Proceedings of

Algebra and Computation 2009

Tokyo Metropolitan University

December 2–4, 2009

Edited by AC2009 Proceedings Committee

Organizers

Ken Nakamula (Tokyo Metropolitan Univ.)

Katsushi Waki (Yamagata Univ.)

Hirofumi Tsumura (Tokyo Metropolitan Univ.)

Shigenori Uchiyama (Tokyo Metropolitan Univ.)

プログラム [Program]

12 月 2 日（水）

9:55 - 10:00: Opening

10:00 - 10:20: 宋慧玲, 伊藤浩行 (広島大)

“巨大有限体の構成について”

10:20 - 10:40: 新谷誠 (静岡大)

“互いに素な シュタイナー系 S(5,8,24) と 5-(24,12,48) デザイン”

11:00 - 11:40: 松岡聡 (産業技術総合研究所)

“MLL プルーフネットの符号理論的研究”

13:30 - 14:20: [特別講演] 蓮尾一郎 (京大数理解析研究所/JST さきがけ)

“小宇宙原理とコンポーネント計算：計算機システムの基礎理論としての普遍代数・余代数をめぐって”

14:40 - 15:10: 知念宏司 (近畿大)

“一般 Hamming 符号から作られる不変式の Riemann 予想について”

15:10 - 15:40: 原田昌晃 (山形大/JST さきがけ)

“ Extremal Type II $\mathbb{Z}_{2k}$-codes”

16:00 - 16:20: 三枝崎剛 (北海道大), 坂内英一 (九州大)

“ユークリッド空間における 2 次元整数格子のある性質”

16:20 - 16:50: 藤田育嗣 (日本大), 寺井伸浩 (足利工大)

“楕円曲線 $E : y^2 = x^3 \quad nx$ の生成元”

12 月 3 日（木）

10:00-10:20: 森川良三 (首都大)

“ワーリングタイプの問題を探求する為の、いくつかの概念と方法 II”

10:20 - 10:50: 酒井祐貴子, 橋本喜一朗 (早稲田大)

“$\sqrt{2}$ 乗法をもつ曲線と Humbert のモジュラー方程式の一般化について”

11:10 - 11:40: 大石亮子 (高エネルギー加速器研究機構)

“トポグラフを用いた 3 次元粉末結晶の格子を決定するアルゴリズム”

13:30 - 14:20: [特別講演] 黒田茂 (首都大)

“多項式環をめぐるいくつかの話題”

14:35 - 15:10: 清野善裕, 吉田仁, 金田康正 (東大)

“Riemann zeta 函数の零点とその計算の基礎について”

15:10 - 15:40: 村田玲音 (明治学院大), 神谷諭一 (大東文化大)

“数論的関数とコード・システムのある関係について”

16:00 - 16:20: 谷口哲也 (東京理科大)

“非正則素数の高速計算”

16:20 - 16:40: 長谷川武博 (都留文科大), 犬塚美代子, 鈴木隆文

“関数体の塔に関する Elkies 予想の数値的証拠”

12 月 4 日 (金)

10:00 - 10:20: 小松尚夫 (弘前大), Chris K. Caldwell (University of Tennessee at Martin)

" Powers of Sierpinski numbers base b"

10:20 - 10:40: 堀口直之 (千葉大)

"Hall-Janko 群で不変な rank 3 グラフと rank 4 グラフについて"

11:00 - 11:30: 平野貴人, 田中圭介 (東工大)

"1 のベキ乗根とその暗号への応用"

11:30 - 12:00: 佐々木義卓, 大野泰生, 山崎知佳 (近畿大)

"ある離散対数問題に関する古典アルゴリズムと量子アルゴリズムの比較について"

– JANT セッション 『格子と暗号の数理』 –

14:00 - 14:10: 小暮淳 (富士通研)

"格子と暗号の数理"

14:10 - 15:00: 島田伊知朗 (広島大)

"超特異 K3 曲面と格子理論"

15:20 - 16:10: 田中圭介 (東工大)

"イデアル格子を用いた Fully Homomorphic Encryption について"

16:10 - 17:00: 國廣昇 (東大)

"RSA 暗号に対する格子攻撃"

17:00 - 17:10: Closing

On the construction of huge finite fields

Huiling Song Hiroyuki Ito

February 12, 2010

Abstract

When one constructs a finite field, one needs to find a primitive irreducible polynomial of given degree. Thus, this construction is hard to apply for the construction of huge finite fields. To avoid the decision problem of primitivity, we give the another construction of finite fields using the Artin-Schreier tower which has a beautiful recursive structure. We also give the multiplication algorithm using this recursive structure.

1 Introduction

Standard method to construct a finite field, such as $\mathbb{F}_{p^s}$, requires an irreducible primitive polynomial of degree s with coefficients in $\mathbb{F}_p$. Once such a polynomial is found, the field can be represented like $\mathbb{F}_{p^s} = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^s-1}\}$, where α is a primitive root of the polynomial. Such a polynomial is usually obtained by choosing it randomly and then verifying that it is irreducible and primitive. For these purposes, the existence, distribution and other properties of irreducible trinomials over $\mathbb{F}_2$ have been extensively studied. A table of low-weight irreducible polynomials over the finite field $\mathbb{F}_2$ is presented in [4]. For each integer n in the range $2 \leq n \leq 10000$, a binary irreducible polynomial $f(x)$ of degree n with minimum posible weight is listed. And the table in [5] gives one primitive binary polynomial of degree n with $2 \leq n \leq 5000$ and weight k for $k \in \{3, 5, 7\}$. However, it is difficult to verify that whether the polynomial is primitive or not when $n \gg 5 \times 10^3$. In this paer, we give a method that one can construct a field such as $\mathbb{F}_{p^{p^r}}$, not requiring to have a primitive polynomial, and at the same time, yields a simple recursive basis of the generated field. And give a multiplication algorithm using the recursive basis. It is possible to construct and execute various operations in a finite field.

Note that the idea of using Artin-Shreier tower for constructing finite fields was first treated by Cantor in [1] and developed by Feo and Schost in [2] along the way by Cantor. But our formulation and view point is slightly different from them.

Here are the plan of this report. Section 2 consists of preliminaries such as basics on Artin-Schreier extensions and the definition of specific Artin-Schreier tower. In sections 3 and 4, we give a detailed constuction of finite fields using the specific Artin-Schreier tower for $p = 2$ and give a multiplication algorithm in that field. In section 5, we give the same method for general p. Finally, we explain experimental results in section 6.

2 Construction using Artin-Schreier towers

In this section we describe a specific Artin-Schreier tower where the multiplication is easy, and explain how to construct this tower.

Definition 1 *Let $\mathbb{F}_q$ be a field of q elements in characteristic p, suppose $x^p - x - \alpha$ ($\alpha \in \mathbb{F}_q$) is an irreducible polynomial, then the quotient ring*

$$\mathbb{F}_{q^p} := \mathbb{F}_q[x]/(x^p - x - \alpha)$$

is called the Artin-Schreier extension of $\mathbb{F}_q$.

Note that if λ is a root of $x^p - x - \alpha = 0$, then all of $\lambda, \lambda+1, \lambda+2, \cdots, \lambda+p-1$ are roots of $x^p - x - \alpha = 0$. We define the Artin-Schreier tower of $\mathbb{F}_p$.

Definition 2 (*Ito-Kajiwara-Song* [3]) *Let* K_0 *be the prime field* $\mathbb{F}_p$ *and* $f_1(x) := x^p + x + 1$ *be the polyomial in* $\mathbb{F}_p[x]$*, we define*

$$K_1 := K_0[x]/(f_1(x)) = K_0(\alpha_1) = \mathbb{F}_p(\alpha_1) = \mathbb{F}_{p^2},$$

where $\alpha_1 := \bar{x} \in K_1$ *be the image of* x *in* K_1*. And define*

$$f_2(x) := x^p + x + \alpha_1^{p-1} \in K_1[x].$$

Suppose that α_{r-1} *and* f_r *are defined for* $r \geq 2$*, then define*

$$K_r := K_{r-1}[x]/(f_r(x)) = K_{r-1}(\alpha_r)$$

where $\alpha_r := \bar{x} \in K_r$ *be the image of* x *in* K_r*. And define*

$$f_r(x) := x^p + x + \alpha_1 \cdots \alpha_{r-1}{}^{p-1}.$$

Then we have the tower of finite fields:

$$K_0 \subset K_1 = K_0(\alpha_1) \subset K_2 = K_1(\alpha_2) \subset \cdots \subset K_r = K_{r-1}(\alpha_r).$$

We call this tower as the Artin-Schreier tower.

Since it is clear that $f_r(x)$ is irreduable for every $r \geq 1$, the above definition is well-defined. Using this definition, we give an algorithm of producing irreducible polynomials whose decomposition field is $\mathbb{F}_{p^{p^r}}$.

Proposition 1 (*Ito-Kajiwara-Song* [3]) *For* $r \geq 0$*, define* $f_r(X) \in \mathbb{F}_p[x]$ *and* $g_r(X, A, \alpha) \in \mathbb{F}_p[X, A, \alpha]$ *as follows. Set*

$$f_{(0)}(X, A) := X + A^{p-1}, \ g_{(0)}(X, A, \alpha) := f_{(0)}(X, A\alpha)$$

Suppose that we have $f_r(X, A)$ *and* $g_r(X, A, \alpha)$ *for* $r \geq 0$*. Set*

$$G_r(X, A, \alpha) := \prod_{i=0}^{p-1} g_r(X, A, \alpha + i) \in \mathbb{F}_p[X, A, \alpha].$$

Since G_r *is stable under the automorphism* $(X, A, \alpha) \to (X, A, \alpha + 1)$ *and the invariant ring of this automorphism is* $\mathbb{F}_p[X, A, \alpha^p - \alpha]$*, one can write* $G_r(X, A, \alpha) = {G_r}^0(X, A, \alpha^p - \alpha)$ *for a unique* ${G_r}^0(X, A, c) \in \mathbb{F}_p[X, A, c]$*. Now define* $f_{r+1}(X, A)$ *and* $g_{r+1}(X, A, \alpha)$ *as follows:*

$$f_{r+1}(X, A) := {G_r}^0(X, A, A^{p-1}), \ g_{r+1}(X, A, \alpha) := f_{r+1}(X, A\alpha).$$

Then $f_r(X, \alpha_0) \in K_0[X]$ *is an irreducible polynomial of degree* p^r *for each* $r \geq 2$*.*

3 Recursive structures for $p = 2$

The Artin-Schreier tower which we have defined in the previous section has a beautiful recursive structure. Since the binary case is especially usefull in practice, we give a detail of it for the case.

Since the basis of K_1 over K_0 is 1 and α_1, we have

$$K_1 = \{s_0 1 + t_0 \alpha_1 | s_0, t_0 \in K_0\}.$$

The basis of K_2 over K_1 is 1 and α_2, thus the basis of K_2 over K_0 is $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$, and we have

$$\begin{aligned} K_2 &= \{s_1 1 + t_1\alpha_2 | s_1, t_1 \in K_1\} \\ &= \{s_{01}1 + t_{01}\alpha_1 + s_{02}\alpha_2 + t_{02}\alpha_1\alpha_2 | s_{01}, t_{01}, s_{02}, t_{02} \in K_0\} \end{aligned}$$

Similarly, the basis of K_r over K_{r-1} is 1 and α_r, so that we have the basis over K_0 as

$$\overbrace{\overbrace{\overbrace{(1, \underbrace{\alpha_1}_{2} | \alpha_2, \alpha_1\alpha_2 | \ldots | \alpha_{r-1}, \alpha_1\alpha_{r-1}, \ldots, \alpha_1\cdots\alpha_{r-2}\alpha_{r-1}}^{2^{r-1}} | \alpha_r, \alpha_1\alpha_r, \ldots\ldots, \alpha_1\cdots\alpha_{r-1}\alpha_r)}^{2^r}}^{2^2}}^{2^{r-2}} .$$

4 Multiplication algorithm for $p = 2$

Using the recursive structures of the basis shown above, we give an algorithm of multiplication on the Artin-Schreier extensions. Frist we give a vector expression of the elements of the fields. We write $s_1 + s_2\alpha_r \in K_r$ as (s_1, s_2), where $s_1, s_2 \in K_{r-1}$. And we also write the multiplication of two elements of K_r , $(s_1+s_2\alpha_r)(t_1+t_2\alpha_r)$ as $(s_1, s_2)(t_1, t_2)$. On the other hand, for two elements $s_1+s_2\alpha_r, t_1+t_2\alpha_r \in K_r$, we have

$$(s_1 + s_2\alpha_r)(t_1 + t_2\alpha_r) = s_1t_1 + (s_1t_2 + s_2t_1)\alpha_r + s_2t_2\alpha_r^2.$$

Since α_r is a root of $f_r(x) = x^2 + x + \alpha_{r-1}\cdots\alpha_1$, we have

$$\alpha_r^2 = \alpha_r + \alpha_{r-1}\cdots\alpha_1,$$

thus we can write

$$(s_1 + s_2\alpha_r)(t_1 + t_2\alpha_r) = (s_1t_1 + s_2t_2\alpha_{r-1}\cdots\alpha_1) + (s_1t_2 + s_2t_1 + s_2t_2)\alpha_r.$$

Note that $(s_1t_1 + s_2t_2\alpha_{r-1}\cdots\alpha_1)$ and $(s_1t_2 + s_2t_1 + s_2t_2)$ are the elements of K_{r-1}.

Doing the above operation recursively, we can express an element of K_r as a vector of length 2^r over K_0 with the basis shown in the end of last section. By the argument above, we have the matrix which expresses the multiplication of two elements.

Theorem 1 *For elements (s_1, s_2) and (t_1, t_2) of K_1, let $A^{(1)}(t_1, t_2)$ be the 2×2 matrix defined by $A^{(1)}(t_1, t_2) := \begin{pmatrix} t_1 & t_2 \\ t_2 & t_1 + t_2 \end{pmatrix}$. Then the multiplication of (s_1, s_2) and (t_1, t_2) is expressed as*

$$(s_1, s_2)(t_1, t_2) = (s_1, s_2)\begin{pmatrix} t_1 & t_2 \\ t_2 & t_1 + t_2 \end{pmatrix} .$$

Similarly, for each $r \geq 1$ and two elements $(s_1, s_2, \ldots, s_{2^r})$ and $(t_1, t_2, \cdots, t_{2^r})$ of K_r, define the $2^r \times 2^r$ block matrix $A^{(r)}(t_1, \ldots, t_{2^r})$ as $\begin{pmatrix} S & T \\ U & V \end{pmatrix}$, where $2^{r-1} \times 2^{r-1}$ matrices S, T, U, V are defined recursively as follows:

$$\begin{aligned} S &= A^{(r-1)}(t_1, \ldots, t_{2^{(r-1)}}) \\ T &= A^{(r-1)}(t_{2^{(r-1)}+1}, \ldots, t_{2^r}) \\ U &= A^{(r-1)}(t_{2^{(r-1)}+1}, \ldots, t_{2^r})A^{(r-1)}(0, \ldots, 1) \\ V &= A^{(r-1)}(t_1, \ldots, t_{2^{(r-1)}}) + A^{(r-1)}(t_{2^{(r-1)}+1}, \ldots, t_{2^r}). \end{aligned}$$

Then the matrix $A^{(r)}(t_1,\ldots,t_{2^r})$ *gives the multiplication of* $(s_1,s_2,\ldots,s_{2^r})$ *and* $(t_1,t_2,\cdots,t_{2^r})$ *as*

$$(s_1,s_2,\ldots,s_{2^r})(t_1,t_2,\ldots,t_{2^r}) = (s_1,s_2,\ldots,s_{2^r})A^{(r)}(t_1,\ldots,t_{2^r}) = (s_1,s_2,\ldots,s_{2^r})\begin{pmatrix} S & T \\ U & V \end{pmatrix}$$

Proof The case for K_1 is clear from the argument above the theorem.
When $r=2$, let $(s_1,s_2,s_3,s_4),(t_1,t_2,t_3,t_4)$ be two elements of K_2, then

$$\begin{aligned}
&(s_1,s_2,s_3,s_4)(t_1,t_2,t_3,t_4)\\
&\qquad = (s_1,s_2,s_3,s_4)\times\begin{pmatrix} A^{(1)}(t_1,t_2) & A^{(1)}(t_3,t_4) \\ A^{(1)}(t_3,t_4)A^{(1)}(0,1) & A^{(1)}(t_1,t_2)+A^{(1)}(t_3,t_4)\end{pmatrix}\\
&\qquad = (s_1,s_2,s_3,s_4)\times A^{(2)}(t_1,t_2,t_3,t_4).
\end{aligned}$$

For general case K_r, we obtain the following by induction:

$$\begin{aligned}
&(s_1,\ldots,s_{2^r})(t_1,\ldots,t_{2^r})\\
&\quad = ((s_1,\ldots,s_{2^{r-1}})+(s_{2^{r-1}+1},\ldots,s_{2^r})\alpha_r)\times((t_1,\ldots,t_{2^{r-1}})+(t_{2^{r-1}+1},\ldots,t_{2^r})\alpha_r)\\
&\quad = (s_1,\ldots,s_{2^{r-1}})(t_1,\ldots,t_{2^{r-1}})\\
&\qquad +((s_1,\ldots,s_{2^{r-1}})(t_{2^{r-1}+1},\ldots,t_{2^r})+(s_{2^{r-1}+1},\ldots,s_{2^r})(t_1,\ldots,t_{2^{r-1}}))\alpha_r\\
&\qquad +(s_{2^{r-1}+1},\ldots,s_{2^r})(t_{2^{r-1}+1},\ldots,t_{2^r})\alpha_r^2\\
&\quad = (s_1,\ldots,s_{2^{r-1}})(t_1,\ldots,t_{2^{r-1}})\\
&\qquad +((s_1,\ldots,s_{2^{r-1}})(t_{2^{r-1}+1},\ldots,t_{2^r})+(s_{2^{r-1}+1},\ldots,s_{2^r})(t_1,\ldots,t_{2^{r-1}}))\alpha_r\\
&\qquad +(s_{2^{r-1}+1},\ldots,s_{2^r})(t_{2^{r-1}+1},\ldots,t_{2^r})(\alpha_r+(\alpha_{r-1}\cdots\alpha_1))\\
&\quad = (s_1,\ldots,s_{2^{r-1}})(t_1,\ldots,t_{2^{r-1}})\\
&\qquad +((s_1,\ldots,s_{2^{r-1}})(t_{2^{r-1}+1},\ldots,t_{2^r})+(s_{2^{r-1}+1},\ldots,s_{2^r})(t_1,\ldots,t_{2^{r-1}}))\alpha_r\\
&\qquad +(s_{2^{r-1}+1},\ldots,s_{2^r})(t_{2^{r-1}+1},\ldots,t_{2^r})(\alpha_r+A^{(r-1)}(0,\ldots,1))\\
&\quad = (s_1,\ldots,s_{2^r})\begin{pmatrix} S & T \\ U & V\end{pmatrix}\\
&\quad = (s_1,\ldots,s_{2^r})A^{(r)}(t_1,\ldots,t_{2^r})
\end{aligned}$$

Along the way, we can get an algorithm for multiplication of two elements of K_r as follows:

Algorithm
Input: $r,(s_1,\ldots,s_{2^r}),(t_1,\ldots,t_{2^r})$
Output: $(u_1,\ldots,u_{2^r})$
Procedure:
1. $M_i^0 \leftarrow t_i (1\le i\le 2^r), U^0\leftarrow 1$;
2. for $(j=1, j\le r, j=j+1)$;
   for $(i=1, i\le 2^{r-j}, i=i+1)$;

$$U^r \leftarrow \begin{pmatrix} 0 & U^{(j-1)} \\ (U^{(j-1)})^2 & 2U^{(j-1)}\end{pmatrix}$$

$$M_i^j \leftarrow \begin{pmatrix} M_{2i-1}^{(j-1)} & M_{2i}^{(j-1)} \\ M_{2i}^{(j-1)}U^{(j-1)} & M_{2i-1}^{(j-1)}+M_{2i}^{(j-1)}\end{pmatrix}$$

3. $(u_1,\ldots,u_{2^r})\leftarrow(s_1,\ldots,s_{2^r})M_1^r$
4. return $(u_1,\ldots,u_{2^r})$

We give an example for $r = 3$. The matrix can be generated as follow.

Example 1 *Input* : $r = 3, (t_1, \cdots, t_8)$

1. $M_1^{(0)} = t_1, \cdots, M_8^{(0)} = t_8; U^{(0)} = 1$
2. $j = 1, 1 \le i \le 4$

$$M_1^{(1)} = \begin{pmatrix} M_1^{(0)} & M_2^{(0)} \\ M_2^{(0)}U^{(0)} & M_1^{(0)} + M_2^{(0)} \end{pmatrix}$$
$$M_2^{(1)} = \begin{pmatrix} M_3^{(0)} & M_4^{(0)} \\ M_4^{(0)}U^{(0)} & M_3^{(0)} + M_4^{(0)} \end{pmatrix}$$
$$M_3^{(1)} = \begin{pmatrix} M_5^{(0)} & M_6^{(0)} \\ M_6^{(0)}U^{(0)} & M_5^{(0)} + M_6^{(0)} \end{pmatrix}$$
$$M_4^{(1)} = \begin{pmatrix} M_7^{(0)} & M_8^{(0)} \\ M_8^{(0)}U^{(0)} & M_7^{(0)} + M_8^{(0)} \end{pmatrix}$$
$$U^{(1)} = \begin{pmatrix} 0 & U^{(0)} \\ (U^{(0)})^2 & U^{(0)} \end{pmatrix}$$

$j = 1 + 1 = 2, 1 \le i \le 2$

$$M_1^{(2)} = \begin{pmatrix} M_1^{(1)} & M_2^{(1)} \\ M_2^{(1)}U^{(1)} & M_1^{(1)} + M_2^{(1)} \end{pmatrix}$$
$$M_2^{(2)} = \begin{pmatrix} M_3^{(1)} & M_4^{(1)} \\ M_4^{(1)}U^{(1)} & M_3^{(1)} + M_4^{(1)} \end{pmatrix}$$
$$U^{(2)} = \begin{pmatrix} 0 & U^{(1)} \\ (U^{(1)})^2 & U^{(1)} \end{pmatrix}$$

$j = 2 + 1 = 3, i = 1;$

$$M_1^{(3)} = \begin{pmatrix} M_1^{(2)} & M_2^{(2)} \\ M_2^{(2)}U^{(1)} & M_1^{(2)} + M_2^{(2)} \end{pmatrix}$$
$$U^{(3)} = \begin{pmatrix} 0 & U^{(1)} \\ (U^{(1)})^2 & U^{(1)} \end{pmatrix}$$

By the algorithm above, we can calculate the complexity of it.

Theorem 2 *For $r \ge 1$ and $n = 2^r$, the complexity of the algorithm is $O(n^3)$.*

Proof The claim is clear from the algorithm and the calculation as follows:

$$\begin{aligned} & 2^{r-2} \cdot 2^3 + 2^{r-3} \cdot (2^2)^3 + \cdots + (2^{r-1})^3 \\ =& 2^{r-1}(2^2 + (2^2)^2 + (2^3)^2 + (2^3)^2 + \cdots + (2r-1)^2 \\ =& 2^{r-1}(\frac{2^{2r} - 2^2}{3}) \\ \approx& (2^r)^3. \end{aligned}$$

5 Recursive structures for general p

Similarly, it has the same recursive structure for general p. Set $K_0 = \mathbb{F}_p$ and write the basis of K_1 over K_0 as $\{1, \alpha_1, \ldots, {\alpha_1}^{p-1}\}$. Then

$$K_1 = \{s_0 1 + s_1\alpha_1 + s_2{\alpha_1}^2 + \cdots + s_{p-1}{\alpha_1}^{p-1} | s_0, s_1, \ldots, s_{p-1} \in K_0\}.$$

Write also the basis of K_2 over K_1 as $\{1, \alpha_2, \ldots, {\alpha_2}^{p-1}\}$, then the basis of K_2 over K_0 is given by

$$\{1, \alpha_1, \ldots, {\alpha_1}^{p-1}, \alpha_2, \alpha_2\alpha_1, \ldots, \alpha_2{\alpha_1}^{p-1}, {\alpha_2}^2, {\alpha_2}^2\alpha_1, \ldots, {\alpha_2}^2{\alpha_1}^{p-1}, \ldots, {\alpha_2}^{p-1}, {\alpha_2}^{p-1}\alpha_1, \ldots, {\alpha_2}^{p-1}{\alpha_1}^{p-1}\}.$$

It is clear that the basis of K_r over K_{r-1} is given by $\{1, \alpha_r, \ldots, {\alpha_r}^{p-1}\}$, so we can obtain the basis of K_r over K_0 as

$$\overbrace{(\overbrace{1, \alpha_1, \ldots, {\alpha_1}^{p-1}}^{p} \Big| \alpha_2, \ldots, {\alpha_1}^{p-1}\alpha_2 \Big| \ldots \Big| {\alpha_2}^{p-1}, \ldots, {\alpha_1}^{p-1}{\alpha_2}^{p-1} \Big| \cdots \Big| \ldots, {\alpha_1}^{p-1} \cdots {\alpha_r}^{p-1})}^{p^r}$$

Using the recursive basis, we can multiply two elements without primitive representation.

Theorem 3 *The multiplication of two elements over $\mathbb{F}_{p^p}$ can be expressed as follow:*

$$(s_1, \ldots, s_p)(t_1, \ldots, t_p) = (s_1, \ldots, s_p) \begin{pmatrix} t_1 & t_2 & \ldots & t_{p-1} & t_p \\ t_p & t_1 + t_p & \ldots & t_{p-2} & t_{p-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_3 & t_3 + t_4 & \ldots & t_1 + t_p & t_2 \\ t_2 & t_2 + t_3 & \ldots & t_{p-1} + t_p & t_1 + t_p \end{pmatrix}$$

Let call this $p \times p$ matrix $T_1^{(1)}$. Making the matrices $T_1^{(1)}$ recursively like

$$T_i{}^{r-1} = T^{r-1}(t_{(i-1)p^{r-1}+1}, \ldots, t_{ip^{r-1}}) \ (1 \le i \le p) \text{ and } O^{(r-1)} = T^{r-1}(0, \ldots, 0, 1),$$

one gets the multiplication of two elements over $\mathbb{F}_{p^{p^r}}$ as follow:
$(s_1, \ldots, s_{p^r})(t_1, \ldots, t_{p^r}) = (s_1, \ldots, s_{p^r})$

$$\times \begin{pmatrix} T_1^{(r-1)} & T_2^{(r-1)} & \ldots & T_{p-1}^{(r-1)}. & T_p^{(r-1)} \\ T_p^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_p^{(r-1)} & \ldots & T_{p-2}^{(r-1)} & T_{p-1}^{(r-1)} \\ T_{p-1}^{(r-1)} * O^{(r-1)} & T_{p-1}^{(r-1)} + T_p^{(r-1)} * O^{(r-1)} & \ldots, & T_{p-3}^{(r-1)} & T_{p-2}^{(r-1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ T_3^{(r-1)} * O^{(r-1)} & T_3^{(r-1)} + T_4^{(r-1)} * O^{(r-1)} & \ldots & T_1^{(r-1)} + T_p^{(r-1)} & T_2^{(r-1)} \\ T_2^{(r-1)} * O^{(r-1)} & T_2^{(r-1)} + T_3^{(r-1)} * O^{(r-1)} & \ldots & T_{p-1}^{(r-1)} + T_p^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_p^{(r-1)} \end{pmatrix}.$$

We give the example for $p = 5$ precisely.

Example 2 *Take two elements of $\mathbb{F}_{5^5}$, $(s_1, s_2, s_3, s_4, s_5), (t_1, t_2, t_3, t_4, t_5) \in \mathbb{F}_{5^5}$, then*

$(s_1, s_2, s_3, s_4, s_5)(t_1, t_2, t_3, t_4, t_5) =$

$$(s_1, s_2, s_3, s_4, s_5) \begin{pmatrix} t_1 & t_2 & t_3 & t_4 & t_5 \\ t_5 & t_1 + t_5 & t_2 & t_3 & t_4 \\ t_4 & t_4 + t_5 & t_1 + t_5 & t_2 & t_3 \\ t_3 & t_3 + t_4 & t_4 + t_5 & t_1 + t_5 & t_2 \\ t_2 & t_2 + t_3 & t_3 + t_4 & t_4 + t_5 & t_1 + t_5 \end{pmatrix}$$

Here set $T_1 = \begin{pmatrix} t_1 & t_2 & t_3 & t_4 & t_5 \\ t_5 & t_1 + t_5 & t_2 & t_3 & t_4 \\ t_4 & t_4 + t_5 & t_1 + t_5 & t_2 & t_3 \\ t_3 & t_3 + t_4 & t_4 + t_5 & t_1 + t_5 & t_2 \\ t_2 & t_2 + t_3 & t_3 + t_4 & t_4 + t_5 & t_1 + t_5 \end{pmatrix}.$

Now let $(s_1,\ldots,s_{5^r}),(t_1,\ldots,t_{5^r}) \in \mathbb{F}_{5^{5^r}}$*, then the multiplication is given as follows:*
$(s_1,\ldots,s_{5^r})(t_1,\ldots,t_{5^r}) = (s_1,\ldots,s_{5^r})$

$$\times \begin{pmatrix} T_1^{(r-1)} & T_2^{(r-1)} & T_3^{(r-1)} & T_4^{(r-1)} & T_5^{(r-1)} \\ T_5^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_5^{(r-1)} & T_2^{(r-1)} & T_3^{(r-1)} & T_4^{(r-1)} \\ T_4^{(r-1)} * O^{(r-1)} & T_4^{(r-1)} + T_5^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_5^{(r-1)} & T_2^{(r-1)} & T_3^{(r-1)} \\ T_3^{(r-1)} * O^{(r-1)} & T_3^{(r-1)} + T_4^{(r-1)} * O^{(r-1)} & T_4^{(r-1)} + T_5^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_5^{(r-1)} & T_2^{(r-1)} \\ T_2^{(r-1)} * O^{(r-1)} & T_2^{(r-1)} + T_3^{(r-1)} * O^{(r-1)} & T_3^{(r-1)} + T_4^{(r-1)} * O^{(r-1)} & T_4^{(r-1)} + T_5^{(r-1)} * O^{(r-1)} & T_1^{(r-1)} + T_5^{(r-1)} \end{pmatrix},$$

where ${T_i}^{r-1} = T^{r-1}(t_{(i-1)5^{(r-1)}+1},\ldots,t_{i5^{(r-1)}})$ $(1 \le i \le 5)$ *and* $O^{(r-1)} = T^{r-1}(0,\ldots,0,1)$.

6 Experimental results when $p = 2$

In this section, we mention the experimental results [1] for the algorithm given in the section 4. The multiplication algoritm is implemented with GCC 4.0 to the machine with Core 2 Duo CPU 2.2GHz and 2GB Memory. For randomly chosen two elements of $K_r = \mathbb{F}_{2^{2^r}}$, average time for the multiplication of these two elements are shown below.

r	8	9	10	11	12	13
time (second)	0.223	1.412	9.503	95.32	1343	12578

7 Concluding remarks

We gave the method to construct a finite field start with a prime field $\mathbb{F}_p$ for simplicity on the talk. One can easily imagine the ame construction is possible using the Artin-Schreier tower start from a finite field $\mathbb{F}_q$. Moreover, we can develop the similar theory for any extenion of the Artin-Schreier type, and we will treat this in another occasion. As an application of our Artin-Shcreier tower, we are developing a better pseudo random numeber generation method, and we will treat this in another occasion also.

References

[1] *David G.Cantor*:On Arithmetical over Finite Fields, Journal of Combinatorial Theory, Series A 50, 285-300, 1989.

[2] *Luca De Feo and Éric Schost*: Fast Arithmetics in Artin-Schreier Towers over Finite Fields, ISSAC'09, 2009.

[3] *Ito,H. and Kajiwara,T. and Song*: A Tower of Artin-Schreier extensions of finite fields and its applications, preprint.

[4] *Gadiel Seroussi*: Table of Low-Weight Binary Irreducible Polynomials, 1998, available at http://www.hpl.hp.com/techreports/98/HPL-98-135.html

[5] *Miodrag Živković*: A Table of Primitive Binary Polynomials, **62**, Issue 205, 385–386, Jan. 1994.

Graduate School of Engineering, Hiroshima University, Higashi-Hiroshima, 739-8527, Japan.

E-mail address: huiling@amath.hiroshima-u.ac.jp

E-mail address: hiroito@amath.hiroshima-u.ac.jp

[1] The authors would like to thank Mr. Wiying Wei who helped to the first author for getting the experimental results.

互いに素なシュタイナー系 S(5,8,24) と 5-(24,12,48) デザイン

新谷 誠
静岡大学情報学部

2009 年 12 月 2 日

Proceedings には講演で使用したスライドをもとにした報告書を作成しました。講演を行った内容の論文 M. Araya and M. Harada, Mutually disjoint Steiner systems $S(5,8,24)$ and 5-$(24,12,48)$ designs, The Electronic Journal of Combinatorics, 17(1), N1, 2010. が、電子ジャーナル（http://www.combinatorics.org/）に出版されましので、そちらも参照してください。

概 要

互いに素なシュタイナー系 $S(5,8,24)$ が 50 個以上、互いに素な 5-$(24,12,48)$ デザインが 35 個以上存在することを示した。

1 記号と定義

この節では記号、用語の定義を行う。

Definition 1 X : v-*set,* $k \in \mathbb{Z}$ とする。このとき

$$\binom{X}{k} := \{\ Y \subset X \mid |Y| = k\ \}, \binom{v}{k} := \left|\binom{X}{k}\right|$$

と定義する。

Definition 2 $t, v, k, \lambda \in \mathbb{Z},\ 0 < t \leq k \leq v$
X : v point *set,* $\mathcal{B} \subset \binom{X}{k}$: block *set* とする。

- $D = (X, \mathcal{B})$: $\underline{t\text{-}(v,k,\lambda)\ design}$
  $\overset{def}{\iff} |\{B \in \mathcal{B} | T \subset B\}| = \lambda\ for\ {}^{\forall}T \in \binom{X}{t}$
- $D = (X, \mathcal{B})$: $\underline{Steiner\ system\ S(t,k,v)}$
  $\overset{def}{\iff} D = (X, \mathcal{B})$: t-$(v,k,1)$ *design*

Example 3 $X = \{1,2,3,4,5,6,7\}$, $\mathcal{B} = \{\{1,2,3\},\{1,4,5\},\{1,6,7\},\{2,4,7\},\{2,5,6\},\{3,4,6\},\{3,5,7\}\} \subset \binom{X}{3}$ とする。
$^{\forall}T \in \binom{X}{2} = \{\{i,j\} \mid 1 \leq i < j \leq 7\}$ に対して

$$|\{B \in \mathcal{B} \mid T \subset B\}| = 1$$

となる。ゆえに $D = (X, \mathcal{B})$ は 2-$(7,3,1)$ デザインである。*($D = (X, \mathcal{B})$ は Steiner system $S(2,3,7)$ である。)*

Definition 4 $D_1 = (X, \mathcal{B}_1), \ldots, D_n = (X, \mathcal{B}_n)$ *: t-(v,k,λ) designs* とする。
$D_1, \ldots, D_n$ *: mutually disjoint designs*
$\overset{def}{\iff} \mathcal{B}_i \cap \mathcal{B}_j = \phi \ (i \neq j)$

Remark 5 $D_1, \ldots, D_n$ *: mutually disjoint t-(v,k,λ) designs*
$\Longrightarrow (X, \cup_{i=1}^{n} \mathcal{B}_i)$ *: t-$(v,k,n\lambda)$ design*

Definition 6 $D = (X, \mathcal{B})$ *: t-(v,k,λ) design,*
S_X*: symmetric group on X* とする。
$\sigma \in S_X$ に対し、 $\mathcal{B}^{\sigma} := \{B^{\sigma} | B \in \mathcal{B}\}$ と定義する。

2 5-designs

1 節で定義を行ったデザインは t, v, k, λ の 4 つのパラメータで定義される組合せ対象である。そこで、次の問題が考えられる。

研究問題　与えられた t, v, k, λ に対して、t-(v,k,λ) デザインが存在するのか？

次の定理により、t, v, k を与えた時に λ の範囲、λ がある数の倍数になることがわかる。

Theorem 7 $D = (X, \mathcal{B})$*: t-(v,k,λ) design* $\Longrightarrow |\mathcal{B}| = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$

例　本報告で扱ったパラメータに関しては次のようになる。

- D : $S(5,8,24) \Longrightarrow |\mathcal{B}| = 759$
- D : 5-$(24,12,48)$ design $\Longrightarrow |\mathcal{B}| = 2576$
- $\mathbb{Z} \ni |\mathcal{B}| \leq \binom{v}{k}$ より
  - D : 5-$(24,8,\lambda)$ design $\Longrightarrow \lambda = 1, 2, \ldots, 969$
  - D : 5-$(24,12,\lambda)$ design $\Longrightarrow \lambda = 6m,\ m = 1, \ldots, 4199$

5-$(24,8,\lambda)$ design の存在については解決している。

- $\lambda \leq 9$ by Kramer and Magliveras [5].
- $\lambda \geq 16$ by Betten, Haberberger, Laue and Wassermann.
- $\lambda \leq 15$ by Araya [1].

特に、Araya によりコンピュータを用いた計算で互いに素な $S(5,8,24)$ が 15 個以上存在することが示されている。

5-$(24,12,6m)$ design の存在については未解決である。[4]

- $m=1,2$ のとき非存在
- 存在が知られている最小の $m=8$, i.e., $\lambda=48$

Jimbo-Shiromoto[3] では互いに素な $S(5,8,24)$ が 22 個以上存在することを、コンピュータを使わずに $S(5,8,24)$ から生成される Golay 符号の共通集合を計算することにより示している。

$H=\begin{pmatrix} & & 1 \\ I_{12} & A & . \\ & & 1 \\ & 1\dots1 & 0 \end{pmatrix}$, A : circulant matrix に対し、
$C:=\{\boldsymbol{x}\in\mathbb{F}_2^{24}|H\boldsymbol{x}=0\}$: Golay $[24,12,8]$ code とする。
$\mathcal{B}:=\{supp(\boldsymbol{x})|\boldsymbol{x}\in C, wt(x)=8\}$ とすると、
$(X,\mathcal{B})$: $S(5,8,24)$ である。

Theorem 8 $\sigma=(13,14,\dots,23), \tau=(1,13)(2,14)\dots(11,23)\in S_X$, $G=\{\sigma^i\tau^j|i=0,\dots,10,\ j=0,1\}\Longrightarrow\{(X,\mathcal{B}^g)|g\in G\}$ *: 22 mutually disjoint* $S(5,8,24)$

3 研究目的と方法

$D=(X,\mathcal{B})$ を $S(5,8,24)$ または 5-$(24,12,48)$ デザインとする。コンピュータによる計算で $\mathcal{B}^{\sigma_i}\cap\mathcal{B}^{\sigma_j}=\phi$ を満たす置換 $\sigma_1,\dots,\sigma_n\in S_X$ を探すことにより互いに素なデザインを構成することを目的とする。

$S(5,8,24)$ について知られている結果についてまとめておく。次に書いたように、同型を除いて一意的であり、自己同型群も計算されている。

- $D=(X,\mathcal{B}), D'=(X,\mathcal{B}')$: $S(5,8,24)$
  $\Longrightarrow{}^{\exists}\sigma\in S_X$ s.t. $\mathcal{B}^\sigma=\mathcal{B}'$
- $D=(X,\mathcal{B})$: $S(5,8,24)$ $Aut(D):=\{\sigma\in S_X|\mathcal{B}^\sigma=\mathcal{B}\}$
  $\Longrightarrow Aut(D)=M_{24}$: the Mathieu group, $|M_{24}|=244823040$
- $M_{24}\sigma=M_{24}\tau$ とすると $\mathcal{B}^\sigma=\mathcal{B}^\tau$ より、$\sigma_1,\dots,\sigma_n\in S_X$ $(\mathcal{B}^{\sigma_i}\cap\mathcal{B}^{\sigma_j}=\phi)$ を S_{24}/M_{24} の代表元から探す。
  $|S_{24}/M_{24}|=2534272925184000$

次のようなアルゴリズムにより計算を行った。Step 0 では Jimbo-Shiromoto で求められた 22 個の互いに素な $S(5,8,24)$ を初期値としている。Step 1 では完全代表系を求めることが困難であるので、その部分集合でである V を求めている。Step 2 で得られた maximum clique を成す置換が互いに素な $S(5,8,24)$ を与える。

Step 0 (cf. Jimbo and Shiromoto[3])

- $D_0=(X,\mathcal{B})$: $S(5,8,24)$
- $\mathcal{B}_1=\cup_{g\in G}\mathcal{B}^g$, $D_1=(X,\mathcal{B}_1)$: 5-$(24,8,22)$ design

Step 1 (cf. Dixon and Majeed[2])

- Find $V \subset \{\sigma \in S_X | \mathcal{B}^\sigma \cap \mathcal{B}_1 = \phi, M_{24}\sigma \neq M_{24}g (g \in G)\}$.

Step 2

- Define a graph Γ with a vertex set V
  and a edge set $E = \{\{\sigma, \tau\} | \mathcal{B}^\sigma \cap \mathcal{B}^\tau = \phi\}$.
- Find a maximum clique in Γ.

Step1 で剰余類の代表元を求める計算を Dixon-Majeed [2] の方法により行っている。その計算結果を簡単にまとめておく。

$\Delta, \Delta' \subset X,\ \Delta \cap \Delta' = \phi$ に対し、次のような置換の集合を考える。
Select$(\Delta, \Delta') := \{id\} \cup (\cup_{i=1}^{k} \{(\gamma_1, \delta_1)(\gamma_2, \delta_2) \cdots (\gamma_i, \delta_i) \mid \gamma_1 < \cdots < \gamma_i \in \Delta, \delta_1 < \cdots < \delta_i \in \Delta'\})$
$(k = \min\{|\Delta|, |\Delta'|\}$, id: identity permutation)

このとき
$\Delta_1 = \{6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 23, 24\}$
$\Delta_2 = \{8, 9, 11, 12, 14, 15, 16, 17, 18, 20, 23, 24\}$
$U_6 = \text{Select}(\Delta_1, \{10, 19, 22\})$
$U_7 = \text{Select}(\{7, 13, 21\}, \Delta_2)$
$H^{(7)} = S_{\{13,21\}} \times S_{\Delta_2} \times S_{\{10,19,22\}}$
に対し $H^{(7)}U_7U_6$ が剰余類の完全代表系を与える。

4 結果

コンピュータによる計算により次の結果が得られた。正確なデータは M. Araya and M. Harada, Mutually disjoint Steiner systems $S(5, 8, 24)$ and 5-$(24, 12, 48)$ designs, The Electronic Journal of Combinatorics, 17(1), 2010. を参照してください。

Theorem 9 *There are at least* 50 *mutually disjoint* $S(5, 8, 24)$.
There are at least 35 *mutually disjoint* 5-$(24, 12, 48)$ *designs.*

特に $m = 24, 32, 40, 48, 56, 64, 72, 80, 112, 120, 128, 136, 144, 152, 160, 168, 200, 208, 216, 224, 232, 240, 248, 256,$ に対して、5-$(24, 12, 6m)$ デザインがはじめて構成できた。

5 今後の課題

互いに素な 969 個の $S(5, 8, 24)$ が存在するかどうかが今後の課題である。また、計算量を減らすために次のように小さなデザイン D' で互いに素な 969 個の $S(2, 5, 21)$ が存在するかどうかも今後の課題である。

Theorem 10 $D = (X, \mathcal{B})$ *:* $S(5, 8, 24)$
$X' := X - \{22, 23, 24\}$
$\mathcal{B}' := \{B - \{22, 23, 24\} | 22, 23, 24 \in B \in \mathcal{B}\}$
$\Longrightarrow D' = (X', \mathcal{B}')$ *:* $S(2, 5, 21)$

参考文献

[1] M. Araya, More mutually disjoint Steiner systems $S(5, 8, 24)$, *J. Combin. Theory Ser. A* **102** (2003), 201–203.

[2] J.D. Dixon and A. Majeed, Coset representatives for permutation groups, *Portugal. Math.* **45** (1988), 61–68.

[3] M. Jimbo and K. Shiromoto, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, *J. Combin. Theory Ser. A* **116** (2009), 1245–1251.

[4] G.B. Khosrovshahi and R. Laue, "t-Designs with $t \geq 3$," Handbook of Combinatorial Designs (Second edition), C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2007, pp. 79–101.

[5] E.S. Kramer and S.S. Magliveras, Some mutually disjoint Steiner systems, *J. Combin. Theory Ser. A* **17** (1974), 39–43.

A Coding Theoretic Study on MLL Proof Nets (Extended Abstract)

Satoshi Matsuoka
National Institute of Advanced Industrial Science and Technology (AIST),
1-1-1 Umezono,
Tsukuba, Ibaraki,
305-8563 Japan
matsuoka@ni.aist.go.jp

Abstract

Linear Logic has been one of most exciting topics in computer science oriented researches of logic for the last few decades. One of striking features of Linear Logic is the notion of proof nets, which are a representation method of proofs or programs (via Curry-Howard correspondence) in Linear Logic using directed graphs. MLL proof nets are the core part of proof nets and their theory has a firm status, while larger fragments of proof nets not. Therefore studying MLL proof nets in depth is meaningful.
In this talk, we propose a novel approach to analyze MLL proof nets using coding theory. We define families of proof structures and introduce a metric space for each family. In each family,

1. an MLL proof net is a true code element;
2. a proof structure that is not an MLL proof net is a false (or corrupted) code element.

The definition of our metrics reflects the duality of the multiplicative connectives elegantly. Our main theorem in the framework states that one error-detecting is possible but one error-correcting not. Our proof of the impossibility of one error-correcting is interesting in the sense that a proof theoretical property is proved using a graph theoretical argument.

Keywords: Linear Logic, proof nets, error-correcting codes, graph isomorphisms, combinatorics

1 Introduction

Linear Logic is a logical system proposed by J.Y. Girard in 1987 [Gir87]. A way to understand Linear Logic is a decomposition of **LK**, which is a formal system for Classical Logic invented by Gentzen, into three parts: (a) multiplicative part, (b) additive part, and (c) exponential part. Among them, multiplicative part is the core and can be studied solely: the other parts must be studied with the multiplicative part. The multiplicative part is also called the multiplicative fragment.
Moreover, the study of the multiplicative fragment of Linear Logic without multiplicative constants (for short MLL) [Gir87] is successful from both semantical and syntactical point of view. In semantical point of view there are good semantical models including coherent spaces. In syntactical point of view the theory of MLL proof nets has obtained a firm status without doubt. On the other hand the intuitionistic multiplicative fragment of Linear Logic without multiplicative constants (for short IMLL) is also studied, for example, in [Mat07]. IMLL can be seen as a subsystem of MLL. IMLL is easier to be studied more deeply than MLL, because we can use intuitions inspired from the conventional lambda-calculus theory as well as graph-theoretic intuitions from the MLL proof nets theory. We exploited both benefits in [Mat07].
In order to study MLL more deeply, how should we do? One approach is to interpret MLL intuitionistically by using Gödel's double negation interpretation. One example is [Has05]. However in such an approach multiplicative constants must be introduced. Definitely introducing multiplicative constants makes things complicated. Another approach we propose in this paper is to adopt *coding theoretic* framework.
Basically, coding theory [Bay98, MS93] is to study a way of detecting and/or correcting data that may be true or false. Moreover coding theory is an area of mathematics, in which there is an interplay between many

branches of mathematics, e.g., abstract algebra, combinatorics, discrete geometry, information theory, etc. In this paper we propose a novel approach for analyzing proof nets of Multiplicative Linear Logic (MLL) by coding theory. We define families of proof structures and introduce a metric space for each family. In each family,

1. an MLL proof net is a true code element, which is usually called a *codeword* in the literature of coding theory;

2. a proof structure that is not an MLL proof net is a false (or corrupted) code element.

Figure 1 shows an explanatory example. All three examples in Figure 1 are MLL proof nets in a standard notation of [Gir87]. In our framework the left and the middle proof nets belong to the same family, because when we forget $\otimes$ and $\parr$ symbols, these are the same (although in fact, these are equal without forgetting those symbols. We will discuss the matter later). But the right proof net does not belong to the family, because when we forget $\otimes$ and $\parr$ symbols from the right one, we can not identify this one with the previous one by the mismatch of the literals p and $p^{\perp}$. The subtle point will be discussed later in a more precise way (see Subsection 3.1). The definition of our metrics reflects the duality of the multiplicative connectives

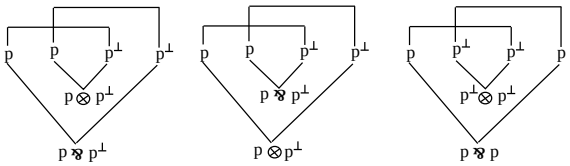

Figure 1: An explanatory example

elegantly. Moreover introducing the framework makes it possible to apply different results and techniques of other branches of mathematics to the study of MLL proof nets. In particular, our concern is closely related to the following question: given a condition about proof nets (for example, that of the number of ID-links), how many proof nets do we have such that they satisfy the condition? As far as we know, in the literature, there are only a few discussions about such a counting problem on proof theory.
So far, most of the study of MLL proof nets have focused on individual proof nets (e.g., sequentialization theorem [Gir87]) or the relationship between identifiable proof nets (e.g., cut-elimination and η-expansion). On the other hand, our approach focuses on a relationship between similar, but different proof nets. In particular, our notion of similarity of proof nets seems to be unable to be understood by conventional type theory.
The main technical achievement of this paper is Theorem 3, which says that in our framework one error-detecting is possible but one error-correcting not. Our proof of the theorem is interesting in the sense that a proof-theoretic property is proved by a graph-theoretic argument.

The Structure of the Paper: Section 2 introduces basic properties of MLL proof nets. MLL proof nets are defined and sequentialization theorem on them is described. Moreover, the notion of empires, which are needed in order to prove the main theorems, is introduced. Section 3 introduces the notion of PS-families (families of proof structures) and distances on them. It is shown that they are metric spaces. Then other basic properties w.r.t PS-families and the main theorems are stated. Most of details of the proofs are omitted and given in [Mat10]. An example is also given (Example 1). Finally, future research directions about PS-families and elementary results on them are stated.

2 The MLL System

2.1 The Basic Theory of MLL Proof Nets

In this section, we present multiplicative proof nets. We also call these *MLL proof nets* (or simply, *proof nets*). First we define MLL formulas. In this paper, we only consider MLL formulas with the only one propositional variable p because the restriction does not give any essential differences w.r.t our main results.

By the same reason we restrict ID-links to them with literal conclusions. Moreover we do not consider Cut-links and Cut-elimination because our main results do not concern them.

Definition 1 (Literals) *A literal is p or $p^\perp$. The positive literal is p and the negative literal is $p^\perp$.*

Definition 2 (MLL Formulas) *MLL formulas (or simply formulas) F is any of the followings:*

- *F is a literal;*
- *F is $F_1 \otimes F_2$, where F_1 and F_2 are MLL formulas. Then F is called $\otimes$-formula.*
- *F is $F_1 \parr F_2$, where F_1 and F_2 are MLL formulas. Then F is called $\parr$-formula.*

We denote the set of all the MLL formulas by MLLFml.

Definition 3 (Negations of MLL Formulas) *Let F be an MLL formula. The negation $F^\perp$ of F is defined as follows according to the form of F:*

- *if F is p, then $F^\perp \equiv_{\mathrm{def}} p^\perp$;*
- *if F is $p^\perp$, then $F^\perp \equiv_{\mathrm{def}} p$;*
- *if F is $F_1 \otimes F_2$, then $F^\perp \equiv_{\mathrm{def}} F_1^\perp \parr F_2^\perp$;*
- *if F is $F_1 \parr F_2$, then $F^\perp \equiv_{\mathrm{def}} F_1^\perp \otimes F_2^\perp$.*

So, $F^\perp$ is actually an MLL formula.

Definition 4 (Indexed MLL Formulas) *An indexed MLL formula is a pair $\langle F, i\rangle$, where F is an MLL formula and i is a natural number.*

Figure 2 shows the links we use in this paper. We call each link in Figure 2 *an MLL link* (or simply *link*). In Figure 2,

1. In ID-link, $\langle A, i\rangle$ and $\langle A^\perp, j\rangle$ are called conclusions of the link.
2. In $\otimes$-link (resp. $\parr$-link) $\langle A, i\rangle$ is called the left premise, $\langle B, j\rangle$ the right premise and $\langle A \otimes B, k\rangle$ (resp. $\langle A \parr B, k\rangle$) the conclusion of the link.

Moreover we call links except ID-links *multiplicative links*.

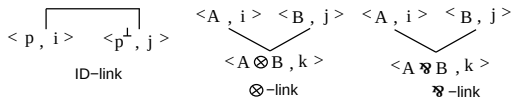

Figure 2: MLL links

Definition 5 (MLL Proof Structures) *Let $\mathbb{F}$ be a finite set of MLL formula occurrences, i.e., a finite set of indexed MLL formulas and $\mathbb{L}$ be a finite set of MLL link occurrences such that for each $L \in \mathbb{L}$, the conclusions and the premises of L belong to $\mathbb{F}$. The pair $\Theta = \langle \mathbb{F}, \mathbb{L}\rangle$ is an MLL proof structure (or simply, a proof structure) if Θ satisfies the following conditions:*

1. *for any $\langle F_0, i\rangle$ and $\langle F_0', j\rangle$ in $\mathbb{F}$, if $i = j$, then $F_0 = F_0'$ (i.e., in $\mathbb{F}$, each element has a different index number).*
2. *for each formula occurrence $F \in \mathbb{F}$ and for each link occurrence $L \in \mathbb{L}$, if F is a premise of L then L is unique, i.e., F is not a premise of any other link $L' \in \mathbb{L}$.*
3. *for each formula occurrence $F \in \mathbb{F}$, there is a unique link occurrence $L \in \mathbb{L}$ such that F is a conclusion of L.*

Remark. In the following, when we discuss proof structures or proof nets, in many cases, we conveniently forget indices for them, because such information is superfluous in many cases. Moreover, when we draw a proof structure or a proof net, we also forget such an index, because locative information in such drawings plays an index.

We say that in $\Theta = \langle \mathbb{F}, \mathbb{L} \rangle$, a formula occurrence $F \in \mathbb{F}$ is a conclusion of Θ if for any $L \in \mathbb{L}$, F is not a premise of L.
It is well-known that a proof structure does not necessarily correspond to a sequent calculus proof. For example, two MLL proof structures in Figure 3 do not the corresponding sequent calculus proofs. The following sequentializability is a judgement on the correspondence.

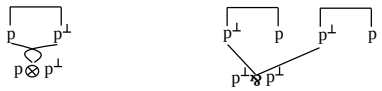

Figure 3: Two examples of MLL proof structures

Definition 6 (Sequentializability) *A MLL proof structure $\Theta = \langle \mathbb{F}, \mathbb{L} \rangle$ is sequentializable if any of the following conditions holds:*

1. *$\mathbb{L} = \{L\}$ and L is an ID-link;*
2. *There is a $\parr$-link $L \in \mathbb{L}$ such that the conclusion $A \parr B$ of L is a conclusion of Θ and $\langle \mathbb{F} - \{A \parr B\}, \mathbb{L} - \{L\} \rangle$ is sequentializable.*
3. *There is a $\otimes$-link $L \in \mathbb{L}$ and there are two subsets $\mathbb{F}_1$ and $\mathbb{F}_2$ of $\mathbb{F}$ and two subsets $\mathbb{L}_1$ and $\mathbb{L}_2$ of $\mathbb{L}$ such that (a) the conclusion $A \otimes B$ of L is a conclusion of Θ, (b) $\mathbb{F} = \mathbb{F}_1 \uplus \mathbb{F}_2 \uplus \{A \otimes B\}$, (c) $\mathbb{L} = \mathbb{L}_1 \uplus \mathbb{L}_2 \uplus \{L\}$, and (d) $\langle \mathbb{F}_1, \mathbb{L}_1 \rangle$ (respectively $\langle \mathbb{F}_2, \mathbb{L}_2 \rangle$) is an MLL proof structure and sequentializable, where $\uplus$ denotes the disjoint union operator.*

Definition 7 (MLL Proof Nets) *An MLL proof structure Θ is an MLL proof net if Θ is sequentializable.*

Next we give a graph-theoretic characterization of MLL proof nets, following [Gir96]. The characterization was firstly proved in [Gir87] and then an improvement was given in [DR89]. In order to characterize MLL proof nets among MLL proof structures, we introduce *Danos-Regnier graphs (for short, DR-graphs)*. Let Θ be an MLL proof structure. We assume that we are given a function S from the set of the occurrences of $\parr$-links in Θ to $\{0, 1\}$. Such a function is called a *DR-switching* for Θ. Then the Danos-Regnier graph Θ_S for Θ and S is a undirected graph such that

1. the nodes are all the formula occurrences in Θ, and
2. the edges are generated by the rules of Figure 4.

In the following we also use the alternative notation $S(\Theta)$ for the Danos-Regnier graph Θ_S.
The following theorem by Girard, Danos, and Regnier [Gir87, DR89], which is called *sequentialization theorem*, is the most important theorem in the theory of MLL proof nets.

Theorem 1 *An MLL proof structure Θ is an MLL proof net iff for each switching function S for Θ, the Danos-Regnier graph Θ_S is acyclic and connected.*

2.2 Empires

In this subsection, we introduce *empires* following [Gir06]. The notion is needed to establish our main results. First we fix a proof structure $\Theta = \langle \mathbb{F}_\Theta, \mathbb{L}_\Theta \rangle$. Moreover we introduce the notations $\mathrm{fml}(\Theta) \equiv_{\mathrm{def}} \mathbb{F}_\Theta$ and $\mathrm{lnk}(\Theta) \equiv_{\mathrm{def}} \mathbb{L}_\Theta$.

Definition 8 (Empires) *The empire of a formula A in a proof net $\Theta = \langle \mathbb{F}, \mathbb{L} \rangle$ (denoted by $e_\Theta(A)$) is defined in the following manner: let S be a DR-switching for Θ. Then an undirected maximal connected graph $(\Theta_S)^A$ (or simply ${\Theta_S}^A$) is defined as follows:*

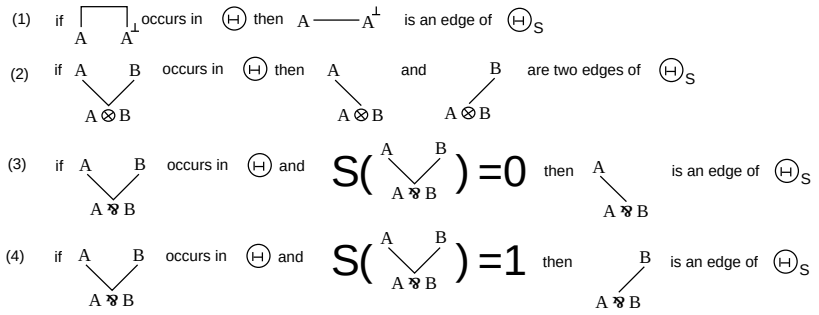

Figure 4: The rules for the generation of the edges of a Danos-Regnier graph Θ_S

1. *If there is a link $L \in E$ such that A is a premise of L and there is the edge e from A to the conclusion of L in Θ_S, then $(\Theta_S)^A$ is the maximal connected graph including A obtained from Θ_S by deleting e;*

2. *otherwise, $(\Theta_S)^A = \Theta_S$.*

Then the empire A in Θ (denoted by $e_\Theta(A)$) is defined as follows:

$$e_\Theta(A) \equiv_{\mathrm{def}} \bigcap_{S \text{ is a DR-switching for } \Theta} \mathrm{fml}({\Theta_S}^A)$$

From the definition it is obvious that $A \in e_\Theta(A)$. Although the empire $e_\Theta(A)$ is defined as a set of formula occurrences, by considering the set $\mathbb{L}_{e_\Theta(A)}$ of links whose conclusions and premises are all included in $e_\Theta(A)$, the empire $e_\Theta(A)$ can be considered as the pair $\langle e_\Theta(A), \mathbb{L}_{e_\Theta(A)}\rangle$.
Basic properties on empires are given, for example, in [Gir87, BW95, Mat10]. Many of them are used to prove statements in Section 3.

3 Families of Proof Structures

3.1 Our Framework

Firstly we define families of proof-structures. Informally two proof structures Θ_1 and Θ_2 that belong to the same family means that Θ_2 is obtained from Θ_1 by replacing several $\otimes$-links (resp. $\parr$-links) by $\parr$-links (resp. $\otimes$-links). We define such families using graph isomorphisms on directed graphs in a mathematically rigorous way. The reader might feel that the following definitions in this subsection are too cumbersome. But there is a subtle point of the definitions. That is the reason why we insist on a rigorous style. We will discuss this matter at the end of the subsection.

Definition 9 (Strip Function) *A function $\mathrm{strp}_{\otimes\parr} : \mathrm{MLLFml} \to \{p, p^\perp, \otimes, \parr\}$ is defined as follows:*

1. $\mathrm{strp}_{\otimes\parr}(p) = p$ *and* $\mathrm{strp}_{\otimes\parr}(p^\perp) = p^\perp$;

2. $\mathrm{strp}_{\otimes\parr}(A \otimes B) = A \otimes B$ *and* $\mathrm{strp}_{\otimes\parr}(A \parr B) = \parr$.

Definition 10 (Labelled Directed Graphs) *Let $\mathbb{A}$ and $\mathbb{B}$ be sets. A labelled directed graph with labels $\mathbb{B}$ (resp. $\mathbb{A}$ and $\mathbb{B}$) is a tuple $\langle V, E, \ell_E : E \to \mathbb{B}\rangle$ (resp. $\langle V, E, \ell_V : V \to \mathbb{A}, \ell_E : E \to \mathbb{B}\rangle$) satisfying the following conditions:*

1. *V is a set;*

2. *E is a set with two functions* $\mathrm{src} : E \to V$ *and* $\mathrm{tgt} : E \to V$.

In the following, we suppose $\mathbb{A} = \{p, p^\perp, \otimes, \parr\}$ and $\mathbb{B} = \{\mathbf{L}, \mathbf{R}, \mathbf{ID}\}$.

Next we define a translation from proof structures to labelled directed graphs and that with a function $f : \mathrm{MLLFml} \to \mathbb{A}$ as a parameter.

Definition 11 (Labelled Directed Graphs Induced by Proof Structures) *Let $\Theta = \langle \mathbb{F}, \mathbb{L} \rangle$ be a proof structure and $f : \mathrm{MLLFml} \to \mathbb{A}$. A labelled directed graph $G(\Theta) = \langle V, E, \ell_E : E \to \{\mathbf{L}, \mathbf{R}, \mathbf{ID}\} \rangle$ and $G^f(\Theta) = \langle V, E, \ell_V^f : V \to \mathbb{A}, \ell_E : E \to \{\mathbf{L}, \mathbf{R}, \mathbf{ID}\} \rangle$ is defined from Θ in the following way:*

1. *$V = \{i \mid \langle A, i \rangle \in \mathbb{F}\}$ and $\ell_V^f = \{\langle i, f(A) \rangle \mid \langle A, i \rangle \in \mathbb{F}\}$;*
   Since in Θ, each formula occurrence has a unique index, we can easily see that V is bijective to $\mathbb{F}$.
2. *E and ℓ_E is the least set satisfying the following conditions:*
   - *If $L \in \mathbb{L}$ is an ID-link occurrence with conclusions $\langle p, i \rangle$ and $\langle p^\perp, j \rangle$, then there is an edge $e \in E$ such that $\mathrm{src}(e) = i$ and $\mathrm{tgt}(e) = j$ and $\langle e, \mathbf{ID} \rangle \in \ell_E$;*
   - *If $L \in \mathbb{L}$ is a $\otimes$-link occurrence with the form $\frac{\langle A, i \rangle \quad \langle B, j \rangle}{\langle A \otimes B, k \rangle}$, then there are two edges $e_1 \in E$ and $e_2 \in E$ such that $\mathrm{src}(e_1) = i$, $\mathrm{tgt}(e_1) = k$, $\mathrm{src}(e_2) = j$, $\mathrm{tgt}(e_2) = k$, $\langle e_1, \mathbf{L} \rangle \in \ell_E$, and $\langle e_2, \mathbf{R} \rangle \in \ell_E$;*
   - *If $L \in \mathbb{L}$ is a $\parr$-link occurrence with the form $\frac{\langle A, i \rangle \quad \langle B, j \rangle}{\langle A \parr B, k \rangle}$, then there are two edges $e_1 \in E$ and $e_2 \in E$ such that $\mathrm{src}(e_1) = i$, $\mathrm{tgt}(e_1) = k$, $\mathrm{src}(e_2) = j$, $\mathrm{tgt}(e_2) = k$, $\langle e_1, \mathbf{L} \rangle \in \ell_E$, and $\langle e_2, \mathbf{R} \rangle \in \ell_E$.*

The next definition is a slight extension of the standard definition of graph isomorphisms.

Definition 12 (Graph Isomorphisms on Labelled Directed Graphs) *Let $G_1 = \langle V_1, E_1, \ell_{E_1} \rangle$ (resp. $G_1 = \langle V_1, E_1, \ell_{V_1}, \ell_{E_1} \rangle$) and $G_2 = \langle V_2, E_2, \ell_{V_2}, \ell_{E_2} \rangle$ (resp. $G_2 = \langle V_2, E_2, \ell_{E_2} \rangle$) be labelled directed graphs. Then a graph homomorphism from G_1 to G_2 is a pair $\langle h_V : V_1 \to V_2, h_E : E_1 \to E_2 \rangle$ satisfying the following conditions:*

1. *for any $e \in E_1$, $h_V(\mathrm{src}(e)) = \mathrm{src}(h_E(e))$ and $h_V(\mathrm{tgt}(e)) = \mathrm{tgt}(h_E(e))$;*
2. *(only the case where ℓ_{V_1} and ℓ_{V_2} are specified) for any $v \in V_1$, $\ell_{V_1}(v) = \ell_{V_2}(h_V(v))$;*
3. *for any $e \in E_1$, $\ell_{E_1}(e) = \ell_{E_2}(h_E(e))$.*

The graph homomorphism $\langle h_V, h_E \rangle$ is a graph isomorphism if $h_V : V_1 \to V_2$ and $h_E : E_1 \to E_2$ are both bijections (then, we write $\langle h_V, h_E \rangle : G_1 \simeq G_2$).

Definition 13 (PS-families) *Let Θ_1 and Θ_2 be proof structures. Then $\Theta_1 \sim \Theta_2$ if there is a graph isomorphism $\langle h_V : V_1 \to V_2, h_E : E_1 \to E_2 \rangle$ from $G(\Theta_1) = \langle V_1, E_1, \ell_{E_1} \rangle$ to $G(\Theta_2) = \langle V_2, E_2, \ell_{E_2} \rangle$. It is obvious that $\sim$ is an equivalence relation. Therefore for a given proof structure Θ, we can define the equivalence class $[\Theta]$ such that $\Theta' \in [\Theta]$ iff $\Theta \sim \Theta'$. Then we say $[\Theta]$ is a* **PS-family** *of Θ. We also say Θ belongs to the PS-family $[\Theta]$.*

Remark. We define a PS-family as an equivalence class generated by the relation $\sim$. Of course, we can define a PS-family as an MLL proof structure in which all the occurrences of multiplicative links are of $\frac{A \quad B}{A @ B}$ instead of $\otimes$- and $\parr$-links, where @ is a new symbol. The reader might prefer to this form. But it seems a matter of taste.

We denote a PS-family by $\mathscr{F}$.
Next, given a PS-family $\mathscr{F}$, we introduce a metric $d_{\mathscr{F}}$ on $\mathscr{F}$.

Definition 14 *Let $\mathscr{F}$ be a PS-family. We assume that two MLL proof structures Θ_1 and Θ_2 belong to $\mathscr{F}$. So, by definition we have at least one graph isomorphism $\langle h_V, h_E \rangle$ from $G(\Theta_1)$ to $G(\Theta_2)$. Moreover let $G^{\mathrm{strp}_{\otimes\parr}}(\Theta_1) = \langle V_1, E_1, \ell_{V_1}^{\mathrm{strp}_{\otimes\parr}}, \ell_{E_1} \rangle$ and $G^{\mathrm{strp}_{\otimes\parr}}(\Theta_2) = \langle V_2, E_2, \ell_{V_2}^{\mathrm{strp}_{\otimes\parr}}, \ell_{E_2} \rangle$. Then $d_{\mathscr{F}}(\Theta_1, \Theta_2) \in \mathbb{N}$ is defined as follows:*

$$d_{\mathscr{F}}(\Theta_1, \Theta_2) = \min\{|\{v_1 \in V_1 \mid \ell_{V_2}^{\mathrm{strp}_{\otimes\parr}}(h_V(v_1)) \neq \ell_{V_1}^{\mathrm{strp}_{\otimes\parr}}(v_1)\}| \mid \langle h_V, h_E \rangle : G(\Theta_1) \simeq G(\Theta_2)\}$$

Before proving that $\langle \mathscr{F}, d_{\mathscr{F}} \rangle$ is a metric space, we must define an equality between two MLL proof structures, because the statement concerns the equality on $\mathscr{F}$. In order to define the equality, we use Definition 11 with the parameter $\mathrm{strp}_{\otimes\parr}$.

Definition 15 (Equality on MLL Proof Structures) *Let Θ_1 and Θ_2 be proof structures. Then $\Theta_1 = \Theta_2$ if there is a graph isomorphism $\langle h_V : V_1 \to V_2, h_E : E_1 \to E_2 \rangle$ from $G^{\mathrm{strp}_{\otimes\parr}}(\Theta_1) = \langle V_1, E_1, \ell_{V_1}^{\mathrm{strp}_{\otimes\parr}}, \ell_{E_1} \rangle$ to $G^{\mathrm{strp}_{\otimes\parr}}(\Theta_2) = \langle V_2, E_2, \ell_{V_2}^{\mathrm{strp}_{\otimes\parr}}, \ell_{E_2} \rangle$.*

It is obvious that $=$ is an equivalence relation.

Proposition 1 *The pair* $\langle \mathscr{F}, d_{\mathscr{F}} : \mathscr{F} \to \mathbb{N} \rangle$ *is a metric space.*

We give a justification of the definitions above using Figure 1. Let Θ_1, Θ_2, and Θ_3 be the left proof net, the middle proof net, and the right proof net of Figure 1 respectively. Then $G(\Theta_1) \sim G(\Theta_2)$, since $G(\Theta_1)$ and $G(\Theta_2)$ are graph-isomorphic to the left directed graph of Figure 5. But note that there are two graph isomorphisms $\{\otimes \mapsto \otimes, \parr \mapsto \parr\}$ and $\{\otimes \mapsto \parr, \parr \mapsto \otimes\}$ between $G(\Theta_1)$ and $G(\Theta_2)$. By the former one, we can identify Θ_1 with Θ_2, while in the latter one, there are two differences w.r.t multiplicative nodes. Therefore $d_{\mathbb{F}}(\Theta_1, \Theta_2) = 0$. That's why we need the min operator for the definition of $d_{\mathbb{F}}(\Theta_1, \Theta_2)$. So, Θ_1 and Θ_2 belong to the same PS-family. But $\neg(G(\Theta_1) \sim G(\Theta_3))$ (and also $\neg(G(\Theta_2) \sim G(\Theta_3))$), since $G(\Theta_3)$ is graph-isomorphic to the right directed graph of Figure 5 and the left one of Figure 5 are not graph-isomorphic to the right one. So, Θ_3 does not belong to the same PS-family as Θ_1 and Θ_2.
Note that direction of edges labelled with **ID** are indispensable, because if we eliminated the information, then the two graphs of Figure 5 would be isomorphic. However, direction of edges labelled with **L** or **R** is redundant, because we can always identify the conclusions of the graph without the information by looking for the nodes without an outgoing edge. But we prefer to the conventional definition of directed graphs.
In order to avoid the min operator for the definition of $d_{\mathbb{F}}(\Theta_1, \Theta_2)$, we need to consider only PS-families in which there is the unique graph isomorphism between $G(\Theta_1)$ and $G(\Theta_2)$ for each two members Θ_1 and Θ_2. In order to do that, we restrict PS-families to them with exactly one conclusion, because each multiplicative link in an element in such a PS-family is given an absolute position from the root of the proof structure. We call such a PS-family *closed PS-family*. A closed PS-family is PS-connected in the sense of Definition 17 (Subsection 3.4). For example, two proof structures in Figure 6 belonging to the same closed PS-family has the unique graph isomorphism between them. The restriction is similar to that of closed loops in knot theory (see [Ada94]).
On the other hand, for any MLL proof net without closedness condition, the following proposition holds.

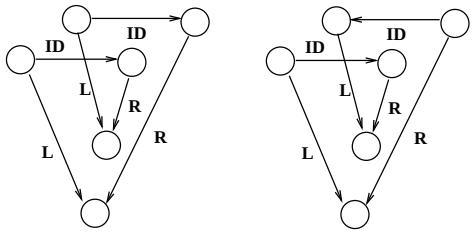

Figure 5: The induced directed graphs from Θ_1 and Θ_2, and that of Θ_3

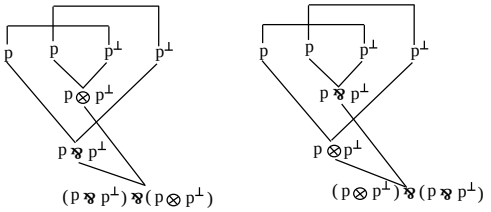

Figure 6: Two elements of a closed PS-family

Proposition 2 *Let* Θ *be an MLL proof net. Then the identity map* $\langle \mathrm{id}_V, \mathrm{id}_E \rangle$ *is the only one graph automorphism on* $G^{\mathrm{strp}_{\otimes\parr}}(\Theta) = \langle V, E, \ell_V^{\mathrm{strp}_{\otimes\parr}}, \ell_E \rangle$.

3.2 Basic Results

Our proposal in this paper starts from the following trivial proposition. We note that this proposition is stated in Subsection 11.3.3 of [Gir06].

Proposition 3 *Let Θ be an MLL proof net.*

1. *Let $L_{\otimes} : \frac{A \quad B}{A \otimes B}$ be a $\otimes$-link in Θ. Let Θ' be the proof structure Θ except that $L_{\otimes}$ is replaced by $L'_{\parr} : \frac{A \quad B}{A \parr B}$. Then Θ' is not an MLL proof net.*
2. *Let $L_{\parr} : \frac{C \quad D}{C \parr D}$ be a $\parr$-link in Θ. Let Θ'' be the proof structure Θ except that $L_{\parr}$ is replaced by $L'_{\otimes} : \frac{C \quad D}{C \otimes D}$. Then Θ' is not an MLL proof net.*

Remark. Proposition 3 does not hold in neither MLL+MIX [Gir87] nor Affine Logic [Bla92]. For example $(p \parr p^{\perp}) \otimes (p \parr p^{\perp})$ is provable in MLL, MLL+MIX, and Affine Logic. The formula $(p \parr p^{\perp}) \parr (p \parr p^{\perp})$ is not provable in MLL, but provable in both MLL+MIX and Affine Logic,

The following corollary is obvious.

Corollary 1 *Let Θ_1 and Θ_2 be MLL proof nets belonging to the same PS-family $\mathscr{F}$. Then $d_{\mathscr{F}}(\Theta_1, \Theta_2) \geq 2$.*

This corollary says that if a PS-family $\mathscr{F}$ has n MLL proof nets, then $\mathscr{F}$ can be used as a **one error-detecting code system** with n different code elements. But since neither MLL+MIX nor Affine Logic has the property, these can not be used as such a system.
The following proposition is basically a slight extension of Corollary 17.1 of Subsection 11.A.2 of [Gir06]. The extension is by a suggestion of an anonymous referee of the previous version of this paper.

Proposition 4 *Let $\Theta = \langle \mathbb{F}_{\Theta}, \mathbb{L}_{\Theta} \rangle$ be an MLL proof net. Let $\mathbb{L}^{\mathrm{ID}}_{\Theta}$, $\mathbb{L}^{\otimes}_{\Theta}$, and $\mathbb{L}^{\parr}_{\Theta}$ be the set of the ID-links, the $\otimes$-links, and the $\parr$-links in $\mathbb{L}$ respectively and con_{Θ} be the set of the conclusions in $\mathbb{F}_{\Theta}$. Then $|\mathrm{con}_{\Theta}| + |\mathbb{L}^{\parr}_{\Theta}| = |\mathbb{L}^{\mathrm{ID}}_{\Theta}| + 1$ and $|\mathbb{L}^{\mathrm{ID}}_{\Theta}| - |\mathbb{L}^{\otimes}_{\Theta}| = 1$.*

Remark. Proposition 4 does not hold in MLL+MIX. A counterexample in MLL+MIX is again $(p \parr p^{\perp}) \parr (p \parr p^{\perp})$.

Corollary 2 *Let $\mathscr{F}$ be a PS-family. Let Θ_1 and Θ_2 be MLL proof nets belonging to $\mathscr{F}$. Then the number of $\otimes$-links (resp. $\parr$-links) occurring in Θ_1 is the same as that of Θ_2.*

Proof. Since Θ_1 and Θ_2 are members of $\mathscr{F}$, $|\mathrm{con}_{\Theta_1}| = |\mathrm{con}_{\Theta_2}|$ and $|\mathbb{L}^{\mathrm{ID}}_{\Theta_1}| = |\mathbb{L}^{\mathrm{ID}}_{\Theta_2}|$. Therefore by Proposition 4, $|\mathbb{L}^{\otimes}_{\Theta_1}| = |\mathbb{L}^{\otimes}_{\Theta_2}|$ and $|\mathbb{L}^{\parr}_{\Theta_1}| = |\mathbb{L}^{\parr}_{\Theta_2}|$. □

Next, we define an important notion in the next subsection.

Definition 16 ($\otimes$-$\parr$-exchange) *Let Θ be a proof structure. Moreover let $L_{\otimes} : \frac{A \quad B}{A \otimes B}$ and $L_{\parr} : \frac{C \quad D}{C \parr D}$ be a $\otimes$-link and a $\parr$-link in Θ respectively. Then $\mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes}, L_{\parr})$ be a proof structure obtained from Θ replacing $L_{\otimes}$ by $L'_{\parr} : \frac{A \quad B}{A \parr B}$ and $L_{\parr}$ by $L'_{\otimes} : \frac{C \quad D}{C \otimes D}$ simultaneously. Then $\mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes}, L_{\parr})$ is called a $\otimes$-$\parr$-exchange of Θ by $L_{\otimes}$ and $L_{\parr}$.*
More generally, when $\langle L_{\otimes_1}, \ldots, L_{\otimes_{\ell_1}} \rangle$ is a list of $\otimes$-links and $\langle L_{\parr_1}, \ldots, L_{\parr_{\ell_2}} \rangle$ a list of $\parr$-links, then $\mathrm{ex}_{\otimes\parr}(\Theta, \langle L_{\otimes_1}, \ldots, L_{\otimes_{\ell_1}} \rangle, \langle L_{\parr_1}, \ldots, L_{\parr_{\ell_2}} \rangle)$ is defined to be a proof structure obtained from Θ by replacing $L_{\otimes_1}, \ldots, L_{\otimes_{\ell_1}}$ by the list of $\parr$-links $L'_{\parr_1}, \ldots, L'_{\parr_{\ell_1}}$ and $L_{\parr_1}, \ldots, L_{\parr_{\ell_2}}$ by the list of $\otimes$-links $L'_{\otimes_1}, \ldots, L'_{\otimes_{\ell_2}}$ simultaneously.

It is obvious that Θ and $\mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes}, L_{\parr})$ belong to the same PS-family. Moreover, $\mathrm{ex}_{\otimes\parr}(\mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes}, L_{\parr}), L'_{\otimes}, L'_{\parr})$ is Θ. Then for each two proof structures Θ_1 and Θ_2, we define a relation $\Theta_1 \Leftrightarrow \Theta_2$ if there are $\otimes$-link $L_{\otimes}$ and $\parr$-link $L_{\parr}$ in Θ_1 such that Θ_2 is $\mathrm{ex}_{\otimes\parr}(\Theta_1, L_{\otimes}, L_{\parr})$. Then $\Leftrightarrow$ is a symmetric relation from the observation above. On the other hand, if Θ is an MLL proof net and $\Theta \Leftrightarrow \Theta'$, then Θ' is not always an MLL proof net. Figure 7 shows such an example. Theorem 2 below describes a necessary and sufficient condition that Θ' is an MLL proof net.
As to general $\otimes$-$\parr$-exchange $\mathrm{ex}_{\otimes\parr}(\Theta, \langle L_{\otimes_1}, \ldots, L_{\otimes_{\ell_1}} \rangle, \langle L_{\parr_1}, \ldots, L_{\parr_{\ell_2}} \rangle)$, note that we do not assume that each element of $\langle L_{\otimes_1}, \ldots, L_{\otimes_{\ell_1}} \rangle$ (resp. $\langle L_{\parr_1}, \ldots, L_{\parr_{\ell_2}} \rangle$) does not appear in Θ like substitution of λ-calculus, because of convenience. In addition, note that Proposition 3 states when Θ is an MLL proof net and $L_{\otimes} : \frac{A \quad B}{A \otimes B}$ (resp. $L_{\parr} : \frac{C \quad D}{C \parr D}$) appears in Θ, then $\mathrm{ex}_{\otimes\parr}(\Theta, \langle L_{\otimes} \rangle, \langle\rangle)$ (resp. $\mathrm{ex}_{\otimes\parr}(\Theta, \langle\rangle, \langle L_{\parr} \rangle)$) is not an MLL proof net (although these two belong to the same PS-family as Θ).
Moreover from Corollary 2, we can easily see that if Θ_1 and Θ_2 are MLL proof nets that belong to the same PS-family, then there is a sequence of proof structures $\Theta'_1, \ldots, \Theta'_k$ ($k \geq 0$) such that $\Theta_1 \Leftrightarrow \Theta'_1 \Leftrightarrow \cdots \Leftrightarrow \Theta'_k \Leftrightarrow \Theta_2$. Theorem 3 below says that we can always find such a sequence $\Theta'_1, \ldots, \Theta'_k$ such that each element $\Theta'_i (1 \leq i \leq k)$ is an **MLL proof net**. This does not seem trivial.

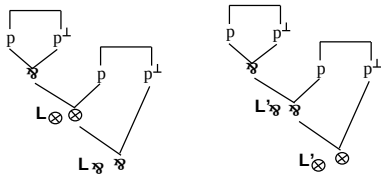

Figure 7: A counterexample

3.3 Main Theorems

In this section, we answer the following question: "in our framework is error-correcting possible?" Our answer is negative. Corollary 3 says that this is impossible even for one error-correcting.
Before that, we state a characterization of the condition $d_{\mathscr{F}}(\Theta_1, \Theta_2) = 2$, where $\mathscr{F}$ is a PS-family and Θ_1 and Θ_2 are MLL proof nets belonging to $\mathscr{F}$. The characterization is used in the proof of Lemma 1, which is needed to prove Theorem 3.

Theorem 2 *Let Θ be an MLL proof net. Moreover let $L_{1\otimes} : \frac{A \quad B}{A \otimes B}$ and $L_{2\parr} : \frac{C \quad D}{C \parr D}$ be a $\otimes$-link and a $\parr$-link in Θ respectively. Then $\mathrm{ex}_{\otimes\parr}(\Theta, L_{1\otimes}, L_{\parr 2})$ is an MLL proof net iff one of the followings holds in Θ:*

(1) C is a conclusion of $e_\Theta(A)$ and D is a conclusion of $e_\Theta(B)$;

(2) D is a conclusion of $e_\Theta(A)$ and C is a conclusion of $e_\Theta(B)$.

Theorem 3 *Let Θ and Θ' be two MLL proof nets belonging to the same PS-family $\mathscr{F}$. Then there is $n \in \mathbb{N}$ and a sequence of MLL proof nets $\Theta_1, \ldots, \Theta_n$ such that*

$$\Theta \Leftrightarrow \Theta_1 \Leftrightarrow \cdots \Leftrightarrow \Theta_n \Leftrightarrow \Theta'.$$

Proof. We assume that Θ and Θ' are MLL proof nets, but we do not have such a sequence of MLL proof nets for any $n \in \mathbb{N}$. Moreover we can choose two MLL proof nets Θ and Θ' in $\mathscr{F}$ such that there is no MLL proof net Θ'' such that $d(\Theta, \Theta'') < d(\Theta, \Theta')$ and $d(\Theta'', \Theta') < d(\Theta, \Theta')$ since it is sufficient to prove the theorem. Then from Corollary 2, we can easily deduce that $d_{\mathscr{F}}(\Theta, \Theta')$ is even, i.e., $d_{\mathscr{F}}(\Theta, \Theta') = 2m$. In addition there are m $\otimes$-links $L_{\otimes 1} : \frac{A_1 \quad B_1}{A_1 \otimes B_1}, \ldots, L_{\otimes m} : \frac{A_m \quad B_m}{A_m \otimes B_m}$ in Θ and m $\parr$-links $L_{\parr 1} : \frac{C_1 \quad D_1}{C_1 \parr D_1}, \ldots, L_{\parr m} : \frac{C_m \quad D_m}{C_m \parr D_m}$ in Θ such that Θ' is $\mathrm{ex}_{\otimes\parr}(\Theta, \langle L_{\otimes 1}, \ldots, L_{\otimes m}\rangle, \langle L_{\parr 1}, \ldots, L_{\parr m}\rangle)$. Let $\Theta_{i,j}$ $(1 \leq i, j \leq m)$ be $\mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes i}, L_{\parr j})$. Then our assumption means that $\Theta_{i,j}$ is not an MLL proof net for any i, j $(1 \leq i, j \leq m)$ (The assumption is used in the proof of Lemma 1). Then we derive a contradiction from these settings by induction on lexicographic order $\langle m, |\mathbb{L}_\Theta|\rangle$, where $|\mathbb{L}_\Theta|$ is the number of link occurrences in Θ.

(1) The case where $m = 0$ and $m = 1$:
It is obvious.

(2) The case were $m > 1$:

(a) The case where Θ consists of exactly one ID-link:
In this case there is neither a $\otimes$-link nor a $\parr$-link in Θ. This is a contradiction to $m > 1$.

(b) The case where Θ includes a $\parr$-formula $C \parr D$ as a conclusion:
We choose such a $\parr$-link $L_\parr : \frac{C \quad D}{C \otimes D}$.

(i) The case where $C \parr D$ is not $C_j \parr D_j$ for any j $(1 \leq j \leq m)$:
Let Θ_0 be Θ except that $L_\parr$ is eliminated. Then we can apply inductive hypothesis to Θ_0 and a subproof net of Θ', $\mathrm{ex}_{\otimes\parr}(\Theta_0, \langle L_{\otimes 1}, \ldots, L_{\otimes m}\rangle, \langle L_{\parr 1}, \ldots, L_{\parr m}\rangle)$. We derive a contradiction.

(ii) The case where $C \parr D$ is $C_{j_0} \parr D_{j_0}$ for some j_0 $(1 \leq j_0 \leq m)$:
In this case, by Lemma 1, Θ' is not an MLL proof net. This is a contradiction.

(c) The case where the conclusions of Θ do not have any $\parr$-formula:
In this case, by Splitting lemma (see, for example, [Gir87, Mat10]), we have a $\otimes$-conclusion $A \otimes B$ and its $\otimes$-link $L_{A\otimes B}$ in Θ such that Θ is decomposed into $e^{PN}_{\Theta}(A)$, $e^{PN}_{\Theta}(B)$, and $\otimes$-link $L_{A\otimes B}$

(i) The case where $A \otimes B$ is not $A_i \otimes B_i$ for any $i\,(1 \leq i \leq m)$:
In this case if the number of $\parr$-links from $L_{\parr 1}, \ldots, L_{\parr m}$ in $e_{\Theta}(A)$ is the same as the number of $\otimes$-links from $L_{\otimes 1}, \ldots, L_{\otimes m}$ in $e_{\Theta}(A)$, then we can apply inductive hypothesis to $e_{\Theta}(A)$ and a subproof net of Θ', $\mathrm{ex}_{\otimes\parr}(e_{\Theta}(A), \langle L_{\otimes 1}, \ldots, L_{\otimes m}\rangle, \langle L_{\parr 1}, \ldots, L_{\parr m}\rangle)$. Then we derive a contradiction. Otherwise, let Θ'_A be
$\mathrm{ex}_{\otimes\parr}(e_{\Theta}(A), \langle L_{\otimes 1}, \ldots, L_{\otimes m}\rangle, \langle L_{\parr 1}, \ldots, L_{\parr m}\rangle)$. Then by Corollary 2, Θ'_A is not an MLL proof net. Therefore Θ' is not an MLL proof net. This is a contradiction.

(ii) The case where $A \otimes B$ is $A_i \otimes B_i$ for some $i\,(1 \leq i \leq m)$:
Then we can find a DR-switching S' for Θ' such that $S'(\Theta')$ is disconnected since The $\otimes$-link $L_{\otimes i}$ is replaced by a $\parr$-link $L_{\otimes i}$. Therefore Θ' is not an MLL proof net. This is a contradiction.

Therefore, for some $i_0, j_0\,(1 \leq i_0, j_0 \leq m)$, $\Theta_{i_0,j_0}\,(= \mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes i_0}, L_{\parr j_0}))$ is an MLL proof net. We have done. □

Lemma 1 *The assumptions are inherited from the case (2-b-ii) of the proof above of Theorem 3. Then,* $\Theta' = \mathrm{ex}_{\otimes\parr}(\Theta, \langle L_{\otimes 1}, \ldots, L_{\otimes m}\rangle, \langle L_{\parr 1}, \ldots, L_{\parr j_0}, \ldots, L_{\parr m}\rangle)$ *is not an MLL proof net.*

When a PS-family $\mathscr{F}$ has at least two MLL proof nets, we define the distance $d(\mathscr{F})$ of $\mathscr{F}$ itself in the usual manner:

$$d(\mathscr{F}) = \min\{d_{\mathscr{F}}(\Theta_1, \Theta_2) \,|\, \Theta_1, \Theta_2 \in \mathscr{F} \wedge (\Theta_1 \text{ and } \Theta_2 \text{ are MLL proof nets}) \wedge \Theta_1 \neq \Theta_2\}$$

Then from Theorem 3 the following corollary is easily derived.

Corollary 3 *For any PS-family $\mathscr{F}$, if the number of the MLL proof nets in $\mathscr{F}$ is equal to or greater than 2, then $d(\mathscr{F}) = 2$.*

Corollary 3 means that one error-correcting is impossible for any PS-family of MLL.

Example 1 *Our proof of Theorem 3 states that when Θ and Θ' are MLL proof nets belonging to the same PS-family $\mathscr{F}$ and $d_{\mathscr{F}}(\Theta, \Theta') \geq 2$, we can always find an MLL proof net Θ'' such that $d_{\mathscr{F}}(\Theta, \Theta'') = 2$ and $d_{\mathscr{F}}(\Theta'', \Theta') = d_{\mathscr{F}}(\Theta, \Theta') - 2$. We show an example in the following.*
For two MLL proof nets Θ of the left side of Figure 8 and Θ' of the right side of Figure 8 belonging to the same PS-family, $d(\Theta, \Theta') = 4$ holds. Then when we let the left side of Figure 9 be Θ_1, then $\Theta_1 = \mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes 1}, L_{\parr 2})$ (and $\Theta = \mathrm{ex}_{\otimes\parr}(\Theta_1, L'_{\otimes 2}, L'_{\parr 1})$). Moreover we find $d(\Theta, \Theta_1) = 2$ and $d(\Theta_1, \Theta') = 2$. But such a Θ_1 is not unique. In fact when we let Θ_2 be the right side of Figure 9, then $\Theta_2 = \mathrm{ex}_{\otimes\parr}(\Theta, L_{\otimes 2}, L_{\parr 2})$ (and $\Theta = \mathrm{ex}_{\otimes\parr}(\Theta_2, L'_{\otimes 2}, L'_{\parr 2})$). By the way, the PS-family has nine MLL proof nets.

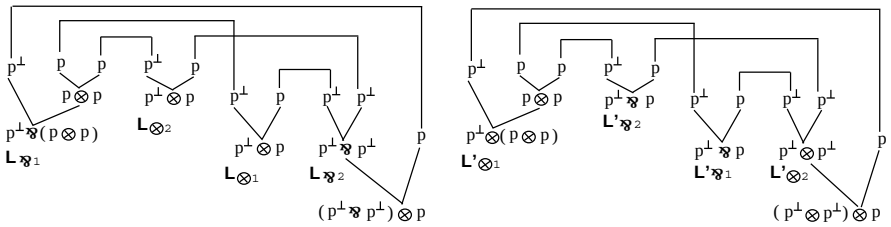

Figure 8: MLL proof nets Θ and Θ'

3.4 Other Topics

In this section we discuss ongoing research directions in our framework.

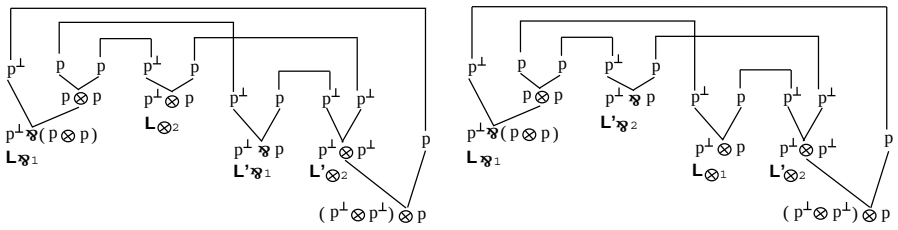

Figure 9: MLL proof nets Θ_1 and Θ_2

3.4.1 The Number of MLL Proof Nets in a PS-family

It is interesting to consider how many MLL proof nets a given PS-family has. We have a characterization of the PS-families without any MLL proof nets as an elementary result.
Firstly we note that the number of the multiplicative links in an element of a given PS family $\mathscr{F}$ is always the same.

Definition 17 (PS-connected) *Let $\mathscr{F}$ be a PS-family. Then $\mathscr{F}$ has the element $\Theta_{\otimes}$ that has only $\otimes$-links as its multiplicative links (if any). Then there is exactly one DR-switching S for $\Theta_{\otimes}$ that is empty set. $\mathscr{F}$ is PS-connected if the unique DR-graph $S(\Theta_{\otimes})$ is connected.*

Proposition 5 *Let $\mathscr{F}$ be a PS-family. Then $\mathscr{F}$ does not have any MLL proof nets iff $\mathscr{F}$ is not PS-connected.*

But it is not so easy to give a similar characterization of PS-families with exactly m MLL proof nets for a given $m\,(\geq 1)$. At this moment we just obtain the following elementary result.

Proposition 6 *For any positive integer m, there are denumerable PS-families with exactly m MLL proof nets.*

Proof. If $m = 1$, then it is enough to see the left side of Figure 10 in order to confirm that the statement is correct. Similarly if $m > 1$, it is enough to see the right side of Figure 10 for the same purpose. □

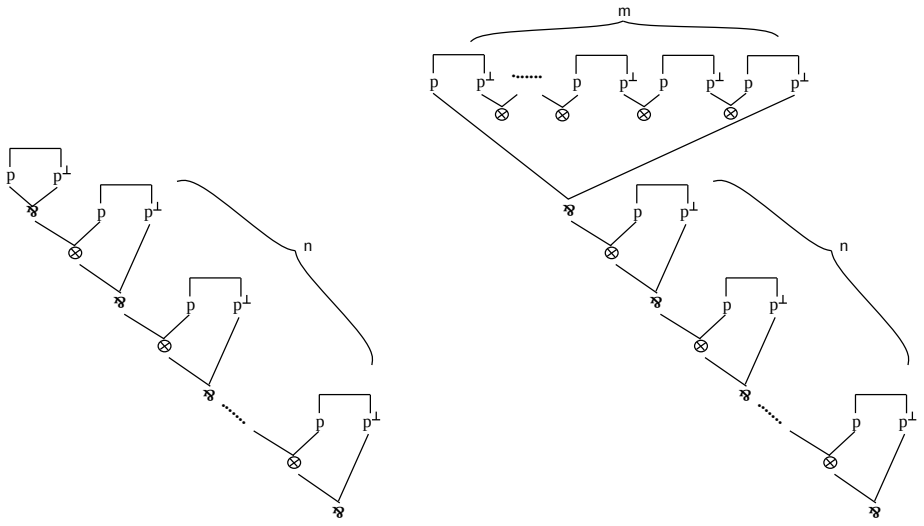

Figure 10: Witnesses for Proposition 6

But it seems difficult to obtain a characterization of the PS-families even with exactly one MLL proof net. The reason is as follows:

1. There are primitive patterns of such PS-families.

2. Moreover by combining such primitive patterns appropriately, we can get compound PS-families with exactly one MLL proof net.

In order to get such a characterization, it seems that an appropriate language that describes (denumerable) sets of PS-families is needed like the regular language for describing sets of words. But since the purpose of this paper is to introduce the new notion of PS-families and metric spaces associated with them, the question is left open as an interesting one.

4 Concluding Remarks

In this paper, we introduced the notion of PS-families over MLL proof structures and metric spaces with associated with them. Moreover we proved that in the case where A PS-family has more than two MLL proof nets, the distance of the PS-family is 2.

Acknowledgements. The author thanks the participants of the 205th Computer Language Colloquium at the Senri office of the Research Center for Semantics and Verification, which is a part of AIST. He also thanks Lorenzo Tortora de Falco for helpful comments.

References

[Ada94] Colin Adams. The Knot Book. W.H. Freeman & Co, 1994.

[Abr07] Samson Abramsky. Temperley-Lieb algebra: from knot theory to logic and computation via quantum mechanics. In *Mathematics of Quantum Computing and Technology*, G.Chen, L.Kauffman and S.Lomonaco, eds, Pages 515-558, Taylor and Francis, 2007.

[Bay98] John Baylis. Error-Correcting Codes: A Mathematical Introduction, Chapman & Hall, 1998.

[BW95] G. Bellin and J. van de Wiele. Subnets of Proof-nets in MLL$^-$. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, Advances in Linear Logic, pages 249-270. Cambridge University Press, 1995.

[Bla92] Andreas Blass. A game semantics for linear logic. *Annals of Pure and Applied Logic*, 56:183-220, 1992.

[DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28:181-203, 1989.

[DR95] Vincent Danos and Laurent Regnier. Proof-nets and the Hilbert space. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, Advances in Linear Logic, pages 307-328. Cambridge University Press, 1995.

[Gir87] Jean-Yves Girard. Linear Logic. *Theoretical Computer Science*, 50:1-102, 1987.

[Gir96] Jean-Yves Girard. Proof-nets: the parallel syntax for proof-theory. In A. Ursini and P. Agliano, editors, *Logic and Algebra, New York, Marcel Dekker*, 1996.

[Gir06] Jean-Yves Girard. Le Point Aveugle: Tome I, vers la perfection. Hermann, 2006.

[Has05] Masahito Hasegawa. Classical linear logic of implications. *Mathematical Structures in Computer Science* 15(2):323-342, 2005.

[Mat07] Satoshi Matsuoka. Weak Typed Böhm Theorem on IMLL. *Annals of Pure and Applied Logic*, 145:37-90, 2007.

[Mat10] Satoshi Matsuoka. A Coding Theoretical Study on MLL Proof Nets. Draft, ver. 23, Available from `http://arxiv.org/abs/cs/0703018`, 2010.

[MS93] F.J. MacWilliams and N.J.A. Sloane. The Theory of Error-correcting Codes. North-Holland, 1993.

一般 Hamming 符号から作られる 不変式の Riemann 予想について

知念 宏司 (近畿大学 理工学部)

2009.12.2
第 8 回「代数学と計算」研究集会 (AC2009)
(首都大学東京)

概 要

線型符号の zeta 関数は 1999 年, Iwan Duusma により, 重み多項式の一種の母関数として定義された. 自己双対線型符号の zeta 関数は, 代数曲線の合同 zeta 関数の場合と同じ形の関数等式をもち, Riemann 予想の類似も定式化される. 実は, 符号の重み多項式とは限らない, より広い範囲の不変式に対しても, zeta 関数は定義される. 本稿では, まず任意の線型符号の重み多項式を利用して不変式を構成する方法を述べる. そして, この考え方を用いて一般 Hamming 符号の重み多項式から不変式を構成する. するとその zeta 関数はほとんどの場合, Riemann 予想を満たすことが証明される.

1 導 入

まず線型符号の zeta 関数について簡単に説明しよう. これは 1999 年, Iwan Duursma によって定義された ([8]). C を有限体 $\mathbf{F}_q$ ($q = p^r$, p: 素数, $r \geq 1$) 上の $[n, k, d]$-線型符号とし,

$$W_C(x, y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \qquad (A_d \neq 0)$$

をその重み多項式とする. このとき, 符号 C の zeta 関数は次のように定義される:

定 義 1.1 C に対して, 次数 $n-d$ 以下のある多項式 $P(T) \in \mathbf{Q}[T]$ がただ 1 つ存在して,

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_C(x,y) - x^n}{q-1} T^{n-d} + \cdots$$

が成立する. $P(T)$ を C の **zeta 多項式**, $Z(T) := P(T)/\{(1-T)(1-qT)\}$ を C の **zeta 関数**と呼ぶ.

多項式 $P(T)$ の存在と一意性は Duursma ([8]) で証明されたが, あまりわかりやすい形で書かれていない. 初等的証明が筆者らの総合報告 [3, pp.92-93], [12, p.44], [4, pp.32-33] にある. また [6, Appendix A] も参照.

この定義にいう「符号の zeta 関数」に関して詳しいことは Duursma の論文 [9], [10] あるいは [3], [12] などをご参照いただきたいが, 彼の一連の結果のうち筆者にとって特に興味深いのは自己双対符号の zeta 多項式に対する関数等式

$$P(T) = P\Big(\frac{1}{qT}\Big) q^g T^{2g} \tag{1.1}$$

である ($g = n/2+1-d$). ここで, C が自己双対とは, $\mathbf{F}_q{}^n$ の通常の内積に関して, $C^\perp = C$ となる (直交補空間が自分自身と一致する) ことである. 関数等式は, あとで述べるように, 重み多項式 $W_C(x, y)$ が MacWilliams 変換で不変であることの帰結である. またこれは代数曲線の zeta 多項式 (いわゆる合同 zeta 関数の分子) がもつ関数等式と全く同じ形であり, したがって「符号の Riemann 予想」を次のように定式化できる:

定 義 1.2 C を自己双対符号, その zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, C は Riemann 予想を満たすという.

符号の Riemann 予想はすべての自己双対符号によって満たされるわけではなく, 実在の自己双対符号で Riemann 予想を満たすもの, 満たさないもの, 両方の実例が存在する. 符号が Riemann 予想を満たすための必要十分条件を求めることはまだ未解決であるが, Duursma は

問 題 1.3 「Extremal な自己双対符号は Riemann 予想を満たす」は正しいか.

という問題を提出している ([10]). ここで, extremal な自己双対符号とは, $\mathbf{F}_2$, $\mathbf{F}_3$ または $\mathbf{F}_4$ 上の自己双対符号で, Mallows-Sloane 限界式 ([11, §1.1]) を等号で満たすものである. これは結局, 与えられた符号長において, 最も大きな最小距離をもつ, ということであるから, extremal という性質は応用上からもよい性質である (最小距離が大きいほど訂正能力は高い). このように, 符号の Riemann 予想は, 代数曲線の場合との単なる形式的類似ではなく, よい符号の一種の特徴づけであると期待されているのである. Duursma は, いわゆる Type IV 自己双対符号で符号長が 6 で割り切れる場合にこれを肯定的に解決している ([11]). さらに最近, 符号長が $6n-2$ の形の場合が奥田 [15] により肯定的に解決された. なお, extremal 自己双対符号で実在するのは有限個であることはすでに古くから知られているが (例えば [14, pp.624-628]), 重み多項式は無限系列として存在する. これらの結果は重み多項式の無限列に対する結果であることにも注意を要する (以下に述べるように, このことは本稿の内容にも関連する).

さて, 定義 1.1 を見てみると, $P(T)$ の存在と一意性の証明においては, $W_C(x, y)$ が実在する符号の重み多項式であることよりも, それが **x, y の斉次 n 次式であることがより本質的**であることがわかる. この事実はすでに MDS 符号 (最大距離分離符号) の zeta 関数の考察において Duursma 自身によっても暗に用いられているが, 筆者はより積極的にこの点に注目し, 必ずしも符号と関連をもたない複素数係数の斉次多項式

$$W(x, y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \quad (A_d \neq 0) \tag{1.2}$$

に対してその zeta 多項式 $P(T)$ を, 全く同様に定義できることを指摘した ([4, p.40]. また [6, Appendix A] も参照).

さらに, 実在する $\mathbf{F}_q$ 上の符号の場合, $P(T)$ の関数等式はどこから来るかというと, $W_C(x,y)$ が MacWilliams 変換

$$\sigma_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \tag{1.3}$$

で不変であるという事実の帰結である. ここで, 1 次変換 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の多項式 $f(x,y)$ への作用は $f^\sigma(x,y) = f(ax+by, cx+dy)$ とする. ところで, σ_q で不変な $W(x,y)$ 全体 (不変式環) の構造は知られていて,

$$\mathbf{C}[x,y]^{\langle\sigma_q\rangle} := \{W(x,y) \in \mathbf{C}[x,y]\ ;\ W(x,y)^{\sigma_q} = W(x,y)\} = \mathbf{C}[x+(\sqrt{q}-1)y, y(x-y)]$$

である (MacWilliams-Sloane [14, p.605, Theorem 5]). そこで, $P(T)$ が関数等式 (1.1) を満たすような $W(x,y)$ を考えるには, $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ の元を考えればよい. こうして「不変式の Riemann 予想」を考えることができる:

定 義 1.4 $W(x,y) \in \mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ は (1.2) の形の斉次多項式とし, $W(x,y)$ の zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, $W(x,y)$ は Riemann 予想を満たすという.

注 意. (1) $W(x,y)$ が σ_q 不変でなくても (したがって対応する $P(T)$ は関数等式を満たさない) Riemann 予想を満たす, という例もあるにはある. $\mathbf{F}_2$ 上の $[7,4,3]$ Hamming 符号の重み多項式がその一例である.

(2) 少し違った形の関数等式 $P(T) = -P(\frac{1}{qT})q^gT^{2g}$ (マイナスがつく) を満たす不変式もあり (もちろん $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ とは別の不変式環の元), やはり Riemann 予想を満たすものの実例が見つかっている ([5]).

不変式環 $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ において, 定義 1.4 の意味で Riemann 予想を満たす不変式を見つけることは, 非常に興味深い問題と思われる. しかし, 闇雲に不変式を構成しても Riemann 予想を理論的に調べることはやりづらい. 何か系統的に不変式を構成する方法が必要である. そのため本稿では, 実在の符号の重み多項式を利用することを考える. これは, $W_C(x,y)$ と $W_{C^\perp}(x,y)$ を適当に組み合わせるもので, この方法を利用すると任意の線型符号の重み多項式から MacWilliams 不変な多項式 $\tilde{W}_C(x,y)$ を得ることができる (命題 2.1).

さらに本稿では C が一般 Hamming 符号 $\mathrm{Ham}(r,q)$ の場合を考える. これは $\mathbf{F}_q$ 上定義される $[n := (q^r-1)/(q-1), n-r, 3]$ 符号である ($r \geq 2$, 定義 3.1). すると, C から作った不変式はほとんどの場合, Riemann 予想を満たすことが示される. 次が主結果である:

定 理 1.5 $r \geq 3$, $q \geq 4$ のとき, $C = \mathrm{Ham}(r,q)$ から作った不変式 $\tilde{W}_C(x,y)$ は Riemann 予想を満たす.

注 意. (1) $r = 2$ の場合, $\mathrm{Ham}(2, q)$ は MDS 符号となり, この場合は本稿と別の方法で Riemann 予想を証明することができる (下の注意参照). したがって, 証明できずに残っているのは $r \geq 3$, $q = 2, 3$ の場合ということになる. ただ, 数値実験によると, これらの場合にも Riemann 予想は成り立つのではないかと予想される.

(2) 他に, C が MDS 符号の場合, (自己双対でない) Golay 符号の場合にも, 不変式 $\tilde{W}_C(x, y)$ は Riemann 予想を満たす ([6]).

なお, 本稿の内容は [6] の一部である.

2 任意の線型符号からの不変式の構成

p を素数, $q = p^r$ $(r \geq 1)$ とし, C を有限体 $\mathbf{F}_q$ 上の $[n, k, d]$ 符号とする. また

$$W_C(x, y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \qquad (A_d \neq 0)$$

をその重み多項式とする. この $W_C(x, y)$ から MacWilliams 不変な多項式 $\tilde{W}_C(x, y)$ を構成し, その zeta 多項式 $\tilde{P}_C(T)$ を明示するのが本節の目標である. 重み多項式 $W_C(x, y)$ とその双対符号の重み多項式 $W_{C^\perp}(x, y)$ を組み合わせて

$$\tilde{W}_C(x, y) := \frac{1}{1 + q^{k-n/2}} \{W_C(x, y) + q^{k-n/2} W_{C^\perp}(x, y)\} \tag{2.1}$$

とする. このとき, 次が成り立つ:

命 題 2.1 多項式 $\tilde{W}_C(x, y)$ は MacWilliams 変換で不変である. つまり $\tilde{W}_C(x, y) \in \mathbf{C}[x, y]^{G_q}$.

証 明. これは MacWilliams の等式

$$W_C^{\sigma_q}(x, y) = q^{k-n/2} W_{C^\perp}(x, y) \quad \text{または} \quad W_{C^\perp}^{\sigma_q}(x, y) = q^{n/2-k} W_C(x, y)$$

(see [14, p.146, Theorem 13]) から容易に得られる. ∎

つまり, $W_C(x, y)$ と $W_{C^\perp}(x, y)$ が, 言わば互いに移り合うことで, 全体として不変に保たれるように係数を調整したものが $\tilde{W}_C(x, y)$ である. $\tilde{W}_C(x, y)$ の zeta 多項式 $\tilde{P}_C(T)$ は, もとの符号 C の zeta 多項式 $P_C(T)$ によって, 次のように表される:

定 理 2.2 $W_C(x, y)$ の zeta 多項式を $P_C(T)$ とすると, $\tilde{W}_C(x, y)$ の zeta 多項式 $\tilde{P}_C(T)$ は

$$\tilde{P}_C(T) = \frac{T^{\max(0, d-d^\perp)}}{1 + q^{k-n/2}} \left\{ P_C(T) + q^{n/2+1-d} P_C\left(\frac{1}{qT}\right) T^{n+2-2d} \right\} \tag{2.2}$$

で与えられる ($d^\perp$ は $C^\perp$ の最小距離). さらに $\tilde{g} := n/2 - 1 - \min(d, d^\perp)$ とおくと, $\deg \tilde{P}_C = 2\tilde{g}$ であり, 関数等式

$$\tilde{P}_C(T) = \tilde{P}_C\left(\frac{1}{qT}\right) q^{\tilde{g}} T^{2\tilde{g}} \tag{2.3}$$

が成立する.

証 明. 定義から

$$\frac{P_C(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_C(x,y)-x^n}{q-1}T^{n-d} + \cdots. \tag{2.4}$$

また, $C^\perp$ の zeta 多項式を $P_{C^\perp}(T)$ とすると,

$$\frac{P_{C^\perp}(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_{C^\perp}(x,y)-x^n}{q-1}T^{n-d^\perp} + \cdots. \tag{2.5}$$

いま, $d \le d^\perp$ の場合を考える. (2.5) 式を $q^{k-n/2}T^{d^\perp-d}$ 倍したものと (2.4) 式を加え, その結果を $1+q^{k-n/2}$ で割ったものは

$$\frac{\{P_C(T)+q^{k-n/2}P_{C^\perp}(T)T^{d^\perp-d}\}/(1+q^{k-n/2})}{(1-T)(1-qT)}(y(1-T)+xT)^n$$

$$= \cdots + \frac{\tilde{W}_C(x,y)-x^n}{q-1}T^{n-d} + \cdots$$

である. したがって, zeta 多項式の存在と一意性により, $\tilde{W}_C(x,y)$ の zeta 多項式は

$$\tilde{P}_C(T) = \frac{1}{1+q^{k-n/2}}\left\{P_C(T)+q^{k-n/2}P_{C^\perp}(T)T^{d^\perp-d}\right\} \tag{2.6}$$

でなければならない. ここで, Duursma の理論によると

$$P_{C^\perp}(T) = P_C\left(\frac{1}{qT}\right)q^gT^{g+g^\perp}$$

(ただし $g = n+1-k-d$, $g^\perp = k+1-d^\perp$, [9, p.59]) であるから, これを代入して (2.2) 式を得る. $d \ge d^\perp$ の場合も同様である. また, $\tilde{P}_C$ の次数, 関数等式は Duursma の場合と同様にして得られる. ∎

注 意. もし $C^\perp = C$ が成り立つならば $\tilde{P}_C(T) = P_C(T)$ となり, Duursma の定義と一致する. したがって, $\tilde{P}_C(T)$ は自己双対でない符号の場合も zeta 多項式が関数等式をもつように $P_C(T)$ の定義を拡張したものになっている.

3 一般 Hamming 符号

まず [16, p.22] にしたがって一般 Hamming 符号 $\mathrm{Ham}(r,q)$ を定義すると次のようになる:

定 義 3.1 $r \ge 2$ とする. 行列 H を, $\mathbf{F}_q{}^r$ の, 定数倍 ($\neq 0$) で移り合わない $n := (q^r-1)/(q-1)$ 個の非零列ベクトルを並べて得られる $r \times n$ 行列とする. これをパリティ検査行列にもつ線型符号

$$\mathrm{Ham}(r,q) := \{\boldsymbol{x} \in \mathbf{F}_q{}^n \mid H\boldsymbol{x}^{\mathsf{T}} = \mathbf{0}\}$$

を一般 Hamming 符号という.

例えば $r=3$, $q=2$ ならば,

$$H=\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}$$

とすればよく, これはよく知られている $[7,4,3]$ Hamming 符号を与える. $q\geq 3$ のときは, 例えば $[2,2,2]^{\mathsf{T}}$ というベクトルは $[2,2,2]^{\mathsf{T}}=2[1,1,1]^{\mathsf{T}}$ と, 他のベクトルの定数倍 $(\neq 0)$ で表されるため, これらの一方だけを並べて他は並べない. そのため符号長が $n=(q^r-1)/(q-1)$ という形となる. また, $r=2$ ならば MDS 符号となるため, $r\geq 3$ の場合が本質的である. そこで, 以下 $r\geq 3$ とする.

われわれに必要なのは重み多項式であるが, $\mathrm{Ham}(r,q)$ よりも双対 $\mathrm{Ham}(r,q)^{\perp}$ の方が簡単で扱いやすい:

命 題 3.2 $\mathrm{Ham}(r,q)^{\perp}$ の重み多項式は

$$\begin{aligned}W_{\mathrm{Ham}(r,q)^{\perp}}(x,y) &= x^n+(q-1)nx^{\frac{n-1}{q}}y^{\frac{(q-1)n+1}{q}} \\ &= x^n+(q^r-1)x^{n-q^{r-1}}y^{q^{r-1}}\end{aligned} \tag{3.1}$$

で与えられる.

証 明. Brouwer [2, p.316]. ∎

こうした事情から, $C=\mathrm{Ham}(r,q)^{\perp}$ ($\mathrm{Ham}(r,q)$ ではなく) として, 前節の結果を利用する. まず $P_C(T)$ を求めておく必要があるが, それには「正規化重み多項式」を用いる:

定 義 3.3 重み多項式 $W_C(x,y)$ に対し, 正規化重み多項式 $a_C(t)$ を

$$a_C(t)=\frac{1}{q-1}\sum_{i=d}^{n}\left\{A_i \Big/ \binom{n}{i}\right\}t^{i-d}$$

により定義する.

次の定理が $a_C(t)$ と $P_C(T)$ を関連付ける:

定 理 3.4 (Duursma) $a_C(t)$ と $P_C(T)$ の間には次の関係がある:

$$\frac{P(T)}{(1-T)(1-qT)}(1-T)^{d+1}\equiv a_C\left(\frac{T}{1-T}\right)\pmod{T^{n-d+1}}.$$

証 明. [9, Theorem 2]. ∎

つまり, $a_C(T/(1-T))(1-T)(1-qT)/(1-T)^{d+1}$ をべき級数展開して, その T^{n-d} までの項を取れば, それで $P_C(T)$ が求まるわけだ. われわれの場合は次が成り立つ:

補 題 3.5 $C = \mathrm{Ham}(r,q)^{\perp}$ の正規化重み多項式を $a_{r,q}(t)$ とすると

$$a_{r,q}(t) = n \Big/ \binom{n}{q^{r-1}}.$$

つまり $a_{r,q}(t)$ は定数となってしまう. 定数ほど簡単な多項式はなかろう, というわけだ. 証明は (3.1) 式から明らかである. これを用いると, まず $C = \mathrm{Ham}(r,q)^{\perp}$ に対する $P_C(T)$ が求まる:

命 題 3.6 $r \geq 3$, $q \geq 2$ に対して, $P_C(T) = P_{\mathrm{Ham}(r,q)^{\perp}}(T)$ は

$$P_C(T) = N_{r,q}\left[1 + \sum_{j=1}^{n-d-1}\left\{\binom{j+d-1}{d-1} - q\binom{j+d-2}{d-1}\right\}T^j\right] \tag{3.2}$$

で与えられる. ただし $N_{r,q} = n/\binom{n}{q^{r-1}}$.

証 明. 上で述べたことから

$$P_C(T) \equiv N_{r,q}\frac{1-qT}{(1-T)^d} \pmod{T^{n-d+1}} \tag{3.3}$$

となる. あとは $\deg P_C = n+2-d-3 = n-d-1$ に注意して, べき級数展開

$$\frac{1-qT}{(1-T)^d} = 1 + \sum_{j=1}^{\infty}\left\{\binom{j+d-1}{d-1} - q\binom{j+d-2}{d-1}\right\}T^j. \tag{3.4}$$

を用いればよい. ∎

これで, $\mathrm{Ham}(r,q)$ の重み多項式から命題 2.1 の方法で作った不変式 $\tilde{W}_{\mathrm{Ham}(r,q)}(x,y)$ の zeta 多項式 $\tilde{P}_{r,q}(T) := \tilde{P}_{\mathrm{Ham}(r,q)}(T)$ を求める準備が整った:

定 理 3.7 $r \geq 3$, $q \geq 2$ とし, $\tilde{P}_{r,q}(T) := \tilde{P}_{\mathrm{Ham}(r,q)}(T)$ とすれば,

$$\tilde{P}_{r,q}(T) = \frac{N_{r,q}}{1+q^{r-n/2}}(F_1(T) - qF_2(T)),$$

ただし

$$\begin{aligned} F_1(T) &= \sum_{i=0}^{n-d-1}\binom{n-i-2}{d-1}q^{i+2-n/2}T^i + \sum_{i=d-3}^{n-4}\binom{i+2}{d-1}T^i, \\ F_2(T) &= \sum_{i=0}^{n-d-2}\binom{n-i-3}{d-1}q^{i+2-n/2}T^i + \sum_{i=d-2}^{n-4}\binom{i+1}{d-1}T^i. \end{aligned}$$

これが本節の目標となる定理である. 証明は単純な式変形であるが, かなり複雑なので省略する (詳しくは [6, Theorem 17] を参照).

主結果である $\tilde{P}_{r,q}(T)$ の Riemann 予想とは, $\tilde{P}_{r,q}(T)$ の根がすべて $|T| = 1/\sqrt{q}$ という円周上にある, という主張である. それは $T \mapsto T/\sqrt{q}$ という一種の「正規化」を施して「$\tilde{P}_{r,q}(T/\sqrt{q})$ の根がすべて単位円周上にある」と言い換えても同じである. 以下, これを示すことを目標とする. 証明には関数論を用いる. 節をあらためて見ていこう.

4 $\tilde{P}_{r,q}(T)$ の Riemann 予想

実数係数の多項式 $f(T)=\sum_{i=0}^{n}a_iT^i$ が任意の i $(0\le i\le n)$ に対して $a_i=a_{n-i}$ を満たすとき, $f(T)$ を自己相反多項式 (self-reciprocal polynomial) という. つまり, 係数を前から読んでも逆から読んでも同じになっているような多項式である. われわれの場合, 正規化した $\tilde{P}_{r,q}(T/\sqrt{q})$ が実は自己相反となる.

ここでの目標は次の定理である:

定 理 4.1 多項式 $f(T)=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m$ $(m>2k)$ が $a_0>a_1>\cdots>a_k>0$ を満たすなら, $f(T)$ の根はすべて単位円周上にある.

これは, 次の古典的結果の自己相反多項式への拡張とも言えるもので, 主張を見比べてみるとなかなかおもしろい:

定 理 4.2 (Eneström - 掛谷) 多項式 $f(T)=a_0+a_1T+\cdots+a_kT^k$ が $a_0>a_1>\cdots>a_k>0$ を満たすなら, $f(T)$ の根はすべて単位円周の外側 $(|T|>1)$ にある.

証 明. 楠 [13, p.14, 練習問題 5]. ∎

本稿の主結果である $\tilde{P}_{r,q}(T)$ の Riemann 予想は, 正規化した $\tilde{P}_{r,q}(T/\sqrt{q})$ が定理 4.1 の仮定を満たすことを証明することによって得られる. 定理 4.1 は古典的な関数論の結果を利用することによって証明される (この定理については [7] も参照). 以下, 証明の概略を見よう.

多項式

$$f(T)=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m\quad(m>2k)\quad(4.1)$$

が $a_0>a_1>\cdots>a_k>0$ を満たしているとする. $f(T)$ を 2 つの多項式

$$\begin{aligned}P(T)&:=a_0+a_1T+\cdots+a_kT^k,\\ Q(T)&:=a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m,\end{aligned}\qquad(4.2)$$

の和で $f(T)=P(T)+Q(T)$ と表す. このとき仮定 $a_0>a_1>\cdots>a_k>0$ から, 定理 4.2 により $P(T)$ は $|T|\le 1$ に根を持たないことがわかる. この $P(T)$, $Q(T)$ に対して, 次が成り立つ:

定 理 4.3 単位円の内部 $|T|<1$ において $|P(T)|>|Q(T)|$.

これが言えれば, $|T|<1$ において $f(T)=P(T)+Q(T)\neq 0$ がわかる. 実際, もし $f(T)=0$ となるなら, $P(T)=-Q(T)$, したがって $|P(T)|=|Q(T)|$ $(\exists T,\ |T|<1)$ となり, 定理 4.3 に矛盾する. ところで, $f(T)$ が自己相反という仮定から

$$T^mf\left(\frac{1}{T}\right)=f(T)$$

が成り立つ. この式は, 単位円の内部にある $f(T)$ の根と単位円の外部にある $f(T)$ の根が 1 対 1 に対応することを示しており (α が根ならば $1/\alpha$ も根), このことと $f(T) \neq 0$ ($|T| < 1$) を合わせると, $f(T)$ は単位円の内部にも外部にも根を持たないこと, つまりすべての根が単位円周上にあることがわかり, 定理 4.1 が示せることとなる. そこで, 定理 4.3 を証明すればよい. まず簡単な計算により, (4.2) 式の $P(T)$, $Q(T)$ に対し, $|T| = 1$ 上で

$$|P(T)| = |Q(T)|. \tag{4.3}$$

であることが示せる. さらに, 次のよく知られた結果を準備する:

定 理 4.4 (最大値の原理) 関数 $g(T)$ は有界領域 $D \subset \mathbf{C}$ で正則かつ非定数, $\overline{D}$ (D の閉包) で連続とする. すると $|g(T)|$ はその最大値 M を $\overline{D} - D$ 上でとり, しかも D において

$$|g(T)| < M.$$

証 明. Ahlfors [1, p.134]. ∎

さて, 定理 4.4 を関数 $g(T) := Q(T)/P(T)$, 領域 $D := \{T \in \mathbf{C}\ ;\ |T| < 1\}$ に対して適用する. 明らかに $g(T)$ は有理型かつ非定数. しかも定理 4.2 より $g(T)$ は $\overline{D}$ 上で極を持たない. さらに (4.3) 式より, D の境界上で $|g(T)| = 1$. したがって定理 4.4 により D の内部で $|g(T)| < 1$ となることがわかり定理 4.3 が得られる.

主結果である定理 1.5 は, $r \geq 3$, $q \geq 4$ のときに $\tilde{P}_{r,q}(T/\sqrt{q})$ が定理 4.1 の仮定を満たすことを証明して得られる. その計算は全く初等的であり, ここでは省略する (詳しくは [6, §6] を参照). 前にも述べたが, $q = 2, 3$ の場合に定理 1.5 が証明できないのは, $\tilde{P}_{r,q}(T/\sqrt{q})$ が定理 4.1 の仮定を満たさないからである. しかし, 数値実験してみると, これらの場合にも $\tilde{P}_{r,q}(T/\sqrt{q})$ の根は単位円周上にあるようである.

論文 [6] では, C が MDS 符号のとき, そして Golay 符号 (自己双対でないもの, 2 つある) のときにも, 上の方法で作った不変式が Riemann 予想を満たすことを示した ([6, §3, §7]). ところで, ある種の MDS 符号, 一般 Hamming 符号, Golay 符号は「完全符号」(Pless [16, p.21]) という効率的な一群の符号を形成し, 応用上も重要なものである. 実在の符号 C から (2.1) によって得られる不変式, およびその Riemann 予想が応用上意味を持つのかどうか, まだわからない. しかし完全符号から得られる不変式がそろって Riemann 予想を満たす (一部は予想だが), という現象にはちょっと興味を惹かれる. さらに完全符号以外の MDS 符号も存在するときには非常によい符号となる. 定義 1.4 の Riemann 予想が符号の何らかのよい性質を反映している可能性もなくはない気がする.

Submitted on February 28, 2010.

参考文献

[1] Ahlfors, L. V. : Complex Analysis, third ed., McGraw-Hill, NewYork, 1979.

[2] Brouwer, A. E. : Bounds on the size of linear codes, in V. S. Pless, W. C. Huffman (eds.), Handbook of Coding Theory, I, II, Elsevier Science B. V., Amsterdam, 1998, 295-461.

[3] 知念 宏司, 平松 豊一 : 線形符号のゼータ関数とリーマン予想の類似 (Iwan Duursma の仕事の紹介), 符号と暗号の代数的数理, 京都大学数理解析研究所講究録 1361 (2004), 91-101.

[4] 知念 宏司 : 線型符号のゼータ関数とそのリーマン予想 (Iwan Duursma の仕事の紹介, 及び 1 つの拡張), 仙台数論及び組合せ論小研究集会 2004 報告集 (2005), 31-44.

[5] Chinen, K : Zeta functions for formal weight enumerators and the extremal property, Proc. Japan Acad. **81** Ser. A. (2005), 168-173.

[6] _____ : An abundance of invariant polynomials satisfying the Riemann hypothesis, Discrete Math. **308** (2008), 6426-6440.

[7] _____ : Distribution of the zeros of certain self-reciprocal polynomials, 解析的整数論とその周辺, 京都大学数理解析研究所講究録 1665 (2009), 9-16.

[8] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[9] _____ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[10] _____ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[11] _____ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[12] 平松 豊一, 知念 宏司 : 線形符号のゼータ関数とそのリーマン予想, 特集「符号化理論の新時代」, 数理科学 **497** (2004), 42 - 47.

[13] 楠 幸男 : 解析函数論, 廣川書店, 1962 年.

[14] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[15] 奥田 隆幸 : 不変式環上のリーマン仮説類似について, 有限群論と代数的組合せ論, 京都大学数理解析研究所講究録 1593 (2008), 145-153.

[16] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).

Extremal Type II $\mathbb{Z}_{2k}$-codes

山形大学理学部／ＪＳＴさきがけ
原田 昌晃

1 準備

代数的符号理論において, 理論面だけでなく応用面においても注目されているクラスの一つに self-dual code があり binary extended Golay code (2 元体上の code を binary とよぶ) などの良く知られた code がこのクラスに属する. 古くから有限体上の self-dual code の研究が行なわれているが, その中でも binary self-dual code の特別な場合である Type II code が特に活発に研究されて来た. 1990 年代から有限環上の符号理論の研究もさかんに行なわれていて, 例えば binary Type II code の一般化として Type II $\mathbb{Z}_{2k}$-code が考えられている ([5] を参照). 講演では $k \leq 6$ の Type II $\mathbb{Z}_{2k}$-code に対して minimum Euclidean weight に関する上限を与えて extremal を定義し, これらの code の存在について紹介をした. なお, この結果は三枝崎剛氏との共同研究 [3] に基づく.

位数 $2k$ の整数の剰余環を $\mathbb{Z}_{2k} = \mathbb{Z}/2k\mathbb{Z}$ $(= \{0, 1, 2, \ldots, 2k-1\})$ と表す. 長さ n の $\mathbb{Z}_{2k}$-code C とは $\mathbb{Z}_{2k}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{Z}_{2k}\}$ の $\mathbb{Z}_{2k}$-部分加群のことである. $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_{2k}^n$ に対しての Euclidean weight $\mathrm{wt}_E(x)$ を $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$ と定義する. C の minimum Euclidean weight $d_E(C)$ は 0 でない最小の Euclidean weight のことである. C の dual code $C^\perp$ を $\{x \in \mathbb{Z}_{2k}^n \mid x \cdot y = 0 \ (\forall y \in C)\}$ と定義する, ここで内積 $\cdot$ は標準的なものを考える. $C = C^\perp$ のとき C は self-dual とよばれる. self-dual $\mathbb{Z}_{2k}$-code C で $\mathrm{wt}_E(x) \equiv 0 \pmod{4k}$ $(\forall x \in C)$ であるとき Type II code と呼ばれる [1]. $k = 1$ の場合は古くから知られている binary Type II code の定義と一致する. 一般の k に対しても $k = 1$ の場合と同じような結果が多く成り立つことが知られており [1], 例えば Type II code が存在するのは長さ $n \equiv 0 \pmod 8$ であることが分かっている.

binary Type II code の minimum (Euclidean) weight については次が知られている.

定理 1 (Mallows–Sloane [4]). C を長さ n の binary Type II code とすると

$$d_E(C) \le 4\Big(\Big[\frac{n}{24}\Big] + 1\Big).$$

等号が成立する場合を extremal とよぶ. 以下の長さ

$$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136.$$

で binary extremal Type II code の存在が知られている: 存在性の分かっていない最小の長さは 72 で, 既に 1973 年には Sloane [6] によって問題として提案されていて, 有名な未解決問題の一つとなっている.

2 結果

長さ n の Type II $\mathbb{Z}_{2k}$-code の minimum Euclidean weight $d_E(C)$ に対して次が成り立つことが分かった.

定理 2. $k \le 6$ と仮定する. C を長さ n の Type II $\mathbb{Z}_{2k}$-code とすると

$$d_E(C) \le 4k\Big(\Big[\frac{n}{24}\Big] + 1\Big).$$

注意 3. この結果は, $k = 1$ の場合は既に定理 1 で述べており, $k = 2$ の場合は [2] で示されている.

binary の場合と同様に, 等号が成立する長さ n の Type II $\mathbb{Z}_{2k}$-code を extremal とよぶ. 新たに, 次の場合に

$$(k, n) = (4, 56), (4, 64), (5, 48), (5, 56), (5, 64), (6, 32), (6, 40), (6, 48), (6, 56), (6, 64)$$

extremal Type II $\mathbb{Z}_{2k}$-code を構成することが出来た. 今までに知られている結果と併せることで次を得る.

命題 4. $k \le 6$ であれば長さ $n < 72$ かつ $n \equiv 0 \pmod 8$ で extremal Type II $\mathbb{Z}_{2k}$-code が存在する.

上で述べた Sloane [6] による未解決問題を含む形で新たな問題を提案する.

問題 5. $k \le 6$ に対して長さ 72 の extremal Type II $\mathbb{Z}_{2k}$-code は存在するか?

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 257–269.

[2] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

[3] M. Harada and T. Miezaki, An upper bound on the minimum weight of Type II $\mathbb{Z}_{2k}$-codes, (submitted).

[4] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[5] E. Rains and N.J.A. Sloane, "Self-dual codes," Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam, 1998, pp. 177–294.

[6] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.

ユークリッド空間における 2 次元整数格子のある性質

三枝崎 剛 Tsuyoshi Miezaki *

この原稿は, 2009 年 12 月の第 8 回「代数学と計算」研究集会 (首都大学東京) の三枝崎による上の題での講演の記録です. タイトルの英訳は “On a property of 2-dimensional integral Euclidean lattices (joint work with Eiichi Bannai) ” であり, 坂内 · 三枝崎の著者によるこのタイトルのプレプリント [1](投稿中) に基づいています.

1 序

ユークリッド空間における 2 次元整数格子 $\Lambda \subset \mathbb{R}^2$ に関する以下の性質を考えます.

定義 1.1. 任意の自然数 n に対して, ちょうど n 個の Λ の格子点を通るような円が存在するとき, Λ を universally concyclic と呼ぶ.

$(a,b),(c,d) \in \mathbb{R}^2$, $(ad-bc \neq 0)$ で生成される格子を $L[(a,b),(c,d)]$ と書くことにします. その時 universally concyclic に関して以下のことがが知られています.

- [cf. [4]] $\mathbb{Z}^2 (= L[(1,0),(0,1)])$ は universally concyclic.
- [cf. [5]] $L[(1,0),(-1/2,\sqrt{3}/2])$ 及び $L[(1,0),(0,\sqrt{3}])$ は universally concyclic.
  $(d = 2,7,11,19,43,67,163$ に対して $L[(1,0),(0,\sqrt{d}])$ は universally concyclic.)

*Department of Mathematics, Hokkaido University, Hokkaido 060–0810, Japan, e-mail: miezaki@math.sci.hokudai.ac.jp. The author is supported by JSPS Research Fellowship.

- [cf. [5]] $q := ad - bc$ を $q \equiv 3 \pmod 4$ となる素数とする. その時 $L[(a,b),(c,d)]$ は universally concyclic.
- [cf. [5]] $\tau =$ 超越数. $L[(1,\tau),(0,1)]$ の 4 点を通る円は存在しない. 即ち universally concyclic でない.
- [cf. [5]] (α/β) が無理数 $\Longleftrightarrow$ $L[(\alpha,0),(0,\beta)]$ の 5 点を通る円は存在しない.

この講演では, 以下の定理を証明しました:

定理 1.1. 全ての 2 次元整数格子 は *universally concyclic.*

ここでは, 簡単のため $L[(1,0),(0,\sqrt{2})]$ の証明を述べ, それを, 一般にどう拡張するかを述べたいと思います. 詳しくは [1] を参照してください.

2 $L[(1,0),(0,\sqrt{2})]$ が universally concyclic であることの証明

$\mathbb{Z}[x] := \{a + bx \mid a, b \in \mathbb{Z}\}$ と定義します. 以下では, 虚二次体に関する幾つかの事実を使います. 詳しくは, [2, 3, 7] を参照してください. $L[(1,0),(0,\sqrt{n}])]$ を虚二次体の整環と考えます. 即ち, 格子 $\Lambda = L[(1,0),(0,\sqrt{n}])]$ $(\leftrightarrow f_\Lambda = x^2 + ny^2)$ に対して

$$\Lambda \simeq \mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}(\sqrt{-d}),$$

ここで $-4n = f^2 d_K$, $d_K = \begin{cases} -4d & \text{if } -d \equiv 2,\ 3 \pmod 4, \\ -d & \text{if } -d \equiv 1 \pmod 4. \end{cases}$

例えば

$$L[(1,0),(0,\sqrt{3}])] \simeq \mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3}).$$

の様にです.

定理 2.1 (cf. [5])**.** $L[(1,0),(0,\sqrt{2})]$ は *universally concyclic.*

補題 2.1. $A(k) := \{z \in \mathbb{Z}[\sqrt{-2}] \mid |z|^2 = 41^k\}$ と定義すると, $\sharp A(k) = 2(k+1)$.

Proof. $(41) = P\overline{P}, P = (3 + 4\sqrt{-2})$ を, イデアル (41) の素イデアル分解する. その時ノルム p^k の整イデアルは以下のみである: P^k, $P^{k-1}P'$, ..., $(P')^k$. $z \in \mathbb{Z}[\sqrt{-2}]$ に対して, (z) と $(-z)$ は同じイデアルを定めるので, 題意は示された. □

補題 2.2. $\check{A}(k) := \{x + y\sqrt{-2} \in A(k) \mid x + y \equiv -1 \pmod 4\}$ と定義すると, $\sharp\check{A}(k) = k + 1$.

Proof. 補題 2.1 の証明より任意の $x+y\sqrt{-2} \in A(k)$ に対して, $x+y \equiv \pm 1 \pmod 4$. もし $x+y\sqrt{-2} \in A(k)$, $x+y \equiv 1 \pmod 4$ ならば $-x+y \equiv -1 \pmod 4$ となる. □

Proof of Theorem 2.1. 任意の正整数 $k > 0$ に対して, 円 Γ_k を以下で定義する:

$$|4z - 1|^2 = 41^k.$$

$C(k)$ を L の部分集合で Γ_k が通る点と定義する. $\sharp C(k) = k + 1$ を示す. 写像 $f : C(k) \to \check{A}(k)$ を以下で定義する:

$$z \mapsto 4z - 1.$$

$$\left(\begin{array}{c} \because \text{もし } z = x + y\sqrt{-2} \in C(k) \text{ ならば } 4z - 1 = 4x - 1 + 4y\sqrt{-2}, \\ \text{よって } 4x - 1 + 4y \equiv -1 \pmod 4. \text{ 即ち } 2\sqrt{a}z - j \in \check{A}(k). \end{array} \right)$$

一方, 写像 $\check{A}(k) \to C(k)$ を以下で定義する: $x+y\sqrt{-n} \mapsto (x+1)/4+y/4$.

$$\left(\begin{array}{c} \because \text{もし } x + y\sqrt{-2} \in \check{A}(k) \text{ ならば } x + y \equiv -1 \pmod 4, \\ \text{よって } x + 1 \equiv 0 \pmod 4. \text{ 即ち } (x + 1)/4 + y/4 \in C(k). \end{array} \right)$$

ゆえに f は全単射, よって $\sharp C(k) = \sharp\check{A} = k + 1$.

3 一般の場合

$L[(1, 0), (0, \sqrt{2})]$ の証明で本質的な部分は以下の 2 点でした.

1. 任意の格子 L $(ax^2 + bxy + cy^2, n = b^2 - 4ac)$ に対して, 次の様な表示を持つ素数 p が存在するか: $p = x^2 + ny^2$ かつ $y \equiv 0 \pmod{2a}$.
   (その様な素数を $p_{n,a}$ と書く.)
   ($L[(1, 0), (0, \sqrt{-2})]$ $(x^2 + 2y^2)$ の時は, $41 = 3^2 + 2 \times 4^2$.)

2. もし上の素数が存在するならば, $A_{n,a}(k) := \{z \in \mathbb{Z}[\sqrt{-n}] \mid |z|^2 = {p_{n,a}}^k\}$ と定義した時 $\sharp A_{n,a}(k) = 2(k+1)$ か?

これは, 以下のように証明されます (数論に関する詳しい事は, [3, 7-9 章] もしくは [1] を参照してください):

命題 3.1. 任意の正整数 n, a に対して, 次の様な素数 $p(\neq n)$ が存在する : $p = x^2 + ny^2$ かつ $y \equiv 0 \pmod{2a}$.

Proof. Dirichlet の算術級数定理の一般化を使い, その様な素数は密度 $1/[L:K]$ を持つ, 即ち無限に存在する事がわかります, ここで L は $\mathbb{Z}[\sqrt{-n}]$ の ring class field を表します [3]. よって, 命題は従います. □

命題 3.2. $n \neq 1$, $\mathbb{Z}[\sqrt{-n}] = \mathcal{O}_f \subset K = \mathbb{Q}(\sqrt{-d})$ と仮定します. p を次の条件を満たす素数とします : $|z|^2 = p$, $(d_K/p) = 1$, $(p, f) = 1$ を満たす $z \in \mathbb{Z}[\sqrt{-n}]$ が存在する. この時, $\sharp\{z \in \mathbb{Z}[\sqrt{-n}] \mid |z|^2 = p^k\} = 2(k+1)$.

Proof. (p) は, $\mathcal{O}_K$ の中で, $(p) = PP'$ と分解します. 条件 $z \in \mathbb{Z}[\sqrt{-n}]$ より P と P' は主イデアルとなり, Q と Q' を次の様に定義します: $Q := P \cap \mathcal{O}_f$, $Q' := P' \cap \mathcal{O}_f$. すると, Q と Q' は, $\mathcal{O}_f$ の f と素な proper な主イデアルとなります [3]. proper イデアルの分解の一意性を使うと, ノルム p^k のイデアルは以下のように書き下せます:

$$Q^k,\ Q^{k-1}Q', \ldots, {Q'}^k.$$

$z \in \mathbb{Z}[\sqrt{-n}]$ に対して, (z) と $(-z)$ は同じイデアルを定める事に注意すると, 題意は従います. □

以上 2 つの命題を使う事により, 一般の 2 次元整数格子が universally concyclic である事が示せます. 詳しくは [1] を参照してください.

4 高次元の場合

3 次元以上の場合はどうか, 自然に疑問が起きます. しかし, 3 次元以上の整数格子は, 2 次元の結果を使い, 全て universally concyclic になる事が示せます. しかし, 円上の格子点は, 全て同一 2 次元平面上に存在しており, あまり面白い例とはいえません. そこで前原氏は, 定義 1.1 に幾つか条件を付けた, 高次元格子の新たな universally concyclic の定義をいくつか

提示しておられます [6]. この定義に関して, 全ての整数格子は universally concyclic か否か決定するのは興味ある問題といえます.

最後になりましたが，世話人の皆様，旅費を援助してくださりました脇克志氏に感謝いたします.

参考文献

[1] E. Bannai and T. Miezaki, On a property of 2-dimensional integral Euclidean lattices, submitted, arXiv:0912.1659.

[2] A. I. Borevich and I. R. Shafarevich, *Number theory*, translated from the Russian by Newcomb Greenleaf, Pure and Applied Mathematics, **20** Academic Press, New York-London 1966.

[3] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.*, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[4] H. Maehara and M. Matsumoto, Is there a circle that passes through a given number of lattice points?, *Europ. J. Combinatorics* **19** (1998), 591–592, doi:10.1006/eujc.1997.0189.

[5] H. Maehara, On the number of concyclic points in planar lattices, preprint.

[6] H. Maehara, On a sphere that passes through n lattice points, *Europ. J. Combinatorics* (2009), doi:10.1016/j.ejc.2009.03.034.

[7] D. B. Zagier, *Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie*, Springer-Verlag, Berlin, Heidelberg, New York, 1981.

楕円曲線 $E : y^2 = x^3 - nx$ の生成元

藤田育嗣* 寺井伸浩†

1 定理

n を平方数でない正の整数とし，E を $y^2 = x^3 - nx$ で定義された $\mathbb{Q}$ 上の楕円曲線とする．Mordell の定理によって E の $\mathbb{Q}$ 有理点のなす群 $E(\mathbb{Q})$ は有限生成アーベル群である．$E(\mathbb{Q})$ ねじれ部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ が $\mathbb{Z}/2\mathbb{Z}$ と同型であることは容易に分かるが，自由部分 $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ の構造を決定することは容易ではない．

[FT] で，n が素数べき (特に素数) のときに E 上の整数点や $E(\mathbb{Q})$ の生成元について調べ，例えば，奇数 t に対して $n = 4t^2 + 1$ が素数であるとき，$E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ は 1 点 $(-1, 2t)$ で生成されることが分かった．しかし，$n = a^4 + b^4$ (a, b は自然数) の形の素数 n に対しては，2 点 $P_1 = (-b^2, a^2b)$, $P_2 = (-a^2, ab^2)$ が $E(\mathbb{Q})$ の指数有限な部分群を生成することは分かったが，$E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ の生成元になり得るか否かは分からなかった．一方 Duquesne ([Duq]) は，整数 k に対して $n = (2k^2 - 2k + 1)(18k^2 + 30k + 17)$ が平方因子をもたないならば，$G_1 = (-(2k^2 - 2k + 1), 4(k + 1)(2k^2 - 2k + 1))$ と $G_2 = (9(2k^2 - 2k + 1), 12(3k - 2)(2k^2 - 2k + 1))$ の 2 点がいつも $E(\mathbb{Q})$ の生成元の系に入り得ることを示した．ここで $s = 2k^2 - 2k + 1$, $t = 18k^2 + 30k + 17$ とおくと，$t - s$, $3^4 s - t$ は共に平方数になり，このことが $G_1, G_2 \in E(\mathbb{Q})$ に寄与している．これを端緒として，Duquesne の結果を次のように大きく一般化できることに気づいた．

定理. n を平方数でなく 4 乗因子をもたない正整数で，$n = st$ (s, t は平方数でない正整数) と表されるものとする．また

$$t - s = \alpha^2, \qquad m^4 s - t = \beta^2 \tag{1.1}$$

なる正整数 α, β, m が存在すると仮定し，E を $y^2 = x^3 - nx$ で定義される楕円曲線とする．もし $m = 2$ または 3 ならば，2 点 $G_1 = (-s, s\alpha), G_2 = (m^2 s, ms\beta)$ はいつも $E(\mathbb{Q})$ の生成元の系に入り得る．$m \geq 4$ の場合には，$n \geq m^{29.2}$ ならば同じことが成り立つ．

2 定理の証明

有理点 $P = (x, y)$ が 2 等分点をもつ (つまり $2E(\mathbb{Q})$ に入る) ならば，x, $x + \sqrt{n}$, $x - \sqrt{n}$ がすべて $\mathbb{Q}(\sqrt{n})$ において平方数でければならない ([Kn, Theorem 4.2])．このことを使って次が示される．

補題 1. $T = (0, 0)$ とおくと，定理の仮定の下で，$G_1, G_2, G_1 + T, G_2 + T, G_1 + G_2, G_1 + G_2 + T \notin 2E(\mathbb{Q})$ が成り立つ．従って，2 点 G_1, G_2 は $E(\mathbb{Q})_{\mathrm{tors}}$ を法として独立である．

この補題と次の Siksek の定理とを合わせて，定理は証明される．

*日本大学生産工学部
†足利工業大学（工学部共通課程）

補題 2. (cf. [Sik, Theorem 3.1]) E を $\mathbb{Q}$ 上定義された階数 2 以上の楕円曲線とし，G_1, G_2 を $E(\mathbb{Q})_{\mathrm{tors}}$ を法として独立な $E(\mathbb{Q})$ の点とする．$\{P_1, P_2, \ldots, P_r\}$ を $E(\mathbb{Q})_{\mathrm{tors}}$ を法とする $E(\mathbb{Q})$ の生成元の系で $G_1, G_2 \in \langle P_1\rangle + \langle P_2\rangle$ なるものとし，$\langle P_1\rangle + \langle P_2\rangle$ における G_1, G_2 の張る部分格子の指数を ν とする．もし，$E(\mathbb{Q})$ が $\hat{h}(Q) \leq c$ (c はある正の実数) なる無限位数の点 Q を含まないならば,

$$\nu \leq \frac{2}{\sqrt{3}} \cdot \frac{\sqrt{R(G_1, G_2)}}{c}$$

が成り立つ.

ここで,

$$R(G_1, G_2) = \hat{h}(G_1)\hat{h}(G_2) - \frac{1}{4}\left(\hat{h}(G_1 + G_2) - \hat{h}(G_1) - \hat{h}(G_2)\right)^2$$

であり，$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ は

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$$

で定義される canonical height，$h : E(\mathbb{Q}) \to \mathbb{R}$ は $h(P) = \log \max\{|a|, |b|\}$ ($P = (b/a, *)$, $\gcd(a, b) = 1$) で定義される naïve height である (この定義は [Duq] と同じもので，[Sil1, Sil2, Coh] の定義の 2 倍である)．canonical height は local height $\hat{\lambda}_p$ に分解することにより計算される (cf. [Sil3, Chapter VI])：

$$\hat{h}(P) = \sum_{p:\text{prime or } \infty} \hat{\lambda}_p(P) \qquad (P \in E(\mathbb{Q}) \setminus \{O\}).$$

まず，有限部分 $\hat{h}_{\mathrm{fin}}(P) = \sum_{p:\text{prime}} \hat{\lambda}_p(P)$ は Cohen のアルゴリズム ([Coh, Algorithm 7.5.6]) を使えば容易に計算できる (今 n は 4 乗因子をもたないので $y^2 = x^3 - nx$ は E の global minimal model であり，従ってこのアルゴリズムを適用できる).

補題 3. $E(\mathbb{Q})$ の任意の点 $P = (a/d^2, b/d^3)$ ($a, b, d \in \mathbb{Z}$, $\gcd(a, d) = \gcd(b, d) = 1$, $d > 0$) に対し,

$$\hat{h}_{\mathrm{fin}}(P) = 2\log d - \frac{1}{2}\log\left(\prod_{p_i | a,b,n,\, p_i \neq 2} p_i^{e_i}\right) + \hat{h}_2(P)$$

が成り立つ．ここで，$p_i^{e_i} \| n$ ($e_i \in \{1, 2, 3\}$) であり，d が偶数のときは $\hat{h}_2(P) = 0$, d が奇数のときは $\hat{h}_2(P)$ は次で与えられる：

n	a	b	$\hat{h}_2(P)$
偶数	奇数	奇数	0
奇数	偶数	偶数	0
奇数	奇数	偶数	$-\frac{1}{2}\log 2$
$v_2(n) = 1$	偶数	偶数	$-\frac{1}{2}\log 2$
$v_2(n) = 2$ *and* $n/4 \equiv 1 \pmod 4$	$v_2(a) = 1$	$v_2(b) \geq 3$	$-\frac{3}{2}\log 2$
$v_2(n) = 2$ *and* $n/4 \equiv 3 \pmod 4$	$v_2(a) = 1$	$v_2(b) = 2$	$-\frac{7}{4}\log 2$
$v_2(n) = 2$	$v_2(a) \geq 2$	$v_2(b) \geq 2$	$-\log 2$
$v_2(n) = 3$	$v_2(a) \geq 3$	$v_2(b) \geq 3$	$-\frac{3}{2}\log 2$

任意の点 $P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_{\mathrm{tors}}$ に対する無限部分 $\hat{\lambda}_\infty(P)$ の計算には，Cohen による次の公式 ([Coh, Algorithm 7.5.7]) を使う：

$$\hat{\lambda}_\infty(P) = \frac{1}{16}\log\left|\frac{64n^3}{q}\right| + \frac{1}{4}\log\left(\frac{\omega_1}{2\pi}y(P)^2\right) - \frac{1}{2}\log|\theta|. \tag{2.1}$$

ここで，

$$q = e^{2\pi i\frac{\omega_2}{\omega_1}},\ \omega_1 > 0,\ \mathrm{Im}(\omega_2) > 0,\ \mathrm{Re}(\omega_2) = 0,$$
$$\mathrm{Im}(z) = 0,\ 0 \le z < \omega_1 \quad \text{または} \quad \mathrm{Im}(z) = \mathrm{Im}(\omega_2/2),\ 0 \le z - \omega_2/2 < \omega_1,$$
$$\theta = \sum_{k=0}^{\infty}(-1)^k q^{k(k+1)/2}\sin\left((2k+1)\frac{2\pi}{\omega_1}\mathrm{Re}(z)\right)$$

で，$z = z(P)$ は P の楕円対数である (θ は自明な上限 $|\theta| < 1/(1-|q|)$ をもつ).

補題 4. $n \not\equiv 12 \pmod{16}$ ならば，任意の無限位数の点 $P \in E(\mathbb{Q})$ に対し，

$$\hat{h}(P) > 0.125\log n + 0.3917$$

が成り立つ.

注意 1. (1.1) から $n = st \not\equiv 12 \pmod{16}$ が分かるので，定理の証明に補題 4 を使うことができる.

一方，$\hat{\lambda}_\infty(G_1)$, $\hat{\lambda}_\infty(G_2)$ の計算には Tate 級数 (cf. [Sil2]) を使う：

$$\hat{\lambda}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{k=0}^{N-1}\frac{c_k}{4^k} + R(N). \tag{2.2}$$

ここで，

$$c_k = \log|z(2^kP)|,\ \ z(Q) = \left(1 + \frac{n}{x(Q)^2}\right)^2 \text{ for } Q \in E(\mathbb{Q}) \setminus \{(0,0)\},$$
$$\frac{1}{3\cdot 4^N}\log\left(\frac{(64n^3)^2}{2^{60}H^8}\right) \le R(N) \le \frac{1}{3\cdot 4^N}\log\left(2^{11}H\right)$$

で，$H = \max\{4n, n^2\}$ である.

補題 5.

$$\hat{h}(G_1) < \frac{24577}{98304}\log n + \log m + \frac{131081}{196608}\log 2,$$
$$\hat{h}(G_2) < \frac{24577}{98304}\log n + \frac{1}{2}\log\left(m^2\left(m^4+1\right)\right) + \frac{32777}{196608}\log 2.$$

[定理の証明]　補題 1 より，格子指数 $\nu < 3$ を示せばよい．$m \ge 4$, $n \ge m^{29.2}$ の場合には，補題 3, 4, 5 を合わせて $\nu < 3$ が分かる．$m = 2$ のとき，$n \ge 4885$ ならば $\nu < 3$ となるのであとは

$$(s,t) = (3,39),\ (6,15),\ (6,87),\ (15,159),\ (30,39),\ (51,87)$$

の各場合に G_1, G_2 が $E(\mathbb{Q})$ の生成元の系に入り得ることを確認すればよい (Magma ([BC]) 等でチェックできる)．$m = 3$ のとき，$\nu < 3$ となるためには $n \ge 1.587\cdot 10^8$ でなければならない．このとき定理の仮定をみたす (s,t) は 2493 組あり，各場合に生成元を確認することは非常に困難である．しかしながら，一般に $\nu < 5$ であることは分かり，補題 1 から $\nu \ne 4$ なので，この 2493 組の各 (s,t) に対して

$$G_1, G_2, G_1+G_2, G_1-G_2 \notin 3E(\mathbb{Q})$$

となっていることを確認すればよい (Magma ([BC]) の “DivisionPoints($*$, 3)” でチェックできる)．□

注意 2. (1) 定理のような楕円曲線に対して格子指数 ν が小さい理由は，G_i $(i \in \{1,2\})$ の canonical height $\hat{h}(G_i)$ が非常に小さいことにある．G_i の x 座標を $x(G_i)$ とかくと，

- $x(G_i)$ が (おおよそ) n を割る $\Longrightarrow \hat{h}_{\mathrm{fin}}(G_i)$ が (おおよそ) $-\dfrac{1}{2}\log|x(G_i)|$ より小さい (補題 3)
- $|x(G_i)| \fallingdotseq \sqrt{n} \Longrightarrow \log|x(G_i)| \fallingdotseq \dfrac{1}{2}\log n, \quad \hat{\lambda}_\infty(G_i) \fallingdotseq \dfrac{1}{2}\log n$ ((2.2) 参照)

であり，従って $\hat{h}(G_i)$ は (おおよそ) $(\log n)/4$ より小さくなる (補題 5).

(2) [FT] で考察した $n = a^4 + b^4$ の場合には $x(P_i) \in \{-b^2, -a^2\}$ が n と素なので，$\hat{h}_{\mathrm{fin}}(P_i)$ はそんなに小さくならない．このため生成元を決定できなかった.

3 無限族の構成

(1.1) から t を消去すると，$(m^4-1)s = \alpha^2 + \beta^2$ となり，$\alpha = uk + vl$, $\beta = ul - vk$ とおけば,

$$s = \frac{\alpha^2+\beta^2}{m^4-1} = \frac{u^2+v^2}{m^4-1}(k^2+l^2), \qquad t = s + (uk+vl)^2$$

となる．よって，$u^2 + v^2 \equiv 0 \pmod{(m^4-1)}$ をみたす u, v をとれば 2 次形式 $n = st \in \mathbb{Z}[k,l]$ が得られる．この議論を基にして，次の命題を得た.

命題. 整数 $m > 1$ に対し，$m^4 - 1 = m_0 m_1 m_2^2$ とおく．ここで，m_0, m_1, m_2 は正整数で $m_0 m_1$ は平方因子をもたず，m_0, m_1 の任意の素因子は 4 を法としてそれぞれ 3, 1 または 2 と合同であるとする．$p_1, \ldots, p_r$ を 4 を法として 1 または 2 と合同な相異なる素数で，どの奇数 p_i も $m^4 - 1$ を割り切らないとする ($r = 0$ も許容する．もし $m_1 = 1$ ならば $r \geq 1$, $m_1 = p_1 = 2$ ならば $r \geq 2$ と仮定する)．u', v' を

$$(u')^2 + (v')^2 = m_1 p_1 \cdots p_r$$

をみたす正整数とし $u = m_0 m_2 u'$, $v = m_0 m_2 v'$ とおくとき,

$$s = \frac{u^2+v^2}{m^4-1}(k^2+l^2) \quad \text{and} \quad t = s + (uk+vl)^2$$

をみたす 2 次形式 $n = st$ は定理の仮定をみたす無限個の整数を表す.

[命題の証明]　Greaves の定理 ([Gr, Theorem (i)]) により，判別式が 0 でなく，7 次以上の既約因子をもたず，また $\gcd\{f(k,l); k, l \in \mathbb{Z}\}$ が平方因子をもたないような 2 次形式 $f(k,l) \in \mathbb{Z}[k,l]$ は無限個の平方因子をもたない整数を表す．これを n/m_0^2 または $n/(2m_0^2)$ に適用すればよい. □

注意 3. 4 を法として 1 と合同な素数は無限に存在するので，命題から，各 $m \geq 2$ に対し，定理の仮定をみたす無限個の整数 n を表すような 2 次形式 $n = n(k,l) \in \mathbb{Z}[k,l]$ が無限個存在することが分かる.

例. k, l を 0 でない整数とする．以下の各 s, t に対して，$s, t, n = st$ が平方数でなく n が 4 乗因子をもたないならば，2 点 $G_1 = (-s, s\alpha)$, $G_2 = (m^2 s, ms\beta)$ $(\alpha = \sqrt{t-s}$, $\beta = \sqrt{m^4 s - t}$, $m \in \{2, 3\})$ は $E(\mathbb{Q})$ の生成元の系に入り得る：

(I) $m = 2$ の場合：

(i) $s = 3(k^2 + l^2)$, $t = 3(4k^2 + 12kl + 13l^2)$;

(ii) $s = 6(k^2 + l^2)$, $t = 3(5k^2 + 18kl + 29l^2)$;

(iii) $s = 15(k^2 + l^2)$, $t = 3(32k^2 + 72kl + 53l^2)$.

(II) $m = 3$ の場合：

(i) $s = k^2 + l^2$, $t = 17k^2 + 64kl + 65l^2$;

(ii) $s = 2(k^2 + l^2)$, $t = 2(9k^2 + 48kl + 73l^2)$;

(iii) $s = 5(k^2 + l^2)$, $t = 149k^2 + 384kl + 261l^2$.

ここで，命題の (u, v) として次のものをとった：

(I) (i) $(u, v) = (3, 6)$; (ii) $(u, v) = (3, 9)$; (iii) $(u, v) = (9, 12)$.

(II) (i) $(u, v) = (4, 8)$; (ii) $(u, v) = (4, 12)$; (iii) $(u, v) = (12, 16)$.

注意 4. $s = (1-k)^2 + k^2$, $t = 17(1-k)^2 + 64(1-k)k + 65k^2$ なので，Duquesne の族 ($s = 2k^2 - 2k + 1$, $t = 18k^2 + 30k + 17$) は，例 (II) (i) に含まれる．

References

[BC] 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/.

[Coh] H. Cohen, *A Course in computational algebraic number theory*, Springer-Verlag, 1993.

[Duq] S. Duquesne, Elliptic curves associated with simplest quartic fields, J. Theor. Nombres Bordeaux 19 (2007), 81–100.

[FT] Y. Fu ita and N. Terai, Integer points and independent points on the elliptic curve $y = x^3 - p^k x$, preprint.

[Gr] G. Greaves, Power-free values of binary forms, Quart. J. Math. Oxford (2), 43 (1992), 45–65.

[Kn] A. W. Knapp, *Elliptic Curves*, Princeton, Princeton Univ. Press, 1992.

[Sik] S. Siksek, Infinite descent on elliptic curves, Rocky Mountain J. Math. 25 (1995), 1501–1538.

[Sil1] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[Sil2] J. H. Silverman, Computing heights on elliptic curves, Math. Comp. 51 (1988), 339–358.

[Sil3] J. H. Silverman, *The advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1994

SOME CONCEPTS AND METHODS TO INVESTIGATE PROBLEMS OF WARING TYPE II

R. MORIKAWA

1. Introduction

1-1. (W-Problems and a V-Problem) We fix $k \in N$ and take m natural numbers $(a_1, \ldots, a_m)$ 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 aim is to study the structure of $W(A)$. We call this problem by a general name $W(k,m)$-Problem. 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, Shulze-Pillot)

(c) W(3,4)-Problem

I gave a talk at AC 2007 on the theme. [6] refers my paper in Proceedings AC 2007. This report is a continuation of that. [4] refers T. Matsui's paper in the same Proceedings.

Adding to these W-Problem, I will take up the following V-Problem.

(d) V(a,b)-Problem : Let $V(a,b) = \{ax^2 + by^2 | \ x, y \in N\}$ with $(a,b) = 1$. About $V(1,1)$, the famous Fermat's criterion is known. Our aim is to obtain a similar criterion for general (a,b)'s.

1-2. (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 functions 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 [7] 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 31, 2010.

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.

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 $\boldsymbol{B} = \{\boldsymbol{b}(r) \mid 1 \leq r \leq a\}$. Here W is determined by $\boldsymbol{B}$. Thus in this case ∂W is $\{h(r)\}$.

Fact 3. For $m = 3, 4$ this $\boldsymbol{B}$ has a beautiful structure.

For W-Problems with $k \geq 2$, ∂W for $w \in W$ is usually taken as rw with a suitable $r \in N$. We call this r a realizer of w, and denote it as (r).

§ 2 tells that this method is useful to investigate $V(a, b)$.

1-3. (Cell and Lifting, Head-Tail Principle, DMH and FGH decmposition)

Adding to three devices (A)-(C), we propose the following (D),(E) and (F). These devices will appear in this report. But they have already used in other papers. Thus we indicate the place where they are used.

(D) (Cell and Lifting Principle)

1. We use this to investigate $V(a, b)$. For details see § 2.

2. This concept plays an important role for F-Problem wth $m = 4$. This is explained in [5] p.8 and in [6] p.7.

(E) (Head-Tail Principle)

1. For many list up problems of mathematical structures, it is usuful to define suitable diagrams. (Please remind the beautiful theory of Dynkin Diagrams.)

For W(1,4) Problem, a generalized tree with three sources works well (cf. [5] p.6). And in the case, Head or Tail of the tree characterize the corresponding mathematical structure. (The middle parts usually have stable structures.) Note that Dynkin Diagrams have this property. This ambiguous Principle is useful in many cases as a heuristic one. For example this explains Fraenkel's Conjecture about rational Beatty sequences (cf. [5] p.4). And this Principle is closely related with 'Surgery of Diagrams' and 'Stop Lemma' (cf. [5] p.7).

2. This Principle also works for $V(a, b)$-Problem (cf. § 2).

(F) (DMH decomposition and FGH decomposition)

1. As shown in § 2, any $v \in W(1,B) \setminus R$ is decomposed to dmh with $d \in cl(DP)$, $m \in cl(MP)$ and $h \in cl(HP)$. (Please consult § 2 for precise definitions.)

2. § 3 tells that any $w \in W(\star)$ is decomposed to fgh with $f \in cl(P(1))$, $g \in cl(\Psi(D))$ and $h \in H$.

3. Similar decomposition seems to appear widely in W-Problems with $k \geq 3$ (cf. § 4).

1-4. (Contents of this report)
1. § 2 treats $V(a,b)$ Problem. And RDS Problem is treated in § 3. In § 4, a bold conjecture with respect to $W(3,4)$-Problem is proposed.

2. Throughout this report, V and W have the same meaning. And for L a set of primes, $cl(L)$ denotes {the free products of primes in L } $\cup$ {1}. Other Notations used in each § are independent.

3. (Important Remarks) (a) It is regrettable that many propositions given in the report have no proofs. But they are supported by enomous numerical research. Thus we denote Assertion for proposition of that type.
(b) About Numerical Examples given in this report, "all properties" are not proved.

2. $V(a,b)$ Problem

2-1(Introduction)
In this section, we treat $V(ax^2+by^2)$. We denote it $V(a,b)$ or simply V. $V(1,1)$ allows the famous Fermat's criterion. Recently I found a suitable generalization of it. No proof has been obtained. But numerical search of about 100 cases of (a,b) supports Assertions (with no exception!)

($V(1,B)$-Problem) In this report we consider the case, $(a,b) = 1$ and a, b both are square free. In the case $t \in V(a,b)$ if and only if $at \in V(1,ab)$. Thus we may confine to the case $V(1,B)$ with square free B.

(Notations) 1. We put $4B = D$. We put $DP = \{$ prime divisors of $D\ \}$. And we put $|DP| = \rho$. For $U \subset [1, D-1]$, We put $Q(D;U) = \{p \mid \text{prime},\ p \equiv u \pmod D$ for some $u \in U\}$.

2. An element of $V(1,B)$ is called a V-element. We separate V-elements into three types :
(a) $R(1,B) = \{p \in V \mid p \text{ prime},\ p \nmid D\}$,
(b) $S(1,B) = \{n \in V \mid n \text{ composite}, (n,D) = 1\}$,
(c) $T(1,B) = \{n \in V \mid (n,D) > 1\}$.
These sets are simply noted R, S, T.

3. (Head system) For $V(1,B)$, we attach $\boldsymbol{H}(B) = \{B + r^2 \mid 0 \leq r \leq s\}$. ($s$ is taken a suitable number for each situation.) We call $\boldsymbol{H}(B)$ Head system of $V(1,B)$.

4. For a subset M of V, we define $CoreM$ as follows.
(i) Note that $v \in V$ implies $t^2 v \in V$ for any $t \in N$. Thus if $w \in M$ allows $t \geq 2$ for which w/t^2 is in V, we omit w from M.
(ii) Note that for $V(1,B)$, $v, w \in V$ implies $vw \in V$. Thus we let $CoreM$ so that its member has no decomposition of this type.
In this situation, we say that the members of $CoreM$ are irreducible.

5. ($Core\hat{T}$) T contains V-elements of special type. We define following three sets: $T(0) = \{t \in T \mid t \in cl(DP)\}$, $T(1) = \{By \in T \mid y > 1, (y, D) = 1\}$ and $T(2) = \{2By \mid y > 1, (y, D) = 1\}$. Note the facts $Bt \in V(1, B) \Leftrightarrow t \in V(1, B)$ and $2Bt \in V(1, B) \Leftrightarrow 2t \in V(1, B)$. Hence we make $\hat{T} = T \setminus (T(0) \cup T(1) \cup T(2))$. And study $Core\hat{T}$ instead of $CoreT$, and study $T(0)$ separately.

2-2 (Sets $F, G, M, Q(j)(2 \leq j \leq J)$)

We define the following sets step by step. (See Example 2.4.1.)

Step 1. Let $D = 4B$. And $F = \{n \mid n \in [1, D-1], (n, D) = 1\}$. Then $|F| = \varphi(D)$. Here F is a multiplicative group. We put $G = \{u^2 \pmod D | (u, D) = 1\}$, and consider G as a subgroup of F. Then $[F : G] = 2^\rho$.

Step 2. We take M where M is minimal for which $R \subset Q(D; M)$.

Assertion 2.2.1. M is the square class mod B. Thus G is a subgroup of M, whose index is m. Here $m = 1$ for $B \equiv 1 \pmod 4$ and $m = 2$ for other cases.

We say $V(1, B)$ is Full-case if $R = Q(D; M)$. And NF-case in otherwise. In NF-case, we put $M(\tau) = Q(D; M) \setminus R$. And MP denotes the set of pimes in $M(\tau)$.

Step3. We arrange Cosets of F/M as follows.

($\sharp$) $\quad M,\ t_2M, \ldots, t_{2^J}M$.

The cardinality satisfies $2mJ = 2^\rho$. From ($\sharp$), we choose t_jM $(2 \leq j \leq J)$ by the following rule :

(Choosing-rule) Let $\boldsymbol{H}(B)$ be Head system of $V(1, B)$. We decompose $B + r^2$ $(r = 1, 2, \ldots)$. We consider p primes which satisfy ;

(a) $p \mid B + r^2$, (b) $p \nmid D$, (c) $p \neq B + r^2$.

We choose p's which belong to different Cosets. We explain the process taking $B = 105$:

($B = 105$) In the case $M = \{1, 109, 121, 169, 289, 361\}$. We have

$B + 1 = 106 = 2.53$, $B + 4 = 109 =$ prime, $B + 9 = 114 = 2.3.19$, $B + 16 = 121 = 11^2$, $B + 25 = 130 = 2.5.13$, $B + 36 = 141 = 3.47$, $B + 49 = 154 = 2.7.11$, $B + 64 = 169 = 13^2$, $B + 81 = 186 = 2.3.31$, $B + 100 = 205 = 5.41$, $B + 121 = 226 = 2.113$, $B + 144 = 249 = 3.83$, $B + 169 = 274 = 2.137$, $B + 196 = 301 = 7.43$, etc.

We choose 7 numbers 53, 19, 11, 13, 47, 41, 43. And we get 7 Cosets which contain these numbers.

Assertion 2.2.2. Applying Choosing-rule, we obtain $J - 1$ Cosets from ($\sharp$). We make $Q(j) = Q(D; t_jM)$ for such j. Let x_j be the least member of $Q(j)$. Here we rearrange $Q(j)$ so that $x_2 < x_3 < \cdots < x_J$.

We call each $Q(j)$ a Cell.

2-3. (R, $CoreS$, $Core\hat{T}$ for Full-case)

For Full-case, we write $Q(j) = (x_j; \sim)$. We define multiple law of $Q(j)$'s as follows:

($\star$) $\quad$ Let $L(M) = L(1) = \{n \in N \mid n \equiv m \pmod D \text{ for some } m \in M\}$, and $L(j) = \{n \in N \mid n \equiv x_jm \pmod D \text{ for some } m \in M\}$, $(2 \leq j \leq J)$. We define $\{i, j\} = k$ if $x_ix_j \in L(k)$.

Assertion 2.3.1 ($CoreS$) Let $V(1, B)$ be Full-case. Then $s \in CoreS$ if and only if s satifies the following three conditions:

(1) s is a product of primes which are in $Q(j)$ $(2 \leq j \leq J)$.

(2) $s \in L(M)$.
(3) s is irreducible.

(Taking-combination) Let HP be the set of primes contained in $Q(j)$ with $(2 \leq j \leq J)$. Make $cl(HP)$. Take $t \in cl(HP)$. Let $t = p_1^{e_1} \cdots p_f^{e_f}$. We put $s(j)$ the sum of e_i for which $p_i \in Q(j)$. We call $(s(2), \ldots, s(J))$ Taking combination of t.

Then Taking-combination of $CoreS$ is finite. In Example 2.4.1. $CoreS$ of $V(1, 105)$ have Taking-combinations of (1), (2), (3).

To clarify $Core\hat{T}$, we use the following concepts. Let $U = \{u \in N \mid 1 < u < 2B,\ u|2B,\ u \neq B\}$. For $u \in U$, we put $((u)) = \{uy \in T \mid y > 1, (y, D) = 1\}$. We define $(u) \Rightarrow Q(j)$ if $ux_j \in V$.

Assertion 2.3.2. (Transfer rule) Assume $(u) \Rightarrow Q(j)$ for $u \in U$. Then $Core((u)) = uC$ where C is given by Transfer rule.
(Transfer rule) : List up Taking-combination $(s(2), \ldots, s(j), \ldots, s(J))$ of $CoreS$ which satisfy the condition $s(j) \geq 1$. Then $C = \{c \in cl(HP) \mid$ Taking-combination of $c = (s(2), \ldots, s(j) - 1, \ldots, s(J))$.
By this rule, $Core\hat{T}$ is obtainable from $CoreS$. (See the following Example.)
Remark. We see $V(1, B)$'s are Full-case for B with { 1, 2, 3, 5, 7, 10, 13, 15, 21, 22, 30, 33, 37, 42, 57, 58, 70, 105 }.

2-4. (Example) : We give an Example to clarify these Assertions.
Example 2.4.1. $V(1, 105)$: Here $D = 420$ and $G = \{1, 109, 121, 169, 289, 361\}$. We have $m = 1$. Namely $G = M$ and $R = Q(420; G)$. Under some caluculations, we have the following $Q(2) - Q(8)$:
$Q(2) = (11; \sim)$, $Q(3) = (13; \sim)$, $Q(4) = (19; \sim)$, $Q(5) = (41; \sim)$, $Q(6) = (43; \sim)$, $Q(7) = (47; \sim)$, $Q(8) = (53; \sim)$.

On the other hand we obtain the following $(\star)$-rule:
{2,3} = 7, {2,4} = 5, {2,5} = 4, {2,6} = 8, {2,7} = 3, {2,8} = 6, {3,4} = 6,
{3,5} = 8, {3,6} = 4, {3,7} = 2, {3.8} = 5, {4,5} = 2, {4,6} = 3, {4,7} = 8,
{4,8} = 7, {5,6} = 7, {5,7} = 6, {5,8} = 3, {6,7} = 5, {6,8} = 2, {7,8} = 4.

($CoreS$) Thus $CoreS$ consists of
(1) $\{s^2 \mid s \in Q(j)\}(2 \leq j \leq 8)$.
(2) $\{stu \mid s \in Q(i), t \in Q(j), u \in Q(k)\}$ where $(i, j, k) = (2,3,7), (2,4,5), (2,6,8), (3,4,6), (3,5,8), (4,7,8), (5,6,7)$
(3) $\{stuv \mid s \in Q(i), t \in Q(j), u \in Q(k), v \in Q(l)\}$ with $(i, j, k, l) = (2,3,4,8), (2,3,5,6), (2,4,6,7), (2,5,7,8), (3,4,5,7), (3,6,7,8), (4,5,6,8)$.

For $Core\hat{T}$, note that $(2) \Rightarrow Q(8)$, $(3) \Rightarrow Q(7)$, $(5) \Rightarrow Q(5)$, $(7) \Rightarrow Q(6)$, $(6) \Rightarrow Q(4)$, $(10) \Rightarrow Q(3)$, $(14) \Rightarrow Q(2)$, $(15) \Rightarrow Q(6)$, $(21) \Rightarrow Q(5)$, $(35) \Rightarrow Q(7)$, $(30) \Rightarrow Q(2)$, $(42) \Rightarrow Q(3)$, $(70) \Rightarrow Q(4)$.
Thus we get $Core\hat{T}$ by Assertion 2.3.4. For example, $Core((2))$ is $2Q(8)$, $2Q(2)Q(6)$, $2Q(3)Q(5)$, $2Q(4)Q(7)$, $2Q(2)Q(3)Q(4)$, $2Q(2)Q(5)Q(7)$, $2Q(3)Q(6)Q(7)$, $2Q(4)Q(5)Q(6)$.

2-5. (τ-separation, h-separtion)
The situation is much more complicated for NF-case. First we introduce two $\sim$ classifications.

(τ-separation) Let $M(\tau) = Q(D; M) \setminus R$. We take y_1 the smallest member of $M(\tau)$. We put $(y_1; \sim) = \{y_1\} \cup \{y \in M(\tau) \mid y_1 y \in V\}$. We denote $M(\tau_1) = (y_1; \sim)$. If $M(\tau_1) = M(\tau)$, the process stops. And if $M(\tau) \setminus M(\tau_1) \neq \emptyset$, we take the smallest member y_2 of $M(\tau) \setminus M(\tau_1)$. And make $(y_2; \sim) = \{y \in M(\tau) \setminus M(\tau_1) \mid y_2 y \in V\} \cup \{y_2\}$. We put $M(\tau_2) = (y_2; \sim)$. If $M(\tau) \setminus (M(\tau_1) \cup M(\tau_2)) \neq \emptyset$, we continue the process taking y_3. Thus finally we obtain $\sim$ classification of $M(\tau)$.

Assertion 2.5.1. By $\sim$ classification of $M(\tau)$, we obtain a finite classification $M(\tau) = \cup_{k=1}^{K} M(\tau_k)$ where $M(\tau_k) = (y_k; \sim)$ with $1 \leq k \leq K$.

We denote $t \sim u$ for $t, u \in N$, if $tu \in V$. About τ-separation, there are two types. Namely if $y_k \sim y_k$, we say $M(\tau_k)$ to be square type, and denote $M(\tau_k)$ (sqr). And $M(\tau_k)$ is said to be different type if $y_k \not\sim y_k$. For that, we write $M(\tau_k)$(dif).

Assertion 2.5.2. If $M(\tau_k)$ is of square type, $y \sim y$ for all $y \in M(\tau_k)$. The same property holds for $M(\tau_k)$ of different type.

Remarks : (1) The differece between (sqr) and (dif) is serious.
(2) Numerical examples of $K = 1, 2, 3, 4$ are obtained. We think the value K to be unbounded.

(h-separation) We operate $\sim$ clasification for each $Q(j)$. We call this operation as h-separation. Many numerical examples suggest that h-separation separates $Q(j)$ into at most two sets.

Assertion 2.5.3. Each $Q(j)$ separates at most two sets. In h-separate case, we denote them $Q(j; \sigma) = (x_j; \sim)$ and $Q(j; \tau) = (x_j(\tau); \sim)$.

Remarks : (1) There appears (sqr) and (dif) in h-separation.
(2) In case $B = 231 = 3.7.11$, all $Q(2), Q(3), Q(4)$ have h-separation.

2-6. (DMH-decomposition, Lifting Principle)
We call $Q(M(\tau_k)$ with $1 \leq k \leq K$ M-Cells. And $Q(j)$ with no separation and $Q(j; \sigma), Q(j; \tau)$ of h-separate case for $2 \leq j \leq J$ are called H-Cells. We use Y as a general name of a Cell. And we use ω as a general name of $y_k, x_j, x_j(\tau)$.

Assertion 2.6.1. (DMH decomposition) Let $v \in Core(V \setminus R)$. Then $v = dmh$ with $d \in cl(DP)$, $m \in cl(MP)$, $h \in cl(HP)$.

(Taking combination) As for mh, m is a product of primes taken from $M(\tau_k)(1 \leq k \leq K)$. Taking ways are ($\emptyset$), (one), ($\forall$ two), (different two), ($\forall$ three), (t^4), (t^6) etc.
A similar property hold for h. Collecting those taking-ways, we get Taking-combination of mh.

Assertion 2.6.2. (Lifting Principle) All mh with the same Taking-combination are $\in V$ or $\notin V$ simultaneously.

For NF-case, we have no theoretical method to find all Taking-combination of $CoreS$. To study $Core\hat{T}$ we define as follows:
Let $Y = (\omega; \sim)$. Take $u \in U$. We define $(u) \Rightarrow Y$ if $u\omega \in V$. In some cases, Transfer rule works to obtain $Core((u))$.
We give five numerical Examples which suggest the complexity of the nature of $CoreS$ and $Core\hat{T}$.

2-7. (Numerical Examples)

Example 2.7.1. $V(1,11)$: We see $D=44$, $m=2$, $G=\{1,5,9,25,37\}$ and $M=G\cup 3G$, and $R=\{47,53,103,163,199,257,269\ldots\}$. We put $M(\tau)=Q(44;M)\setminus R$. We have $M(\tau)=\{3,5,23,31,37,59,67,71\ldots\}$. $M(\tau)$ does not separates. Some caluculation show that $CoreS$ consists of (1) $\{st \mid s,t\in M(\tau), s\neq t\}$, (2) $\{stu \mid s,t,u\in M(\tau)\}$.

With respect to T, $T(0)=\emptyset$. And we see $Core\hat{T}=4M(\tau)\cup\{4t^2 \mid t\in M(\tau)\}$.

Example 2.7.2. $V(1,47)$: Then $D=188$. We see $J=1$, and $|M|=46$. In this case, $M(\tau)$ separates to two Cells. $M(\tau_1)=(3;\sim)$ and $M(\tau_2)=(7;\sim)$. We denote each as $M(I)$ and $M(2)$.

Some calculations show that $CoreS$ consists of

(1) $\{st \mid s,t\in M(k), s\neq t\}$ for $k=1,2$, (2) $\{t^5 \mid t\in M(k)$ for $k=1,2$, (3) $\{stu \mid s,t\in M(1), u\in M(2)\}$, (4) $\{stu \mid s\in M(1), t,u\in M(2)\}$, (5) $\{stuv \mid s,t,u\in M(1), v\in M(2)\}$, (6) $\{stuv \mid s\in M(1), t,u,v\in M(2)\}$.

We see $CoreT(0)$=128. $Core\hat{T}$ consists of (1) $8M(2)$, (2) $\{8tu \mid t,u\in M(1)\}$,
(3) $\{8tu \mid t\in M(1), u\in M(2)\}$, (4) $\{8tuv \mid t.u,v\in M(1)\}$,
(5) $16M(1)$, (6) $\{16st \mid s,t\in M(1), s\neq t\}$, (7) $\{16st \mid s\in M(1), t\in M(2)\}$, (8) $\{16st \mid s,t\in M(2)\}$, (9) $\{16stu \mid s,t,u\in M(1), s,t,u$ all differs$\}$, (10) $\{16t^4 \mid t\in M(1)\}$, (11) $32M(1)$, (12) $\{32st \mid s,t\in M(2)\}$, (13) $\{64s \mid s\in M(2)\}$, (14) $\{64t^2 \mid t\in M(1)\}$.

(The complexity of T seems to become from the fact that $\boldsymbol{H}(43)=\{47,\ 48=2^43,\ 51=3.17,\ 58=2.29,\ldots\}$.)

Example 2.7.3, $V(1,17)$: Here $M(\tau)$ and $Q(2)$ do not separates.

$CoreS$ cnsists of (1) $\{st \mid s,t\in M(\tau)\}$, (2) $\{st \mid s,t\in Q(2), s\neq t\}$, (3) $\{t^4 \mid t\in Q(2)\}$, (4) $\{stu \mid s\in M(\tau), t,u\in Q(2)\}$.

And we see $Core\hat{T}$ consists of $2M(\tau)$ and $\{2tu \mid t,u\in Q(2)\}$.

Example 2.7.4. $V(1,65)$: Here we have five Cells, namely $M(\tau)=(29;\sim)$, $Q(2)=(3;\sim)$, $Q(3)=(11;\sim)$, $Q(4;\sigma)=(37;\sim)$ and $Q(4,\tau)=(97;\sim)$. (For simplicity, we denote $M(\tau)$ as M, $Q(4;\sigma)$ as $Q(\sigma)$ and $Q(4;\tau)$ as $Q(\tau)$.)

$CoreS$ consists of the following sets :(1) $\{st \mid s,t\in Q(j), s\neq t\}$ for $j=1,2$. (2) $\{t^4 \mid t\in Q(j)\}$ for $j=1,2$. (3) $\{st \mid s,t\in Q(\sigma)\}$, (4) $\{st \mid s,t\in Q(\tau)\}$, (5) $\{stu \mid s\in Q(2), t\in Q(3), u\in Q(4)\}$, (6) $\{t^2u^2 \mid t\in Q(2), u\in Q(3)\}$, (7) $\{stuv \mid s,t\in Q(j), u\in Q(\sigma), v\in Q(\tau)\}$ for $j=2,3.$, (8) $\{st \mid s,t\in M\}$, (9) $\{stu \mid s\in M, t,u\in Q(j)\}$ for $j=2,3.$, (10) $\{stu \mid s\in M, t\in Q(\sigma), u\in Q(\sigma)\}$ (11) $\{stuv \mid s\in M, t\in Q(2), u\in Q(3), v\in Q(4)\}$.

Core T are given by Transfer rule. Note that (2) $\Rightarrow Q(\sigma)$, (5) $\Rightarrow Q(\tau)$, (13) $\Rightarrow Q(\tau)$, (10) $\Rightarrow M$, and (26) $\Rightarrow M$.

Example 2.7.5. V(1,41) : We have four Cell's. They are $M(\tau_1)$, $M(\tau_2)$, $Q(2;\sigma)$, and $Q(2;\tau)$. (We write them as $M(1), M(2), Q(\sigma), Q(\tau)$.)

$CoreS$ consists of the following sets : (1) $\{st \mid s,t\in M(1), s\neq t\}$, (2) $\{t^4 \mid t\in M(1)\}$, (3) $\{st \mid s,t\in M(2)\}$, (4) $\{st \mid s,t\in Q(\sigma), s\neq t\}$, (5) $\{st \mid s,t\in Q(\tau), s\neq t\}$, (6) $\{stu \mid s,t\in M(1), u\in M(2)\}$, (7) $\{stuv \mid s,t,u\in Q(\sigma), v\in Q(\tau)\}$, (8) $\{stuv \mid s\in Q(\sigma), t,u,v\in Q(\tau)\}$, (9) $\{t^2u^2 \mid t\in Q(\sigma), u\in Q(\tau)\}$, (10) $\{stu \mid s\in M(1), t,u\in Q(2)\}$, (11) $\{stuv \mid s,t\in M(1), u\in Q(\sigma), v\in Q(\tau)\}$, (12) $\{stu \mid s\in M(2), t\in Q\sigma), u\in Q(\tau)\}$, (13) $\{stuvw \mid s\in M(2), t,u,\in Q(\sigma), v,w\in Q(\tau)\}$, (14) $\{stuvw \mid s\in M(2), t,u,v,w\in Q(\sigma)\}$, (15) $\{stuvw \mid s\in M(2), t,u,v,w\in Q(\tau)\}$, (16) $\{stuv \mid s\in M(1), t\in M(2), u,v\in Q(2)\}$.

$Core\hat{T}$ is given easily by noting the fact $(2) \Rightarrow M(2)$.

2-8 (Concluding Remarks)
1. For $V(1,71)$ we have $K=3$. And for $V(1,59), V(1,83), V(1,107)$, we have $K=4$.

2. Note the followng facts :
(1) $\boldsymbol{H}(71) = \{71,\ 72 = 2^3 3^2,\ 75 = 3.5^2,\ 80 = 2^4 5, \dots\}$,
(2) $\boldsymbol{H}(59) = \{59,\ 60 = 2^2 5,\ 63 = 3^2 7,\ 68 = 2^2 17, \dots\}$,
(3) $\boldsymbol{H}(83) = \{83,\ 84 = 2^2 37,\ 87 = 3.29,\ 92 = 2^2 23, \dots\}$,
(4) $\boldsymbol{H}(107) = \{107,\ 108 = 2^2 3^3,\ 111 = 3.37,\ 116 = 2^2 29, \dots\}$.
It seems plausible that the nature of Head system controles $V(1,B)$.

3. $V(1,231)$ have six H-Cells. They are $Q(2;\sigma) = (5;\sim),\ Q(2;\tau) = (89;\sim),\ Q(3;\sigma) = (13;\sim),\ Q(3;\tau) = (61;\sim),\ Q(4;\sigma) = (29;\sim),\ Q(4;\tau) = (197;\sim)$.
Note the fact: $\boldsymbol{H}(231) = \{231 = 3.7.11,\ 232 = 2^3 29,\ 235 = 5.47,\ 240 = 2^4 3.5,\ 247 = 13.19,\ 256\ \in T(0), \dots\}$.

3. RDS-Problem

3-1 (History, RDS-Problem)
1. Ramanujan [7] determined all (a,b,c,d) for which $\bar{W}(ax^2+by^2+cz^2+du^2) = \emptyset$. He treated in $\bar{N}$-frame. To indicate that, we use notations with a bar. He commented in the paper that " $\bar{W}(x^2+y^2+10z^2)$ is composed of $\bar{W}$(even) and $\bar{W}$(odd). Here $\bar{W}$(even) $= \{4^\lambda(16\mu+6)\}$ where λ and μ run through $\bar{N}$. On the other hand, $\bar{W}$(odd) is $\{3,7,21,33,43,67,79,87,133,217,219,223,253,307,391\dots\}$. And this set does not seem to obey any simple law."

2. Duke, Schulze-Pillot [3] proved that $|\bar{W}(\text{odd})|$ is finite. It is notable that their bound is non-effective.

3. After these forrunners, we call $W(2,3)$-Problem RDS-Problem. In treating it, we take the standpoints (A), (B) and (C).

4. We take (a,b,c) whose GCD $= 1$. Let $a = A\alpha^2, b = B\beta^2, c = C\gamma^2$ where A,B,C are square free.

5. For $W(A,B,C)$, we introduce the following numbers : $\Delta = ABC$.
Let $P(0) = \{p \mid p \text{ prime},\ p|\Delta\ \}$. We put $P(-1) = P(0) \setminus \{2\}$ and $P(1) = P(0) \cup \{2\}$.

6. (primitive) We say (A,B,C) to be primitive if all $p \in P(0)$ divides only one of A,B,C.

7. ((λ,μ)-sets) We put $T = \{(16),(8),(q)$ odd primes$\}$. For $(t) \in T$, we define the following sets, by letting λ,μ run through $\bar{N}$:
(a) $(\lambda,\mu)(16) = 4^\lambda(16\mu+2u)$ where $u \in \{1,3,5,7\}$.
(b) $(\lambda,\mu)(8) = 4^\lambda(8\mu+u)$ where $u \in \{1,3,5,7\}$.
(c) $(\lambda,\mu)(q) = q^{2\lambda}(q^2\mu+qR)$ or $q^{2\lambda}(q^2\mu+qS)$ where R means the quadratic residues modulo q, and S means the non-residues.

3-2. ($F(0)$-criterion, $W(\star)$)
In the folowing we consider only $W(A,B,C)$ of primitive type. We put $F(0) = \{(t) \in T \mid (\lambda,\mu)(t)\ \subset W(A,B,C)\ \}$. Then we have a good criterion to determine the set $F(0)$.

Proposition 3.2.1. ($F(0)$-criterion) Let $W(A,B,C)$ be primitive. For $(t) \in T$, we have following Criterion for $(t) \in F(0)$.

(1) $(8) \in F(0)$ if and only if $(A,B,C) \equiv (1,1,1) \pmod 4$ or $\equiv (3,3,3) \pmod 4$. And corresponding u is determined as follows :

$u = 1$ for $(A,B,C) \equiv (3,3,7) \pmod 8$ or $\equiv (7,7,7) \pmod 8$,
$u = 3$ for $(A,B,C) \equiv (1,1,5) \pmod 8$ or $\equiv (5,5,5) \pmod 8$,
$u = 5$ for $(A,B,C) \equiv (3,3,3) \pmod 8$ or $\equiv (3,7,7) \pmod 8$,
$u = 7$ for $(A,B,C) \equiv (1,1,1) \pmod 8$ or $\equiv (1,5,5) \pmod 8$.

(2) To $(16) \in F(0)$, it is necessary that one of A,B,C is even. We put $C = 2\hat{C}$. Then $(16) \in F(0)$ if and only if $(A,B,\hat{C}) \pmod 8$ is contained in the following Table.

(a) $u = 1$ for (3,3,3), (7,7,3), (5,7,5), (1,3,5), (1,5,3),
(b) $u = 3$ for (5,5,5), (1,1,5), (5,7,7), (1,3,7), (3,7,1),
(c) $u = 5$ for (7,7,7), (3,3,7), (1,3,1), (1,5,7), (5,7,1),
(d) $u = 7$ for (1,1,1), (5,5,1), (1,3,3), (3,7,5), (5,7,3).

(3) To $(q) \in F(0)$, it is necessary that one of A,B,C is a multiple of q. We put $C = q\hat{C}$. Then $(q) \in F(0)$ if and only if

$(A/q) = -(B/q)$ for $q \equiv 1 \pmod 4$ and $(A/q) = (B/q)$ for $q \equiv 3 \pmod 4$.

(Here $(/)$ means Legendre symbol)

We choose R if $\hat{C} \in S$, and choose S if $\hat{C} \in R$.

Proposition 3.2.2. We put $|F(0)| = \rho$. Then ρ is an odd number.

We define $W(\mathrm{Tr}) = \cup\,(\lambda,\mu)(t)$ with $(t) \in F(0)$. And we put $W(\star) = W \setminus W(\mathrm{Tr})$. Thus RDS-Problem for primitive (A,B,C) is reduced to clarify the structure of $W(\star)$.

3-3. (FGH decomposition)

We define the following set.

(1) Let $\Psi(D) = \{$prime factors of $d-1$ or of $d+1$ where d runs through $d|D\,\} \setminus P(1)$.

(2) Let H consist of the following three kinds of numbers.

(a) A prime number p (called p-type),
(b) product pq of two different primes (called pq-type),
(c) p^2 with a prime p (called square-type).

(N.B. Here p,q are taken so that $\notin P(1) \cup \Psi(D)$.)

Assertion 3.3.1. (FGH conjecture) All $w \in W(\star)$ has the decomposition $w = fgh$ where $f \in cl(P(1)$, $g \in cl(\Psi(D))$ and $h \in H$.

The reason of this conjecture is in the dark. In partuclar, the definitions of $\Psi(D)$ and H are curious. But enormous Numerical Research supports this Assertion. Note the analogous flavour to DMH decomposition. To illustrate properties of $W(\star)$, we give here three Examples.

3-4. (Examples)

Before stating we explain some Notations.

1.(critical order λ_0) Let $r \in N$. For $w \in W$ with $r^2 \nmid w$, we put $\lambda_0 = \mathrm{Max}\{r^{2\lambda} w \in W\}$. We call λ_0 the r^2-critical order of w.

2,($r^2(\infty)$-proprty) We say W satifies $r^2(\infty)$-property in case $r^2 w \in W$ for all $w \in W$.

If $(8) \in F(0)$, Then W stisfies $4(\infty)$-property. And if $(q) \in F(0)$, W satisfies $q^2(\infty)$-property. On the other hand, in case $(16) \in F(0)$, 4-critical order of $w \in W$ takes various value. Thus in Example 3.4.2., 3.4.3, we write 4-critical order of $w \in W(\star)$ as $w((\lambda_0))$.

Example 3.4.1. $W(1,1,13) : F(0) = 8$. $W(\mathrm{Tr}) = 4^{\lambda}(8\mu + 3)$. We see $W(\star) = K_1 \cup K_2$, where $K_1 = 4^{\lambda}C_1$ with

C_1 : 1, 5, 7, 3^2, 13, 17, 5^2, 29, 37, 41, 7^2, 5.11, 61, 73, 79, $3^2$11, 101, 109, 11^2, 7.19, 5.29, 181, 229, 241, 271, 17^2, 337, 439, $3^2$61, 19.31, 7.103, 769.

$K_2 = 4^{\lambda}(2C_2)$, with

C_2 : 1, 3, 5, 7, 11, 17, 23, 41, $3^2 5^2$, 47, 53, 59, 5^3, 167, 317, 353.

Example 3.4.2. $W(1,1,10)$: $F(0) = (16)$. $W(\mathrm{Tr}) = 4^{\lambda}(16\mu + 6)$. We see $W(\star) = K_1 \cup K_2$, where $K_1 = C_1$ with

C_1 : 1((∞)), 3, 5, 7, 3^2, 11, 13((∞)), 17, 19((∞)), 3.7, 5^2, 29, 31, 3.11, 37, 41, 43, 7^2, 59, 61, 67, 73, 79, 3.29, 89, 7.13, 97, 109, $3^2$13, 11^2, 7.19, 139, 5.29, 7.23, 13^2, $3^2$19, 181, 211, 7.31, 3.73, 223, 229, 241, 11.23, 17^2, 293, 307, $5^2$13, 337, 349, 19^2, $3^2$41, 17.23, 11.41, 13.3 577, 613, 661, 7.97, 13.53, 7.103, 739, 829, 877, 7.127, 23.47, 1171, 1249, 1321, 1993, 2089, 2719, 3001.

We have $K_2 = 4^{\lambda}(2C_2)$ with

C_2 : 1, 5, 7, 13, 17, 23, 47, 53, 7.11, 11.13 7.41.

Example 3.4.3 $W(1,3,5) : (F(0) = (5)$. $W(\mathrm{Tr}) = 25^{\lambda_1}(25\mu + 10) \cup 25^{\lambda_2}(25\mu + 15)$. $W(\star) = 25^{\lambda_1}K_1 \cup 25^{\lambda_2}K_2 \cup 25^{\lambda_3}K_3 \cup 25^{\lambda_4}K_4$. Here $K_1 = C_1$ where

C_1 : 1((2)), 3, 7((1)), 11, 13, 19, 23, 29, 31, 37, 43, 47, 67, 71, 79, 7.13((1)), 103, 107, 127, 7.19, 139, 151, 163, 179, 181, 7.41, 17.19, 367, 443, 499, 571, 631, 19.73.

$K_2 = 2C_2$ with

C_2 : 1((1)), 3, 7, 11, 17, 19, 23, 37, 43, $3^2$7, 79, 83, 149, 167, 347.

$K_3 = 5C_3$ with

C_3 : 1((2)), 3^2, 11, 19, 31, 41, 7^2, 59, 79, 7.13, 7.17, 139, 151, 271, 311, 439, 499, 631, 691.

Finally $K_4 = 10C_4$ with

C_4 : 3, 7, 13, 17((1)), 23, 3^3, 43, 47, $3^2$7, 67, 83, 3.29, 107, 173, 179, 7.31, 263, 307, 367, 443, 887.

4. W(3,4)-Problem

4-1. (Mysterious property A)

The structure of $W(3,4)$ lies completely in the dark. But we propose here a bold conjecture. We denote $W(ax^3 + by^3 + cz^3 + dw^3)$ as $W(a,b,c,d)$, or W. $\| W \|$ denotes Max W. W has the following two mysterious properties.

(A) All the members of W are products of no, one or two large primes and small factors.

1. Deshoullier et. al. [2] found $7373170279850 = 2.5^2 18521.7961957$ is in $W(1,1,1,1)$. And Bohman- Fröberg [1] gave two numbers
$400000468109 = 11.59.787.$ 783143 and $400000802954 = 2.47.613.6941807$ are in $W(1,1,1,1)$.

2. The following 5 numbers seem to be the largest 5 members of $W(1,2,3,4)$.

$42532 = 2^2 7^3 31$, $45813 = 3.15271$, $56544 = 2^5 3.19.31$, $132244 = 2^2 7.4723$, and $260448 = 2^5 3.2713$. (T. Matsui [4]).

3. The following 5 numbers seem to be the largest 5 members of $W(1,1,2,2)$ (cf. [4]).

$17050452 = 2^2 3.23.163.379$, $17120244 = 2^2 3.83.17189$, $18022060 = 2^2 5.916103$,
$18987387 = 3.41.154369$, $25872330 = 2.3.5.11.78401$.

4-2. (Mysterious property B)
Observing Matsui's Table [4] of $\| W(a,b,c,d) \|$ for $(k,m) = (3,4)$ it seems plausible that they are classified into the following three types.

Type I. $\| W \|$ is of order 10^6, for $(a,b,c,d) = (1,1,2,d); d = 3,4,5,6$, $(1,1,2,d); d =$ 3, 4, (1,1,2,6), $(1,2,3,d); d = 3,4,5,6,7,9$, (1,2,4,5), (1,3,4,6), (2,3,4,5) etc.

Type II. $\| W \|$ is of order 10^{10}, for $(a,b,c,d) = (1,1,1,d); d = 2,3,4$, (1,1,2,2), (1,1,2,7), (1,1,2,9), (1,1,3,3), (1,1,4,4), (1,2,2,2), (1,3,3,6), (2,2,3,3), (2,3,3,6) etc.

Type Ⅲ. $\| W \|$ is of order 10^{13}, for $(a,b,c,d) =$ (1,1,1,1), (1,1,1,7), (1,2,7,7), (1,2,13,13), (1,3,3,3), (1,5,5,5), (2,3,3,3) etc.
(B) The differences of their magnitude are very mysterious.

4-3. (A bold conjecture)
Property A, B are very curious ones. As a explanation of them, we propose the following conjecture.
(Definition of Outer Form) Take (a,b,c,d). We decompose $a = A\alpha^3, b = B\beta^3, c = C\gamma^3, d = D\delta^3$ where A,B,C,D are 3-power free. We make the following four forms.
$Ax^3 + By^3 + Cz^3 / GCD(A,B,C)$, $\quad Ax^3 + Cz^3 + Dw^3 / GCD(A,C,D)$
$Ax^3 + By^3 + Dw^3 / GCD(A,B,D)$ $\quad By^3 + Cz^3 + Dw^3 / GCD(B,C,D)$.
We call them Outer Forms of $W(a,b,c,d)$.

Here we try to explain (A), (B) using this concept.
Step 1. For $(k,m) = (3,4)$, we classify Outer Forms into three kinds.
(The criterion for classification is yet not clear. Thus we suggest it by showing numerical examples.)
type 1. (1,2,3) type : $(1,2,c); c = 3,4,5,6$, (1,3,4), (2,3,4), (2,3,5) etc.
type 2. (1,1,2) type : $(1,1,c); c = 2,3,4,5,6$, (1,2,2), (1,3,6), (2,2,3) (2,3,6) etc.
type 3. (1,1,1) type : (1,1,1), (1,1,7), (1,2,7), (1,2,13), $(1,b,b); b = 3,5,7$, (2,3,3) etc.

For $W(a,b,c,d)$, we classify Type I - Ⅲ by the following rule:
(Rule) We observe the four Outer Forms of $W(a,b,c,d)$. Then
(a) If there exist Outer Form of type 1, (a,b,c,d) is of Type I,
(b) If there exist Outer Form of type 2, and no form of type 1, (a,b,c,d) is of Type II,
(c) If all the four Outer Forms are type 3, (a,b,c,d) is of Type Ⅲ.

Now a bold conjecture is
TTC (Three type conjecture).
(a) If $W(a,b,c,d)$ is of Type I, $\| W \| = 10^6 \mu(a,b,c,d)$,
(b) If $W(a,b,c,d)$ is of Type II, $\| W \| = 10^{10} \mu(a,b,c,d)$
(c) If $W(a,b,c,d)$ is of Type Ⅲ, $\| W \| = 10^{13} \mu(a,b,c,d)$
Here the value of $\mu(a,b,c,d)$ remains within a reasonable range.

Remarks: TTC is a bold one. But it explains (B). And for (A), Examples given above suggest that the differences of Types induce differences of natures of large divisors.
(2) Classification theory which has a similar fravour works in F-Problem of 4 variables.

References

[1] J. Bohman and C. E. Fröberg, Numerical investigation of Waring's problem for cubes, BIT, 21 (1981), 118-122.

[2] J.M.Deshouillers, F. Hennecart and B.Landreau, 7373170279850, Math. Comp. 229 (1999), 421-439.

[3] 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.

[4] T.Matsui, A note on computing $W(3,4)$ sets. Proceedings of AC2007, $http://tnt.math.metro-u.ac.jp$

[5] R.Morikawa, Search of mathematical structures using a computer, Proceedings AC 2005, $ftp://tnt.math.metro-u.ac.jp$

[6] R.Morikawa, Some concepts and methods to investigate problems of Waring type , Proceedings of AC 2007, $http://tnt.math.metro-u.ac$

[7] S.Ramanujan, On the expression of a number in the form $ax^2+by^2+cz^2+du^2$, Collected papers (Chelsea).

3-8-22-4,Nihonmatsu, Sagamihara 229-1137 Japan
E-mail address: rmorikawa@muj.biglobe.ne.jp

$\sqrt{2}$ 乗法をもつ曲線とHumbertのモジュラー方程式の一般化について

酒井 祐貴子 (早稲田大学　基幹理工学研究科)

1　はじめに

代数曲線 X に対し, $\mathrm{End}_{\mathbb{C}}(\mathrm{Jac}(X))$ が判別式 Δ の実二次体の整数環を含むとき, X は 判別式 Δ の実乗法をもつという. $\mathbb{Q}$ 上のアーベル多様体 A は $E := \mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ が $[E : \mathbb{Q}] = \dim(A)$ を満たす可換体となるとき特に GL_2-type というが, 実乗法をもつ超楕円曲線はこの GL_2-type アーベル多様体の一例となっている. GL_2-type のアーベル多様体に関しては, その概念を導入した Ribet と Serre により GL_2 予想という Serre 予想の特別な場合にあたる予想が知られている. GL_2 予想は全ての $\mathbb{Q}$ 上の楕円曲線はモジュラーであるという志村-谷山予想の高次元化としてもとらえられ, 数論幾何学の重要な話題の一つである. 近年, Serre 予想は Khare などにより解決されたが, modularity を使わない GL_2-type のアーベル多様体の具体例はほとんど知られていない. 筆者の取り組みは GL_2-type のアーベル多様体を出来る限り一般的かつ具体的に構成し, GL_2 予想を検証することである.

特に $\Delta = 5, 8$ の実乗法をもつ超楕円曲線については, Humbert [7] によって古典的な射影幾何学の定理である Poncelet の閉形定理 ([1] 参照) と深い関係があることが知られている. また Humbert はその結果として曲線 X を $y^2 = f(x)$:

$$f(x) \;=\; \begin{cases} (x-x_1)\cdots(x-x_5), & \Delta = 5, \\ x(x-x_1)\cdots(x-x_4), & \Delta = 8 \end{cases}$$

と正規化したとき, X が $\Delta = 5, 8$ の実乗法を持つための条件式 (以下, Humbert のモジュラー方程式と呼ぶ.) $H_5(x_1, \ldots, x_5) = 0$, $H_8(x_1, \ldots, x_4) = 0$ をそれぞれ求めている. Humbert はテータ関数やクンマー曲面の理論を使ってそれらを示したが, 筆者は修士論文において, 幾何学を使ったより初等的な方法で $\Delta = 5$ の実乗法をもつ超楕円曲線を構成し, さらに曲線上の代数対応が引き起こす写像が, $\mathrm{End}_{\mathbb{C}}(\mathrm{Jac}(X))$ において判別式 $\Delta = 5$ の実二次体の整数環となることを示した. またその応用として, $y^2 = (6\text{次式})$ で定義される曲線に対し, Humbert の条件式の一般化と言える, より一般的で対称性が見やすい条件式を与えた. その後の橋本喜一朗氏との共同研究で $\Delta = 8$ の場合にも類似の結果が得られている ([5] 参照).

本稿は Poncelet の 5 角形及び 4 角形を用いた, $\Delta = 5, 8$ それぞれの実乗法をもつ超楕円曲線の構成と Humbert のモジュラー方程式の一般化に関する結果の紹介である.

2 Humbert の結果

射影平面 $\mathbb{P}^2(\mathbb{C})$ の双対空間を $(\mathbb{P}^2)^* = \{\mathbb{P}^2$ 内の直線 $\}$, また, $D \subset \mathbb{P}^2$ を 2 次曲線としたとき D^* で D の接線全体の集合を表すことにする. 本稿を通じて, D_0, D_1 は 4 点で交わる射影平面 $\mathbb{P}^2$ 上の相異なる 2 次曲線を表すものとする. D_0 上の点列 $K = (P_1, \ldots, P_{n+1})$ が D_1 に関する Poncelet の折れ線である, とは $P_{i+1} \neq P_{i-1}$ かつ P_i と P_{i+1} を結ぶ直線 P_iP_{i+1} が全て D_1 に接することをいう. 更に $P_1 = P_{n+1}$ のとき K を Poncelet の n 角形という.

Theorem 2.1 (Poncelet, 1822)**.** D_0, D_1 を 4 点で交わる射影平面 $\mathbb{P}^2$ 上の相異なる 2 次曲線, n を 3 以上の整数とする. このとき $P_iP_{i+1} \in {D_1}^*, P_{n+1} = P_1$ $(1 \leq i \leq n)$ をみたす D_0 上の n 個の点列が存在するならば, 任意の $Q_1 \in D_0$ に対し $Q_iQ_{i+1} \in {D_1}^*, Q_{n+1} = Q_1$ をみたす点列 $Q_2, \ldots, Q_{n+1}$ が存在する.

Humbert はテータ関数や Kummer 曲面の理論を用いて Poncelet の多角形と判別式 $\Delta = 5, 8$ の実乗法を持つ種数 2 の曲線との関係を導いた.

Theorem 2.2 (Humbert [7], $\Delta = 5$)**.** $K = (P_0, P_1, \ldots, P_5 = P_0)$ を D_0, D_1 に対する Poncelet の 5 角形とし, P_6 を D_0, D_1 の交点の 1 つとする. このとき, C の 2 重被覆 X でその分岐点がちょうど $\{P_1, \ldots, P_6\}$ となるものは種数 2 の超楕円曲線で, そのヤコビ多様体は $\Delta = 5$ の実乗法をもつ. すなわち $\mathbb{Z}[\frac{1}{2}(-1+\sqrt{5})] \subseteq \mathrm{End}(\mathrm{Jac}X)$ を満たしている.

Theorem 2.3 (Humbert [7], $\Delta = 5$)**.** X を次式で定義される種数 2 の曲線とする:

$$X : y^2 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5). \tag{1}$$

このとき, $\mathrm{Jac}(X)$ が $\Delta = 5$ の実乗法を持つ必要十分条件は $x_1, \ldots, x_5$ の適当な並べ替えに対して等式 $H_5(x_1, \ldots, x_5) = 0$ が成立することである. ただし, H_5 は

$$\begin{aligned} H_5(x_1, \ldots, x_5) = &\left(\sum_{i=0}^{4} \sigma^i\big(x_1^2(x_3 - x_4)(x_2 + x_5)\big)\right)^2 \\ &- 4\left(\sum_{i=0}^{4} \sigma^i\big(x_1^2(x_3 - x_4)\big)\right)\left(\sum_{i=0}^{4} \sigma^i\big(x_1^2x_2x_5(x_3 - x_4)\big)\right), \end{aligned} \tag{2}$$

$\sigma : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto x_5 \mapsto x_1$.

$\Delta = 8$ の場合, Humbert の結果は次のように述べられる.

Theorem 2.4 (Humbert [7], $\Delta = 8$)**.** $K = (P_1, \ldots, P_4)$ を D_0, D_1 に対する Poncelet の 4 角形とし, P_5, P_6 を D_0 と D_1 の交点とする. このとき, D_0 の 2 重被覆 X でその分岐点がちょうど $\{P_1, \ldots, P_6\}$ となるものは種数 2 の曲線で, その Jacobi 多様体は二つの楕円曲線の積に分解する ($\Delta = 4$ の場合) か, $\Delta = 8$ の実乗法を持つ. 後者の場合は $\mathbb{Z}[\sqrt{2}] \subseteq \mathrm{End}(\mathrm{Jac}X)$ となる.

Theorem 2.5 (Humbert [7], $\Delta = 8$)**.** X を次式で定義される種数 2 の曲線とする.

$$X : y^2 = x(x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

このとき, $\mathrm{Jac}(X)$ が $\Delta = 8$ の実乗法を持つ必要十分条件は $x_1, \ldots, x_4$ の適当な並べ替えに対して等式 $H_8(x_1, \ldots, x_4) = 0$ が成立することである. ただし, H_8 は

$$\begin{aligned} H_8(x_1, x_2, x_3, x_4) = 4x_1x_2x_3x_4\Big((x_1 + x_3)(x_2 + x_4) - 2(x_1x_3 + x_2x_4)\Big)^2 \\ - (x_1 - x_3)^2(x_2 - x_4)^2(x_1x_3 + x_2x_4)^2. \end{aligned} \tag{3}$$

3 平面 2 次曲線上の代数対応

実乗法を持つ代数曲線の構成において重要となるのが平面 2 次曲線に対する Poncelet 型の代数対応 T である. $D_0, D_1 \subset \mathbb{P}^2$ を 4 点で交わる 2 次曲線, P を D_0 上の一般の点とすると P から D_1 には 2 本の接線 ℓ, ℓ' が引け, それぞれの D_0 との (P とは異なる) 交点 Q_1, Q_1' が得られる. このようにして $P \mapsto \{Q_1, Q_1'\}$ なる 2 次の代数対応

$$T = \{(P, Q) \in D_0 \times D_0 \mid \ell := PQ \in D_1^*\}$$

が得られる. 最初の問題は, T の定義方程式を具体的に求めることであるが, ここでは簡単のため, D_0 を

$$D_0 : y = x^2 \tag{4}$$

と取り, $D_0 \ni (x, x^2) \mapsto x \in \mathbb{P}^1$ によって D_0 と $\mathbb{P}^1$ を同一視する. もう一方の 2 次曲線 D_1 は一般形

$$D_1 : c_6 + c_4x + c_1x^2 + c_5y + c_3xy + c_2y^2 = 0, \quad c_i \in \mathbb{C} \tag{5}$$

で与えておく. このとき, 上記の代数対応を考えると, D_0 上の一般の位置にある 2 点 $P = (x, x^2)$, $Q = (z, z^2)$ を通る直線が D_1 に接する条件を書き下すことにより次の結果を得る. $\mathbb{P}^2$ における 2 つの 2 次曲線 D_0, D_1 が上式 (4), (5) で与えられるとき, D_0 上の Poncelet 型の代数対応 T の定義方程式は次式で与えられる:

$$A_1(x, z) := a_6 + a_4xz + a_1x^2z^2 + a_5(x + z) + a_2xz(x + z) + a_3(x + z)^2 = 0, \tag{6}$$

$$\begin{aligned} (a_1, a_2, a_3, a_4, a_5, a_6) = (-4c_1c_2 + c_3^2, -2(2c_2c_4 - c_3c_5), c_5^2 - 4c_2c_6 \\ - 2(c_3c_4 - 2c_1c_5), 2(c_4c_5 - 2c_3c_6), c_4^2 - 4c_1c_6). \end{aligned} \tag{7}$$

ここで, $A_1(x, z)$ は x, z の対称式で各変数について 2 次式であることに注意する. また, (7) を逆に解いて $\{a_i\}$ から $\{c_i\}$ を求めるには根号が必要だが, 次の結果は 2 次曲線 D_1 が $A_1(x, z)$ から有理的に決定されることを示している. $c_1, \ldots, c_6$ を独立変数とみなし,

$$\lambda := 8(c_2{c_4}^2 - c_3c_4c_5 + c_1{c_5}^2 - 4c_1c_2c_6 + {c_3}^2c_6)$$

とおく. $\lambda \neq 0$ のとき, $(a_1, \ldots, a_6)$ を (7) で定めると次の恒等式が成立する:

$$\begin{cases} \lambda c_1 = ({a_4}^2 - 4a_1a_6)/2, \\ \lambda c_2 = ({a_2}^2 - 4a_1a_3)/2, \\ \lambda c_3 = a_2a_4 - 2a_1a_5, \\ \lambda c_4 = a_4a_5 - 2a_2a_6, \\ \lambda c_5 = 2a_3a_4 - a_2a_5, \\ \lambda c_6 = ({a_5}^2 - 4a_3a_6)/2. \end{cases} \tag{8}$$

次に上で述べた代数対応 T の合成を考える. $T^2 = T \circ T$ は 4 価の代数対応になるが, 定義よりそのうちの 2 価は恒等写像であり, 残りの 2 価の部分が長さ 2 の Poncelet の折れ線によって得られる点を対応させる代数対応 T_2 を定める. 作図により, T_2 の定義方程式 $A_2(x, z) = 0$ は終結式を用いて

$$A_2(x, z) = \frac{1}{(x-z)^2}\mathrm{Res}_u\Big(A_1(x, u),\ A_1(z, u)\Big)$$

によって与えられる. 右辺の $(x-z)^2$ は恒等写像にあたる部分である. 係数を整理すれば $A_2(x, z)$ は (6) と同様に

$$A_2(x, z) = a'_6 + a'_4xz + a'_1x^2z^2 + a'_5(x+z) + a'_2xz(x+z) + a'_3(x+z)^2$$

と書ける. ここで $a'_1, \ldots, a'_6$ は $a_1, \ldots, a_6$ の 4 次同次式である.

以上の結果を用いると, Poncelet の $4, 5$ 角形に関して次の補題が得られる.

Lemma 3.1. D_0, D_1 に対して Poncelet の 4 角形が得られるための必要十分条件は, 上記の $A_2(x, z)$ が x, z の完全平方式の定数倍になることである：

$$A_2(x, z) = c \cdot B(x, z)^2, \quad c \in \mathbb{C}.$$

Remark 3.2. $B(x, z) = 0$ は D_0 の対合写像

$$(x, x^2) \in D_0 \mapsto (z, z^2) \in D_0$$

を与えている. このとき $z = \overline{x}$ とも記す.

Lemma 3.3. D_0, D_1 に対して Poncelet の 5 角形が得られるための必要十分条件は 上記の $A_1(x, z), A_2(x, z)$ に対し,

$$\frac{1}{(x-z)^2}\mathrm{Res}_u(A_2(u, z), A_2(u, x)) = c' \cdot A_1(x, z), \quad c' \in \mathbb{C}$$

が成り立つことである.

4 種数 2 の曲線と Poncelet 型代数対応の持ち上げ

一般に種数 2 の曲線は超楕円曲線となる．これを射影直線 $\mathbb{P}^1$ の二重被覆とみなすと, ちょうど 6 個の点で分岐する．本研究の基本的アイデアの一つは, $\mathbb{P}^1$ を射影平面上の 2 次曲線 D_0 で置き換え, 前節の結果を種数 2 の曲線と関連付けることである．

まず $\Delta = 5$ の場合の結果について述べる (詳細は [8] 参照)．この場合, 分岐点として D_0 に内接する Poncelet の 5 角形の 5 頂点 $P_1, \dots, P_5$ を選ぶ．残りの 1 個 の分岐点は 2 つの 2 次曲線の交点から選ぶことにする．この時, 曲線の同型類は 4 点の交点のうちどの 1 点を選んでも変わらないことがわかる．この点を P_6 とし, 今後のために

$$P_i = (x_i, x_i^2) \qquad (1 \le i \le 6)$$

と定める．このとき $A_1(x, x_6) = c\ (x-\alpha)^2, A_2(x, x_6) = c'(x-\beta)^2$ をみたす $\alpha, \beta \in \mathbb{C}$ がそれぞれ唯一存在する $(c, c' \in \mathbb{C})$.

以上の設定の下で, 超楕円曲線

$$X : y^2 = f(x) := (x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)(x-x_6) \tag{9}$$

が得られる．更に, X 上の有理関数

$$j(x) := (x-x_6)(x-\alpha)(x-\beta)$$

を考える．このとき次の定理が成り立つ.

Theorem 4.1 ([8], $\Delta = 5$)**.** 写像 $\pi : X \to D_0$ を上記の 2 重被覆写像とするとき, D_0 上の Poncelet 型代数対応 $T = T_1, T_2$ を X 上の 2 次の代数対応 $\hat{T}_1, \hat{T}_2$ に持ち上げることができる．$\hat{T}_i \subset X \times X$ は次のように定まる:

$$\big((x,y),(u,w)\big) \in \hat{T}_i \quad (i=1,2) \quad \overset{\text{def}}{\Longleftrightarrow} \quad j(u)y = j(x)w,\ A_1(x,u) = 0.$$

さらに, $\hat{T}_i$ は $\mathrm{Pic}^0(X)$ の自己準同型写像 ϕ_i を引き起こし, 次式が成立する.

$$\phi_i{}^2 + \phi_i - 1 = 0 \quad (i = 1, 2).$$

一方 $\Delta = 8$ の場合は Poncelet の 4 角形の 4 頂点 $P_1, \dots, P_4$ の他にもう 2 点を選ぶ必要があるが $\Delta = 5$ の場合と違い, $D_0 \cap D_1$ から 2 点を選ぶ際は少々注意が必要である．実際, D_0, D_1 の 4 つの交点 $D_0 \cap D_1 = \{P_5, P_5', P_6, P_6'\}$ は対合 $B(x,z) = 0$ によって 2 点ずつ対になり, $B(x_5, x_5') = 0, B(x_6, x_6') = 0$ をみたすことがわかる．更に $A_1(x, x_5) = c(x-\eta_1)^2, A_1(x, x_6) = c'(x-\eta_2)^2$ をみたす $\eta_1, \eta_2 \in \mathbb{C}$ がそれぞれ唯一決まる．よって $\Delta = 8$ の場合は 6 個の分岐点として, Poncelet の 4 角形の頂点 $P_i (1 \le i \le 4)$ と $P_5, P_6 \in D_0 \cap D_1$ を選ぶことにする．すなわち $B(x_5, x_6) \neq 0$ となるように D_0, D_1 の 2 つの交点を選んで, 種数 2 の曲線を方程式 (9) によって定める．この曲線上への前節の D_0 上の代数対応 T の「持ち上げ」を考える．その際, 鍵になるのが次の補題である．まず P_∞ を $x = \infty$ に対応する D_0 の点とし, P_∞ から D_1 への 2 本の接線が再び D_0 と交わる点を $Q_\infty, \overline{Q_\infty} \in D_0$ とする.

Lemma 4.2 ($\Delta = 8$)**.** 上記の $Q_\infty, \overline{Q_\infty}$ の座標を $Q_\infty = (u_\infty, {u_\infty}^2)$, $\overline{Q_\infty} = (\overline{u_\infty}, \overline{u_\infty}^2)$ とし, X 上の有理関数を

$$j(x) := \frac{(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-\eta_1)(x-\eta_2)}{(x-u_\infty)^3(x-\overline{u_\infty})^3}$$

とおくと, 次が成り立つ.

$$\begin{aligned}&(1)\quad j(\overline{x}) = -j(x),\\ &(2)\quad A_1(u,x_i) = 0\ (i=1,2) \Rightarrow f(x_1)f(x_2) = j(u)^2.\end{aligned}$$

有理関数 $j(x)$ により, $\Delta = 8$ の場合の代数対応 T の「持ち上げ」の存在とその表示式を与えることが可能になる.

Theorem 4.3 ($\Delta = 8$)**.** 超楕円曲線 X を上のように定めるとき, D_0 上の Poncelet 型代数対応 T を X 上の 2 次の代数対応 $\hat{T}$ に持ち上げることができる. $\hat{T} \subset X \times X$ は次のように定まる: $A_1(x,u_i) = 0$ $(i=1,2)$, $B(u_1,u_2) = 0$ とするとき

$$\Big((x,y),(u_i,w_i)\Big) \in \hat{T} \quad (i=1,2) \quad \overset{\text{def}}{\Longleftrightarrow} \quad w_1w_2 = j(x). \tag{10}$$

このとき, $\hat{T}$ は $\mathrm{Pic}^0(X)$ の自己準同型写像 ϕ_i を引き起こし, 次式が成立する:

$$\phi^2 - 2 = 0.$$

最後の関係式は, 以下の様に因子の計算から示される.

$$\begin{aligned}\phi : (u,w) &\mapsto (x_1,y_1) + (x_2,y_2),\\ \phi^2 : (u,w) &\mapsto (u,w) + (\overline{u},\overline{w_1}) + (u,w) + (\overline{u},\overline{w_2})\\ &= (u,w) + (\overline{u},\overline{w_1}) + (u,w) + (\overline{u},-\overline{w_1})\end{aligned}$$

より

$$\begin{aligned}\phi^2 - 2\mathrm{id} : (u,w) &\mapsto (\overline{u},\overline{w_1}) + (\overline{u},-\overline{w_1})\\ &= \mathrm{div}(x-\overline{u})_0 \sim \mathrm{div}(x-\overline{u})_\infty = \mathrm{div}(x)_\infty\end{aligned}$$

となり, これは $\mathrm{Pic}^0(X)$ で $\phi^2 - 2$ がゼロ写像であることを示している.

5 モジュラー方程式の一般化

Humbert のモジュラー方程式 (2) は (1) で定義される曲線が $\Delta = 5$ の実乗法を持つ条件を与えていた. ここでは (9) で定まる曲線に対するモジュラー方程式を与える.

Theorem 5.1 ($\Delta = 5$)**.** (9) で定めた超楕円曲線 X のヤコビ多様体が $\Delta = 5$ の実乗法を持つ条件は $x_1, \dots, x_6$ の適当な並べ替えに対して等式 $H_5'(x_1, \dots, x_6) = 0$ が成立することである. ただし, H_5' は以下のように表示される多項式である.

$$
\begin{aligned}
&H_5'(x_1, \dots, x_6)\\
:=&(x_3-x_4)^2(x_2-x_5)^2(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_1-x_5)(x_6-x_2)(x_6-x_3)(x_6-x_4)(x_6-x_5)\\
&+(x_1-x_3)^2(x_4-x_5)^2(x_2-x_1)(x_2-x_3)(x_2-x_4)(x_2-x_5)(x_6-x_1)(x_6-x_3)(x_6-x_4)(x_6-x_5)\\
&+(x_1-x_5)^2(x_2-x_4)^2(x_3-x_1)(x_3-x_2)(x_3-x_4)(x_3-x_5)(x_6-x_1)(x_6-x_2)(x_6-x_4)(x_6-x_5)\\
&+(x_1-x_2)^2(x_3-x_5)^2(x_4-x_1)(x_4-x_2)(x_4-x_3)(x_4-x_5)(x_6-x_1)(x_6-x_2)(x_6-x_3)(x_6-x_5)\\
&+(x_2-x_3)^2(x_1-x_4)^2(x_5-x_1)(x_5-x_2)(x_5-x_3)(x_5-x_4)(x_6-x_1)(x_6-x_2)(x_6-x_3)(x_6-x_4).
\end{aligned}
$$

更に, $H_5'(x_1, \dots, x_6)$ は $x_1, \dots, x_6$ の置換群の中で $(12)(34)(56), (12345)$ で生成され, S_5 と同型な 6 次可移群の作用で不変である.

[証明の概略]
$K = (P_1, \dots, P_5)$ を Poncelet の 5 角形の頂点, $P_6 \in D_1 \cap D_2$ とすると

$$A_1(x_1, x_2) = A_1(x_2, x_3) = A_1(x_3, x_4) = A_1(x_4, x_5) = A_1(x_5, x_1) = 0$$

が成立する. これを $A_1(x, z)$ の係数 $a_1, \dots, a_6$ の連立 1 次方程式とみなして解き, 分母を払うと $a_1, \dots, a_6$ が次のように表わされる:

$$
\begin{cases}
a_1 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1^2(x_4 - x_3)\big),\\
a_2 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1^2(x_3 - x_4)(x_2 + x_5)\big),\\
a_3 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1 x_2^2 x_3(x_4 - x_5)\big),\\
a_4 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1^2 x_2^2(x_3 - x_5) + x_1^2 x_3^2(x_5 - x_4)\big),\\
a_5 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1^2 x_2^2 x_4(x_5 - x_3) + x_1^2 x_3^2 x_2(x_4 - x_5)\big),\\
a_6 = \displaystyle\sum_{i=0}^{4} \sigma^i\big(x_1^2 x_2^2 x_4^2(x_3 - x_5)\big).
\end{cases}
\tag{11}
$$

ここで, σ は次の位数 5 の巡回置換を表す :

$$x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto x_5 \mapsto x_1.$$

一方, $(x_6, x_6^2) \in D_0 \cap D_1$ であることから次式が成り立つ :

$$c_6 + c_4 x_6 + c_1 x_6^2 + c_5 x_6^2 + c_3 x_6^3 + c_2 x_6^4 = 0.$$

この式に (8) の結果を代入し, 更に (11) を代入すると $x_1,\dots,x_6$ の関係式 $H_5'(x_1,\dots,x_6)=0$ が得られる. これは同次 12 次式, 各 x_i については 4 次式である. さらに次の注目すべき等式が成り立つ：

$$\begin{aligned}
H_5'|_{x_6=x_1} &= \Big((x_1-x_2)(x_1-x_3)(x_1-x_4)(x_3-x_4)(x_1-x_5)(x_2-x_5)\Big)^2,\\
H_5'|_{x_6=x_2} &= \Big((x_1-x_2)(x_1-x_3)(x_2-x_3)(x_2-x_4)(x_2-x_5)(x_4-x_5)\Big)^2,\\
H_5'|_{x_6=x_3} &= \Big((x_1-x_3)(x_2-x_3)(x_2-x_4)(x_3-x_4)(x_1-x_5)(x_3-x_5)\Big)^2,\\
H_5'|_{x_6=x_4} &= \Big((x_1-x_2)(x_1-x_4)(x_2-x_4)(x_3-x_4)(x_3-x_5)(x_4-x_5)\Big)^2,\\
H_5'|_{x_6=x_5} &= \Big((x_2-x_3)(x_1-x_4)(x_1-x_5)(x_2-x_5)(x_3-x_5)(x_4-x_5)\Big)^2.
\end{aligned}$$

これを用いて Lagrange の補間公式を適用すると H_5' は対称性の高い与式のような表示に出来る. □

Remark 5.2. この式で $x_6=\infty$ とすると Humbert の与えたモジュラー方程式 (2) を得ることが出来る. より正確には, 以下の等式が成立する:

$$\Big({x_6}^4 H_5'(x_1,\dots,x_5,1/x_6)\Big)\Big|_{x_6=0} = -H_5(x_1,\dots,x_5).$$

$\Delta=8$ の場合についても, 同様に次の結果が得られる.

Theorem 5.3 ($\Delta=8$)**.** 式 (9) で定めた超楕円曲線 X について X のヤコビ多様体が $\Delta=8$ の実乗法を持つ条件は $x_1,\dots,x_6$ の適当な並べ替えに対して等式 $H_8'(x_1,\dots,x_6)=0$ が成立することである. ただし, H_8' は以下のように表示される多項式である.

$$\begin{aligned}
&H_8'(x_1,\dots,x_6) :=\\
&(x_2-x_4)^2(x_3-x_5)^2(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_1-x_5)(x_6-x_2)(x_6-x_3)(x_6-x_4)(x_6-x_5)\\
+&(x_1-x_3)^2(x_4-x_5)^2(x_2-x_1)(x_2-x_3)(x_2-x_4)(x_2-x_5)(x_6-x_1)(x_6-x_3)(x_6-x_4)(x_6-x_5)\\
+&(x_1-x_5)^2(x_2-x_4)^2(x_3-x_1)(x_3-x_2)(x_3-x_4)(x_3-x_5)(x_6-x_1)(x_6-x_2)(x_6-x_4)(x_6-x_5)\\
+&(x_1-x_3)^2(x_2-x_5)^2(x_4-x_1)(x_4-x_2)(x_4-x_3)(x_4-x_5)(x_6-x_1)(x_6-x_2)(x_6-x_3)(x_6-x_5)\\
+&16(x_1-x_2)(x_2-x_3)(x_1-x_4)(x_3-x_4)(x_1-x_5)(x_2-x_5)(x_3-x_5)(x_4-x_5)(x_1-x_6)(x_2-x_6)\\
&(x_3-x_6)(x_4-x_6).
\end{aligned}$$

$H_8'(x_1,\dots,x_6)$ は $x_1,\dots,x_6$ の置換群の中で $(126)(345),(12)(34)(56),(13)(24)(65)$ で生成される位数 48 の 6 次可移群 $S_4\times C_2$ の作用で不変である.

Remark 5.4. この式で $x_5=0$, $x_6=\infty$ とすると Humbert の与えたモジュラー方程式 (3) が得られる. より正確には, 以下の等式が成立する:

$$\Big({x_6}^4 H_8'(x_1,x_2,x_3,x_4,0,1/x_6)\Big)\Big|_{x_6=0} = -H_8(x_1,x_2,x_3,x_4).$$

参考文献

[1] H. J. M. Bos, C. Kers, F. Oort and D. W. Raven, *Poncelet's closure theorem*, Exposition. Math. **5** (1987), 289–364.

[2] L. Flatto, Chapter 15 by S. Tabachnikov. *Poncelet's theorem*, American Mathematical Society, Providence, RI, 2009

[3] P. Griffiths and J. Harris, *On Cayley's explicit solution to Poncelet's porism*, Enseign. Math. (2), **24** (1978), 31–40.

[4] K. Hashimoto, *The structure of real multiplications connected with algebraic correspondences of algebraic curves of genus* 2, (Japanese), Sūrikaisekikenkyūsho Kōkyūroku (1996), 153–163.

[5] K. Hashimoto and Y. Sakai, *Poncelet's theorem and versal family of curves of genus two with* $\sqrt{2}$*-multiplication* , RIMS Kôkyûroku Bessatsu **B12** (2009), 249–261.

[6] K. Hashimoto and Y. Sakai, *General form of Humbert's modular equation for curves with real multiplication of* $\Delta = 5$, Proc. Japan Acad. Ser. A Math. Sci., **85** (2009), 171–176.

[7] G. Humbert, *Sur les fonctions abeliennes singulieres*, Œuvres de G. Humbert 2, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars, (1936), 297–401.

[8] Y. Sakai, *Poncelet's theorem and hyperelliptic curve with real multiplication of* $\Delta = 5$, J. Ramanujan Math. Soc., **24** (2009), 143–170.

非正則素数の高速計算

谷口 哲也

1. 序

小論では, 非正則素数や非正則対の計算について既存の方法に触れた後, それを受けて計算量を削減するための方向性を述べる.

以下, p で奇素数を表す. Bernoulli 数 B_t は次の形式的巾級数の係数で定義される:

$$\frac{x}{e^x-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n \tag{1}$$

B_1 以外の奇数番目の Bernoulli 数 B_{2n+1} はすべて 0 である. 対 $(p,2t)(0<t<(p-1)/2)$ が非正則であるとは, p が B_{2t} を割り切ることである. p に対する非正則対の個数のことを p の非正則指数とよび $i(p)$ で表す. p が正則であるとは $i(p)=0$ であることをいい, そうでない場合は非正則であるという. p が非正則素数であることと 円分体 $\mathbb{Q}(\zeta_p)$ の類数 h_p を p が割りることは同値である.

非正則素数は無限に多く存在することが示されている. (たとえば Washington[23, p.62]) しかし正則素数の密度が $\exp(-1/2)=0.60653\cdots$ であろうという予想は未解決であり, 無限に多く存在するかどうかも分かっていない. 非正則素数は岩澤不変量とも関連している. 非正則素数の他のいくつかの話題については Ribenboim(吾郷 訳編)[13], [14] を参照されたい.

過去の非正則素数の計算の一覧は Table 1 のとおりである. 谷口 [18] は $p<100000$ の素数と $p-1$ の素因子が 7 以下であるような素数 $p\le 40,824,001$ に対する円分体 $\mathbb{Q}(\zeta_p)$ の相対類数 h_p^- を計算し, h_p^- の p-整除性によって非正則素数を判別した. その結果 $p=40,824,001$ のとき h_p^-(61,384,565 桁) は p で整除されること, すなわちこの p は非正則素数であることを確かめた.

2. 計算方法

非正則対 $(p,2k)$ を求めるためには, Bernoulli 数の分子の p-整除性をみればよい. 方法としては

- Bernoulli 数を表す合同式を用いる方法 ($O(p^2)$)
- 形式的巾級数を用いる方法 ($O(p\log^2 p\log\log p)$)
- 多項式の零点を用いる方法 ($O(p\log^2 p\log\log p)$)

[1]このプレプリントは, 奇しくも AC2009 の講演終了後 (v.1 は 12/10, v.2 は 12/12)arXiv にアップロードされていました. このことは木村巌先生からご教示いただきました.

TABLE 1. 過去の非正則素数計算

範囲	著者
$p < 165$	Kummer
$p < 619$	Vandiver [20]
$p \leq 4,001$	Vandiver, D. H. Lehmer, E. Lehmer, Selfridge, Nicol [11], [15], [21]
$p < 5,500$	Kobelev [9]
$p < 8,000$	Johnson [7]
$p < 10,000$	D. H. Lehmer [10]
$p < 25,000$	Selfridge, Pollack [16]
$p < 30,000$	Johnson [8]
$p < 32,768$	Wada [24]
$p < 125,000$	Wagstaff [22]
$p < 150,000$	Tanner, Wagstaff [19], [6]
$p < 1.0 \times 10^6$	Buhler, Crandall, Sompolski [1]
$p < 4.0 \times 10^6$	Buhler, Crandall, Ernvall, Metsänkylä [3]
$p < 8.0 \times 10^6$	Shokrollahi [17]
$p < 1.2 \times 10^7$	Buhler, Crandall, Ernvall, Metsänkylä [4]
$p < 1.63 \times 10^8$	Buhler, Harvey [2][1]

がある. まずこれらの概要を述べた後, 計算の下支えをしている Newton 法や FFT 乗算, Nussbaumer 法について触れる.

2.1. $B_{2k} \mod p$ の既存の計算方法.

2.1.1. *Bernoulli* 数を表す合同式を用いる方法. 初期の非正則対の計算は, Bernoulli 数 $B_{2k} \mod p$ に関する合同式によって行われた. これらの合同式による非正則対の計算には $O(p^2)$ の計算量が必要である.

基本となる合同式は

$$(b - b^{p-2k})\frac{B_{2k}}{2k} \equiv \sum_{0<s<p} \left\lfloor \frac{bs}{p} \right\rfloor a^{2k-1} \pmod{p}, \quad (p-1) \nmid 2k,\ p \nmid b,\ b \in \mathbb{N}$$

であるが, 右辺の項数は $p-1$ 項もある. より項数の少ない合同式として以下のものなどが知られている.

Proposition 1. $c(x,y,z) = x^{p-2k} + y^{p-2k} - z^{p-2k} - 1$ とおく. 素数 $p > 8$ と $2 \le 2k \le p-3$ に対して次が成り立つ:

(2)
$$c(3,4,6)B_{2k}/4k \equiv \sum_{p/6<s<p/4} s^{2k-1} \pmod p,$$

(3)
$$c(2,3,4)B_{2k}/4k \equiv \sum_{p/4<s<p/3} s^{2k-1} \pmod p,$$

(4)
$$c(4,5,8)B_{2k}/4k \equiv \sum_{p/8<s<p/5} s^{2k-1} + \sum_{3p/8<s<2p/5} s^{2k-1} \pmod p,$$

(5)
$$c(2,5,6)B_{2k}/4k \equiv (2^{2k-1}+1) \sum_{p/6<s<p/5} s^{2k-1} - 2^{2k-1} \sum_{3p/10<s<p/3} s^{2k-1} \pmod p,$$

(6)
$$(2^{2k-1} + 3^{2k-1} + 6^{2k-1} - 1)B_{2k}/4k \equiv \sum_{0<s<p/4} (p-6s)^{2k-1} \pmod{p^2}.$$

(5) は Vandiver[20], (6) は E.Lehmer[12] で示されている. (2), (3) では $p/12$ 項ほど, (4), (5) ではそれぞれ $p/10$ 項, $p/15$ 項ほどの計算で済む. これらに類似した合同式に関連する話題は [14] を参照されたい.

実際に $B_{2k} \mod p$ が 0 になるかどうかの判定は次のように行う. まず (5) の右辺を計算し, 結果が $\mod p$ で 0 にならなかった場合は $(p, 2k)$ は非正則対ではない. 0 なった場合は $c(2,5,6) \mod p$ を求め, この値が 0 でなければ $(p, 2k)$ は非正則対である. もし $c(2,5,6) \equiv 0 \mod p$ になった場合は (2), (3), (4) でなどで再計算する. これらも 0 になる場合は (6) を用いる. Wagstaff[22] はこの方法で $p < 125000$ の非正則対の計算を行い, さらに上記の合同式より項数の少ないものを探索したが発見することができなかった. Tanner ら [19] は $p/18$ 項ほどで $B_{2k} \mod p$ を計算することができる合同式を発見し, $p < 150000$ の範囲の非正則対を求めた.

2.1.2. 形式的巾級数を用いる方法. 1990 年代に入ると形式的巾級数を用いて非正則対を求める手法が登場した.

基本的には Bernoulli 数に関する等式 (1) を用いて素数 p に対する非正則対 (p,t) を求める. そのためには (1) を $\mathbb{F}_p$ 係数で考えて第 $p-1$ 項まで近似計算すればよい. これは $\mathbb{F}_p$ 係数の形式的巾級数

$$\frac{e^x - 1}{x} = \sum_{n=0}^{\infty} \frac{1}{n!} x^{n-1} \tag{7}$$

を $\mod x^{p-1}$ で考え, 逆数近似を Newton 反復で求めることによって実現できる.

この方法の計算量の評価は次のとおりである. まず, (7) から近似計算に必要な多項式を切り出す. その次数は p に比例する. Newton 反復の中の多項式乗算に必要な計算量は $O(p \log p \log\log p)$ である. これは上記多項式の次数が p に比例すること, 多項式の乗算に FFT による高速乗算を用いることで得られる. また, 必要な近似精度を得るのに必要な Newton 反復の回数は $\log p$ に比例する. まとめると, この方法で非正則対を求めるのに必要な計算量は $O(p \log^2 p \log\log p)$ である.

Buhler ら [1] は, $p < 10^6$ の非正則対を求めた. 彼は (7) の逆数近似による (1) の計算をベースとしているが, (1) の代わりに

$$\frac{x^2}{\cosh(x) - 1} = -2 + \sum_{n=0}^{\infty} \frac{(2n-1)B_{2n}}{(2n)!} x^{2n}$$

を用いている. この巾級数の係数には $B_{2n+1}(= 0)$ は現れず B_{2n} のみが現れる. したがって必要な項数も $p/2$ 程度となりメモリの無駄が省け計算の手間も削減される. さらに彼らは "Multisectionning idea" を用いた. これは, 式

$$\frac{x}{\sqrt{2}} \frac{\cosh(x/\sqrt{2})}{\sinh(x\sqrt{2})} = \sum_{n=0}^{\infty} \frac{2^n B_{an}}{(2n)!} x^{2n} = \frac{A_0(x) + A_2)(x) + A_4(x) + A_6(x)}{D(x)}$$

を用いるものである. ただし,

$$A_k(x) = \sum_{n=0}^{\infty} \frac{A_{kn}}{(8n+k+3)!} x^{8n+k}, \quad D(x) = \sum_{n=0}^{\infty} \frac{D_n}{(8n+4)!} x^{8n}$$

であり, A_i, D_i は簡単な漸化式で求められる数である. したがって, この計算では $p/8$ 次程度の多項式 $D(x)$ の逆数近似をすれば十分であり, メモリ使用量のピークをさらに抑えることができる.

Buhler ら [3] では基本的に上記と同じアイデアを用いて計算しているが, 計算範囲の拡大に伴い, 分割数を 8 から 12 へと増加させている.

2.1.3. 多項式の零点を用いる方法. Shokrollahi[17] は 8×10^6 以下の非正則対の計算を発表した. 彼の方法は $B_{2k} \mod p$ の計算を ある 2 つの多項式のネガサイクリックコンボリューションに帰着するものである. 計算量は $O(p \log^2 p \log\log p)$ である.

まず, 用語の定義を述べる.

Definition 2 (サイクリック/ネガサイクリックコンボリューション)**.** 長さ D の 2 つの配列

$$f = (f_0, f_1, \ldots, f_{D-1}), \quad g = (g_0, g_1, \ldots, g_{D-1})$$

に対して, 長さ D の配列 h を

$$h = (h_0, h_1, \ldots, h_{D-1}), \quad h_n = \sum_{i+j \equiv n \mod D} f_i g_j$$

と定義する. h を $f \times g$ で表し, f と g のサイクリックコンボリューションとよぶ. また, 長さ D の配列 k を

$$k = (k_0, k_1, \ldots, k_{D-1}), \quad k_n = \sum_{i+j=n} f_i g_j - \sum_{i+j=D+n} f_i g_j$$

と定義する. k を $f \times_- g$ で表し, f と g のネガサイクリックコンボリューションとよぶ.

p を奇素数とし, $0 < w < p$ を法 p に関する原始根, $1 \le c \le p-1$ を整数とする. 多項式

$$h_c(x) := \sum_{j=0}^{p-2} \left\lfloor \frac{c(w^{-j} \mod p)}{p} \right\rfloor x^k \in F_p[x]$$

について次が成り立つ.

Proposition 3 ([4, Theorem 2.1])**.** 奇素数 p と自然数 $1 \le c \le p-1$, $1 \le k \le p-2$ に対して

$$h_c(w^k) \equiv (c - c^k)\frac{B_{p-k}}{p-k} \mod p.$$

したがって $(p, 2t)$ が非正則対であることと $h_w(w^{p-2t}) = 0$ であることは同値であり, 問題は多項式の零点の計算に帰着された. さらに $\eta(x) = (x-1)h_w(x)/(x^{(p-1)/2} - 1)$ とおくと, $p \neq 2$ より $h_w(w^{p-2t}) = 0$ と $\eta(w^{p-2t}) = 0$ は同値である. よって $(p-1)/2$ 次以下の多項式の零点計算をすれば十分である.

いわゆる Bluesten's trick により, 多項式の零点を求めることは (ネガ) サイクリックコンボリューションの計算に帰着できる. $(p-1)/d$ が偶数となるような d に対して, d 次未満の多項式 $f(x) = \sum_{i<d} f_i x^i \in \mathbb{F}_p(x)$ の零点を $\mathbb{F}_p^\times$ の位数 d の巡回部分群 $\langle u \rangle$ の coset $C = \{\alpha u^i \mid 0 \le j < d\}$ の中から探すためには次のようにすればよい. 多項式 $g(x) \in \mathbb{F}_p[x]$ を

$$g(x) = \sum_{i<d} f_i \alpha^i x^i = \sum_{i<d} g_i x^i$$

とおく. $f(x)$ の C 上の零点を求めるためには $g(x)$ の $\langle u \rangle$ 上の零点を求めれば十分である. さて, $(p-1)/d$ が偶数であるので $u = v^2$ となる $F_p^\times$ の元 v が存在する. v を用いて $g(u^j)$ を次のように変形する:

$$g(u^j) = \sum_i g_i v^{i^2+j^2-(j-i)^2} = v^{j^2} \sum_i v^{-(j-i)^2}.$$

$h_i := g_i v^{i^2}$, $v_i := v^{-i^2}$ とおくと上の最右辺は, d が偶数のときは $(h_i) \times (v_i)$, d が奇数のときは $(h_i) \times_- (v_i)$ で計算することができる.

Buhler ら [4] はこの手法を利用して, 1.2×10^7 以下の非正則素数の計算を行った.

2009 年 12 月 10 日に Buhler らは非正則素数の計算を 1.63×10^8 まで拡張した, という報告を arXiv にアップロードしている [2]. この計算では形式的巾級数による方法と Voronoi の合同式による方法を用いている. 両者の計算量は等しく $O(p \log^{2+\varepsilon} p)$ である.

2.2. 計算を下支えするアルゴリズム.

2.2.1. *Newton* 法. 形式的巾級数 $f \in \mathbb{Z}[[x]]$ の逆数 f^{-1} の近似 g を求めるためには, 以下の方法をとる.

まず, 形式的巾級数の基本的な性質であるが, $f(t) = \sum_{j=0}^{D-1} f_j t^j$ に対して f_0 が可逆ならば $f(t)^{-1}$ が存在し, その形は具体的に $1/f(t) = 1-(f_1/f_0^2)\,t+(f_1^2/f_0^3 - f_2/f_0^2)\,t^2+\cdots$ と書くことができる. このとおりに逆数を計算すると速度的に不利であるため, Newton 反復 (Algorithm 1) で逆数近似を行う. $f_0 = 1$ ならば各係数の分母を考慮する必要がないため, 逆数計算はとくに簡潔になる.

Algorithm 1 Newton 法

Require: $f(t)$: $f_0 = 1$ なる多項式.
Ensure: 逆元近似 $g \in R[x, N]$ 多項式.
1.[Init] $g(t) = 1; n = 1;$
2. [Newton 反復]
while $n < N + 1$ **do**
$n = 2n;$
if$(n > N + 1)$ $n = N + 1;$
$h(t) = f(t) \mod t^n;$
$h(t) = h(t)g(t) \mod t^n;$
$g(t) = g(t)(2 - h(t) \mod t^n);$
end while
return $g(t);$

2.2.2. *FFT* 乗算. 多項式の高速乗算のよく知られたテクニックとして FFT 乗算がある. $n-1$ 次以下の多項式 $f(x), g(x) \in \mathbb{Z}[x]$ を

$$f(x) = \sum_{i=0}^{n-1} f_i x^i, \quad g(x) = \sum_{i=0}^{n-1} g_i x^i$$

と表す. 次数が $n-1$ より真に小さい場合は先頭に 0 を詰めて見かけの次数を $n-1$ 次に揃える. $f(x)$, $g(x)$ から長さ $2n$ の配列 f, g を次のように作る:

$$f = (f_0, f_1, \ldots, f_{n-1}, 0, \ldots, 0), \quad g = (g_0, g_1, \ldots, g_{n-1}, 0, \ldots, 0)$$

f, g の長さ $2n$ の離散フーリエ変換をそれぞれ $\mathrm{DFT}_{2n}(f)$, $\mathrm{DFT}_{2n}(g)$ で表すと, 離散フーリエ変換の畳み込み定理から

$$f \times g = \frac{1}{2n} \mathrm{DFT}_{2n}^{-1} \left(\mathrm{DFT}_{2n}(f) \cdot \mathrm{DFT}_{2n}(g) \right),$$

が成立する. $f(x)g(x)$ は $f \times g$ の係数から復元することができる. ここで DFT の計算に FFT を用いると, $f(x)g(x)$ の計算には $O(p \log p \log\log p)$ のみが必要であることが分かる.

2.2.3. *Nussbaumer*法. ネガサイクリックコンボリューションの計算方法として Nussbaumer 法がある. これは次の命題を基礎においている.

Proposition 4 ([5, p.503]). f, g を長さが偶数 D の配列, $u_\pm = L(f) \pm H(f)$, $v_\pm = L(g) \pm H(g)$ とする. サイクリックコンボリューション $\times$ とネガサイクリックコンボリューション $\times_-$ の間には次の関係が成り立つ:

$$2(f \times g) = [(u_+ \times v_+) + (u_- \times_- v_-)] \cup [(u_+ \times v_+) - (u_- \times_- v_-)] .$$

ただし, $L(f)$, $H(f)$ はそれぞれ配列 f の前半部分, 後半部分である.

この命題の意味するところは, ネガサイクリックコンボリューションの計算は長さが半分のサイクリックコンボリューションとネガサイクリックコンボリューションの計算に帰着することができる, ということである.

Proposition 5 (Nussbaumer). R を可換環, $D = 2^k = mr$, $m \mid r$ とする. このとき, R 係数の長さ D の配列のネガサイクリックコンボリューションは, 多項式環の剰余環 $S = R[t]/(t^D + 1)$ 内で, 先の配列に対応する係数をもつ多項式の乗算に対応する. さらに S は剰余環 $T = R[t]/(z - t^m)$ と同型である. ただし $T = R[z]/(z^r + 1)$ である. また, $z^{r/m}$ は T の中の -1 の m 乗根である.

この命題を次のように多項式乗算に適用する. R の元を係数する多項式 $f(t) = f_0 + f_1 t + \cdots + f_{D-1} t^{D-1}$, $g(t) = g_0 + g_1 t + \cdots + g_{D-1} t^{D-1}$ に対し, 対応する配列 $f = (f_0, f_1, \ldots, f_{D-1})$, $g = (g_0, g_1, \ldots, g_{D-1})$ を考える. ネガサイクリックコンボリューション $f \times_- g$ は環 S 内での多項式の積 $f(t)g(t)$ と対応する. さて, 多項式 $f(t)$, $g(t)$ を次のように分割する:

$$f(t) = \sum_{j=0}^{m-1} F_j(t^m) t^j,$$

$$g(t) = \sum_{j=0}^{m-1} G_j(t^m) t^j.$$

ここで各多項式 F_j, G_j は環 T の元として解釈する. すなわち,

$$F_j(z) = f_j + f_{j+m} z + \cdots + f_{j+m(r-1)} z^{r-1},$$

$$G_j(z) = g_j + g_{j+m} z + \cdots + g_{j+m(r-1)} z^{r-1}$$

とみる. 積 $f(t)g(t)$ の計算は (先頭に 0 を詰めて長さ $2m$ に調整した配列の) サイクリックコンボリューション

$$Z = (F_0, F_1, \ldots, F_{m-1}, 0, \ldots, 0) \times (G_0, G_1, \ldots, G_{m-1}, 0, \ldots, 0)$$

の計算に帰着された. $z^{r/m}$ が 1 の原始 $2m$ 乗根であることより, この計算は DFT で計算できる. また, 各要素同士の積には再帰的にネガサイクリックコンボリューションを用いればよい.

2.3. アルゴリズムの改良の方向性. これまででみた非正則対の計算には, いずれも何らかの方法で DFT の計算に帰着して高速アルゴリズムに落とし込んでいるが, 計算量は $O(p\log^2 p\log\log p)$ が必要であった. これを改良することを考える.

ベースとして巾級数による計算方法をとる. 前述のとおり, ある多項式 $f(x)$ の逆数近似によって $B_{2k} \mod p$ を求めるのであるが, Newton 法では $O(p)$ 次の多項式の積を $O(\log p)$ 回計算するため全体の計算量は $O(p\log^2 p\log\log p)$ である. そこで, 積をとる回数を $O(1)$ 回にすれば全体の計算量が $O(p\log p\log\log p)$ となる. その方法としてデコンボリューションを用いることを考えた. すなわち与えられた多項式 $f(x)$ に対して x^m を $f(x)$ で割った商 $g(x)$ を求めるものであるから, $x^m = f(x)g(x)+r(x)$ という関係が成り立つことに着目し, $g(x)$ をデコンボリューションで推定する.

この考えに基づき数値実験をおこなっており, デコンボリューション 1 回で割り算ができる場合とそうでない場合があることが分かった. 現在この点を追求しているところである.

References

[1] J. P. Buhler, R. E. Crandall, and R. W. Sompolski. Irregular primes to one million. *Math. Comp.*, 59(200):717–722, 1992.

[2] J. P. Buhler and D. Harvey. Irregular primes to 163 million. Technical Report arXiv:0912.2121, Dec 2009. Comments: 9 pages.

[3] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä. Irregular primes and cyclotomic invariants to four million. *Math. Comp.*, 61(203):151–153, 1993.

[4] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. A. Shokrollahi. Irregular primes and cyclotomic invariants to 12 million. *J. Symbolic Comput.*, 31(1-2):89–96, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[5] R. Crandall and C. Pomerance. *Prime numbers*. Springer, New York, second edition, 2005. A computational perspective.

[6] R. Ernvall and T. Metsänkylä. Cyclotomic invariants for primes between 125 000 and 150 000. *Math. Comp.*, 56(194):851–858, 1991.

[7] W. Johnson. Irregular prime divisors of the Bernoulli numbers. *Math. Comp.*, 28:653–657, 1974.

[8] W. Johnson. Irregular primes and cyclotomic invariants. *Math. Comp.*, 29:113–120, 1975. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

[9] V. V. Kobelev. A proof of Fermat's theorem for all prime ewponents less that 5500. *Dokl. Akad. Nauk SSSR*, 190:767–768, 1970.

[10] D. H. Lehmer. Automation and pure mathematics. In *in Applictions of Digital Computers*, pp. 219–231, 1963.

[11] D. H. Lehmer, E. Lehmer, and H. S. Vandiver. An application of high-speed computing to Fermat's last theorem. *Proc. Nat. Acad. Sci. U. S. A.*, 40:25–33, 1954.

[12] E. Lehmer. On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson. *Ann. of Math. (2)*, 39(2):350–360, 1938.

[13] P. Ribenboim, 吾郷 (訳編). 素数の世界.

[14] P. Ribenboim, 吾郷 (訳). フェルマーの最終定理 13 講.

[15] J. L. Selfridge, C. A. Nicol, and H. S. Vandiver. Proof of Fermat's last theorem for all prime exponents less than 4002. *Proc. Nat. Acad. Sci. U.S.A.*, 41:970–973, 1955.
[16] J. L. Selfridge and B. W. Pollack. Fermat's last theorem is true for any exponent up to 25 000. *Notices Amer. Math. Soc.*, 11:17, 1964. Abstract #608-138.
[17] M. Shokrollahi. Computation of irregular primes up to eight million. Technical report, 1996.
[18] 谷口. 円分体の相対類数計算 –多倍長係数多項式の高速乗算の応用–. 情報処理学会論文誌, 50(8):1768–1774, 2009.
[19] J. W. Tanner and S. S. Wagstaff, Jr. New congruences for the Bernoulli numbers. *Math. Comp.*, 48(177):341–350, 1987.
[20] H. S. Vandiver. On Bernoulli's numbers and Fermat's last theorem. *Duke Math. J.*, 3(4):569–584, 1937.
[21] H. S. Vandiver. Examination of methods of attack on the second case of Fermat's last theorem. *Proc. Nat. Acad. Sci. U. S. A.*, 40:732–735, 1954.
[22] S. S. Wagstaff, Jr. The irregular primes to 125000. *Math. Comp.*, 32(142):583–591, 1978.
[23] L. C. Washington. *Introduction to cyclotomic fields*, Vol. 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
[24] 和田. 非正則な素数の見付け方 : Fermat の予想の検証実験 (実験整数論および組合せ理論と計算機). 数理解析研究所講究録, 301:32–49, 1977.

東京理科大学理工学部数学科 非常勤講師, 278-8510 千葉県野田市山崎 2641
E-mail address: taniguti_tetuya@ma.noda.tus.ac.jp

関数体の塔に関する Elkies 予想の数値的証拠

長谷川武博 (thasegawa@suou.waseda.jp)，犬塚美代子，鈴木隆文

27/Feb/2010

Contents

1 関数体の塔

p を素数とし $\mathbb{F}_{p^2}$ を p^2 個の元からなる有限体とする．その定数体が $\mathbb{F}_{p^2}$ であるものを $\mathbb{F}_{p^2}$ 上の関数体 $F/\mathbb{F}_{p^2}$ という．その種数を $g(F)$ と，その有理点の個数を $N(F)$ と書くことにする．

$\mathcal{F} = (F_0, F_1, F_2, \ldots)$ が $\mathbb{F}_{p^2}$ 上の **関数体の塔** とは，次の 2 条件をみたすものをいう．(1) すべての i に対し F_{i+1}/F_i は次数 2 以上の分離拡大である．(2) ある s に対し $g(F_s) > 1$ である．

$\lambda(\mathcal{F}) = \lim_{i\to\infty} N(F_i)/g(F_i)$ を $\mathcal{F}/\mathbb{F}_{p^2}$ の **極限** という．$\mathcal{F}/\mathbb{F}_{p^2}$ が **最良** とは $\lambda(\mathcal{F}) = p - 1$ となるときをいう．ただし一般に $0 \le \lambda(\mathcal{F}) \le p - 1$ が知られている (Drinfeld-Vladut (1983))．

$f(x, y)$ を $\mathbb{F}_{p^2}$ 上の 2 変数多項式とする．$\mathcal{F}/\mathbb{F}_{p^2}$ が方程式 $f(x, y) = 0$ **によって再帰的に定義される関数体の塔** とは，次の条件をみたすものをいう．(0) $F_0 = \mathbb{F}_{p^2}(x_0)$ は有理関数体である．(1) $F_1 = \mathbb{F}_{p^2}(x_0, x_1)$ は 1 つの方程式 $f(x_0, x_1) = 0$ が定義する関数体である．(2) $F_2 = \mathbb{F}_{p^2}(x_0, x_1, x_2)$ は 2 つの方程式 $f(x_0, x_1) = f(x_1, x_2) = 0$ が定義する関数体である．$\cdots$

例 1 (Garcia-Stichtenoth (1996))：方程式

$$y^2 + (1 - x)^2 - 1 = 0$$

によって再帰的に定義される $\mathbb{F}_9$ 上の関数体の塔は 最良 である． □

注意：この方程式は数学的な背景は考えずにただがむしゃらに探したように思われる．

Elkies (1997, 2001) は，上の Garcia-Stichtenoth の関数体の塔を次のような解釈を与えた．方程式 $y^2 + (1 - x)^2 = 1$ の 2 変数 x と y に同時に 1 次分数変換 M を施すと，方程式 $x^2 = y(y + 1)(x + 1)$ を得る．ただし

$$Mt = \frac{1}{-t + 1}, \qquad M = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_3)$$

とする．さらに，この方程式を標数零の体上にリフトすれば $x^2 = y(y+16)(x+16)$ となる．現代の立場からみれば，この解釈では不十分 (標数零の体上にリフトするところが曖昧).

この最後の方程式は次のような意味をもつ．$\mathfrak{H}$ を上半平面とし $q = e^{2\pi iz}$ $(z \in \mathfrak{H})$ とする．$\eta(q) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$ を Dedekind η 関数とする．

$$y(q) = \left(\frac{\eta(q)}{\eta(q^4)}\right)^8, \qquad x(q) = y(q^2)$$

に対し

$$x^2(q) = y(q)\Big(y(q)+16\Big)\Big(x(q)+16\Big)$$

が成り立つ．ただし $y(q)$ はモジュラー曲線 $X_0(4)$ のハウプトモジュールである．

例 2 (Garcia-Stichtenoth (1996))：方程式

$$y^3 + (1-x)^3 - 1 = 0$$

によって再帰的に定義される $\mathbb{F}_4$ 上の関数体の塔は 最良 である． □

2 Elkies 予想

代数曲線 X がある保型関数によってパラメトライズされるとき，X を **モジュラー** という．

Elkies 予想 1 (1997)：ある方程式 $f(x,y) = 0$ によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の最良塔はモジュラー (elliptic，Shimura または Drinfeld modular curves) である． □

例 3 (Garcia-Stichtenoth (2003))：$p > 2$ ($p = 2$ は悪い還元) とする．このとき，方程式

$$y^2 + \left(\frac{1-x}{1+3x}\right)^2 = 1$$

によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔は 最良 である (注意：例 1 の一般化)． □

注意：この関数体の塔はガウスの算術幾何平均と関係がある．

Elkies (2001) の解釈によれば，上の方程式の 2 変数 x と y に同時にある 1 次分数変換を施せば，方程式 $x^2 = y(y+16)(x+16)$ を得る．この場合はリフトの必要がない．曖昧さがない．

例 4 (Garcia-Stichtenoth (2003))：$p > 2$ とする．このとき，方程式

$$y^2 + \left(\frac{1-x}{1+x}\right)^2 = 1$$

によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔は 最良 である． □

注意：この関数体の塔は Deuring 多項式や算術幾何平均と関係がある．

上の方程式にある 1 次分数変換を施せば，方程式 $x^2 = y(y+8)(x+4)$ を得る (Elkies).

$$y(q) = \frac{\eta^4(q)\eta^2(q^4)}{\eta^2(q^2)\eta^4(q^8)}, \qquad x(q) = y(q^2)$$

に対し

$$x^2(q) = y(q)\Big(y(q)+8\Big)\Big(x(q)+4\Big)$$

が成り立つ．ただし $y(q)$ はモジュラー曲線 $X_0(8)$ のハウプトモジュールである．

例 5 (Garcia-Stichtenoth (2003))：$p > 2$ とする．このとき，方程式

$$y^2 = \frac{x^2+1}{2x}$$

によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔は 最良 である． □

注意：この関数体の塔は Deuring 多項式や算術幾何平均と関係がある．

上の方程式にある 1 次分数変換を施せば，$x^2 = y(y+4)(x+2)$ を得る (Elkies).

$$y(q) = \frac{\eta^2(q)\eta(q^8)}{\eta(q^2)\eta^2(q^{16})}, \qquad x(q) = y(q^2)$$

に対し

$$x^2(q) = y(q)\Big(y(q)+4\Big)\Big(x(q)+2\Big)$$

が成り立つ．ただし $y(q)$ はモジュラー曲線 $X_0(16)$ のハウプトモジュールである．

3 次数 2 (Elkies)

ここでは，第 1 章と第 2 章では紹介していないモジュラー方程式を紹介する．いずれも Elkies によって発見された (2001).

モジュラー曲線 $X_0(N), X_0(N)/\omega$ のレベル N が $N = 2\times$ (偶数) の場合：その標準形は

$$x^2 = y(y+A)(x+B)$$

である．モジュラー方程式と，それによって再帰的に定義される関数体の塔のもっとも底の有理関数体 F_0 に対応するモジュラー曲線の順に記述する．

$$\begin{aligned} x^2 &= y(y+4)(x+4), && X_0(12)/\omega_3 \\ x^2 &= y(y+2)(x+2), && X_0(28)/\omega_7 \\ x^2 &= y(y-2)(x-2), && X_0(12) \end{aligned}$$

注意：3 番目の方程式によって再帰的に定義される $\mathbb{F}_{p^2}$ $(p \neq 2,3)$ 上の関数体の塔は 最良 だろう (これは数値実験の結果)．他方，1 番目と 2 番目は最良では ない．ところが，ある条件をみたす素数 p に対しては，これらの関数体の塔は of finite ramification type になる (その条件とは，1 番目については $p \equiv 5 \pmod 6$，2 番目については $p \equiv 3,5,6 \pmod 7$ である).

関数体の塔 $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ が **of finite ramification type** とは，すべての i に対し F_0 のある点の集合 $\{P \mid P \text{ は } F_i/F_0 \text{ における分岐 (branch) 点}\}$ が有限集合になるときをいう．

Elkies 予想 2：ある方程式 $f(x,y) = 0$ によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔がもし of finite ramification type なら，それはモジュラーである． □

モジュラー曲線 $X_0(N), X_0(N)/\omega$ のレベル N が $N = 2\times$ (奇数) の場合：その標準形は

$$x^2 = y(xy + Ax + B)$$

である．

$$\begin{aligned} x^2 &= y(yx + 48x + 4096), && X_0(2) \\ x^2 &= y(yx + 12x + 64), && X_0(6)/\omega_3 \end{aligned}$$

$$x^2 = y(yx + 8x + 16), \qquad X_0(10)/\omega_5$$
$$x^2 = y(yx + 6x + 8), \qquad X_0(14)/\omega_7$$
$$x^2 = y(yx + 4x + 4), \qquad X_0(22)/\omega_{11}$$
$$x^2 = y(yx + 2x + 2), \qquad X_0(46)/\omega_{23}$$
$$x^2 = y(yx - 6x - 8), \qquad X_0(6)$$
$$x^2 = y(yx - 2x - 4), \qquad X_0(10)$$
$$x^2 = y(yx + 6x + 4), \qquad X_0(18)/\omega_9$$
$$x^2 = y(yx + 2x + 4), \qquad X_0(30)/\omega_3, \omega_5$$
$$x^2 = y(yx + 4x + 2), \qquad X_0(30)/\omega_{15}$$
$$x^2 = y(yx + 16), \qquad [9]\backslash\mathfrak{H}^*$$
$$x^2 = y(yx + 4), \qquad [27]\backslash\mathfrak{H}^*$$
$$x^2 = y(yx + 2), \qquad [63]\backslash\mathfrak{H}^*$$

$\mathfrak{H}$ を上半平面とし $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ とする．3 つの群 [9], [27], [63] の定義は，ここには書かない.

$$x^2 = y(yx - 2), \qquad X_0(18)$$

4 次数 3 (オリジナル)

例 6 (例 2 の一般化)：$p \neq 3$ とする．このとき，方程式

$$y^3 + \left(\frac{1-x}{1+2x}\right)^3 = 1$$

によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔は 最良 である． □

解釈：ある 1 次分数変換を施すと，方程式 $x^3 = y(y^2 + 9y + 27)(x^2 + 9x + 27)$ を得る．この方程式は次のような意味をもつ.

$$y(q) = \left(\frac{\eta(q)}{\eta(q^9)}\right)^3, \qquad x(q) = y(q^3)$$

に対し

$$x^3(q) = y(q)\Big(y^2(q) + 9y(q) + 27\Big)\Big(x^2(q) + 9x(q) + 27\Big)$$

が成り立つ．ただし $y(q)$ はモジュラー曲線 $X_0(9)$ のハウプトモジュールである． □

例 7：$p \neq 3$ とする．このとき，方程式

$$y^3 = \frac{x(x^2 + 2x + 4)}{x^2 - x + 1}$$

が定義する $\mathbb{F}_{p^2}$ 上の関数体の塔は of finite ramification type である． □

注意：この関数体の塔は最良だろう (これは数値実験の結果).

解釈：ある 1 次分数変換を施すと，方程式 $x^3 = y(y^2 - 3y + 3)(x^2 - 3x + 3)$ を得る．この方程式は次のような意味をもつ．

$$y(q) = \frac{\eta(q^9)\eta^2(q^2)}{\eta(q)\eta^2(q^{18})}, \qquad x(q) = y(q^3)$$

に対し

$$x^3(q) = y(q)\Big(y^2(q) - 3y(q) + 3\Big)\Big(x^2(q) - 3x(q) + 3\Big)$$

が成り立つ．ただし $y(q)$ はモジュラー曲線 $X_0(18)$ のハウプトモジュールである． □

ほかにも次のようなモジュラー方程式がある．

モジュラー曲線 $X_0(N), X_0(N)/\omega$ のレベル N が $N = 3\times$(3 の倍数) の場合：その標準形は

$$x^3 = y(y^2 + A_1y + A_0)(x^2 + B_1x + B_0)$$

である．

$$x^3 = y(y^2 + 3y + 9)(x^2 + 3x + 9), \qquad X_0(18)/\omega_2$$
$$x^3 = y(y^2 + 3y + 3)(x^2 + 3x + 3), \qquad X_0(36)/\omega_4$$

注意：上の 2 番目の方程式と例 7 の方程式は，1 次分数変換 $\varepsilon(t) = -t$ によって移る．

モジュラー曲線 $X_0(N), X_0(N)/\omega$ のレベル N が $N = 3\times$(3 の倍数以外) の場合：その標準形は

$$x^3 = y\Big((y^2 + A_1y + A_0)x^2 + (B_1y + B_0)x + C\Big)$$

である．

$$x^3 = y\Big((y^2 + 36y + 270)x^2 + (729y + 26244)x + 531441\Big), \qquad X_0(3)$$
$$x^3 = y\Big((y^2 + 12y + 54)x^2 + (81y + 972)x + 6561\Big), \qquad X_0(6)/\omega_2$$
$$x^3 = y\Big((y^2 + 6y + 15)x^2 + (9y + 54)x + 81\Big), \qquad X_0(15)/\omega_5$$
$$x^3 = y\Big((y^2 + 3y + 6)x^2 + (3y + 9)x + 9\Big), \qquad X_0(33)/\omega_{11}$$
$$x^3 = y\Big((y^2 - 12y + 30)x^2 + (9y - 108)x + 81\Big), \qquad X_0(6)$$
$$x^3 = y\Big((y^2 + 12y + 30)x^2 + (9y + 108)x + 81\Big), \qquad X_0(12)/\omega_4$$
$$x^3 = y\Big((y^2 + 6y + 12)x^2 + (3y + 18)x + 9\Big), \qquad X_0(24)/\omega_8$$
$$x^3 = y\Big((y^2 + 18)x^2 - 27yx + 729\Big), \qquad [4]_2\backslash\mathfrak{H}^*$$
$$x^3 = y\Big((y^2 + 6)x^2 + 9yx + 81\Big), \qquad [8]_3\backslash\mathfrak{H}^*$$
$$x^3 = y\Big((y^2 + 3)x^2 + 3yx + 9\Big), \qquad [20]_6\backslash\mathfrak{H}^*$$
$$x^3 = y\Big((y^2 - 6)x^2 - 3yx + 9\Big), \qquad X_0(12)$$
$$x^3 = y\Big((y^2 + 6)x^2 - 3yx + 9\Big), \qquad [16]_6\backslash\mathfrak{H}^*$$
$$x^3 = y\Big(y^2x^2 + 9yx + 27\Big), \qquad [16]_4\backslash\mathfrak{H}^*$$
$$x^3 = y\Big(y^2x^2 + 3yx + 9\Big), \qquad [32]_6\backslash\mathfrak{H}^*$$
$$x^3 = y\Big(y^2x^2 - 3yx + 3\Big), \qquad [8]_{12}\backslash\mathfrak{H}^*$$
$$x^3 = y\Big(y^2x^2 + 3yx + 3\Big), \qquad [64]_{12}\backslash\mathfrak{H}^*$$

5 次数 5 (オリジナル)

モジュラー曲線 $X_0(N), X_0(N)/\omega$ **のレベル** N **が** $N = 5\times$**(5 の倍数) の場合**：

$$x^5 - y(y^4 + 5y^3 + 15y^2 + 25y + 25)(x^4 + 5x^3 + 15x^2 + 25x + 25), \qquad X_0(25)$$

注意：$p \neq 5$ を素数とする ($p = 5$ は悪い還元). この方程式によって再帰的に定義される $\mathbb{F}_{p^2}$ 上の関数体の塔は of finite ramification type である.

モジュラー曲線 $X_0(N), X_0(N)/\omega$ **のレベル** N **が** $N = 5\times$**(5 の倍数以外) の場合**：その標準形は

$$x^5 = y(f_4(y)x^4 + f_3(y)x^3 + f_2(y)x^2 + f_1(y)x + A), \qquad \deg f_n = n$$

である.

$$\begin{aligned} x^5 =& y\Big((y^4 + 30y^3 + 315y^2 + 1300y + 1575)x^4 + (125y^3 + 3750y^2 + 39375y + 162500)x^3 \\ &+ (15625y^2 + 468750y + 4921875)x^2 + (1953125y + 58593750)x + 244140625\Big), \qquad X_0(5) \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 + 10y^3 + 55y^2 + 140y + 175)x^4 + (25y^3 + 250y^2 + 1375y + 3500)x^3) \\ &+ (625y^2 + 6250y + 34375)x^2 + (15625y + 156250)x + 390625\Big), \qquad X_0(10)/\omega_2 \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 + 10y^3 + 35y^2 + 60y + 55)x^4 + (5y^3 + 50y^2 + 175y + 300)x^3 \\ &+ (25y^2 + 250y + 875)x^2 + (125y + 1250)x + 625\Big), \qquad X_0(20)/\omega_4 \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 - 10y^3 + 35y^2 - 60y + 55)x^4 + (5y^3 - 50y^2 + 175y - 300)x^3 \\ &+ (25y^2 - 250y + 875)x^2 + (125y - 1250)x + 625\Big), \qquad X_0(10) \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 + 15y^2 + 45)x^4 + (-25y^3 - 225y)x^3 \\ &+ (375y^2 + 1875)x^2 - 3125yx + 15625\Big), \qquad [4]_2\backslash\mathfrak{H}^* \end{aligned}$$

$$x^5 = y\Big((y^4 + 10y)x^4 + (5y^3 + 50)x^3 + 25y^2x^2 + 125yx + 625\Big), \qquad [9]_3\backslash\mathfrak{H}^*$$

$$\begin{aligned} x^5 =& y\Big((y^4 + 5y^2 + 15)x^4 + (-5y^3 - 25y)x^3 \\ &+ (25y^2 + 125)x^2 - 125yx + 625\Big), \qquad [8]_3\backslash\mathfrak{H}^* \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 + 5y^2 + 5)x^4 + (5y^3 + 15y)x^3 \\ &+ (15y^2 + 25)x^2 + 25yx + 25\Big), \qquad [16]_6\backslash\mathfrak{H}^* \end{aligned}$$

$$\begin{aligned} x^5 =& y\Big((y^4 - 5y^2 + 5)x^4 + (-5y^3 + 15y)x^3 \\ &+ (15y^2 - 25)x^2 - 25yx + 25\Big), \qquad [4]_6\backslash\mathfrak{H}^* \end{aligned}$$

$$x^5 = y(y^4x^4 + 5y^3x^3 + 15y^2x^2 + 25yx + 25), \qquad [36]_6\backslash\mathfrak{H}^*$$