[1\ 1\ 1]) \times p[1]$$
$$= \frac{1}{n^4}(6a[2\ 1\ 1] + a[1\ 1\ 1\ 1]) \tag{31}$$

のように，計算量とメモリ使用量を減らすことができる．

2.2 パーティションの長さ優先全順序によるソート

P2A 変換が進むと ASF の同類項が増えていき，中間膨張を起こす原因になるため，変換途中で同類項をまとめる必要がある．整理するタイミングとしては，ASF の荷重和に PS をかけ，同類項が生成された後である．ここで，P2A 変換途中の ASF の長さに注目すると，同類項は同長の ASF の間にしか存在しないことは自明であり，同類項の整理は同長の ASF 間だけで行えばよい．さらに (17) より，長さ l の ASF に PSP をかけると，長さ l と l+1 の ASF が生成される．このことから，ASF の荷重和に PS をかけると同時に，生成される ASF を長さごとにまとめることができ，そのために計算量が増えることは無い．その上で，同長の ASF 間ごとに同類項の整理を行うことで，全ての ASF を一緒くたに整理するよりもソートが速くなると考えられる．また，長さごとの集合に並ぶことを利用し，不要な高次項の削除判断を一括で行え，条件判断の回数を減らすことができる．

さらに，PS をかける際に “全ての ASF に PS をかけた後，長さごとにソート” するより，“特定の長さになる ASF ごとに PS をかけ，その度にソート” を繰り返すことで，PS をかけた直後（最もメモリを圧迫する瞬間）の同類項の大量発生による中間膨張を小さくすることができる．

以上をふまえ，ASF 集合における長さ優先全順序を以下のように定義する．ただし，パーティション間順序 $\underset{\text{rlex}}{\succ}$ は，逆辞書式順序を表す．

- 従来の順序 [9] (Reverse Lexical ordering)

$$a[\boldsymbol{\pi}] \succ a[\boldsymbol{\rho}] \underset{\text{def}}{\Leftrightarrow} \boldsymbol{\pi} \underset{\text{rlex}}{\succ} \boldsymbol{\rho} \qquad \text{(ただし係数は無視)} \tag{32}$$

- 新しい順序 (Length and Reverse Lexical ordering)

$$a[\boldsymbol{\pi}] \succ a[\boldsymbol{\rho}] \underset{\text{def}}{\Leftrightarrow} |\boldsymbol{\pi}| > |\boldsymbol{\rho}| \ \vee\ (|\boldsymbol{\pi}| = |\boldsymbol{\rho}| \ \wedge\ \boldsymbol{\pi} \underset{\text{rlex}}{\succ} \boldsymbol{\rho}) \tag{33}$$

- Reverse Lexical ordering によるソートの例

$$\begin{aligned} & p[4\ 3\ 2\ 1] \\ &= a[10] + a[9\ 1] + a[8\ 2] + 2a[7\ 3] + a[7\ 2\ 1] + 2a[6\ 4] + a[6\ 3\ 1] \\ &\quad + a[5\ 5] + a[5\ 4\ 1] + a[5\ 3\ 2] + a[4\ 4\ 2] + a[4\ 3\ 3] + a[4\ 3\ 2\ 1] \end{aligned} \tag{34}$$

- Length and Reverse Lexical ordering によるソートの例

$$
\begin{aligned}
&p[4\ 3\ 2\ 1] \\
&= a[10] + a[9\ 1] + a[8\ 2] + 2a[7\ 3] + 2a[6\ 4] + a[5\ 5] + a[7\ 2\ 1] \\
&\quad + a[6\ 3\ 1] + a[5\ 4\ 1] + a[5\ 3\ 2] + a[4\ 4\ 2] + a[4\ 3\ 3] + a[4\ 3\ 2\ 1]
\end{aligned} \tag{35}
$$

以降では，Reverse Lexical ordering に従ったソートおよび Length and Reverse Lexical ordering に従ったソートを，それぞれ “RL ソート” および “LRL ソート” と呼ぶ.

同長の ASF 間で同類項を整理する際は，それぞれに特徴を持つ 2 つの ASF の集まりをソートする必要がある．例えば,

$$
\begin{aligned}
&(a[9\ 1] + a[7\ 3] + a[5\ 5] + a[7\ 2\ 1] + a[6\ 3\ 1] + a[5\ 4\ 1]) \times p[1] && (36)\\
&= +a[10\ 1] + a[9\ 2] + a[8\ 3] + a[7\ 4] + a[6\ 5] + a[6\ 5] && (37)\\
&\quad + a[9\ 1\ 1] + a[7\ 3\ 1] + a[5\ 5\ 1] && (38)\\
&\quad + a[8\ 2\ 1] + a[7\ 3\ 1] + a[7\ 2\ 2] + a[7\ 3\ 1] + a[6\ 4\ 1] + a[6\ 3\ 2] \\
&\qquad\qquad + a[6\ 4\ 1] + a[5\ 5\ 1] + a[5\ 4\ 2] && (39)\\
&\quad + a[7\ 2\ 1\ 1] + a[6\ 3\ 1\ 1] + a[5\ 4\ 1\ 1] && (40)
\end{aligned}
$$

において，PS をかける前後のパーティション長に注目すると，長さが 1 増えた (38), (40) と，長さが変わらなかった (37), (39) があることがわかる.

ここで，ASF の集合をリストと呼ぶことにし，それぞれの特徴を整理すると,

- 長さが 1 増えたリスト
  初めから整列している
- 長さ変わらなかったリスト
  全体としてはある程度整列している中で，小さな整列した集合が並ぶ

同類項を整理すべき 2 つのリストがこのような特徴を持つため，その特徴を生かしたアルゴリズムを用いることでソートを高速化することができる．長さが 1 増えたリストを S，長さが変わらなかったリストを P，最終的に逆順ソートされて出力されるリストを L とし，メタ言語に Lisp の関数を用いてソートアルゴリズムのフローチャートを Fig. 1 に示す.

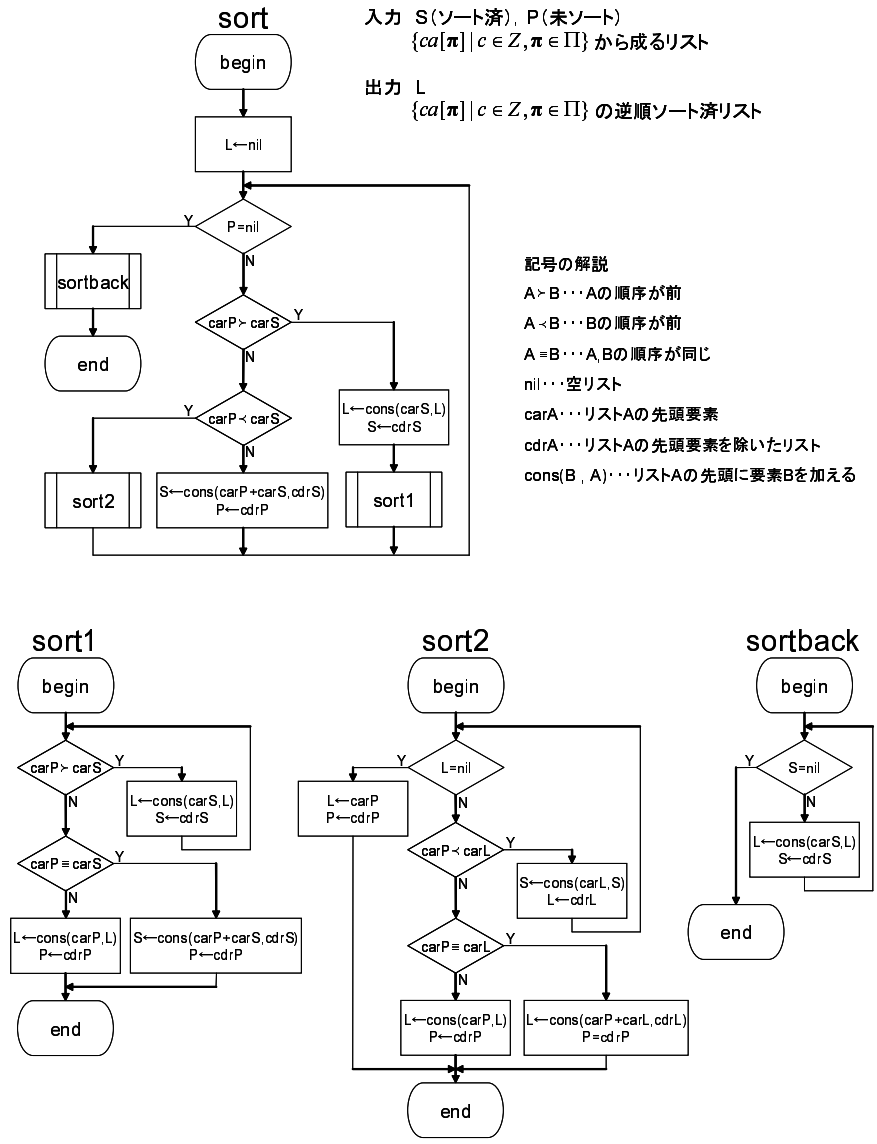

Fig. 1: ソートアルゴリズムのフローチャート

2.3 Augmented Symmetric Function の重複度表現

ASF のパーティション中に同じ数値が多数含まれていると，PS をかけた際に多数の同類項が生成される．そのため，データ内でのパーティションの表現を重複度表現にしておくことで，いたずらに同類項が生成されることを防ぎ，計算量，メモリ使用量の両方を節約することができる．通常の表現との違いは以下のようになる．

- 通常のパーティション表現

$$a[2\ 2\ 2\ 1\ 1\ 1\ 1] \tag{41}$$

- パーティションの重複度表現

$$a[2^3\ 1^4] \tag{42}$$

- 通常表現に PS をかけた場合

$$\begin{aligned} &a[2\ 2\ 2\ 1\ 1\ 1\ 1] \times p[1] \\ &= a[3\ 2\ 2\ 1\ 1\ 1\ 1] + a[3\ 2\ 2\ 1\ 1\ 1\ 1] + a[3\ 2\ 2\ 1\ 1\ 1\ 1] + a[2\ 2\ 2\ 2\ 1\ 1\ 1] \\ &+a[2\ 2\ 2\ 2\ 1\ 1\ 1] + a[2\ 2\ 2\ 2\ 1\ 1\ 1] + a[2\ 2\ 2\ 2\ 1\ 1\ 1] + a[2\ 2\ 2\ 1\ 1\ 1\ 1\ 1] \end{aligned} \tag{43}$$

- 重複度表現に PS をかけた場合

$$\begin{aligned} &a[2^3\ 1^4] \times p[1] \\ &= 3a[3^1\ 2^2\ 1^4] + 4a[2^4\ 1^3] + a[2^3\ 1^5] \end{aligned} \tag{44}$$

なお，P2A 変換途中において，重複度表現中の係数の平均値が小さく，係数中に 1 の割合が多いとき，重複度表現では係数を計算する手間が無駄になってしまい，通常表現で変換するより効率が悪くなる．そのため，どのような引数の組み合わせを持つ PSP の変換に重複度表現が有効であるかをあらかじめ確かめておき，実際にどちらの表現で変換するかを選ぶ必要がある．

3 効果の検証と考察

従来法（通常法）に対する提案法の効果を検証するため，Table 2 にある 3 つのバージョンの P2A 変換関数を Gnu Common Lisp を用いて作成し，実験を行う．LRL ソートの効果は p2a-2 と p2a-3 を比較し，重複度表現の効果は p2a-1 と p2a-2 を比較することで検証する．なお，不要な高次項の早期削除はどのバージョンでも行えるため，LRL ソートと重複度表現の効果の検証結果から，実験に用いるバージョンを検討する．

計算に使った環境は以下である．

- CPU ⋯ Intel Core 2 Duo E6600 2.40GHz

Table 2: P2A 変換関数のバージョン

バージョン	ソートの方法	ASF の表現
p2a-1	LRL	重複度
p2a-2	LRL	通常
p2a-3	RL	通常

- Memory ⋯ PC2-6400(DDR2-800) 1GB × 2
- Chipset ⋯ Intel P965 (FSB 1066MHz)

比較の内容は以下である.

- real ⋯ P2A 変換が終了するまでにかかった実時間（0.01 秒刻み）
- gbc ⋯ ガベージコレクションにかかった実時間（0.01 秒刻み）
- real-gbc ⋯ real − gbc　（P2A 変換自体にかかった実時間）
- gbc/real ⋯ $\frac{\text{gbc}}{\text{real}}$
- memory ⋯ メモリの割り当て容量（メモリ使用量の目安．MB 単位）
- real 効率 ⋯ $\frac{\text{従来法の real}}{\text{提案法の real}}$
- gbc 効率 ⋯ $\frac{\text{従来法の gbc}}{\text{提案法の gbc}}$
- real-gbc 効率 ⋯ $\frac{\text{従来法の real-gbc}}{\text{提案法の real-gbc}}$
- memory 効率 ⋯ $\frac{\text{提案法の memory}}{\text{従来法の memory}}$

3.1 パーティションの長さ優先全順序によるソート

LRL ソートの効果を検証するため，p2a-2 と p2a-3 を用いて次の 2 パターンの PSP を P2A 変換し，RL ソートとの比較を行った.

- 同類項があまり生成されない
  $p[11\ 10\ 9\ \cdots\ 1]$, $p[12\ 11\ 10\ \cdots\ 1]$, $p[13\ 12\ 11\ \cdots\ 1]$
- 同類項が大量に生成される（統計量の計算で頻出する）
  $p[1^{30}]$, $p[1^{35}]$, $p[1^{40}]$

LRL ソートを用いて P2A 変換を行った結果を Table 3 に，RL ソートを用いた結果を Table 4 に，およびそれらの比較による LRL ソートの効率を Table 5 に示す.

同類項があまり生成されない場合について Tables 3, 4 を比較すると，RL ソートに比べて LRL ソートのほうが real が短く，メモリ使用量が少ない. length が長くなった際の real の変化を比較をすると，RL ソートでは増加割

合が非常に大きい．さらに，Table 5 を見ると，大きい問題になるにつれて LRL ソートの効率が良くなっていく．これにより，LRL ソートは大量の ASF が生成される変換であるほどその効果が大きくなることが予想できる．

同類項が大量に生成される場合について Tables 3, 4 を比較すると，LRL ソートのほうが高速で，メモリ使用量が少ない．同類項があまり生成されない場合と比較すると，より効果を発揮していることがわかる．さらに，Table 5 の効率を見ると，大量の ASF が生成される変換ほど real time に対する LRL ソートの効果が増している．$p[1^{40}]$ の P2A 変換に至っては，real に約 50 倍もの差があり，より大きな問題になるほどその差は広がっていくと予想できる．また，メモリ使用量に対する効果も大きく，これについても同類項があまり生成されない場合に比べて効果が大きい．

これらの結果から，LRL ソートは特に実行時間への効果が高く，長い時間がかかる P2A 変換ほど LRL ソートの効果が大きくなり，その重要度は増していく傾向にある．さらに，同類項が大量に生成される P2A 変換では，実行時間とメモリ使用量のどちらの効果も大きく，統計量モーメントの導出に必要不可欠な対策であると言える．

Table 3: LRL ソートによる P2A 変換結果

PSP	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
$p[11\cdots1]$	1.38	1.15	0.23	0.17	21.1
$p[12\cdots1]$	15.07	12.58	2.49	0.17	50.5
$p[13\cdots1]$	208.84	153.24	55.60	0.27	71.7
$p[1^{30}]$	0.25	0.21	0.04	0.16	4.4
$p[1^{35}]$	1.04	0.90	0.14	0.13	14.8
$p[1^{40}]$	4.63	4.00	0.63	0.14	25.7

Table 4: RL ソートによる P2A 変換結果

PSP	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
$p[11\cdots1]$	8.07	6.53	1.54	0.19	50.5
$p[12\cdots1]$	109.38	84.45	24.93	0.23	71.7
$p[13\cdots1]$	2335.68	1440.23	895.45	0.38	97.3
$p[1^{30}]$	4.12	3.61	0.51	0.12	37.2
$p[1^{35}]$	32.20	27.48	4.72	0.15	50.5
$p[1^{40}]$	228.53	189.34	39.19	0.17	71.7

Table 5: LRL ソートの効率

PSP	real 効率	real-gbc 効率	gbc 効率	memory 効率
$p[11\cdots1]$	5.85	5.68	6.70	0.42
$p[12\cdots1]$	7.26	6.71	10.01	0.70
$p[13\cdots1]$	11.18	9.40	16.11	0.74
$p[1^{30}]$	16.48	17.19	12.75	0.12
$p[1^{35}]$	30.96	30.53	33.71	0.29
$p[1^{40}]$	49.36	47.34	62.21	0.36

3.2 Augmented Symmetric Function の重複度表現

重複度表現の効果を検証するため，p2a-2 と p2a-3 を用いて，前小節と同様に 2 パターンの PSP を P2A 変換し，通常表現との比較を行った．

重複度表現を用いて P2A 変換を行った結果を Table 6 に，通常表現を用いた結果を Table 7 に，およびそれらの比較による重複度表現の効率を Table 8 に示す．

同類項があまり生成されない場合について Tables 6, 7 を比較すると，メモリ使用量は同じだが，real については提案法のほうが長い．これは，同類項があまり生成されないためであり，重複度表現による効果が期待される対象ではないためである．Table 8 を見ると，大きな問題になるほど効率が悪くなることも予想でき，こういった問題には通常表現を使うべきである．

同類項が大量に生成される場合について Tables 6, 7 の比較では，重複度表現の効果を期待していたパターンの変換であるが，全体的にあまり効果を上げられておらず，$p[1^{45}]$, $p[1^{50}]$ の変換では重複度表現のほうが遅くなってしまっている．この原因を詳しく調べるため，Table 8 を Fig. 2 にグラフ化し，効率の変化を追ってみると，その原因が real-gbc 効率の悪化によることがわかる．また，重複度表現に処理が遅くなるのは，重複度表現中の係数の平均値が小さく，係数中に 1 の割合が多いときである．そこで，変換する PSP ごとに係数の平均値と係数中の 1 の割合を Table 9 に示し，重複度表現への適正を見直すと，長さが長くなってもそれぞれの値はほとんど変化しておらず，重複度表現への適正が上がっているとは言えない．一方で，生成される ASF の長さは長くなり，$a[9^1\ 8^1\ 6^1\ 5^1\ 3^3\ 2^4\ 1^4]$ のように，パーティション中の大きい数値が重複を起こしにくくなり，係数 1 が大きい数値に集中する．すると，ASF 同士の比較をする際に大きい数値から順に比較すると，係数 1 を比較する手間が無駄にかかってしまい，ソート中の ASF 同士の比較が通常表現に比べて遅くなる．その結果，real-gbc 効率の悪化につながったと考えられる．

以上の考察から，元の重複度表現の弱点である係数 1 を比較する手間を減らすため，ASF のパーティション中の数値を逆順にし，小さい数値から順に比較を行う方法が考えられる．この順序に従う関数を新しく作成し，同様にパターン B の変換を行った結果を Table 10 に，元の重複度表現である Table 6 と比較した効率を Table 11 に示す．結果はどれも好転しておらず，時間がかかる変換ほど real 効率が悪化している．これは，引数中の小さい数値とその係数の組み合わせが同じ ASF が多いため，ASF 同士の比較をする際に，大きい数値まで比較しなければならなくなったことが原因であると考えられる．

Table 6: 重複度表現による P2A 変換結果

PSP	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
$p[11\cdots1]$	1.78	1.53	0.25	0.14	21.1
$p[12\cdots1]$	19.43	16.68	2.75	0.14	50.5
$p[13\cdots1]$	288.90	217.66	71.24	0.25	71.7
$p[1^{30}]$	0.20	0.18	0.02	0.10	1.6
$p[1^{35}]$	0.93	0.79	0.14	0.15	8.1
$p[1^{40}]$	4.44	3.91	0.53	0.12	24.0
$p[1^{45}]$	21.79	18.93	2.86	0.13	36.5
$p[1^{50}]$	108.44	89.84	18.60	0.17	52.4
$p[1^{55}]$	530.14	405.15	124.99	0.24	78.2

Table 7: 通常表現による P2A 変換結果

PSP	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
$p[11\cdots1]$	1.38	1.15	0.23	0.17	21.1
$p[12\cdots1]$	15.07	12.58	2.49	0.17	50.5
$p[13\cdots1]$	208.84	153.24	55.60	0.27	71.7
$p[1^{30}]$	0.25	0.21	0.04	0.16	4.4
$p[1^{35}]$	1.04	0.90	0.14	0.13	14.8
$p[1^{40}]$	4.63	4.00	0.63	0.14	25.7
$p[1^{45}]$	21.61	18.24	3.37	0.16	48.5
$p[1^{50}]$	106.81	83.11	23.70	0.22	48.5
$p[1^{55}]$	550.17	372.46	177.71	0.32	99.7

Table 8: 重複度表現の効率

PSP	real 効率	real-gbc 効率	gbc 効率	memory 効率
$p[11\cdots1]$	0.78	0.75	0.92	1.00
$p[12\cdots1]$	0.78	0.75	0.91	1.00
$p[13\cdots1]$	0.72	0.70	0.78	1.00
$p[1^{30}]$	1.25	1.17	2.00	0.36
$p[1^{35}]$	1.12	1.14	1.00	0.55
$p[1^{40}]$	1.04	1.02	1.19	0.93
$p[1^{45}]$	0.99	0.96	1.18	0.75
$p[1^{50}]$	0.98	0.93	1.27	1.08
$p[1^{55}]$	1.04	0.92	1.42	0.78

Table 9: 重複度表現中における係数の平均値と 1 の割合

PSP	係数の平均値	係数中の 1 の割合
$p[1^{30}]$	2.370	0.554
$p[1^{35}]$	2.427	0.551
$p[1^{40}]$	2.481	0.548
$p[1^{45}]$	2.527	0.545
$p[1^{50}]$	2.569	0.543
$p[1^{55}]$	2.608	0.541

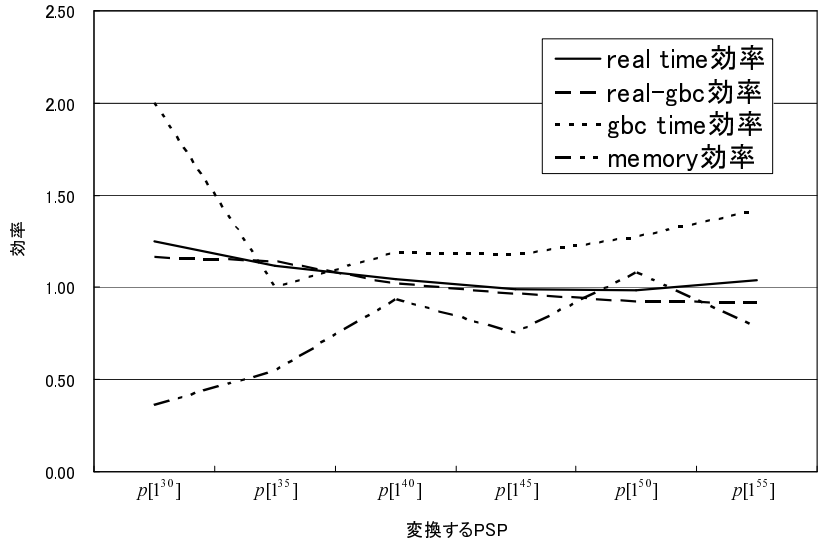

Fig. 2: 重複度表現の効率

Table 10: 逆順重複度表現による P2A 変換結果

PSP	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
$p[1^{30}]$	0.26	0.20	0.06	0.23	4.4
$p[1^{35}]$	1.30	1.10	0.20	0.15	10.7
$p[1^{40}]$	6.95	6.28	0.67	0.10	24.6
$p[1^{45}]$	36.57	32.64	3.93	0.11	45.6
$p[1^{50}]$	190.53	162.28	28.25	0.15	65.6
$p[1^{55}]$	1003.20	785.40	217.80	0.22	96.0

Table 11: 逆順重複度表現の効果

PSP	real 効率	real-gbc 効率	gbc 効率	memory 効率
$p[1^{30}]$	0.77	0.90	0.33	2.76
$p[1^{35}]$	0.72	0.72	0.70	1.32
$p[1^{40}]$	0.64	0.62	0.79	1.03
$p[1^{45}]$	0.60	0.58	0.73	1.25
$p[1^{50}]$	0.57	0.55	0.66	1.25
$p[1^{55}]$	0.53	0.52	0.57	1.23

3.3 不要な高次項の早期削除

ここでは，標本分散 V について，n^{-10} までの Edgeworth 展開をする場合を例とし，実際の統計量モーメントを求める場合で比較する．手順を以下に示す．

V について，標準化を行う．

$$X_n = \frac{\sqrt{n}(V - c_1)}{c_2} \tag{45}$$

なお，c_1，c_2 はそれぞれ，$c_1 = \sigma^2$，$c_2 = \sqrt{2}\sigma^2$ であるが，σ^2 は母集団パラメータであり，定数であるので c_1，c_2 のまま計算を進める．標準化を行ったことで Cornish-Fisher assumption を満たし，n^{-10} までの Edgeworth 展開に必要な X_n のモーメントが 22 次までであることがわかり，最も高次のものは，

$$X_n^{22} = \frac{n^{11}}{c_2^{22}}(V^{22} + 22c_1V^{21} + 231c_1^2V^{20} + \cdots + c_1^{22}) \tag{46}$$

である．(46) で，最も中間膨張が懸念される V^{22} は，(18) より，

$$V^{22} = \frac{1}{n^{22}}p[2^{22}] + \frac{22}{n^{23}}p[2^{21}\ 1^2] + \frac{231}{n^{24}}p[2^{20}\ 1^4] + \cdots + \frac{1}{n^{44}}p[1^{44}] \tag{47}$$

である．係数 $\frac{n^{11}}{c_2^{22}}$ をかけると，

$$\frac{n^{11}}{c_2^{22}}V^{22} = \frac{1}{c_2^{22}}\Big(\frac{1}{n^{11}}p[2^{22}] + \frac{22}{n^{12}}p[2^{21}\ 1^2] + \frac{231}{n^{13}}p[2^{20}\ 1^4] + \cdots + \frac{1}{n^{33}}p[1^{44}]\Big) \tag{48}$$

となる．(48) 中のそれぞれの PSP について，最終的に必要な次数が n^{-10} であることから，P2A 変換後に求めるべき ASF の長さを以下のように決めることができる．

- $p[2^{22}]$ ⋯ 長さ 1 以上
- $p[2^{21}\ 1^2]$ ⋯ 長さ 2 以上

  ⋮
- $p[1^{44}]$ ⋯ 長さ 23 以上

これにより，必要な長さ未満の ASF を不要な高次項として，P2A 変換中に途中削除することができる．(48) について，途中削除する場合としない場合を，それぞれ p2a-2 を用いて計算した．ここでは，Fig. 2 より，通常表現に対する重複度表現の効率が一定ではないため，通常表現である p2a-2 を実験に用いた．また，求める統計量モーメントの次数による効率の変化を比較するため，n^{-9} までの V^{20} と，$n^{-\frac{19}{2}}$ までの V^{21} を (48) と同様に求め，結果を Tables 12〜14 に示す．

Tables 12, 13 より，不必要な高次項を早期削除したほうが高速で，メモリ使用量も低く抑えられている．高速化に関しては，削除した以降の変換の手間が減った分高速化されているが，RL ソートに対する LRL ソートほどではない．なお，高次の変換ほど real time 効率は高くなっており，より高次の統計量モーメントの導出において効果が大きくなることが予想できる．メモリ使用量への効果に関しては,（この対策自体がメモリ使用量の減少に直結するため）メモリ使用量に対する効果は大きく，目安ではあるが V^{22} の導出では約半分のメモリ消費量に抑えられている．

この結果から，不要な高次項の早期削除は，メモリ使用量への効果という観点から，統計量モーメントの導出に必要な対策であると言える．

Table 12: 高次項を早期削除する場合の P2A 変換結果

V^r	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
V^{20}	42.48	31.14	11.34	0.27	41.2
V^{21}	85.62	59.68	25.94	0.30	64.0
V^{22}	179.70	115.27	64.43	0.36	63.2

Table 13: 高次項を早期削除しない場合の P2A 変換結果

V^r	real [s]	real-gbc [s]	gbc [s]	gbc/real	memory [MB]
V^{20}	91.91	60.31	31.60	0.34	58.3
V^{21}	205.37	120.50	84.87	0.41	89.3
V^{22}	450.50	238.57	211.93	0.47	116.6

Table 14: 高次項の早期削除の効率

V^r	real 効率	real-gbc 効率	gbc 効率	memory 効率
V^{20}	2.16	1.94	2.79	0.71
V^{21}	2.40	2.02	3.27	0.72
V^{22}	2.51	2.07	3.29	0.54

4 結語

Edgeworth 展開に用いる統計量モーメントを導出するため，その汎用的な方法である P2A 変換を取り上げた．P2A 変換には，変換途中に計算量・必要メモリの中間膨張を起こしてしまうという問題がある．そのため，中間膨張対策として 3 つの提案をし，検証実験を行った．

まず LRL ソートは，計算量・メモリ使用量の両方で大きな効果を挙げた．また，同類項が大量に生成される変換や，長い時間がかかる変換ほど効率を上げ，実行時間を大幅に短くすることができた．次に不要な高次項の早期削除は，計算量・メモリ使用量の両方で効果を挙げ，特にメモリ使用量を抑える効果が大きかった．最後に ASF の重複度表現は，同類項が大量に生成される PSP の変換での効果を期待していたが，検証実験ではあまり効果を挙げられなかった．これは，変換する PSP の長さが長くなっても重複度表現への適正がほとんど上がらず，逆にソート中に ASF 同士の比較が遅くなることに原因があった．

これらの結果から，LRL ソートと不要な高次項の早期削除の 2 つの対策は，中間膨張の抑制効果が確実にあり，P2A 変換をする際に行うべき対策であると結論付けられる．ASF の重複度表現は，本研究では十分な効果を挙げられなかったため，その効果をよりうまく引き出せるアルゴリズムを提案することが今後の課題となる．

参考文献

[1] Bruce E. Sagan (2001). *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions (Graduate Texts in Mathematics)*, Springer.

[2] Guy L. , Jr. Steele (著), 井田 昌之 (翻訳) (1992). *COMMON LISP*, 共立出版.

[3] Jan Vrbik (2005). Finite-n Corrections to Normal Approximation. *Communications in Statistics - Simulation and Computation*, Volume 34, 827-837.

[4] Naoto Niki and Sadanori Konishi (1984). Higher order asymptotic expansions for the distribution of the sample correlation coefficient. *Communications in statistics - Simulation and computation*, 13, 169-182.

[5] Paul Graham (著), 久野 雅樹 (翻訳), 須賀 哲夫 (翻訳) (2002). *ANSI Common Lisp*, ピアソン・エデュケーション.

[6] Stuart and Ord (1987). *Kendall's Advanced Theory of Statistics*, Volume 1 Distribution Theory, Charles Griffin.

[7] 中川重和・仁木直人 (1991). 対称式の変換アルゴリズムと その多変量統計分布論への応用. 計算機統計学, 4(1), 35-43.

[8] 仁木直人 (1986). 確率分布漸近展開の数式処理. 数学, 岩波書店, 38, 65-70.

[9] 仁木直人 (1986). 対称式の計算パッケージ. 数式処理通信, 4(2), 14-17.

[10] 仁木直人 (1987). 対称式の計算と統計への応用. 数式処理通信, 4(3), 6-10.

Examples of discriminants of quadratic orders with large fundamental units attached to a fixed length of the period of continued fractions

HASHIMOTO Ryūta *

1 Formulation of question

Let d be a positive non-square integer which is congruent to 1 modulo 4. Let (t, u), a pair of positive integers, be the fundamental solution of a diophantine equation $X^2 - dY^2 = -4$, that is, if a pair of positive integers (t', u') is also a solution, then it holds that $u \leq u'$. In other words, $(t + u\sqrt{d})/2$ is the fundamental unit of the quadratic order of discriminant d. In this paper, we consider the following question:

Question 1. For which d does it hold that $d < u$?

In case when d is prime and $d > u$, then the so-called Ankeny-Artin-Chowla conjecture (see [1], [3]) for d is true, namely, it holds that $d \nmid u$. Thus the cases $d < u$ seem interesting for us.

Solvability of $X^2 - dY^2 = -4$ is known to have a close relation to the regular continued fraction expansion of $(1 + \sqrt{d})/2$. In this paper we denote the regular continued fraction expansion of $(1 + \sqrt{d})/2$ by

$$\frac{1 + \sqrt{d}}{2} =: [\ c_0,\ c_1,\ c_2,\ c_3,\ \dots\ ].$$

*Takuma National College of Technology

Let l be the minimal positive integer such that $c_{k+l} = c_k$ for all $k \geq 1$. It is well known that such l exists. And we denote

$$\frac{1+\sqrt{d}}{2} =: [\ c_0,\ \overline{c_1,\ \ldots,\ c_l}\ ].$$

Moreover, it holds that $c_{l-k} = c_k$ for $1 \leq k < l$ and $c_l = 2c_0 - 1$. The following proposition is well-known:

Proposition 1. *A diophantine equation $X^2 - dY^2 = -4$ is solvable if and only if l is odd.*

From the viewpoint of continued fraction expansions, cases $d < u$ seldom seem to happen. Here are two examples.

Example 1. Consider d's which satisfy

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{1,\ 4,\ 2,\ 2,\ 4,\ 1,\ *}\ ].$$

Such d's are 113, 24553, 91585, etc. For these d's, it holds that $u = 146$. Thus it holds $d > u$ except the case when $d = 113$.

Example 2. Consider d's which satisfy

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{1,\ 3,\ 2,\ 2,\ 3,\ 1,\ *}\ ].$$

Such d's are 32597, 140285, 323245, etc. For these d's, it holds that $u = 97$. Thus it holds $d > u$ for all such d's.

In fact, we have the following:

Proposition 2 (e.g. [2])**.** *Let l be odd and l' be $(l-1)/2$. Let $c_1, \ldots, c_{l'}$ be given l' positive integers. Then the number of positive integers d, which satisfy (i) d is congruent to 1 modulo 4; (ii) $(1+\sqrt{d})/2$ is of form*

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ \ldots,\ c_{l'},\ c_{l'},\ \ldots,\ c_1,\ *}\ ];$$

and (iii) $d < u$, is at most one.

Moreover, such d does not exist when $l \leq 5$.

Thus we reformulate Question 1 into the following:

Question 2. Determine odd l and positive integers $c_1, \ldots, c_{l'}$, where $l' = (l-1)/2$, such that there exists an integer d satisfying (i) $d \equiv 1 \pmod 4$; (ii) $(1+\sqrt{d})/2$ is of form

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ \ldots,\ c_{l'},\ c_{l'},\ \ldots,\ c_1,\ *}\ ];$$

(iii) $d < u$.

But this qustion is too difficult to solve completely. Proposition 2 implies that $l \geq 7$. So we concentrate on the easiest case, that is, when $l = 7$.

Question 3. Determine positive integers c_1, c_2, c_3 such that there exists an integer d satisfying (i) $d \equiv 1 \pmod 4$; (ii) $(1+\sqrt{d})/2$ is of form

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ c_2,\ c_3,\ c_3,\ c_2,\ c_1,\ *}\ ];$$

(iii) $d < u$.

Yet this question is too difficult. So we let computers help us.

2 Families of d's satisfying $u > d$

Computer calculations easily find that up to 10^9, there are 474 d's satisfying (i) $d \equiv 1 \pmod 4$; (ii) The regular continued fraction expansion of $(1+\sqrt{d})/2$ is of form

$$\frac{1+\sqrt{d}}{2} = [\ *, \overline{c_1,\ c_2,\ c_3,\ c_3,\ c_2,\ c_1,\ *}\ ];$$

(iii) $d < u$.

For these d's, we have the followings:

- In 267 cases it holds that $c_1 = ({c_3}^2+1)c_2 + 2c_3$;
- In 116 cases it holds that $c_3 = (c_1c_2+1)(c_1-c_2) + c_1$;
- In 55 cases it holds that $(c_2, c_3) = (c_1c^2, c_1c)$ for some c;
- 36 cases are exceptional.

The first three cases above appear to be parts of answers to Question 3. Indeed, we can prove the following three theorems straightforwardly.

Theorem 1. *Let c_2 and c_3 be positive integers. Assume that $(c_2, c_3) \not\equiv (0,0) \pmod 2$. Let $c_1 = ({c_3}^2 + 1)c_2 + 2c_3$. Let d be the smallest positive integer such that $(1+\sqrt{d})/2$ is of form*

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ c_2,\ c_3,\ c_3,\ c_2,\ c_1,\ *}\ ].$$

Then we have

$$d = \{c_3({c_3}^2+1){c_2}^2 + (3{c_3}^2+1)c_2 + 3c_3\}^2 + 4(c_3c_2+1)$$

and

$$u = d + ((c_3c_2+1)^2 + {c_2}^2)^2 - 4(c_3c_2+1),$$

which implies that $d < u$. Moreover, we have $1 < u/d < 2$.

Theorem 2. *Let c_1 and c_2 be positive integers. Assume that $c_1 > c_2$ and $(c_1, c_2) \not\equiv (0,0) \pmod 2$. Let $c_3 = (c_2c_1+1)(c_1-c_2) + c_1$. Let d be the smallest positive integer such that $(1+\sqrt{d})/2$ is of form*

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ c_2,\ c_3,\ c_3,\ c_2,\ c_1,\ *}\ ].$$

Then we have

$$d = ((c_2c_1+1)(c_1-c_2)(c_2(c_1-c_2)+2)+c_1)^2 + 4(c_2(c_1-c_2)+1)^2$$

and

$$u = d + ((c_2c_1+1)^2(c_2(2c_1-c_2)+2)-5)(c_2(c_1-c_2)+1)^2 + {c_2}^4,$$

which implies that $d < u$.

Theorem 3. *Let c_1 and c be positive integers. Let d be the smallest positive integer such that $d \equiv 1 \pmod 4$ and $(1+\sqrt{d})/2$ is of form*

$$\frac{1+\sqrt{d}}{2} = [\ *,\ \overline{c_1,\ c_1c^2,\ c_1c,\ c_1c,\ c_1c^2,\ c_1,\ *}\ ].$$

Then it holds that $d < u$ if and only if one of the following two conditions holds:

- c_1 *is odd and* $c \equiv 1 \pmod{c_1}$*;*
- c_1 *is even and* $c \equiv c_1 + 1 \pmod{2c_1}$.

Moreover, one of the two conditions above implies that

$$d = \left(c_1 c^3 + \frac{c-1}{c_1}\right)^2 + 4c^3,$$
$$u = {c_1}^4 d + ({c_1}^2 c^2 + 1)^2 + 4{c_1}^2 c$$

and ${c_1}^4 < u/d < {c_1}^4 + 1$.

References

[1] Ankeny, N. C., Artin, E., and Chowla, S. "The Class-Number of Real Quadratic Fields," Annals of Math, vol. 56, no. 3 (1952), pp. 479–493.

[2] Hashimoto, Ryūta. "Ankeny-Artin-Chowla Conjecture and Continued Fraction Expansion," J. Number Th., vol. 90 (2001), pp. 143–153.

[3] van der Poorten, A. J., te Riele, J. J., and Williams, H. C. "Computer Verification of the Ankeny-Artin-Chowla Conjecture for All Primes Less Than 100 000 000 000," Math. Comp. vol. 70 (2001), pp. 1311–1328; Corrigenda and Addition, Math. Comp. vol. 72 (2003), pp. 521–523.

生成的多項式の同型問題への考察

星　明考　　三宅　克哉

概 要

任意の体 k に対し，k 上生成的多項式の同型問題に対処する一般的手法を，チルンハウス変換の定義体を考察する事によって与える．前半における一般的考察の結果を基にして，3 次の場合の計算結果を紹介し，3 次対称群，3 次巡回群それぞれに対する k 上生成的多項式の同型問題への解を具体的に与える．また，応用として幾つかの 6 次生成的多項式が具体的に得られる．[1] [2]

§ 1　はじめに

有限群 G を定め，任意の標数の体 k を基礎体として固定する．さらに k 上の m 個の独立変数 $\mathbf{t} = (t_1, \ldots, t_m)$ を取り，$k(\mathbf{t})$ を k 上の m 変数有理関数体とする．多項式 $F(\mathbf{t}; X) \in k(\mathbf{t})[X]$ は，$k(\mathbf{t})$ 上のガロア群が G と同型，かつ各無限体 $M \supset k$ とその G-拡大 L/M に対し，L が $F(\mathbf{a}; X)$ の M 上の最小分解体となるような $\mathbf{a} = (a_1, \ldots, a_m) \in M^m$ が存在するとき，G に対する k-生成的多項式という．

体 $M \supset k$ 上の任意の G-拡大は k-生成的多項式の変数の特殊化によって得られる．よって，G-拡大体全体の構造を明らかにするためには，次の問題を考える必要がある：

生成的多項式の同型問題. 無限体 $M \supset k$ と $\mathbf{a}, \mathbf{b} \in M^m$ に対して, $\mathrm{Spl}_M F(\mathbf{a}; X)$ と $\mathrm{Spl}_M F(\mathbf{b}; X)$ が M 上同型となるための必要十分条件を与えよ.

また，任意の部分群 $H \subset G$ に対し，M 上の全ての H-ガロア拡大は同様に生成的多項式 $F(\mathbf{t}; X)$ の変数の特殊化 $\mathbf{t} \mapsto \mathbf{a}$ によって得られる ([Kem01])．これより，自然に次の同型問題の一般化が考えられる：

生成的多項式の部分体問題. $F(\mathbf{t}; X)$ を G に対する k-生成的多項式とする．無限体 $M \supset k$ と $\mathbf{a}, \mathbf{b} \in M^m$ に対して, $\mathrm{Spl}_M F(\mathbf{b}; X)$ が $\mathrm{Spl}_M F(\mathbf{a}; X)$ の部分体となるための必要十分条件を与えよ.

§ 2, § 3 では，n 次対称群 $\mathfrak{S}_n$ に対する k-生成的多項式の同型問題への解法を，チルンハウス変換の定義体を通じて考察する．また § 4, § 5 では，$\mathfrak{S}_3, C_3$ に対する k-生成的多項式の部分体問題への解を与える．§ 6 では，3 次の場合の応用として，いくつかの 6 次生成的多項式を構成する．

体 K とその代数閉体を固定し，K 上の分離的でモニックな n 次多項式 $f(X), g(X) \in K[X]$ に対して $\alpha_1, \ldots, \alpha_n$ を $f(X)$ のそこでの根とする．次の形の多項式 $g(X)$ を $f(X)$ の体 K 上のチルンハウス変換という：

$$g(X) = \prod_{i=1}^{n} \big(X - (c_0 + c_1\alpha_i + \cdots + c_{n-1}\alpha_i^{n-1})\big), \quad c_i \in K.$$

多項式 $f(X), g(X) \in K[X]$ が互いに K 上のチルンハウス変換で移り合うとき，多項式 $f(X)$ と $g(X)$ を K 上チルンハウス同値という．既約分離的多項式 $f(X), g(X) \in K[X]$ に対して，次は同値である：
(i) $f(X)$ と $g(X)$ は K 上チルンハウス同値である；
(ii) 商体 $K[X]/(f(X))$ と $K[X]/(g(X))$ は K 上同型である.

§ 2　チルンハウス変換 (幾何学的な解釈)

まず $n \geq 3$ を正整数とし，$\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ を k 上の $2n$ 個の独立変数とする．さらに $f_n(\mathbf{s}; X) = f_n(s_1, \ldots, s_n; X) \in k(\mathbf{s})[X]$, $f_n(\mathbf{t}; X) = f_n(t_1, \ldots, t_n; X) \in k(\mathbf{t})[X]$ をモニックな n 次多

[1] 本研究の一部は，日本学術振興会科学研究費補助金 基盤研究 (C) 19540057，早稲田大学特定課題研究助成費 2007B-067 の助成を受けている.
[2] 本稿のより詳細な内容は，[HM-j] 又はプレプリント “A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation” [HM] として Web から入手可能である.

項式とし，それらの根をそれぞれ $\{x_1,\dots,x_n\},\{y_1,\dots,y_n\}$ とすれば

$$f_n(\mathbf{s};X) \;=\; \prod_{i=1}^{n}(X-x_i) \;=\; X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n,$$
$$f_n(\mathbf{t};X) \;=\; \prod_{i=1}^{n}(X-y_i) \;=\; X^n - t_1X^{n-1} + t_2X^{n-2} + \cdots + (-1)^n t_n$$

が得られる．但し，$s_i,\, t_i$ はそれぞれ $x_1,\dots,x_n$ 及び $y_1,\dots,y_n$ に対する i 次基本対称式である．体 K を

$$K \;:=\; k(\mathbf{s},\mathbf{t})$$

によって定めれば，K は自然に k 上の $2n$ 変数有理関数体と見なせる．また，

$$L_{\mathbf{s}} \;:=\; \mathrm{Spl}_K f_n(\mathbf{s};X) \;=\; K(x_1,\dots,x_n), \qquad L_{\mathbf{t}} \;:=\; \mathrm{Spl}_K f_n(\mathbf{t};X) \;=\; K(y_1,\dots,y_n)$$

とおけば，$L_{\mathbf{s}} \cap L_{\mathbf{t}} = K$ かつ $L_{\mathbf{s}}L_{\mathbf{t}} = k(\mathbf{x},\mathbf{y})$ である．したがって，体の拡大 $k(\mathbf{x},\mathbf{y})/K$ はガロア拡大であり，そのガロア群は n 次対称群 $\mathfrak{S}_n$ の 2 つの直積 $\mathfrak{S}_n \times \mathfrak{S}_n$ と同型になる．ここで

$$G_{\mathbf{s}} \;:=\; \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/L_{\mathbf{t}}),\;\; G_{\mathbf{t}} \;:=\; \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/L_{\mathbf{s}}),\;\; G_{\mathbf{s},\mathbf{t}} \;:=\; G_{\mathbf{s}} \times G_{\mathbf{t}}$$

と置く．群 $G_{\mathbf{s},\mathbf{t}} \cong \mathrm{Gal}(L_{\mathbf{s}}L_{\mathbf{t}}/K)$ は $k(\mathbf{x},\mathbf{y})$ に右から作用するとする．そこで，$g=(\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ に対して，逆同型

$$\varphi : G_{\mathbf{s}} \to \mathfrak{S}_n,\;\; \sigma \mapsto \varphi(\sigma), \qquad \psi : G_{\mathbf{t}} \to \mathfrak{S}_n,\;\; \tau \mapsto \psi(\tau),$$

を固定し，群 $G_{\mathbf{s},\mathbf{t}}$ と $\mathfrak{S}_n \times \mathfrak{S}_n$ を以下の作用で同一視する：

$$x_i^{\sigma} = x_{\varphi(\sigma)(i)},\;\; y_i^{\sigma} = y_i,\;\; x_i^{\tau} = x_i,\;\; y_i^{\tau} = y_{\psi(\tau)(i)},\;\; (i=1,\dots,n). \tag{1}$$

さて $f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換は，K の代数閉体の中では $n!$ 個存在する．我々はまず，$f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換の定義体 (K の拡大体) を考察する．行列 D を

$$D := \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

と定義する (Vandermonde 行列)．行列 D の行列式は

$$\det D \;=\; \Delta_{\mathbf{s}},\;\; \text{但し}\;\; \Delta_{\mathbf{s}} := \prod_{1\le i<j\le n}(x_j - x_i)$$

によって与えられ，D は可逆である．体 $k(\mathbf{s})(\Delta_{\mathbf{s}})$ は $\mathrm{char}\, k \neq 2$，すなわち体 k の標数が 2 でないならば，$k(\mathbf{s})$ の 2 次拡大を与えていることに注意しよう．体 $k(\mathbf{x},\mathbf{y})$ の中で n 個の元の組 $(u_0(\mathbf{x},\mathbf{y}),\dots,u_{n-1}(\mathbf{x},\mathbf{y})) \in k[\mathbf{x},\mathbf{y},\Delta_{\mathbf{s}}^{-1}]^n$ を以下のように定義する：

$$\begin{pmatrix} u_0(\mathbf{x},\mathbf{y}) \\ u_1(\mathbf{x},\mathbf{y}) \\ \vdots \\ u_{n-1}(\mathbf{x},\mathbf{y}) \end{pmatrix} := D^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}. \tag{2}$$

クラメールの公式から

$$u_i(\mathbf{x},\mathbf{y}) = \Delta_{\mathbf{s}}^{-1} \cdot \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{i-1} & y_1 & x_1^{i+1} & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{i-1} & y_2 & x_2^{i+1} & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{i-1} & y_n & x_n^{i+1} & \cdots & x_n^{n-1} \end{pmatrix} \tag{3}$$

を得る．また，表記を簡略にするために

$$u_i := u_i(\mathbf{x}, \mathbf{y}), \quad (i = 0, \ldots, n-1)$$

と書くことにする．ガロア群 $G_{\mathbf{s},\mathbf{t}}$ は軌道 $\{u_i^{(\sigma,\tau)} \mid (\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}\}$ に右から作用するが，この作用は忠実ではない．ここで，部分群 $H \subset G_{\mathbf{s},\mathbf{t}}$ を

$$H := \{(\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}} \mid \varphi(\sigma) = \psi(\tau)\} \cong \mathfrak{S}_n$$

によって定め，$\overline{g} = Hg$ を H の $G_{\mathbf{s},\mathbf{t}}$ における右剰余類とする．このとき $(\sigma,\tau) \in H$ に対して $u_i^{(\sigma,\tau)} = u_i, (i = 0, \ldots, n-1)$ であることが下の補題から分かる．これより，群 $G_{\mathbf{s},\mathbf{t}}$ は集合 $\{u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ に右剰余類からなる集合 $H\backslash G_{\mathbf{s},\mathbf{t}}$ への作用を通して作用する．また，集合 $\{\overline{(1,\tau)} \mid (1,\tau) \in G_{\mathbf{s},\mathbf{t}}\}$ 及び $\{\overline{(\sigma,1)} \mid (\sigma,1) \in G_{\mathbf{s},\mathbf{t}}\}$ は $H\backslash G_{\mathbf{s},\mathbf{t}}$ の完全代表系である．実際，たとえば $g = (\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ に対して $\varphi(\sigma) = \psi(\tau')$ とすれば $\overline{g} = H(\sigma,\tau')^{-1}g = H(1,(\tau')^{-1}\tau)$ が成り立つ．

補題 2.1. 整数 i, $(0 \le i \le n-1)$, を固定する．もし $(\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ に対し $u_i^{(\sigma,\tau)} = u_i$ であるならば，$\varphi(\sigma) = \psi(\tau)$ であり，またその逆も成り立つ．すなわち，$H = \mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i)$ である．

証明. [HM] 参照. □

この補題から，特に $\#H\backslash G_{\mathbf{s},\mathbf{t}} = n!$ であり，$G_{\mathbf{s},\mathbf{t}}$ の部分群 $G_{\mathbf{s}}$ 及び $G_{\mathbf{t}}$ は集合 $\{u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ に忠実に作用する．特に $\overline{g} = \overline{(1,\tau)}$ に対して，定義 (2) より次の等式が得られる：

$$y_{\psi(\tau)(i)} = u_0^g + u_1^g x_i + \cdots + u_{n-1}^g x_i^{n-1}, \quad (i = 1, \ldots, n).$$

これは各 $\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，集合 $\{(u_0^g, \ldots, u_{n-1}^g) \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}\}$ が $f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換の係数を与えることを意味している．

定義. 各 $\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，体 $K(u_0^g, \ldots, u_{n-1}^g)$ を $f_n(\mathbf{s};X)$ から $f_n(\mathbf{t};X)$ へのチルンハウス変換の係数の体と呼ぶ．

また $u_i(\mathbf{x},\mathbf{y})$ の $\mathbf{x}$ と $\mathbf{y}$ を入れ換えて

$$v_i(\mathbf{x},\mathbf{y}) := u_i(\mathbf{y},\mathbf{x}), \quad (i = 0, \ldots, n-1)$$

と置き，簡単の為に $v_i = v_i(\mathbf{x},\mathbf{y})$ と書くことにする．体 $K(v_0^g, \ldots, v_{n-1}^g)$ は $f_n(\mathbf{t};X)$ から $f_n(\mathbf{s};X)$ へのチルンハウス変換の係数の体を与える．

命題 2.2. 各整数 $i, (0 \le i \le n-1)$, 及び $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$(L_{\mathbf{s}}L_{\mathbf{t}})^{g^{-1}Hg} = K(u_0^g, \ldots, u_{n-1}^g) = K(v_0^g, \ldots, v_{n-1}^g) = K(u_i^g) = K(v_i^g)$ であり，かつ $[K(u_i^g) : K] = n!$ が成り立つ．

証明. $\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i^g) = \mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(v_i^g) = g^{-1}Hg$ から直接従う ([HM] 参照). □

系 2.3. 各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$\mathrm{Spl}_{K(u_i^g)} f_n(\mathbf{s};X) = \mathrm{Spl}_{K(u_i^g)} f_n(\mathbf{t};X)$ である．

証明. 多項式 $f_n(\mathbf{s};X)$ と $f_n(\mathbf{t};X)$ は体 $K(u_0^g, \ldots, u_{n-1}^g) = K(u_i^g) = K(v_i^g)$ の上でチルンハウス同値である．よって，商体 $K(u_i^g)[X]/(f_n(\mathbf{s};X))$ と $K(u_i^g)[X]/(f_n(\mathbf{t};X))$ は $K(u_i^g)$ 上同型である． □

命題 2.4. 次が成り立つ．

(i) $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$L_{\mathbf{s}} \cap K(u_i^g) = L_t \cap K(u_i^g) = K$ であり，

(ii) $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$L_{\mathbf{s}}L_{\mathbf{t}} = L_{\mathbf{s}}(u_i^g) = L_{\mathbf{t}}(u_i^g)$ である．

証明. (i) は $(g^{-1}Hg)G_{\mathbf{t}} = (g^{-1}Hg)G_{\mathbf{s}} = G_{\mathbf{s},\mathbf{t}}$ を, (ii) は $g^{-1}Hg \cap G_{\mathbf{s}} = g^{-1}Hg \cap G_{\mathbf{t}} = \{1\}$ を示せばよい ([HM] 参照). □

さらに，次の命題が得られる．

命題 2.5. 各整数 $i, (0 \le i \le n-1)$, に対して，$L_{\mathbf{s}}L_{\mathbf{t}} = K(u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}})$ が成り立つ．

証明. $\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u_i^g) = g^{-1}Hg$ であるから，$\bigcap_{\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}} g^{-1}Hg = \{1\}$ を示せばよい ([HM] 参照)． □

ここで，次数 $n!$ の多項式を以下のように定義する：

$$F_i(\mathbf{s},\mathbf{t};X) := \prod_{\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}} (X - u_i^g) \in K[X], \quad (i = 0,\ldots,n-1).$$

命題 2.2 より $F_i(\mathbf{s},\mathbf{t};X), (i = 0,\ldots,n-1)$, は $k(\mathbf{s},\mathbf{t})$ 上既約である．さらに，命題 2.5 から次の定理が得られる．

定理 2.6. 多項式 $F_i(\mathbf{s},\mathbf{t};X) \in k(\mathbf{s},\mathbf{t})[X]$ は $\mathfrak{S}_n \times \mathfrak{S}_n$ に対して k-生成的である．

証明. 定理の主張は，$\mathrm{Spl}_K F_i(\mathbf{s},\mathbf{t};X) = K(u_i^g \mid \overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}) = L_{\mathbf{s}}L_{\mathbf{t}}$ であること，および，$f_n(\mathbf{s};X)$ と $f_n(\mathbf{t};X)$ がそれぞれ $\mathfrak{S}_n$ に対する k-生成的多項式であることから従う． □

体 k の標数が 2 である場合には，$\Delta_{\mathbf{s}} \in k(\mathbf{s})$ となり，$k(\mathbf{s})(\Delta_{\mathbf{s}}) = k(\mathbf{s})$ である．よって，$k(\mathbf{s})(\Delta_{\mathbf{s}})$ は $k(\mathbf{s})$ の 2 次拡大体にはならない．そこで標数が 2 の場合には，Berlekamp [Ber76] に従って Berlekamp の判別式と呼ばれる

$$\beta_{\mathbf{s}} := \sum_{i<j} \frac{x_i}{x_i + x_j}$$

を通常の差積 $\Delta_{\mathbf{s}}$ の代わりに用いる．このとき，$k(\mathbf{s})(\beta_{\mathbf{s}})$ は $k(\mathbf{s})$ の 2 次拡大体となる．

次数 n の交代群 $\mathfrak{A}_n$ に対して，

$$\begin{aligned}(H\backslash G_{\mathbf{s},\mathbf{t}})^+ &:= \{\overline{g} = \overline{(1,\tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}} \mid \psi(\tau) \in \mathfrak{A}_n\},\\ (H\backslash G_{\mathbf{s},\mathbf{t}})^- &:= \{\overline{g} = \overline{(1,\tau)} \in H\backslash G_{\mathbf{s},\mathbf{t}} \mid \psi(\tau) \notin \mathfrak{A}_n\}\end{aligned}$$

とおき，多項式 $F_i^+(X), F_i^-(X)$ を以下の様に定義する．

$$F_i^{\pm}(X) := \prod_{\overline{g}\in (H\backslash G_{\mathbf{s},\mathbf{t}})^{\pm}} (X - u_i^g), \quad (i = 0,\ldots,n-1). \tag{4}$$

命題 2.7. 多項式 $F_i(\mathbf{s},\mathbf{t};X)$ は K の 2 次拡大体 $K(\Delta_{\mathbf{s}}/\Delta_{\mathbf{t}})$ 上で (char $k = 2$ の場合は，$K(\beta_{\mathbf{s}} + \beta_{\mathbf{t}})$ 上で)，2 つの $n!/2$ 次既約多項式 $F_i^+(X)$, $F_i^-(X)$ の積となる．

証明. [HM] 参照. □

§ 3 無限体への変数の特殊化

さて M $(\supset k)$ を無限体とする．ここで考察する多項式 $f_n(\mathbf{s};X)$, $f_n(\mathbf{t};X)$ の変数の特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^n \times M^n$ については，$f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ は M 上分離的であると仮定することにする (すなわち $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$)．多項式 $f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ の固定された M の代数閉包の中での最小分解体を $L_{\mathbf{a}} = \mathrm{Spl}_M f_n(\mathbf{a};X)$, $L_{\mathbf{b}} = \mathrm{Spl}_M f_n(\mathbf{b};X)$ とおく．また $f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ の M 上のガロア群をそれぞれ $G_{\mathbf{a}}$, $G_{\mathbf{b}}$ とする，(すなわち，$G_{\mathbf{a}} = \mathrm{Gal}(L_{\mathbf{a}}/M)$, $G_{\mathbf{b}} = \mathrm{Gal}(L_{\mathbf{b}}/M)$)．さらに，$G_{\mathbf{a},\mathbf{b}} := \mathrm{Gal}(L_{\mathbf{a}}L_{\mathbf{b}}/M)$ とおく．固定しておいた M の代数閉包の中で，$f_n(\mathbf{a};X)$, $f_n(\mathbf{b};X)$ それぞれの根 $\boldsymbol{\alpha} := (\alpha_1,\ldots,\alpha_n)$, $\boldsymbol{\beta} := (\beta_1,\ldots,\beta_n)$ をとる．根の順序を固定することによって，ガロア群 $G_{\mathbf{a},\mathbf{b}}$ の各要素は，2 つの添え字集合の置換を引き起こす．よって，$G_{\mathbf{a},\mathbf{b}}$ は $G_{\mathbf{s},\mathbf{t}}$ の部分群と見なすことができる．より正確に言えば，要素 $h \in G_{\mathbf{a},\mathbf{b}}$ が $\alpha_i^h = \alpha_{\varphi(\sigma)(i)}$, $\beta_i^h = \beta_{\psi(\tau)(i)}, (i = 1,\ldots,n)$, を満たすとき，$h = (\sigma,\tau) \in G_{\mathbf{s},\mathbf{t}}$ と書くことにする．ここで $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ が基本的にきいている．

各 $g=(\sigma,\tau)\in G_{\mathbf{s},\mathbf{t}}$ に対して，次のようにおく：

$$\begin{aligned}(c_0^g,\dots,c_{n-1}^g) &:= (u_0^g(\boldsymbol{\alpha},\boldsymbol{\beta}),\dots,u_{n-1}^g(\boldsymbol{\alpha},\boldsymbol{\beta})),\\ (d_0^g,\dots,d_{n-1}^g) &:= (u_0^g(\boldsymbol{\beta},\boldsymbol{\alpha}),\dots,u_{n-1}^g(\boldsymbol{\beta},\boldsymbol{\alpha})).\end{aligned} \tag{5}$$

定義から，$i=1,\dots,n$ に対して

$$\beta_{\psi(\tau)(i)} \;=\; c_0^g + c_1^g\alpha_{\varphi(\sigma)(i)} + \cdots + c_{n-1}^g\alpha_{\varphi(\sigma)(i)}^{n-1}, \tag{6}$$

$$\alpha_{\varphi(\sigma)(i)} \;=\; d_0^g + d_1^g\beta_{\psi(\tau)(i)} + \cdots + d_{n-1}^g\beta_{\psi(\tau)(i)}^{n-1} \tag{7}$$

が成り立つ．したがって，各 $\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，$f_n(\mathbf{a};X)$ から $f_n(\mathbf{b};X)$ への $M(c_0^g,\dots,c_{n-1}^g)$ 上のチルンハウス変換が存在する．また $(c_0^g,\dots,c_{n-1}^g)$ に対して，$(d_0^g,\dots,d_{n-1}^g)$ はその逆変換のチルンハウス変換の係数を与える．

仮定 $\Delta_{\mathbf{a}}\cdot\Delta_{\mathbf{b}}\neq 0$ より，次の補題が得られる．

補題 3.1. 体の拡大 M'/M に対して，もし $f_n(\mathbf{b};X)$ が M' 上において $f_n(\mathbf{a};X)$ のチルンハウス変換であるならば， $f_n(\mathbf{a};X)$ は $f_n(\mathbf{b};X)$ の M' 上でのチルンハウス変換である．特に，各 $g\in G_{\mathbf{s},\mathbf{t}}$ に対して $M(c_0^g,\dots,c_{n-1}^g)=M(d_0^g,\dots,d_{n-1}^g)$ が成り立つ．

証明. [HM] 参照. □

本稿の主題の一つは，$f_n(\mathbf{a};X)$ から $f_n(\mathbf{b};X)$ へのチルンハウス変換の係数の体 $M(c_0^g,\dots,c_{n-1}^g)$ の振る舞いを考察することである．

命題 3.2. 仮定 $\Delta_{\mathbf{a}}\cdot\Delta_{\mathbf{b}}\neq 0$ の下で，次が成立する：

(i) $g\in G_{\mathbf{s},\mathbf{t}}$ に対し，$\mathrm{Spl}_{M(c_0^g,\dots,c_{n-1}^g)}f_n(\mathbf{a};X)=\mathrm{Spl}_{M(c_0^g,\dots,c_{n-1}^g)}f_n(\mathbf{b};X)$;

(ii) $g\in G_{\mathbf{s},\mathbf{t}}$ に対し，$L_{\mathbf{a}}L_{\mathbf{b}}=L_{\mathbf{a}}\,M(c_0^g,\dots,c_{n-1}^g)=L_{\mathbf{b}}\,M(c_0^g,\dots,c_{n-1}^g)$.

証明. 補題 3.1 より，$M'=M(c_0^g,\dots,c_{n-1}^g)$ に対して $M'[X]/(f_n(\mathbf{a};X))$ と $M'[X]/(f_n(\mathbf{b};X))$ は M' 上同型である．よって (i) が従う．また (i) より，$L_{\mathbf{a}}\,M(c_0^g,\dots,c_{n-1}^g)=L_{\mathbf{b}}M(c_0^g,\dots,c_{n-1}^g)$ であり，(ii) が従う. □

命題 2.2 と命題 2.5 から，$j,(0\le j\le n-1)$, を固定したとき，次が成り立つ：

$$K(u_0^g,\dots,u_{n-1}^g) \;=\; K(u_j^g),\quad (g\in G_{\mathbf{s},\mathbf{t}}), \tag{8}$$

$$L_{\mathbf{s}}L_{\mathbf{t}} \;=\; K(u_j^g \mid \overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}) \tag{9}$$

かつ $[K(u_j^g):K]=n!$. しかしながら，式 (5) における特殊化の後，一般に成り立つのは包含関係

$$\begin{aligned}M(c_0^g,\dots,c_{n-1}^g) &\supset M(c_j^g),\quad (g\in G_{\mathbf{s},\mathbf{t}}),\\ L_{\mathbf{a}}L_{\mathbf{b}} &\supset M(c_j^g \mid \overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}})\end{aligned}$$

のみであり，$M(c_0^g,\dots,c_{n-1}^g)=M(c_j^g)$ が成り立つかどうかは，特殊化 $(\mathbf{s},\mathbf{t})\mapsto(\mathbf{a},\mathbf{b})\in M^n\times M^n$ に依存して決まる．式 (8) から， 次のような多項式 $P_{i,j}(\mathbf{s},\mathbf{t};X)\in K[X]$ が存在する事が分かる：

$$u_i=P_{i,j}(\mathbf{s},\mathbf{t};u_j)\quad\text{かつ}\quad \deg_X(P_{i,j}(\mathbf{s},\mathbf{t};X))<n!.$$

よって $P_{i,j}(\mathbf{s},\mathbf{t};X)$ の X に関する各係数の分母を (重複を除いて) 取り出せば,

$$u_i=\frac{1}{D_{i,j}^0(\mathbf{s},\mathbf{t})}\,P_{i,j}^0(\mathbf{s},\mathbf{t};u_j)\quad\text{かつ}\quad \deg_X(P_{i,j}^0(\mathbf{s},\mathbf{t};X))<n! \tag{10}$$

を満たすような多項式 $P_{i,j}^0(\mathbf{s},\mathbf{t};X)\in k[\mathbf{s},\mathbf{t}][X]$ と $D_{i,j}^0(\mathbf{s},\mathbf{t})\in k[\mathbf{s},\mathbf{t}]$ が得られる．

補題 3.3. ある $j, (0 \le j \le n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n$ に対し，もし各 $i = 0, \ldots, n-1$, に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ であるならば，各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して $M(c^g_0, \ldots, c^g_{n-1}) = M(c^g_j)$ が成り立つ.

式 (5) による特殊化後に対しても，次数 $n!$ の多項式

$$F_i(\mathbf{a}, \mathbf{b}; X) = \prod_{\overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}} (X - c^g_i) \in M[X], \quad (i = 0, \ldots, n-1)$$

を用いる．ただし $F_i(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとは限らない.

補題 3.4. ある $j, (0 \le j \le n-1)$, に対し，$F_j(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとする．このとき，$i = 0, \ldots, n-1$, に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ である.

証明. 実際，ある i に対して $D^0_{i,j}(\mathbf{a}, \mathbf{b}) = 0$ であると仮定すれば $P^0_{i,j}(\mathbf{a}, \mathbf{b}; c_j) = 0$ でなくてはならない．ところが $P^0_{i,j}(\mathbf{a}, \mathbf{b}; X) \in k[\mathbf{a}, \mathbf{b}][X]$ の次数は $n!$ 未満であり，これはやはり c_j を根に持つ次数 $n!$ の多項式 $F_j(\mathbf{a}, \mathbf{b}; X) \in k[\mathbf{a}, \mathbf{b}][X]$ が M 上既約であることに矛盾する． □

命題 3.5. ある $j, (0 \le j \le n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n, (\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0)$, に対して，もし各 $i = 0, \ldots, n-1$, について $D^0_{i,j}(\mathbf{a}, \mathbf{b}) \neq 0$ であるならば，$F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たない.

証明. [HM] 参照. □

更に分析を進める前に，ここで集合 $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$, $(0 \le i \le n-1)$ への群 $G_{\mathbf{s},\mathbf{t}}$ と群 $G_{\mathbf{a},\mathbf{b}}$ の作用について考察しておく．ここで $g \in G_{\mathbf{s},\mathbf{t}}$ は右剰余類の集合 $H \backslash G_{\mathbf{s},\mathbf{t}}$ の完全代表系を動き，c^g_i は $c^g_i = u^g_i(\boldsymbol{\alpha}, \boldsymbol{\beta})$ によって定義されたのであった．独立な $2n$ 変数 $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ の有理関数 $u_i(\mathbf{x}, \mathbf{y})$ は体 $L_{\mathbf{s}} L_{\mathbf{t}} = k(\mathbf{x}, \mathbf{y})$ に属し，ガロア群 $G_{\mathbf{s},\mathbf{t}} = \mathrm{Gal}(L_{\mathbf{s}} L_{\mathbf{t}} / k(\mathbf{s}, \mathbf{t}))$ は集合 $\{x_1, \ldots, x_n\}$ と $\{y_1, \ldots, y_n\}$ への置換を通して，自然に $u_i(\mathbf{x}, \mathbf{y})$ たちに作用する： $g = (\sigma, \tau) \in G_{\mathbf{s},\mathbf{t}}$ に対し，$u^g_i(\mathbf{x}, \mathbf{y}) = u_i(\mathbf{x}^g, \mathbf{y}^g)$, $\mathbf{x}^g = (x_{\varphi(\sigma)(1)}, \ldots, x_{\varphi(\sigma)(n)})$, $\mathbf{y}^g = (y_{\psi(\tau)(1)}, \ldots, x_{\psi(\tau)(n)})$.

しかしながら，群 $G_{\mathbf{s},\mathbf{t}}$ はガロア群として直接 u^g_i の値の集合 $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に作用しているわけではない．数値 c^g_i は右剰余類 Hg の値だけで決まることから，c^g_i, $(\overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}})$, を，$H \backslash G_{\mathbf{s},\mathbf{t}}$ 上定義された関数 $\mathbf{c}_i(g) := c^g_i$ とみなす．このとき，$h \in G_{\mathbf{s},\mathbf{t}}$ に対し，$\mathbf{c}^h_i(g) := c^{gh}_i$ は $H \backslash G_{\mathbf{s},\mathbf{t}}$ 上の h による平行移動と関数 $\mathbf{c}_i$ との合成として捉えられ，各 $h \in G_{\mathbf{s},\mathbf{t}}$ は値の集合 $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ の置換を引き起こす．この様にして，$G_{\mathbf{s},\mathbf{t}}$ は $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に可移的に作用している．もし $\#\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\} = n!$ であれば，$\#(H \backslash G_{\mathbf{s},\mathbf{t}}) = n!$ であるから $\mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(c^g_i) = \mathrm{Stab}_{G_{\mathbf{s},\mathbf{t}}}(u^g_i(\mathbf{x}, \mathbf{y})) = g^{-1} H g$ が成り立つ.

ガロア群 $G_{\mathbf{a},\mathbf{b}}$ に対しては，状況は異なる．各 c^g_i は体 $L_{\mathbf{a}} L_{\mathbf{b}}$ に含まれているので，$G_{\mathbf{a},\mathbf{b}}$ は集合 $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ に対して直接にガロア群 $\mathrm{Gal}(L_{\mathbf{a}} L_{\mathbf{b}} / M)$ として作用する．さらに，仮定 $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ の下で，$G_{\mathbf{a},\mathbf{b}}$ は $G_{\mathbf{s},\mathbf{t}}$ の部分群と見なすことができた.

補題 3.6. 群 $G_{\mathbf{a},\mathbf{b}}$ の集合 $\{c^g_i \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}\}$ へのガロア群 $\mathrm{Gal}(L_{\mathbf{a}} L_{\mathbf{b}} / M)$ としての作用と，$G_{\mathbf{s},\mathbf{t}}$ の部分群としての $G_{\mathbf{s},\mathbf{t}}$ の $H \backslash G_{\mathbf{s},\mathbf{t}}$ への作用から得られる作用とは一致する.

証明. [HM] 参照. □

命題 3.7. 通例のように $\mathbf{a}, \mathbf{b} \in M^n$ に対して $\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0$ を仮定する．さらに，ある $j, (0 \le j \le n-1)$, に対して多項式 $F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たないとする．このとき，次が成り立つ：
(i) 各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$M(c^g_0, \ldots, c^g_{n-1}) = M(c^g_j)$;
(ii) $L_{\mathbf{a}} L_{\mathbf{b}} = M(c^g_j \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}})$.

証明. [HM] 参照. □

定理 3.8. ある $j, (0 \le j \le n-1)$, と $\mathbf{a}, \mathbf{b} \in M^n$ $(\Delta_{\mathbf{a}} \cdot \Delta_{\mathbf{b}} \neq 0)$ に対して，多項式 $F_j(\mathbf{a}, \mathbf{b}; X)$ は重根を持たないとする．このとき，剰余環 $M[X]/(f_n(\mathbf{a}; X))$ と $M[X]/(f_n(\mathbf{b}; X))$ が M 上同型となるためには，$F_j(\mathbf{a}, \mathbf{b}; X)$ が M 内に根を持つことが必要十分である.

証明. [HM] 参照. □

系 3.9. 整数 j と $\mathbf{a}, \mathbf{b} \in M^n$ を定理 3.8 と同様とする．また $G_{\mathbf{a}}$ と $G_{\mathbf{b}}$ はある群 G に同型であって，G の指数 n の全ての部分群は G-共役であると仮定する．このとき，$\mathrm{Spl}_M(f_n(\mathbf{a}; X))$ と $\mathrm{Spl}_M(f_n(\mathbf{b}; X))$ が一致するためには，$F_j(\mathbf{a}, \mathbf{b}; X)$ が M 内に根を持つことが必要十分である．

もし群 G が，n 次対称群 $\mathfrak{S}_n$, $(n \neq 6)$, n 次交代群 $\mathfrak{A}_n$, $(n \neq 6)$, または，ある素数 p に対する，p 次対称群 $\mathfrak{S}_p$ の可解な可移部分群であるとすると，指数 n (最後の場合には p) の全ての部分群は G-共役となる ([Hup67], [BJY86] 参照).

さて H_1, H_2 を $\mathfrak{S}_n$ の部分群とする．定理 2.6 の類似として，直積 $H_1 \times H_2$ に対する k-生成的多項式が次のようにして得られる．

定理 3.10. 基礎体 k 上の $(k+l)$ 変数有理関数体を $M = k(q_1, \ldots, q_k, r_1, \ldots, r_l)$, $(1 \leq k, l \leq n-1)$ とし，$\mathbf{a} \in k(q_1, \ldots, q_k)^n$, $\mathbf{b} \in k(r_1, \ldots, r_l)^n$ に対して，$f_n(\mathbf{a}; X) \in M[X]$ と $f_n(\mathbf{b}; X) \in M[X]$ はそれぞれ H_1 と H_2 に対する k-生成的多項式であるとする．さらに，ある $j, (0 \leq j \leq n-1)$, に対し，$F_j(\mathbf{a}, \mathbf{b}; X) \in M[X]$ は重根を持たないとする．このとき，$F_j(\mathbf{a}, \mathbf{b}; X)$ は $H_1 \times H_2$ に対する k-生成的多項式である．但し，$F_j(\mathbf{a}, \mathbf{b}; X)$ は M 上既約であるとは限らない.

証明. 命題 3.7 より $M(c_j^g \mid \overline{g} \in H \backslash G_{\mathbf{s},\mathbf{t}}) = L_{\mathbf{a}} L_{\mathbf{b}}$ が従う．よって定理の主張は $f_n(\mathbf{a}; X)$ の H_1-生成性と $f_n(\mathbf{b}; X)$ の H_2-生成性から従う. □

チルンハウス同値の各同値類に対し，$a_1 = 0$ かつ $a_{n-1} = a_n$ を満たす多項式 $f_n(\mathbf{s}; X)$ が存在することが知られている．すなわち，$a_1 = 0$ かつ $a_{n-1} = a_n$ である特殊化 $\mathbf{s} \mapsto \mathbf{a} \in M^n$ が常に選べる ([JLY02, §8.2] 参照)．よって多項式

$$\begin{aligned} g_n(q_2, \ldots, q_{n-1}; X) &:= (-1)^n \cdot f_n(0, q_2, \ldots, q_{n-2}, q_{n-1}, q_{n-1}; -X) \\ &= X^n + q_2 X^{n-2} + \cdots + q_{n-2} X^2 + q_{n-1} X + q_{n-1} \end{aligned}$$

は任意の基礎体 k に対し，$\mathfrak{S}_n$ に対する $(n-2)$ パラメータ $q_2, \ldots, q_{n-1}$ 付きの k-生成的多項式である.

系 3.11. $M = k(q_2, \ldots, q_{n-1}, r_2, \ldots, r_{n-1})$ を k 上 $2(n-2)$ 変数有理関数体, $\mathbf{a} = (0, q_2, \ldots, q_{n-1}, q_{n-1})$, $\mathbf{b} = (0, r_2, \ldots, r_{n-1}, r_{n-1}) \in M^n$ とする．ある $j, (0 \leq j \leq n-1)$, に対して，$F_j(\mathbf{a}, \mathbf{b}; X) \in M[X]$ が重根を持たなければ，$F_j(\mathbf{a}, \mathbf{b}; X)$ は $\mathfrak{S}_n \times \mathfrak{S}_n$ に対する $2(n-2)$ 個のパラメータ $q_2, \ldots, q_{n-1}, r_2, \ldots, r_{n-1}$ を持つ k-生成的多項式である.

生成的多項式の部分体問題の解を得るために，各 $g \in G_{\mathbf{s},\mathbf{t}}$ に対してチルンハウス変換の係数の体 $M(c_0^g, \ldots, c_{n-1}^g)$ の M 上の次数を考察する．我々の多項式 $F_i(\mathbf{a}, \mathbf{b}; X)$ の M 上の既約多項式への因数分解の型は，特殊化 $(\mathbf{s}, \mathbf{t}) \mapsto (\mathbf{a}, \mathbf{b})$ による $f_n(\mathbf{a}; X)$ と $f_n(\mathbf{b}; X)$ のガロア群の退化の様子，及び $f_n(\mathbf{a}; X)$ と $f_n(\mathbf{b}; X)$ の M 上の根体の共通部分の大きさを，命題 3.2 のようにして，体 $M(c_0^g, \ldots, c_{n-1}^g)$ の M 上の次数を通じて我々に教えてくれる.

命題 3.12. 体 M の標数が 2 でない場合には $\Delta_{\mathbf{a}}/\Delta_{\mathbf{b}} \in M$，標数が 2 の場合には $\beta_{\mathbf{a}} + \beta_{\mathbf{b}} \in M$ とする．このとき多項式 $F_i(\mathbf{a}, \mathbf{b}; X)$ は次数 $n!/2$ の 2 つの因子に M 上で分解する．但し，これら 2 つの多項式は M 上既約であるとは限らない.

証明. 命題 2.7 から従う. □

系 3.13. もし $G_{\mathbf{a}}, G_{\mathbf{b}} \subset \mathfrak{A}_n$ であれば，$F_i(\mathbf{a}, \mathbf{b}; X)$ は (M 上で既約であるとは限らない) 次数 $n!/2$ の 2 つの因子に M 上で分解する.

§ 4　3 次多項式の場合

これまでの § 2, § 3 における一般論を基にして，生成的多項式の部分体問題を 3 次の場合に限定し，より具体的に考察する．多項式

$$f_3(\mathbf{s};X) := X^3 - s_1X^2 + s_2X - s_3 \in k(\mathbf{s})[X],$$

$$s_1 = x_1 + x_2 + x_3, \quad s_2 = x_1x_2 + x_1x_3 + x_2x_3, \quad s_3 = x_1x_2x_3$$

を用意し，§ 3 の様に差積 $\Delta_{\mathbf{s}}$，または $\mathrm{char}\ k = 2$ の場合には Berlekamp の判別式 $\beta_{\mathbf{s}}$ を取る：

$$\begin{aligned}
\Delta_{\mathbf{s}} &:= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2),\\
\beta_{\mathbf{s}} &:= \frac{x_1}{x_1 + x_2} + \frac{x_1}{x_1 + x_3} + \frac{x_2}{x_2 + x_3} = \frac{x_1^2x_2 + x_2^2x_3 + x_1x_3^2 + x_1x_2x_3}{x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2^2 + x_2x_3^2 + x_3x_1^2}.
\end{aligned} \tag{11}$$

差積 $\Delta_{\mathbf{s}}$，Berlekamp の判別式 $\beta_{\mathbf{s}}$ はそれぞれ

$$\begin{aligned}
\Delta_{\mathbf{s}}^2 &= s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 + 18s_1s_2s_3 - 27s_3^2,\\
\beta_{\mathbf{s}}(\beta_{\mathbf{s}} + 1) &= \frac{s_2^3 + s_1^3s_3 + s_1s_2s_3 + s_3^2}{s_1^2s_2^2 + s_3^2}
\end{aligned}$$

を満たし，体 $k(\mathbf{s})(\Delta_{\mathbf{s}})$ (k の標数が 2 の場合には $k(\mathbf{s})(\beta_{\mathbf{s}})$) は $k(\mathbf{s})$ の 2 次拡大となる．定義 (2) から (u_0, u_1, u_2) は次の形のように直接計算できる：

$$\begin{aligned}
u_0 &= \frac{x_2x_3y_1}{(x_2 - x_1)(x_3 - x_1)} - \frac{x_1x_3y_2}{(x_2 - x_1)(x_3 - x_2)} + \frac{x_1x_2y_3}{(x_3 - x_1)(x_3 - x_2)},\\
u_1 &= -\frac{(x_2 + x_3)y_1}{(x_2 - x_1)(x_3 - x_1)} + \frac{(x_1 + x_3)y_2}{(x_2 - x_1)(x_3 - x_2)} - \frac{(x_1 + x_2)y_3}{(x_3 - x_1)(x_3 - x_2)},\\
u_2 &= \frac{y_1}{(x_2 - x_1)(x_3 - x_1)} - \frac{y_2}{(x_2 - x_1)(x_3 - x_2)} + \frac{y_3}{(x_3 - x_1)(x_3 - x_2)}.
\end{aligned}$$

多項式 $f_3(\mathbf{s};X)$ のチルンハウス変換の一般形は

$$\begin{aligned}
g_3(\mathbf{s}, u_0, u_1, u_2; X) :=\ & \mathrm{Resultant}_Y\big(f_3(\mathbf{s};Y), X - (u_0 + u_1Y + u_2Y^2)\big)\\
=\ & X^3 + (-3u_0 - s_1u_1 - s_1^2u_2 + 2s_2u_2)X^2 + (3u_0^2 + 2s_1u_0u_1 + s_2u_1^2\\
& + 2s_1^2u_0u_2 - 4s_2u_0u_2 + s_1s_2u_1u_2 - 3s_3u_1u_2 + s_2^2u_2^2 - 2s_1s_3u_2^2)X\\
& - u_0^3 - s_1u_0^2u_1 - s_2u_0u_1^2 - s_3u_1^3 - s_1^2u_0^2u_2 + 2s_2u_0^2u_2 - s_1s_2u_0u_1u_2\\
& + 3s_3u_0u_1u_2 - s_1s_3u_1^2u_2 - s_2^2u_0u_2^2 + 2s_1s_3u_0u_2^2 - s_2s_3u_1u_2^2 - s_3^2u_2^3
\end{aligned} \tag{12}$$

によって与えられる．また，定義から u_0, u_1, u_2 は

$$f_3(\mathbf{t};X) = g_3(\mathbf{s}, u_0^g, u_1^g, u_2^g; X), \quad (g \in G_{\mathbf{s},\mathbf{t}}) \tag{13}$$

を満たす．以下において，便宜上，記号

$$\begin{aligned}
&A_{\mathbf{s}} := s_1^2 - 3s_2, \quad B_{\mathbf{s}} := 2s_1^3 - 9s_1s_2 + 27s_3, \quad C_{\mathbf{s}} := s_1^4 - 4s_1^2s_2 + s_2^2 + 6s_1s_3,\\
&D_{\mathbf{s}} := \mathrm{Disc}_X f_3(\mathbf{s};X) = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 + 18s_1s_2s_3 - 27s_3^2 \quad (= \Delta_{\mathbf{s}}^2)
\end{aligned} \tag{14}$$

を使う事にする．直接計算から等式

$$4A_{\mathbf{s}}^3 - B_{\mathbf{s}}^2 = 27D_{\mathbf{s}} \tag{15}$$

が成り立つことが確かめられる．計算代数を用いて，6 次多項式

$$F_i(\mathbf{s}, \mathbf{t}; X) = \prod_{\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}} (X - u_i^g) \in K[X], \quad (i = 1, 2)$$

を求めると以下のようになる：

$$F_1(\mathbf{s},\mathbf{t};X) := X^6 - \frac{2A_{\mathbf{t}}C_{\mathbf{s}}}{D_{\mathbf{s}}}X^4 - \frac{(s_1s_2-s_3)B_{\mathbf{t}}}{D_{\mathbf{s}}}X^3 + \frac{A_{\mathbf{t}}^2C_{\mathbf{s}}^2}{D_{\mathbf{s}}^2}X^2 + \frac{(s_1s_2-s_3)A_{\mathbf{t}}B_{\mathbf{t}}C_{\mathbf{s}}}{D_{\mathbf{s}}^2}X + \frac{(s_1s_2-s_3)^2A_{\mathbf{t}}^3D_{\mathbf{s}} - C_{\mathbf{s}}^3D_{\mathbf{t}}}{D_{\mathbf{s}}^3}, \tag{16}$$

$$F_2(\mathbf{s},\mathbf{t};X) := X^6 - \frac{2A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X^4 + \frac{B_{\mathbf{t}}}{D_{\mathbf{s}}}X^3 + \frac{A_{\mathbf{s}}^2A_{\mathbf{t}}^2}{D_{\mathbf{s}}^2}X^2 - \frac{A_{\mathbf{s}}A_{\mathbf{t}}B_{\mathbf{t}}}{D_{\mathbf{s}}^2}X + \frac{A_{\mathbf{t}}^3D_{\mathbf{s}} - A_{\mathbf{s}}^3D_{\mathbf{t}}}{D_{\mathbf{s}}^3}. \tag{17}$$

多項式 $F_0(\mathbf{s},\mathbf{t};X)$ の表示は，その根 u_0^g が $F_1(\mathbf{s},\mathbf{t};X)$ と $F_2(\mathbf{s},\mathbf{t};X)$ の根から式 (20) と (22) を用いて得られることもあり，複雑なので省略する．多項式 $F_2(\mathbf{s},\mathbf{t};X)$ の X に関する判別式は

$$D_{\mathbf{s},\mathbf{t}} := \frac{B_{\mathbf{s}}^6D_{\mathbf{t}}^3(A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}})^2}{D_{\mathbf{s}}^{15}} \tag{18}$$

で与えられる．また，char $k \neq 2$ の場合には，式 (15) から次のようにも表示できる：

$$A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}} = 4A_{\mathbf{s}}^3A_{\mathbf{t}}^3 - 27(A_{\mathbf{t}}^3D_{\mathbf{s}} + A_{\mathbf{s}}^3D_{\mathbf{t}}) = \frac{B_{\mathbf{s}}^2B_{\mathbf{t}}^2 - 3^6D_{\mathbf{s}}D_{\mathbf{t}}}{4}. \tag{19}$$

命題 2.7 より $F_2(\mathbf{s},\mathbf{t};X)$ の分解

$$F_2(\mathbf{s},\mathbf{t};X) = F_2^+(X)F_2^-(X)$$

が得られる；但し $F_2^+(X)$, $F_2^-(X)$ は $K(\Delta_{\mathbf{s}}/\Delta_{\mathbf{t}})$ 上 (char $k=2$ のときは $K(\beta_{\mathbf{s}}+\beta_{\mathbf{t}})$ 上) 定義された多項式である．まず char $k \neq 2$ なる場合には，定義 (4) より

$$F_2^{\pm}(X) = X^3 - \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{B_{\mathbf{t}} \mp B_{\mathbf{s}}(\Delta_{\mathbf{t}}/\Delta_{\mathbf{s}})}{2D_{\mathbf{s}}}$$

である．また char $k=2$ の場合には,

$$F_2^+(X) = X^3 + \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{s_1A_{\mathbf{s}}B_{\mathbf{t}} + t_1A_{\mathbf{t}}B_{\mathbf{s}} + B_{\mathbf{s}}B_{\mathbf{t}}(\beta_{\mathbf{s}}+\beta_{\mathbf{t}})}{B_{\mathbf{s}}D_{\mathbf{s}}},$$
$$F_2^-(X) = X^3 + \frac{A_{\mathbf{s}}A_{\mathbf{t}}}{D_{\mathbf{s}}}X + \frac{s_1A_{\mathbf{s}}B_{\mathbf{t}} + t_1A_{\mathbf{t}}B_{\mathbf{s}} + B_{\mathbf{s}}B_{\mathbf{t}}(\beta_{\mathbf{s}}+\beta_{\mathbf{t}}+1)}{B_{\mathbf{s}}D_{\mathbf{s}}}$$

が得られる．

無限体 M に対して，特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^3 \times M^3$ は，常に $f_3(\mathbf{a};X)$, $f_3(\mathbf{b};X)$ が M 上分離的になるように選ばれるものと前提する．すなわち，以下 $D_{\mathbf{a}} \cdot D_{\mathbf{b}} \neq 0$ を仮定する．また

$$L_{\mathbf{a}} := \mathrm{Spl}_M f_3(\mathbf{a};X), \quad L_{\mathbf{b}} := \mathrm{Spl}_M f_3(\mathbf{b};X), \quad G_{\mathbf{a}} := \mathrm{Gal}(L_{\mathbf{a}}/M), \quad G_{\mathbf{b}} := \mathrm{Gal}(L_{\mathbf{b}}/M)$$

と置き，$\#G_{\mathbf{a}} \geq \#G_{\mathbf{b}}$ であるとする．さらに，$f_3(\mathbf{a};X)$ は M 上既約であると仮定する．群 $G_{\mathbf{a}}$ は $\mathfrak{S}_3$ または $\mathfrak{A}_3 = C_3$ と同型であり，群 $G_{\mathbf{b}}$ は $\mathfrak{S}_3, C_3, C_2$ または $\{1\}$ と同型となる．我々は $F_j(\mathbf{s},\mathbf{t};X)$ を通して $f_3(\mathbf{s};X)$ に対する部分体問題の解を与える．すなわち $\mathbf{a},\mathbf{b} \in M^3$ に対し，$L_{\mathbf{a}} \supseteq L_{\mathbf{b}}$ となる必要十分条件を与える．

4.1 char $k \neq 3$ の場合

最初に，体 k の標数が 3 ではない場合を取り扱い，char $k=3$ の場合は小節 4.4 で論じる．

式 (13) の多項式を X について展開し，各項を比較することで

$$u_0 = \frac{t_1 - s_1u_1 - s_1^2u_2 + 2s_2u_2}{3}, \quad u_1 = \frac{Q_{1,2}(\mathbf{s},\mathbf{t};u_2)}{D_{1,2}(\mathbf{s},\mathbf{t};u_2)} \tag{20}$$

但し,

$$Q_{1,2}(\mathbf{s},\mathbf{t};u_2) := 3A_{\mathbf{s}}^2B_{\mathbf{t}} - A_{\mathbf{t}}(6A_{\mathbf{s}}^3 - B_{\mathbf{s}}^2 + 2A_{\mathbf{s}}B_{\mathbf{s}}s_1)u_2 + 6D_{\mathbf{s}}(A_{\mathbf{s}}^2 + B_{\mathbf{s}}s_1)u_2^3,$$
$$D_{1,2}(\mathbf{s},\mathbf{t};u_2) := 3B_{\mathbf{s}}(A_{\mathbf{s}}A_{\mathbf{t}} - 3D_{\mathbf{s}}u_2^2)$$

が得られる．また，u_1 を消去することによって次式を得る：

$$u_0 = \frac{(t_1 - s_1^2 u_2 + 2s_2 u_2) D_{1,2}(\mathbf{s},\mathbf{t};u_2) - s_1 Q_{1,2}(\mathbf{s},\mathbf{t};u_2)}{3D_{1,2}(\mathbf{s},\mathbf{t};u_2)}. \tag{21}$$

式 (20) と (21) から，命題 2.2 のようにして，任意の $g \in G_{\mathbf{s},\mathbf{t}}$ に対して，$K(u_0^g, u_1^g, u_2^g) = K(u_2^g)$, $K = k(\mathbf{s},\mathbf{t})$ であることが直接確認できる．さらには，式 (10) を満たす $D_{0,2}^0(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ と $D_{1,2}^0(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ が次のように得られる：まず,

$$\frac{1}{D_{1,2}(\mathbf{s},\mathbf{t};u_2)} = \frac{1}{3B_{\mathbf{s}}(A_{\mathbf{s}}A_{\mathbf{t}} - 3D_{\mathbf{s}}u_2^2)} = \frac{1}{D_{1,2}^0(\mathbf{s},\mathbf{t})} \sum_{i=0}^{5} h_i(\mathbf{s},\mathbf{t}) u_2^i$$

となる $D_{1,2}^0(\mathbf{s},\mathbf{t})$, $h_i(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ を取る．実際，計算代数を用いて

$$\begin{aligned}
&D_{1,2}^0(\mathbf{s},\mathbf{t}) := 3B_{\mathbf{s}}(A_{\mathbf{s}}^3 B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3 D_{\mathbf{s}})^2,\\
&\big\{h_0(\mathbf{s},\mathbf{t}),\dots,h_5(\mathbf{s},\mathbf{t})\big\} = \big\{4A_{\mathbf{s}}^2A_{\mathbf{t}}^2(A_{\mathbf{s}}^3B_{\mathbf{t}}^2 + 27A_{\mathbf{t}}^3D_{\mathbf{s}} - 27B_{\mathbf{t}}^2D_{\mathbf{s}}), 27B_{\mathbf{t}}D_{\mathbf{s}}(4A_{\mathbf{s}}^3A_{\mathbf{t}}^3 + 9A_{\mathbf{t}}^3D_{\mathbf{s}} - 9A_{\mathbf{s}}^3D_{\mathbf{t}}),\\
&-3A_{\mathbf{s}}A_{\mathbf{t}}D_{\mathbf{s}}(5A_{\mathbf{s}}^3B_{\mathbf{t}}^2 + 135A_{\mathbf{t}}^3D_{\mathbf{s}} - 54B_{\mathbf{t}}^2D_{\mathbf{s}}), -270A_{\mathbf{s}}^2A_{\mathbf{t}}^2B_{\mathbf{t}}D_{\mathbf{s}}^2, 9D_{\mathbf{s}}^2(A_{\mathbf{s}}^3B_{\mathbf{t}}^2 + 27A_{\mathbf{t}}^3D_{\mathbf{s}}), 162A_{\mathbf{s}}A_{\mathbf{t}}B_{\mathbf{t}}D_{\mathbf{s}}^3\big\}
\end{aligned}$$

を得る．ここで，式 (21) から，$D_{0,2}^0(\mathbf{s},\mathbf{t}) := 3 \cdot D_{1,2}^0(\mathbf{s},\mathbf{t}) \in k[\mathbf{s},\mathbf{t}]$ と定義する．以上によって,

$$u_i = \frac{1}{D_{i,2}^0(\mathbf{s},\mathbf{t})} P_{i,2}^0(\mathbf{s},\mathbf{t};u_2), \quad \text{かつ} \quad \deg_X(P_{i,2}^0(\mathbf{s},\mathbf{t};X)) = 5$$

を満たす $P_{i,2}^0(\mathbf{s},\mathbf{t};X) \in k[\mathbf{s},\mathbf{t}][X], (i = 0,1)$, が具体的に得られる．

変数の特殊化 $(\mathbf{s},\mathbf{t}) \mapsto (\mathbf{a},\mathbf{b}) \in M^3 \times M^3$ の後，次の補題が成り立つ．

補題 4.1. (1) もし $f_3(\mathbf{a};X)$ が M 上既約ならば，$B_{\mathbf{a}} \neq 0$.
(2) もし $A_{\mathbf{a}} = 0$ ならば，$f_3(\mathbf{a};X)$ と $X^3 - B_{\mathbf{a}}$ は M 上チルンハウス同値である．よって，$f_3(\mathbf{a};X)$ の $M(\sqrt{-3})$ 上のガロア群は位数 3 の巡回群となる．
(3) もし $A_{\mathbf{a}} = 0$ ならば，$f_3(\mathbf{a};X)$ と $Y^3 - 3Y - (B_{\mathbf{a}} + 1/B_{\mathbf{a}})$ は M 上チルンハウス同値である．

証明. (1), (2) は等式 $3^3 \cdot f_3(\mathbf{s};X) = (3X - s_1)^3 - 3A_{\mathbf{s}}(3X - s_1) - B_{\mathbf{s}}$ から従う．また $X^3 - B_{\mathbf{a}} = 0$ の場合には，$Y = X + 1/X = X(1 + X/B_{\mathbf{a}})$ と置くことによって $Y^3 - 3Y - (B_{\mathbf{a}} + 1/B_{\mathbf{a}}) = 0$ を得る． □

補題 4.1 (1) により，$f_3(\mathbf{a};X)$ が M 上既約という仮定から $B_{\mathbf{a}} \neq 0$ が従う．また，補題 4.1 (3) により，一般性を失うことなく $A_{\mathbf{a}} \neq 0$ かつ $A_{\mathbf{b}} \neq 0$ と仮定してよい．式 (18) より，$B_{\mathbf{a}} \neq 0$ かつ $D_{\mathbf{b}} \neq 0$ という仮定の下では，多項式 $F_2(\mathbf{a},\mathbf{b};X)$ が重根をもつためには $A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} = 0$ が必要十分である事が分かる．前節 § 3 の定理 3.8(系 3.9) の特別な場合として，生成的多項式 $f_3(\mathbf{s};X)$ の同型問題の解を得る．

定理 4.2. (1) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} = 0$ ならば，$\mathrm{Spl}_M f_3(\mathbf{a};X) = \mathrm{Spl}_M f_3(\mathbf{b};X)$.
(2) もし $A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} \neq 0$ ならば，次の 2 つの条件は同値である :
(i) $\mathrm{Spl}_M f_3(\mathbf{a};X) = \mathrm{Spl}_M f_3(\mathbf{b};X)$;
(ii) 6 次多項式 $F_2(\mathbf{a},\mathbf{b};X)$ は M 内に根を持つ.

証明. [HM] 参照. □

さらには，k-生成的多項式 $f_3(\mathbf{s};X)$ の部分体問題の解は，次のように与えられる.

定理 4.3. 条件 $A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} \neq 0$ を満たす $\mathbf{a},\mathbf{b} \in M^3$ に対して，$F_2(\mathbf{a},\mathbf{b};X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型により，生成的多項式 $f_3(\mathbf{s};X)$ の部分体問題の解は表 1 のように与えられる．また，各既約因子 $h_\mu(X)$ の根体 M_μ は $\mathrm{Spl}_{M_\mu} f_3(\mathbf{a},X) = \mathrm{Spl}_{M_\mu} f_3(\mathbf{b},X)$ を満たす.

$G_{\mathbf{a}}$	$G_{\mathbf{b}}$		$(d_\mu), d_\mu = \deg(h_\mu(X))$
$\mathfrak{S}_3$	$\mathfrak{S}_3$	$L_{\mathbf{a}} \neq L_{\mathbf{b}}, L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
		$L_{\mathbf{a}} \neq L_{\mathbf{b}}, [L_{\mathbf{a}} \cap L_{\mathbf{b}} : K] = 2$	(3)(3)
		$L_{\mathbf{a}} = L_{\mathbf{b}}$	(1)(2)(3)
	C_3	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
	C_2	$L_{\mathbf{a}} \not\supset L_{\mathbf{b}}$	(6)
		$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(3)(3)
	$\{1\}$	$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(6)
C_3	C_3	$L_{\mathbf{a}} \neq L_{\mathbf{b}}$	(3)(3)
		$L_{\mathbf{a}} = L_{\mathbf{b}}$	(1)(1)(1)(3)
	C_2	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	(6)
	$\{1\}$	$L_{\mathbf{a}} \supset L_{\mathbf{b}}$	(3)(3)

表 1

証明. [HM] 参照. □

4.2 特別な場合 : $X^3 + sX + s$

この小節でも $\mathrm{char}\ k \neq 3$ とする．また，前小節のように $A_2 := -A_{\mathbf{a}}/3, A_3 := B_{\mathbf{a}}/27$ と置く．このとき，$A_{\mathbf{a}} \neq 0$ かつ $B_{\mathbf{a}} \neq 0$ であるような $\mathbf{a} = (a_1, a_2, a_3) \in M^3$ に対して，多項式 $f_3(\mathbf{a}; X)$ と $f_3(0, a, -a; X) = X^3 + aX + a$ は M 上チルンハウス同値である；但し，

$$a := \frac{A_2^3}{A_3^2} = -\frac{27A_{\mathbf{a}}^3}{B_{\mathbf{a}}^2} = -\frac{27(a_1^2 - 3a_2)^3}{(2a_1^3 - 9a_1a_2 + 27a_3)^2}.$$

これは，次の等式から直接従う：

$$X^3 + A_2X - A_3 = -\frac{A_3^3}{A_2^3}\Big(\Big(-\frac{A_2X}{A_3}\Big)^3 + a\Big(-\frac{A_2X}{A_3}\Big) + a\Big).$$

注意 4.4. 上記のチルンハウス同値及び前小節のチルンハウス同値は，根のアフィン変換のみによって与えられていることに注意しておく．すなわち，根の 1 次式による変換である．

さて $\mathbf{a} = (0, a, -a) \in M^3$, $\mathbf{b} = (0, b, -b) \in M^3$ とすると，

$$D_{\mathbf{a}} = \mathrm{Disc}_X f_3(0, a, -a; X) = -a^2(4a + 27),$$
$$A_{\mathbf{a}}^3B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3D_{\mathbf{a}} = -729a^2b^2(4ab + 27a + 27b),$$

$$F_0(\mathbf{a}, \mathbf{b}; X) = X^6 - \frac{8a^3b}{D_{\mathbf{a}}}X^4 - \frac{8a^3b}{D_{\mathbf{a}}}X^3 + \frac{16a^6b^2}{D_{\mathbf{a}}^2}X^2 + \frac{32a^6b^2}{D_{\mathbf{a}}^2}X - \frac{64a^8b^2(a-b)}{D_{\mathbf{a}}^3},$$
$$F_1(\mathbf{a}, \mathbf{b}; X) = X^6 + \frac{6a^2b}{D_{\mathbf{a}}}X^4 + \frac{27ab}{D_{\mathbf{a}}}X^3 + \frac{9a^4b^2}{D_{\mathbf{a}}^2}X^2 + \frac{81a^3b^2}{D_{\mathbf{a}}^2}X + \frac{a^4b^2(27a^2 + 729b + 108ab + 4a^2b)}{D_{\mathbf{a}}^3},$$
$$F_2(\mathbf{a}, \mathbf{b}; X) = X^6 - \frac{18ab}{D_{\mathbf{a}}}X^4 - \frac{27b}{D_{\mathbf{a}}}X^3 + \frac{81a^2b^2}{D_{\mathbf{a}}^2}X^2 + \frac{243ab^2}{D_{\mathbf{a}}^2}X - \frac{729a^2b^2(a-b)}{D_{\mathbf{a}}^3}$$

が得られる，但し $D_{\mathbf{a}} = -a^2(4a + 27)$ である．

定理 4.3 より，$D_{\mathbf{a}} \cdot D_{\mathbf{b}} \neq 0$ であるような $a, b \in M$ に対し，もし $4ab+27a+27b = 0$ ならば，X^3+aX+a と $X^3 + bX + b$ は M 上チルンハウス同値である．よって

$$X^3 + aX + a \quad と \quad X^3 - \frac{27a}{4a + 27}X - \frac{27a}{4a + 27}$$

は M 上で同じ最小分解体を持つ.

ここで

$$G_2(a,b;X) := F_2(0,a,-a,0,b,-b;X)$$

と置けば，次の定理が成り立つ．

定理 4.5. もし $D_{\mathbf{a}} \cdot D_{\mathbf{b}} \neq 0$ であるような $a,b \in M$ に対して $4ab+27a+27b \neq 0$ であれば，$G_2(a,b;X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって，生成的多項式 X^3+sX+s の部分体問題の解は定理 4.3 の表 1 のように与えられる．

論文 [HM07] において，我々は char $k \neq 3$ という仮定の下で生成的多項式 X^3+sX+s の同型問題の解を与えた．ここでは，論文 [HM07] の結果を，少し変形させた形で与える ([HM07] の Theorem 1, Theorem 7 を参照)．まず，$G_2(a,b;X)$ が 0 を根に持つ，すなわち $G_2(a,b;0)=0$ ならば，$ab(a-b)=0$ となることに注意する．以下，$a \neq b$ を仮定する．剰余類 $\overline{g} \in H\backslash G_{\mathbf{s},\mathbf{t}}$ に対して，$c_2^g \neq 0$ であることから，$u := 3c_1/c_2$ が定義され，$(c_0,c_1) = (2ac_2/3, uc_2/3)$ かつ

$$c_2 = \frac{3(u^2+9u-3a)}{u^3-2au^2-9au-2a^2-27a}$$

が成り立つ．さらに，$a(4a+27) \neq 0$ の仮定の下で，$u^3-2au^2-9au-2a^2-27a \neq 0$ であることが分かる．これより $M(c_0,c_1,c_2) = M(u)$ である．また，直接計算から $(a-b)\cdot\prod_{g\in H\backslash G_{\mathbf{s},\mathbf{t}}}(X-u^g) =: H(a,b;X)$ とするとき，

$$H(a,b;X) = a(X^2+9X-3a)^3 - b(X^3-2aX^2-9aX-2a^2-27a)^2$$

が得られる．また $\mathrm{Disc}_X H(a,b;X) = a^{10}b^4(a-b)(4a+27)^{15}(4b+27)^3$ である．

定理 4.6 ([HM07])**.** 上記の記号の下で，$a,b \in M$, $(a \neq b,\ a\cdot b \neq 0)$ に対して，生成的多項式 X^3+sX+s の部分体問題の解は $H(a,b;X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって定理 4.3 の表 1 のように与えられる．特に，X^3+aX+a と X^3+bX+b の 2 つの M 上の最小分解体が一致するためには，次の条件を満たす $u \in M$ が存在することが必要十分である：

$$b = \frac{a(u^2+9u-3a)^3}{(u^3-2au^2-9au-2a^2-27a)^2}.$$

注意 4.7. Komatsu [Ko] は，char $k \neq 2,3$ の仮定の下で，3 次生成的多項式 $g(t,Y) = Y^3-t(Y+1) \in k(t)[Y]$ を取り扱っている．$\mathrm{Spl}_{k(t_1,t_2)}P(t_1,t_2;Z) = \mathrm{Spl}_{k(t_1,t_2)}g(t_1,Y)\cdot\mathrm{Spl}_{k(t_1,t_2)}g(t_2,Y)$ を満たす 6 次式 $P(t_1,t_2;Z)$ を，降下クンマー理論 ([Ko04] も参照) によって構成し，$P(t_1,t_2;Z)$ を用いて $g(t,Y)$ の部分体問題の解を与えている．

4.3 char $k=3$ の場合

この小節では，char $k=3$ の場合を取り扱う．この場合，

$$A_{\mathbf{s}} = s_1^2, \quad B_{\mathbf{s}} = -s_1^3, \quad D_{\mathbf{s}} = s_1^2s_2^2 - s_2^3 - s_1^3s_3$$

となる．式 (13) の X に関する係数を比較する事によって，

$$u_0 = \frac{s_2t_1^2 - s_1^2t_2 - s_2t_1(s_1^2-s_2)u_2 - D_{\mathbf{s}}u_2^2}{s_1^2t_1}, \qquad u_1 = \frac{t_1-(s_1^2+s_2)u_2}{s_1} \tag{22}$$

が得られる．さらに $F_2(\mathbf{s},\mathbf{t};X)$ は

$$F_2(\mathbf{s},\mathbf{t};X) = X^6 + \frac{s_1^2t_1^2}{D_{\mathbf{s}}}X^4 - \frac{t_1^3}{D_{\mathbf{s}}}X^3 + \frac{s_1^4t_1^4}{D_{\mathbf{s}}^2}X^2 + \frac{s_1^2t_1^5}{D_{\mathbf{s}}^2}X + \frac{t_1^6D_{\mathbf{s}} - s_1^6D_{\mathbf{t}}}{D_{\mathbf{s}}^3}$$

で与えられ，その X に関する判別式は以下で与えられる：

$$D_{\mathbf{s},\mathbf{t}} = \frac{B_{\mathbf{s}}^6D_{\mathbf{t}}^3(A_{\mathbf{s}}^3B_{\mathbf{t}}^2 - 27A_{\mathbf{t}}^3D_{\mathbf{s}})^2}{D_{\mathbf{s}}^{15}} = \frac{s_1^{18}D_{\mathbf{t}}^3(s_1^6t_1^6)^2}{D_{\mathbf{s}}^{15}} = \frac{s_1^{30}t_1^{12}D_{\mathbf{t}}^3}{D_{\mathbf{s}}^{15}}.$$

定理 4.8. 条件 $a_1b_1 \neq 0$ を満たす $\mathbf{a} = (a_1, a_2, a_3), \mathbf{b} = (b_1, b_2, b_3) \in M^3$ に対して，生成的多項式 $X^3 - s_1X^2 + s_2X - s_3$ の部分体問題の解は $F_2(\mathbf{a}, \mathbf{b}; X)$ の M 上の既約因子 $h_\mu(X)$ への分解の型によって定理 4.3 の表 1 のように与えられる．

次に $(a_1, a_2, a_3) = (0, a, -a)$ の場合を考察する．多項式 $f_3(0, s, -s) = X^3 + sX + s$ は，$\mathfrak{S}_3$ に対する k-生成的多項式であり，実際 $f_3(\mathbf{s}; X) = X^3 - s_1X^2 + s_2X - s_3 = 0$ に対して

$$Y = \frac{s_1^2}{-s_2 - s_1X}$$

と置けば

$$Y^3 + \frac{-s_1^6}{s_1^2s_2^2 - s_2^3 - s_1^3s_3}Y + \frac{-s_1^6}{s_1^2s_2^2 - s_2^3 - s_1^3s_3} = 0$$

が得られる．よって，$a_1 \cdot D_{\mathbf{a}} \neq 0$ を満たす $\mathbf{a} = (a_1, a_2, a_3) \in M^3$ に対して，多項式 $f_3(\mathbf{a}; X)$ と

$$X^3 + \frac{-a_1^6}{a_1^2a_2^2 - a_2^3 - a_1^3a_3}X + \frac{-a_1^6}{a_1^2a_2^2 - a_2^3 - a_1^3a_3}$$

は M 上チルンハウス同値である．変数の特殊化 $(s_1, s_2, s_3, t_1, t_2, t_3) = (0, s, -s, 0, t, -t)$ を行い，式 (13) の X に関する係数を比較することで，

$$u_1 = \frac{s_2(t + tu_0 + u_0^3)}{st}, \quad u_2 = 0$$

が確認される．また $\mathbf{a} = (0, a, -a), \mathbf{b} = (0, b, -b)$ に対して，

$$\begin{aligned} F_0(\mathbf{a}, \mathbf{b}; X) &= X^6 - bX^4 - bX^3 + b^2X^2 - b^2X + \frac{b^2(a-b)}{a}, \\ F_1(\mathbf{a}, \mathbf{b}; X) &= \left(X^2 - \frac{b}{a}\right)^3, \qquad F_2(\mathbf{a}, \mathbf{b}; X) = X^6 \end{aligned}$$

を得る．また $f_3(\mathbf{a}; X) = X^3 + aX + a$ に対し，$\mathrm{Disc}_X f_3(\mathbf{a}; X) = -a^3$ に注意しておく．ここで

$$G_0(a, b; X) := F_0(\mathbf{a}, \mathbf{b}; X) = X^6 - bX^4 - bX^3 + b^2X^2 - b^2X + \frac{b^2(a-b)}{a}$$

と定義する；$\mathrm{Disc}_X G_0(a, b; X) = b^{15}/a^3$ である．

命題 4.9. $G_0(s, t; X)$ は $\mathfrak{S}_3 \times \mathfrak{S}_3$ に対する k-生成的多項式である．

定理 4.10. 条件 $ab \neq 0$ を満たす $a, b \in M$ に対して，生成的多項式 $X^3 + sX + s$ の部分体問題の解は $G_0(a, b; X)$ の M 上での既約因子 $h_\mu(X)$ への分解の型によって定理 4.3 の表 1 のように与えられる．

§ 5 3 次巡回多項式の場合

巡回置換 $\sigma = (123) \in \mathfrak{S}_3$ は体 $k(x_1, x_2, x_3)$ に変数の置換

$$\sigma \ : \ x_1 \longmapsto x_2, \ x_2 \longmapsto x_3, \ x_3 \longmapsto x_1$$

として作用しているとする．また，

$$z_1 := \frac{x_1 - x_2}{x_2 - x_3}, \quad z_2 := \frac{x_2 - x_3}{x_3 - x_1}, \quad z_3 := \frac{x_3 - x_1}{x_1 - x_2}$$

と置くと，

$$z_2 = \frac{-1}{1 + z_1}, \quad z_3 = \frac{-(1 + z_1)}{z_1}$$

が得られる．さらに $K_1 := k(z_1, z_2, z_3)$ と置くと $K_1 \subset k(x_1, x_2, x_3)$ であり，K_1 の k 上の超越次数は 1 である．また $C_3 = \langle\sigma\rangle$ は体 $K_1 = k(z_1)$ に

$$\sigma \ : \ z_1 \longmapsto \frac{-1}{1 + z_1} \longmapsto \frac{-(1 + z_1)}{z_1} \longmapsto z_1$$

として忠実に作用する．そこで C_3-拡大 $K_1/K_1^{C_3}$ を考察するために，次の多項式 $g^{C_3}(\widetilde{m};X)$ を導入する：

$$g^{C_3}(\widetilde{m};X) := \prod_{x\in \mathrm{Orb}_{\langle\sigma\rangle}(z_1)}(X-x) = \Big(X-z_1\Big)\Big(X+\frac{1}{1+z_1}\Big)\Big(X+\frac{1+z_1}{z_1}\Big)$$
$$= X^3-\widetilde{m}X^2-(\widetilde{m}+3)X-1,$$

$$\widetilde{m} = \frac{z_1^3-3z_1-1}{z_1(z_1+1)} = \frac{-(x_1^3+x_2^3+x_3^3-3x_1^2x_2-3x_2^2x_3-3x_3^2x_1+6x_1x_2x_3)}{(x_2-x_1)(x_3-x_1)(x_3-x_2)}.$$

このとき，$K_1^{C_3}=k(\widetilde{m})$ であり，さらに $g^{C_3}(\widetilde{m};X)$ の $k(\widetilde{m})$ 上の最小分解体は K_1 である．

補題 5.1. 多項式 $f_3(\mathbf{s};X)=X^3-s_1X^2+s_2X-s_3$ と $g^{C_3}(\widetilde{m};X)=X^3-\widetilde{m}X^2-(\widetilde{m}+3)X-1$ は体 $k(x_1,x_2,x_3)^{C_3}$ 上でチルンハウス同値である．

証明. 多項式 $g^{C_3}(\widetilde{m};X)$ の $k(x_1,x_2,x_3)^{C_3}$ 上の最小分解体は $k(x_1,x_2,x_3)$ である．実際，まず

(i) char $k\neq 2$ の場合：$k(x_1,x_2,x_3)^{C_3}=k(s_1,s_2,s_3,\Delta_{\mathbf{s}})$，但し $\Delta_{\mathbf{s}}=(x_2-x_1)(x_3-x_1)(x_3-x_2)$ である．更には，$i=1,2,3$ に対して

$$x_i=\frac{-\Delta_{\mathbf{s}}+s_1s_2-9s_3-2\Delta_{\mathbf{s}}z_i}{2(s_1^2-3s_2)},\quad z_i=-\frac{\Delta_{\mathbf{s}}-s_1s_2+9s_3}{2\Delta_{\mathbf{s}}}-\frac{(s_1^2-3s_2)x_i}{\Delta_{\mathbf{s}}} \tag{23}$$

が成り立つ．

(ii) char $k=2$ の場合：$k(x_1,x_2,x_3)^{C_3}=k(s_1,s_2,s_3,\beta_{\mathbf{s}})$; 但し $\beta_{\mathbf{s}}$ は式 (11) によって与えられた Berlekamp の判別式である．整数 $i=1,2,3$ に対して，

$$x_i=\frac{(s_1s_2+s_3)(\beta_{\mathbf{s}}+z_i)}{s_1^2+s_2},\quad z_i=\beta_{\mathbf{s}}+\frac{(s_1^2+s_2)x_i}{s_1s_2+s_3}$$

が成り立つ． □

ここで，$\widetilde{m}$ を s_1,s_2,s_3 と $\Delta_{\mathbf{s}}$ (char $k=2$ のときには $\beta_{\mathbf{s}}$) によって記述することを考える．任意の体 k 上において

$$k(x_1,x_2,x_3)^{C_3}=k(s_1,s_2,s_3,x_1x_2^2+x_2x_3^2+x_3x_1^2)$$

および

$$\widetilde{m}=\frac{-s_1^3+6s_1s_2-18s_3-3(x_1x_2^2+x_1^2x_3+x_2x_3^2)}{-s_1s_2+3s_3+2(x_1x_2^2+x_1^2x_3+x_2x_3^2)}$$

が成り立つ．よって char $k\neq 2$ の場合は

$$x_1x_2^2+x_2x_3^2+x_3x_1^2=(\Delta_{\mathbf{s}}+s_1s_2-3s_3)/2$$

となり，さらに

$$\widetilde{m}=-\frac{3\Delta_{\mathbf{s}}+2s_1^3-9s_1s_2+27s_3}{2\Delta_{\mathbf{s}}}\quad\Big(=-\frac{3\Delta_{\mathbf{s}}+B_{\mathbf{s}}}{2\Delta_{\mathbf{s}}}\Big)$$

が成り立つ．また char $k=2$ の場合には

$$x_1x_2^2+x_2x_3^2+x_3x_1^2=s_1s_2+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3$$

であり，これより

$$\widetilde{m}=\frac{s_1^3+s_1s_2+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3}{s_1s_2+s_3}\quad\Big(=\frac{s_1A_{\mathbf{s}}+\beta_{\mathbf{s}}B_{\mathbf{s}}}{B_{\mathbf{s}}}\Big)$$

が得られる．

定理 4.3 を $M=k(x_1,x_2,x_3)^{C_3}$ に対して用いると，$f_3(\mathbf{s};X)$ から $g^{C_3}(\widetilde{m};X)$ への $k(x_1,x_2,x_3)^{C_3}$ 上で定義されたチルンハウス変換が 3 つ存在することが分かる．多項式 $F_2(\mathbf{s},\mathbf{t};X)$ の変数の特殊化 $(t_1,t_2,t_3)\mapsto(\widetilde{m},-(\widetilde{m}+3),1)\in k(x_1,x_2,x_3)^{C_3}$ によって，$f_3(\mathbf{s};X)$ から $g^{C_3}(\widetilde{m};X)$ への $k(x_1,x_2,x_3)^{C_3}$ 上のチルンハウス変換の係数 (c_0^g,c_1^g,c_2^g) を具体的に求めることができる：

$$g^{C_3}(\widetilde{m};X)=\mathrm{Resultant}_Y\big(f_3(\mathbf{s};Y),X-(c_0^g+c_1^gY+c_2^gY^2)\big).$$

まず $\mathrm{char}\,k\neq 2$ の場合には，式 (17) から $F_2(\mathbf{s},\widetilde{m},-(\widetilde{m}+3),1;X)$ の具体的な因数分解

$$\begin{aligned}&F_2(s_1,s_2,s_3,\widetilde{m},-(\widetilde{m}+3),1;X)\\&=X\Big(X-\frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big)\Big(X+\frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big)\Big(X^3-\frac{A_{\mathbf{s}}^4}{\Delta_{\mathbf{s}}^4}X-\frac{A_{\mathbf{s}}^3(2A_{\mathbf{s}}s_1-3s_1s_2+27s_3)}{\Delta_{\mathbf{s}}^5}\Big)\end{aligned}$$

が得られる．よって $\big\{c_2^g\mid \overline{g}=\overline{(1,\tau)}\in H\backslash G_{\mathbf{s},\mathbf{t}},\ \psi(\tau)\in\mathfrak{A}_3\big\}=\{0,A_{\mathbf{s}}^2/\Delta_{\mathbf{s}}^2,-A_{\mathbf{s}}^2/\Delta_{\mathbf{s}}^2\}$ となる．また，式 (23) から $c_2=0$ を得る．さらに式 (20) と (21) によって，c_2^g の値から c_0^g, c_1^g が次のように計算できる：

$$\begin{aligned}&(c_0,c_1,c_2)=\Big(\frac{E_{\mathbf{s}}-\Delta_{\mathbf{s}}}{2\Delta_{\mathbf{s}}},-\frac{A_{\mathbf{s}}}{\Delta_{\mathbf{s}}},0\Big),\\&(c_0^{g_1},c_1^{g_1},c_2^{g_1})=\Big(\frac{A_{\mathbf{s}}(A_{\mathbf{s}}s_2-s_2^2+3s_1s_3)-(A_{\mathbf{s}}s_1-E_{\mathbf{s}})\Delta_{\mathbf{s}}-\Delta_{\mathbf{s}}^2}{2\Delta_{\mathbf{s}}^2},\frac{A_{\mathbf{s}}(-2A_{\mathbf{s}}s_1+E_{\mathbf{s}}+\Delta_{\mathbf{s}})}{2\Delta_{\mathbf{s}}^2},\frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big),\\&(c_0^{g_2},c_1^{g_2},c_2^{g_2})=\Big(\frac{-A_{\mathbf{s}}(A_{\mathbf{s}}s_2-s_2^2+3s_1s_3)-(A_{\mathbf{s}}s_1-E_{\mathbf{s}})\Delta_{\mathbf{s}}-\Delta_{\mathbf{s}}^2}{2\Delta_{\mathbf{s}}^2},\frac{A_{\mathbf{s}}(2A_{\mathbf{s}}s_1-E_{\mathbf{s}}+\Delta_{\mathbf{s}})}{2\Delta_{\mathbf{s}}^2},-\frac{A_{\mathbf{s}}^2}{\Delta_{\mathbf{s}}^2}\Big);\end{aligned}$$

但し $E_{\mathbf{s}}=s_1s_2-9s_3$, $\overline{g_i}=\overline{(1,\tau_i)}\in H\backslash G_{\mathbf{s},\mathbf{t}}$, $\psi(\tau_i)\in\mathfrak{A}_3\backslash\{1\}$, $(i=1,2)$. 計算代数を使って，直接

$$z_2=\frac{x_2-x_3}{x_3-x_1}=c_0^{g_1}+c_1^{g_1}x_1+c_2^{g_1}x_1^2,\quad z_3=\frac{x_3-x_1}{x_1-x_2}=c_0^{g_2}+c_1^{g_2}x_1+c_2^{g_2}x_1^2 \tag{24}$$

であることが確認でき，これより $\psi(\tau_1)=(123)\in\mathfrak{A}_3$ かつ $\psi(\tau_2)=(132)\in\mathfrak{A}_3$ が得られる．

他方，$\mathrm{char}\,k=2$ の場合には，$A_{\mathbf{s}}^3B_{\mathbf{t}}^2-27A_{\mathbf{t}}^3D_{\mathbf{s}}=0$，但し $\mathbf{t}=(t_1,t_2,t_3)=(\widetilde{m},-(\widetilde{m}+3),1)$, となり

$$F_2(s_1,s_2,s_3,\widetilde{m},-(\widetilde{m}+3),1;X)=X\Big(X+\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big)^2\Big(X^3+\frac{(s_1^2+s_2)^4}{(s_1s_2+s_3)^4}X+\frac{(s_1^2+s_2)^3}{(s_1s_2+s_3)^4}\Big)$$

が得られる．式 (20) と (21) によって

$$(c_0,c_1,c_2)=\Big(\beta_{\mathbf{s}},\frac{s_1^2+s_2}{s_1s_2+s_3},0\Big)$$

を求めることができ，その他，式 (24) を満たすあと 2 つのチルンハウス変換の係数も

$$\begin{aligned}&(c_0^{g_1},c_1^{g_1},c_2^{g_1})=\Big(\frac{\beta_{\mathbf{s}}(s_1^3+s_3)}{s_1s_2+s_3},\frac{(s_1^2+s_2)(s_1^3+s_3+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3)}{(s_1s_2+s_3)^2},\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big),\\&(c_0^{g_2},c_1^{g_2},c_2^{g_2})=\Big(\frac{s_1^3+s_1s_2+\beta_{\mathbf{s}}s_1^3+\beta_{\mathbf{s}}s_3}{s_1s_2+s_3},\frac{(s_1^2+s_2)(s_1^3+s_1s_2+\beta_{\mathbf{s}}s_1s_2+\beta_{\mathbf{s}}s_3)}{(s_1s_2+s_3)^2},\frac{(s_1^2+s_2)^2}{(s_1s_2+s_3)^2}\Big)\end{aligned}$$

として得られる．

ここで $f_3(\mathbf{a};X)=X^3-a_1X^2+a_2X-a_3$ の M 上のガロア群は C_3 と同型であると仮定する．補題 5.1 において，変数の特殊化 $\mathbf{s}=(s_1,s_2,s_3)\mapsto\mathbf{a}=(a_1,a_2,a_3)\in M^3$，(但し $A_{\mathbf{a}}\neq 0$, $B_{\mathbf{a}}\neq 0$ とする)，を行うことで，$f_3(\mathbf{a};X)$ と $g^{C_3}(m;X)=X^3-mX^2-(m+3)X-1$ は M 上でチルンハウス同値となる．そのとき m は次のように与えられる：

$$m=\begin{cases}-\dfrac{3\Delta_{\mathbf{a}}+2a_1^3-9a_1a_2+27a_3}{2\Delta_{\mathbf{a}}}, & \mathrm{char}\,k\neq 2\ \text{のとき},\\[2ex] \dfrac{a_1^3+a_1a_2+\beta_{\mathbf{a}}a_1a_2+\beta_{\mathbf{a}}a_3}{a_1a_2+a_3}, & \mathrm{char}\,k=2\ \text{のとき}.\end{cases} \tag{25}$$

以下，$\mathbf{a}=(m,-(m+3),1),\mathbf{b}=(n,-(n+3),1)$ とすると，$f_3(\mathbf{a};X)=X^3-mX^2-(m+3)X-1$, $f_3(\mathbf{b};X)=X^3-nX^2-(n+3)X-1$ および

$$D_{\mathbf{a}}=\mathrm{Disc}_X f_3(\mathbf{a};X)=(m^2+3m+9)^2,$$
$$A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=D_{\mathbf{a}}D_{\mathbf{b}}(2mn+3m+3n+18)(2mn+3m+3n-9)$$

が得られる．また $\Delta_{\mathbf{a}}=m^2+3m+9$, $\Delta_{\mathbf{b}}=n^2+3n+9$ および

$$F_2(\mathbf{a},\mathbf{b};X)=F_2^+(m,n;X)F_2^-(m,n;X),$$

$$F_2^+(m,n;X)\ =\ X^3-\frac{\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}}X-\frac{(m-n)\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}^2},\quad F_2^-(m,n;X)\ =\ X^3-\frac{\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}}X+\frac{(m+n+3)\Delta_{\mathbf{b}}}{\Delta_{\mathbf{a}}^2}$$

かつ

$$\mathrm{Disc}_X(F_2^+(m,n;X))=\frac{\Delta_{\mathbf{b}}^2(2mn+3m+3n+18)^2}{\Delta_{\mathbf{a}}^4},$$
$$\mathrm{Disc}_X(F_2^-(m,n;X))=\frac{\Delta_{\mathbf{b}}^2(2mn+3m+3n-9)^2}{\Delta_{\mathbf{a}}^4}$$

となることが分かる．ここで $F_2^-(m,n;X)=F_2^+(m,-n-3;X)$ に注意しておく．もし $m+n+3=0$ であれば，$X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ は M 上同じ最小分解体をもつ．これより $X^3-mX^2-(m+3)X-1$ と $X^3+(m+3)X^2+mX-1$ は M 上でチルンハウス同値である．もし $(2mn+3m+3n+18)(2mn+3m+3n-9)=0$ であれば，定理 4.2 (1) から，$X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ は M 上で同じ最小分解体をもつ．

定理 5.2. 条件

$$(2mn+3m+3n+18)(2mn+3m+3n-9)\neq 0$$

を満たす $m,n\in M$ に対して，2 つの多項式 $X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ の M 上の最小分解体が一致するためには，$F_2^+(m,n;X)F_2^-(m,n;X)$ が M 内に根を持つことが必要十分である．

例 5.3. $M=\mathbb{Q}$ とする．もし $(m,n)\in\{(-1,5),\,(-1,1259),\,(0,54),\,(5,1259)\}$ であれば $F_2^+(m,n;X)$ は $\mathbb{Q}$ 上 1 次因子 3 つに完全分解する．もし $(m,n)\in\{(-1,12),\,(0,3),\,(1,66),\,(2,2389),\,(3,54),\,(5,12),\,(12,1259)\}$ であれば $F_2^-(m,n;X)$ は $\mathbb{Q}$ 上 1 次因子 3 つに完全分解する．よって

$$L_{-1}=L_5=L_{12}=L_{1259},\quad L_0=L_3=L_{54},\quad L_1=L_{66},\quad L_2=L_{2389}$$

を得る．但し，$L_m=\mathrm{Spl}_{\mathbb{Q}}(X^3-mX^2-(m+3)X-1)$．我々は計算機を用いることによって，$-1\leq m<n\leq 100000$ の範囲の整数 m, n については，$F_2^+(m,n;X)F_2^-(m,n;X)$ が $\mathbb{Q}$ 内に一次因子を持つのは，上記の (m,n) に限られることを確認している．

もし $\mathrm{char}\,k\neq 2,3$ であれば，式 (25) を用いることによって，$F_2^+(m,n;X)$ と

$$g^+(m,n;X):=X^3+\frac{3(mn+6m-3n+9)}{2mn+3m+3n+18}X^2-\frac{3(mn-3m+6n+9)}{2mn+3m+3n+18}X-1$$

は M 上でチルンハウス同値であることが分かる．また，同様にして $F_2^-(m,n;X)$ と

$$g^-(m,n;X):=X^3+\frac{3(mn-3m-3n-18)}{2mn+3m+3n-9}X^2-\frac{3(mn+6m+6n+9)}{2mn+3m+3n-9}X-1$$

は M 上でチルンハウス同値であることが分かる．

今，$Z=(X-1)/(X+2)$ とすると，$X=-(2Z+1)/(Z-1)$ であり，

$$h^+(m,n;Z)=\frac{1}{3^3(m-n)}\,g^+\Big(m,n;\frac{-(2Z+1)}{Z-1}\Big)=Z^3-\frac{mn+3n+9}{m-n}Z^2-\frac{mn+3m+9}{m-n}Z-1,$$
$$h^-(m,n;Z)=\frac{-1}{3^3(m+n+3)}\,g^-\Big(m,n;\frac{-(2Z+1)}{Z-1}\Big)=Z^3+\frac{mn+3m+3n}{m+n+3}Z^2+\frac{mn-9}{m+n+3}Z-1$$

が成り立つ．また

$$\mathrm{Disc}_Z(h^+(m,n;Z))=\frac{\Delta_{\mathbf{a}}^2\Delta_{\mathbf{b}}^2}{(m-n)^4},\quad \mathrm{Disc}_Z(h^-(m,n;Z))=\frac{\Delta_{\mathbf{a}}^2\Delta_{\mathbf{b}}^2}{(m+n+3)^4}$$

を得る．

他方，char $k=3$ の場合には，小節 4.3 の結果を用いて，$F_2^+(m,n;X)$ と $h^+(m,n;Z)$，ならびに，$F_2^-(m,n;X)$ と $h^-(m,n;Z)$ がそれぞれ M 上でチルンハウス同値であることを直接に確認できる．よって Morton [Mor94], Chapman [Cha96] の結果の類似として，次の定理が得られる．

定理 5.4. 体 k の標数は 2 ではないと仮定する．また，$m,n\in M$ に対して

$$(m-n)(m+n+3)(2mn+3m+3n+18)(2mn+3m+3n-9)\neq 0$$

とする．このとき，2 つの多項式 $X^3-mX^2-(m+3)X-1$ と $X^3-nX^2-(n+3)X-1$ の M 上の最小分解体が一致するためには，次の条件を満たす $z\in M$ が存在することが必要十分である：

$$n=\frac{m(z^3-3z-1)-9z(z+1)}{mz(z+1)+z^3+3z^2-1}\ \text{または}\ n=-\frac{m(z^3+3z^2-1)+3(z^3-3z-1)}{mz(z+1)+z^3+3z^2-1}.$$

§ 6　幾つかの 6 次生成的多項式

まず char $k\neq 3$ とする．また H_1, H_2 を $\mathfrak{S}_3$ の部分群，$k(s,t)$ を k 上の 2 変数有理関数体とする．群 H_1 に対する，1 パラメータ s 付きの k-生成的多項式 $f_3(\mathbf{a};X)\in k(s)[X]$ と，群 H_2 に対する，1 パラメータ t 付きの k-生成的多項式 $f_3(\mathbf{b};X)\in k(t)[X]$ を用意する ($\mathbf{a}\in k(s)^3$, $\mathbf{b}\in k(t)^3$)．また，多項式 $g^{(H_1,H_2)}(s,t;X):=F_2(\mathbf{a},\mathbf{b};X)$ は重根を持たないと仮定する．このとき，定理 3.10 より $g^{(H_1,H_2)}(s,t;X)$ は $H_1\times H_2$ に対する 2 つのパラメータ s,t 付きの k-生成的多項式となる．ここで，1 パラメータの $\mathbb{Q}$-生成的多項式は群 $\{1\},C_2,C_3,\mathfrak{S}_3$ に対するものを除けば，存在しないことに注意しておく (cf. [BR97], [Le07], [CHKZ])．さて，$(H_1,H_2)\in\{(\mathfrak{S}_3,\mathfrak{S}_3),(\mathfrak{S}_3,C_3),(\mathfrak{S}_3,C_2),(\mathfrak{S}_3,\{1\}),(C_3,C_2)\}$ とする．このとき，$L_{\mathbf{a}}\cap L_{\mathbf{b}}=k(s,t)$ であり，定理 4.3 から，$g^{(H_1,H_2)}(s,t;X)$ は $k(s,t)$ 上で既約になる．したがって，このとき $H_1\times H_2$ は自然に $\mathfrak{S}_6$ の可移部分群と見なすことができる．

また，多項式 $g^{(H_1,H_2)}(s,t;X)$ と $k(s,t)$ 上同じ最小分解体を持つ多項式として $h^{(H_1,H_2)}(s,t;X):=\prod_{\overline{g}\in H\backslash G_{\mathbf{s},\mathbf{t}}}(X-(\alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3)^g)$ をとる事ができる．多項式 $h^{(H_1,H_2)}(s,t;X)$ は $k[s,t]$ 上で定義され，簡明な表示を持つのでここに付記しておく．

(1) $(H_1,H_2)=(\mathfrak{S}_3,\mathfrak{S}_3)$ の場合：$\mathbf{a}=(0,s,-s)$, $\mathbf{b}=(0,t,-t)$ とすると，$f_3(\mathbf{a};X)=X^3+sX+s$, $f_3(\mathbf{b};X)=X^3+tX+t$, $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=-729s^2t^2(4st+27s+27t)$ であり，

$$\begin{aligned}g^{(\mathfrak{S}_3,\mathfrak{S}_3)}(s,t;X)&:=\frac{1}{3^6}F_2(0,s,-s,0,t,-t;3X)\\&=X^6+\frac{2t}{s(4s+27)}X^4+\frac{t}{s^2(4s+27)}X^3+\frac{t^2}{s^2(4s+27)^2}X^2+\frac{t^2}{s^3(4s+27)^2}X+\frac{(s-t)t^2}{s^4(4s+27)^3},\end{aligned}$$

$$h^{(\mathfrak{S}_3,\mathfrak{S}_3)}(s,t;X):=X^6-6stX^4-27stX^3+9s^2t^2X^2+81s^2t^2X-s^2t^2(4st+27s+27t)$$

は $\mathfrak{S}_3\times\mathfrak{S}_3$ に対する k-生成的多項式である．

(2) $(H_1,H_2)=(\mathfrak{S}_3,C_3)$ の場合：$\mathbf{a}=(0,s,-s)$, $\mathbf{b}=(t,-t-3,1)$ とすれば，$f_3(\mathbf{a};X)=X^3+sX+s$, $f_3(\mathbf{b};X)=X^3-tX^2-(t+3)X-1$, $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=729s^2(t^2+3t+9)^2(t^2+3t+9+s)$ を得る．このとき，

$$\begin{aligned}g^{(\mathfrak{S}_3,C_3)}(s,t;X)&:=F_2(0,s,-s,t,-t-3,1;X)\\&=X^6-\frac{6(t^2+3t+9)}{s(4s+27)}X^4-\frac{(2t+3)(t^2+3t+9)}{s^2(4s+27)}X^3+\frac{9(t^2+3t+9)^2}{s^2(4s+27)^2}X^2\\&+\frac{3(2t+3)(t^2+3t+9)^2}{s^3(4s+27)^2}X+\frac{(t^2+3t+9)^2(4st^2+27t^2+12st+9s+81t+243)}{s^4(4s+27)^3},\end{aligned}$$

$$\begin{aligned}h^{(\mathfrak{S}_3,C_3)}(s,t;X):=&X^6+2s(t^2+3t+9)X^4+s(2t+3)(t^2+3t+9)X^3+s^2(t^2+3t+9)^2X^2\\&+s^2(2t+3)(t^2+3t+9)^2X+s^2(t^2+3t+9)^2(t^2+3t+9+s)\end{aligned}$$

は群 $\mathfrak{S}_3\times C_3\cong C_3\wr C_2\cong(C_3\times C_3)\rtimes C_2$ に対する k-生成的多項式である．

さらに特殊化 $(s,t)\mapsto(a,b)\in M^2$ に対して，もし $b^2+3b+9+a=0$ であれば X^3+aX+a と $X^3-bX^2-(b+3)X-1$ は M 上で同じ最小分解体を持つ．すなわち，

$$X^3-(b^2+3b+9)X-(b^2+3b+9)\quad\text{と}\quad X^3-bX^2-(b+3)X-1$$

は M 上でチルンハウス同値である．また，もし $4ab^2+27b^2+12ab+9a+81b+243=0$ であれば X^3+aX+a と $X^3-bX^2-(b+3)X-1$ は M 上で同じ最小分解体を持つ．よって

$$X^3-\frac{27(b^2+3b+9)}{(2b+3)^2}X-\frac{27(b^2+3b+9)}{(2b+3)^2}\quad\text{と}\quad X^3-bX^2-(b+3)X-1$$

は M 上でチルンハウス同値である．これは根のアフィン変換によって得られる．

(3) $(H_1,H_2)=(\mathfrak{S}_3,C_2)$ の場合：$\mathbf{a}=(0,s,-s)$, $\mathbf{b}=(0,-t,0)$ とすると，$f_3(\mathbf{a};X)=X^3+sX+s$, $f_3(\mathbf{b};X)=X(X^2-t)$, $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=729s^2t^3(4s+27)$ となる．このとき，

$$\begin{aligned}g^{(\mathfrak{S}_3,C_2)}(s,t;X)&:=\frac{1}{3^6}F_2(0,s,-s,0,-t,0;3X)\\&=X^6-\frac{2t}{s(4s+27)}X^4+\frac{t^2}{s^2(4s+27)^2}X^2+\frac{t^3}{s^4(4s+27)^3},\end{aligned}$$

$$h^{(\mathfrak{S}_3,C_2)}(s,t;X):=X^6+6stX^4+9s^2t^2X^2+s^2(4s+27)t^3$$

は $\mathfrak{S}_3\times C_2\cong D_6$ に対する k-生成的多項式である．但し D_6 は位数 12 の二面体群である．

(4) $(H_1,H_2)=(\mathfrak{S}_3,\{1\})$ の場合：更に，$\mathrm{char}\,k\neq2$ を仮定する．この場合，$\mathbf{a}=(0,s,-s)$, $\mathbf{b}=(0,-1,0)$ とすると，$f_3(\mathbf{a};X)=X^3+sX+s$, $f_3(\mathbf{b};X)=X(X+1)(X-1)$, $A_{\mathbf{a}}^3B_{\mathbf{b}}^2-27A_{\mathbf{b}}^3D_{\mathbf{a}}=729s^2(4s+27)$. したがって，$\mathfrak{S}_3$ に対する k-生成的多項式

$$\begin{aligned}g^{(\mathfrak{S}_3,\{1\})}(s;X)&:=\frac{1}{3^6}F_2(0,s,-s,0,-1,0;3X)\\&=X^6-\frac{2}{s(4s+27)}X^4+\frac{1}{s^2(4s+27)^2}X^2+\frac{1}{s^4(4s+27)^3},\end{aligned}$$

$$h^{(\mathfrak{S}_3,\{1\})}(s;X):=X^6+6sX^4+9s^2X^2+s^2(4s+27)$$

が得られる．特に，2 つの多項式 $f_3(\mathbf{a};X)=X^3+sX+s$ と $h^{(\mathfrak{S}_3,\{1\})}(s;X)$ は $k(s)$ 上同じ最小分解体を持つ．

(5) $(H_1, H_2) = (C_3, C_2)$ の場合：$\mathbf{a} = (s, -s-3, 1)$, $\mathbf{b} = (0, -t, 0)$ とすると，$f_3(\mathbf{a}; X) = X^3 - sX^2 - (s+3)X - 1$, $f_3(\mathbf{b}; X) = X(X^2 - t)$, $A_{\mathbf{a}}^3 B_{\mathbf{b}}^2 - 27A_{\mathbf{b}}^3 D_{\mathbf{a}} = -729t^3(s^2+3s+9)^2$ である．このとき，

$$\begin{aligned} g^{(C_3,C_2)}(s,t;X) &:= F_2(s,-s-3,1,0,-t,0;X) \\ &= X^6 - \frac{6t}{s^2+3s+9}X^4 + \frac{9t^2}{(s^2+3s+9)^2}X^2 - \frac{(2s+3)^2t^3}{(s^2+3s+9)^4}, \end{aligned}$$

$$h^{(C_3,C_2)}(s,t;X) := X^6 - 2(s^2+3s+9)tX^4 + (s^2+3s+9)^2t^2X^2 - (s^2+3s+9)^2t^3$$

は $C_3 \times C_2 \cong C_6$ に対する k-生成的多項式となる．

また char $k = 3$ の場合，小節 4.3 の結果から，多項式 $F_2(\mathbf{a}, \mathbf{b}; X)$ の代わりに $F_0(\mathbf{a}, \mathbf{b}; X)$ を用る必要がある．以下に各 (H_1, H_2) に対する $g^{(H_1,H_2)}(s,t;X) := F_0(\mathbf{a}, \mathbf{b}; X)$ の計算結果を記述しておく：

$$\begin{aligned} g^{(\mathfrak{S}_3,\mathfrak{S}_3)}(1/s,t;X) &= X^6 - tX^4 - tX^3 + t^2X^2 - t^2X - t^2(st-1), \\ g^{(\mathfrak{S}_3,C_3)}(1/s,t;X) &= X^6 + tX^5 + t(t+1)X^4 + (st^3 - t^2 + 1)X^3 \\ &\quad - t(st^3 - t + 1)X^2 - t(st^3+1)X + s^2t^6 + st^4 - st^3 + 1, \\ g^{(\mathfrak{S}_3,C_2)}(1/s,t;X) &= X^6 - tX^4 + t^2X^2 + st^3, \\ g^{(\mathfrak{S}_3,\{1\})}(1/s,t;X) &= X^6 - X^4 + X^2 + s, \\ g^{(C_3,C_2)}(1/s,t;X) &= X^6 + \frac{t^2}{s^4+s^2+1}X^2 + \frac{s^2t^3}{s^8+s^4+1}. \end{aligned}$$

参考文献

[Ber76] E. R. Berlekamp, *An analog to the discriminant over fields of characteristic two*, J. Algebra **38** (1976), 315–317.

[BJY86] A. A. Bruen, C. U. Jensen, N. Yui, *Polynomials with Frobenius groups of prime degree as Galois Groups II*, J. Number Theory **24** (1986), 305–359.

[BR97] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[Cha96] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), 283–291.

[CHKZ] H. Chu, S. Hu, M. Kang, J. Zhang, *Groups with essential dimension one*, preprint. arXiv:math/0611917v1 [math.AG].

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[HH05-1] K. Hashimoto, A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74**, 1519-1530 (2005).

[HH05-2] K. Hashimoto, A. Hoshi, *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, Tokyo J. Math. **28** 13-32 (2005).

[HM99] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications, Dev. Math., 2, Doredrecht: Kluwer Acad. Publ. 165–181, 1999.

[HM07] A. Hoshi, K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation*, Proc. Japan Acad., Series A **83** (2007), 21–26.

[HM] A. Hoshi, K. Miyake, *A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation*, preprint. arXiv:0710.0287v1 [math.NT] http://arxiv.org/abs/0710.0287

[HM-j] 星 明考，三宅 克哉，生成的多項式の部分体問題に対するチルンハウス変換を用いた幾何学的枠組みについて，早稲田大学教育学部 学術研究–数学編–第 56 号 (2008 年 2 月), 5–36.

[Hup67] B. Huppert, *Endliche Gruppen. I.*, Grundlehren der Mathematischen Wissenschaften 134, Springer-Verlag, Berlin-New York 1967.

[JLY02] C. Jensen, A. Ledet, N. Yui, *Generic polynomials, constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Cambridge, 2002.

[Kem96] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta Math. **90** (1996), 343–363.

[Kem01] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[KM00] G. Kemper, E. Mattig, *Generic polynomils with few parameters*, J. Symbolic Comput. **30** (2000), 843-857.

[Ki05] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), 427–447.

[Ki06] M. Kida, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 102–113, 2006.

[Ko04] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta math. **114** (2004), 265-279.

[Ko] T. Komatsu, *Generic sextic polynomial related to the subfield problem of a cubic polynomial*, preprint. http://www.math.kyushu-u.ac.jp/coe/report/pdf/2006-9.pdf

[Le07] A. Ledet, *On groups with essential dimension one*, J. Algebra, **311** (2007) 31–37.

[Miy99] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Algebraic number theory (Hapcheon/Saga, 1996). Adv. Stud. Contemp. Math. (Pusan) 1 (1999), 137–142.

[Miy03] K. Miyake, *Some families of Mordell curves associated to cubic fields*, J. Comput. Appl. Math. **160** (2003), 217–231.

[Miy04] K. Miyake, *An introduction to elliptic curves and their Diophantine geometry—Mordell curves*, Ann. Sci. Math. Québec **28** (2004), 165–178.

[Miy06] K. Miyake, *Cubic fields and Mordell curves*, Number theory, 175–183, Dev. Math., 15, Springer, New York, 2006.

[Mor94] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), 183–208.

[Sha74] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

Akinari HOSHI (hoshi@ruri.waseda.jp), Department of Mathematics, School of Education, Waseda University,1–6–1 Nishi-Waseda Shinjuku-ku, Tokyo, 169–8050, Japan.

Katsuya MIYAKE (miyakek@aoni.waseda.jp), Department of Mathematics, School of Fundamental Science and Engineering, Waseda University, 3–4–1 Ohkubo Shinjuku-ku, Tokyo, 169–8555, Japan.

A Brief Introduction to NZMATH

ICHIKI Shingo, OGURA Naoki, KOIZUMI Masahiro,
NISHIMOTO Keiichiro, TANAKA Satoru, MATSUI Tetsushi,
UCHIYAMA Shigenori, NAKAMULA Ken
Tokyo Metropolitan University

Abstract

NZMATH is a system for number theory which is being developed at Tokyo Metropolitan University. From the viewpoint of a NZMATH user, we show how you can use this system and what you can do with it. Moreover, we demonstrate how to install, execute commands and link NZMATH with other softwares.

1 Introduction

NZMATH[5] is a number theory oriented calculation system mainly developed by the Nakamula laboratory at Tokyo Metropolitan University. It is freely available and distributed under the BSD license at `http://tnt.math.metro-u.ac.jp/nzmath/`. The most distinctive feature of NZMATH is that it is written entirely using a scripting language called Python. Although NZMATH is at an early stage of development, it holds enormous potential.

This paper is organized as follows. In section 2, we will discuss NZMATH features and advantages against other similar systems. In section 3, we will show how to use NZMATH for beginners.

2 The Advantage of NZMATH

In this section, we will provide a detailed discussion on the advantages of NZMATH compared to other similar systems.

2.1 Open Source Software

Computational algebra systems, such as Maple[7], Mathematica[8], and Magma[9] are fare-paying systems. These non-free systems are not distributed with source codes. In this regard, users cannot modify such systems. It narrows these system's potentials for users not to take part in developing it. NZMATH, on the other hand, is an open-source software and the source code is openly available. Furthermore, NZMATH is distributed under the BSD license. BSD license claims as-is and redistribution or commercial use are permitted provided that these packages retain the copyright notice.

2.2 Speed of Development

We took over developing of SIMATH[6], which was developed under the leadership of Prof.Zimmer at Saarlandes University in Germany. However, it costs a lot of time and efforts to develop these system. Almost all systems including SIMATH are implemented in C or C++ for execution speed, but we have to take the time to work memory management, construction of an interactive interpreter, preparation for multiple precision package and so on. In this regard, we chose Python which is a modern programming language. Python provides automatic memory management, a sophisticated interpreter and many useful packages. We can concentrate on development of mathematical matters by using Python.

2.3 Bridging the Gap between Users and Developers

KANT/KASH[10] and PARI/GP[11] are similar systems to NZMATH. But these systems have different languages for users and developers. We think the gap between languages makes evolution of systems slow. NZMATH is being developed with using Python, we bridge this gap. Users are easy to understand Python grammar and read codes written by Python. And NZMATH which is one of Python libraries works on very wide platform including UNIX/Linux, Macintosh, Windows, and so forth. Users can modify the programs and feedback to developers. Developers can absorb their thinking. Then NZMATH will progress to more flexible user-friendly system.

2.4 Link with Other Softwares

NZMATH distributed as a Python library enables us to link other Python packages with it. For example, NZMATH can use with IPython[12] which is a comfortable interactive interpreter. And it can be linked with matplotlib[13] which is a powerful graphic software. There are many libraries and packages for softwares implemented in Python. Many of these packages are freely available. Users can use NZMATH with these packages and create an unthinkable powerful system.

3 How to Use

In this section, we will illustrate installation procedures and sample sessions of NZMATH.

3.1 Installation

There are three steps for installation of NZMATH.

First, check that Python is installed in the computer. Python 2.3 or a higher version is needed for NZMATH. If you do not have a copy of Python, please install it first. Python is available from `http://www.python.org/`.

Second, download NZMATH package and expand it. It is distributed at official web site:

`http://tnt.math.metro-u.ac.jp/nzmath/download`

or at sourceforge.net:

`http://sourceforge.net/project/showfiles.php?group_id=171032`

The latest version is 0.7.0. The package can be easily extracted, depending on the operating system. For systems with recent GNU tar, type a single command below:

```
% tar xf NZMATH-0.7.0.tar.gz
```

where, `%` is a command line prompt. Or with standard tar, type a following command:

```
% gzip -cd NZMATH-0.7.0.tar.gz | tar xf -
```

Then, a subdirectory named NZMATH-0.7.0 is created.

Finally, install NZMATH to the standard python path. Usually, this translates to writing files somewhere under `/usr/lib` or `/usr/local/lib`, and thus appropriate write permission is required. Typically, type commands below:

```
% cd NZMATH-0.7.0
% su
# python setup.py install
```

We also distribute the installation packages for specific platforms. Especially, we started distributing installer for Windows in 2007. This installer enables us to install NZMATH with only three clicks.

Figure 1: Windows installer for NZMATH 0.7.0

3.2 Sample Session

NZMATH is a Python library. So, it can be used in the same way as standard python packages. We will demonstrate how to use NZMATH and briefly discuss about some modules.

Start the Python interpreter:

```
% python
Python 2.3.4 (#1, Dec 11 2007, 05:28:55)
[GCC 3.4.6 20060404 (Red Hat 3.4.6-9)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Here, '>>>' is a Python prompt. Please type

```
>>> from nzmath import *
>>>
```

With this command, the whole NZMATH modules are imported.

```
>>> gcd.gcd(350, 525)
175
>>>
```

The `gcd` is a module for the greatest common divisors of integers. The example above means that 175 is the greatest common divisor of 350 and 525.

```
>>> factor.methods.factor(175)
[(5, 2), (7, 1)]
>>>
```

The `factor` module has functions for prime factorization. The sample command above shows that 175 is factorized $5^2 \times 7$ into prime factors.

```
>>> prime.nextPrime(175)
179
>>>
```

The `prime` module provides functions related with primality. For example, the command illustrated above gives us 179 which is the smallest prime larger than 175.

```
>>> arith1.legendre(3, 7)
-1
>>>
```

The `arith1` is module for miscellaneous arithmetic functions. One command in this module is `legendre` for legendre symbol. From the example above, $(\frac{3}{7}) = -1$. So 3 is quadratic non-residue modulo 7.

There is a trivial example of Python programming with NZMATH below.

```
>>> for i in range(10):
        [combinatorial.binomial(i, j) for j in range(i+1)]
...
...
[1]
[1, 1]
[1, 2L, 1]
[1, 3L, 3L, 1]
[1, 4L, 6L, 4L, 1]
[1, 5L, 10L, 10L, 5L, 1]
[1, 6L, 15L, 20L, 15L, 6L, 1]
[1, 7L, 21L, 35L, 35L, 21L, 7L, 1]
[1, 8L, 28L, 56L, 70L, 56L, 28L, 8L, 1]
[1, 9L, 36L, 84L, 126L, 126L, 84L, 36L, 9L, 1]
>>>
```

The `combinatorial` module includes combinatorial theoretical functions. This program outputs binomial coefficient ${}_n\mathrm{C}_m$ for $n = 0, \ldots, 9$. The `range` is one of a Python function. For example, we can express [0, 1, 2, 3, 4, 5, 6, 7, 8, 9] by the `range(10)`. The "`L`" denotes long integer type.

NZMATH also has a module for elliptic curves called `elliptic`.

```
>>> E = elliptic.ECoverFp([1,2], 37)
>>>
```

We define the elliptic curve $E: \ y^2 = x^3 + x + 2$ over finite field F_{37}.

```
>>> P, Q = E.point(), E.point()
>>> print P, Q
[1, 35] [27, 19]
>>>
```

The `point` function returns a random point on elliptic curve. Now the point $P = (1, 35)$ and $Q = (27, 19)$ are taken from $E(F_{37})$.

```
>>> E.add(P, Q)
[5, 13]
>>>
```

This means that $P + Q = (5, 13)$ in $E(F_{37})$.

```
>>> E.mul(3, P)
[1, 2]
>>>
```

This shows that $3P = (1, 2)$ in $E(F_{37})$.

NZMATH may be used with other softwares. We show an example for using NZMATH with matplotlib which is one of powerful packages drawing graphs. It draws k-scalar($k <$ order of point) multiplication points for some point in curve $y^2 = x^3 + x + 2$ over F_{37}. We put the source code for it in Appendix.

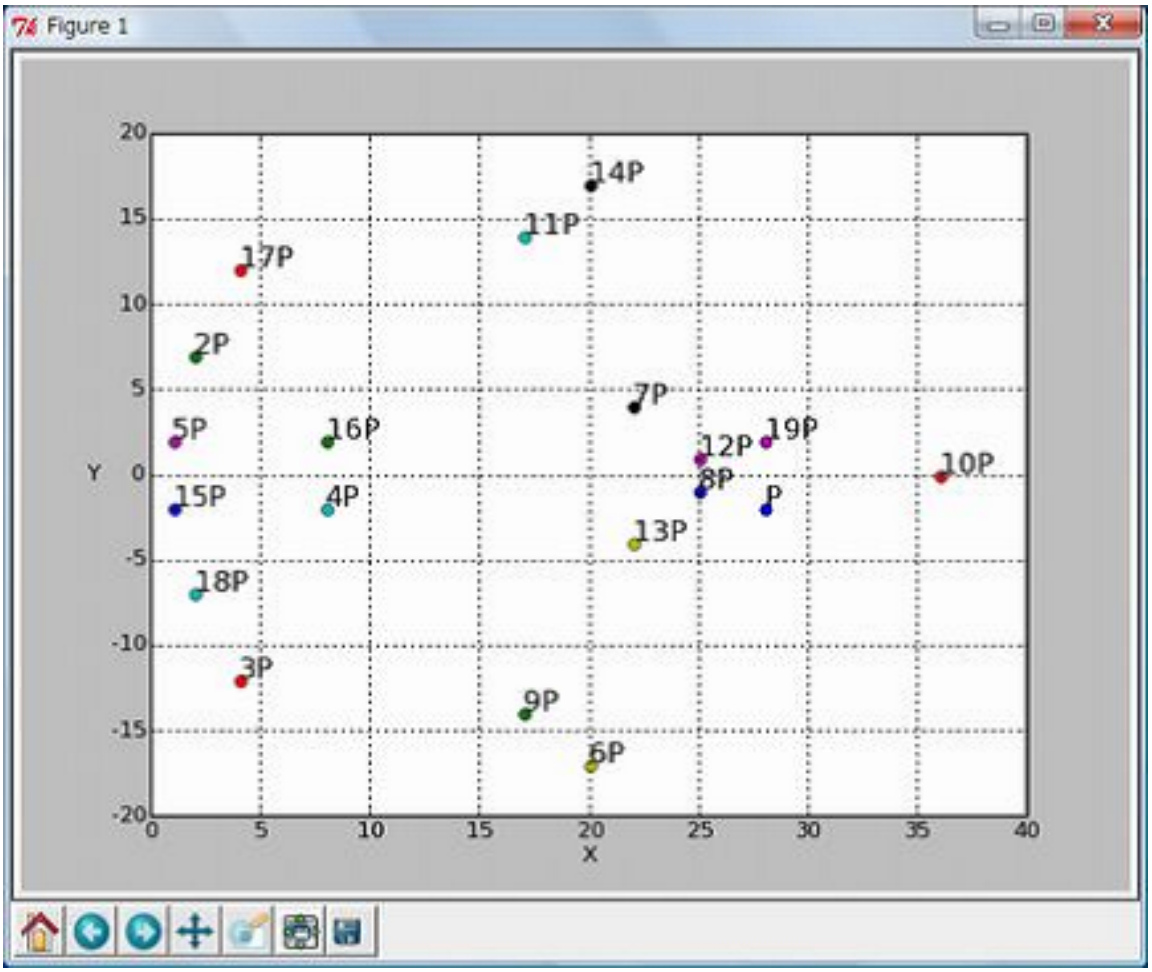

Figure 2: k-scalar multiplication in $y^2 = x^3 + x + 2$ over F_{37}

3.3 More Information

NZMATH has more than 25 modules. It has modules related with elementary number theory, combinatorial theory, solving equations, primality, factorization, multiplicative number theoretic functions, matrix, vector, polynomial, rational field, finite field, elliptic curve, and so on. NZMATH manual for users is at:

`http://tnt.math.metro-u.ac.jp/nzmath/manual/`

If you are interested in NZMATH, please visit the official website below to get more information about it.

`http://tnt.math.metro-u.ac.jp/nzmath/`

Note that NZMATH can be used even if user do not have experience writing programs in Python.

We have a mailing list called nzmath-user for NZMATH users. To join this mailing list, send a mail to

`nzmath-user-request@tnt.math.metro-u.ac.jp`

only with a line “subscribe” in the message. Then the address from which you send the mail will be added on the nzmath-user mailing list.

4 Conclusion

We have been developing NZMATH for four years. NZMATH is still at an early stage, but possibilities of NZMATH are pretty much unlimited. As the number of NZMATH users and developers increase, NZMATH becomes better. We will continue promoting NZMATH based on our philosophy and creating new NZMATH features.

References

[1] Tanaka S., Nishimoto K., MATSUI T., Uchiyama S., and NAKAMULA K. "Status and issues on development NZMATH." *AC2007 presentation* (2007)

[2] Matsui T. "NZMATH: Past and Future of the Development." *AC2005 proceedings*, `ftp://tnt.math.metro-u.ac.jp/pub/ac05/Matsui/nzmath.pdf` (2005)

[3] Matsui T. "Development of computational number theory system by a scripting language."(Japanese) *Computer Algebra . Design of Algorithms, Implementations and Applications*, RIMS Kokyuroku, No.1395 pp.144-149, Kyoto University (2004)

[4] Nakamula K. and Matsui T. "Developing a system for number theory by script language — Announcement of the release of NZMATH 0.1.1" *Algorithms and Number Theory*, Dagstuhl, `http://tnt.math.metro-u.ac.jp/~nakamula/talk/dag2004-s.pdf` (2004)

[5] NZMATH, `http://tnt.math.metro-u.ac.jp/nzmath/`

[6] SIMATH, `http://tnt.math.metro-u.ac.jp/simath/`

[7] Maple, `http://www.maplesoft.com/`

[8] Mathematica, `http://www.wolfram.com/products/mathematica/`

[9] Magma, `http://magma.maths.usyd.edu.au/magma/`

[10] KANT/KASH, `http://www.math.tu-berlin.de/~kant/kash.html`

[11] PARI/GP, `http://pari.math.u-bordeaux.fr/`

[12] IPython, `http://ipython.scipy.org/`

[13] matplotlib, `http://matplotlib.sourceforge.net/`

Appendix A Demo Code

The Python source code with nzmath and matplotlib for the demonstration which draws k-scalar multiplication points for some point in elliptic curve $y^2 = x^3 + x + 2$ over F_{37} is here.

```
import nzmath.elliptic
from pylab import *

p = 37
A = 1 # A>0
B = 2 # B>0

E = nzmath.elliptic.ECoverFp([A, B], p)
while True:
    P = E.point()
    if E.pointorder(P) > E.order()//3: # point whose order is large
        break

x_y = []
for i in range(E.pointorder(P)):
    pnt = E.mul(i, P)
    if len(pnt) > 1: # not point at infinity
        if pnt[1] > p//2:
            ele = [ [pnt[0]], [pnt[1] - p] ]
        else:
            ele = [ [pnt[0]], [pnt[1]] ]
        if i == 1:
            x_y.append(ele + ["P"])
        else:
            x_y.append(ele + [str(i) + "P"])

figure()
grid(True)
axis([-p//2, p//2 + 1, 0, p])
xlabel("X")
ylabel("Y", rotation=0)

for x, y, lab in x_y:
    plot(x, y, 'o')
    text(x[0], y[0], lab, size=15, weight='bold')
show()
```

SOME CONCEPTS AND METHODS TO INVESTIGATE PROBLEMS OF WARING TYPE

R. MORIKAWA

1. Introduction

We fix $k \in N$ and take m natural numbers $(a_1, \ldots, a_m) = A$ whose GCD $= 1$. We put

$$V(A) = \{ \sum_{i=1}^{m} a_i x_i^k \mid x_i \in N \ (1 \leq i \leq m)\} \quad \text{and} \quad W(A) = N \setminus V(A). \tag{1}$$

Our main concern is the structure of $W(A)$. We call this by a general name "$W(k,m)$-Problem". $\| W \|$ denotes Max W. Taking various (k,m), we obtain the following problems.

(a) F-Problem ($k = 1, m = 3, 4, , ,$; Frobenius)

(b) RDS-Problem ($k = 2, m = 3$; Ramanujan, Duke, Schulze-Pillot)

(c) W(3)-Problem ($k = 3, m = 4$)

In § 2, we explain three unified devices to treat general W-Problems, namely "N-frame", "Ramanujan Sieve" and "wirklich method".

In § 3, we restate the known results for $W(1,3)$-Problem so as to fit the general standpoint. In that Theorem 3 is a new result, which gives a simple method to determine W. A precise proof of it will be given. In § 4, we try to extend these result to $W(1,4)$-Problem.

§ 5 discusses RDS-Problem. And § 6 contains (1) comments for various $W(k,m)$-Problems and (2) some applications of "Cell-Principle","Use of Trees" and "Trunk-Star Principle" for various N-Problems.

2. N-frame, R-Sieve, wirklich method

We first seek a unified standpoint to treat these various W-Problems.

(A) N-frame : In (1), we let x_i's run through N. Usually W-Problems are considered in $\bar{N}$-frame. The reasons are :

(a) As the four square Theorem of Lagrange, "All property" usually fails in N-frame.

(b) If we use generating function e.g. Modular functions or zeta-functions, their summension domain must be modules.

But we think "N-frame" is essential to investigate purely arithmetic properties of $W(k,m)$. The reason is that " The main part of the theory are interplays of a_i's of A. And their interplays are broken in $\bar{N}$-frame."

(B) Ramanujan Sieve : Ramanujan used in [12] a simple, elementary but ingenious argument. Gradually its deep meaning becomes clear. Thus we call it after him.

(R-Sieve) Let $A = (a_1, \ldots, a_m)$. We take some a_i from A, say $a_1 = a$. We make $V(\breve{a}) = V(a_2, \ldots, a_m)$. For $n \in N$, we apply the following sieve.

Date: March 10, 2008.

Let x run $1 \leq x \leq [(n/a)^{1/k}]$. Putting $n(x) = n - ax^k$, judge whether (a) $n(x) \in V(\check{a})$ or (b) $n(x) \notin V(\check{a})$. We call this process R-Scan. In case (a), we say x hits the Scan. If n has no-hits, $n \in W$.

(1) For $n \in N$, we put $H(n) = \{x | n(x) \in V(\check{a})\}$. The nature of this $H(n)$ is important.

(2) By taking various a_i as a, we obtain usually m different sieves. The relations of these sieves are subtle and important.

(C) wirklich method : We use the terminology "wirklich" recalling Kummer's Geist.

(wirklich method) For W, we choose a suitable subset $\partial W \subset V$. And we clarify the structure of W by scrutinizing the representations of this ∂W in V.

We explain the idea by taking F-Problem. Let $A = (a_1, \ldots, a_m)$. We take $a_1 = a$ and operate $R(ax)$-sieve.

Fact 1. For r with $1 \leq r \leq a$, we put $N(r) = \{r + ta \mid t \in \bar{N}\}$. And apply $R(ax)$-scan taking n from $N(r)$ as $r, r + a, r + 2a, \ldots$. We put $h(r)$ the first hit member of $N(r)$.

Fact 2. Here $h(r) - a$ is contained in $V(\check{a})$. For $\boldsymbol{y} = (y_2, \ldots y_m)$, we put $J(\boldsymbol{y}) = a_2y_2 + \cdots + a_my_m$. We take $\boldsymbol{b}(r) \in N^{m-1}$ which satifies $h(r) - a = J(\boldsymbol{b}(r))$. Let $B = \{\boldsymbol{b}(r) \mid 1 \leq r \leq a\}$. Here W is determined by B. Thus in this case ∂W is $\{h(r)\}$.

Fact 3. For $m = 3, 4$ this B has a beautiful structure. This will be explained in § 3, 4. For other W-Problems, suitable definition of ∂W is yet not clear. But we believe the effectiveness of the concept.

3. F-Problems (General, $m = 3$)

3-1. We fix $k = 1$ and take $(a_1, \ldots, a_m) = A$ whose GCD $= 1$. We use $W(A), V(A)$ introduced in § 1. We denote $\| W \|$ by $F(A)$ and call it Frobenius number of A. Let $A(\check{a}_i) = (a_1 \ldots, a_{i-1}, a_{i+1} \ldots, a_m)$ and $V(\check{a}_i) = V(A(\check{a}_i))$. We start with two useful Lemmas which are given by Johnson [7]. (Propositions given in this § are known ones except Theorem 3. Thus we ommit Proofs. A precise proof of Theorem 3 will be given.)

Lemma 1 ([7] Theorem 1). $F(A)(= F)$ is contained in $\bigcap_{i=1}^{m} V(\check{a}_i)$.

Lemma 2 ([7] Theorem 2). Let d be GCD of $A(\check{a}_1)$. Then we have $F(A) = dF(a_1, \tilde{a}_2, \ldots, \tilde{a}_m)$ where $a_j = d\tilde{a}_j$ $(2 \leq j \leq m)$.

Lemma 3. If a_i is in $V(\check{a}_i)$, $F(A) = a_i + F(A(\check{a}_i))$.

From these three lemmas, we may impose on A the following condition (♯):

(♯) For all $1 \leq i \leq m$, GCD of $A(\check{a}_i) = 1$, and $a_i \notin V(\check{a}_i)$.

Hereafter, we assume (♯) and $R(ax)$-sieve is operated on N with $a = a_1$. Let $B = \{\boldsymbol{b}(r) | 1 \leq r \leq a\}$ and $J(\boldsymbol{y})$ as defined in § 2.

Lemma 4 (Completeness Criterion). B satisfies the following two properties.

(1) $B = \{\boldsymbol{b}(r)\}$ makes a complete residue system modulo a.

(2) Let $\boldsymbol{b} \in B$. For all $\boldsymbol{c} \in N^{m-1}$ with $J(\boldsymbol{b}) \equiv J(\boldsymbol{c}) \pmod{a}$, the inequality $J(\boldsymbol{b}) \leq J(\boldsymbol{c})$ holds.

As noted in § 2, F-Problem is reduced to find B which satisfies "Completeness Criterion".

3-2. We study the case $m = 3$. The discussion of this § depends on [1]. Take a, b, c with (♯). Let $E = \{(x, y, z) \in Z^3 \mid ax + by + cz = 0\}$. We take from E three vectors $\boldsymbol{a} = (-a_1, a_2, a_3)$, $\boldsymbol{b} = (b_1, -b_2, b_3)$ and $\boldsymbol{c} = (c_1, c_2, -c_3)$, which satisfy the following conditions.

(A) $a_i, b_j, c_k (1 \leq i, j, k \leq 3) \in N$.

(B) a_1, b_2, c_3 are the least positive under (A).

Lemma 5 ([1] Lemma 4). Three vectors $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ are determined uniquely and satisfy

(1) $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} = \boldsymbol{0}$.

(2) Any two of them makes a base of E.

Lemma 6. Let $J(y, z) = by + cz$. Make U_1, U_2 for which

$U_1 = \{(y, z) | \ 1 \leq y \leq b_2, 1 \leq z \leq a_3\}$ and $U_2 = \{(y, z) | \ 1 \leq y \leq a_2, 1 \leq z \leq c_3\}$. Then

(1) $J(U_1 \cup U_2)$ makes a complete residue system modulo a,

(2) For any $\boldsymbol{b} \in U_1 \cup U_2$ and $\boldsymbol{c} \in N^3$ for which $J(\boldsymbol{b}) \equiv J(\boldsymbol{c}) \pmod{a}$, the inequality $J(\boldsymbol{b}) \leq J(\boldsymbol{c})$ holds.

Lemma 6 means that $U_1 \cup U_2$ satifies completeness criterion. Using (1) of Lemma 5, we have

Theorem 1. For (a, b, c) with (♯), $F(a, b, c) = \mathrm{Max}(J(b_2, c_3 - b_3), J(b_2 - c_2, c_3))$.

3-3. Since $|B| = a$, we have $a = b_2c_3 - b_3c_2$. By symmetry and (1) of Lemma 5, we have

Lemma 7. $a = b_2c_3 - b_3c_2$, $b = b_1c_3 + c_1b_3$, $c = b_1c_2 + c_1b_2$.

Combining Theorem 1 and Lemma 7 we have

Theorem 2. $F = \mathrm{Max}(F_1, F_2)$ where $F_1 = b_1b_2c_3 + b_1c_2c_3 + c_1b_2c_3 - b_1c_2b_3$, $F_2 = b_1b_2c_3 + c_1b_2b_3 + c_1b_2c_3 - c_1c_2b_3$.

3-4. Now to solve W(1,3)-problem completely, we need some algorithm to obtain $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ from a, b, c. Here we give a simple method to get them.

Step 1. Take $a \in N$ and $t \in N$ for which $2 \leq t \leq a - 2$. We put $H(t) = \{(b, c) \in N^2 \mid b \equiv ct \pmod{a}\}$. And define a map with $\varphi(b, c) = b/c$. In considering W(1,3)-Problem for (a, b, c) with (♯), we fix $(a,\ t)$ and treat (b, c)'s in $H(t)$ simultaneously.

To determine $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$, it is sufficent to determine four members b_2, b_3, c_2, c_3.

Step 2. For $[u_0, \ldots, u_s]$, we put $[\emptyset] = 1$, and $[u_0] = u_0$. For $s \geq 1$, we define $[u_0, \ldots, u_s] = u_s[u_0, \ldots, u_{s-1}] + [u_0, \ldots, u_{s-2}]$.

Let $(a,\ t)$ be as in Step 1. We take a continued fraction of a/t so that

$a = [v_0, \ldots, v_{2s}]$, and $t = [v_1, \ldots, v_{2s}]$ with even $2s$.

Step 3. For a generally given $[k_0, \ldots, k_{2s}]$, we make a sequence $\{h_j\}$ of $K + 1$-terms where $K = \sum k_{odd}$. We put $K_q = \sum_{i=1}^{q} k_{2i-1}$.

(Rule) : (1) $h_j = l + jk_0$ for $0 \leq j \leq K_1$.

(2) For j with $K_q + 1 \leq j \leq K_{q+1}$, we put $j = K_q + r.$ and $h_j = [k_0, \ldots, k_{2q},\ r]$.

Step 4. Retering to a/t, we make sequence $\{f_j\}$ of $V + 1$ terms where $V = \sum v_{odd}$ applying the rule for $[v_0, \ldots, v_{2s}]$. Note that $f_V = \tilde{t}$ where $\tilde{t}t \equiv 1 \pmod{a}$.

Next taking $[v_{2s}, v_{2s-1}, \dots, v_0]$, we make $\{g_j\}$ with $V+1$-terms. And combining these two sequences, we make Chain of pairs $(g_j,\ f_{V-j})$.

Step 5. We put $\beta_j = g_j/f_{V-j}$. Then (β_j) is an increasing sequence, and they divide the interval $[1/\tilde{t},\ t]$.

Theorem 3. Take (a, b, c) with $(\sharp)$ and $(b, c) \in H(t)$. We put $I_j = (\beta_j, \beta_{j+1})$ $(0 \le j \le V-1)$. Then $b/c \in\ I_j$ for unique j. And we have $b_2 = f_{V-j}, b_3 = g_j, c_2 = f_{V-j-1}, c_3 = g_{j+1}$.

For a proof of Theorem 3, we need the following two Lemmas.

Let $[\boldsymbol{u}] = [u_0, \dots, u_s]$. We denote $[-\boldsymbol{u}] = [u_1, \dots, u_s]$, $[\boldsymbol{u}-] = [u_0, \dots, u_{s-1}]$ and $[-\boldsymbol{u}-] = [u_1, \dots, u_{s-1}]$ $(s \ge 1)$.

Lemma 8. Let $[\boldsymbol{u}] = [u_0, \dots, u_s]$ and $[\boldsymbol{v}] = [v_0, \dots, v_t]$. Then
(1) $[\boldsymbol{uv}] = [\boldsymbol{u}][\boldsymbol{v}] + [\boldsymbol{u}-][-\boldsymbol{v}]$,
(2) For $s \ge 1$, $[-\boldsymbol{u}][\boldsymbol{u}-] - [\boldsymbol{u}][-\boldsymbol{u}-] = (-1)^s$.
(3) $[\boldsymbol{u}] = [u_s, u_{s-1}, \dots, u_0]$.

Proof. (1) follows by induction on t. For (2), it is trivial for $s = 1$. For $s \ge 2$, we note the relation $[-\boldsymbol{u}][\boldsymbol{u}-] - [\boldsymbol{u}][-\boldsymbol{u}-] = [\boldsymbol{w}][-\boldsymbol{w}-] - [-\boldsymbol{w}][\boldsymbol{w}-]$ where $[\boldsymbol{w}] = [u_0, \dots, u_{s-1}]$. Thus the induction on s holds.
(3) is a well known fact.

Lemma 9. $f_j,\ g_j (0 \le j \le V-1)$ satisfy the following three relations.
(1) $g_{j+1}f_{V-j} - g_j f_{V-j-1} = a$ for $0 \le j \le V-1$.
(2) Let j be $V_q + 1 \le j \le V_{q+1}$. Then we have $g_j[v_0, \dots, v_{2q}] + f_{V-j}[v_{2q+2}, \dots, v_{2s}] = a$.
(3) $f_{V-j}t \equiv g_j \pmod{a}$.

Proof. (Step 1) For $V-j$, we take q for which $V_q + 1 \le V - j \le V_{q+1}$. We put $V - j = V_q + r$. Then (A) $f_{V-j} = [v_0, \dots, v_{2q}, r]$. (B) $f_{V-j-1} = [v_0, \dots, v_{2q-3}]$ for $r = 1$, (C) $f_{V-j-1} = [v_0, \dots, v_{2q}, r-1]$ for $2 \le r \le v_{2q+1}$.
Similarly (D) $g_j = [v_{2q+1} - r, v_{2q+2}, \dots, v_{2s}]$ for $1 \le r \le v_{2q+1} - 1$, (E) $g_j = [v_{2q+3}, \dots, v_{2s}]$ for $r = v_{2q+1}$. (F) $g_{j+1} = [v_{2q+1} - r + 1, v_{2q+2}, \dots, v_{2s}]$.

(Step2) In the proof we use the following Notations: $\sigma([\boldsymbol{u}]|[\boldsymbol{v}]) = [\boldsymbol{u}][\boldsymbol{v}] - [\boldsymbol{u}-][-\boldsymbol{v}]$. For $a = [v_0, \dots, v_{2s}]$, $\sigma_1(k|k+1) = \sigma([v_0, \dots, v_k]|[v_{k+1}, \dots, v_{2s}])$. For $t = [v_1, \dots, v_{2s}]$, $\sigma_2(k|k+1) = \sigma([v_1, \dots, v_k]|[v_{k+1} \dots v_{2s}])$.

(Step 3) For (1) and $2 \le r \le v_{2q+1} - 1$, taking (A), (C), (D), (F), we obtain easily the relation $g_{j+1}f_{V-j} - g_j f_{V-j-1} = \sigma_1(2q+1|2q+2)$. For other three cases, we obtain the same $\sigma_1(2q+1|2q+2)$.

(Step 4) For (2), taking g_j as (D) or (E), we obtain the same relation $g_j[v_0, \dots, v_{2q}] + f_{V-j}[v_{2q+2}, \dots, v_{2s}] = \sigma_1(2q+1|2q+2)$.

(Step 5) Proof of (3) is slightly complicated. We introduce $i([\boldsymbol{u}])$ which means the relation (2) of Lemma 8.

Let $1 \le r \le a_{2q+1} - 1$. Taking (A) and (D), we obtain $f_{V-j}t - g_j = r([v_0, \dots, v_{2q}]t + [v_{2q+2}, \dots, v_{2s}]) + ([v_0, \dots, v_{2q-1}]t - [v_{2q+1}, \dots, v_{2s}])$. Here we show the following two relations;
(a) $[v_0, \dots, v_{2q}]t - [v_1, \dots, v_{2q}]a + [v_{2q+2}, \dots, v_{2s}] = 0$,
(b) $[v_0, \dots, v_{2q-1}]t - [v_1, \dots, v_{2q-1}]a - [v_{2q+1} \dots, v_{2s}] = 0$.
For (a), we put $a = \sigma_1(2q+1|2q+2)$ and $t = \sigma_2(2q+1|2q+2)$, then we have $i([v_0, \dots, v_{2q+1}])$

and get (a). For (b), we use $a = \sigma_1(2q|2q+1)$ and $t = \sigma_2(2q|2q+1)$, and $i([v_0, \ldots, v_{2q}])$. In case $r = v_{2q+1}$, we use $a = \sigma_1(2q+2|2q+3)$, $t = \sigma_2(2q+2|2q+3)$ and $i([v_0, \ldots, v_{2q+2}])$.

By Lemma 4.1 of [2] (or Lemma 7 of [10]), we see Lemma 9 ascertains Therem 3.

Example 1. We take $(a, b, c) = (15667, 18083, 25269)$. Then $t = 7434$ and $\tilde{t} = 3804$. We have $a = [2, 9, 3, 3, 2, 8, 4]$, and $V = 20$. Now our chain is (1, 3804), (5, 3353), (9, 2862), (13, 2451), (17, 2000), (21, 1549), (25, 1098), (29, 647), (33, 196), (103, 137), (173, 78), (243, 19), (1042, 17), (1841, 15), (2640, 13), (3439, 11), (4238, 9), (5037, 7), (5836, 5), (6635, 3), (7434, 1).

Thus by the inequality $33/196 < 18083/25269 < 103/137$, we have $b_2 = 196, b_3 = 33, c_2 = 137, c_3 = 103$. We get $b_1 = 173, c_1 = 8$.

4. F-Problem with $m = 4$

4-1. We try to find a similar Theory for $m = 4$ with $W(1, 3)$-Problem.

(Definition of $\pi(B, C)$-Plane) We fix a and take B, C for which $2 \le B, C \le a - 2$. We put

$$H = H(B, C) = \{(b, c, d) \mid b \equiv Bd \pmod a,\ c \equiv Cd \pmod a,\ d \in N\}. \tag{2}$$

We take Y-Z plane π, and let $\varphi : H \to \pi$ be defined by $\varphi(b, c, d) = (b/d, c/d)$. We fix a and consider $(b, c, d) \in H(B, C)$. Then (a, b, c, d) with ($\sharp$) make a polygon $D(B, C)$ in π-plane.

To seek the direction of the theory, we scrutinize a Numerical Example.

Step 1. Let a =907, and $(B, C) = (683, 629)$.

Proposition 1.The vertices of $D(B, C)$ are as follows. (Arranged in positive direction. And we denote $(b/d, c/d)$ as (b, c, d).)
(1, 641, 660), (2, 375, 413), (3, 109,166), (10, 61, 251), (17, 13, 336), (75, 4, 522), (283, 3, 854), (491, 2, 1168), (699, 1, 584), (491, 2, 261), (774, 5, 199), (1057, 8, 137), (1340, 11, 75), (76, 14, 13), (235, 7, 3), (459, 351, 2), (683, 629, 1), (459, 1258, 2), (235, 980, 3), (11, 702, 4), (7, 859, 85), (3, 1016, 166), (2, 1282, 413).

Proof. The edges of $D(B, C)$ consist of lines $uY + vZ + w = 0$ with $(u, v, w) \in N^3$ for which

$683u + 629v + w \equiv 0 \pmod{907}$ and some of $u, v, w = 1$.

Step 2. We take two subsets of D.

(I) C_1: Triangle whose vertices are (39, 510, 344), (46, 462, 429), (43, 353, 263). The Edges are $33Y - 7Z + 4 = 0$, $14Y - 5Z - 9 = 0$, $66Y - Z - 6 = 0$.

(Ⅱ) C_2: Quadrilateral whose vertices are (46, 462, 429), (43, 353, 263), (53, 414, 514), (50,305, 348). The Edges are $33Y - 7Z + 4 = 0$, $66Y - z - 6 = 0$, $47Y - 2Z - 5 = 0$, $14Y - 8Z + 5 = 0$.

Step 3. We denote $U = U(s, t, v) = \{(y, z, w) \mid 1 \le y \le s, 1 \le z \le t, 1 \le w \le u\}$. We call U a box, and (s, t, u) End vertex of U.

(I) For C_1,we make Boxes whose End vertices are (5, 2, 9), (24, 1, 8), (66, 1, 3), (19, 5, 3), (19, 4, 4), (19, 3, 5) (19, 2, 8), (52, 1, 6), (43, 1, 7), (19, 7, 2), (10, 7, 3). We put B_1 the union of these 11 Boxes.

(Ⅱ) For C_2, we make Boxes whose End vertices are (5, 2, 9), (24, 1, 8), (66, 1, 3), (19, 5, 3), (19, 4, 4), (19, 3, 5), (19, 2, 8), (52, 1, 4), (33, 1, 7), (19, 8, 2) (10, 8, 3). We put B_2 the union of these 11 Boxes.

Proposition 2. For $i = 1, 2$, B_i satisfies Completeness Criterion for $W(907, b, c, d)$ where $(b, c, d) \in H(683, 629)$ and $\varphi(b, c, d) \in C_i$.

Let $J(\boldsymbol{y})$ be as in § 2. Each B_i satisfies the following two coditions.

(1) $J(B_i)$ makes a complete residue set modulo 907.

(2) For each $\boldsymbol{b} \in B_i$, and $\boldsymbol{c} \in N^3$ which satisfies $J(\boldsymbol{b}) \equiv J(\boldsymbol{c}) \pmod{907}$, the inequality $J(\boldsymbol{b}) \leq J(\boldsymbol{c})$ holds.

Proof. We remark Three facts. (a) For the congruence relations, we may consider $660\tilde{d}J(B_i)$ where $d\tilde{d} \equiv 1 \pmod{907}$. Namely we may consider $\tilde{J} = y + 641z + 660w$.

(b) Since the second element of Boxes are small, we consider B_i by cutting $z = k$ with $1 \leq k \leq 8$. Now it is easy to ascertain (1).

(c) By the linearity of J and the covexity of B, it is sufficient to ascertain the second condition (2) for 11 End vertices. And taking $\boldsymbol{b} = (b_2, b_3, b_4)$ it is easy to determine the set of $\boldsymbol{c} = (c_2, c_3, c_4) \in N^3$ which satisfy

$J(\boldsymbol{b}) \equiv J(\boldsymbol{c}) \pmod{907}$, and $b_i > c_i$ for some $1 \leq i \leq 3$.

For example in (Ⅱ), $J(19, 2, 8) \equiv J(85, 1, 2) \pmod{907}$. And the Edge $66Y - Z - 6 = 0$ works to judge that (19, 2, 8) is an End vertex.

To construct suitable cell C, and $B = \bigcup U_\lambda$ for general (a, b, c, d) with (♯), we have now an imcomplete theory. Above C_i, B_i $(i = 1, 2)$ are obtained applying the theory. Under some calculation, in case $a = 907$, $D(683, 629)$ separates 130 Cells (118 Triangle, 12 Quadriterals). Here we give a rough sketch of the theory, and explain the obstacles.

Step 1. For (a, b, c, d) with (♯), we put $E = \{(x, y, z, w) \in Z^4 \mid ax + by + cz + dw = 0\}$. From E, we choose four vectors $\boldsymbol{a} = (-a_1, a_2, a_3, a_4)$, $\boldsymbol{b} = (b_1, -b_2, b_3, b_4)$, $\boldsymbol{c} = (c_1, c_2, -c_3, c_4)$ and $\boldsymbol{d} = (d_1, d_2, d_3, -d_4)$ which satify the following conditions:

(A) $(a_i, b_j, c_k, d_\ell) \in \bar{N}$ for $1 \leq i, j, k, \ell \leq 4$.

(B) a_1, b_2, c_3, d_4 are the least positive number under (A).

Here $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d})$ are not unique for some (a, b, c, d). But a_1, b_2, c_3, d_4 are uniquely determined.

Step 2. From E, we take L which satisfy

$L = \{(x, y, z, w) \in E \mid 1 \leq x < a_1, |y| < b_2, |z| < c_3, |w| < d_4\}$.

$|L|$ becomes large for some (a, b, c, d). We need a complicated discussion to determine L. This is the first difficulty. (In case $m = 3$, $L = \emptyset$. And this allows a simple theory.)

Step 3. We put $M = L \cup \{-\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}\}$. Using this M, we can define suitable C and B. We obtain C, fairly easily. But to determine $B = \bigcup U_\lambda$. We must follow a very long and winding road.

(Maybe it is lucky if I can overcome these obstacles within a year.)

5. RDS-Problem

5-1. (History) (1) In 1917, Ramanujan [12] determined all $(a, b, , c, d)$ for which $\bar{W}(a, b, c, d) = \emptyset$. (N.B. He treated in $\bar{N}$- frame. Hence we use notations with a bar.) And he commented that " $\bar{W}(1, 1, 10) = \bar{W}(\text{odd}) \cup \bar{W}(\text{even})$. where $\bar{W}(\text{even}) = \{4^\lambda(16\mu +$

$6)|\lambda, \mu \in \bar{N}\ \}$, and $\bar{W}(\text{odd}) = \{3, 7, 21, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, \ldots\}$. Here $\bar{W}(\text{odd})$ does not seem to obey any simple law."

(2) In 1990,Duke and Schulze-Pillot [6] proved that $|\bar{W}(\text{odd})|$ is finite. It is notable that their proof does not yield an explicit bound for $\| \bar{W}(\text{odd}) \|$. [5] says that $\bar{W}(\text{odd})$ seems to be complete by adding two numbers 679, 2719.

5-2. After these forrunnners, we call $W(2,3)$-Problem RDS-Problem. In treating it, we take the standpoint stated in § 2. And besides that we make use the following:

(a) (Trunk-Star Principle) We separate $W(a,b,c)$ into two parts. $W(\text{Tr})$: Infinite set which is parametrizable, and $W(\star) = W \setminus W(\text{Tr})$. Here $|W(\star)| < \infty$ is a bold conjecture. For example, in the case stated above, $\bar{W}(\text{even}) = \bar{W}(\text{Tr})$ and $\bar{W}(\text{odd}) = \bar{W}(\star)$.

(b) (Absolute theory and Relative theory) We investigate $W(a,b,c)$ by separating two steps. Let $a = A\alpha^2, b = B\beta^2, c = C\gamma^2$, where A, B, C are square free.

Step 1. We study $W(A,B,C)$. (Ω-theory),

Step 2. Putting $W(A,B,C) = W_1$ and $W(a,b,c) = W_2$, we have $W_1 \subset W_2$. We say W_2 an $(\alpha^2, \beta^2, \gamma^2)$ -extension of W_1. Here we investigate the structure of
(New W_2) $= W_2 \setminus W_1$. (Γ-theory)

(Important Remark) The statement in the following consists mainly of mysterious phenomena observed from numerical tables. The reasons of them remain in the dark. And by the non-existence of a "completeness criterion", given table of W are that obtained by search of a reasonable range. In the Table, parameters λ, λ_i $(1 \leq i \leq 3)$, μ run through $\bar{N}$.

5.4 (Ω-Theory) We put $\Delta = ABC$. Since $(A,B,C) = 1$ and A, B, C are square free, any prime $p|\Delta$ appears in at most two of them. We say $W(A,B,C)$ to be primitive if all prime $p|\Delta$ appears only in one of A, B, C. From primitive $W(A,B,C)$ for which $p|A$, we get $W(A/p, pB, pC)$. We denote this process by $(p, \wedge)$.

Example 1. Let $W_1 = W(1,1,21)$ which is primitive. We get $W_2 = W(3,3,7)$ by $(3;\wedge)$, $W_3 = W(3,7,7)$ by $(7;\wedge)$ and $W_4 = W(1,21,21)$ by $(3,7;\wedge)$.

We make the following 8 sequences. C_1= 1, 5, 13, 17, 25, 37, 65, 85, 205, C_2=1, 5, 11, C_3= 19, 55, C_4 = 19, 31, 55, C_5= 5, 17, C_6 = 5, 17, C_7 =1, 25, 37, 85, 253, C_8 = 1, 11, 95. Then we obtain

W_1: $4^\lambda(8\mu+3)$, $9^\lambda(9\mu+6)$, $49^\lambda(49\mu+7)$, $49^\lambda(49\mu+14)$, and $49^\lambda(49\mu+28)$. And $4^{\lambda_1}9^{\lambda_2}49^{\lambda_3}K_1$, where $K_1 = \{C_1, 2C_2, 3C_3, 7C_4, 6C_5, 14C_6, 21C_7, 42C_8\}$.

W_2: $4^\lambda(8\mu+1)$, $9^\lambda(3\mu+2)$, $49^\lambda(49\mu+21)$, $49^\lambda(49\mu+35)$, $49^\lambda(49\mu+42)$, $4^{\lambda_1}9^{\lambda_2}49^{\lambda_3}K_2$, where $K_2 = \{C_3, 2C_5, 3C_1, 7C_7, 6C_2, 14C_8, 21C_4, 42C_6\}$.

W_3: $4^\lambda(8\mu+5)$, $9^\lambda(9\mu+6)$, $49^\lambda(7\mu+1)$, $49^\lambda(7\mu+2)$, $49^\lambda(7\mu+4)$. $4^{\lambda_1}9^{\lambda_2}49^{\lambda_3}K_3$ where $K_3 = \{C_4, 2C_6, 3C_7, 7C_1, 6C_8, 14C_2, 21C_3, 42C_5\}$.

W_4 : $4^\lambda(8\mu+7)$, $9\lambda(3\mu+2)$, $49^\lambda(7\mu+3)$, $49^\lambda(7\mu+5)$,$49^\lambda(7\mu+6)$. $4^{\lambda_1}9^{\lambda_2}49^{\lambda_3}K_4$ where $K_4 = \{C_7, 2C_8, 3C_4, 7C_3, 6C_6, 14C_5, 21C_1, 42C_2\}$.

Remarks. (1) Each $C_1 - C_8$ is called a core sequence. They are the essential parts of $W(A,B,C)$. We expect each core sequence to play a role of B in F-Problem.

(2) (divisor property) (a) The factors of core sequence have a very curious property. Namely except for 5, they are (a) one prime or (b) two different primes. Similar property holds for all known RDS cases.

(b) In Example 1, 5 appears as a small factor, but in other cases, several small factors may appear. And in other cases, square of a prime appears. (cf. Exmple 2)

(c) More curious fact is that this property seems to hold in $k \geq 2$ cases with no exceptions. For example, Deshouillers [3] proposed 7373170279850 as a plausible value of $\| W(1,1,1,1) \|$. Factoring the number we have $2.5^2 18521.7961157$. Namely two small factors 2, 5 and two primes.
If you factorize all numbers which appear in [9], you may incline to admit this incredible fact. The reason of this property is in the dark. We think the only hope is to find out a suitable ∂W.

Example 2. Let $W_1 = W(1,1,13)$. This has two core sequences. Namely we put
C_1= 1, 5, 7, 9, 13, 17, 25, 29, 37, 41, 49, 55, 61, 73, 99, 11, 101, 109, 121, 133, 145, 181, 229, 241, 271, 289, 337, 439, 549, 589, 721, 769.
C_2= 1, 3, 5, 7, 11, 17, 23, 41, 45, 47, 53, 59,167, 315, 353.
We have W_1: $4^\lambda(8\mu+3)$, $4^\lambda K_1$, where $K_1 = \{C_1, 2C_2\}$.
(N.B. (A) C_1 contains many numbers of type p^2. (B) 3, 5, 7 seem to be small factors.)

Let $W_2 = W(1,13,13)$. Here we define two more core sequences. Namely
D_1 = 1, 3, 9, 17, 25, 29, 43, 49, 53, 61, 77, 121, 133, 181, 217, 277, 289, 237, 373, 433, 445, 673, 907, 913, 997, 1197, 1213, 1239, 1439, 1479, 1559, 1639, 1717, 1719, 1759.
D_2 = 5, 7, 11, 19, 41, 47, 151, 323, 371, 401, 461, 791, 879, 899.

We have W_2: $4^\lambda(8\mu+7)$, $169^\lambda(169\mu+13.M)$ with $M = \{1,3,4,9,10,12\}$. $4^\lambda K_2$ where $K_2 = \{D_1, 2D_2, 13C_1, 26C_2\}$. (N.B. M is the residue class modulo 13.)

5-5. (Γ-Theory) Γ-Theory seems to be much complicated. We note one Example.

Example 3. Let $W_0 = W(1,2,3)$. W_0 has three 4-extensions. Namely $W_1 = W(4,2,3)$, $W_2 = W(1,8,3), W_3 = W(1,2,12)$. We see
W_0 : $4^\lambda(16\mu+10)$. $4^\lambda K_0$ where $K_0 = \{1,2,7,13\}$. And as a $W(\star)$ we have 3, 5, 11, 17, 19, 35, 43, 73, 83.
Here we define the following four sequences.
E_1= 23, 31, 53, 59, 67, 107, 127, 131, 187.
E_2 = 29, 53, 101, 125, 133, 257, 259, 365, 443, 467, 523, 607, 875.
E_3 = 9, 25, 33, 37, 41, 49, 61, 97, 113, 153, 159, 173, 193, 217, 277, 283, 353, 377, 737, 835, 937, 1153.
E_4= 27, 103, 139, 16, 307, 347, 803, 913.
We put $W_i \setminus W_0 = W_i(\text{even}) \cup W_i(\text{odd})$. Then
$W_1(\text{even}) = \{4W_0(\star), 6, 14, 22, 38, 62, 94\}$. $W_1(\text{odd}) = E_1 \cup E_2$.
$W_2(\text{even}) = \{4\mu+2\}$. $W_2(\text{odd}) = E_1 \cup E_3$.
$W_3(\text{even}) = W_1(\text{even})$, $W_3(\text{odd}) = E_3 \cup E_4$.
We expect E_i's to play a role of core sequences of Ω-Theory.

6. Concluding Remarks

6-1. (Various $W(k,m)$) (1) To consider $W(1,5)$-Problem is desirable. We think it is doubtful that the case $m=5$ needs more complicated theory than the case $m=4$.

(2) Kloosterman [8] studied $W(2,4)$-Problem. He treated in $\bar{N}$-frame, and his main concern is $|W| = \infty$ or not. We think it necessary to treat $W(2,4)$-Problem (a) in N-frame and (b) with Trunk-Star Principle.

(3) $W(3,4)$-Problem is treated by T.Matsui [9]. It is mysterious that the magnitude of $\| W(1,1,1,1) \|$ differs much from that of $\| W(1,1,2,3) \|$.

(4) For $k=4$, we use the folowing notation: $\bar{W}(1;m)$ means $\bar{W}(1,1,\ldots,1)$ where 1 is repeated m times. Davenport [2] proved $|\bar{W}(1;16)| < \infty$. In [2], he noted $\{16^{\lambda}31 \,|\lambda \in \bar{N}\}$ is contained in $\bar{W}(1;15)$. It suggest the existence of Trunk set of type $16^{\lambda}K$. To clarify this K is desirable.

6-2. The concepts and methods used to investigate W-Problems is applicable for other problems. A general setting is explained in [11]. We add here a few remarks.

(1) (Trunk-Star Principle) This Principle springs from the beautiful theory of Dyinkin Diagram. Basic idea is explained in [11]. The aim of this principle and "wirklich method" is to treat exceptional cases.

(2) (Cell-Principle and Net-Theory) This principle plays an important role in F-Problem. Main aim is to seek Descartes Principle for discrete structures. Namely " Near N-sets allow near property".

(3) (Use of trees) In search of N-system, Tree is usuful in many cases. This theme also is treated in [11]. Here we propose a pair of (Sieve, Tree) to treat Subset-sum problem. (Not new?)

SSP: Take $a_0 > a_1 > \cdots > a_n$, where $a_i \in N$. For $s \in N$, find all the $\{m_i\}$'s which satisfy $m_i \in \{0,1\}$ and $\sum_i a_i m_i = s$.

For this SSP, we define SS-sieve and SS-tree T as follows. We put $s(i) = \sum_{j=i}^{n} a_j$. We construct T inductively. t denotes a vertex of T. O is its source. $\rho(t)$ denotes the step number from O to t.

Step 1. For each vertex of T, we put number v. We denote $\psi(t) = v$. Let $\psi(O) = s$.

Step 2. Take $t \in T$. Let $\psi(t) = v$ and $\rho(t) = i$.
(SS-sieve): (a) If $0 \le v \le s_{i+1}$, we draw an arc from t, and put v at the head of it.
(b) If $0 \le v - a_i \le s_{i+1}$, we draw another arc from t, and put $v - a_i$ at the head of it.
(c) Neither case of (a) and (b), t is an endig vertex.
Applying this sieve to final step, we get T. And all solutions appear in T as routes from O to vertices which have 0.

The merit of this method is to make visible all the solutions. As Gaussian plane, we think it to be useful.

References.

[1] A.Brauer, J.E.Shockley, On a problem of Frobenius, Crelle's J. 211 (1962), 215-220.
[2] H.Davenport, On Waring problem for fouth power, Ann. Math 40 (1939), 731-747.

[3] J.L.Davison, On the linear diophantine problem of Frobenius, J.Number Theory 48 (1994) 353-363.

[4] J.M.Deshouillers, F. Hennecart and B.Landreau, 7373170279850, Math. Comp. 229 (1999), 421-439.

[5] W.Duke, Some old problems and new results about quadratic forms, Notice of AMS, 44(1997), 190-195.

[6] W.Duke and Shulze-Pillot, Representations of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, Invent. Math. 99 (1990), 49-57.

[7] S.M.Johnson, A linear diophantine problem, Cnad. J. Math. 12 (1960), 390-398.

[8] A.D. Kloosterman, On the rerpresentation of numbers in the form $ax^2+by^2+cz^2+dt^2$. Acta Math. 49 (1926) 407-464.

[9] T.Matsui, A note on computing $W(3,4)$ sets. Proceedings of AC2007.

[10] R.Morikawa, On the linear diophantine problem of Frobenius in three variables, Bull. Liberal Arts, Nagasaki Univ. 38 (1997), 1-17.

[11] R.Morikawa, Search of mathematical structures using a computer, Proceedings AC 2005, ftp://tnt.math.metro-u.ac.jp/pub/ac05.

[12] S.Ramanujan, On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$, Collected papers (Chelsea).

3-8-22, Nihonmatsu, Sagamihara 229-1137 Japan
E-mail address: rmorikawa@muj.biglobe.ne.jp

Computational Complexity and Transcendence of Numbers

MATSUI, Tetsushi*

Abstract

There are some algebraically closed fields related to computational concepts; a classical example is the whole set of computable numbers and more recently obtained example is the whole set of polynomial time computable numbers. Numbers outside these sets are transcendental because those fields obviously contain the algebraic number field. It will be shown that the number defined by the busy beaver function and the numbers defined by decision problems whose time complexities are not bounded by $2^{c \log n}$ are transcendental.

1 Introduction

There are uncountably many transcendental numbers, as Cantor showed in 19th century. Mere mortals can, however, name only the countable number of transcendental numbers, since there are at most only countably many numbers having finite definitions at all. Such numbers are called "definable numbers", and form a field $\mathbb{C}_{\mathcal{DEF}}$ as a whole. The problem of finding transcendental numbers is, thus, to name numbers in the difference between two countable fields $\mathbb{C}_{\mathcal{DEF}}$ and $\overline{\mathbb{Q}}$.

Since 1950s, it is known that the set of whole computable numbers forms an algebraically closed field [6]. The existence of uncomputable functions had been established by Turing in his famous paper of 1936 [8]. It is, thus, clear that there exist complex numbers defined well but transcendental because they are uncomputable. The most well-known such a number is Chaitin's Ω [1].

The set of whole polynomial time computable numbers also forms an algebraically closed field, and other fields corresponding to the classes of complexity as well [7]. By the theorem of hierarchy, there are numbers computable in exponential time but uncomputable in polynomial time, and they are transcendental by the fact stated above.

*Department of Mathematics and Information Sciences, Tokyo Metropolitan University. tetsushi@tnt.math.metro-u.ac.jp

In this paper, we shall give examples of transcendental numbers whose proofs of transcendence are based on theory of computation: a number transcendental by uncomputability is in section 2 and by computational hierarchy in section 3. Then, we shall discuss about limits of the method.

We will use the following notations. All script letters $\mathcal{COMP}$, $\mathcal{EXP}$, $\mathcal{NP}$ and $\mathcal{P}$ denote the class of computable functions, exponential time computable, non-deterministic polynomial time computable and deterministic polynomial time computable, respectively. For any class C, $\mathbb{C}_C$ denotes the whole set of C-computable numbers. Roman capital letters NP, P, etc., on the other hand, denote the class of decision problems of non-deterministic polynomial time computable, of deterministic polynomial time computable, etc., respectively.

2 Transcendence from Uncomputability

Rado introduced in 1962 the busy beaver function Σ, and showed it is definable but uncomputable [5]. We shall define a number using the function and show in two different ways that the number is a transcendental number.

We call the following real number β *the busy beaver number.*

$$\beta = \sum_{n=1}^{\infty} 2^{-\Sigma(n)}.$$

Proposition 1. *The busy beaver number β is a transcendental number.*

The first proof is based on the fact that $\mathbb{C}_{\mathcal{COMP}}$ is an algebraically closed field [6].

proof of Proposition 1. Assume that β is computable. Then, by its binary expansion, one can easily construct a computable version of the function Σ. It contradicts the fact that Σ is uncomputable, thus, β is an uncomputable number. In other words, β is not in $\mathbb{C}_{\mathcal{COMP}}$. The field $\mathbb{C}_{\mathcal{COMP}}$ is algebraically closed. Therefore, all algebraic numbers are in $\mathbb{C}_{\mathcal{COMP}}$. It means β can not be an algebraic number. □

The second proof is in more familiar way. It is based on the classical Liouville's criterion:

Theorem 1 (Liouville's criterion)**.** *A real number τ is a transcendental number if for any natural number n there exists a rational approximation p/q of τ satisfying*

$$\left|\tau - \frac{p}{q}\right| \leq \frac{1}{q^n}.$$

proof of Proposition 1. The busy beaver function Σ grows so rapidly that for any computable function f there exists an integer n_0 such that for any integer $n > n_0$ it satisfies:

$$\Sigma(n) > f(n)$$

[5]. Then, for any n there exists m such that $\Sigma(m+1) > n\Sigma(m)$. We compute the difference between β and its m-th convergent.

$$\begin{aligned}\left|\beta - \sum_{i=1}^{m} 2^{-\Sigma(i)}\right| &= \sum_{i=m+1}^{\infty} 2^{-\Sigma(i)} \\ &\leq 2^{-\Sigma(m+1)+1} \\ &\leq 2^{-n\Sigma(m)}.\end{aligned}$$

Because the denominator of the m-th convergent is $2^{\Sigma(m)}$, β satisfies Liouville's criterion. □

Remark 1. One can also prove transcendence of similar numbers

$$\beta(\theta) = \sum_{n=1}^{\infty} \theta^{-\Sigma(n)}$$

for any algebraic numbers θ, whose absolute value is greater than 1, using the fact about rapid growth of the function Σ.

Remark 2. The argument is not special to the busy beaver function and number. One can show the transcendence of any uncomputable numbers whose defining functions are too rapidly growing to be computable, in the same way.

By these proofs, we know that β has a very rapidly converging series, but most of its terms are impossible to know[1]. These two statements do not contradict with each other. It means that usual sense of "rapid convergence" concerning only the speed of convergence for given terms, while we are discussing about how to give them.

3 Transcendence from Computational Hierarchy

3.1 Polynomial Time Computable Numbers

There are several definitions of polynomial time computable numbers, but they are equivalent [3]. We use the following definition.

Definition 1. A complex number z is a *polynomial time computable number* if and only if there exists $F \in \mathcal{P}$ from $\mathbb{N}$ to $\mathbb{Q}[i]$ satisfying

$$|z - F(n)| \leq \frac{1}{n}$$

for any natural number n.

[1] Of course, some terms are computed and known.

Note that, although the definition seems to require a function be defined for all natural numbers, it is not hard to show that a function has to be defined only for a certain subset like $\{2^m | m \in \mathbb{N}\}$.

Likewise, one may pick a class of computational complexity C and define C-computable numbers.

The set of whole polynomial time computable numbers forms an algebraically closed field. It is not so well-known, but by referring Ko [2] the proof is attributed to Schönhage [7]. Since the main point is that roots of an equation can be approximated in polynomial time of specified precision[2], other complexity classes which are defined by polynomial time equivalence are connected to each an algebraically closed field. Therefore, the hierarchy of complexity classes induces the tower of algebraically closed fields. The hierarchy $\mathcal{P} \subset \mathcal{NP} \subset \mathcal{EXP} \subset \mathcal{COMP}$ corresponding the tower $\mathbb{C}_{\mathcal{P}} \subset \mathbb{C}_{\mathcal{NP}} \subset \mathbb{C}_{\mathcal{EXP}} \subset \mathbb{C}_{\mathcal{COMP}}$. It is known that $\mathcal{P} \neq \mathcal{EXP} \neq \mathcal{COMP}$ but unknown whether other inclusions are proper or not.

The definition of the polynomial time computable numbers uses very special type of polynomial time computable functions. Decision problems are more familiar type of functions, we shall try to establish a way to construct a number from a decision problem.

Let D be a decision problem, i.e., a function from $\mathbb{N}$ to $\{0, 1\}$. It is possible to identify D with a subset of $\mathbb{N}$ through interpreting D as its characteristic function.

We define a number $\alpha(D)$ for a decision problem D by:

$$\alpha(D) = \sum_{i=1}^{\infty} D(i) 2^{-i}$$

that is a binary expansion.

Now, let us consider the computational complexity. For a denominator 2^k, input size for F, in a sense of the definition 1, is k. On the other hand, input size for D is $\log k$. The gap leads to unintuitive conclusion that the number $\alpha(D)$ is a polynomial time computable number if the time complexity of D is bounded by $2^{O(\log k)}$ from above. Thus, D can be an *exponential time* decision problem.

3.2 Polynomial Time Uncomputable Numbers

We would like to construct a polynomial time uncomputable number, for showing the concept of "transcendence by hierarchy of complexities".

As stated above, a number $\alpha(D)$ for a decision problem D whose time complexity is bounded by $2^{O(\log k)}$ from above is polynomial time computable. It is, thus, sufficient to construct a decision problem whose computational complexity exceeds $2^{O(\log k)}$.

There may be interesting decision problem examples, but we use a canonical problem approach.

[2] It is in fact in $\mathcal{NC}$, shown by Neff [4].

Definition 2. Let n be a code of triple "(M, x, m)" with M a Turing machine, x an input for M and m a natural number. The problem K_2 is:

$$K_2 = \left\{ n = "(M, x, m)" | M \text{ accepts } x \text{ at most } m^{\text{len}(n)} \text{ steps.} \right\},$$

where $\text{len}(\cdot)$ denotes $\lfloor \log_2(\cdot) + 1 \rfloor$.

Though the definition depends on the choice of coding scheme, we do not pick one. We only assume that the code can be interpreted as a binary representation of integer. It, then, lets us to think K_2 be a subset of $\mathbb{N}$.

Proposition 2. *The time complexity of K_2 is $O(2^{\log^2 n})$ but not $2^{O(\log n)}$.*

Proof. We do not show every detail. One can construct a Turing machine which accepts K_2 by combining trivial input check and emulation of M on input x for at most $m^{\text{len}(n)}$ steps.

The most important point is that on a valid input n the emulation of M may take $O(m^{\text{len}(n)}) = O(2^{\text{len}(m)\text{len}(n)})$ steps. Obviously, $\text{len}(m) < \text{len}(n)$ holds and $\text{len}(m)$ cannot be bounded by any constant. Therefore, the number of steps exceed $2^{O(\log n)}$ yet is bounded by $O(2^{\log^2 n})$. □

Finally, we obtain the following result.

Corollary 1. *The number $\alpha(K_2)$ is not polynomial time computable, and thus transcendental.*

Proof. Assume that $\alpha(K_2)$ is polynomial time computable. Then, by its binary expansion, one can easily construct another implementation of K_2 that is computable in $2^{O(\log n)}$ time. It contradicts the result of the proposition 2. Thus, $\alpha(K_2)$ is not a polynomial time computable number. In other words, $\alpha(K_2)$ is not in $\mathbb{C}_{\mathcal{P}}$. The field $\mathbb{C}_{\mathcal{P}}$ is algebraically closed and all algebraic numbers are in the field. It means $\alpha(K_2)$ can not be an algebraic number. □

4 Discussions

4.1 Applicability

The number $\alpha(K_2)$ defined in the previous section is not in $\mathbb{C}_{\mathcal{P}}$ but obviously in $\mathbb{C}_{\mathcal{EXP}}$. It is deduced from the hierarchy theorem that $\mathbb{C}_{\mathcal{P}}$ is a proper subfield of $\mathbb{C}_{\mathcal{EXP}}$, and the number is in the gap. Since $\mathbb{C}_{\mathcal{P}}$ is an algebraically closed field, $\alpha(K_2)$ is a transcendental number.

The proof is completely analogous to the one for β in section 2, which is shown transcendental by that it is out of an algebraically closed field $\mathbb{C}_{\mathcal{COMP}}$. There can be more proofs in analogous arguments that a number is transcendental because it is in an algebraically closed field but not in a proper algebraically closed subfield, both defined in computational manner.

A difficulty for using this method is that there are only a few fact is known about proper inclusions of computational classes and thus corresponding fields.

For example, if $\mathcal{P} \neq \mathcal{NP}$ holds, there exist transcendental numbers because they are not deterministic but non-deterministic polynomial time computable, but the condition has been unproven.

Moreover, this kind of approach to the transcendence of numbers have not been fully explored, probably because the most of numbers to be questioned, Euler-Mascheroni's constant γ for example, are defined in analytics and have easily computable efficiently converging series. It means that such numbers are in $\mathbb{C}_{\mathcal{P}}$, the smallest algebraically closed field ever shown by computational complexity theory, and we cannot say anything about their transcendence by the method above.

4.2 Future Works / Open Questions

As we already discussed, $\alpha(D)$ is polynomial time computable number if the decision problem D has time complexity $2^{O(\log n)}$. It is obviously better if only polynomial time computable decision problems are connected to polynomial time computable number. We are investigating possible definitions.

The hardest problem remained open is whether $\mathbb{C}_{\mathcal{P}} = \mathbb{C}_{\mathcal{NP}}$ or not. It is in fact equivalent to P=NP problem. If $\mathbb{C}_{\mathcal{P}} \neq \mathbb{C}_{\mathcal{NP}}$, there are numbers non-deterministic polynomial time computable but deterministic polynomial time uncomputable.

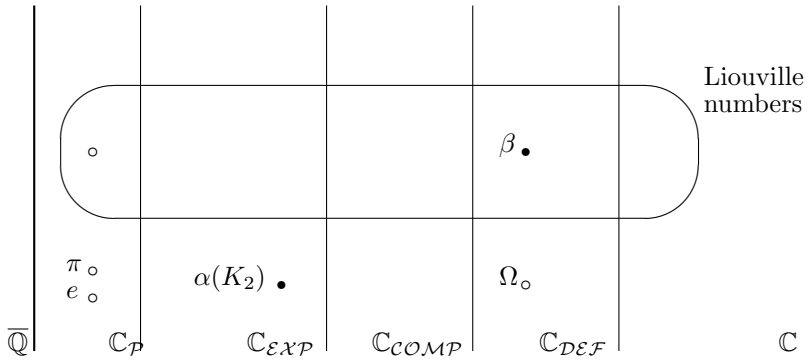

Figure 1: Transcendental Numbers

References

[1] G. J. Chaitin. A theory of program size formally identical to information theory. *Journal of the ACM*, 22:329–340, 1975.

[2] K.-I. Ko. *Complexity Theory of Real Functions*. Birkhäuser, 1991.

[3] T. Matsui. *On Development of Systems for Number Theoretic Computation and Related Problems*. Doctoral thesis, Tokyo Metropolitan University, 2007.

[4] C. A. Neff. Specified precision polynomial root isolation is in NC. In *31st IEEE Symposium on Foundations of Computer Science*, pages 152–162. IEEE, 1990.

[5] T. Rado. On non-computable functions. *The Bell System Technical Journal*, 41(3):877–884, May 1962.

[6] H. G. Rice. Recursive real numbers. *Proc. American Math. Soc.*, 5:784–791, October 1954.

[7] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. preprint, Mathematicshes Institut der Universität Tübingen, 1982.

[8] A. C. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proc. London Math. Soc.*, 42:230–265, November 1936.

$\langle q, r\rangle$ 数系におけるパターン数列の性質について

塩川宇賢, 立谷 洋平 (慶應義塾大学)

1 序

1.1 パターン数列の定義と性質

$q \geq 2$ を任意に固定した整数, $r = 0, 1, \ldots, q-2$ とする. $\langle q, r\rangle$ 数系とは q^i $(i \geq 0)$ を基底とし, $\Sigma_{q,r} := \{-r, 1-r, \ldots q-1-r\}$ 上の線形結合で自然数を一意的に表現する数系のことである. 自然数 n が

$$n = a_l q^l + a_{l-1} q^{l-1} + \cdots + a_1 q + a_0, \quad a_i \in \Sigma_{q,r}$$

と表現されるとき,

$$(n)_{q,r} := a_l a_{l-1} \cdots a_1 a_0$$

を n の $\langle q, r\rangle$ 展開と呼ぶ. $\langle d, 0\rangle$ 展開は通常の整数の d 進展開である. これまで $\langle q, r\rangle$ 数系を特徴づける q-linear functions やその具体例である sum of digit functions が研究されている (cf. [1], [2], [4], and [7]).

集合 $\Sigma_{q,r}$ の中の数字の有限列を word と呼び, word 全体の集合を $\Sigma_{q,r}^*$ とおく. また $w \in \Sigma_{q,r}^*$ に対し, $w^l = ww\cdots w$ (w を l 個並べたもの) とおく.

Definition 1. $w \in \Sigma_{q,r}^*$ に対し, 整数 $n \geq 1$ の $\langle q, r\rangle$ 展開の中に現れる w の個数を $e_{q,r}(w; n)$ で表す. ただし $w \neq 0^l$ のときは n の $\langle q, r\rangle$ 展開の最高次の位の数字の前に 0 がいくつか並んでいるものとし, $w = 0^l$ のときはこの補正は行わないことにする. また $e_{q,r}(w; 0) = 0$ とする. このとき得られる数列

$$\{e_{q,r}(w; n)\}_{n \geq 0}$$

を w に対するパターン数列と呼ぶ.

Example 1.

$$e_{10,0}(1; 12321) = 2, \quad e_{10,0}(02; 202202) = 3, \quad e_{2,0}(1; 2^n - 1) = n \ \ (n \geq 0).$$

以下, $w = b_{l-1} \cdots b_1 b_0 \in \Sigma_{q,r}^*$ $(b_i \in \Sigma_{q,r})$ に対して $l := |w|$ を w の長さと呼ぶ. また $[w]_{q,r} := \sum_{i=0}^{l-1} b_i q^i$ と定義する. パターン数列は次の性質を持つ:

Proposition 1.

$$e_{q,r}(w;n)=\sum_{a=-r}^{q-1-r}e_{q,r}(aw;n).$$

Proposition 2. 任意の整数 $n\geq 1$ に対し,

$$e_{q,r}(w;n)=e_{q,r}\left(w;\left[\frac{n+r}{q}\right]\right)+\begin{cases}1, & n\equiv[w]_{q,r}\pmod{q^{|w|}},\\ 0, & otherwise.\end{cases}$$

1.2 代数的独立性

パターン数列 $\{e_{q,r}(w;n)\}_{n\geq 0}$ の母関数, すなわち

$$f_w(z)=\sum_{n\geq 0}e_{q,r}(w;n)z^n \tag{1}$$

を考える. 任意の $w\in\Sigma_{q,r}^*$ に対して $f_w(z)$ の収束半径は 1 である. 実際, $n=a_lq^l+a_{l-1}q^{l-1}+\cdots+a_0$, $a_i\in\Sigma_{q,r}$ とすると十分大きい n に対して

$$e_{q,r}(w;n)\leq l+1\leq q^l-r\frac{q^l-1}{q-1}\leq n$$

が成り立ち, $\limsup_{n\to\infty}e_{q,r}(w;n)^{\frac{1}{n}}\leq\limsup_{n\to\infty}n^{\frac{1}{n}}=1$ となる. 一方, $e_{q,r}(w;n)\geq 1$ となる n は無限に多く存在する. よって $1/\limsup_{n\to\infty}e_{q,r}(w;n)^{\frac{1}{n}}=1$ である.

内田は $r=0$ のとき, m 個の word $w_1,\ldots,w_m\in\Sigma_{q,0}^*$ に対するパターン数列の母関数 $f_{w_1}(z),\ldots,f_{w_m}(z)$ が $\mathbb{C}(z)$ 上代数的独立になるための必要十分条件を与えた.

Theorem (内田 [9]) $w_1,\ldots,w_m\in\Sigma_{q,0}^*$ とする. このとき次の 3 条件は同値である.
(i) $f_{w_1}(z),\ldots,f_{w_m}(z)$ は $\mathbb{C}(z)$ 上代数的従属である.
(ii) $f_{w_1}(z),\ldots,f_{w_m}(z)$ は $\bmod\mathbb{C}(z)$ で $\mathbb{C}$ 上線形従属である.
(iii) $\left\{\sum_{i=1}^m c_ie_{q,0}(w_i;n)\right\}_{n\geq 0}$ が周期 q^{l-1} の周期列となるような $(c_1,\ldots,c_m)\in\mathbb{C}^m\setminus\{\mathbf{0}\}$ が存在する. ここで $l=\max\{|w_1|,\ldots,|w_m|\}$.

任意の $w\in\Sigma_{q,r}^*$ に対し, $n_j=[(1w)^j]_{q,r}$ とおけば $e_{q,r}(w;n_j)\to\infty$ $(j\to\infty)$ となるので, パターン数列 $\{e_{q,r}(w;n)\}_{n\geq 0}$ は周期列でない. 従って, 任意の $w\in\Sigma_{q,0}^*$ に対し $f_w(z)=\sum_{n\geq 0}e_{q,0}(w;n)z^n$ は $\mathbb{C}(z)$ 上超越的である. 一方, word が 2 個以上の場合, $f_{w_1}(z),\ldots,f_{w_m}(z)$ は $\mathbb{C}(z)$ 上代数的従属になりうる:

Example 2. *Proposition 1* より任意の $w \in \Sigma_{q,r}^*$ に対して次が成り立つ.

$$\begin{aligned} 0 &= \sum_{n=0}^{\infty} \left(e_{q,r}(w;n) - \sum_{a=-r}^{q-1-r} e_{q,r}(aw;n) \right) z^n \\ &= f_w(z) - \sum_{a=-r}^{q-1-r} f_{aw}(z). \end{aligned}$$

つまり $f_w(z)$, $f_{aw}(z)$ $(a = -r, 1-r, \ldots, q-1-r)$ は $\mathbb{C}(z)$ 上線形従属である.

Example 3.

$$\begin{aligned} f_1(z) &= \sum_{n\geq 0} e_{2,0}(00;n) z^n, \quad f_2(z) = \sum_{n\geq 0} e_{2,0}(01;n) z^n, \\ f_3(z) &= \sum_{n\geq 0} e_{2,0}(10;n) z^n, \quad f_4(z) = \sum_{n\geq 0} e_{2,0}(11;n) z^n. \end{aligned}$$

とおくと,

$$\text{trans. deg}_{\mathbb{C}(z)}(f_1(z), f_2(z), f_3(z), f_4(z)) = 3.$$

ここで $\{e_{2,0}(01;n) - e_{2,0}(10;n)\}_{n\geq 0} = \{\overline{0,1}\}$ は周期列であり

$$f_2(z) - f_3(z) = \frac{z}{1-z^2}.$$

つまり $f_2(z)$ と $f_3(z)$ は $\bmod \mathbb{C}(z)$ で $\mathbb{C}$ 上線形従属である.

内田の結果は $r = 0$, すなわち $\langle q, 0\rangle$ 数系のパターン数列に限定されている. 本稿での我々の目標は, r を動かしたとき, つまり和集合 $\cup_{r=0}^{q-2} \Sigma_{q,r}^*$ から選んだ複数の word に対するパターン数列の相互関係を調べることである. 例えば, $q = 3$, $r = 0, 1$, $w_1 = w_2 = 0$ に対するパターン数列

$$\{e_{3,0}(0;n)\}_{n\geq 0}, \quad \{e_{3,1}(0;n)\}_{n\geq 0}$$

をとる. 我々の定理 (Theorem 1) は自然数 n の 3 進展開と $\langle 3, 1\rangle$ 展開における 0 の現れ方が (ある意味で) 独立であることを示している.

2 主定理

我々は内田の結果を拡張し, 次の結果を得た.

Theorem 1. 任意の $w_{r,1}, \ldots, w_{r,m(r)} \in \Sigma_{q,r}^*$ $(r = 0, \ldots, q-2)$ に対し,

$$f_{r,i}(z) = \sum_{n\geq 0} e_{q,r}(w_{r,i};n) z^n \quad (r = 0, \ldots, q-2,\ i = 1, \ldots, m(r)) \tag{2}$$

とおく. このとき次の 3 条件は同値である.
(i) $f_{r,i}(z)$ $(r=0,\dots,q-2,\ i=1,\dots,m(r))$ は $\mathbb{C}(z)$ 上代数的従属である.
(ii) ある r に対し, $f_{r,1}(z),\dots,f_{r,m(r)}(z)$ は $\bmod \mathbb{C}(z)$ で $\mathbb{C}$ 上線形従属である.
(iii) ある r に対し, 数列

$$\left\{\sum_{i=1}^{m(r)} c_i e_{q,r}(w_{r,i};n)\right\}_{n\geq 0}$$

が十分大きい n で周期 q^{l-1} の周期列となるような $(c_1,\dots,c_{m(r)})\in\mathbb{C}^{m(r)}\setminus\{\mathbf{0}\}$ が存在する. ここで $l=\max\limits_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}}|w_{r,i}|$.

定理 (の対偶) より, $m(0)+\cdots+m(q-2)$ 個の関数

$$f_{r,i}(z)=\sum_{n\geq 0} e_{q,r}(w_{r,i};n)z^n \quad (r=0,\dots,q-2,\ i=1,\dots,m(r))$$

の $\mathbb{C}(z)$ 上の代数的独立性は, 各 $r=0,1,\dots,q-2$ に対する $m(r)$ 個の関数

$$f_{r,i}(z)=\sum_{n\geq 0} e_{q,r}(w_{r,i};n)z^n \quad (i=1,\dots,m(r))$$

の $\bmod \mathbb{C}(z)$ での $\mathbb{C}$ 上の線形独立性に帰着される. 特に, $m(r)=1$ $(r=0,\dots,q-2)$ の場合においては, 各関数 $f_r(z)=\sum_{n\geq 0} e_{q,r}(w_r;n)$ $(r=0,\dots,q-2)$ の無理性と $q-1$ 個の関数

$$f_0(z)=\sum_{n\geq 0} e_{q,0}(w_0;n)z^n,\dots,f_{q-2}(z)=\sum_{n\geq 0} e_{q,q-2}(w_{q-2};n)z^n$$

の $\mathbb{C}(z)$ 上の代数的独立性は同値である. しかし前述したように各 $f_r(z)$ $(r=0,\dots,q-2)$ は超越関数なので, $f_0(z),\dots,f_{q-2}(z)$ は $\mathbb{C}(z)$ 上で代数的独立となる. よって $f_0(z),\dots,f_{q-2}(z)$ の非自明な $\mathbb{C}$ 上の線形結合 $R(z)=c_0f_0(z)+\cdots+c_{q-2}f_{q-2}(z)$ は有理関数では表せず, ベキ級数 $R(z)$ の係数列

$$\left\{\sum_{i=0}^{q-2} c_i e_{q,i}(w_i;n)\right\}_{n\geq 0}$$

は線形回帰数列では表現できないことがわかる. 特に異なる $\langle q,r\rangle$ 数系におけるパターン数列は $\mathbb{C}$ 上線形独立である. これは $\langle q,r\rangle$ 数系 $(r=0,\dots,q-2)$ による自然数の表示のある種の独立性を示唆している.

また Theorem 1 より次の系が従う:

Corollary 1. 任意の整数 $m\geq 1$ に対して,

$$f_r(z)=\sum_{n\geq 0} e_{q,r}((m)_{q,r};n)z^n, \quad r=0,\dots,q-2$$

は $\mathbb{C}(z)$ 上代数的独立である.

$\cap_{r=0}^{q-2}\Sigma_{q,r}=\{0,1\}$ に注意することにより次を得る.

Corollary 2. $w=b_k\cdots b_0$, $b_i\in\{0,1\}$ とおく. このとき

$$f_r(z)=\sum_{n\geq 0}e_{q,r}(w;n)z^n,\quad r=0,\ldots,q-2$$

は $\mathbb{C}(z)$ 上代数的独立である. 特に $q=3$, $w=0$ とすれば非自明な $\mathbb{C}$ 上の線形結合

$$\{c_1e_{3,0}(0;n)+c_2e_{3,1}(0;n)\}_{n\geq 0}$$

は線形回帰数列では表現できない.

3 Theorem 1の証明

本節で Theorem 1 (i)⇒(iii) の証明を解説する. (iii)⇒(ii) 及び (ii)⇒(i) は容易.

関数 $f_{r,i}(z)$ を Theorem 1 で定義されたものとする. Proposition 2 から $f_{r,i}(z)$ は Mahler 型関数方程式

$$f_{r,i}(z)=\frac{1-z^q}{z^r(1-z)}f_{r,i}(z^q)+\frac{z^{\nu(w_{r,i})}}{1-z^{q^{|w_{r,i}|}}}$$

をみたすことが確かめられる. ここで

$$\nu(w_{r,i})=\begin{cases}[w_{r,i}]_{q,r}, & [w_{r,i}]_{q,r}>0,\\ q^{|w_{r,i}|}+[w_{r,i}]_{q,r}, & otherwise.\end{cases}$$

いま $L=q^2-1$, $u_r=r(q+1)$,

$$F_{r,i}(z)=z^{-u_r}(1-z^L)f_{r,i}(z^L)$$

とおくと, $F_{r,i}(z)\in\mathbb{C}[[z]]$ であり, $F_{r,i}(z)$ は関数方程式

$$F_{r,i}(z)=F_{r,i}(z^q)+\frac{z^{\nu(w_{r,i})L-u_r}(1-z^L)}{1-z^{q^{|w_{r,i}|}L}}\tag{3}$$

をみたす.

Lemma 1 ([3], [5]). $d\geq 2$ を整数とする. $g_1(z),\ldots,g_m(z)\in\mathbb{C}[[z]]$ が $\mathbb{C}(z)$ 上代数的従属であり, 関数方程式

$$g_i(z^d)=g_i(z)+a_i(z),\quad a_i(z)\in\mathbb{C}(z),\quad i=1,2,\ldots,m.$$

をみたすならば, $g_1(z),\ldots,g_m(z)$ は $\bmod\mathbb{C}(z)$ で $\mathbb{C}$ 上線形従属である.

Lemma 2. $d \geq 2$, $L \geq 1$, $l \geq 1$ を整数とする．もし有理関数 $c(z) \in \mathbb{C}(z)$ が関数方程式

$$c(z^d) = c(z) + \frac{(1-z^L)a(z)}{1-z^{d^l L}}, \quad a(z) \in \mathbb{C}[z]$$

をみたすならば,

$$c(z) = \frac{(1-z^L)b(z)}{1-z^{d^{l-1}L}}$$

となる $b(z) \in \mathbb{C}[z]$ が存在する.

関数 $F_{r,i}(z)$ の定義より, $\{f_{r,i}(z)\}_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}}$ と $\{F_{r,i}(z)\}_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}}$ の $\mathbb{C}(z)$ 上での代数的従属性は同値である．よって $\{f_{r,i}(z)\}_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}}$ が $\mathbb{C}(z)$ 上で代数的従属ならば, Lemma 1 より, $\{F_{r,i}(z)\}_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}}$ は $\bmod \mathbb{C}(z)$ で $\mathbb{C}$ 上線形従属となる．つまり,

$$R(z) := \sum_{r=0}^{q-2}\sum_{i=1}^{m(r)} c_{r,i}F_{r,i}(z) = \sum_{r=0}^{q-2}\sum_{i=1}^{m(r)} c_{r,i}z^{-u_r}(1-z^L)f_{r,i}(z^L) \tag{4}$$

が有理関数となるような少なくとも 1 つは 0 でない $c_{r,i} \in \mathbb{C}$ が存在する．このとき (3) から有理関数 $R(z)$ は関数方程式

$$R(z) = R(z^q) + \frac{(1-z^L)a(z)}{1-z^{q^l L}}, \quad a(z) \in \mathbb{C}[z]$$

をみたす．ここで $l = \max\limits_{\substack{0\leq r\leq q-2\\ 1\leq i\leq m(r)}} |w_{r,i}|$．従って Lemma 2 より, ある $b(z) \in \mathbb{C}[z]$ が存在して

$$R(z) = \frac{(1-z^L)b(z)}{1-z^{q^{l-1}L}}$$

とかける．上式を (4) に代入し

$$\begin{aligned} b(z) &= (1-z^{q^{l-1}L})\sum_{r=0}^{q-2}\sum_{i=1}^{m(r)} z^{-u_r}f_{r,i}(z^L) \\ &= (1-z^{q^{l-1}L})\sum_{n\geq 0}\left(\sum_{r=0}^{q-2}\sum_{i=1}^{m(r)} c_{r,i}e_{q,r}(w_{r,i};n)\right)(z^{q+1})^{(q-1)n-r} \\ &= Q(z) + \sum_{n\geq q^{l-1}}\sum_{r=0}^{q-2}\left(a_{n,r} - a_{n-q^{l-1},r}\right)(z^{q+1})^{(q-1)n-r} \end{aligned}$$

を得る．ここで $\deg Q(z) < q^{l-1}$, $a_{n,r} = \sum_{i=1}^{m(r)} c_{r,i}e_{q,r}(w_{r,i};n)$．従って $0 \leq r \leq q-2$ かつ $b(z)$ が多項式であることに注意すれば, 任意の r に対し $a_{n,r} - a_{n-q^{l-1},r} = 0$ が十分大きい n で成り立つ. すなわち数列

$$\left\{\sum_{i=1}^{m(r)} c_{r,i}e_{q,r}(w_{r,i};n)\right\}_{n\geq 0}$$

は十分大きいところで周期 q^{l-1} の周期列となっている.

References

[1] J. P. Allouche and J. Shallit. *Automatic Sequences, Theory, Applications, Generalizations* (Cambridge University Press. 2003).

[2] D. E. Knuth. *The Art of Computer Programming.* vol. **2** (Addison Wesley, London. 1981).

[3] K. K. Kubota. On the algebraic independence of holomorphic solutions of certain functional equations and their values. *Math. Ann.* **227** (1977), 9–50.

[4] T. Kurosawa and I. Shiokawa. q-linear functions and algebraic independence. *Tokyo J. Math.* **25** (2002), 459–472.

[5] J. H. Loxton and A. J. van der Poorten. A class of hypertranscendental functions. *Aequationes Math.* **16** (1977), 93–106.

[6] K. Nishioka. *Mahler functions and Transcendence.* Lecture Notes in Math. vol. **1631** (Springer-Verlag. 1996).

[7] S. Okada and I. Shiokawa. Algebraic independence results related to $\langle q, r\rangle$-number systems. *Monatsh. Math.* **147** (2006), 319–335.

[8] I. Shiokawa and Y. Tachiya. Pattern sequences in $\langle q, r\rangle$-numeration systems. submitted.

[9] Y. Uchida. Algebraic independence of the power series defined by blocks of digits. *J. Number Theory* **78** (1999), 107–118.

WEBER の類数問題に対する計算的アプローチ

小松啓一 AND 福田隆

1. Introduction

$\alpha_n = 2\cos(2\pi/2^{n+2})$, $\Omega_n = \mathbb{Q}(\alpha_n)$ とおく。Ω_n は有理数体 $\mathbb{Q}$ の 2^n 次巡回拡大であり、$\Omega_\infty = \cup_n \Omega_n$ は $\mathbb{Q}$ の $\mathbb{Z}_2$-拡大になる。1886 年に Weber [20] は Ω_n の類数 h_n は全ての $n \geq 1$ に対し奇数であることを示し、1956 年に岩澤は、今日岩澤理論と呼ばれる理論の萌芽となる論文 [13] で、鮮やかな別証明を与えた。

h_n そのものについては Weber は $h_n = 1$ $(1 \leq n \leq 3)$ を示し、$h_4 > 1$ だろうと予想したらしい (cf. [21, p. 808])。しかしながら Cohn [4], Bauer [3], Masley [15] により $h_4 = 1$ が、van der Linden [14] により $h_5 = 1$ が示された。GRH を仮定すれば $h_6 = 1$ であることもわかっている。

h_n そのものは難しいが、奇素数 ℓ に対し h_n の ℓ-part は $\mathbb{Z}_p$-拡大の理論を用いて調べることができる。1975 年に Washington [18] は h_n の ℓ-part は $n \longrightarrow \infty$ の時に有界であること、つまり $h_n = \ell^{e_n} q$, $\ell \nmid q$ と表す時 e_n は有界であることを示した。Washington は e_n の増加が止まる n を具体的に評価できる形で与えたが、e_n の大きさについてはそこからは直ちにはわからない。堀江は 2002 年から始まる一連の研究において、ℓ が適当な条件をみたせば全ての $n \geq 1$ に対し $\ell \nmid h_n$ であることを示した (cf. [8], [9], [10], [11], [12])。堀江の結果の一部は次のように述べられる。

定理 1.1 (堀江)**.** 奇素数 ℓ に対し

(1) $\ell \equiv 3, 5 \pmod 8$
$\Longrightarrow \ell \nmid h_n$ for all $n \geq 1$

(2) $\ell \equiv 9 \pmod{16}$, $\ell > 34797970939$
$\Longrightarrow \ell \nmid h_n$ for all $n \geq 1$

(3) $\ell \equiv 7 \pmod{16}$, $\ell > 210036365154018$
$\Longrightarrow \ell \nmid h_n$ for all $n \geq 1$

(4) $\ell \equiv 17 \pmod{32}$, $\ell > 990588768036872329883152003 02$
$\Longrightarrow \ell \nmid h_n$ for all $n \geq 1$

(5) $\ell \equiv 15 \pmod{32}$, $\ell > 135879627945676644173677679336829027603311790 94$
$\Longrightarrow \ell \nmid h_n$ for all $n \geq 1$

ℓ に関する合同条件を固定すれば、その条件をみたす殆んど全ての ℓ に対して $\ell \nmid h_n$ $(n \geq 1)$ であることがわかる。しかし、一方で、$\ell = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, ...$ に対しては $\ell \nmid h_n$ $(n \geq 6)$ かどうかこの定理からはわからない。我々は次の結果を得た。

定理 1.2. ℓ を奇素数とし $c \in \mathbb{Z}$ を

$$\begin{cases} 2^c \mid\mid \ell - 1 & \textit{if } \ell \equiv 1 \pmod 4 \\ 2^c \mid\mid \ell^2 - 1 & \textit{if } \ell \equiv 3 \pmod 4 \end{cases}$$

で定め、

$$m = 3c + 1 + 2[\log_2(\ell - 1)] + [\log_2(2c + [\log_2(\ell - 1)] + 2)]$$

とおく。もし $\ell \nmid h_m$ なら、全ての $n \geq 1$ に対して $\ell \nmid h_n$ である。

いくつかの ℓ に対する m は次のようになる。

ℓ	3	5	7	17	31	257	8191	65537	524287
m	16	15	21	26	34	46	75	87	106

計算機を用いて $\ell \nmid h_m$ を確かめれば、次の結果を得る。

系 1.3. $\ell < 10^5$: 素数 $\Longrightarrow \forall\, n \geq 1 \quad \ell \nmid h_n$

定理 1.2 は Sinnott-Washington の手法に基づいて証明される (cf. [19], [5])。ここでは系 1.3 を導くために行った計算について解説する。

1.1. General Settings.

A_n で Ω_n のイデアル類群の ℓ-part を表し、$\Delta_n = G(\Omega_n/\mathbb{Q})$ とする。$\mathbb{Q}_\ell$ の代数閉包を $\overline{\mathbb{Q}}_\ell$ とし、指標 $\chi : \Delta_n \longrightarrow \overline{\mathbb{Q}}_\ell$ に対し

$$e_\chi = \frac{1}{|\Delta_n|} \sum_{\sigma \in \Delta_n} \mathrm{Tr}(\chi^{-1}(\sigma))\sigma \ \in \ \mathbb{Z}_\ell[\Delta_n]$$

とおく。Tr は $\mathbb{Q}_\ell(\chi(\Delta_n))$ から $\mathbb{Q}_\ell$ への trace である。A_n の χ-part が $A_{n,\chi} = e_\chi A_n$ で定義され、A_n は

$$A_n = \oplus_\chi A_{n,\chi}$$

と直和分解される。ただし χ は $\mathbb{Q}_\ell$ 共役類の代表を動く。従って $\ell \nmid |A_n|$ を確かめるには、全ての χ について $\ell \nmid |A_{n,\chi}|$ を確かめればよい。χ が単射でなければ $\mathrm{Ker}\chi$ に対応する Ω_n の部分体 Ω_k に対し、自然に $A_{n,\chi} \cong A_{k,\chi}$ となる。よって χ が単射の時に $\ell \nmid |A_{n,\chi}|$ を確かめることができればよい。

$\zeta_{n+2} \in \mathbb{C}$ を 1 の原始 2^{n+2} 乗根とし

$$\xi_n = (\zeta_{n+2} - 1)(\zeta_{n+2}^{-1} - 1) = 2 - \zeta_{n+2} - \zeta_{n+2}^{-1} \in \Omega_n$$

とおく。$e_{\chi,\ell} = \sum_{\sigma \in \Delta_n} a_\sigma \sigma \in \mathbb{Z}[\Delta_n]$ s.t. $e_{\chi,\ell} \equiv e_\chi \pmod{\ell}$ を作ると、$e_{\chi,\ell}$ を ξ_n に作用させることができる。$e_{\chi,\ell}$ の取り方は何通りもあるが、$\sum_\sigma a_\sigma = 0$ になるようにとれば $\xi_n^{e_{\chi,\ell}}$ は Ω_n の単数になる。いわゆる円単数である。ξ_n を用いて $|A_{n,\chi}|$ を記述できる。$|A_{n,\chi}|$ が ℓ で割れることを示すのは難しいが、割れないことを示すのは易しい。次の補題はより精密な Gras 予想の一部であり、Gras 予想は、Mazur-Wiles によって証明された岩澤主予想の帰結として、肯定的に解決された (cf. [6], [7], [16], [2, Lemma 1])。これを使うときは $\sum_\sigma a_\sigma = 0$ でなくてもよい。

補題 1.4. p を $p \equiv 1 \pmod{2^{n+2}\ell}$ である素数とする。p の上にある Ω_n の適当な素イデアル $\mathfrak{p}$ に対して

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{\mathfrak{p}} \tag{1}$$

となれば $|A_{n,\chi}| = 1$ である。

$\overline{\mathbb{F}}_\ell$ を $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ の代数閉包とする。$\varepsilon_{\chi,\ell}$ を考えるのだから $\chi : \Delta_n \longrightarrow \overline{\mathbb{F}}_\ell^\times$ としてよい。$\eta_n \in \overline{\mathbb{F}}_\ell$ を 1 の原始 2^n 乗根、$K = \mathbb{F}_\ell(\eta_n)$ とし Δ_n の生成元 ρ を $\zeta_{n+2}^\rho = \zeta_{n+2}^5$ で定める。$\chi(\rho) = \eta_n^{-1}$ で定まる χ は Δ_n の指標群を生成し、

$$e_{\chi^j} = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{ij})\rho^i \in \mathbb{F}_\ell[\Delta_n]\,.$$

p を $p \equiv 1 \pmod{2^{n+2}\ell}$ をみたす素数とし、g_p を p の原始根とする。p は $\Omega_n/\mathbb{Q}$ で完全分解するから、p の上にある Ω_n の適当な素イデアル $\mathfrak{p}$ に対し、

$$\zeta_{n+2} \equiv g_p^{\frac{p-1}{2^{n+2}}} \pmod{\mathfrak{p}}\,.$$

従って $e_{\chi^j} = \sum_i a_{ij}\rho^i$ の時

$$\begin{aligned}\xi_n^{e_{\chi^j}} &= \prod_{i=0}^{2^n-1} \left(2-\zeta_{n+2}-\zeta_{n+2}^{-1}\right)^{a_{ij}\rho^i} \\ &= \prod_{i=0}^{2^n-1} \left(2-\zeta_{n+2}^{5^i}-\zeta_{n+2}^{-5^i}\right)^{a_{ij}} \\ &\equiv \prod_{i=0}^{2^n-1} \left(2-g_p^{\frac{p-1}{2^{n+2}}5^i}-g_p^{-\frac{p-1}{2^{n+2}}5^i}\right)^{a_{ij}} \pmod{\mathfrak{p}}\end{aligned}$$

となり、最後の積は $\bmod p$ で計算すればよい。

$$\begin{cases} 2^s \mid\mid \ell-1 & \text{if } \ell \equiv 1 \pmod 4 \\ 2^s \mid\mid \ell+1 & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

で $s \in \mathbb{Z}$ を決める。合同式 (1) を用いて $\ell \nmid h_n$ を確かめる方法を四つの場合にわけて説明する。$h_1 = 1$ だから $n \geq 2$ としてよい。

$p \equiv 1 \pmod{2^{n+2}\ell}$ をみたす素数 p および p の原始根 g_p に対し $z_1, z_2 \in \mathbb{Z}$ を

$$\begin{aligned} z_1 &\equiv g_p^{\frac{p-1}{2^{n+2}}} \pmod p \\ z_2 &\equiv z_1^{-1} \pmod p \end{aligned}$$

で決めておく。

1.2. $\ell \equiv 1 \pmod 4$, $2 \leq n \leq s$ **の場合.** $[K : \mathbb{F}_\ell] = 1$ であり $\eta_n \in \mathbb{F}_\ell$. 従って $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n) = \eta_n$ で

$$e_{\chi^j} = \frac{1}{2^n}\sum_{i=0}^{2^n-1} \eta_n^{ij}\rho^i \,.$$

g_ℓ を ℓ の原始根とすると、

$$\eta_n \equiv g_\ell^{\frac{\ell-1}{2^n}} \pmod \ell$$

と思ってよい。従って $a_{ij} \in \mathbb{Z}$ を

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{2^n}ij} \pmod \ell$$

で定めれば $e_{\chi^j} = (1/2^n)\sum_i a_{ij}\rho^i$. 補題 1.4 を使う時 $1/2^n$ は無視してよい。

$X = \{\, j \in \mathbb{Z} \mid 1 < j < 2^n :\ \text{odd} \,\}$ とおくと $\{\, \chi^j \mid j \in X \,\}$ が Δ_n の単射指標の全体であり、それらは $\mathbb{F}_\ell$ 上共役でない。従って補題 1.4 は次の形になる。

判定法 1. $b = 5$ とおく。全ての $j \in X$ に対し、$p \equiv 1 \pmod{2^{n+2}\ell}$ および

$$\left(\prod_{i=0}^{2^n-1}(2-z_1^{b^i}-z_2^{b^i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p$$

をみたす素数 p が存在すれば、$\ell \nmid h_n/h_{n-1}$ である。

1.3. $\ell \equiv 1 \pmod 4$, $n \geq s+1$ **の場合.** $[K:\mathbb{F}_\ell] = 2^{n-s}$ であり、η_n の $\mathbb{F}_\ell$ 上の最小多項式は

$$X^{2^{n-s}} - \eta_n^{2^{n-s}}\,.$$

従って $2^{n-s} \nmid i$ なら $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i) = 0$ であり、

$$\begin{aligned} e_{\chi^j} &= \frac{1}{2^n}\sum_{i=0}^{2^s-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{2^{n-s}ij})\rho^{2^{n-s}i} \\ &= \frac{1}{2^s}\sum_{i=0}^{2^s-1} \eta_s^{ij}\,\rho^{2^{n-s}i}\,. \end{aligned}$$

$\overline{\mathbb{F}}_\ell$ の中に 1 の原始 2^n 乗根は 2^{n-1} 個あるが、$\mathbb{F}_\ell$ 上共役でないものは 2^{s-1} 個あり、それらが Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類に対応する。$\ell \equiv 1 \pmod{2^s}$ に注意すると、

$$\begin{aligned} \chi^i \text{ と } \chi^j \text{ が } \mathbb{F}_\ell \text{ 上共役} &\iff \eta_n^i = \eta_n^{j\ell^m} \quad \exists\, m \\ &\iff i \equiv j\ell^m \pmod{2^n} \\ &\implies i \equiv j\ell^m \pmod{2^s} \\ &\implies i \equiv j \pmod{2^s} \end{aligned}$$

だから、

$$X = \{\, j \in \mathbb{Z} \mid 1 \leq j \leq 2^s - 1 :\ \text{odd} \,\}$$

とおけば $\{\, \chi^j \mid j \in X \,\}$ が Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類の代表になる。

g_ℓ を ℓ の原始根とし、$a_{ij} \in \mathbb{Z}$ を

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{2^s}ij} \pmod{\ell}$$

で定める。補題 1.4 は次の形になる。

判定法 2. $b = 5^{2^{n-s}}$ とおく。全ての $j \in X$ に対し、$p \equiv 1 \pmod{2^{n+2}\ell}$ および

$$\left(\prod_{i=0}^{2^s-1}(2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p$$

をみたす素数 p が存在すれば、$\ell \nmid h_n/h_{n-1}$ である。

1.4. $\ell \equiv 3 \pmod 4$, $2 \leq n \leq s$ **の場合.** $[K:\mathbb{F}_\ell] = 2$ であり、η_n の $\mathbb{F}_\ell$ 上の最小多項式は

$$X^2 - aX + 1$$

の形 (この形であることは使わないが一応書いておく)。

$$e_{\chi^j} = \frac{1}{2^n}\sum_{i=0}^{2^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{ij})\rho^i\,.$$

$\overline{\mathbb{F}}_\ell$ の中に 1 の原始 2^n 乗根は 2^{n-1} 個あるが、$\mathbb{F}_\ell$ 上共役でないものは 2^{n-2} 個あり、それらが Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類に対応する。$\ell \equiv -1 \pmod{2^n}$ に注意すると

$$\begin{aligned} \chi^i \text{ と } \chi^j \text{ が } \mathbb{F}_\ell \text{ 上共役} &\iff \eta_n^i = \eta_n^j \text{ or } \eta_n^i = \eta_n^{j\ell} \\ &\iff i \equiv j \pmod{2^n} \text{ or } i \equiv j\ell \pmod{2^n} \\ &\iff i \equiv \pm j \pmod{2^n}\,. \end{aligned}$$

従って

$$X = \{\, j \in \mathbb{Z} \mid 1 \leq j \leq 2^{n-1} - 1 :\ \text{odd} \,\}$$

とおけば $\{\chi^j \mid j \in X\}$ が Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類の代表になる。

§1.5 (2) の t_i を用いて

$$a_{ij} = t_{2^{s+1-n}ij}$$

とおくと、補題 1.4 は次の形になる。

判定法 3. $b = 5$ とおく。全ての $j \in X$ に対し、$p \equiv 1 \pmod{2^{n+2}\ell}$ および

$$\left(\prod_{i=0}^{2^n-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p}$$

をみたす素数 p が存在すれば、$\ell \nmid h_n/h_{n-1}$ である。

1.5. $\ell \equiv 3 \pmod 4$, $n \geq s+1$ **の場合.** $[K : \mathbb{F}_\ell] = 2^{n-s}$ であり、η_{s+1} の $\mathbb{F}_\ell$ 上の最小多項式は

$$X^2 - aX - 1$$

の形。この時 η_n の最小多項式は

$$X^{2^{n-s}} - aX^{2^{n-s-1}} - 1$$

であり、$2^{n-s-1} \nmid i$ なら $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i) = 0$ となる。従って、

$$\begin{aligned} e_{\chi^j} &= \frac{1}{2^n} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{2^{n-s-1}ij})\, \rho^{2^{n-s-1}i} \\ &= \frac{1}{2^{s+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{ij})\, \rho^{2^{n-s-1}i} \end{aligned}$$

となり、

$$t_i = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i) \tag{2}$$

を求めなければならない。まず $t_1 = \eta_{s+1} + \eta_{s+1}^\ell$ を次の漸化式で計算する。

補題 1.5. $a_2 = 0$ とし、$a_i \in \mathbb{F}_\ell$ $(3 \leq i \leq s+1)$ を

$$\begin{aligned} a_i &= \sqrt{2 + a_{i-1}} \quad (3 \leq i \leq s) \\ a_{s+1} &= \sqrt{-2 + a_s}\,. \end{aligned}$$

で定義すると、$t_1 = a_{s+1}$.

Proof. $\eta_{s+1}^{\ell+1} = -1$ に注意すると、

$$\begin{aligned} t_2 &= \eta_{s+1}^2 + \eta_{s+1}^{2\ell} = (\eta_{s+1} + \eta_{s+1}^\ell)^2 - 2\eta_{s+1}^{\ell+1} = t_1^2 + 2 \\ t_{2^2} &= \eta_{s+1}^{2^2} + \eta_{s+1}^{2^2\ell} = (\eta_{s+1}^2 + \eta_{s+1}^{2\ell})^2 - 2\eta_{s+1}^{2(\ell+1)} = t_2^2 - 2 \\ &\vdots \\ t_{2^{s-1}} &= \eta_{s+1}^{2^{s-1}} + \eta_{s+1}^{2^{s-1}\ell} = t_{2^{s-2}}^2 - 2 = 0\,. \end{aligned}$$

これを逆にたどればよい。 □

注意 . 各ステップで平方根が二つ現れるので t_1 は 2^{s-1} 個求まることになる。これらは $\overline{\mathbb{F}}_\ell$ に含まれる 1 の原始 2^{s+1} 乗根で $\mathbb{F}_\ell$ 上共役でないもの (2^{s-1} 個ある) に対応している。任意の t_1 を一つ固定すればよい。t_1 を動かすことで χ の共役を作ってもよいが、χ^j を考える方がプログラムが簡単になる。

t_1 がわかれば t_i $(i \geq 2)$ は次の漸化式で計算できる。

補題 1.6. $t_{i+2} = t_1 t_{i+1} + t_i \quad (i \geq 0)$.

Proof.

$$\begin{aligned} t_1 t_{i+1} &= (\eta_{s+1} + \eta_{s+1}^{\ell})(\eta_{s+1}^{i+1} + \eta_{s+1}^{(i+1)\ell}) \\ &= \eta_{s+1}^{i+2} + \eta_{s+1}^{(i+2)\ell} + \eta_{s+1}^{\ell+1}(\eta_{s+1}^{i} + \eta_{s+1}^{i\ell}) \\ &= t_{i+2} - t_i \,. \end{aligned}$$

□

$\overline{\mathbb{F}}_\ell$ の中に 1 の原始 2^n 乗根は 2^{n-1} 個あるが、$\mathbb{F}_\ell$ 上共役でないものは 2^{s-1} 個あり、それらが Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類に対応する。$\ell \equiv 2^s - 1 \pmod{2^{s+1}}$ に注意すると

$$\begin{aligned} \chi^i \text{ と } \chi^j \text{ が } \mathbb{F}_\ell \text{ 上共役} &\iff \eta_n^i = \eta_n^j \text{ or } \eta_n^i = \eta_n^{j\ell} \\ &\iff i \equiv j \pmod{2^n} \text{ or } i \equiv j\ell \pmod{2^n} \\ &\implies i \equiv j \pmod{2^{s+1}} \text{ or } i \equiv j\ell \pmod{2^{s+1}} \\ &\implies i \equiv j \pmod{2^{s+1}} \text{ or } i \equiv j(2^s - 1) \pmod{2^{s+1}} . \end{aligned}$$

従って

$$X = \{\, j \in \mathbb{Z} : \text{ odd } \mid 1 \leq j \leq 2^{s-1} \text{ or } 2^s + 1 \leq j \leq 2^s + 2^{s-1} - 1 \,\}$$

とおくと、$\{\, \chi^j \mid j \in X \,\}$ は Δ_n の単射指標の $\mathbb{F}_\ell$ 共役類の代表。

$a_{ij} \in \mathbb{Z}$ を

$$a_{ij} \equiv t_{ij} \pmod{\ell}$$

で定義する。t_{ij} の ij は i と j の積である。補題 1.4 は次の形になる。

判定法 4. $b = 5^{2^{n-s-1}}$ とおく。全ての $j \in X$ に対し、$p \equiv 1 \pmod{2^{n+2}\ell}$ および

$$\left(\prod_{i=0}^{2^{s+1}-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p} \tag{3}$$

をみたす素数 p が存在すれば、$\ell \nmid h_n / h_{n-1}$ である。

1.6. **対数版アルゴリズム.** 判定法 1-4 の計算量は ℓ を固定して n を動かす時は $O(n)$ である。例えば Pentium IV 2GHz では 22 分で $3 \nmid h_{1000}$ を確かめることができ、十分に速い。

一方 n を固定して ℓ を動かす時は $O(4^s)$、$\ell^2 - 1$ が 2 の高い巾で割れるような ℓ に対しては大雑把に言って $O(\ell^2)$ である。$\ell = 2^{16} + 1 = 65537$ に対しては $m = 87$ であり、$\ell \nmid h_{87}$ を確かめようとすると 40 日ほどかかる。非現実的な時間ではないが、もう少し速い方法が望まれる。

そこで青木のアルゴリズム [1, Corollary 11] を使うことにする。離散対数関数 $\nu_p : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ を

$$x = g_p^{\nu_p(x)}$$

で定義する。$\ell = 65537$, $n = 87$ に対しては $p \simeq 10^{33}$ 程度であり、$\nu_p(x)$ の計算は難しいと考えられている (Diffie-Hellman 暗号の根拠)。index calculus による準指数時間アルゴリズムもあるが、我々の目的には $\nu_p(x) \bmod \ell$ で十分であるので、$\nu_p(x) = i + j\ell$ をみたす i を

$$x^{\frac{p-1}{\ell}} = \left(g_p^{i+j\ell} \right)^{\frac{p-1}{\ell}} = \left(g_p^{\frac{p-1}{\ell}} \right)^i \tag{4}$$

により決めればよい。$\ell < 10^5$ であれば $0 \le i \le \ell - 1$ に対し (4) の右辺の表を作り、表引きすればよい。従って

$$x_i \equiv \nu_p(2 - z_1^{b^i} - z_2^{b^i}) \pmod{\ell}. \tag{5}$$

をみたす $x_i \in \mathbb{Z}$ は十分高速に計算可能である。

$$c = \begin{cases} n & 2 \le n \le s \\ s & n \ge s+1\,,\ \ell \equiv 1 \pmod 4 \\ s+1 & n \ge s+1\,,\ \ell \equiv 3 \pmod 4 \end{cases}$$

とすれば、判定法 1-4 は次の形に変形できる。

判定法 5. 全ての $j \in X$ に対し、$p \equiv 1 \pmod{2^{n+2}\ell}$ および

$$\sum_{i=0}^{2^c-1} a_{ij} x_i \not\equiv 0 \pmod{\ell} \tag{6}$$

をみたす素数 p が存在すれば、$\ell \nmid h_n/h_{n-1}$ である。

判定法 5 は二つの特徴をもつ。

- 単純な演算のみ　(巾乗が積に変わった)
- $0 \le a_{ij}, x_i < \ell$　($\ell < 10^5$ なら多倍長演算は必要なし)

x_i を求めるオーバーヘッドはあるものの、それを補って余りある。小さい s (e.g. $s < 8$) に対しては判定法 1-4 を、大きい s (e.g. $s \ge 8$) に対しては 判定法 5 を使うとよい。これにより $65537 \nmid h_{87}$ の確認が 10 時間、系 1.3 の導出が 20 時間でできた。

1.7. 実装上の注意.

1.7.1. a_{ij} は見掛け上二重添字だが、実質的には一重である。$\ell \equiv 1 \pmod 4$ の時は

$$A[\,i\,] \equiv g_\ell^{\frac{\ell-1}{2^s} i} \pmod{\ell}, \quad 0 \le i \le 2^s - 1$$

の表を作り、

$$a_{ij} = \begin{cases} A[\,2^{s-n} ij \bmod 2^s\,] & \text{if } 2 \le n \le s \\ A[\,ij \bmod 2^s\,] & \text{if } n \ge s+1 \end{cases}$$

とする。$\ell \equiv 3 \pmod 4$ の時は

$$T[\,i\,] = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i), \quad 0 \le i \le 2^{s+1} - 1$$

の表を作り、

$$a_{ij} = \begin{cases} T[\,2^{s+1-n} ij \bmod 2^{s+1}\,] & \text{if } 2 \le n \le s \\ T[\,ij \bmod 2^{s+1}\,] & \text{if } n \ge s+1 \end{cases}$$

とする。

$$\mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{2^s+i}) = -\mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i)$$

に注意して

$$A[\,i\,] = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i), \quad 0 \le i \le 2^s - 1$$

を作り、

$$T[\,i\,] = \begin{cases} A[\,i\,] & \text{if } 0 \le i \le 2^s - 1 \\ -A[\,i - 2^s\,] & \text{if } 2^s \le i \le 2^{s+1} - 1 \end{cases}$$

とすれば、メモリと時間を半分にできる。しかしこの部分は dominant part ではないので、あまり効果はない。系 1.3 の範囲を $\ell < 10^6$ に広げる時は有効かもしれない。

$A[i]$ は ℓ のみに依存するので一度だけ計算して表を作っておけば、n, p, $j \in X$ を動かしても共通に使える。

1.7.2. 判定法 1-4 は $j \in X$ に対して $p = p_j$ を捜せばよいのだが、大部分の j に対して共通の p が使える。p を与え、それから j を動かすのがよい。そうすれば $2 - z_1^{b^i} - z_2^{b^i}$ は j に依らないので一度だけ計算して表を作っておける。

1.7.3. $\ell \equiv 3 \pmod 4$, $n \geq s+1$ の時、$i' = 2^s + i$ とおけば、

$$b^{i'} = 5^{2^{n-s-1}(2^s+i)} = 5^{2^{n-1}} b^i \equiv (2^{n+1}+1) b^i \pmod{2^{n+2}}$$

$$z_1^{b^{i'}} \equiv g_p^{\frac{p-1}{2^{n+2}}(2^{n+1}+1)b^i} \equiv g_p^{\frac{p-1}{2}} z_1^{b^i} \equiv -z_1^{b^i} \pmod p$$

$$a_{i'j} = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{(2^s+i)j}) = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{2^s j}\eta_{s+1}^{ij}) = -a_{ij}$$

だから、判定法 4 の (3) は

$$\Big(\prod_{i=0}^{2^s-1} \Big(\frac{2 - z_1^{b^i} - z_2^{b^i}}{2 + z_1^{b^i} + z_2^{b^i}} \Big)^{a_{ij}} \Big)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p$$

と変形できる。s がある程度大きければ、これで少し速くなる。乗算の数が半分になった代わりに除算が現れたので、効果が打ち消されるような気がするが、商の部分は j を動かす前に一度だけ計算して表を作っておけばよいので、オーバーヘッドはあまりない。

1.7.4. (5) の x_i はもちろん表引きで求めるが、$0 \leq i < 2^s < \ell$ なのでクイックソートの最も簡単な実装と 2 分探索で十分である。2^s と ℓ が大きく離れている場合は無駄が生じるが、$\ell < 10^5$ であればさほど問題にはならない。

1.7.5. 判定法 1-4 に現れる p は数十桁の数だから、多倍長演算を実装した対話型ソフトを使えばプログラミングが楽になる。しかし判定法 5 の (6) に現れる数は ℓ 以下であるから、例えば $\ell < 10^5$ なら多倍長演算は必要ない。ここは C で書くことにより一層の高速化を図ることができる。多倍長 C 言語インタープリタ TC は、TC の中から C プログラムを実行することができ、データのやりとりもできるので、この用途には向いている。

1.8. **Fourier 変換.** 判定法 5 は判定法 1-4 より高速であるが、依然 $O(4^s)$ アルゴリズムである。系 1.3 を $\ell < 10^6$ に伸ばそうとすると 1 年程かかりそうである。計算機を 10 台使えば 1 月だから、決して不可能なことではないが、実行する前にアルゴリズムを吟味すべきである。実際、$\ell \equiv 1 \pmod 4$ の時は $a_{ij} = \eta_s^{ij}$ であり、$j = 2r+1$ とおくと (6) は

$$\sum_i a_{ij} x_i \quad = \quad \sum_i \eta_s^{i(2r+1)} x_i = \eta_s^{r^2} \sum_i \eta_s^{-(r-i)^2} \eta_s^{i(i+1)} x_i$$

と変形できる。これは $u_i = \eta_s^{-i^2}$ と $v_i = \eta_s^{i(i+1)} x_i$ の convolution であり、FFT を使えば $O(\log_2(2^s)2^s) = O(s2^s)$ で計算できる。$\ell \equiv 3 \pmod 4$ の時もやや面倒になるが同じ原理が使える。FFT は古くから知られているが、整数論では隅田 [17] が Gauss 和の計算に用いたのが初めてではないかと思う。研究集会では修士論文に適当なテーマとして紹介したのであるが、誰も実行する気配がないので我々がやっておく。以下に具体的な実装法を解説する。

1.8.1. $\ell \equiv 1 \pmod 4$, $n \geq s+1$ の場合. $\eta_s^{r^2} \not\equiv 0 \pmod \ell$ だから

$$\sum_{i=0}^{2^s-1} \eta_s^{-(r-i)^2} \eta_s^{i(i+1)} x_i \in \mathbb{F}_\ell \tag{7}$$

を求めればよい。従って

$$\begin{aligned} u_i &= \eta_s^{-i^2} \qquad (0 \leq i \leq 2^s-1) \\ v_i &= \eta_s^{i(i+1)} x_i \quad (0 \leq i \leq 2^s-1) \end{aligned}$$

とおき、

$$w_r = \sum_{i=0}^{2^s-1} u_{r-i} v_i \quad (0 \leq r \leq 2^s-1)$$

を求め、$w_r \neq 0$ $(0 \leq r \leq 2^{s-1}-1)$ を確かめればよい。必要なのは w_r $(0 \leq r \leq 2^{s-1}-1)$ であるが、この部分のみを高速に求める方法はない (と思う)。$2 \leq n \leq s$ の時も同様にできる。

注意 . u_{r-i} の $r-i$ は $\bmod 2^s$ で考えなければならないが、$-(2^s+r-i)^2 \equiv -(r-i)^2 \pmod{2^s}$ だから (7) と矛盾しない。

1.8.2. $\ell \equiv 3 \pmod 4$, $n \geq s+1$ の場合. 1.7.3 に注意して $j = 2r+1$ とおくと (6) は

$$\begin{aligned} \sum_{i=0}^{2^s-1} a_{ij} x_i &= \sum_{i=0}^{2^s-1} (\eta_{s+1}^{ij} + \eta_{s+1}^{ij\ell}) x_i \\ &= \sum_{i=0}^{2^s-1} (\eta_{s+1}^{ij} x_i + \eta_{s+1}^{ij\ell} x_i^\ell) \\ &= \sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i + \Big(\sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i \Big)^\ell \\ &= \mathrm{Tr}\Big(\sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i \Big) \\ &= \mathrm{Tr}\Big(\eta_{s+1}^{r^2} \sum_{i=0}^{2^s-1} \eta_{s+1}^{-(r-i)^2} \eta_{s+1}^{i(i+1)} x_i \Big) \end{aligned}$$

と変形できる。まず $\eta_{s+1}^i = a_i + b_i \eta_{s+1}$ $(a_i, b_i \in \mathbb{F}_\ell,\ 0 \leq i \leq 2^{s+1}-1)$ の表を次の漸化式により作る。

補題 1.7. $a_0 = 1,\ b_0 = 0.\ a_{i+1} = b_i,\ b_{i+1} = a_i + t_1 b_i \quad (i \geq 0).$

Proof. $a_{i+1} + b_{i+1}\eta_{s+1} = (a_i + b_i\eta_{s+1})\eta_{s+1} = a_i\eta_{s+1} + b_i(1 + t_1\eta_{s+1}) = b_i + (a_i + t_1 b_i)\eta_{s+1}.$ □

次に FFT の準備をする。つまり

$$\begin{aligned} A_i &= a_{-i^2} \qquad \in \mathbb{F}_\ell \quad (0 \leq i \leq 2^s-1) \\ B_i &= a_{i+i^2} x_i \quad \in \mathbb{F}_\ell \quad (0 \leq i \leq 2^s-1) \\ C_i &= b_{-i^2} \qquad \in \mathbb{F}_\ell \quad (0 \leq i \leq 2^s-1) \\ D_i &= b_{i+i^2} x_i \quad \in \mathbb{F}_\ell \quad (0 \leq i \leq 2^s-1) \end{aligned}$$

を作る。右辺の添字は $\bmod 2^{s+1}$ で考える。4 種類の cyclic convolution

$$\begin{aligned} X_r &= \sum_{i=0}^{2^s-1} A_{r-i}B_i \quad \in \mathbb{F}_\ell \quad (0 \le r \le 2^s-1) \\ Y_r &= \sum_{i=0}^{2^s-1} A_{r-i}D_i \quad \in \mathbb{F}_\ell \quad (0 \le r \le 2^s-1) \\ Z_r &= \sum_{i=0}^{2^s-1} C_{r-i}B_i \quad \in \mathbb{F}_\ell \quad (0 \le r \le 2^s-1) \\ W_r &= \sum_{i=0}^{2^s-1} C_{r-i}D_i \quad \in \mathbb{F}_\ell \quad (0 \le r \le 2^s-1) \end{aligned}$$

は $O(s2^s)$ で計算でき、

$$\begin{aligned} \sum_{i=0}^{2^s-1} \eta_{s+1}^{-(r-i)^2} \eta_{s+1}^{i(i+1)} x_i &= \sum_{i=0}^{2^s-1} (A_{r-i} + C_{r-i}\eta_{s+1})(B_i + D_i\eta_{s+1}) \\ &= \sum_{i=0}^{2^s-1} (A_{r-i}B_i + (A_{r-i}D_i + C_{r-i}B_i)\eta_{s+1} + C_{r-i}D_i(1+t_1\eta_{s+1}) \\ &= X_r + W_r + (Y_r + Z_r + t_1W_r)\eta_{s+1} \end{aligned}$$

となる。A_{r-i}, C_{r-i} の $r-i$ は $\bmod 2^{s+1}$ で考えてよいが、convolution にするには $\bmod 2^s$ で考えなければならない。しかし $(2^s+i)^2 = 2^{2s} + 2^{s+1}i + i^2 \equiv i^2 \pmod{2^{s+1}}$ だから、これは確かに convolution になる。

従って

$$\eta_{s+1}^{r^2} \sum_{i=0}^{2^s-1} \eta_{s+1}^{-(r-i)^2} \eta_{s+1}^{i(i+1)} x_i = E_r + F_r\eta_{s+1} \quad (E_r, F_r \in \mathbb{F}_\ell,\ 0 \le r \le 2^s-1)$$

は $O(s2^s)$ で計算でき、

$$w_r = \sum_{i=0}^{2^s-1} a_{ij}x_i = E_r + F_r\eta_{s+1} + (E_r + F_r\eta_{s+1})^\ell = 2E_r + t_1F_r \quad (0 \le r \le 2^s-1)$$

も $O(s2^s)$ で計算できることになる。$0 \le r \le 2^{s-2}-1$, $2^{s-1} \le r \le s^{s-1} + 2^{s-2} - 1$ の 2^{s-1} 個の r に対して $w_r \ne 0$ を確かめればよい。

$2 \le n \le s$ の時は $a_{ij} = \eta_n^{ij} + \eta_n^{il\ell} = \eta_{s+1}^{2^{s+1-n}ij} + \eta_{s+1}^{2^{s+1-n}ij\ell}$ に注意すれば、長さ 2^n の convolution になる。

1.8.3. *convolution* の計算. convolution は多倍長乗算と関係している。K 個の非負整数の組

$$\begin{aligned} u_i \quad & (0 \le i \le K-1) \\ v_i \quad & (0 \le i \le K-1) \end{aligned}$$

から、K 個の整数

$$w_r = \sum_{i=0}^{K-1} u_{r-i}v_i \quad (0 \le r \le K-1)$$

を作りたい。ただし $r-i$ は $\bmod K$ で考える。

計算機の 1 語長を N とし、

$$X = 2^{kN} > K \cdot \max\{u_i \mid 0 \le i \le K-1\} \cdot \max\{v_i \mid 0 \le i \le K-1\} \tag{8}$$

となるように基数 X をとり、多倍長数

$$\begin{aligned} U &= \sum_{i=0}^{K-1} u_i X^i \\ V &= \sum_{i=0}^{K-1} v_i X^i \end{aligned}$$

を考える。FFT を使えば

$$UV = \Big(\sum_{i=0}^{K-1} u_i X^i\Big)\Big(\sum_{j=0}^{K-1} v_j X^i\Big) = \sum_{k=0}^{2K-2}\Big(\sum_{i+j=k} u_i v_j\Big)X^k$$

は $O(K \log_2 K \log_2 \log_2 K)$ で計算でき、(8) より

$$0 \le a_k = \sum_{i+j=k} u_i v_j < X$$

である。従って a_k $(0 \le k \le 2K-2)$ も $O(K \log_2 K \log_2 \log_2 K)$ で計算できる。

$$\begin{aligned} w_0 &= u_0v_0 + u_{K-1}v_1 + \cdots + u_1v_{K-1} = a_0 + a_K \\ w_1 &= u_1v_0 + u_0v_1 + u_{K-1}v_2 + \cdots + u_2v_{K-1} = a_1 + a_{K+1} \\ &\vdots \\ w_{K-2} &= u_{K-2}v_0 + \cdots + u_0v_{K-2} + u_{K-1}v_{K-1} = a_{K-2} + a_{2K-2} \\ w_{K-1} &= u_{K-1}v_0 + \cdots + u_0v_{K-1} = a_{K-1} \end{aligned}$$

となるから、$a_{2K-1} = 0$ としておけば

$$w_r = a_r + a_{K+r} \quad (0 \le r \le K-1)$$

も $O(K \log_2 K \log_2 \log_2 K)$ で計算できる。

TC には GMP の多倍長乗算を利用した簡易 convolution 関数が組み込まれている。本来は convolution を利用して多倍長乗算を高速化するのであるからこれは本末転倒であるが、この用途には十分高速である。$\ell \nmid h_n/h_{n-1}$ を確かめる時の主要部分は次のようになる。

(1) $2 - z_1^{b^i} - z_2^{b^i}$ $(0 \le i \le 2^s - 1)$ の計算

(2_a) $\big(g_p^{\frac{p-1}{\ell}}\big)^i$ $(0 \le i \le \ell - 1)$ の計算

(2_b) $\big(g_p^{\frac{p-1}{\ell}}\big)^i$ $(0 \le i \le \ell - 1)$ のソート

(2_c) $\nu_p(2 - z_1^{b^i} - z_2^{b^i})$ $(0 \le i \le 2^s - 1)$ の計算

(3_a) convolution の準備

(3_b) convolution の実行

(3_b) convolution 後の処理

代表的な (ℓ, n) に対する Pentium IV 2GHz での計算時間 (秒) は次の通り。n が大きくなると $(1), (2_c)$ が遅くなるのは $\bmod p$ での巾乗計算に時間がかかるようになるからである。

AC2007 145

ℓ	s	n	(1)	(2_a)	(2_b)	(2_c)	(3_a)	(3_b)	(3_c)
131071	17	17	0.88	0.22	0.44	1.15	2.23	2.99	1.60
131071	17	95	5.11	0.26	0.43	3.45	1.97	3.01	1.66
786431	18	18	1.75	1.33	3.39	2.48	4.56	7.08	3.10
786431	18	103	14.02	1.65	3.69	10.06	3.99	7.10	3.11
524287	19	19	3.50	0.87	2.09	5.28	9.08	14.85	6.46
524287	19	106	27.77	1.10	2.32	21.00	7.98	15.11	6.64

系 1.8 は 50 時間で、系 1.9 は計算機を 3 台使って 2 週間で確認することができた。

系 1.8. $10^5 < \ell < 10^6$: 素数 $\Longrightarrow \forall\, n \geq 1 \quad \ell \not| \, h_n$

系 1.9. $10^6 < \ell < 10^7$: 素数 $\Longrightarrow \forall\, n \geq 1 \quad \ell \not| \, h_n$

References

[1] M. Aoki, *Notes on the Structure of the Ideal Class Groups of Abelian Number Fields*, Tokyo Metropolitan Univ. Math. Preprint Series, No.18, 2002.

[2] M. Aoki and T. Fukuda, *An algorithm for computing p-class groups of abelian number fields*, Algorithmic Number Theory, 56–71, Lecture Notes in Computer Science, vol. 4076, Springer, Berlin, 2006.

[3] H. Bauer, *Numeriche Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper*, J. Number Theory, **1** (1969), 161–162.

[4] H. Cohn, *A numerical study of Weber's real class number calculation I*, Numer. Math. **2** (1960), 347–362.

[5] T. Fukuda and K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, preprint, 2007.

[6] G. Gras, *Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés*, Ann. Inst. Fourier, **27** (1977), 1–66.

[7] R. Greenberg, *On p-adic L-functions and cyclotomic fields II*, Nagoya Math. J. **67** (1977), 139–158.

[8] K. Horie, *Ideal class groups of Iwasawa-theoritical abelian extensions over the rational field*, J. London Math. Soc., **66** (2002), 257–275.

[9] K. Horie, *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field*, Tohoku Math. J., **57** (2005), 375–394.

[10] K. Horie, *Triviality in ideal class groups of Iwasawa-theoretical abelian number fields*, J. Math. Soc. Japan, **57** (2005), 827–857.

[11] K. Horie, *Primary components of the ideal class groups of Iwasawa-theoretical abelian number field*, J. Math. Soc. Japan, **59** (2007), 811–824.

[12] K. Horie, *Certain primary components of the ideal class group of the $\mathbb{Z}_p$-extension oer the rationals*, Tohoku Math. J., **59** (2007), 259–291.

[13] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257–258.

[14] F. J. van der Linden, *Class Number Computations of Real Abelian Number Fields*, Math. Comp. **39** (1982), 693–707.

[15] , J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), 297–319.

[16] B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. math. **76** (1984), 179–330.

[17] H. Sumida, *Computation of Iwasawa invariants of certain real abelian fields*, J. Number Theory, **105** (2004), 235–250.

[18] L. C. Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. **214** (1975), 177–193.

[19] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math., 83, Springer-Verlag, New York, Heidelberg, Berlin, 1997.

[20] H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Math., **8** (1886), 193–263.

[21] H. Weber, *Lehrbuch der Algebra*, vol. 2, 3rd ed., Chelsea, 1961.

Department of Mathematical Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan
E-mail address: kkomatsu@waseda.jp

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
E-mail address: fukuda@math.cit.nihon-u.ac.jp

A Note on Computation of $W(3,4)$ Sets

MATSUI Tetsushi
tetsushi@tnt.math.metro-u.ac.jp

March 17, 2008

1 Notations and Terminology

This note is written by R. Morikawa's request, for supporting his exposition [3]. In the first section, we shall settle definitions, notations and terminology, which follow the same conventions with him. Then in section 2, we shall explain how computation is carried out, followed by its result in section 3. The final section shall randomly note about the result of computation.

Let $\mathbb{N}$ denote the set of *positive* integers.

The main target of this note is called $W(3,4)$ sets. $W(k,m)$ denotes a family of sets

$$W_k(a_1,\ldots,a_m)=\left\{ n\in\mathbb{N} \;\middle|\; \forall(x_1,\ldots,x_m)\in\mathbb{N}^m\ n\neq\sum_{i=1}^m a_i x_i^k \right\},$$

with parameters $(a_1,\ldots,a_m)\in\mathbb{N}^m$. That is, $W_k(a_1,\ldots,a_m)$ is a set of integers which can not be represented in a form $\sum_{i=1}^m a_i x_i^k$. In other words, it is the complement of the set of representable numbers

$$V_k(a_1,\ldots,a_m)=\left\{ \sum_{i=1}^m a_i x_i^k \;\middle|\; (x_1,\ldots,x_m)\in\mathbb{N}^m \right\}.$$

It is obvious that the order of parameters does not matter, thus we often sort them in ascending order.

A family $W(k,m)$ is split into two disjoint families. Since $W_k(a_1\mu_1^k,\ldots,a_m\mu_m^k)$ includes $W_k(a_1,\ldots,a_m)$ for integers $\mu_i\geq 1$ and $\prod\mu_i>1$, a set of parameters $(a_1,\ldots,a_m)$ is called "absolute" if all a_i's are k-th-power-free, or "relative" otherwise.

A set $W_k(a_1,\ldots,a_m)$ can be split into two distinctive sets: a parametrizable infinite part called "trunk" denoted $W(Tr)$ and the rest called "star" denoted $W(*)$ [2]. Of course, a W-set may lack its trunk, since there is no "parametrizable infinite part". For example, $W(1,1,1,1)$ is expected to be finite – it is a well-believed conjecture for Waring's problem that $G(3)=4$ – and then lacks its trunk part. A trunk of W-set can consist of arithmetic progressions:

Lemma 1. *Let* $(a_1, \ldots, a_m) \in \mathbb{N}^m$. *If* $\exists q$ *and* r *such that:*

$$r \notin \left\{ \sum_{i=1}^{m} a_i x_1^k \bmod q \;\middle|\; x_i \in \mathbb{N}(i = 1, \ldots, m) \right\}$$

then the set $r + q\mathbb{N}$ *is in* $W_k(a_1, \ldots, a_m)(Tr)$.

We will often omit a subscript 3 for $W_3(a_1, \ldots, a_4)$ in the following sections.

2 Computation

2.1 Method

By the definition of the set $W(a_1, \ldots, a_4)$, one can obtain it by computing the complement of the set $V(a_1, \ldots, a_4)$. It is, however, an excessive work. Instead, one can do as the following.

$$\begin{aligned} W(a_1, \ldots, a_4) &= \mathbb{N} \setminus V(a_1, \ldots, a_4) \\ &= \{\, m \in \mathbb{N} \mid m \notin V(a_1, \ldots, a_4) \,\} \\ &= \left\{\, m \in \mathbb{N} \;\middle|\; \nexists x_1 \text{ s.t. } m \in \left(a_1 x_1^3 + V(a_2, a_3, a_4)\right) \right\} \\ &= \left\{\, m \in \mathbb{N} \;\middle|\; \nexists x_1 \text{ s.t. } (m - a_1 x_1^3) \in V(a_2, a_3, a_4) \right\} \end{aligned}$$

A process to test the condition of the right hand side is called the "Ramanujan sieve" [4]. Since $V(a_2, a_3, a_4)$ consists of positive integers only, for any m there are only finite possibilities of x_1: $0 < x_1 \leq \left\lfloor \sqrt[3]{\frac{m}{a_1}} \right\rfloor$.

Using the Ramanujan sieve does, however, make sense only for the last step of the construction. The set $V(a_2, a_3, a_4)$ used in the Ramanujan sieve, for example, is obtained as the sum of $V(a_2)$ and $V(a_3, a_4)$, i.e.,

$$V(a_2, a_3, a_4) = \{\, u + v \mid u \in V(a_2), v \in V(a_3, a_4) \,\}.$$

2.2 Program

The program used to obtain the result in the following section is written in Python[1] with some modules from NZMATH[2]. The source code is available online at `http://tnt.math.metro-u.ac.jp/~tetsushi/program/w34.tar.gz`.

The program needs Python 2.5 or higher built with `sqlite3` support, because sets will be stored in a database. The sets appeared in computation are generally too large to compute everything on memory. The disks are, however, much slower than the memories. For that reason, the program tries to do computation on memory as much as possible, with dividing sets into smaller subsets.

The time complexity is dominated by the Ramanujan sieve process. The sieve for a $W(k, m)$-set needs at worst $O(n^{1+1/k})$ set membership tests, where n is the maximum of testing range. Constructing V-sets requires less.

[1] `http://www.python.org/`
[2] `http://tnt.math.metro-u.ac.jp/nzmath/`

3 Results

This section devotes to present computational results.

3.1 Absolute Cases

The table 1 consists of four columns: the parameters $a_1, \ldots, a_4$, the upper limit of computation, the maximum element of $W(a_1, \ldots, a_4)$ obtained in the computed range, and the number of $W(a_1, \ldots, a_4)$ in the computed range.

Some factorizations of W-set elements are in the tables 2 through 5. Morikawa suggests a certain possibility of relationship between the parameters and factors.

3.2 Relative Cases and Cases with Trunk

The table 6 consists of five columns similar to those of the table 1 except that the base parameter is inserted to the second column, and the maximum element of $W(a_1, \ldots, a_4)$ and the number of $W(a_1, \ldots, a_4)$ obtained in the computed range, are of only the relative portion.

The computation of the cases with trunk set is very limited. The table 7 consists of five columns similar to the table 1 except that the last column is appended to represent trunk set and both the maximum and the size of the set are of $W(*)$ ever obtained instead of the whole W.

3.3 $W(5, 7)$

We have been carrying out some computation of $W(5, 7)$ sets also. Though it is believed that the number of terms needed for Waring's problem for fifth power is 6, this subsection presents a result about seven terms. The reason of this choice is that computing W-sets for six terms is much harder than for seven terms. We will expand the result to W-sets for six terms in the future.

The table 8 consists of four columns same as those of the table 1.

2179501 of $W_5(1, 1, 2, 3, 4, 5, 6)$ is factored into $191 \cdot 11411$ and 658192 of $W_5(1, 2, 3, 4, 5, 6, 7)$ into $2^4 \cdot 31 \cdot 1327$.

4 Discussions

Here is a random note about the result of computation.

There still is not a theory which tells whether a W-set for given parameters is finite or not. Rather, there are empirical arguments.

The first of such empirical argument is given by Western [5]. His observation is that for density δ of $W_3(1, 1, 1, 1)$ within a certain range with center x, $\log(-\log \delta)$ is linear to $\log x$.

The distributions of other W-sets look very similar to that of $W_3(1, 1, 1, 1)$, even in higher power cases. Therefore, a theory which explains the distribution of a W-set, say $W_3(1, 1, 1, 1)$ for example, may explain other W-sets also.

Table 1: absolute cases

$a_1, \ldots, a_4$	up to	$\max(W)$	$\lvert W\rvert$
$1,1,1,1$	2^{25}	$33554426^{\dagger}$	4269847
$1,1,1,2$	2^{30}	768097876	43710
$1,1,1,3$	2^{25}	31510150	20058
$1,1,1,4$	2^{25}	33475834	44767
$1,1,1,5$	2^{25}	33549885	53401
$1,1,1,6$	2^{25}	33522591	59271
$1,1,1,7$	2^{25}	33554372	302409
$1,1,2,2$	2^{25}	25872330	10349
$1,1,2,3$	2^{24}	524668^{*}	1243
$1,1,2,4$	2^{23}	1886184^{*}	1538
$1,1,2,5$	2^{25}	8223956^{*}	3846
$1,1,2,6$	2^{25}	4274676^{*}	3863
$1,1,2,7$	2^{25}	17659300	11006
$1,1,2,9$	2^{25}	33541780	31466
$1,1,3,3$	2^{25}	32810334	22741
$1,1,4,4$	2^{25}	33551738	88167
$1,2,2,2$	2^{25}	33531428	78901
$1,2,2,3$	2^{23}	1048189^{*}	2364
$1,2,2,4$	2^{25}	3772368^{*}	2928
$1,2,2,6$	2^{25}	5938988^{*}	6754
$1,2,3,3$	2^{25}	6704868^{*}	4008
$1,2,3,4$	2^{22}	260448^{*}	636
$1,2,3,5$	2^{21}	337951^{*}	1062
$1,2,3,6$	2^{21}	405687^{*}	1129
$1,2,3,7$	2^{22}	607540^{*}	1290
$1,2,3,9$	2^{21}	612572^{*}	1537
$1,2,4,4$	2^{25}	7544736^{*}	5744
$1,2,4,5$	2^{20}	400828^{*}	1192
$1,2,7,7$	2^{25}	33554395	1823388
$1,2,7,13$	2^{25}	33554430	1004122
$1,2,13,13$	2^{25}	33554430	1437754
$1,3,3,3$	2^{25}	33554430	2804837
$1,3,3,6$	2^{25}	33474318	39919
$1,3,4,6$	2^{24}	4161876^{*}	1926
$1,5,5,5$	2^{25}	33554355	1470200
$2,2,3,3$	2^{25}	33553830	100806
$2,3,3,3$	2^{25}	33554427	3079163
$2,3,3,6$	2^{25}	33548541	55209
$2,3,4,5$	2^{25}	9117243^{*}	3003

legend:

† 7373170279850 seems to be the largest [1]

$*$ the element seems to be the largest

Table 2: factorization of the largest 100 elements of W(1,2,3,4)

$7522 (= 2 \cdot 3761)$,	$7721 (= 7 \cdot 1103)$,	$7733 (= 11 \cdot 19 \cdot 37)$,
$7840 (= 2^5 \cdot 5 \cdot 7^2)$,	$7929 (= 3^2 \cdot 881)$,	$7978 (= 2 \cdot 3989)$,
$8001 (= 3^2 \cdot 7 \cdot 127)$,	$8119 (= 23 \cdot 353)$,	$8138 (= 2 \cdot 13 \cdot 313)$,
$8187 (= 3 \cdot 2729)$,	$8190 (= 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13)$,	$8355 (= 3 \cdot 5 \cdot 557)$,
$8435 (= 5 \cdot 7 \cdot 241)$,	$8511 (= 3 \cdot 2837)$,	$8655 (= 3 \cdot 5 \cdot 577)$,
$8675 (= 5^2 \cdot 347)$,	$8786 (= 2 \cdot 23 \cdot 191)$,	$8922 (= 2 \cdot 3 \cdot 1487)$,
$9078 (= 2 \cdot 3 \cdot 17 \cdot 89)$,	$9297 (= 3^2 \cdot 1033)$,	$9332 (= 2^2 \cdot 2333)$,
$9406 (= 2 \cdot 4703)$,	$9411 (= 3 \cdot 3137)$,	$9457 (= 7^2 \cdot 193)$,
$9526 (= 2 \cdot 11 \cdot 433)$,	$9708 (= 2^2 \cdot 3 \cdot 809)$,	$9877 (= 7 \cdot 17 \cdot 83)$,
$9951 (= 3 \cdot 31 \cdot 107)$,	$9981 (= 3^2 \cdot 1109)$,	$10185 (= 3 \cdot 5 \cdot 7 \cdot 97)$,
$10205 (= 5 \cdot 13 \cdot 157)$,	$10305 (= 3^2 \cdot 5 \cdot 229)$,	$10359 (= 3^2 \cdot 1151)$,
$10397 (= 37 \cdot 281)$,	$10401 (= 3 \cdot 3467)$,	10559,
$10580 (= 2^2 \cdot 5 \cdot 23^2)$,	$10784 (= 2^5 \cdot 337)$,	$10810 (= 2 \cdot 5 \cdot 23 \cdot 47)$,
$11267 (= 19 \cdot 593)$,	$11505 (= 3 \cdot 5 \cdot 13 \cdot 59)$,	$11722 (= 2 \cdot 5861)$,
$11749 (= 31 \cdot 379)$,	$11871 (= 3^2 \cdot 1319)$,	$12584 (= 2^3 \cdot 11^2 \cdot 13)$,
$12596 (= 2^2 \cdot 47 \cdot 67)$,	$12688 (= 2^4 \cdot 13 \cdot 61)$,	$12914 (= 2 \cdot 11 \cdot 587)$,
$13052 (= 2^2 \cdot 13 \cdot 251)$,	$13465 (= 5 \cdot 2693)$,	$13628 (= 2^2 \cdot 3407)$,
$13795 (= 5 \cdot 31 \cdot 89)$,	$13860 (= 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11)$,	$13890 (= 2 \cdot 3 \cdot 5 \cdot 463)$,
$14183 (= 13 \cdot 1091)$,	$14245 (= 5 \cdot 7 \cdot 11 \cdot 37)$,	$14512 (= 2^4 \cdot 907)$,
$14844 (= 2^2 \cdot 3 \cdot 1237)$,	$14880 (= 2^5 \cdot 3 \cdot 5 \cdot 31)$,	$14924 (= 2^2 \cdot 7 \cdot 13 \cdot 41)$,
$15928 (= 2^3 \cdot 11 \cdot 181)$,	$15951 (= 3 \cdot 13 \cdot 409)$,	$16466 (= 2 \cdot 8233)$,
$17408 (= (2 \cdot 10) \cdot 17)$,	$18242 (= 2 \cdot 7 \cdot 1303)$,	$19058 (= 2 \cdot 13 \cdot 733)$,
$19350 (= 2 \cdot 3^2 \cdot 5^2 \cdot 43)$,	$19566 (= 2 \cdot 3^2 \cdot 1087)$,	$21015 (= 3^2 \cdot 5 \cdot 467)$,
$21053 (= 37 \cdot 569)$,	$21270 (= 2 \cdot 3 \cdot 5 \cdot 709)$,	$21972 (= 2^2 \cdot 3 \cdot 1831)$,
$22139 (= 13^2 \cdot 131)$,	$22149 (= 3^2 \cdot 23 \cdot 107)$,	22277,
$22480 (= 2^4 \cdot 5 \cdot 281)$,	$22688 (= 2^5 \cdot 709)$,	22853,
$23884 (= 2^2 \cdot 7 \cdot 853)$,	$26444 (= 2^2 \cdot 11 \cdot 601)$,	$27093 (= 3 \cdot 11 \cdot 821)$,
$28318 (= 2 \cdot 14159)$,	$28333 (= 29 \cdot 977)$,	$28764 (= 2^2 \cdot 3^2 \cdot 17 \cdot 47)$,
29137,	$29142 (= 2 \cdot 3^2 \cdot 1619)$,	$31828 (= 2^2 \cdot 73 \cdot 109)$,
$32109 (= 3 \cdot 7 \cdot 11 \cdot 139)$,	$32219 (= 11 \cdot 29 \cdot 101)$,	$32556 (= 2^2 \cdot 3 \cdot 2713)$,
34403,	$34974 (= 2 \cdot 3^2 \cdot 29 \cdot 67)$,	$39101 (= 61 \cdot 641)$,
$41405 (= 5 \cdot 7^2 \cdot 13^2)$,	$41600 (= 2^7 \cdot 5^2 \cdot 13)$,	$42532 (= 2^2 \cdot 7^3 \cdot 31)$,
$45813 (= 3 \cdot 15271)$,	$56544 (= 2^5 \cdot 3 \cdot 19 \cdot 31)$,	$132244 (= 2^2 \cdot 7 \cdot 4723)$,
$260448 (= 2^5 \cdot 3 \cdot 2713)$		

Table 3: factorization of the largest 100 elements of W(1,1,2,3)

$39276 (= 2^2 \cdot 3^2 \cdot 1091)$,	$39941 (= 11 \cdot 3631)$,	$40156 (= 2^2 \cdot 10039)$,
$40310 (= 2 \cdot 5 \cdot 29 \cdot 139)$,	$40999 (= 7 \cdot 5857)$,	$41034 (= 2 \cdot 3 \cdot 7 \cdot 977)$,
$41193 (= 3^2 \cdot 23 \cdot 199)$,	$41214 (= 2 \cdot 3 \cdot 6869)$,	$41589 (= 3^2 \cdot 4621)$,
$41760 (= 2^5 \cdot 3^2 \cdot 5 \cdot 29)$,	$41767 (= 11 \cdot 3797)$,	$42252 (= 2^2 \cdot 3 \cdot 7 \cdot 503)$,
$42972 (= 2^2 \cdot 3 \cdot 3581)$,	$43015 (= 5 \cdot 7 \cdot 1229)$,	$43860 (= 2^2 \cdot 3 \cdot 5 \cdot 17 \cdot 43)$,
$44586 (= 2 \cdot 3^2 \cdot 2477)$,	$44801 (= 71 \cdot 631)$,	$45234 (= 2 \cdot 3^2 \cdot 7 \cdot 359)$,
$45348 (= 2^2 \cdot 3 \cdot 3779)$,	$45393 (= 3 \cdot 15131)$,	$46563 (= 3 \cdot 11 \cdot 17 \cdot 83)$,
$47244 (= 2^2 \cdot 3 \cdot 31 \cdot 127)$,	$47772 (= 2^2 \cdot 3^2 \cdot 1327)$,	$48454 (= 2 \cdot 7 \cdot 3461)$,
$48540 (= 2^2 \cdot 3 \cdot 5 \cdot 809)$,	48661,	$48695 (= 5 \cdot 9739)$,
$48825 (= 3^2 \cdot 5^2 \cdot 7 \cdot 31)$,	$48852 (= 2^2 \cdot 3^2 \cdot 23 \cdot 59)$,	$49300 (= 2^2 \cdot 5^2 \cdot 17 \cdot 29)$,
$49470 (= 2 \cdot 3 \cdot 5 \cdot 17 \cdot 97)$,	49499,	$49551 (= 3 \cdot 83 \cdot 199)$,
$49562 (= 2 \cdot 24781)$,	$50308 (= 2^2 \cdot 12577)$,	$51028 (= 2^2 \cdot 12757)$,
$52556 (= 2^2 \cdot 7 \cdot 1877)$,	$52635 (= 3 \cdot 5 \cdot 11^2 \cdot 29)$,	$52775 (= 5^2 \cdot 2111)$,
$53492 (= 2^2 \cdot 43 \cdot 311)$,	$53860 (= 2^2 \cdot 5 \cdot 2693)$,	$56124 (= 2^2 \cdot 3^2 \cdot 1559)$,
56687,	$57905 (= 5 \cdot 37 \cdot 313)$,	$58235 (= 5 \cdot 19 \cdot 613)$,
$58675 (= 5^2 \cdot 2347)$,	$58686 (= 2 \cdot 3 \cdot 9781)$,	$59400 (= 2^3 \cdot 3^3 \cdot 5^2 \cdot 11)$,
$60219 (= 3^2 \cdot 6691)$,	$60740 (= 2^2 \cdot 5 \cdot 3037)$,	$62324 (= 2^2 \cdot 15581)$,
63521,	$64001 (= 7 \cdot 41 \cdot 223)$,	$64529 (= 173 \cdot 373)$,
$68292 (= 2^2 \cdot 3^2 \cdot 7 \cdot 271)$,	$68980 (= 2^2 \cdot 5 \cdot 3449)$,	$69951 (= 3 \cdot 7 \cdot 3331)$,
$70796 (= 2^2 \cdot 11 \cdot 1609)$,	$71275 (= 5^2 \cdot 2851)$,	$71380 (= 2^2 \cdot 5 \cdot 43 \cdot 83)$,
$71388 (= 2^2 \cdot 3^3 \cdot 661)$,	$71640 (= 2^3 \cdot 3^2 \cdot 5 \cdot 199)$,	$72516 (= 2^2 \cdot 3 \cdot 6043)$,
$73500 (= 2^2 \cdot 3 \cdot 5^3 \cdot 7^2)$,	$73726 (= 2 \cdot 191 \cdot 193)$,	$78268 (= 2^2 \cdot 17 \cdot 1151)$,
$78380 (= 2^2 \cdot 5 \cdot 3919)$,	$78764 (= 2^2 \cdot 7 \cdot 29 \cdot 97)$,	$80940 (= 2^2 \cdot 3 \cdot 5 \cdot 19 \cdot 71)$,
$81052 (= 2^2 \cdot 23 \cdot 881)$,	$81876 (= 2^2 \cdot 3 \cdot 6823)$,	$85650 (= 2 \cdot 3 \cdot 5^2 \cdot 571)$,
$87485 (= 5 \cdot 17497)$,	$88443 (= 3^2 \cdot 31 \cdot 317)$,	$88740 (= 2^2 \cdot 3^2 \cdot 5 \cdot 17 \cdot 29)$,
89839,	$90205 (= 5 \cdot 18041)$,	91423,
$95692 (= 2^2 \cdot 47 \cdot 509)$,	$96332 (= 2^2 \cdot 24083)$,	$100740 (= 2^2 \cdot 3 \cdot 5 \cdot 23 \cdot 73)$,
$101860 (= 2^2 \cdot 5 \cdot 11 \cdot 463)$,	$105861 (= 3 \cdot 7 \cdot 71^2)$,	$107580 (= 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 163)$,
$112634 (= 2 \cdot 199 \cdot 283)$,	$114460 (= 2^2 \cdot 5 \cdot 59 \cdot 97)$,	$131068 (= 2^2 \cdot 7 \cdot 31 \cdot 151)$,
141811,	$148172 (= 2^2 \cdot 17 \cdot 2179)$,	$150381 (= 3^2 \cdot 7^2 \cdot 11 \cdot 31)$,
$181866 (= 2 \cdot 3 \cdot 17 \cdot 1783)$,	$186868 (= 2^2 \cdot 11 \cdot 31 \cdot 137)$,	$187076 (= 2^2 \cdot 46769)$,
$199092 (= 2^2 \cdot 3 \cdot 47 \cdot 353)$,	$225468 (= 2^2 \cdot 3^2 \cdot 6263)$,	$235935 (= 3^2 \cdot 5 \cdot 7^2 \cdot 107)$,
$239164 (= 2^2 \cdot 59791)$,	$320668 (= 2^2 \cdot 80167)$,	$388052 (= 2^2 \cdot 7 \cdot 13859)$,
$524668 (= 2^2 \cdot 29 \cdot 4523)$		

Table 4: factorization of the largest 100 elements of W(1,1,2,2)

$3574815 (= 3, 5 \cdot 238321)$,	$3594380 (= 2^2 \cdot 5 \cdot 179719)$,
$3662499 (= 3 \cdot 1220833)$,	$3664884 (= 2^2 \cdot 3 \cdot 305407)$,
$3664893 (= 3 \cdot 1221631)$,	$3675279 (= 3 \cdot 1225093)$,
$3683444 (= 2^2 \cdot 241 \cdot 3821)$,	$3685380 (= 2^2 \cdot 3 \cdot 5 \cdot 239 \cdot 257)$,
$3686764 (= 2^2 \cdot 619 \cdot 1489)$,	$3699212 (= 2^2 \cdot 11^2 \cdot 7643)$,
$3738316 (= 2^2 \cdot 934579)$,	$3760870 (= 2 \cdot 5 \cdot 71 \cdot 5297)$,
$3781534 (= 2 \cdot 271 \cdot 6977)$,	$3846324 (= 2^2 \cdot 3 \cdot 251 \cdot 1277)$,
$3848916 (= 2^2 \cdot 3 \cdot 41 \cdot 7823)$,	$3890396 (= 2^2 \cdot 972599)$,
$3899316 (= 2^2 \cdot 3 \cdot 53 \cdot 6131)$,	$3927876 (= 2^2 \cdot 3 \cdot 29 \cdot 11287)$,
$3929890 (= 2 \cdot 5 \cdot 17 \cdot 23117)$,	$3952985 (= 5 \cdot 409 \cdot 1933)$,
$3972732 (= 2^2 \cdot 3 \cdot 97 \cdot 3413)$,	$3973838 (= 2 \cdot 11 \cdot 180629)$,
$3990300 (= 2^2 \cdot 3 \cdot 5^2 \cdot 47 \cdot 283)$,	$4019828 (= 2^2 \cdot 37 \cdot 157 \cdot 173)$,
$4022276 (= 2^2 \cdot 53 \cdot 18973)$,	$4041580 (= 2^2 \cdot 5 \cdot 17 \cdot 11887)$,
$4068212 (= 2^2 \cdot 61 \cdot 16673)$,	$4073397 (= 3 \cdot 61 \cdot 22259)$,
$4078012 (= 2^2 \cdot 1019503)$,	$4091331 (= 3 \cdot 61 \cdot 79 \cdot 283)$,
$4106922 (= 2 \cdot 3 \cdot 29 \cdot 23603)$,	$4120932 (= 2^2 \cdot 3 \cdot 343411)$,
$4131149 (= 11 \cdot 375559)$,	$4134180 (= 2^2 \cdot 3 \cdot 5 \cdot 68903)$,
$4149636 (= 2^2 \cdot 3 \cdot 345803)$,	$4160148 (= 2^2 \cdot 3 \cdot 23 \cdot 15073)$,
$4169355 (= 3 \cdot 5 \cdot 239 \cdot 1163)$,	$4200636 (= 2^2 \cdot 3 \cdot 11^3 \cdot 263)$,
$4201884 (= 2^2 \cdot 3^2 \cdot 116719)$,	$4226396 (= 2^2 \cdot 1056599)$,
$4235748 (= 2^2 \cdot 3 \cdot 11 \cdot 32089)$,	$4307332 (= 2^2 \cdot 61 \cdot 127 \cdot 139)$,
$4424748 (= 2^2 \cdot 3 \cdot 368729)$,	$4489484 (= 2^2 \cdot 1122371)$,
$4491420 (= 2^2 \cdot 3 \cdot 5 \cdot 74857)$,	$4578603 (= 3 \cdot 79 \cdot 19319)$,
$4625356 (= 2^2 \cdot 359 \cdot 3221)$,	$4625515 (= 5 \cdot 925103)$,
$4656460 (= 2^2 \cdot 5 \cdot 232823)$,	$4710084 (= 2^2 \cdot 3 \cdot 83 \cdot 4729)$,
$4739820 (= 2^2 \cdot 3 \cdot 5 \cdot 197 \cdot 401)$,	$4763415 (= 3 \cdot 5 \cdot 23 \cdot 13807)$,
$4782588 (= 2^2 \cdot 3 \cdot 398549)$,	$4788708 (= 2^2 \cdot 3 \cdot 399059)$,
$4846836 (= 2^2 \cdot 3 \cdot 17 \cdot 23 \cdot 1033)$,	$4852156 (= 2^2 \cdot 211 \cdot 5749)$,
$4904292 (= 2^2 \cdot 3 \cdot 408691)$,	$5028612 (= 2^2 \cdot 3 \cdot 419051)$,
$5120905 (= 5 \cdot 59 \cdot 17359)$,	$5133099 (= 3 \cdot 17 \cdot 100649)$,
$5156717 (= 367 \cdot 14051)$,	$5181798 (= 2 \cdot 3 \cdot 863633)$,
$5247948 (= 2^2 \cdot 3 \cdot 163 \cdot 2683)$,	$5277756 (= 2^2 \cdot 3 \cdot 11 \cdot 39983)$,
$5508831 (= 3 \cdot 1836277)$,	5550763,
$5671364 (= 2^2 \cdot 1417841)$,	$5722340 (= 2^2 \cdot 5 \cdot 13^2 \cdot 1693)$,
$5871839 (= 107 \cdot 54877)$,	$5928476 (= 2^2 \cdot 73 \cdot 79 \cdot 257)$,
$5983377 (= 3 \cdot 1994459)$,	$6139111 (= 11 \cdot 197 \cdot 2833)$,
$6144214 (= 2 \cdot 3072107)$,	$6238996 (= 2^2 \cdot 1559749)$,
$6315476 (= 2^2 \cdot 41 \cdot 97 \cdot 397)$,	$6322756 (= 2^2 \cdot 11 \cdot 143699)$,
$6506620 (= 2^2 \cdot 5 \cdot 263 \cdot 1237)$,	$6989676 (= 2^2 \cdot 3 \cdot 199 \cdot 2927)$,
$7081675 (= 5^2 \cdot 283267)$,	$7121715 (= 3 \cdot 5 \cdot 167 \cdot 2843)$,
$7467692 (= 2^2 \cdot 17 \cdot 109819)$,	$7571535 (= 3 \cdot 5 \cdot 653 \cdot 773)$,
$7845692 (= 2^2 \cdot 307 \cdot 6389)$,	$8047292 (= 2^2 \cdot 11 \cdot 182893)$,
$8272860 (= 2^2 \cdot 3 \cdot 5 \cdot 173 \cdot 797)$,	$8468060 (= 2^2 \cdot 5 \cdot 423403)$,
$8580965 (= 5 \cdot 53 \cdot 32381)$,	$9913044 (= 2^2 \cdot 3 \cdot 826087)$,
$9942836 (= 2^2 \cdot 199 \cdot 12491)$,	$9998220 (= 2^2 \cdot 3 \cdot 5 \cdot 71 \cdot 2347)$,
$10141167 (= 3 \cdot 907 \cdot 3727)$,	$11521292 (= 2^2 \cdot 463 \cdot 6221)$,
$13735212 (= 2^2 \cdot 3 \cdot 29^2 \cdot 1361)$,	$16434564 (= 2^2 \cdot 3 \cdot 67 \cdot 20441)$,
$16487204 (= 2^2 \cdot 461 \cdot 8941)$,	$17050452 (= 2^2 \cdot 3 \cdot 23 \cdot 163 \cdot 379)$,
$17120244 (= 2^2 \cdot 3 \cdot 83 \cdot 17189)$,	$18322060 (= 2^2 \cdot 5 \cdot 916103)$,
$18987387 (= 3 \cdot 41 \cdot 154369)$,	$25872330 (= 2 \cdot 3 \cdot 5 \cdot 11 \cdot 78401)$

Table 5: factorization of the largest 100 elements of W(1,1,1,2)

$83966701 = 7 \cdot 13 \cdot 83 \cdot 11117$,	$83984108 = 2^2 \cdot 13 \cdot 1615079$,
$84027937 = 7 \cdot 19 \cdot 631789$,	$84545428 = 2^2 \cdot 11 \cdot 1181 \cdot 1627$,
$86479484 = 2^2 \cdot 7 \cdot 13 \cdot 237581$,	$87018260 = 2^2 \cdot 5 \cdot 7 \cdot 67 \cdot 9277$,
$88283767 = 11 \cdot 13 \cdot 617369$,	$90323284 = 2^2 \cdot 29 \cdot 47 \cdot 16567$,
$90572764 = 2^2 \cdot 4327 \cdot 5233$,	$91215068 = 2^2 \cdot 7^2 \cdot 465383$,
$92094548 = 2^2 \cdot 7 \cdot 13 \cdot 113 \cdot 2239$,	$92126524 = 2^2 \cdot 7 \cdot 373 \cdot 8821$,
$92368094 = 2 \cdot 7 \cdot 13 \cdot 317 \cdot 1601$,	$92395940 = 2^2 \cdot 5 \cdot 7 \cdot 13 \cdot 50767$,
$93155972 = 2^2 \cdot 7 \cdot 13 \cdot 255923$,	$94173196 = 2^2 \cdot 13 \cdot 19 \cdot 95317$,
$94761212 = 2^2 \cdot 7 \cdot 13 \cdot 29 \cdot 47 \cdot 191$,	$95249084 = 2^2 \cdot 7 \cdot 3401753$,
$95580716 = 2^2 \cdot 7 \cdot 11 \cdot 19 \cdot 16333$,	$95850391 = 7 \cdot 13 \cdot 1053301$,
$96695914 = 2 \cdot 7^2 \cdot 986693$,	$98116636 = 2^2 \cdot 47 \cdot 521897$,
$98369068 = 2^2 \cdot 7^2 \cdot 23 \cdot 21821$,	$99394295 = 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 2837$,
$99772673 = 7^2 \cdot 11 \cdot 13 \cdot 29 \cdot 491$,	$100873948 = 2^2 \cdot 7^2 \cdot 29 \cdot 17747$,
$103047700 = 2^2 \cdot 5^2 \cdot 7 \cdot 147211$,	$103828396 = 2^2 \cdot 7 \cdot 3708157$,
$103895428 = 2^2 \cdot 7 \cdot 13 \cdot 79 \cdot 3613$,	$104014652 = 2^2 \cdot 7^2 \cdot 97 \cdot 5471$,
$104375236 = 2^2 \cdot 7 \cdot 3727687$,	$104693953 = 7 \cdot 13 \cdot 23 \cdot 50021$,
$104810251 = 7 \cdot 13^2 \cdot 19 \cdot 4663$,	$106382353 = 7 \cdot 11^2 \cdot 29 \cdot 61 \cdot 71$,
$106795220 = 2^2 \cdot 5 \cdot 7 \cdot 762823$,	$108302980 = 2^2 \cdot 5 \cdot 5415149$,
$108978961 = 7 \cdot 13 \cdot 1197571$,	$109108363 = 7 \cdot 13 \cdot 17 \cdot 70529$,
$109367564 = 2^2 \cdot 27341891$,	$110223932 = 2^2 \cdot 7^2 \cdot 13 \cdot 181 \cdot 239$,
$110718643 = 7 \cdot 19 \cdot 53 \cdot 113 \cdot 139$,	$110930036 = 2^2 \cdot 7 \cdot 151 \cdot 26237$,
$112186165 = 5 \cdot 7 \cdot 13 \cdot 19^2 \cdot 683$,	$112211636 = 2^2 \cdot 28052909$,
$113029700 = 2^2 \cdot 5^2 \cdot 7 \cdot 161471$,	$113211436 = 2^2 \cdot 13 \cdot 2177143$,
$113423828 = 2^2 \cdot 7^2 \cdot 578693$,	$115367252 = 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 28813$,
$117858748 = 2^2 \cdot 7 \cdot 19 \cdot 221539$,	$121264241 = 7 \cdot 17323463$,
$123189332 = 2^2 \cdot 7^2 \cdot 29 \cdot 21673$,	$123236204 = 2^2 \cdot 7 \cdot 13 \cdot 19 \cdot 103 \cdot 173$,
$124158407 = 19 \cdot 2251 \cdot 2903$,	$127299830 = 2 \cdot 5 \cdot 7 \cdot 1818569$,
$128552620 = 2^2 \cdot 5 \cdot 7 \cdot 61 \cdot 15053$,	$132525076 = 2^2 \cdot 19 \cdot 73 \cdot 23887$,
$134155714 = 2 \cdot 7 \cdot 11 \cdot 61 \cdot 14281$,	$136821748 = 2^2 \cdot 7 \cdot 4886491$,
$137669476 = 2^2 \cdot 7 \cdot 379 \cdot 12973$,	$138590438 = 2 \cdot 7 \cdot 67 \cdot 71 \cdot 2081$,
$138694612 = 2^2 \cdot 7 \cdot 79 \cdot 62701$,	$143283236 = 2^2 \cdot 89 \cdot 277 \cdot 1453$,
$143941252 = 2^2 \cdot 7 \cdot 13 \cdot 395443$,	$144462316 = 2^2 \cdot 36115579$,
$146691148 = 2^2 \cdot 23 \cdot 139 \cdot 11471$,	$146766263 = 7 \cdot 1489 \cdot 14081$,
$147631729 = 7 \cdot 19 \cdot 1110013$,	$154969780 = 2^2 \cdot 5 \cdot 7 \cdot 1106927$,
$157377892 = 2^2 \cdot 7 \cdot 127 \cdot 44257$,	$157586828 = 2^2 \cdot 7 \cdot 5628101$,
$157851365 = 5 \cdot 7 \cdot 4510039$,	$161137606 = 2 \cdot 7 \cdot 11509829$,
$163046884 = 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 947$,	$171843980 = 2^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 839$,
$172345180 = 2^2 \cdot 5 \cdot 7 \cdot 157 \cdot 7841$,	$173195932 = 2^2 \cdot 7 \cdot 13^2 \cdot 17 \cdot 2153$,
$176805356 = 2^2 \cdot 7 \cdot 13 \cdot 485729$,	$181804532 = 2^2 \cdot 7 \cdot 13 \cdot 37 \cdot 13499$,
$188901284 = 2^2 \cdot 11 \cdot 13 \cdot 330247$,	$191056684 = 2^2 \cdot 7^2 \cdot 13 \cdot 167 \cdot 449$,
$194062036 = 2^2 \cdot 7 \cdot 701 \cdot 9887$,	$201561178 = 2 \cdot 7 \cdot 13 \cdot 1107479$,
$204992564 = 2^2 \cdot 7 \cdot 7321163$,	$210744716 = 2^2 \cdot 7 \cdot 13 \cdot 17 \cdot 34057$,
$214550420 = 2^2 \cdot 5 \cdot 7^2 \cdot 37 \cdot 61 \cdot 97$,	$216780746 = 2 \cdot 7 \cdot 13 \cdot 1191103$,
$216812596 = 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 173 \cdot 313$,	$220828468 = 2^2 \cdot 7 \cdot 7886731$,
$224032324 = 2^2 \cdot 17 \cdot 3294593$,	$226109884 = 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 149 \cdot 379$,
$240537388 = 2^2 \cdot 7 \cdot 13 \cdot 660817$,	$246505252 = 2^2 \cdot 7 \cdot 8803759$,
$255939404 = 2^2 \cdot 7 \cdot 59 \cdot 154927$,	$261951044 = 2^2 \cdot 79 \cdot 389 \cdot 2131$,
$265807724 = 2^2 \cdot 7 \cdot 13 \cdot 827 \cdot 883$,	$286040300 = 2^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 43^2$,
$334519556 = 2^2 \cdot 7 \cdot 11947127$,	$343024708 = 2^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 1571$,
$372652826 = 2 \cdot 7 \cdot 13 \cdot 37 \cdot 55339$,	$768097876 = 2^2 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 47 \cdot 139$

Table 6: relative cases

$a_1, \ldots, a_4$	base	up to	$\max(W_{rel})$	$\lvert W_{rel}\rvert$
$1,1,1,8$	$1,1,1,1$	2^{25}	33554390	318297
$1,2,3,8$	$1,1,2,3$	2^{25}	1697724*	2282
$2,3,4,8$	$1,2,3,4$	2^{25}	2083584*	3734
$1,3,4,16$	$1,2,3,4$	2^{25}	9657982*	9457
$1,2,4,24$	$1,2,3,4$	2^{25}	5911607*	3964
$1,2,3,32$	$1,2,3,4$	2^{25}	11509380*	6912

legend:

$*$ the element seems to be the largest

Table 7: cases with trunk set

$a_1, \ldots, a_4$	up to	$\max(W(*))$	$\lvert W(*)\rvert$	trunk set
$1,1,1,9$	2^{20}	1048557	71394	$4,5 \bmod 9$
$1,1,7,7$	2^{20}	1048566	34878	$3,4 \bmod 7$
$1,1,9,9$	2^{20}	1048466	23773	$3,4,5,6 \bmod 9$
$1,1,28,63$	2^{20}	1048573	97679	$3,4 \bmod 7$ & $4,5 \bmod 9$
$1,4,4,4$	2^{20}	1048569	111092	$2 \bmod 4$
$1,7,7,7$	2^{20}	1048565	69965	$2,3,4,5 \bmod 7$
$1,9,9,9$	2^{20}	1048528	29857	$2,3,4,5,6,7 \bmod 9$

Table 8: absolute cases for W(5,7)

$a_1, \ldots, a_7$	up to	$\max(W)$	$\lvert W\rvert$
$1,1,1,1,1,1,1$	2^{25}	33554431	28944592
$1,1,1,1,1,1,2$	2^{25}	33554431	20867928
$1,1,1,1,1,2,2$	2^{25}	33554431	12087809
$1,1,1,1,1,2,3$	2^{25}	33554425	5897853
$1,1,1,1,2,2,2$	2^{25}	33554427	7705353
$1,1,1,1,2,2,3$	2^{25}	33554336	1989680
$1,1,1,1,2,3,4$	2^{21}	2097152	424274
$1,1,1,2,2,2,3$	2^{21}	2097151	618411
$1,1,1,2,2,3,3$	2^{21}	2097138	414611
$1,1,1,2,2,3,4$	2^{21}	2096993	225120
$1,1,1,2,3,4,5$	2^{21}	2096657	93685
$1,1,2,2,3,3,4$	2^{21}	2096707	135566
$1,1,2,2,3,4,5$	2^{21}	2096810	64410
$1,1,2,3,4,5,6$	2^{25}	2179501*	33002
$1,2,3,4,5,6,7$	2^{25}	658192*	21134

legend:

$*$ the element seems to be the largest

Thunk is an obvious obstacle for a W-set to be finite. The trunks in the table 7 are found by the following lemma.

Lemma 2. *The following conditions suffice the condition of Lemma 1 for cube-free and coprime parameters* $(a_1, \ldots, a_4) \in \mathbb{N}^4$ *regardless of order.*

1. *There exists a prime* $p \equiv 1 \bmod 3$ *such that* $p \not| a_1$ *and* $p | a_i$ *for* $i = 2, 3, 4$.
2. *There exists a prime* p *such that* $p \not| a_1$ *and* $p^2 | a_i$ *for* $i = 2, 3, 4$.
3. $a_1 \equiv \pm a_2 \bmod 7$ *and* $7 | a_i$ *for* $i = 3, 4$.
4. $a_1 \equiv \pm a_2, \pm 2a_2, \pm 4a_2 \bmod 9$ *and* $9 | a_i$ *for* $i = 3, 4$.
5. $a_1 \equiv a_2 \equiv a_3 \bmod 9$ *and* $9 | a_4$.

Proof. By taking modulo p, for the first case, $\sum_{i=1}^4 a_i x_1^3$ is congruent to $a_1 x_1^3$. The mapping $x^3 \bmod p$ is not surjective in $\mathbb{Z}/p\mathbb{Z}$, since $p \equiv 1 \bmod 3$. Thus, $\sum_{i=1}^4 a_i x_1^3 \bmod p$ is not surjective, either.

Proofs for the other cases are similar. □

There have not been any evidence that a $W(3, 4)$-set can be infinite without trunk. Probably, trunk may be the only reason a W-set to be infinite, if the number of terms is sufficiently large.

It is clear from the computation above that the maximum element of a W-set and its cardinality are strongly correlated. They both increase when the symmetry group of variables and/or the volume factor $\prod a_i$ become large. The effect of the symmetry group seems to appear through its cardinality. The table 8 of $W(5, 7)$ consists of W-sets for all symmetries. The volume factor also affects as a local condition; even if it does not allow trunk, it may cause an unbalance among residue classes.

References

[1] J.-M. Deshouillers, F. Hennecart, and B. Landreau. 7 373 170 279 850. *Mathematics of Computation*, 69(229):421–439, 1999.

[2] R. Morikawa. Search of mathematical structures using a computer. electronic proceedings of AC 2005, 2005. `ftp://tnt.math.metro-u.ac.jp/pub/ac05/Morikawa/morikawa.pdf`.

[3] R. Morikawa. Some concepts and methods to investigate problems of Waring type. electronic proceedings of AC 2007, 2007. to appear.

[4] S. Ramanujan. On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$. *Proceedings of the Cambridge Philosophical Society*, 19:11–21, 1917. (reprinted in Collected papers of Srinivasa Ramanujan, 169–178, AMS Chelsea Publ., Providence, RI, 2000.).

[5] A. E. Western. Computaions concerning numbers representable by four or five cubes. *Journal of the London Mathematical Society*, 1:244–250, 1926.