

Proceedings of
Algebra and Computation 2015



Tokyo Metropolitan University

December 14-16, 2015

Edited by AC2015 Proceedings Committee

Organizers

Hirofumi Tsumura (Tokyo Metropolitan Univ.)

Shigenori Uchiyama (Tokyo Metropolitan Univ.)

Katsushi Waki (Yamagata Univ.)

Takuya Ikuta (Kobe Gakuin Univ.)

Yukihiro Uchida (Tokyo Metropolitan Univ.)

Masanori Sawa (Kobe Univ.)

第 11 回「代数学と計算」研究集会 (AC2015)

標記の研究集会を下記の要領で開催いたしますので、ご案内申し上げます。

主催者

津村 博文 (首都大学東京)

内山 成憲 (首都大学東京)

脇 克志 (山形大学)

生田 卓也 (神戸学院大学)

内田 幸寛 (首都大学東京)

澤 正憲 (神戸大学)

記

2015 年 12 月 14 日 (月) - 16 日 (水)

首都大学東京 国際交流会館大会議室

特別講演者

Claus Fieker (Tech. Univ. Kaiserslautern)

Andreas Enge (INRIA Bordeaux-Sud-Ouest)

大野泰生 (東北大学)

篠原雅史 (滋賀大学)

篠原直行 (情報通信研究機構)

谷口哲也 (金沢工業大学)

[プログラム]

Dec. 14 (Mon.)

- 12:50 - 12:55:** Opening
13:00 - 13:40: [特別講演] Claus Fieker (Tech. Univ. Kaiserslautern)
“Classical Algorithmic Number Theory”
13:50 - 14:30: [特別講演] Andreas Enge (INRIA Bordeaux-Sud-Ouest)
“Computing with theta functions on abelian surfaces”
14:50 - 15:20: 宮崎隆史 (群馬大学)
“原始ピタゴラス数から生ずる三項指数型不定方程式について”
15:30 - 16:20: [特別講演] 大野泰生 (東北大学)
“多重ベルヌーイ数および関連する話題”
16:30 - 17:00: 田坂浩二 (名古屋大学)
“周期たちの間の線形関係式の数値実験”

Dec. 15 (Tue.)

- 10:00 - 10:30:** 佐竹翔平 (名古屋大学), 澤正憲 (神戸大学), 神保雅一 (中部大学)
“有向グラフの非対称性と自己同型について”
10:40 - 11:00: 宗政昭弘 (東北大学), 原田昌晃 (東北大学)
“二元自己双対符号の被覆半径と影符号”
11:00 - 11:20: 平峰豊 (熊本大学)
“On planar difference sets and related divisible designs admitting SCT groups”
13:30 - 14:20: [特別講演] 篠原雅史 (滋賀大学)
“平面上の距離集合の分類問題と正多角形”
14:40 - 15:10: 野崎寛 (愛知教育大学)
“(0, ±1) ベクトルの最大距離を避ける最大部分集合について”
15:20 - 16:00: 富安亮子 (JST さきがけ (専任))
“結晶学の解析ソフトウェア Conograph の開発中に会った代数学の諸問題について”
16:10 - 16:30: 松木伯元 (富山化学工業株式会社)
“二値変数多項式に対する和公式”

Dec. 16 (Wed.)

- 10:00 - 10:30:** 小貫啓史 (首都大学東京), 照屋唯紀 (産業技術総合研究所), 金山直樹 (筑波大学), 内山成憲 (首都大学東京)
“Elliptic net の並列化による optimal ate pairing の計算”
10:30 - 10:50: 岡野恵司 (都留文科大学)
“ペアリング暗号に適した楕円曲線族が理想的条件をもつ可能性について”
11:00 - 11:20: 安田貴徳 (九州先端科学技術研究所), Xavier Dahan (お茶の水女子大学), 櫻井幸一 (九州大学)
“環の既約分解を用いた NTRU 型格子暗号の安全性評価”
11:20 - 11:40: 横山俊一 (九州大学)
“数論データベース LMFDB の開発について”
13:50 - 14:40: [特別講演] 谷口哲也 (金沢工業大学)
“円分体の相対類数の計算について”
15:00 - 15:50: [特別講演] 篠原直行 (情報通信研究機構)
“小標数の有限体上の離散対数問題の解法”
16:00 - 16:30: 工藤桃成 (九州大学)
“計算機代数システムによる連接層係数コホモロジーの高速計算”
16:30 - 16:40: Closing

Classical Algorithmic Number Theory

Claus Fieker

`fieker@mathematik.uni-kl.de`

University of Kaiserslautern

December 14, 2015

- 1 Intro
- 2 Task 1: Ring of Integers
- 3 Task 2: Galois Group
- 4 Task 3& 4: Unit and Class Group
- 5 Applications

Setting

A number field K is a finite extension of \mathbb{Q} . In particular for some irreducible polynomial $f \in \mathbb{Q}[t]$, the quotient ring

$$K := \mathbb{Q}[t]/f$$

is a number field. We will assume $f \in \mathbb{Z}[t]$ monic - to make life easier.

The main object of interest however, is

$$\mathbb{Z}_K = \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\}$$

the normalisation of $\mathbb{Z}[t]/f$, the ring of integers, or maximal order of K .

Zassenhaus

Zassenhaus formulated the basic tasks/ challenges for constructive number theory, they are the foundations for almost all applications and all more advanced problems:

Zassenhaus

Given K defined by some polynomial f , compute:

- 1 Ring of Integers
- 2 Galois Group
- 3 Unit Group
- 4 Class Group

We will define and discuss them in this order.

Task 1

Zassenhaus

Task 1: Given f find an algorithmic description of \mathbb{Z}_K

Of course, there is

Foundations

Task 0: Find algorithms for K

We assume Task 0 to be done.

Task 1: Ring of Integers

Structure

We have classical structural result(s):

Fact

\mathbb{Z}_K is a free \mathbb{Z} -module of rank $n = K : \mathbb{Q}$.

$$\mathbb{Z}_K \subseteq \frac{1}{f'(t)}\mathbb{Z}[t]/f \subseteq \frac{1}{\text{disc } f}\mathbb{Z}[t]/f$$

The second fact allows to easily use field operations instead of designing ring operations, by bounding the maximal denominator of integral elements relative to $\mathbb{Z}[t]/f$ the equation order of f .

Task 1: Ring of Integers

Concrete

The more concrete Task 1 now is to find a \mathbb{Z} -basis for \mathbb{Z}_K . We have a range of algorithms, coming from diverse parts of algebra. All in common have a decomposition of the problem: if

$$(\mathbb{Z}_K : R) = d_1 d_2$$

for coprime d_1 and d_2 , then the Chinese Remainder Theorem (for modules) implies

$$\mathbb{Z}_K = O_{d_1} + O_{d_2}$$

Typically, one chooses d_i to be a prime power, or defines them via square-free divisors of the discriminant.

Task 1: Ring of Integers

Chistov

Chistov, Buchmann-Lenstra

Finding a basis for \mathbb{Z}_K is polynomial time equivalent to finding the largest square-free factor of $\text{disc } f = \text{disc } R$

Thus, in general, we can't do this as factorisation is too expensive.

Task 1: Ring of Integers

Local solution

Let $O_p = \{x \in \mathbb{Z}_k \mid p^k x \in R\}$

Zassenhaus

There is a polynomial time algorithm to find a \mathbb{Z} -basis for O_p .

And:

Montes

There is a fast and practical polynomial time algorithm that will find a \mathbb{Z} -basis for O_p .

Why both algorithms?

Task 1: Ring of Integers

Comparison

Zassenhaus' is founded in representation theory and utilises only linear algebra. The algorithm has an easy structure.

Montes' is based on polynomial factorisation in completions. The method is intricate and highly technical on an elementary level.

Historically, Zassenhaus' method belongs to the Round-2 family, while Montes' is the ultimate representative of the Round-4 family.

Task 1: Ring of Integers

Extension

Both Zassenhaus' and Montes' methods apply to the geometric setting and allow the normalisation of plane curves. The classical Round-2 is identical to the normalisation in commutative algebra. Zassenhaus' methods, based on linear algebra, also work for square-free integers instead of primes. It computes

$$O_d = \{x \in K \mid d^k x \in R\}$$

for any square-free d not divisible by any prime $p \leq n$.

Currently, Montes' is much faster, but works only if d is a prime.

There is work done by Nart et. al. to lift this restriction.

In serious applications they are used side-by-side: Montes is called for all small primes and primes known to be critical, Zassenhaus is then used to deal with the non-factored rest.

Task 1

Round-2

Let

$$\sqrt{pR} = \{x \in R \mid x^k \in pR\}$$

be the *radical* of the ideal pR , and

$$[\sqrt{pR}/\sqrt{pR}] := \{x \in K \mid x\sqrt{pR} \subseteq \sqrt{pR}\}$$

the endomorphism ring of \sqrt{pR} . Then

Zassenhaus: local maximality

Let $S := [\sqrt{pR}/\sqrt{pR}]$, then

- $R \subseteq S \subseteq O_p$
- $R = O_p$ iff $R = S$

This readily gives an algorithm!

Task 2

Zassenhaus

Task 2: Determine the Galois group of the normal closure of K

In some sense this is trivial: compute the normal closure by repeated factorisation and find the group directly.

This is (probably) polynomial time in the degree of the closure.

Problem: this will be close to $n!$, hence too large.

On the other hand: a few local computations will typically prove the group to be S_n without computing anything expensive.

If the closure is “small”, then this works well.

Task 2: Galois Group

Landau

Susan Landau

There is a polynomial time algorithm to decide if the group is soluble.

The key idea here is that soluble permutation groups are “small”. She shows that repeated factorisation will either prove the group to be too large to be soluble or terminate in polynomial time. The algorithm is sadly enough, not practical.

Task 2: Galois Group

Stauduhar

Stauduhar, F, Klüners, Cannon, ...

There is a (practical) algorithm that will compute the Galois group explicitly.

The idea is to explicitly compute approximations of the roots in a large field (complex numbers, suitable local fields) and then use invariant theory and group theory to find explicit permutations that can and cannot be in the Galois group.

The complexity is unpublished, but exponential in some cases.

The performance is fine for most input up to degree 40. It has been used for degree > 100 .

Task 2: Galois Group

Stauduhar

Let $\alpha_1, \dots, \alpha_n$ be the roots of f in some field and $G \leq S_{\alpha_1, \dots, \alpha_n}$ be such that $\text{Gal}(f) \leq G$.

Finally, let $U \leq G$ be maximal.

Stauduhar

Let $I \in \mathbb{Z}[x_1, \dots, x_n]$ be such that $\text{Stab}_G(I) = U$, then $\text{Gal}(f) \leq U$ iff $I(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$

To test for any conjugate group U^σ , just conjugate the invariant I . This will be iterated for all maximal subgroups until no further descent can be found.

Task 2: Galois Group

Challenges

Challenges

- Clever choice of field for the roots
- The roots are only approximate, how test $I(\alpha) \in \mathbb{Z}$
- Find I
- Find maximal subgroups
- Find transversals $G//U$
- Find good (small) starting group
- Exclude as many subgroups as possible
- Prove the result if shortcuts are taken

Zassenhaus

Task 3: Determine the unit group of \mathbb{Z}_K

Zassenhaus

Task 4: Determine the class group, ie. the ideal structure of \mathbb{Z}_K

Originally, those were attempted independently, units first as the result was used in the last problem.

Currently we favour algorithms that compute both at the same time.

Task 3: Unit group

Structure

Dirichlet

The unit group \mathbb{Z}_K^* is finitely generated, the free part is of rank $r = r_1 + r_2 - 1$ where r_1 is the number of real embeddings of K , and $2r_2$ the number of complex embeddings.

The re-formulated Task 3:

Task

Find fundamental units ϵ_i ($1 \leq i \leq r$) and a torsion unit ζ s.th.
 $\mathbb{Z}_K^* = \langle \zeta, \epsilon_1, \dots, \epsilon_r \rangle$

Task 4: Class Group

Definition

Let $\mathfrak{a}, \mathfrak{b} \leq \mathbb{Z}_K$ be ideals. Then $\mathfrak{a} \sim \mathfrak{b}$ iff $\exists \alpha, \beta \in \mathbb{Z}_K$ s.th.
 $\alpha \mathfrak{a} = \beta \mathfrak{b}$.

Class Group

Under the equivalence, the ideals form a finite abelian group, the class group Cl_K .

Using the language of fractional ideals,

$$\text{Cl}_K = \text{group of fractional ideals/principal ideals}$$

This is the Picard group of \mathbb{Z}_K . It can be generalised to the (Arakelov) divisor class group of K .

Task 4: Class Group

Basics

For any ideal $\mathfrak{a} \leq \mathbb{Z}_K$, we define $N(\mathfrak{a}) = |\mathbb{Z}_K/\mathfrak{a}|$

Finite Generation

The finite generation can be quantified:

- Minkowski: $B := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\text{disc}(\mathbb{Z}_K)|}$
- Bach: $B := 12 \log^2 |\text{disc}(\mathbb{Z}_K)|$

Then Cl_K is generated by (prime) ideals of norm $N(\mathfrak{a}) \leq B$

There are better bounds, not not asymptotically and not by much.

So we have generators, how do we find (all) relations?

Task 4: Class Group

Relations

Set

$$F := \{\mathfrak{p} \leq \mathbb{Z}_K \mid N(\mathfrak{p}) \leq B, \mathfrak{p} \text{ prime}\}$$

the *factor base*. Then a relation $\alpha \in K^*$ is an element s.th.

$$(\alpha) = \prod_{\mathfrak{p} \in F} \mathfrak{p}^{m_{\alpha, \mathfrak{p}}}$$

Buchmann, Pohst, Zassenhaus, Hafner, McCurley, ...

Using short elements in random ideals, there is a good probability to find a relation.

Task 4: Class Group

Relations

The set

$$\mathfrak{R} := \{\alpha \in K^* \mid \alpha \text{ is a relation for } F\}$$

is a fin. gen. \mathbb{Z} -module. The goal of the class group algorithm is to find a finite set $R \subseteq K^*$ s.th.

$$\langle R \rangle = \mathfrak{R}$$

The *relation matrix*

$$M = (m_{\alpha, \mathfrak{p}})_{\alpha \in R, \mathfrak{p} \in F}$$

collects the information about the relations $\alpha \in R$ that we have found.

Task 4: Class Group

How do we know we have “all” relations, ie. a generating set?

A necessary condition is $\text{rank } M = \#F$, the relation matrix must have full rank.

Suppose we have $t \in \mathbb{Z}^R$ s.th. $tM = 0$. Then

$$\prod_{\alpha \in R} \alpha^{t_\alpha} \in \mathbb{Z}_K$$

as the corresponding principal ideal is trivial.

This is the link to Task 3: The relation matrix will have a kernel which defines units.

Let $U \leq \mathbb{Z}_K^*$ be generated by kernel elements (a basis, random elements).

Task 3, 4: Class and Unit Group

Stopping condition: Unit lattice

We have a relation matrix of full rank and a subgroup $U \leq \mathbb{Z}_K^*$ of finite index.

Define

$$L : \mathbb{Z}_K^* \rightarrow \mathbb{R}^n : \epsilon \mapsto (\log |\epsilon^{(i)}|)_i$$

then

Unit Lattice

$L(\mathbb{Z}_K^*) \leq \mathbb{R}^n$ is a lattice of rank r and discriminant $\text{Reg } \mathbb{Z}_K$

Task 3, 4: Class and Unit Group

Stopping condition

Euler Product - Analytic Class Number Formula

The Euler product

$$E = \prod_p \frac{\prod_{\mathfrak{p}|p} (1 - 1/N(\mathfrak{p}))}{1 - 1/p}$$

exists and there is an explicit constant C s.th.

$$E = C \# \text{Cl}_K \text{Reg } \mathbb{Z}_K$$

Task 3, 4: Euler Product

Bach

There is an algorithm and an explicit constant D that will, given

$$\{\mathfrak{p} \leq \mathbb{Z}_K \mid N(\mathfrak{p}) \leq D \log^2 |\text{disc}(\mathbb{Z}_K)|\}$$

compute \tilde{E} s.th.

$$1/\sqrt{2} \leq \frac{E}{\tilde{E}} \leq \sqrt{2}$$

This procedure will run in polynomial time.
It depends on the GRH.

Task 3, 4: Euler Product

Since, by assumption, we have a multiple of the class number and a multiple of the regulator, we get

GRH

If $1/\sqrt{2} \leq \frac{C}{E} \# \text{Cl}_K \text{Reg } \mathbb{Z}_K \leq \sqrt{2}$ then both Cl_K and $\text{Reg } \mathbb{Z}_K$ are correct and the computation is finished.

The problem is in the fine print: this is true if the factor base is large enough, ie $\langle F \rangle = \text{Cl}_K$

Task 3, 4: Alternatives

If the factor base is too small, then if the matrix has full rank, we can ensure completeness of the relations differently:

Let h be the product of all elementary divisors of M and p a prime divisor of h and $V := \langle R \rangle \leq K^*$, then

There is an algorithm to compute the p -saturation

$$V_p := \{\beta \in K \mid \beta^{p^k} \in V\}$$

If we add elements in $V_p \setminus V$ to R , we decrease h by a power of p . Iterating this for all $p \mid h$ we can guarantee completeness of the relations.

At this point, have a subgroup of the class group, missing parts are due to the too small factor base.

Task 3, 4: Alternatives

Applying this p -saturation to the unit group U we can get the complete unit group provided we have a lower bound on the regulator.

Lower Regulator Bound

For all number fields K , we have $\text{Reg } \mathbb{Z}_K \geq 0.25$

The problem here is that, mostly, $\text{Reg } \mathbb{Z}_K = O(\sqrt{|\text{disc } \mathbb{Z}_K|})$, so we have to test a lot of primes - and the units are very large.

Task 3,4: Class Group

Buchmann, Hafner, McCurly, Cohen, Diaz y Diaz, Olivier

The procedure outlined will compute the class group in sub-exponential time.

Problems:

- This works only for bounded degree
- The factor basis used is *much* larger than we did here ... so the linear algebra will not work.
- The analysis holds only under GRH
- ... and under *reasonable assumptions* ... which are not true for interesting large degree fields

Principal ideals

The result of the class group computation is

- The factor base F
- The set R of relations
- The relation matrix M
- (Sometimes) transformation matrices

For any $\mathfrak{a} \in \langle F \rangle$, $\mathfrak{a} = \prod \mathfrak{p}^{m_{\mathfrak{p}}}$ we have

Principal Ideal Testing

\mathfrak{a} is principal iff $(m_{\mathfrak{p}})_F \in \text{colspan} M$

A generator can thus also be computed.

Principal ideals

If $\mathfrak{a} \notin \langle F \rangle$, not all is lost.

We search for α s.th. $\alpha\mathfrak{a} \in \langle F \rangle$ - using the same methods as in the relations search.

Clearly \mathfrak{a} is principal iff $\alpha\mathfrak{a}$ is.

Extending this idea we can also compute a basis for the S -units for any (reasonable) finite set S of primes.

Norm Equations, Galois cohomology

Having S -units, we can easily

- solve Norm equations
- split 2-cocycles

in (relative) normal fields.

This has applications in e.g. representation theory.

Large Degree Fields

Fully homomorphic encryption is using $\mathbb{Q}(\zeta_n)$, the security depends on not being able to find a small generator for some public ideal.

Standard procedure is to find any generator and then use the unit lattice to find a small one.

A standard reduction is to the maximal real subfield (of half the degree).

The current challenge is a field of degree 128.

For NTRU, we are looking at $t^n - 2$ for large n . For algebraic geometry we want $t^p - p$.

For all those fields are the *usual assumptions* wrong:

- it is much easier to find relations than Buchmann predicts
- the relations found this way are not at all randomly distributed, it is very hard to get a full rank matrix.
- for the cyclotomic case we have the unit group for free
- they are “small” for their degree
- the interesting fields have subfields, relations, as small elements, tend to come from subfields.

The curse of the large degree

The classical sub-exponential algorithm needs small elements. Classically, small elements are found using LLL: the LLL basis will contain elements that are within a factor of 2^n of the minimal ones. This factor grows exponentially with the degree. The success probability of choosing relations this way depends on the *norm* and *not on the size*. One can use stronger lattice reduction (BKZ) and recursive reduction techniques (special q -descent)

F-Biasse

This gives an algorithm that is sub-exponential with unbounded degree.

We don't know if this is practical, we're working on an implementation.

Conclusion

We have algorithmic solutions to all of Zassenhaus' problems:

- 1 Ring of Integers
- 2 Galois Group
- 3 Unit Group
- 4 Class Group

All problems are still under active research.

Most of this applies to *relative extensions* in a limited way and also to the geometric setting (plane curves, univariate function fields).

Conclusion

Algorithms are (partly) implemented and available in

- Magma
- Pari/gp
- Sage (Pari/gp)
- Kant/KaSH (defunct)
- Lidia (defunct)
- Hecke/Nemo (upcoming)

Computing with theta functions on abelian surfaces

Andreas Enge

LFANT project-team
INRIA Bordeaux-Sud-Ouest
andreas.enge@inria.fr
<http://www.math.u-bordeaux.fr/~aenge>

11th Symposium on Algebra and Computation (AC2015)
Tokyo Metropolitan University
December 14, 2015



Computing with theta functions

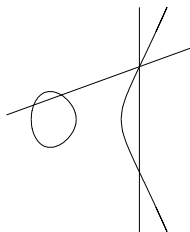
- 1 Abelian varieties and ϑ functions
- 2 Kummer surfaces and the group law
- 3 Complex multiplication and class polynomials
- 4 Modular polynomials

Abelian varieties

- **Abelian variety**
 - ▶ algebraic variety
 - ▶ algebraic group law
- **Examples**
 - ▶ elliptic curves
 - ▶ Jacobians of hyperelliptic curves
- **Cryptology**: smaller key sizes than RSA and more efficient
 - ▶ effective and efficient group law
 - ▶ cardinality
 - ▶ isogenies = maps between varieties

Elliptic curves

$$Y^2 = X^3 + aX + b, \quad a, b \in K$$



- Hasse 1934

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

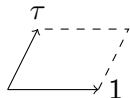
- Isomorphism class determined by

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Complex elliptic curves and modular functions

- Complex elliptic curve

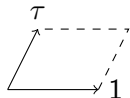
$$E = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$$



Complex elliptic curves and modular functions

- Complex elliptic curve

$$E = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$$



- Modular functions

- ▶ $f : \mathbb{C} \rightarrow \mathbb{C}$ with $f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \text{Sl}_2(\mathbb{Z})$
- ▶ f meromorphic, also “at ∞ ”: $q = e^{2\pi i\tau}$, $f(\tau) = \sum_{\nu=\nu_0}^{\infty} c_{\nu} q^{\nu}$
- ▶ $\mathbb{C}_{\Gamma} = \mathbb{C}(j)$, where j has a simple pole at ∞ :

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

Complex abelian varieties of dimension g

- Principally polarised abelian variety (ppav)

$$\mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$$

- Period matrix $\Omega \in \text{Mat}^{g \times g}$ in the Siegel half space \mathbb{H}_2 :
 - ▶ symmetric
 - ▶ $\Im(\Omega)$ positive definite
- Principally polarised abelian surface (ppas): $g = 2$
Jacobian variety of a hyperelliptic curve of genus 2
- Group action of $\Gamma = \text{Sp}_4(\mathbb{Z})$

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} (\Omega) = (A\Omega + B)(C\Omega + D)^{-1}$$

- Siegel modular functions

$$\mathbb{C}_\Gamma = \mathbb{C}(j_1, j_2, j_3)$$

ϑ functions

- ϑ function with characteristic $a, b \in (\frac{1}{N} \mathbb{Z}/\mathbb{Z})^g$

$$\vartheta_{a,b}(z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i(n+a)^T \Omega(n+a) + 2\pi i(n+a)^T (z+b)}$$

Projective embeddings by ϑ functions

- Quasi-periodicity

$$\vartheta_{a,b}(z + m_1 + m_2\Omega, \Omega) = e^{2\pi i(a^T m_1 - b^T m_2) - \pi i m_2^T \Omega m_2 - 2\pi i m_2^T z} \vartheta_{a,b}(z, \Omega)$$

- Basis of the linear space of functions of level N

$$\vartheta_b(z) = \vartheta_{0,b}(z, \Omega/N)$$

$$\vartheta_b(z + m_1 + m_2\Omega) = e^{-\pi i N m_2^T \Omega m_2 - 2\pi i N m_2^T z} \vartheta_b(z)$$

Same factor for all b .

Projective embeddings by ϑ functions

- Quasi-periodicity

$$\vartheta_{a,b}(z + m_1 + m_2\Omega, \Omega) = e^{2\pi i(a^T m_1 - b^T m_2) - \pi i m_2^T \Omega m_2 - 2\pi i m_2^T z} \vartheta_{a,b}(z, \Omega)$$

- Basis of the linear space of functions of level N

$$\vartheta_b(z) = \vartheta_{0,b}(z, \Omega/N)$$

$$\vartheta_b(z + m_1 + m_2\Omega) = e^{-\pi i N m_2^T \Omega m_2 - 2\pi i N m_2^T z} \vartheta_b(z)$$

Same factor for all b .

- Quasi-periodicity \Rightarrow map

$$\begin{aligned} \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g) &\rightarrow \mathbb{P}^{N^g-1}(\mathbb{C}) \\ z &\mapsto (\vartheta_b(z))_b \end{aligned}$$

- injective for $N \geq 3$

kernel ± 1 for $N = 2$

ϑ constants for elliptic curves

$$a, b \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}; \quad q = e^{2\pi i\tau}$$

$$\vartheta_{a,b}(0, \tau) = \sum_{n \in \mathbb{Z}} e^{2\pi i((n+a)\tau(n+a)/2 + (n+a)b)} = e^{2\pi iab} \sum_{n \in \mathbb{Z}} (e^{2\pi ib})^n q^{(n+a)^2/2}$$

$$\vartheta_{0,0}(0, \tau) = \sum_{n \in \mathbb{Z}} q^{n^2/2} = 1 + 2q^{1/2} + 2q^2 + 2q^{9/2} + \dots$$

$$\vartheta_{0, \frac{1}{2}}(0, \tau) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2/2} = 1 - 2q^{1/2} + 2q^2 - 2q^{9/2} + \dots$$

$$\vartheta_{\frac{1}{2}, 0}(0, \tau) = \sum_{n \in \mathbb{Z}} q^{(2n+1)^2/8} = q^{1/8} (1 + 2q + 2q^3 + \dots)$$

$$\vartheta_{\frac{1}{2}, \frac{1}{2}}(0, \tau) = 0$$

ϑ constants for ppas

- 16 functions ϑ_i in Ω for $N = 2, z = 0$
- 10 not identically 0
- Igusa modular forms

$$h_{10} = \prod_{10i} \vartheta_i^2 \qquad h_6 = \sum_{60 \text{ certain } i,j,k} \pm(\vartheta_i \vartheta_j \vartheta_k)^4$$

$$h_4 = \sum_{10i} \vartheta_i^8 \qquad h_{12} = \sum_{15} \prod_{6i} \vartheta_i^4$$

- Igusa invariants [Igu62, Str10]

$$j_1 = \frac{h_4 h_6}{h_{10}}, \quad j_2 = \frac{h_4^2 h_{12}}{h_{10}^2}, \quad j_3 = \frac{h_4^5}{h_{10}^2}$$

Computing with theta functions

- 1 Abelian varieties and ϑ functions
- 2 Kummer surfaces and the group law
- 3 Complex multiplication and class polynomials
- 4 Modular polynomials

Circle and Kummer half circle

$$\begin{array}{ccc}
 \mathbb{R}/2\pi\mathbb{Z} & \longrightarrow & C : X^2 + Y^2 = 1 \\
 \begin{array}{c} | \text{-----} | \\ -\pi \qquad \qquad \pi \end{array} & & \begin{array}{c} \text{Circle} \end{array} \\
 z \in \mathbb{R} & \longrightarrow & P = (x = \cos z, y = \sin z) \in \mathbb{A}^2(\mathbb{R}) \\
 -z & \longrightarrow & -P = (x, -y) \\
 \downarrow & & \downarrow \\
 z/\{\pm 1\} & \longrightarrow & x = \cos z \in \mathbb{A}^1(\mathbb{R})
 \end{array}$$

Circle group law

- Neutral element

$$(\cos 0, \sin 0) = (1, 0)$$

- Negation

$$-(x, y) = (\cos(-z), \sin(-z)) = (x, -y)$$

- Addition

$$\cos(z_1 + z_2) = \cos(z_1) \cos(z_2) - \sin(z_1) \sin(z_2)$$

$$\sin(z_1 + z_2) = \sin(z_1) \cos(z_2) + \cos(z_1) \sin(z_2)$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_1 x_2 - y_1 y_2, y_1 x_2 + x_1 y_2)$$

- Duplication on the Kummer half circle $C/\{\pm 1\}$

$$\cos(2z) = 2 \cos^2(z) - 1$$

$$X(2P) = 2X(P)^2 - 1$$



Differential addition

The differential addition of $\pm P$, $\pm Q$ on $C/\{\pm 1\}$ is, given also $\pm(P - Q)$, to compute $\pm(P + Q)$.

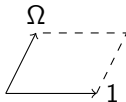
$$\cos(z_1 + z_2) = \frac{\cos^2(z_1) + \cos^2(z_2) - 1}{\cos(z_1 - z_2)}$$

$$X(P + Q) = \frac{X(P)^2 + X(Q)^2 - 1}{X(P - Q)}$$

Elliptic curves and Kummer lines

Theta functions

$$\leftarrow \mathbb{C}/(\mathbb{Z} + \Omega\mathbb{Z}) \rightarrow Y^2 = X^3 + aX + b$$



$$\left(\vartheta_0\left(z, \frac{\Omega}{4}\right), \dots, \vartheta_{3/4}\left(z, \frac{\Omega}{4}\right) \right) \in \mathbb{P}^3 \quad \leftarrow \quad z \in \mathbb{C} \quad \rightarrow \quad (x, y) \in \mathbb{A}^2$$

$$\downarrow$$

$$\downarrow$$

$$\downarrow$$

$$\left(\vartheta_0\left(z, \frac{\Omega}{2}\right), \vartheta_{1/2}\left(z, \frac{\Omega}{2}\right) \right) \in \mathbb{P}^1 \quad \leftarrow \quad z/\{\pm 1\} \quad \rightarrow \quad x \in \mathbb{A}^1$$

Scalar multiplication

Algorithm: Double and add

Input: $P, n > 0$

Output: nP

Write $n = (n_r | n_{r-1} | \dots | n_0)_2$ with $n_r = 1$.

$R \leftarrow P$

for $i = r - 1$ **downto** 0

$R \leftarrow 2R$

if $n_i = 1$

$R \leftarrow R + P$

return R



Scalar multiplication

Algorithm: Montgomery ladder

Input: $P, n > 0$

Output: nP

Write $n = (n_r | n_{r-1} | \dots | n_0)_2$ with $n_r = 1$.

$R_0 \leftarrow P$

$R_1 \leftarrow 2P$

for $i = r - 1$ **downto** 0

if $n_i = 1$

$R_0 \leftarrow R_0 + R_1$

$R_1 \leftarrow 2R_1$

else

$R_1 \leftarrow R_0 + R_1$

$R_0 \leftarrow 2R_0$

return R_0



Addition on Kummer line

[GL09, LR15]

- **Curve parameters**

$$a = \vartheta_0(0, \tau/2) \quad b = \vartheta_{1/2}(0, \tau/2)$$

$$A = \frac{a^2+b^2}{a^2-b^2} \quad B = \frac{a}{b}$$

- **Coordinates**

$$x = \vartheta_0(z, \Omega/2)$$

$$y = \vartheta_{1/2}(z, \Omega/2)$$

- **Doubling**

$$s = (x_P^2 + y_P^2)^2 \quad x_{2P} = s + t$$

$$t = (x_P^2 - y_P^2)^2 A \quad y_{2P} = (s - t)B$$

- **Differential addition**

$$s = (x_P^2 + y_P^2)(x_Q^2 + y_Q^2) \quad x_{P+Q} = (s + t)y_{P-Q}$$

$$t = (x_P^2 - y_P^2)(x_Q^2 - y_Q^2)A \quad y_{P+Q} = (s - t)x_{P-Q}$$

- **Together**

$$4 M + 6 S + 3 m + 8 A$$

- **Montgomery 1987**

$$6 M + 4 S + 1 m + 8 A$$



Kummer surface of p.p.a.s.

- [Gau07], inspired by [CC86]

- ▶ Doubling (x, y, z, t)

$$\begin{aligned} x' &= (x^2 + y^2 + z^2 + t^2)^2 & X &= x' + y' + z' + t' \\ y' &= (x^2 + y^2 - z^2 - t^2)^2 A' & Y &= (x' + y' - z' - t')A \\ z' &= (x^2 + y^2 + z^2 - t^2)^2 B' & Z &= (x' + y' + z' - t')B \\ t' &= (x^2 - y^2 - z^2 + t^2)^2 C' & T &= (x' - y' - z' + t')C \end{aligned}$$

- ▶ Differential addition...

- [GL09]: extension to characteristic 2

- [BCLS14]

- ▶ 72 220 cycles per 256 bit scalar multiplication (Haswell CPU)
- ▶ “constant time” (independent of $\{n_i\}$)

Pairings on the Kummer surface [LR15]

- **Compatible addition**

Given X -coordinates of P, Q, R, S
with $P + Q = R + S$ and $P - Q \neq R - S$,
compute X -coordinate $\pm(P + Q)$.

- ▶ Compute $\{\pm(P + Q), \pm(P - Q)\}$ and $\{\pm(R + S), \pm(R - S)\}$.
- ▶ Intersect to obtain $\pm(P + Q)$.

- **Threeway addition** (simplified presentation)

T a point of order different from 2.

Given X -coordinates of $P, Q, P + T$ and $Q + T$,
compute X -coordinate of $P + Q$ and $P + Q + T$.

- ▶ Compatible addition of $P, Q + T, P + T, Q$ returns $P + Q + T$.
- ▶ Differential addition of Q, T (knowing $Q + T$) returns $Q - T$.
- ▶ Compatible addition of $P, Q, P + T, Q - T$ returns $P + Q$.

- \rightsquigarrow (multi-)scalar multiplication

- \rightsquigarrow **cryptographic pairings**: Weil, Tate, ate, optimal

Computing with theta functions

- 1 Abelian varieties and ϑ functions
- 2 Kummer surfaces and the group law
- 3 Complex multiplication and class polynomials
- 4 Modular polynomials

Complex multiplication of elliptic curves

- Deuring 1941

The endomorphism ring of an elliptic curve is either \mathbb{Z} , or an order

$$\mathcal{O}_D = \left[1, \frac{D + \sqrt{D}}{2} \right]_{\mathbb{Z}}$$

of discriminant $D < 0$ in $K = \mathbb{Q}(\sqrt{D})$:

E with **complex multiplication** by $\mathcal{O}_D / \text{by } D$

- Over \mathbb{C} : usually \mathbb{Z} , sometimes \mathcal{O}_D
- Over \mathbb{F}_p : always \mathcal{O}_D

Complex multiplication of elliptic curves

- **Deuring 1941**

The endomorphism ring of an elliptic curve is either \mathbb{Z} , or an order

$$\mathcal{O}_D = \left[1, \frac{D + \sqrt{D}}{2} \right]_{\mathbb{Z}}$$

of discriminant $D < 0$ in $K = \mathbb{Q}(\sqrt{D})$:

E with **complex multiplication** by $\mathcal{O}_D /$ by D

- Over \mathbb{C} : usually \mathbb{Z} , sometimes \mathcal{O}_D
- Over \mathbb{F}_p : always \mathcal{O}_D
- **Frobenius**: $\pi : (x, y) \mapsto (x^p, y^p)$, fixes $E(\mathbb{F}_p)$
- **Hasse**: $\pi = \frac{t + v\sqrt{D}}{2}$, $\text{Tr}(\pi) = t$, $N(\pi) = \frac{t^2 - v^2 D}{4} = p$

$$\#E(\mathbb{F}_p) = 1 - t + p$$

- **Deuring 1941**: Any (ordinary) curve over \mathbb{F}_p is the reduction of a curve over \mathbb{C} with the same endomorphism ring.

Complex multiplication of complex elliptic curves

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots, \quad q = e^{2\pi i\tau}$$

- $\mathfrak{a} = (\alpha_1, \alpha_2)_{\mathbb{Z}}$ ideal of \mathcal{O}_D with basis quotient $\tau = \frac{\alpha_2}{\alpha_1}$, $\Im(\tau) > 0$
- $j(\mathfrak{a}) := j(\tau)$
 - ▶ Depends only on \mathfrak{a} (modularity)
 - ▶ Depends only on the **ideal class** \mathfrak{a} (quotient)
- Curve with invariant $j(\mathfrak{a})$ has CM by D , there are $h = \# \text{Cl}(\mathcal{O}_D)$

First main theorem of complex multiplication

$$\begin{array}{c}
 \Omega_D = K(j(\mathfrak{a})) \\
 | \\
 K = \mathbb{Q}(\sqrt{D}) \\
 | \\
 \mathbb{Q}
 \end{array}$$

Ω_D = Hilbert class field of K (for D fundamental discriminant)
 = maximal abelian, unramified extension of K

$$\sigma : \text{Cl}(\mathcal{O}_D) \xrightarrow{\cong} \text{Gal}(\Omega_D/K), \quad j(\mathfrak{a})^{\sigma(\mathfrak{b})} = j(\mathfrak{a}\mathfrak{b}^{-1})$$

First main theorem of complex multiplication

$$\begin{array}{c} \Omega_D = K(j(\mathfrak{a})) \\ | \\ K = \mathbb{Q}(\sqrt{D}) \\ | \\ \mathbb{Q} \end{array}$$

Ω_D = Hilbert class field of K (for D fundamental discriminant)
 = maximal abelian, unramified extension of K

$$\sigma : \text{Cl}(\mathcal{O}_D) \xrightarrow{\cong} \text{Gal}(\Omega_D/K), \quad j(\mathfrak{a})^{\sigma(\mathfrak{b})} = j(\mathfrak{a}\mathfrak{b}^{-1})$$

Class polynomial

$$H_D(X) = \prod_{\mathfrak{b} \in \text{Cl}(\mathcal{O}_D)} (X - j(\mathfrak{b}^{-1}))$$

Complex multiplication algorithm

- Fix $D < 0$ and p prime s.t. $p = \frac{t^2 - v^2 D}{4}$
and $N = p + 1 - t$ convenient
- Enumerate the h ideal classes of \mathcal{O}_D :

$$\left(A_i, \frac{-B_i + \sqrt{D}}{2} \right)$$

- Compute over \mathbb{C} the **class polynomial**

$$H_D(X) = \prod_{i=1}^h \left(X - j \left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \in \mathbb{Z}[X]$$

- Find a root \bar{j} modulo p
- Write down the curve $E : Y^2 = X^3 + aX + b$ with

$$c = \frac{\bar{j}}{1728 - \bar{j}}, \quad a = 3c, \quad b = 2c$$

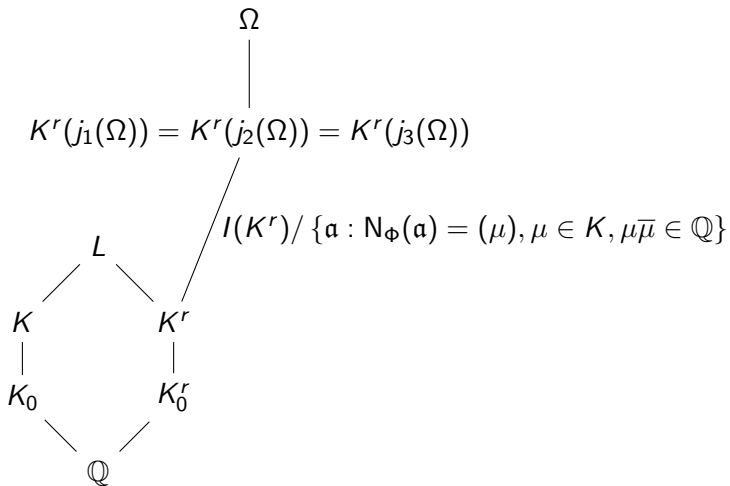
Complexity

- Size of H_D
 - ▶
 - ▶ Degree $h \in O^\sim(\sqrt{|D|})$ [Lit28]
 - ▶ Coefficients with $O^\sim(\sqrt{|D|})$ digits [Sch91, Eng09a]
 - ▶ Total size: $O^\sim(|D|)$
- Evaluation of j : $O^\sim(\sqrt{|D|})$
 - ▶ Precision: $O^\sim(\sqrt{|D|})$ digits
 - ▶ Multievaluation of the “polynomial” j [Eng09a]
 - ▶ Arithmetic-geometric mean for computing ϑ functions [Dup11]

Complexity

- Size of H_D
 - ▶
 - ▶ Degree $h \in O\left(\sqrt{|D|}\right)$ [Lit28]
 - ▶ Coefficients with $O\left(\sqrt{|D|}\right)$ digits [Sch91, Eng09a]
 - ▶ Total size: $O(|D|)$
- Evaluation of j : $O\left(\sqrt{|D|}\right)$
 - ▶ Precision: $O\left(\sqrt{|D|}\right)$ digits
 - ▶ Multievaluation of the “polynomial” j [Eng09a]
 - ▶ Arithmetic-geometric mean for computing ϑ functions [Dup11]
- Total complexity $O(|D|)$ – quasi-linear in the output size [Eng09a]
- Record (with class invariants) [Eng15]
 - ▶ $D = -2\,093\,236\,031$, $h = 100\,000$
 - ▶ precision 264 727 bits, 3 days of computing, 5 GB
- Chinese remainder based approach [BBEL08, ES10]

Class field for p.p.a.s. (dihedral case)



Main algorithm (dihedral case)

- Consider the two CM-types Φ and Φ' .
- Enumerate the class groups and deduce the Ω_i and Ω'_i .
- Evaluate the $\vartheta_{a,b}(\Omega_i^{(')})$ and deduce the $j_k(\Omega_i^{(')})$ [Dup06, ET14b], **quasilinear**.
- Compute the first class polynomial

$$H_1(X) = \prod_{i=1}^h (X - j_1(\Omega_i)) \prod_{i=1}^h (X - j_1(\Omega'_i)) \in \mathbb{Q}[X]$$

- Compute the **Hecke representations** of the algebraic numbers $j_k(\Omega_i)$ with respect to H_1 :

$$\hat{H}_k(X) = \text{polynomial of degree } 2h - 1 \text{ s.t. } j_k(\Omega_i) = \frac{\hat{H}_k(j_1(\Omega_i^{(')}))}{H'_1(j_1(\Omega_i^{(')}))}$$

(roughly **Lagrange interpolation**)

Smaller class polynomials

- Compute factors over K_0^r instead of \mathbb{Q} [ET14b]

$$H_1(X) = \underbrace{\prod_{i=1}^h (X - j_1(\Omega_i))}_{\in K_0^r[X]} \cdot \underbrace{\prod_{i=1}^h (X - i_1(\Omega'_i))}_{\in K_0^r[X]} \in \mathbb{Q}[X]$$

⇒ 4 times smaller

- Compute irreducible factors using class field theory [ET14b]
- Use class invariants [ES16]
 - ⇒ gain constant factor
- Software is available [ET14a]

Computing with theta functions

- 1 Abelian varieties and ϑ functions
- 2 Kummer surfaces and the group law
- 3 Complex multiplication and class polynomials
- 4 Modular polynomials

Isogenies

- **Isogeny** between abelian varieties
= surjective morphism with finite kernel
(compatible with principal polarisation)
- **Applications**
 - ▶ Cryptanalysis: transfer of discrete logarithm
 - ▶ Point counting algorithm SEA on elliptic curves
 - ▶ Class polynomials via Chinese remaindering
 - ▶ Isogeny graphs

Modular polynomials for elliptic curves

- Congruence subgroup: p prime

$$\Gamma^0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : p \mid b \right\}$$

- Modular functions

$$\mathbb{C}_{\Gamma^0(p)} = \mathbb{C}(j, j_p), \quad j_p(\tau) = j(\tau/p)$$

- Modular polynomial

$$\Phi_p(X) = \prod_{M \in \Gamma/\Gamma^0(p)} (X - j_p(M\tau)) \in \mathbb{Z}[X, j]$$

- p -isogenous curves to curve with j -invariant $j(\tau)$
have j -invariant $j_p(M\tau)$.

Evaluation–interpolation [Eng09b]

$$\Phi_p(X) = \prod_{M \in \Gamma/\Gamma^0(p)} (X - j_p(M\tau)) = X^{p+1} + \sum_{i=0}^p c_i(j) X^i, \quad c_i \in \mathbb{Z}[j]$$

- Evaluate $\Phi_p(X, j(\tau_k))$ and obtain the $c_i(\tau_k)$ for many $\tau_k \in \mathbb{H}$.
- Interpolate the c_i .

Evaluation–interpolation [Eng09b]

$$\Phi_p(X) = \prod_{M \in \Gamma / \Gamma^0(p)} (X - j_p(M\tau)) = X^{p+1} + \sum_{i=0}^p c_i(j) X^i, \quad c_i \in \mathbb{Z}[j]$$

- Evaluate $\Phi_p(X, j(\tau_k))$ and obtain the $c_i(\tau_k)$ for many $\tau_k \in \mathbb{H}$.
- Interpolate the c_i .
- Size
 - ▶ $\deg_X \Phi_p = p + 1$
 - ▶ $\deg_j c_i \leq p + 1$
 - ▶ Size of coefficients = floating point precision $\in O^\sim(p)$
 - ▶ $O^\sim(p^3)$
- Complexity $O^\sim(p^3)$ using [Dup11], quasi-linear in output size

• $p = 5$

$$\begin{aligned}\Phi_5(X, j) = & X^6 + (-j^5 + 3720j^4 - 4550940j^3 + 2028551200j^2 - 246683410950j + 1963211489280)X^5 + (3720j^5 + \\ & 1665999364600j^4 + 107878928185336800j^3 + 383083609779811215375j^2 + 128541798906828816384000j + \\ & 1284733132841424456253440)X^4 + (-4550940j^5 + 107878928185336800j^4 - 441206965512914835246100j^3 + \\ & 26898488858380731577417728000j^2 - 192457934618928299655108231168000j + \\ & 280244777828439527804321565297868800)X^3 + (2028551200j^5 + 383083609779811215375j^4 + \\ & 26898488858380731577417728000j^3 + 5110941777552418083110765199360000j^2 + \\ & 36554736583949629295706472332656640000j + 6692500042627997708487149415015068467200)X^2 + \\ & (-246683410950j^5 + 128541798906828816384000j^4 - 192457934618928299655108231168000j^3 + \\ & 36554736583949629295706472332656640000j^2 - 264073457076620596259715790247978782949376j + \\ & 53274330803424425450420160273356509151232000)X + (j^6 + 1963211489280j^5 + 1284733132841424456253440j^4 + \\ & 280244777828439527804321565297868800j^3 + 6692500042627997708487149415015068467200j^2 + \\ & 53274330803424425450420160273356509151232000j + 141359947154721358697753474691071362751004672000)\end{aligned}$$

• [Sch70]

$$X^6 - X^5j^5 + 4Xj + j^6$$

Modular polynomials for abelian surfaces

- PhD thesis [E. Milio 2015](#)
- Congruence subgroup: p prime

$$\Gamma^0(p) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma : p \mid B \right\}$$

- Modular functions

$$\mathbb{C}_{\Gamma^0(p)} = \mathbb{C}(j_1, j_2, j_3, j_{\ell,p}), \quad j_{\ell,p}(\Omega) = j_{\ell}(\Omega/p)$$

Modular polynomials for abelian surfaces

- Modular polynomials

$$\Phi_{1,p}(X) = \prod_{M \in \Gamma/\Gamma^0(p)} (X - j_{1,p}(M\Omega)) \in \mathbb{Q}(j_1, j_2, j_3)[X]$$

$$\Psi_{\ell,p}(X) = \sum_{M \in \Gamma/\Gamma^0(p)} j_{\ell,p}(M\Omega) \frac{\Phi_{1,p}(X)}{X - j_{1,p}(M\Omega)}$$

Hecke representation

- Surfaces (j'_1, j'_2, j'_3) (p, p) -isogenous to given (j_1, j_2, j_3)

$$\Phi_{1,p}(j_1, j_2, j_3, j'_1) = 0$$

$$j'_2 = \Psi_{2,p}(j_1, j_2, j_3, j'_1) / \Phi'_{1,p}(j_1, j_2, j_3, j'_1)$$

$$j'_3 = \Psi_{3,p}(j_1, j_2, j_3, j'_1) / \Phi'_{1,p}(j_1, j_2, j_3, j'_1)$$

Modular polynomials for abelian surfaces

- Quasi-linear complexity

$$O^{\sim}(p^3 d_{j_1} d_{j_2} d_{j_3} N) \stackrel{?}{=} O^{\sim}(p^{15})$$

- $p = 2$
2 MB
- $p = 3$
890 MB

Smaller functions

$$b_i(\Omega) = \frac{\vartheta_{0,b}(\Omega/2)}{\vartheta_{0,0}(\Omega/2)}, \quad b \in \left\{ \begin{pmatrix} 0 \\ 1/2 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} \right\}$$

- Modular functions for $\Gamma(2, 4)$
- Many [symmetries](#)

$$\begin{aligned} D = & 64(b_1^2 b_2^2 b_3^2)(16b_1^4 b_2^4 b_3^4 + 1)(b_1^4 + b_2^4 + b_3^4) \\ & - 32(48b_1^4 b_2^4 b_3^4 + 16b_1^2 b_2^2 b_3^2 + 1)(b_1^4 b_2^4 + b_1^4 b_3^4 + b_2^4 b_3^4) \\ & + 256(b_1^8 b_2^8 + b_1^8 b_3^8 + b_2^8 b_3^8) \\ & + 32(b_1^4 b_2^4 b_3^4)(-24b_1^4 b_2^4 b_3^4 + 80b_1^2 b_2^2 b_3^2 + 13) + 1 \end{aligned}$$

Smaller functions

$$b_i(\Omega) = \frac{\vartheta_{0,b}(\Omega/2)}{\vartheta_{0,0}(\Omega/2)}, \quad b \in \left\{ \begin{pmatrix} 0 \\ 1/2 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} \right\}$$

- Modular functions for $\Gamma(2, 4)$
- Many **symmetries**

$$\begin{aligned} D = & 64(b_1^2 b_2^2 b_3^2)(16b_1^4 b_2^4 b_3^4 + 1)(b_1^4 + b_2^4 + b_3^4) \\ & - 32(48b_1^4 b_2^4 b_3^4 + 16b_1^2 b_2^2 b_3^2 + 1)(b_1^4 b_2^4 + b_1^4 b_3^4 + b_2^4 b_3^4) \\ & + 256(b_1^8 b_2^8 + b_1^8 b_3^8 + b_2^8 b_3^8) \\ & + 32(b_1^4 b_2^4 b_3^4)(-24b_1^4 b_2^4 b_3^4 + 80b_1^2 b_2^2 b_3^2 + 13) + 1 \end{aligned}$$

- $p = 3$: 175 kB (instead of 890 MB)
- $p = 5$: 200 MB
- $p = 7$: 30 GB



Modular polynomials for surfaces with real multiplication

- Work in progress [MR16]
- β -isogenies for

$$p = N_{K_0/\mathbb{Q}}(\beta), \quad \beta \gg 0$$

- Certain cyclic p -isogenies
- Degree of modular polynomials $O(p)$ instead of $O(p^3)$
- Complexity $O^\sim(p^4)$ instead of $O^\sim(p^{15})$ (?)
- $K = \mathbb{Q}(\sqrt{2})$, $p = 97$: 270 MB

Conclusion

ϑ functions are everywhere!

- Group law of (principally polarised) abelian varieties
- Construction of p.p.a.v.
- Maps between p.p.a.v.





Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter.

Computing Hilbert class polynomials.

In Alf van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory — ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, page 282–295, Berlin, 2008. Springer-Verlag.



Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe.

Kummer strikes back: new DH speed records.

Preprint, <http://eprint.iacr.org/2014/134.pdf>, 2014.



D. V. Chudnovsky and G. V. Chudnovsky.

Sequences of numbers generated by addition in formal groups and new primality and factorization tests.

Advances in Applied Mathematics, 7:385–434, 1986.



Régis Dupont.

Moyenne arithmético-géométrique, suites de Borchardt et applications.

Thèse de doctorat, École polytechnique, Palaiseau, 2006.



 Régis Dupont.

Fast evaluation of modular functions using Newton iterations and the AGM.

Mathematics of Computation, 80(275):1823–1847, 2011.

 Andreas Enge.

The complexity of class polynomial computation via floating point approximations.

Mathematics of Computation, 78(266):1089–1107, 2009.

 Andreas Enge.

Computing modular polynomials in quasi-linear time.

Mathematics of Computation, 78(267):1809–1824, 2009.


 Andreas Enge.

cm — *Complex multiplication of elliptic curves*.

INRIA, 0.2.1 edition, March 2015.

Distributed under GPL v2+, <http://cm.multiprecision.org/>.

 Andreas Enge and Andrew V. Sutherland.

 Invariants by the CRT method.

Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory — ANTS-IX*, volume 6197 of *Lecture Notes in Computer Science*, page 142–156, Berlin, 2010. Springer-Verlag.



Andreas Enge and Marco Streng.

Schertz style class invariants for quartic CM fields.
In preparation, 2016.



Andreas Enge and Emmanuel Thomé.

cmh — *Complex multiplication of abelian surfaces*.
INRIA, 1.0 edition, March 2014.
Distributed under GPL v3+, <http://cmh.gforge.inria.fr/>.



Andreas Enge and Emmanuel Thomé.

Computing class polynomials for abelian surfaces.
Experimental Mathematics, 23(2):129–145, 2014.



Pierrick Gaudry.

Fast genus 2 arithmetic based on theta functions.

Journal of Mathematical Cryptology, 1(3):243–265, 2007.



Pierrick Gaudry and David Lubicz.

The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines.

Finite Fields and Their Applications, 15:246–260, 2009.



Jun-Ichi Igusa.

On Siegel modular forms of genus two.

American Journal of Mathematics, 84:175–200, 1962.



J. E. Littlewood.

On the class-number of the corpus $P(\sqrt{-k})$.

Proceedings of the London Mathematical Society, 27:358–372, 1928.



David Lubicz and Damien Robert.

A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties.

Journal of Symbolic Computation, 67:68–92, 2015.



Enea Milio and Damien Robert.

Modular polynomials and real multiplication.

arXiv preprint, 2016.





L. Schläfli.

Beweis der Hermiteschen Verwandlungstafeln für die elliptischen Modulfunktionen.

Journal für die reine und angewandte Mathematik, 72:360–369, 1870.



René Schoof.

The exponents of the groups of points on the reductions of an elliptic curve.

In G. van der Geer, F. Oort, and J. Steenbrink, editors, *Arithmetic Algebraic Geometry*, pages 325–335, Boston, 1991. Birkhäuser.



Marco Streng.

Complex multiplication of abelian surfaces.

Proefschrift, Universiteit Leiden, 2010.

原始ピタゴラス数から生ずる 三項指数型不定方程式について

宮崎 隆史
(群馬大学)

2015年 12月 14日

1 導入

次の不定方程式を考える：

$$(abc) \quad a^x + b^y = c^z.$$

ここで x, y, z は未知の自然数である。以下では、固定された自然数の三つ組み (a, b, c) について方程式 (abc) を考える。すると、特に、方程式 (abc) の各項 a^x, b^y, c^z に現れる素因数の集合は有限集合である。このようなものは単数方程式と呼ばれ、ディオファントス近似の一般論から、その解の個数、すなわち (abc) を満たす自然数の三つ組み (x, y, z) の個数の有限性が得られることが知られている。さらに、対数の一次形式に関する Baker の理論から、解の大きさ、すなわち $\max\{x, y, z\}$ の上界を得ることが出来る。ここで、 a, b, c のうちに 1 に等しいものがある場合には、それに対応する指数変数に制限が無いが、これは考えないことにしている。

方程式 (abc) については多くの研究があるが、そのほとんどは様々な三つ組み (a, b, c) について方程式 (abc) の解を決定するものである。例として、以下の場合を挙げておく：

$$\begin{aligned} 3^x + 4^y &= 5^z, \\ (m^2 - 1)^x + (2m)^y &= (m^2 + 1)^z \quad (m \text{ は正の偶数}), \\ (tb - 1)^x + b^y &= (tb + 1)^z \quad (t, b \text{ は自然数}), \\ F_n^x + F_{n+1}^y &= F_{2n+1}^z \quad (n \text{ は } 3 \text{ 以上の整数}). \end{aligned}$$

ここで、 F_j は j 番前のフィボナッチ数である。これらの解は既に決定されていることを注意する（それぞれ [Si], [Lu], [MiToYu], [Mi4] を参照）。

本稿では、方程式 (abc) の研究において最も興味が注がれてきた問題に焦点を当てる。1956 年に Jeśmanowicz [Je] は次の問題を提起している。

Jeśmanowicz 予想. a, b, c を, $a^2 + b^2 = c^2$ を満たす様などの二つも互いに素な自然数とする. このとき方程式 (abc) は自明な解 $(x, y, z) = (2, 2, 2)$ しか持たない.

この問題に対する研究は数多くあるが, 一未だ般には解決されていない. 予想の条件を満たす三つ組み (a, b, c) は原始ピタゴラス数と呼ばれ, 良く知られているように, 次の様にパラメータ表示される (以下, 一般性を失うことなく, b を偶数とする):

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

ここで, m, n は偶奇が異なる互いに素な自然数である. 従って, Jeśmanowicz 予想は次の様に述べることも出来る:

Jeśmanowicz 予想. m, n は互いに素な自然数で, $m > n$, $m \not\equiv n \pmod{2}$ を満たすとする. このとき, 次の方程式

$$(mn) \quad (m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z \quad x, y, z : \text{自然数}$$

は, 自明な解 $(x, y, z) = (2, 2, 2)$ しか持たない.

Jeśmanowicz 予想は, m, n (あるいは a, b, c) に関する様々な条件下で, 正しいことが証明されている. そのうちのいくつかを以下に列挙する:

- (i) $m = 2, n = 1$ ([Si]).
- (ii) $(m, n) = (3, 2), (4, 3), (5, 4), (6, 5)$ ([Je]).
- (iii) $n = 1$ ([Lu]).
- (iv) $n = m - 1$ ([De]).
- (v) $mn \equiv 2 \pmod{4}$, $m^2 + n^2$ が素数ベキ ([Le]).
- (vi) $m \equiv 2, n \equiv 3 \pmod{4}$, $m > 81n$ ([Le2]).
- (vii) $m \equiv 1, n \equiv 6 \pmod{8}$ または $m \equiv 5, n \equiv 2 \pmod{8}$ ([Ca]).
- (viii) $m \equiv 4 \pmod{8}, n \equiv 7 \pmod{16}$ または $m \equiv 7 \pmod{16}, n \equiv 4 \pmod{8}$ ([Mi]).
- (viii) $a \equiv \pm 1 \pmod{b}$ または $c \equiv \pm 1 \pmod{b}$ ([Mi3]).
- (X) $a \equiv \pm 1 \pmod{b/2^{\nu_2(b)}}$ または $c \equiv \pm 1 \pmod{b/2^{\nu_2(b)}}$ ([MiYuWu]).
- (Xi) $n = 2$ ([Te]).

本稿の研究目的は, 上記における [Lu] や [Te] の様に, 「 n にのみ条件を付けて」 Jeśmanowicz 予想が正しいことを証明することである. 主定理は以下である.

定理 1. 法 4 で 3 と合同となる任意に固定された n に対して, Jeśmanowicz 予想は高々有限個の m を除いて正しい. すなわち, n だけによって定まる定数 C_1 が存在して, $n \equiv 3 \pmod{4}$ かつ $m > C_1$ である限り, Jeśmanowicz 予想は正しい.

後にも触れるが、定理 1 に述べられている定数 C_1 は巨大である。故に、各 n について m が C_1 以下の場合に予想を示すことは（計算機の事情で）難しい。次に挙げる二つの定理はそれを補完するものになる。

以下では、素数 p に対して、 $\nu_p(A)$ で整数 $A \neq 0$ の素因数分解に現われる p の指数を表すことにする。

定理 2. n が法 4 で 3 と合同となる場合を考える。 $\beta = \nu_2(n+1)$ と置く。 β は偶数、または、 $\beta = 3$ を仮定する。さらに、 n は 4^{e_2+1} を超えないと仮定する。ここで、 e_2 は次の様に定義される：

$$e_2 = \begin{cases} \max\{\nu_2(m), 2\} & (\beta \neq 3 \text{ のとき}), \\ \max\{\nu_2(m), 3\} & (\beta = 3 \text{ のとき}). \end{cases}$$

このとき、 n だけによって定まる定数 C_2 が存在して、 $m > C_2$ である限り、Jeśmanowicz 予想は正しい。

定理 3. n が法 4 で 3 と合同となる場合を考える。 β を定理 2 と同様に定義する。

(i) まず、次の不等式を仮定する：

$$3^{\nu_3(n)} \cdot 5^{\nu_5(n)} \geq 2^{s(n)} \sqrt{n}.$$

ここで $s(n)$ は次の様に定義される：

$$s(n) = \frac{\log n}{22 \log(n^{13} - n^4) + 42 \log 2} \left(< \frac{1}{286} \right).$$

さらに、 β は偶数である、または、次の不等式を仮定する：

$$3^{\nu_3(n)} \cdot 5^{\nu_5(n)} \geq \frac{\delta}{2^{e_3}} n.$$

ここで e_3, δ は以下の様に定義される：

$$e_3 = \max \left\{ \nu_2(m) + 1, \frac{\beta + 3}{2}, 3 \right\},$$

$$\delta = \begin{cases} 3^{1/13} & (n \text{ が } 15 \text{ と互いに素なとき}), \\ 31^{1/17} & (n \text{ は } 3 \text{ で割り切れないが, } 5 \text{ では割り切れるとき}), \\ 19^{1/11} & (n \text{ が } 15 \text{ で割り切れるとき}). \end{cases}$$

このとき、 n だけによって定まる定数 C_3 が存在して、 $m > C_3$ である限り、Jeśmanowicz 予想は正しい。

(ii) まず、次の不等式を仮定する：

$$\max_{q \in \{3, 5\}} q^{\nu_q(n)} \geq 1534^{3/2} t(n) \sqrt{n} (\log n)^{3/2}.$$

ここで $t(n)$ は次の様に定義される :

$$t(n) = \sqrt{\frac{1}{1534} + \left(1 + \frac{4}{n}\right) \log\left(1 + \frac{n^2}{6n+9}\right)} \frac{\log\left(1 + \frac{n^2}{6n+9}\right)}{(\log n)^{3/2}} \quad (< 1).$$

さらに, β は偶数である, または, 次の不等式を仮定する :

$$3^{\nu_3(n)} \cdot 5^{\nu_5(n)} \geq \frac{\delta}{2e_3} n.$$

このとき, m には無条件で Jeśmanowicz 予想は正しい.

上記の定理 1~3 について, いくつかの注意をする.

まず, 定理において現われる定数 C_1, C_2, C_3 は, いずれも n の関数として明示的に与えることが出来る. 例えば, 以下の様に選ぶことが出来る :

$$\begin{aligned} C_1 &= n^{\max\{7 \cdot 10^{20}, 4000(\log \log n)^2\}}, \\ C_2 &= \max\{56n, \sqrt{|n^e - n^2|}\}, \quad e = \frac{23 \log 2}{11 \log(4^{e_2+1}/n)}, \\ C_3 &= 56n. \end{aligned}$$

特に, C_2 は, n が仮定された上限 4^{e_2+1} に近くなるにつれて, 大きくなるのがわかる.

定理 1 について: n に課せられる条件は, n の取りうる値の四分の一を指定している. そこで「有限個の m を除いて」を, (無限という立場からなら) 無視出来るぐらい小さいものであると考えることにすると, “Jeśmanowicz 予想の四分の一はほとんど解けた” と言ってもいいだろう.

定理 2 について: すぐに導かれる帰結として, 以下のいずれの場合にも, Jeśmanowicz 予想は高々有限個の m を除いて正しい :

$$\begin{aligned} n &= 3, 7, 11, 15, 19, 23, 27, 35, 39, 43, 47, 51, 55, 59, 63, \\ &71, 87, 103, 119, 135, 151, 167, 183, 199, 215, 231, 247. \end{aligned}$$

実際に, これらを含めた (余り大きくない) 具体的な n の値に対して, m には無条件で Jeśmanowicz 予想は正しいことが証明できる (最終節の系 1 を参照).

定理 3 について: n の素因数分解において, 3 または 5 がたくさん現れれば, Jeśmanowicz 予想は正しいことがわかる. 例えば, 素因数分解に 3 または 5 しか現れない n を考えることで, 予想が成立するような n の “無限族” を与えることが出来る (最終節の系 2 を参照). (筆者は, 講演時には定理 1 を主定理として紹介したが, 理論的に最も深い部分はこの無限族を与えたことだと考えている.)

2 定理の証明の概要

一般に、方程式 (mn) の様にパラメータを含む不定方程式は、良く知られている既知の手法や初等的なものだけで扱うことが困難な（あるいは困難であると思われる）場合には、その方程式を Baker 理論の様な一般論だけで解決することが出来ないことは多分にある。いま、Jeśmanowicz 予想の様に、解の一意性を問うものだけを考えることにする。すると、「もし非自明な解が存在した場合には必ず矛盾が見つかることが出来る」の証明が成されれば良いことになる。方程式 (abc) においては、既に、Baker による対数一次形式の理論から解の大きさの上限評価は可能である：

$$(1 \leq) \quad x, y, z < C.$$

ここで、右辺は考えている方程式によって定まる絶対定数である。しかしながらこれで問題が解けるということでは決してない。実際、 C は方程式の情報に依るのであるから（多くの場合、パラメータの増加関数である）。よって、上記から矛盾を導くことは出来ない。その主たる原因は、括弧付で記された上記不等式の左辺の下限（これは単純に解が自然数であることから従う）が良いものでないからである。

そこで重要となるのが、矛盾を導くために都合が良い、言い換えると、下からの良い評価が期待される様な、(方程式の解から) 構成される“量”を見つけることである。以下、それを Δ と記すことにする。より詳しく書けば次のことを期待するのである：まず、 Δ は解から構成されるのだから、Baker 理論等の一般論を用いて、その上限を見つけることが出来るだろう。それを U とする。また、期待される良い下限を L とすれば、不等式

$$L < \Delta < U$$

が成立する。一方で、もし、反対側の不等式 $L > U$ が示されれば、矛盾を得たことになる。

話を Jeśmanowicz 予想に戻すと、 n を固定する立場の場合には、 $\Delta = \Delta(x, y, z)$ としては、解 x と z の差が選ばれる：

$$\Delta = |x - z|.$$

この量がゼロになることと解が自明解であることは同値であることが知られている。定理の証明は、大きく分けて二つに分かれるが、そのいずれにおいても、不等式

$$L(m, n) < \Delta < U(m, n)$$

が、“非自明な解”について成立し、一方では、 m が n に比べて十分大きい時には、

$$L(m, n) > U(m, n)$$

が成立することが示される。後にも触れるが、「 n を固定する立場」では、 L として自明なものしか採用することが出来ない。そのため、上述した議論が上手く進む為には、相当に良い U の評価が必要になる。その為、定理の証明においては、[Mi4] で示されたガウスの整数環の理論を用いた手法を

使う。加えて、 n の素因数に特別な制限を置くことで、その手法から得られる U の改良もされる。

3 解の偶数性

Jeśmanowicz 予想の研究においては、方程式 (mn) の解 x, y, z の整除性、特に偶奇性を調べることは極めて重要である。それは、「予想が正しければ解はすべて偶数となる」ことに起因している。以下に、解の偶数性が成り立つ為の一つの十分条件を挙げる。

補題. $m \equiv 0 \pmod{4}$ かつ $n \equiv 3 \pmod{4}$ を仮定する。 (x, y, z) を方程式 (mn) の解とする。このとき、 x, y は共に偶数である。

この補題は、方程式 (mn) を法 $4, m-n, m+n$ で考察することに加えて、平方剰余の補充法則を用いた Jacobi 記号の計算を行うことで証明される（これらの証明については、[Mi2] または [Mi6] を参照）。

定理の証明は以下の二つの場合に分けられる：

- $m \equiv 0 \pmod{4}$ かつ $n \equiv 3 \pmod{4}$.
- $m \equiv 2 \pmod{4}$ かつ $n \equiv 3 \pmod{4}$.

前者では、補題3から、 x, y の偶数性が保障される。また、既に知られていることとして、後者の場合には、解 y が1より大ならば、 $x = y = z = 2$ となることが（初等的に）示されている（[Le2] 参照）。故に、 $y = 1$ なる特殊な場合を考えればよいことになる。まとめると、以下の二つの場合を考察することになる：

- x, y が共に偶数,
- $y = 1$.

次節では、前者の場合に得られる解の上限について論じる。

4 解の上限評価

ここでは、 x, y が偶数となる解の上限評価について述べる。いま、 (x, y) を方程式 (mn) の解とし、 x, y の両方が偶数である仮定する。すると、方程式 (mn) の左辺は、次の様に分解できる：

$$(a^{x/2} + b^{y/2}\sqrt{-1}) \cdot (a^{x/2} - b^{y/2}\sqrt{-1}).$$

これら二つの因子は共にガウス整数である。なおかつ、ガウスの整数環上で互いに素である。方程式 (mn) の右辺は (整数の) z 乗だから、上記の二因子のいずれもガウスの整数の z 乗の形をしていることがわかる。特に、

$$(*) \quad a^{x/2} + b^{y/2}\sqrt{-1} = w^z.$$

ここで、 w はあるガウス整数である。この表示式から解 x, y, z についていくつかの情報を引き出すことが出来る。

[Mi4] では、(*) の左辺の実部と虚部を w の情報で書き下し、そこから得られる等式の両辺において適当な素数 (特に 2) の現れる回数を精密に数え上げるにより、かなり強い解の上限を得ている (さらに、フェルマーの方程式を一般化した方程式 ([Be] 参照) に関する既知の研究成果も多分に用いられていることにも言及しておく)。それを我々の場合に適用すると以下の補題が得られる：

補題 4.1. (x, y, z) を、 x, y, z のすべてが偶数である様な方程式 (mn) の解とする。

(i) 次の不等式が成り立つ：

$$y \leq \frac{\log(4c)}{\log 2^{\nu_2(m)+1}}.$$

(ii) n は少なくとも 2, 3, 5 のいずれか一つで割り切れると仮定する。すると、 $y = 2$ 、または、次の不等式が成り立つ：

$$y \leq \frac{\log(\delta_1^2 c)}{\log \prod_{q \in S_1} q^{\nu_q(r)+\nu_q(n)}}.$$

ここで、 S_1 は集合 $\{2, 3, 5\}$ と n の素因数全体の集合の共通部分であり、 δ_1 は次の様に定義される：

$$\delta_1 = \begin{cases} 2 & (S_1 \text{ が } 2 \text{ を含むとき}), \\ 1 & (S_1 \text{ が } 2 \text{ を含まないとき}). \end{cases}$$

補題 4.2. (x, y, z) を、 x, y の両方が偶数かつ z が奇数となる様な方程式 (mn) の解とする。このとき、 $y > 2$ ならば、次の不等式が成り立つ：

$$y \leq \frac{\log(\delta_2^2 c)}{\log(2^{\nu_2(m)+1} \prod_{q \in S_2} (q^{\nu_q(r)+\nu_q(n)}))}.$$

ここで、 S_2 は集合 $\{3, 5\}$ と n の素因数全体の集合の共通部分であり、 δ_2 は次の様に定義される：

$$\delta_2 = \prod_{q \in S_2} q^{\nu_q(z)}.$$

上記補題において現れた素数 3 と 5 は、次の様な性質を持っている：素数 q に対して、次の命題：

$X^2 + Y^2 \equiv A^2 \pmod{q}$ ならば X または Y が q で割り切れる。

が, q で割り切れない任意の整数 A に対して成り立つ. 実際, A は,

$$A^2 \equiv \begin{cases} 1 \pmod{3} & (q = 3 \text{ のとき}), \\ \pm 1 \pmod{5} & (q = 5 \text{ のとき}) \end{cases}$$

を満たすことから確かめることが出来る. この性質が補題 4 の証明では重要な役割を果たす. さらにいうと, この素数 3 と 5 は, $y = 1$ の場合を扱う際に Δ の良い下界を得ることに役に立つ (補題 9.2 参照).

5 三項間の非自明な評価

ここでは, 定理 1 を証明する際に, Δ の良い上限を得る為に必要になることを述べる. 次の補題は, 方程式 (mn) の三項 a^x, b^y, c^z はどの二つもあまり大きさが変わらないことを示している.

補題 5. (x, y, z) を, x, y の両方が偶数である様な方程式 (mn) の解とする. このとき, 絶対定数 $C > 0$ が存在して, 以下の不等式が成り立つ:

$$\min\{a^x, b^y\} > \frac{2}{\pi^2} c^{z - C \log z}.$$

この補題の証明は, 関係式 (*) と Baker の対数一次形式の理論を使って示される. いま簡単のために w は複素平面の第一象限に属する場合だけ考える:

$$w = c^{1/2}(\cos \theta + i \sin \theta).$$

ここで, θ は $0 < \theta < \pi/2$ を満たす実数である. すると, ド・モアブルの定理から,

$$\{|\operatorname{Re} w^z|, |\operatorname{Im} w^z|\} = \{c^{z/2} |\cos(z\theta)|, c^{z/2} |\sin(z\theta)|\}.$$

三角関数の値に関する初等的な考察から, 次の不等式が成り立つ:

$$\min\{|\cos(z\theta)|, |\sin(z\theta)|\} \geq \frac{\sqrt{2}}{\pi} |2z\theta - j\pi|.$$

ここで, j は $|2z\theta - j\pi|$ が最小となる整数である (証明は, 両辺が $X = z\theta$ の関数として周期 $\pi/2$ を持つことを利用する). 重要なことは, この右辺が, 対数の一次形式で表現されることである. 実際, \log で対数の主値を表すことにすると, $\log(-1) = \pi$ であり,

$$\gamma = \cos(2\theta) + i \sin(2\theta)$$

と置くと, $\log \gamma = 2\theta$ なので, 次の不等式が成り立つ:

$$\min\{|\cos(z\theta)|, |\sin(z\theta)|\} \geq \frac{\sqrt{2}}{\pi} |z \log \gamma - j \log(-1)|.$$

この右辺を下から評価するために Baker の理論が適用され、補題の不等式が得られる（実際には、絶対値の中身が消えないことを確認する必要があるが、それは例えば、 γ が 1 のべき根でないことから分かる）。より正確には、次の不等式が成り立つ様な絶対定数 $C > 0$ が存在する：

$$\log |z \log \gamma - j \log(-1)| > -C (\log |w|) \log \max\{z, j\}.$$

ここで、因子 $\log |w|$ は γ の絶対対数高さと呼ばれる量である。この不等式と (j の定義からすぐに従う) 評価 $j \leq z$ を合わせると、補題の証明が成される。

6 Δ の上限評価

Δ を評価する際に、補題 4.5 を使用することで、次が得られる：

補題 6. (x, y, z) を、 x, y の両方が偶数である様な方程式 (mn) の解とする。

(i) $x < z$ を仮定する。すると次の不等式が成り立つ：

$$\Delta < 5C \log z.$$

さらに、以下の不等式が成り立つ：

$$\begin{aligned} \Delta &< \frac{\log b}{2 \log c} y + \frac{\log 2}{2 \log c} - 1 && (z \text{ が偶数であるとき}), \\ \Delta &< \frac{\log b}{\log c} y + \frac{\log 2}{\log c} - x && (z \text{ が奇数であるとき}). \end{aligned}$$

(ii) $x > z$ を仮定する。すると以下の不等式が成り立つ：

$$\begin{aligned} \Delta &< \frac{\log(4c)}{\log c} \frac{\log b^2}{\log a} \frac{\log(c/a)}{\log 2^{\nu_2(m)+1}} && (z \text{ が偶数であるとき}), \\ \Delta &< \frac{2 \log(c/a)}{\log 3} && (z \text{ が奇数であるとき}). \end{aligned}$$

(i) における最初の Δ の上限評価について少し論じてみる。まず、補題 5 から、次の不等式が成り立つ：

$$x > 2 \cdot \frac{(z/2 - C \log z) \log c - \log \pi}{\log a}.$$

これと自明な不等式 $c > a$ と合わせて考えると

$$\begin{aligned}\Delta = z - x &< z - 2 \cdot \frac{(z/2 - C \log z) \log c - \log \pi}{\log a} \\ &= \frac{2C \log c}{\log a} \log z - \frac{\log c - \log a}{\log a} z + \frac{2 \log \pi}{\log a} \\ &< \frac{2C \log c}{\log a} \log z + \frac{2 \log \pi}{\log a}.\end{aligned}$$

となり、これから主張された不等式が得られるが、その評価の途中で z の一次式の部分が消えて z の対数が残った点が重要になる。

7 Δ の下限評価

Δ の下限は、前述した様に、自明なものしか見つけることができない。次の補題は、方程式 (mn) を法 m で考察することでただちに得られる。

補題 7. (x, y, z) を、 x は偶数で、 $y > 1$ となる様な方程式 (mn) の解とする。このとき、 $\Delta > 0$ ならば、次の不等式が成り立つ：

$$\Delta > \frac{\log m}{\log n}.$$

8 $y > 1$ となる場合

$y > 1$ となる非自明解が存在しないことを証明しよう。いま、 (x, y, z) を非自明解とすると、 $\Delta > 0$ となる。このとき、 x, y の両方が偶数であるとしてよいことを思い出しておく。ここでは簡単のために、 z が偶数である場合だけを考える。

まず、 $\Delta = z - x$ の場合を考える。補題 6 の (ii) から、次の不等式が成り立つ：

$$\Delta < \frac{\log(4c)}{\log c} \frac{\log b^2}{\log a} \frac{\log(c/a)}{\log 2^{\nu_2(m)+1}}.$$

右辺は複雑に見えるが、定数と $\log(c/a)$ の積として上から評価することが出来る。この左辺が 1 以上であることを考えれば、 $\log(c/a)$ がある程度大きくならなければいけないことが分かる。それは a, c がある程度離れていることを意味し、 m, n の言葉では、 m/n があまり大きくない（特に有界）ことが分かる。よって、 m/n がある程度大きい場合には、 $z > x$ となることは無いことが分かった。

次に、 $\Delta = x - z$ の場合を考える。補題 4.1 の (i)、補題 6 の (i) および補題 7 から、以下の不等式を得る：

$$\frac{\log m}{\log n} < \Delta < 5C \log z < C'(\log \log m)^2 \quad (C' : \text{絶対定数} > 0).$$

ここで、 z が y に比べて余り無い事実を用いている（例えば、補題 5 から示される）。 m が n に比べて十分に大きければ、上記の不等式において、最左辺が最右辺より大となることが分かる（これで定理 1 の証明が成された）。同様に（といっても、もう少し複雑だが）、定理 2,3 の証明は、補題 6 の (ii) の Δ の上限評価と補題 7 を用いて成される。大雑把に書くと、次の様な不等式が得られる：

$$\frac{\log m}{\log n} < \Delta < \frac{\log m}{\log n'}.$$

ここで、 n' は、 m が 2 でたくさん割り切れるか、あるいは n が 3 または 5 でたくさん割り切れる場合に、大きくなる数である。 $n' > n$ が成り立つ、すなわち上記の不等式が成り立たない程度に「たくさん割り切れること」を意味する不等式が定理 2,3 の中で必要になる。

9 $y = 1$ となる場合

ここでは、方程式 (mn) において、 $y = 1$ とした方程式

$$(y1) \quad (m^2 - n^2)^x + 2mn = (m^2 + n^2)^z \quad x, z : \text{自然数}$$

に焦点を当てる。定理の証明には上記の方程式が解を持たない十分条件が必要になる。まず、Baker 理論が非常に良い上限評価を与える：

補題 9.1. (x, y, z) を方程式 (y1) の解とする。このとき次の不等式が成り立つ：

$$x < 1534 \log c.$$

この補題の証明については、[Mi5] で解説してあるので詳しくはそちらを参照されたい。

補題 9.1 から、 m/n がある程度大きい場合には、方程式 (y1) は解を持たないことがわかる。実際、 $\Delta = x - z (> 0)$ である事がすぐにわかり、自明な不等式 $c^z > a^x$ と合わせて考えると以下の不等式を得る：

$$\Delta < x - \frac{\log a}{\log c} x = \frac{\log(c/a)}{\log c} x < 1534 \log(c/a).$$

Δ は 1 以上なので、6 節で考察した様に、上記は m/n が有界であることを示す ($< 56 = C_3$).

さらに、前述した様に、 n が $q \in \{3, 5\}$ でたくさん割り切れるときには、方程式 (y1) を n を割り切る q の最大ベキを法として考察することによって、

Δ の下からの良い評価が得られる．それと補題 9.1 を組み合わせることで次のことが証明される：

補題 9.2. q は 3 または 5 であるとするとき，次の不等式を仮定する：

$$n_{(q)} > 1534 \sqrt{n + 1534(n+4) \log \left(1 + \frac{n^2}{6n+9}\right) \log \left(1 + \frac{n^2}{6n+9}\right)}.$$

このとき方程式 (mn) は $y = 1$ となる解を持たない．

この補題の良い点は，(補題 9.1 に比べると) m に何ら条件を課していないことである．この点が定理 3 の証明に効いてくるのである．

10 関連するその他の結果

定理 1~3 では， n が法 4 で 3 と合同である場合を考えたが，それは補題 2 が利用できるからである．しかしながら，[Te], [MiTe] で示されたように， n が法 4 で 2 と合同である（非常に特殊な）場合にも定理 1~3 と同様の結果を証明することが出来る．[Te], [MiTe] のわずかな改良と，補題 9.2 のアイデアを組み合わせることで，次の定理を証明することが出来る（詳しくは，[Mi6] を参照）．

定理 4. n が法 4 で 2 と合同となる場合を考える． $n/2$ の無平方部分が素数である，または， $n/2$ の無平方部分が法 8 で 1 と合同となる素因数を持たない，と仮定する．このとき， n だけによって定まる定数 C_4 が存在して， $m > C_4$ である限り，Jeśmanowicz 予想は正しい．さらに，

$$\max_{q \in \{3,5\}} q^{\nu_q(n)} \geq 1534^{3/2} \sqrt{n} (\log n)^{3/2}$$

が成り立つならば， m には無条件で Jeśmanowicz 予想は正しい．

ここで， C_4 は C_3 とほぼ同じ大きさであることに注意する．

定理 1~4 を使うことで以下の系を証明することが出来る（系 1 では，[Te], [MiTe] で扱われた n の値は除いている）．

系 1. n が次に挙げる値と一致する場合には，Jeśmanowicz 予想は正しい．

3, 7, 11, 15, 19, 23, 27, 35, 39, 43, 47, 51, 55, 59, 63,
71, 75, 87, 103, 106, 110, 114, 118, 119, 122, 126,
130, 134, 135, 138, 142, 146, 150, 151, 154, 158,
162, 166, 167, 174, 175, 178, 182, 183, 186, 190,
194, 195, 198, 199, 202, 206, 210, 214, 215, 218,
222, 226, 230, 231, 234, 242, 243, 247, ...

系 2. n が次に挙げる値と一致する場合には, Jeśmanowicz 予想は正しい.

$$3^{2k+1}, 15^{2k+1}, 2 \cdot 3^k, 2 \cdot 5^k, 2 \cdot 15^k.$$

ここで k は任意の非負整数である.

本稿の最後に, 一つの問題を提起しよう. 上記の系によって, 多くの具体的な n の値に対して Jeśmanowicz 予想を証明することが出来た. 当然, これ以降の研究では, 扱うことの出来なかつた値について考察をすべきだが, その中で最も小さい値 (かつ証明が出来そうなもの) は 31 である. 実際, $n = 31$ については, $\beta = \nu_2(n+1) = 5$ かつ 31 は 3, 5 の両方で割り切れな. しかしながら, 定理 1 によって, m は有限の場合を考えればよい. 特に, (Baker 理論から) 解の大きさも有限である. この状況を厳密に記せば次の問題が見つかる:

問題. 次の方程式を解くこと:

$$(m^2 - 31^2)^x + (62m)^y = (m^2 + 31^2)^z \quad x, y, z : \text{自然数.}$$

ここで, m は自然数で, 以下の条件を満たす:

$$31 < m < 10^{10^{21}}, m \equiv 0 \pmod{2}, m \not\equiv 0 \pmod{31}.$$

REFERENCES

- [Be] F. Beukers, *The Diophantine equation $Ax^p + By^q = Cz^r$* , Duke Math. J. **1** (1998), 61–88.
- [Ca] Z.-F. Cao, *A note on the Diophantine equation $a^x + b^y = c^z$* , Acta Arith. **91** (1999), 85–93.
- [De] V.A. Dem'janenko, *On Jeśmanowicz' problem for Pythagorean numbers*, Izv. Vyssh. Ucebn. Zaved. Mat. **48** (1965), 52–56 (in Russian).
- [Je] L. Jeśmanowicz, *Several remarks on Pythagorean numbers*, Wiadom. Mat. **1** (1955/56), 196–202 (in Polish).
- [Le] M.-H. Le, *A note on Jeśmanowicz conjecture*, Colloq. Math. **69** (1995), 47–51.
- [Le2] M. -H. Le, *On Jeśmanowicz conjecture concerning Pythagorean numbers*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), 97–98.
- [Lu] W. T. Lu, *On the Pythagorean numbers $4n^2 - 1$, $4n$ and $4n^2 + 1$* , Acta Sci. Natur. Univ. Szechuan **2** (1959), 39–42 (in Chinese).
- [Mi] T. Miyazaki, *On the conjecture of Jeśmanowicz concerning Pythagorean triples*, Bull. Austral. Math. Soc. **80** (2009), 413–422.
- [Mi2] T. Miyazaki, *Jeśmanowicz' conjecture on exponential Diophantine equations*, Funct. Approx. Comment. Math. **45** (2011), 207–229.
- [Mi3] T. Miyazaki, *Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples*, J. Number Theory **133** (2013), 583–595.
- [Mi4] T. Miyazaki, *Upper bounds for solutions of an exponential Diophantine equation*, Rocky Mountain J. Math. **45** (2015), 303–344.
- [Mi5] T. Miyazaki, *On an exponential equation concerning Pythagorean numbers with congruence relations*, to appear in RIMS Kokyuroku, Kyoto University.
- [Mi6] T. Miyazaki, *Contributions to some conjectures on a ternary exponential Diophantine equation*, preprint.

- [MiTe] T. Miyazaki and N. Terai, *On Jeśmanowicz' conjecture concerning primitive Pythagorean triples II*, Acta Math. Hungar **147** (2015), 286–293.
- [MiToYu] T. Miyazaki, A. Togbé and Pingzhi Yuan, *On the Diophantine equation $a^x + b^y = (a + 2)^z$* , to appear in Acta Math. Hungar.
- [MiYuWu] T. Miyazaki, P. Yuan and D. Wu, *Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples II*, J. Number Theory **141** (2014), 184–201.
- [Si] W. Sierpiński, *On the equation $3^x + 4^y = 5^z$* , Wiadom. Mat. **1** (1955/56), 194–195 (in Polish).
- [Te] N. Terai, *On Jeśmanowicz' conjecture concerning primitive Pythagorean triples*, J. Number Theory **141** (2014), 316–323.

群馬大学 大学院理工学府 理工学基板部門
E-mail address: tmiyazaki@gunma-u.ac.jp

周期たちの間の線形関係式の数値実験

田坂 浩二 (名大多元)

概要

多重ゼータ値や楕円カスプ形式の臨界値といった周期と呼ばれる特殊値たちの間の線形関係式およびこれら値で生成されるベクトル空間の次元予想を紹介する。また、この問題に対する数値実験によるアプローチを詳しく説明し、関連する未解決問題に触れる。

1 序文

1.1 周期

\mathbb{Q} 上の有理関数を \mathbb{Q} 上の多項式で定義される領域で積分して得られる実数値を実部と虚部に持つ複素数のことを周期と呼ぶ。周期は、代数的数のみならず円周率 π などの超越数を含む数のクラスを与え、様々な局面に現れる興味深い数として知られている (詳しくは [2, 15] などを参照されたい)。我々が扱う周期は、多重ゼータ値

$$\zeta(k_1, \dots, k_r) = \sum_{n_1 > \dots > n_r > 0} \frac{1}{n_1^{k_1} \dots n_r^{k_r}} \quad (k_1, \dots, k_{r-1} \in \mathbb{Z}_{>0}, k_r \in \mathbb{Z}_{>1})$$

と楕円カスプ形式の臨界値

$$I_f(n) = \int_0^\infty f(it)t^{n-1} dt \quad (f \in S_k(N), n \in \{1, 2, \dots, k-1\})$$

である。ただし、 $S_k(N)$ は重さ k 、群 $\Gamma_0(N)$ のカスプ形式の空間を表す。我々の目標は、これらの値の間の \mathbb{Q} 線形関係式の存在を示唆する“次元予想”について、実際に計算機の使い方を見ながら数値実験する方法を説明することである (多重ゼータ値の数値実験方法のみに興味のある方は、2.1 節と 3.2 節を参考にされたい)。以下で、本稿で説明する次元予想の主張を復習しておく。

1.2 多重ゼータ値の次元予想

多重ゼータ値の次元予想である Broadhurst–Kreimer 予想 [6] を復習する。

多重ゼータ値 $\zeta(k_1, \dots, k_r)$ に対し、 $k_1 + \dots + k_r$ を重さ、 r を深さと呼ぶ。基本的な事実として (3.1 節参照)、同じ重さの多重ゼータ値の間にたくさんの \mathbb{Q} 線形関係式があることが知られている。我々は、多重ゼータ値の深さが関係式にどう影響するかに興味がある。

そこで, 重さ k , 深さ r 以下の多重ゼータ値で生成される \mathbb{Q} ベクトル空間 $\mathfrak{D}_r \mathcal{Z}_k$ を考える. 例えば, $\mathfrak{D}_2 \mathcal{Z}_4 = \mathbb{Q}\zeta(4) + \mathbb{Q}\zeta(3, 1) + \mathbb{Q}\zeta(2, 2)$ である. 便宜上, $1 \in \mathbb{Q}$ は重さ 0 深さ 0 の多重ゼータ値とする. $k > 0$ であれば, 部分空間の列

$$\mathfrak{D}_0 \mathcal{Z}_k = \{0\} \subset \mathfrak{D}_1 \mathcal{Z}_k \subset \mathfrak{D}_2 \mathcal{Z}_k \subset \cdots \subset \mathfrak{D}_{k-1} \mathcal{Z}_k = \mathcal{Z}_k$$

を得る. ただし, \mathcal{Z}_k は重さ k の多重ゼータ値で生成される \mathbb{Q} ベクトル空間である. 多重ゼータ値の空間 $\mathcal{Z} := \sum_{k \geq 0} \mathcal{Z}_k$ には \mathbb{Q} 代数構造があり, 積は上記のフィルトレーションを保つ. このことから, 重さと深さを固定した多重ゼータ値の関係式を商ベクトル空間 $\mathfrak{D}_r \mathcal{Z}_k / \mathfrak{D}_{r-1} \mathcal{Z}_k$ 上で考えることが自然な問題となる. この商空間 $\mathfrak{D}_r \mathcal{Z}_k / \mathfrak{D}_{r-1} \mathcal{Z}_k$ の次元予想が Broadhurst–Kreimer 予想と呼ばれる. 主張を述べよう. 母関数 $\mathbb{O}(x), \mathbb{E}(x), \mathbb{S}(x)$ たちを次で定義する:

$$\begin{aligned} \mathbb{O}(x) &= \frac{x^3}{1-x^2} = x^3 + x^5 + x^7 + \cdots, \quad \mathbb{E}(x) = \frac{x^2}{1-x^2} = x^2 + x^4 + x^6 + \cdots, \\ \mathbb{S}(x) &= \sum_{k > 0} \dim_{\mathbb{C}} S_k(1) x^k = \frac{x^{12}}{(1-x^4)(1-x^6)} = x^{12} + x^{16} + x^{18} + \cdots. \end{aligned}$$

予想 1. (Broadhurst–Kreimer 1997) 次が成り立つ:

$$1 + \sum_{k > r > 0} \dim_{\mathbb{Q}} (\mathfrak{D}_r \mathcal{Z}_k / \mathfrak{D}_{r-1} \mathcal{Z}_k) x^k y^r \stackrel{?}{=} \frac{1 + \mathbb{E}(x)y}{1 - \mathbb{O}(x)y + \mathbb{S}(x)y^2 - \mathbb{S}(x)y^4}.$$

一見すると非常にわかりにくい予想であるが, 予想 1 は重さと深さを固定した多重ゼータ値で生成される \mathbb{Q} ベクトル空間の次元がカスプ形式の次元と深い関係にあることを示唆している. 予想 1 の信憑性はさほど検証されていないようである (例えば [13] では, 正規化された複シャッフル関係式によるアプローチにより重さ 20 まで確かめられている). $r = 1, 2, 3$ の場合, Goncharov [10] によって $\dim_{\mathbb{Q}} \mathfrak{D}_r \mathcal{Z}_k / \mathfrak{D}_{r-1} \mathcal{Z}_k$ が予想 1 の右辺の $x^k y^r$ の係数以下であることが示されており, 目下 $r = 4$ の場合が盛んに議論されている [4, 5]. 3.3 節で予想 1 の数値実験方法を詳しく説明し, 3.4 節において深さ 3 の場合の予想 1 の精密化に関する Broadhurst 予想について言及する.

1.3 楕円カスプ形式の臨界値の次元予想

重さ k のカスプ形式 $f(z)$ をとる (レベルは厭わない). 奇数 (resp. 偶数) 点での $f(z)$ の臨界値 $I_f(n)$ で生成される \mathbb{Q} ベクトル空間を $\mathcal{P}_f^{\text{od}}$ (resp. $\mathcal{P}_f^{\text{ev}}$) で表す:

$$\mathcal{P}_f^{\text{od}} = \langle I_f(n) \in \mathbb{C} \mid 1 \leq n \leq k-1, (-1)^n = -1 \rangle_{\mathbb{Q}}$$

$$(\text{resp. } \mathcal{P}_f^{\text{ev}} = \langle I_f(n) \in \mathbb{C} \mid 1 \leq n \leq k-1, (-1)^n = 1 \rangle_{\mathbb{Q}}).$$

次元の等号 $\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}} \stackrel{?}{=} \dim_{\mathbb{Q}} \mathcal{P}_f^{\text{ev}}$ および直和性 $\mathcal{P}_f^{\text{od}} \cap \mathcal{P}_f^{\text{ev}} \stackrel{?}{=} \{0\}$ は基本的な問題 (予想?) である. 以下では, 新形式 f に対する $\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}}$ のみを考える.

カスプ形式の臨界値たちの間にはたくさんの \mathbb{Q} 線形関係式が存在する. この事実にはあまり馴染みがないと思うので, 根拠となる次の命題から始めよう:

命題 2. 重さ k の新形式 $f(z) = \sum_{m>0} a_m q^m$ に対し, 空間 $\mathcal{P}_f^{\text{od}}$ の次元は f の Hecke 体 $\mathbb{Q}(f) = \mathbb{Q}(a_m \mid m \geq 1)$ の \mathbb{Q} 上の拡大次数以下である:

$$\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}} \leq [\mathbb{Q}(f) : \mathbb{Q}].$$

証明. Manin [16, p.81, §4] や志村 [20, Theorem 1] により, 整数 $n \equiv m \pmod{2}$ ($1 \leq n, m \leq k-1$) に対し, 臨界値の比 $I_f(n)/I_f(m)$ が f の Hecke 体 $\mathbb{Q}(f)$ に属することが知られている. すると, $I_f(k-1) \neq 0$ (L 関数の Euler 積表示から直ちに従う) より, 欲しい評価が得られる:

$$\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}} = \dim_{\mathbb{Q}} \sum_{\substack{1 \leq n \leq k-1 \\ (-1)^n = -1}} \mathbb{Q} \frac{I_f(n)}{I_f(k-1)} \leq [\mathbb{Q}(f) : \mathbb{Q}].$$

□

新形式 f に対し, 拡大次数 $[\mathbb{Q}(f) : \mathbb{Q}]$ の計算は難しいが, 例えばレベル 1 の場合に前田予想 ([11, 5 節]) を認めると, $[\mathbb{Q}(f) : \mathbb{Q}] = \dim_{\mathbb{C}} S_k(1) \sim \frac{k}{12}$ となる. 空間 $\mathcal{P}_f^{\text{od}}$ の生成元の個数は $\frac{k}{2}$ 個なので, 命題 2 は新形式の臨界値たちの間の \mathbb{Q} 線形関係式の存在を示唆している. 以下で, 空間 $\mathcal{P}_f^{\text{od}}$ の次元予想を提唱する (あくまで, 筆者の観測的な主観であり, 理論的な背景があるわけではないことを注意しておく).

重さ k の $\Gamma_0(N)$ の新形式からなる \mathbb{C} ベクトル空間を $S_k^{\text{new}}(N)$ と表し, 空間 $S_k^{\text{new}}(N)$ への作用 W_N を次で定義する:

$$f(z)|W_N := N^{-k/2} z^{-k} f\left(\frac{-1}{Nz}\right).$$

作用 W_N の各固有空間 $(f(z)|W_N^2 = f(z))$ ゆえ, W_N の固有値は ± 1 を $S_k^{\text{new}}(N)^{\pm}$ と表記する.

予想 3. レベルは $N = 1, 2$ のいずれかとする. このとき, 新形式 $f \in S_k^{\text{new}}(N)^{\pm}$ に対し, 次が成り立つ:

$$\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}} \stackrel{?}{=} \dim_{\mathbb{C}} S_k^{\text{new}}(N)^{\pm}.$$

レベル $N = 1$ の場合は, $S_k^{new}(1)^+ = S_k(1)$ であり, $S_k^{new}(1)^- = \{0\}$ となることに注意しておく. 予想 3 は $k = 36$ まで正しそうだということを確かめている (レベル $N = 3, 4$ の場合も同様の予想が期待出来るが, 現状データ不足である). 左辺の空間の次元の数値計算については, 4 節で詳しく解説する. 一方右辺の空間の次元は, SageMath を使えば計算可能であるが, 少なくとも筆者は $S_k^{new}(N)^\pm$ の場合の次元公式を知らない. 我々の次元予想は空間 $S_k^{new}(N)^\pm$ の次元予想も導く. これは 4.3 節で詳しく取り扱う.

2 準備 (lindep)

2.1 lindep の使い方

数値実験で使う数学ソフトウェアは Pari-GP (ver 2.8) である¹. 特に, Pari-GP の組み込み関数 “lindep” が重要な役割を果たす. 以下で, lindep の基本的な使い方を説明する (数学的な詳しい解説は [7, 2.7.2 節] を参照).

n 個の実数たちの (ある桁数での) 近似値 a_1, \dots, a_n に対し, $\text{lindep}([a_1, \dots, a_n])$ と入力すると, n 組の整数 $[b_1, \dots, b_n]$ が出力される. これは, $b_1 a_1 + \dots + b_n a_n$ が近似値として 0 に近いことを意味する. 例えば, $a_1 = \zeta(2), a_2 = \pi^2$ として, lindep を行うと

```
? lindep([zeta(2), Pi^2])
%1 = [-6, 1]~
```

を得る. この出力は $-6\zeta(2) + \pi^2 = 0$ を示唆しており, 実際, この等式は Euler により得られたものである.

基本的な使い方は上述の通りであるが, 以下 2.2 節でもう少し lindep を使った遊びを考えてみよう (Broadhurst–Kreimer 予想の導出方法に興味がある方は 3 節に進みたい).

2.2 lindep と代数的数

lindep を用いると, 次のような代数的数に関する問題を検証することができる:

問題 4. \mathbb{Q} 上 d 次の代数的数 α が与えられたとき, α を添加した単純拡大 $\mathbb{Q}(\alpha)$ が \mathbb{Q} 上のガロア拡大かを判定せよ.

例えば, $\mathbb{Q}(\sqrt{2})$ はガロア拡大だが, $\mathbb{Q}(\sqrt[3]{2})$ はガロア拡大でない. 問題 4 を検証する一つの方法は, α の \mathbb{Q} 上の最小多項式の全ての根たちが $1, \alpha, \dots, \alpha^{d-1}$ の \mathbb{Q} 線形結合で表せるかを判定することである. この検証には, 言うまでもなく先ほどの lindep が役に立つ. 以

¹ダウンロード方法については, 色々とすぐに記事が探せると思うので, ここでは説明しない. Windows ユーザーであればインストーラーがあり, 実行ファイルを展開するだけで Pari-GP が使えるようになる. Mac ユーザーは SageMath(ver 7 以降) をダウンロードするのが一番手っ取り早く利用する方法だろう.

下で、代数的数 α の代わりに \mathbb{Q} 上のモニック既約多項式を一つ与えて、問題 4 を考えてみよう (ちなみに、代数的数の \mathbb{Q} 上の最小多項式は、“algdep(α, d)” と入力することで近似的に求めることができる).

4 次既約多項式 $p(x) = x^4 - x^3 - 6x^2 + x + 1$ に対する問題 4 を検証しよう. まず, $p(x)$ の根たちを 30 桁精度で計算する:

```
? \p 30
  realprecision = 38 significant digits (30 digits displayed)
? v=real(polroots(x^4-x^3-6*x^2+x+1))
%1 = [-2.04948117773531559962553399795, -0.344150731408910807714759227885,
  0.487928364926485324714829069965,  2.90570354421774108262546415587]~
```

1 行目は計算する桁数を指定するコマンドである. 2 行目で v を $p(x)$ の根たち (近似値) を小さい順に並べたベクトルとしている. この例では $p(x)$ の根は全て実根となるが, “polroots” というコマンドは複素数値を与えるので “real” で実部をとった.

次に, lindep を用いて, 根たち (近似値) の間の関係式を計算しよう:

```
? lindep([1,v[1],v[1]^2,v[1]^3,v[2]])
%2 = [-3, -6, 0, 1, 2]~
```

ただし, $v[1]$ でベクトル v の第一成分を意味する. 出力の読み方は “ $-3 \times 1 - 6 \times v[1] + 0 \times v[1]^2 + 1 \times v[1]^3 + 2 \times v[2] = 0$ ” である. つまり, 近似値 $v[2]$ は $\{1, v[1], v[1]^2, v[1]^3\}$ の一次結合である. 同様に,

```
? lindep([1,v[1],v[1]^2,v[1]^3,v[3]])
%3 = [-1, 6, 1, -1, 1]~
? lindep([1,v[1],v[1]^2,v[1]^3,v[4]])
%4 = [-3, 4, 2, -1, -2]~
```

したがって, $p(x)$ の根たちは $\{1, v[1], v[1]^2, v[1]^3\}$ の一次結合であり, $\mathbb{Q}(v[1])$ は \mathbb{Q} 上 4 次のガロア拡大となることが予期できる (実際, [17] において, $p(x)$ は \mathbb{Q} 上の 4 次巡回拡大を与えることが示されている). すでにいろんな取組があると思うが, 計算機を用いた “ガロア拡大であるような単純拡大の特徴付け” はおもしろい試みかもしれない.

3 多重ゼータ値の次元予想

3.1 Zagier の次元予想

Broadhurst–Kreimer 予想を解説する前に, Zagier による有名な多重ゼータ値の次元予想 [22] とこれに関連する話題を簡単に紹介する.

多重ゼータ値の基本的な事実として、重さが k の多重ゼータ値 (2^{k-2} 個ある) の間にたくさんの \mathbb{Q} 線形関係式が存在する。これは、次の定理からわかる。

定理 5. (Deligne-Goncharov [8], 寺杣 [21]) 重さ k の多重ゼータ値で生成される \mathbb{Q} ベクトル空間を \mathcal{Z}_k と表し、数列 $\{d_k\}_{N \geq 0}$ を母関数 $\sum_{k \geq 0} d_k x^k := 1/(1-x^2-x^3)$ で定義する。このとき、整数 $k \geq 0$ に対し、 $\dim_{\mathbb{Q}} \mathcal{Z}_k \leq d_k$ が成り立つ。

数列 d_k の表は以下のようなになる。定理からたくさんの \mathbb{Q} 線形関係式の存在が示唆されることがわかる。

| | | | | | | | | | | | | | | | | | | | |
|-------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|
| k | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| d_k | 1 | 0 | 1 | 1 | 1 | 2 | 2 | 3 | 4 | 5 | 7 | 9 | 12 | 16 | 21 | 28 | 37 | 49 | 65 |

注意 6. 数列 $\{d_k\}_{N \geq 0}$ は \mathbb{Z} 上の混合 Tate モチーフからなる淡中圏 $\mathcal{MT}(\mathbb{Z})$ の淡中基本群 (モチビクガロア群) の座標環の次数 k 部分の次元から得られる。この事実と、多重ゼータ値が $\mathcal{MT}(\mathbb{Z})$ の周期となるという事実を併せて、定理 5 の次元の評価が得られる。近年、Brown [3] により、空間 \mathcal{Z}_k の d_k 個からなる生成系 (Hoffman 基底) が得られた。これにはモチビクガロア群の具体的な余作用の計算が重要な役割を果たしており、今後この手法の更なる応用が期待されている。未解決事項として、具体的な関係式族 (アソシエータ関係式や複シャッフル関係式など) を用いた不等式 $\dim_{\mathbb{Q}} \mathcal{Z}_k \leq d_k$ の証明は得られていないことに注意しておく。これに対し、アソシエータ関係式や正規化された複シャッフル関係式が多重ゼータ値の全ての関係式を生成しているだろうと予想されている (後者は Zagier による予想 [12])。

注意 7. 重さの異なる多重ゼータ値の間に \mathbb{Q} 線形関係式はないと考えられている。つまり、 $\mathcal{Z} := \sum_k \mathcal{Z}_k \stackrel{?}{=} \bigoplus_k \mathcal{Z}_k$ が成り立つ (Goncharov 予想)。

等式 $\dim_{\mathbb{Q}} \mathcal{Z}_k \stackrel{?}{=} d_k$ は Zagier 予想 [22] と呼ばれる。Zagier は多重ゼータ値の近似値を高速に計算するプログラムを作り、空間 \mathcal{Z}_k の次元を重さ 12 まで数値計算している。以下 3.2 節で次元の数値計算方法を述べる。

3.2 次元予想の検証方法

現在、Pari-GP (ver. 2.8) には多重ゼータ値の近似値を高速に計算する組み込み関数が存在する。整数 $k_1 \in \mathbb{Z}_{>1}, k_2, \dots, k_r \in \mathbb{Z}_{>0}$ に対し、多重ゼータ値 $\zeta(k_1, \dots, k_r)$ の近似値は次で求めることができる:

$$\text{zetamult}([k_1, \dots, k_r]).$$

例えば、 $\zeta(2, 1)$ の近似値を計算させると

```
? zetamult([2,1])
%1 = 1.2020569031595942853997381615114499908
```

を得る. これと `lindep` を使って, 空間 \mathcal{Z}_k の予想次元を低い重さから順に計算していこう.

重さ 0 は $\mathcal{Z}_0 = \mathbb{Q}$ であるので 1 次元である. 重さ 1 の多重ゼータ値はないので, $\mathcal{Z}_1 = \{0\}$ より 0 次元となる. 重さ 2 は $\mathcal{Z}_2 = \mathbb{Q}\zeta(2)$ ゆえに $\dim_{\mathbb{Q}} \mathcal{Z}_2 = 1$ である ($\zeta(2) \neq 0$ はリーマンゼータのオイラー積表示からわかる). 重さが 3 のとき, $\mathcal{Z}_3 = \mathbb{Q}\zeta(3) + \mathbb{Q}\zeta(2, 1)$ となる. そこで, $\zeta(3)$ と $\zeta(2, 1)$ の `lindep` を計算してみる:

```
? \p 200
? lindep([zetamult([2,1]),zeta(3)])
%10 = [-1, 1]~
```

よって, $\zeta(3) = \zeta(2, 1)$ が予想される. これは Euler によって実際に正しい式であることが証明されている. これにより, $\dim_{\mathbb{Q}} \mathcal{Z}_3 = 1$ を得る.

重さが 4 の多重ゼータ値は 4 つある: $\zeta(4), \zeta(3, 1), \zeta(2, 2), \zeta(2, 1, 1)$. これらに対し, `lindep` を計算すると以下ようになる:

```
? lindep([zetamult([3,1]),zeta(4)])
%11 = [-4, 1]~
? lindep([zetamult([2,2]),zeta(4)])
%12 = [4, -3]~
? lindep([zetamult([2,1,1]),zeta(4)])
%13 = [-1, 1]~
```

これは, 空間 $\mathcal{Z}_4 = \mathbb{Q}\zeta(4) + \mathbb{Q}\zeta(3, 1) + \mathbb{Q}\zeta(2, 2) + \mathbb{Q}\zeta(2, 1, 1)$ の次元が 1 であることを示唆する. この場合も $\dim_{\mathbb{Q}} \mathcal{Z}_4 = 1$ は既知である.

最後に, 重さが 5 の場合を見ておこう. 全部で 8 個の多重ゼータ値がある. 例えば, $\zeta(5)$ と $\zeta(4, 1)$ の関係を探してみる:

```
? lindep([zetamult([4,1]),zeta(5)])
%14 = [-2070013214947908776988..., 192744553422687147969023...]~
```

この場合, 係数が非常に大きいため, $\zeta(5)$ と $\zeta(4, 1)$ の間に関係式がなさそうだと判断する (“...” は実際の出力を省略するのに用いている). これに $\zeta(3, 2)$ を加えると

```
? lindep([zetamult([3,2]),zetamult([4,1]),zeta(5)])
%15 = [-2, -6, 1]~
```

となり, 係数が十分小さいことから関係式であろうと判断する. 以下, $\zeta(3, 2)$ を $\zeta(2, 3)$, $\zeta(3, 1, 1)$, $\zeta(2, 2, 1)$, $\zeta(2, 1, 2)$, $\zeta(2, 1, 1, 1)$ たちに順次取り替えて実験する. その際, 出力の係数が大きい場合は残して, 係数が小さければ入れ替えることを繰り返す. これを続けると, 重さ 5 の多重ゼータ値は $\zeta(5)$ と $\zeta(4, 1)$ の一次結合であることが示唆される. これに

より, $\dim \mathcal{Z}_5 \stackrel{?}{=} 2$ という予想に至る.

この実験では, `lindep` の出力を見て “本当に関係式かどうか” という判断を行う必要がある. 多重ゼータ値の \mathbb{Z} 線形関係式の係数の評価があるのか (少なくとも筆者は) 知らないが, 重さが大きくなるにつれ, (観測的に) 関係式の係数が大きくなるため, Zagier 予想の検証は困難になってくる.

3.3 Broadhurst–Kreimer 予想の検証

Broadhurst–Kreimer 予想 (予想 1) を検証しよう. 簡単のため, 重さ k 深さ r 以下の多重ゼータ値で生成される \mathbb{Q} ベクトル空間 $\mathcal{D}_r \mathcal{Z}_k$ の次元を低い深さから考える.

3.3.1 深さ 1

深さ 1 の場合, $\mathcal{D}_1 \mathcal{Z}_k = \mathbb{Q}\zeta(k)$ であるゆえ, この次元は 1 である:

$$\sum_{k>0} \dim_{\mathbb{Q}} \mathcal{D}_1 \mathcal{Z}_k x^k = \frac{x^2}{1-x}.$$

3.3.2 深さ 2

空間 $\mathcal{D}_2 \mathcal{Z}_k$ を考える. 空間 $\mathcal{D}_2 \mathcal{Z}_k$ の次元は, $\mathcal{D}_2 \mathcal{Z}_k \supset \mathcal{D}_1 \mathcal{Z}_k$ であるので, 商空間 $\mathcal{D}_2 \mathcal{Z}_k / \mathcal{D}_1 \mathcal{Z}_k$ の次元を求めれば良い:

$$\dim_{\mathbb{Q}} \mathcal{D}_2 \mathcal{Z}_k / \mathcal{D}_1 \mathcal{Z}_k = \dim_{\mathbb{Q}} \mathcal{D}_2 \mathcal{Z}_k - \dim_{\mathbb{Q}} \mathcal{D}_1 \mathcal{Z}_k.$$

例えば, $k = 6$ の場合を計算してみると,

```
? lindep([zeta(6), zetamult([5, 1])])
%24 = [-1222183950778189302444..., 30672805431176991340709...]~
```

```
? lindep([zeta(6), zetamult([5, 1]), zetamult([4, 2])])
%21 = [-1, 12, 6]~
? lindep([zeta(6), zetamult([5, 1]), zetamult([3, 3])])
%22 = [1, -4, -4]~
? lindep([zeta(6), zetamult([5, 1]), zetamult([2, 4])])
%23 = [-7, -24, 12]~
```

となるので, 商空間 $\mathcal{D}_2 \mathcal{Z}_6 / \mathcal{D}_1 \mathcal{Z}_6$ は $\zeta(5, 1) \bmod \mathbb{Q}\zeta(6)$ で生成される. 従って,

$$\dim_{\mathbb{Q}} \mathcal{D}_2 \mathcal{Z}_6 / \mathcal{D}_1 \mathcal{Z}_6 = 1.$$

同様に, $\dim_{\mathbb{Q}} \mathcal{D}_2 \mathcal{Z}_k / \mathcal{D}_1 \mathcal{Z}_k$ を計算してみると, 次のような表が得られる (興味のある方は, この表を観察して規則を見いだしてみることを勧める):

| | | | | | | | | | | | | | | | | | | | |
|-----|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|
| k | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| | 0 | 0 | 0 | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 3 | 5 | 5 | 6 | 5 | 7 | 6 | 8 | 7 |

注意 8. Broadhurst–Kreimer 予想によれば, 上記の数列は次のような母関数表示を持つ:

$$\sum_{k>0} \dim_{\mathbb{Q}} (\mathcal{D}_2 \mathcal{Z}_k / \mathcal{D}_1 \mathcal{Z}_k) x^k \stackrel{?}{=} \mathbb{O}(x)^2 - \mathbb{S}(x) + \mathbb{O}(x)\mathbb{E}(x). \quad (3.1)$$

これは, 最初に Zagier [22] により示唆されたため, Zagier 予想とも呼ぶ。

3.3.3 深さ 3

空間 $\mathcal{D}_3 \mathcal{Z}_k$ の次元を計算しよう. 方針は, 商空間 $\mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k$ の次元を計算することである. 重さ 6 の場合を見てみよう. 先のデータから, $\zeta(6)$ と $\zeta(5, 1)$ は空間 $\mathcal{D}_2 \mathcal{Z}_6$ の (数値的な) 基底となることがわかっている. したがって, 商空間 $\mathcal{D}_3 \mathcal{Z}_6 / \mathcal{D}_2 \mathcal{Z}_6$ の次元は, 重さ 6 の 3 重ゼータ値たちで $\zeta(6)$ と $\zeta(5, 1)$ でかけないものたちの個数である.

```
? lindep([zeta(6), zetamult([5, 1]), zetamult([4, 1, 1])])
%25 = [-1, 32, -16]~
? lindep([zeta(6), zetamult([5, 1]), zetamult([3, 2, 1])])
%26 = [13, -288, -48]~
```

```
? lindep([zeta(6), zetamult([5, 1]), zetamult([3, 1, 2])])
%27 = [-1, 72, -24]~
? lindep([zeta(6), zetamult([5, 1]), zetamult([2, 3, 1])])
%28 = [-1, 72, -24]~
```

```
? lindep([zeta(6), zetamult([5, 1]), zetamult([2, 2, 2])])
%29 = [-3, 0, 16]~
? lindep([zeta(6), zetamult([5, 1]), zetamult([2, 1, 3])])
%30 = [-11, 32, 16]~
```

これにより, $\dim_{\mathbb{Q}} \mathcal{D}_3 \mathcal{Z}_6 / \mathcal{D}_2 \mathcal{Z}_6 = 0$ であるので, $\dim_{\mathbb{Q}} \mathcal{D}_3 \mathcal{Z}_6 = 2$ を得る.

同様に, 深さ 2 の計算データ (数値的な基底) を用いて, 空間 $\mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k$ の次元を計算した表が以下である:

| | | | | | | | | | | | | | | | |
|--|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| k | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| $\dim \mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 3 | 3 | 6 | 6 | 9 | 8 | 14 |

この表の数列の規則を予想するのは容易ではないと思われる. Broadhurst–Kreimer 予想によれば, 次のような表示を持つ:

$$\sum_{k>0} \dim_{\mathbb{Q}} (\mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k) x^k \stackrel{?}{=} \mathbb{E}(x)(\mathbb{O}(x)^2 - \mathbb{S}(x)) + \mathbb{O}(x)(\mathbb{O}(x)^2 - 2\mathbb{S}(x)). \quad (3.2)$$

3.4 節において, 右辺の母関数の意味を空間 $\mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k$ の生成元とその関係式という観点から詳しく説明する.

3.3.4 一般の深さ (Broadhurst–Kreimer 予想)

深さ 3 で行った計算を続けることにより, 商空間 $\mathcal{D}_r \mathcal{Z}_k / \mathcal{D}_{r-1} \mathcal{Z}_k$ の次元を帰納的に計算していくことができる. 念のため, $k \leq 16, 4 \leq r \leq 6$ における商空間 $\mathcal{D}_r \mathcal{Z}_k / \mathcal{D}_{r-1} \mathcal{Z}_k$ の次元の表を載せておく:

| $r \setminus N$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|-----------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 4 | 10 | 11 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 6 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

これまで導出した次元の表と予想 1 で与えた右辺の母関数の $x^k y^r$ の係数が一致していることは, 右辺の $x = 0$ でのテイラー展開を見れば容易に確認できる:

```
? o(x)=x^3/(1-x^2);
```

```
? E(x)=x^2/(1-x^2);
```

```
? S(x)=x^12/(1-x^4)/(1-x^6);
```

```
? BK(x,y)=(1+E(x)*y)/(1-o(x)*y+S(x)*y^2-S(x)*y^4);
```

```
? taylor(BK(x,y),x,17)
```

```
%14 = 1 + y*x^2 + y*x^3 + y*x^4 + (y^2 + y)*x^5 + (y^2 + y)*x^6
+ (2*y^2 + y)*x^7 + (y^3 + 2*y^2 + y)*x^8 + (y^3 + 3*y^2 + y)*x^9
+ (3*y^3 + 3*y^2 + y)*x^10 + (y^4 + 3*y^3 + 4*y^2 + y)*x^11
+ (2*y^4 + 6*y^3 + 3*y^2 + y)*x^12 + (4*y^4 + 6*y^3 + 5*y^2 + y)*x^13
+ (2*y^5 + 4*y^4 + 9*y^3 + 5*y^2 + y)*x^14
+ (3*y^5 + 10*y^4 + 8*y^3 + 6*y^2 + y)*x^15
+ (6*y^5 + 11*y^4 + 14*y^3 + 5*y^2 + y)*x^16 + 0(x^17)
```

3.4 未解決問題

現在, Broadhurst–Kreimer 予想に対して盛んに研究が進められているのは, 予想 1 の深さ 4 の場合であろうが, この話題には紙面の都合上立ち入らない (最近の進捗は Brown の論文 [4, 5] を参照). ここでは, 深さ 3 の商空間 $\mathcal{D}_3 \mathcal{Z}_k / \mathcal{D}_2 \mathcal{Z}_k$ の生成元に関する未解決問題である Broadhurst 予想とそれに関連する予想について紹介する.

以下, 簡単のため商空間 $\mathcal{D}_r \mathcal{Z}_k / \mathcal{D}_{r-1} \mathcal{Z}_k$ を $\mathcal{Z}_{k,r}$ と書く. また, 重さ k の多重ゼータ値 $\zeta(k_1, \dots, k_r)$ の商空間 $\mathcal{Z}_{k,r}$ での像を $\zeta_{\mathcal{D}}(k_1, \dots, k_r)$ と表記する. 残念ながら適切な文献をあげられないのだが, Broadhurst 予想はおおよそ次のように述べられる:

予想 9. 奇数 $k > 0$ に対し, 空間 $\mathcal{Z}_{k,3}$ は純奇 3 重ゼータ値で生成される:

$$\mathcal{Z}_{k,3} \stackrel{?}{=} \langle \zeta_{\mathcal{D}}(k_1, k_2, k_3) \mid k = k_1 + k_2 + k_3, k_i \geq 3 : \text{odd} \rangle_{\mathbb{Q}}.$$

予想 9 は空間 $\mathcal{Z}_{k,3}$ の生成元に関する予想である. この予想と深さ 3 の Broadhurst–Kreimer 予想 (3.2) を眺めると, つぎのような観察が得られる. 予想 (3.2) を重さ奇数に制限すると,

$$\sum_{k>0:\text{odd}} \dim_{\mathbb{Q}} \mathcal{Z}_{k,3} x^k \stackrel{?}{=} \mathcal{O}(x)^3 - 2\mathcal{O}(x)\mathcal{S}(x)$$

となる. ここで, 右辺の最初の項 $\mathcal{O}(x)^3$ は純奇 3 重ゼータ値の個数の母関数となることに注意する:

$$\mathcal{O}(x)^3 = \sum_{k>0} \#\{(k_1, k_2, k_3) \in \mathbb{Z}_{>1}^3 \mid k = k_1 + k_2 + k_3, k_i \geq 3 : \text{odd}\} x^k.$$

予想 9 が正しいとすると, 予想 (3.2) は純奇 3 重ゼータ値たちの間に “ $-2\mathcal{O}(x)\mathcal{S}(x)$ ” に対応する \mathbb{Q} 線形関係式が存在することを示唆している. したがって, 予想 9 は空間 $\mathcal{Z}_{k,3}$ の生成元とその関係式を決めるという問題を提唱しており, Broadhurst–Kreimer 予想の精密化を与えている. このような精密化は深さ 4 以上では知られていないが, Broadhurst–Kreimer 予想を理解する上で非常に重要な手がかりになりうる.

ついでながら, 重さが偶数の場合の精密化について, 筆者と Ding Ma との共同研究 [19] を紹介しておこう.

予想 10. 偶数 $k > 0$ に対し, 空間 $\mathcal{Z}_{k,3}$ は次の 3 重ゼータ値で生成される:

$$\mathcal{Z}_{k,3} \stackrel{?}{=} \langle \zeta_{\mathcal{D}}(k_1, k_2, k_3) \mid k = k_1 + k_2 + k_3, k_1, k_3 \geq 3 : \text{odd}, k_2 \geq 2 : \text{even} \rangle_{\mathbb{Q}}.$$

これは重さが偶数の場合における Broadhurst 予想の類似と見做せる. 実際, 予想 (3.2)

を重さ偶数に制限すると,

$$\sum_{k>0:\text{even}} \dim_{\mathbb{Q}} \mathcal{Z}_{k,3} x^k \stackrel{?}{=} \mathbb{E}(x)\mathbb{O}(x)^2 - \mathbb{E}(x)\mathbb{S}(x)$$

であり, $\mathbb{E}(x)\mathbb{O}(x)^2$ は予想 10 の右辺の空間の生成元の個数の母関数となっている. 論文 [19] では, これら生成元の間 “ $-\mathbb{E}(x)\mathbb{S}(x)$ ” に対応する関係式があることを示している.

注意 11. Broadhurst–Kreimer 予想の “生成元とその関係式” の研究は, 深さ 2 の場合は完全に解決されている. 偶数重さの場合, Gangl–金子–Zagier [9] により空間 $\mathcal{Z}_{k,2}$ が $\{\zeta_{\mathbb{D}}(k_1, k_2) \mid k = k_1 + k_2, k_1, k_2 \geq 3 : \text{odd}\}$ で生成されることが示されており, これら生成元の間 カスプ形式 (正確には偶周期多項式) と対応する関係式が存在することも知られている. これは, 重さ偶数の場合の予想 (3.1) の右辺の母関数の説明を与える. 奇数重さの場合, Zagier [24] により空間 $\mathcal{Z}_{k,2}$ が $\{\zeta_{\mathbb{D}}(k_1, k_2) \mid k = k_1 + k_2, k_1 \geq 3 : \text{odd}, k_2 \geq 2 : \text{even}\}$ で生成されることが示されている. 重さ奇数の場合の予想 (3.1) を鑑みると, これら生成元は基底になると予想される. 2 重の場合には, モチビック多重ゼータ値を使うと “基底になること” や “次元の等式” を示すことができることを注意しておく.

4 楕円カスプ形式の臨界値

4.1 楕円カスプ形式の臨界値の計算方法

新形式の臨界値の近似値を計算するプログラムを紹介する.

重さ k レベル N の新形式 $f(z) = \sum_{m>0} a_m q^m$ に対し, $f(z)|W_N = \varepsilon_f f(z)$ とおく. $f(z)$ に対する $I_f(n)$ の近似値を計算するには, $I_f(n)$ の不完全ガンマ関数 $\Gamma(s, x) = \int_x^{\infty} e^{-t} t^{s-1} dt$ を用いた表記を利用する:

$$\begin{aligned} I_f(n) &= \left(\int_{1/\sqrt{N}}^{\infty} + \int_0^{1/\sqrt{N}} \right) f(it) t^{n-1} dt \\ &= \int_{1/\sqrt{N}}^{\infty} f(it) t^{n-1} dt + \varepsilon_f N^{k/2-n} \int_{1/\sqrt{N}}^{\infty} f(it) t^{k-n-1} dt \\ &= \sum_{m>1} a_m \left(\int_{1/\sqrt{N}}^{\infty} e^{-2\pi m t} t^{n-1} dt + \varepsilon_f N^{k/2-n} \int_{1/\sqrt{N}}^{\infty} e^{-2\pi m t} t^{k-n-1} dt \right) \\ &= \sum_{m>1} a_m \left(\frac{\Gamma(n, 2\pi m/\sqrt{N})}{(2\pi m)^n} + \varepsilon_f N^{k/2-n} \frac{\Gamma(k-n, 2\pi m/\sqrt{N})}{(2\pi m)^{k-n}} \right). \end{aligned}$$

2 番目の等式は, 変数変換 $t \rightarrow 1/Nt$ である. 簡単にわかるように, 不完全ガンマ関数 $\Gamma(s, x)$ は, $x > 0$ のとき, $e^{-x} \times (x \text{ の多項式})$ という表記を持つ. つまり不完全ガンマ関数

は x が大きくなると急速に 0 に近づく (例: $e^{-2\pi \times 80} = 5.00937... \times 10^{-219}$). この表記を使えば, m を $0 < m < 80\sqrt{N}$ の範囲で足しあげる程度で臨界値 $I_f(n)$ の 200 桁精度での十分な近似値が期待出来る. Pari-GP でのプログラム例をあげる:

```
? p(f,n,k,N,epsilon)=sum(m=1,floor(80*sqrt(N)),
  polcoeff(f,m)*(incgam(n,2*Pi*m/sqrt(N))/(2*Pi*m)^n
  +epsilon*N^(k/2-n)*incgam(k-n,2*Pi*m/sqrt(N))/(2*Pi*m)^(k-n));
```

例 12. 重さ 12 のラマヌジャン・デルタ関数 $\Delta(z) = \eta(z)^{24}$ に対する $I_\Delta(1)$ を計算すると, 以下のようなになる ($\Delta|W_1 = \Delta$ に注意):

```
? f=eta(q)^24*q;
? p(f,1,12,1,1)
%13 = 0.00595896498957823785383556...
```

例 13. 重さ 8 レベル 2 の新形式 $f(z) = \eta(z)^8 \zeta(2z)^8$ に対する $I_f(1)$ を計算する. 先に, ε_f を求める必要があるが, これは $(-i)^k N^{k/2} f(-1/Ni)/f(i)$ の近似値を見れば良い².

```
? f2(q)=q - 8*q^2 + 12*q^3 + 64*q^4 - 210*q^5 - 96*q^6 + 1016*q^7 + ..
? [f2(exp(-2*Pi/2))/2^4,f2(exp(-2*Pi))]
%26 = [0.0018396229153702758..., 0.0018396229153702758...]
```

ラマヌジャン・デルタ関数のときと異なり, ε_f を求める際に値を代入する必要があるため, $f_2(q)$ は変数 q に関する多項式として定義している. 上記計算から $\varepsilon_f = 1$ がわかる. よって, $I_f(1)$ の近似値は以下で求められる:

```
? p(f2(q),1,8,2,1)
%30 = 0.01407435391139164711849290914...
```

4.2 新形式の臨界値の空間の次元

先ほどの関数 p を使って, 新形式に対する空間 $\mathcal{P}_f^{\text{od}}$ の次元を計算し, 予想 3 を検証しよう. 新形式の Fourier 展開については, SageMath のデータベースを次のように参照する. SageMath において, “CuspForms(N,k).newforms('x')” と入力すると, $\Gamma_0(N)$ に対する重さ k の新形式の Fourier 展開がベクトル形式で出力されるので, これを成分の小さい方から $f_{k,N,1}, f_{k,N,2}, \dots, f_{k,N,d}$ と名付ける. 例えば, 重さ 8 レベル 5 の新形式の Fourier 展開のリスト $f_{8,5,1}, f_{8,5,2}$ は以下のようなになる:

```
sage: CuspForms(5,8,prec=5).newforms('x')
[q - 14*q^2 - 48*q^3 + 68*q^4 + 0(q^5),
 q + x1*q^2 + (-8*x1 + 90)*q^3 + (20*x1 - 152)*q^4 + 0(q^5)]
```

² $f(z)$ が $z = i$ を零点に持つ場合は $z = 2i$ などに変える必要がある. また, 後で引用する (4.1) 式と SageMath の新形式の Fourier 展開のデータベースを使っても簡単に計算できる.

ここで, 'x1' は新形式の Hecke 固有値 (\mathbb{Q} でないもの) を意味する.

4.2.1 $\Gamma_0(1)$ の場合

先に, 数値実験による次元の表を与える. レベル $N = 1$ の場合, 重さ 36 以下 (14 を除いて) において新形式のリストは常に一つとなっている (それを $f_{k,1,1}$ と書く).

| k | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $\dim_{\mathbb{Q}} \mathcal{P}_{f_{k,1,1}}$ | 1 | 0 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 |

これは, 予想 3 で述べたように, $\dim S_k(1)$ と一致していることに注意しておく. 以下, 重さ 12 の場合と重さ 24 の場合の計算方法を例解する.

例 14. ラマヌジャン・デルタ関数に対し, 空間 $\mathcal{P}_{\Delta}^{\text{od}}$ の関係式を調べる.

```
? lindep([p(f,1,12,1,1),p(f,3,12,1,1)])
%34 = [691, -1620]~
? lindep([p(f,1,12,1,1),p(f,5,12,1,1)])
%35 = [-691, 2520]~
? lindep([p(f,1,12,1,1),p(f,7,12,1,1)])
%36 = [-691, 2520]~
? lindep([p(f,1,12,1,1),p(f,9,12,1,1)])
%37 = [691, -1620]~
? lindep([p(f,1,12,1,1),p(f,11,12,1,1)])
%39 = [-1, 1]~
```

いくつか観察できる対称性は, 関数等式に他ならない (筆者は周期の比 $I_{\Delta}(1)/I_{\Delta}(3) = 1620/691$ に Bernoulli 数が表れる由緒正しい理由が以前からずっと気になっている). この実験から, $\dim_{\mathbb{Q}} \mathcal{P}_{\Delta}^{\text{od}} = 1$ が示唆される.

注意 15. 最初に述べたように, $\mathcal{P}_{\Delta}^{\text{ev}} \cap \mathcal{P}_{\Delta}^{\text{od}} \stackrel{?}{=} \{0\}$ も観察できる:

```
? lindep([p(f,1,12,1,1),p(f,2,12,1,1)])
%44 = [-508457032499845654368..., 8171829176024575747685...]~
```

例 16. 重さ 24 レベル 1 の新形式の Fourier 展開を SageMath から用意する:

```
sage: CuspForms(1,24,prec=10).newforms('x')
[q + x0*q^2 + (-48*x0 + 195660)*q^3 + (1080*x0 + 12080128)*q^4
+ (-15040*x0 + 44656110)*q^5 + (143820*x0 - 982499328)*q^6
+ (-985824*x0 - 147247240)*q^7 + (4857920*x0 + 22106234880)*q^8
+ (-16295040*x0 - 8700375483)*q^9 + 0(q^10)]
```

ここで, x_0 は新形式の係数の乗法性から $a_2 * a_3 - a_6 = 0$ を解くことで計算できることに注意する. この根たちをベクトル v と置く:

```
? v=real(polroots((-48*x+195660)*x-(143820*x-982499328)))
%46 = [-4016.3511717162451393..., 5096.35117171624513931555...]~
```

重さ 24 の新形式の Fourier 展開を x_0 の多項式として Pari-GP に定義し, 関係式の計算をする:

```
? f(x0)=q + x0*q^2 + (-48*x0 + 195660)*q^3 + (1080*x0 + 12080128)*q^4 ...
```

```
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1)])
%51 = [-4258290237037830..., 4990302813300383...]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),5,24,1,1)])
%52 = [-236364091, 3466670130, -6742820700]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),7,24,1,1)])
%53 = [-24345501373, 299682070380, -1100428338240]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),9,24,1,1)])
%54 = [-22927316827, 271855320660, -1572040483200]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),11,24,1,1)])
%55 = [11109112277, -130589249868, 953704559808]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),13,24,1,1)])
%56 = [11109112277, -130589249868, 953704559808]~
```

したがって, $\dim_{\mathbb{Q}} \mathcal{P}_{\Delta}^{\text{od}} = 2$ が示唆される. しかし, 関係式の係数が大きいので, 本当に関係式を与えているのかやや懐疑的である. こういう場合は, 桁数の設定を変えて係数の変化をみるといい:

```
? \p 230
    realprecision = 231 significant digits (230 digits displayed)
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1)])
%57 = [-17866559816892285640..., 20937873830849700216...]~
? linderp([p(f(v[1]),1,24,1,1),p(f(v[1]),3,24,1,1),p(f(v[1]),5,24,1,1)])
%58 = [236364091, -3466670130, 6742820700]~
```

一行目の出力は変わったのに対し, 関係式だと思われる二行目の出力は変わっていない. これは, 230 桁でもこの一次結合が 0 に近いことを示唆するので, より強力なサポートを得たことになる. いずれにしても, このあたりの判断には注意が必要である.

注意 17. レベル 1 の場合の予想 3 に対し, 具体的な関係式 (2 サイクル関係式, 3 サイクル関係式, Kohnen-Zagier 関係式 [14]) を使うことで, $\dim_{\mathbb{Q}} \mathcal{P}_f^{\text{od}} \leq \dim_{\mathbb{C}} S_k(1)$ を得ることができる.

4.2.2 $\Gamma_0(2)$ の場合

予想 3 を検証するには, $\Gamma_0(2)$ の新形式の W_2 に対する固有値の情報まで必要である. 以下に, $\dim S_k^{\text{new}}(2)^\pm$ の次元の表を与える.

| k | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 |
|------------------------------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $\dim S_k^{\text{new}}(2)^+$ | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 |
| $\dim S_k^{\text{new}}(2)^-$ | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 1 | 2 | 1 |

ここに現れる次元 2 の部分はいずれも Hecke 固有値が 2 次の代数的数となる新形式たちである. したがって, 上記表における限りは, 実質 $f_{k,2}^\pm$ とすれば, 各 k に対して唯一に定まる. これに対し, レベル 1 のときと同様にして空間 $\mathcal{P}_{f_{k,2}^\pm}^{\text{od}}$ の次元を数値計算すると, その次元の表が上記の表と一致することが確かめられる.

4.3 $\Gamma_0(2)$ の新形式の臨界値の具体的な関係式

真新しいアイデアではないが, $\Gamma_0(2)$ の新形式の臨界値の具体的な \mathbb{Q} 線形関係式族を与える方法をひとつ紹介する. ここで得られる関係式を使って空間 $\mathcal{P}_f^{\text{od}}$ の次元を評価し, いくつか考察を述べて本稿を終わる.

まず, 関係式の母関数 (周期多項式) を用いた表示を与える. 重さ $2k$ のカスプ形式 $f(z)$ に対し, 周期多項式 $r_f(x, y)$ を次で定める:

$$r_f(x, y) := \int_0^{i\infty} f(z)(x - yz)^{2k-2} dz = i \sum_{\substack{n_1+n_2=2k \\ n_1, n_2 \geq 1}} (-i)^{n_2-1} \binom{2k-2}{n_2-1} I_f(n_2) x^{n_1-1} y^{n_2-1}.$$

これは, 臨界値 $I_f(n)$ の (多項式) 母関数表示となっていることに注意する. 偶数 $k > 0$ に対し, 2 変数多項式環 $\mathbb{Q}[x, y]$ の $k-2$ 次の斉次多項式からなる部分空間を $V_k := \mathbb{Q}[x, y]_{(k-2)}$ と表記する. 空間 V_k への $\text{PGL}_2(\mathbb{Z})$ の作用を以下で定め, これを線形に群環 $\mathbb{Z}[\text{PGL}_2(\mathbb{Z})]$ に拡張しておく:

$$p(x, y)|\gamma = p(ax + by, cx + dy) \quad (\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(\mathbb{Z})).$$

定理 18. 新形式 $f(z) \in S_{2k}^{\text{new}}(2)^\pm$ に対し, 次が成り立つ:

$$\mp 2^{k-1} r_f(x, y) = r_f(x, y) \Big| \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ -2 & 0 \end{pmatrix} \right).$$

証明. $f(z) = \sum_{m>0} a_m q^m$ に対し, $U_2 f(z) := \sum_{m>0} a_{2m} q^m$ と定義する. Atkin-Lehner [1, Theorem 3] の結果より,

$$U_2 f(z) = a_2 f(z) = \mp 2^{k-1} f(z) \quad (4.1)$$

が成り立つ. 作用素 U_2 は $U_2 f(z) = \frac{1}{2} f\left(\frac{z}{2}\right) + \frac{1}{2} f\left(\frac{z+1}{2}\right)$ と表せるので, 周期多項式への作用に書き直すことで

$$r_{U_2 f}(x, y) = r_f(x, y) \left| \left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ -2 & 0 \end{pmatrix} \right) \right|$$

を得る (この等式のアイデアは [16, 23] を参照). これと (4.1) を合わせて主張を得る. \square

定理 18 から得られる臨界値 $I_f(n)$ たちの具体的な関係式を明示しよう. 整数 $m_1, m_2, n_1, n_2 \geq 1$ に対し, 整数 $b_{\pm} \binom{m_1, m_2}{n_1, n_2}$ を以下で定める³:

$$b_{\pm} \binom{m_1, m_2}{n_1, n_2} = \delta_{n_1, m_1} (2^{m_2-1} \pm 2^{\frac{m_1+m_2}{2}-1}) + 2^{m_2-1} \binom{m_1-1}{n_1-1} - (-2)^{m_2-1} \binom{m_1-1}{n_2-1}.$$

ただし, δ_{n_1, m_1} はクロネッカーデルタ記号である. 定理 18 から直ちに次の系を得る.

系 19. 整数 $n_1, n_2 \geq 1$ ($n_1 + n_2 = 2k$) に対し, 次の系が成り立つ:

$$\sum_{\substack{m_1+m_2=2k \\ m_1, m_2 \geq 1}} (-i)^{m_2-1} \binom{2k-2}{m_2-1} b_{\pm} \binom{m_1, m_2}{n_1, n_2} I_f(m_2) = 0.$$

関係式の係数行列 $B_{2k}^{od, \pm}$ を考えよう:

$$B_{2k}^{od, \pm} = \left((-1)^{(m_2-1)/2} \binom{2k-2}{m_2-1} b_{\pm} \binom{m_1, m_2}{n_1, n_2} \right)_{\substack{m_1+m_2=2k, m_i \geq 1: \text{odd} \\ n_1+n_2=2k, n_i \geq 1}}.$$

ただし, 列と行はそれぞれ (m_1, m_2) と (n_1, n_2) を走るとする. 定義から, 新形式 $f \in S_{2k}^{new}(2)^{\pm}$ に対し, 列を適当に並べ替えると

$$B_{2k}^{od, \pm} \cdot \begin{pmatrix} I_f(1) \\ I_f(3) \\ \vdots \\ I_f(2k-1) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

となる. よって, 行列 $B_{2k}^{od, \pm}$ の階数を計算することにより, 空間 P_f^{od} の上限を得ることができる:

系 20. 新形式 $f \in S_{2k}^{new}(2)^{\pm}$ に対し, 次の不等式が成り立つ:

$$\dim_{\mathbb{Q}} P_f^{od} \leq k - \text{rank } B_{2k}^{od, \pm}.$$

³整数 $b_{\pm} \binom{m_1, m_2}{n_1, n_2}$ は Ding Ma [18] によるモチビック 2 重 Euler 和 (レベル 2 の 2 重ゼータ値) へのガロア余作用の計算にも表れる. 具体的な関係はまだ明らかになっていないが, とても興味深い整数である.

係数が具体的なので、行列 $B_{2k}^{od,\pm}$ の階数は非常に高速に計算できる。重さ 36 以下では次のようになる:

| k | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 |
|----------------------------------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $k - \text{rank } B_{2k}^{od,+}$ | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 |
| $k - \text{rank } B_{2k}^{od,-}$ | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 1 | 2 | 1 |

上記の表は、4.2.2 節の $\dim S_k^{new}(2)^\pm$ の表と一致していることに注意する。この一致は、重さ 36 以下では定理の関係式が $\Gamma_0(2)$ の新形式の臨界値たちのすべての関係式を生成することを示唆している。これを述べておこう:

予想 21. 新形式 $f \in S_k^{new}(2)^\pm$ の臨界値たちの \mathbb{Q} 線形関係式は系 19 で得られる線形関係式からすべて得られる。

Mathematica の組み込み関数 “FindGeneratingFunction” を使って、上記表の数列の母関数表示を計算させると次のような表示を得る:

$$\sum_{k>0} (k - \text{rank } B_{2k}^{od,+}) x^{2k} \stackrel{?}{=} \frac{x^8}{(1-x^6)(1-x^8)},$$

$$\sum_{k>0} (k - \text{rank } B_{2k}^{od,-}) x^{2k} \stackrel{?}{=} \frac{x^{10}(1+x^4-x^6)}{(1-x^6)(1-x^8)}.$$

この表示と予想 21 を併せると、次の $S_k^{new}(2)^\pm$ の次元公式に関する予想が得られる:

$$\sum_{k>0} \dim_{\mathbb{C}} S_{2k}^{new}(2)^+ x^{2k} \stackrel{?}{=} \frac{x^8}{(1-x^6)(1-x^8)},$$

$$\sum_{k>0} \dim_{\mathbb{C}} S_{2k}^{new}(2)^- x^{2k} \stackrel{?}{=} \frac{x^{10}(1+x^4-x^6)}{(1-x^6)(1-x^8)}.$$

これは、[18, Conjecture 4] におけるレベル $N = 2$ に対する予想と等しい。これらはどれも数値実験による予想にすぎないが、臨界値の関係式や次元の研究が $S_k^{new}(N)^\pm$ の次元公式の研究につながるのはとても興味深い。

謝辞

今回、講演の機会をくださいました世話人の方々に感謝の意を表したいと思います。ありがとうございました。

参考文献

- [1] A. O. L. Atkin, J. Lehner, *Hecke Operators on $\Gamma_0(m)$* , Math. Ann., **185** (1970), 134–160.
- [2] Y. André, *Ambiguity theory, old and new*, arXiv:0805.2568.
- [3] F. Brown, *Mixed Tate motives over \mathbb{Z}* , Ann. of Math., **175**(2) (2012), 949–976.
- [4] F. Brown, *Depth-graded motivic multiple zeta values*, arXiv:1301.3053.
- [5] F. Brown, *Zeta elements in depth 3 and the fundamental Lie algebra of a punctured elliptic curve*, arXiv:1504.04737.
- [6] D. Broadhurst, D. Kreimer, *Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops*, Phys. Lett. B **393**, no. 3-4 (1997), 403–412.
- [7] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **193**.
- [8] P. Deligne, A.B. Goncharov, *Groupes fondamentaux motiviques de Tate mixte*, Ann. Sci. École Norm. Sup. **38** (2005), 1–56
- [9] H. Gangl, M. Kaneko, D. Zagier, *Double zeta values and modular forms*, Automorphic forms and Zeta functions, In:Proceedings of the conference in memory of Tsuneo Arakawa, World Scientific, (2006), 71–106.
- [10] A. B. Goncharov, *The dihedral Lie algebras and Galois symmetries of $\pi_1^{(l)}(\mathbb{P}^1 - (\{0, \infty\} \cup \mu_N))$* , Duke Math. J., **110**(3) (2001), 397–487.
- [11] H. Hida, Y. Maeda, *Non-abelian base change for totally real fields*, Pacific J. Math. **181**(3), 189–217 (1997).
- [12] K. Ihara, M. Kaneko, D. Zagier, *Derivation and double shuffle relations for multiple zeta values*, Compositio Math., **142** (2006), 307–338.
- [13] M. Kaneko, M. Noro and K.Tsurumaki, *On a conjecture for the dimension of the space of the multiple zeta values*, Software for Algebraic Geometry, IMA 148, 47–58, (2008).
- [14] W. Kohnen, D. Zagier, *Modular forms with rational periods*, Modular forms (Durham, 1983), Ellis Horwood (1984), 197–249.

- [15] M. Kontsevich, D. Zagier, *Periods*, in Engquist, Björn (ed.) et al., Mathematics unlimited - 2001 and beyond, Springer Verlag, 771–808 (2001).
- [16] S. Lang, *Introduction to modular forms*. Grundlehren der mathematischen Wissenschaften, No. 222. Springer-Verlag, Berlin-New York, (1976).
- [17] A.J. Lazarus, *On the class number and unit index of the simplest quartic fields*, Nagoya Math. J., **121** (1991) 1–13.
- [18] D. Ma, *Connections between double zeta values relative to μ_N , Hecke operators T_N , and newforms of level $\Gamma_0(N)$ for $N = 2, 3$* , arXiv:1511.06102
- [19] D. Ma, K. Tasaka, *On triple zeta values of even weight and their connections with even period polynomials*, arXiv:1603.01013.
- [20] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), 783–804.
- [21] T. Terasoma, *Mixed Tate motives and multiple zeta values*, Invent. Math. **149**(2) (2002), 339–369.
- [22] D. Zagier, *Values of zeta functions and their applications*, First European Congress of Mathematics, Vol. II (Paris, 1992), Progr. Math., **120**, Birkhäuser, Basel (1994), 497–512.
- [23] D. Zagier, *Hecke operators and periods of modular forms*, Israel Math. Conf. Proc. **3** (1990), 321–336.
- [24] D. Zagier, *Evaluation of the multiple zeta values $\zeta(2, \dots, 2, 3, 2, \dots, 2)$* , Ann. of Math., **175**(2) (2012), 977–1000.

(0, ±1) ベクトルの最大距離を避ける最大部分集合について

愛知教育大学・数学教育講座 野崎寛

Hiroshi Nozaki

Department of Mathematics Education

Aichi University of Education

1 はじめに

本稿では、主に [1] の内容を紹介する。極値集合論において、次の Erdős–Ko–Rado の定理はよく知られており、様々な格好で拡張・類似が与えられている [3, 4, 6]。 $[n] = \{1, \dots, n\}$ とし、 $\binom{[n]}{k} = \{A \subset [n] \mid |A| = k\}$ とする。

定理 1.1 (Erdős–Ko–Rado [5]). $n \geq 2k$ とし、 $\mathcal{A} \subset \binom{[n]}{k}$ とする。そのとき、任意の $A, B \in \mathcal{A}$ に対し、 $A \cap B \neq \emptyset$ ならば、

$$|\mathcal{A}| \leq \binom{n-1}{k-1}$$

が成り立つ。 $n < 2k$ のとき、等号を達成する集合族 \mathcal{A} は、 $[n]$ 上の置換を除いて、

$$\mathcal{A} = \{A \in \binom{[n]}{k} \mid 1 \in A\}.$$

$n = 2k$ のとき、等号を達成する集合族 \mathcal{A} は、任意の $A \in \binom{[n]}{k}$ に対して、 A または $[n] \setminus A$ のどちらか一つを元として持つ。

$L_k = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid x_i \in \{0, 1\}, \sum x_i = k\}$ とする。Erdős–Ko–Rado の定理は、 $A \in \binom{[n]}{k}$ の特性ベクトル $x = (x_1, \dots, x_n) \in L_k$ を用いることで、自然な言い換えが出来る。ここで、 $i \in A$ ならば $x_i = 1$ 、 $i \notin A$ ならば $x_i = 0$ 。 $d(x, y)$ をユークリッド距離とし、 $X \subset \mathbb{R}^n$ に対して、 $D(X) = \max\{d(x, y) \mid x, y \in X\}$ とする。

定理 1.2 (Erdős–Ko–Rado の定理の言い換え). $n \geq 2k$ とし、 $X \subset L_k$ とする。そのとき、任意の $x, y \in X$ に対して、 $d(x, y) < D(L_k) = \sqrt{2k}$ ならば、

$$|X| \leq \binom{n-1}{k-1}$$

が成り立つ。

$(0, -1, 1)$ ベクトルに対して, この定理の拡張を考えたい. $L_{mkl} = (-1^m, 0^k, 1^l)^P$ を $-1, 0, 1$ の個数がそれぞれ m, k, l であるベクトル全体の集合であるとする. また, $n = m+k+l$ とする. 本稿では, 主に次の問題を扱う.

問題 1.3. $D(X) < D(L_{mkl})$ を満たす最大な $X \subset L_{mkl}$ を分類せよ.

最大な X の濃度を M_{mkl} とする. $m = l$ の場合と $m+k \leq l$ の場合は, Erdős–Ko–Rado の定理などを用いることで, 最大な集合を簡単に分類することが出来る.

命題 1.4. $m = l$ とする. そのとき,

$$M_{mkl} = \frac{1}{2} \binom{n}{m} \binom{k+m}{m} = \frac{1}{2} |L_{mkl}|$$

が成り立つ. 最大な集合 X は, 任意の $x \in L_{mkl}$ にたいして, x または $-x$ のどちらかのみを含む.

証明. 任意の $x \in L_{mkl}$ に対して, $\{y \in X \mid d(x, y) = D(L_{mkl})\} = \{-x\}$ であることから従う. \square

命題 1.5. $m+k \leq l$ とする. そのとき,

$$M_{mkl} = \binom{n-1}{m+k-1} \binom{m+k}{m}$$

が成り立つ. $m+k > l$ のとき, 最大な集合 X は, $X = \{(x_1, \dots, x_n) \in L_{mkl} \mid x_1 = 0, -1\}$. $m+k = l$ のとき, 最大な集合 X は, 任意の $J \in \binom{[n]}{l}$ に対して, $\{(x_1, \dots, x_n) \in L_{mkl} \mid x_i = 1, \forall i \in J\}$ または $\{(x_1, \dots, x_n) \in L_{mkl} \mid x_i = 1, \forall i \in [n] \setminus J\}$ のいずれかのみを含む.

証明. $X \subset L_{mkl}$ が $D(X) < D(L_{mkl})$ を満たす必要十分条件は, 任意の異なる $x, y \in X$ に対して, $\{i \mid x_i = -1, 0\} \cap \{i \mid y_i = -1, 0\}$ が空集合でないことである. Erdős–Ko–Rado の定理により, $-1, 0$ の成分位置を決定できる. その成分位置は $\binom{n-1}{m+k-1}$ 通り存在する. $-1, 0$ の成分位置を決定したあと, 取りうる全てのベクトルを考えれば $\binom{m+k}{m}$ 通りのベクトルが存在する. したがって, 命題の主張を得る. \square

本稿では, 次に非自明な場合の $m = 1, l = 2$ について,

$$M_{1k2} = \binom{k+3}{3} + 2$$

であることの証明の概略と, それを達成する集合の分類を紹介する. また, $m = 1, k = 6, l = 2$ の場合の応用として, [2] で未解決とされていた, ジョンソンスキーム $J(9, 4)$ の 4 距離集合としての埋め込みを含む 4 距離集合で, 最大なものの分類を与える.

2 $m = 1, l = 2$ の場合

この節では次の定理の証明の概略を与える.

Theorem 2.1 ([1]). 任意の $k \geq 1$ に対して,

$$M_{1k2} = \binom{k+3}{3} + 2$$

が成り立つ.

次の表記を用いる.

$$(x_1^{\lambda_1}, \dots, x_n^{\lambda_n}) = \underbrace{(x_1, \dots, x_1)}_{\lambda_1}, \dots, \underbrace{(x_n, \dots, x_n)}_{\lambda_n} \in \mathbb{R}^{\lambda_1 + \dots + \lambda_n}.$$

$(x_1^{\lambda_1})$ は $x_1^{\lambda_1}$ と略記する. $(x_1, \dots, x_n) \in \mathbb{R}^n$, $X_i \subset \mathbb{R}^n$ に対して,

$$(x_1, \dots, x_n)^P = \{(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \mid \sigma \in S_n\} \subset \mathbb{R}^n,$$

$$(X_1, \dots, X_m) = \{(x^{(1)}, \dots, x^{(m)}) \mid x^{(i)} \in X_i\} \subset \mathbb{R}^{mn},$$

ここで S_n は対称群を表す.

定理 2.1 において, 最大の集合は以下のように帰納的に定義される.

$k = 1$ のとき:

$$X_1 = (-1, (0, 1^2)^P) \cup (0, (-1, 1^2)^P),$$

$$Y_1 = (1, (-1, 0, 1)^P).$$

$k = 2$ のとき:

$$X_2 = (0, X_1) \cup (-1, (0^2, 1^2)^P),$$

$$Y_2 = (0, Y_1) \cup (-1, (0^2, 1^2)^P),$$

$$Z_2 = (1, (-1, 0^2, 1)^P).$$

$k \geq 3$ のとき:

$$X_k = (0, X_{k-1}) \cup (-1, (0^k, 1^2)^P),$$

$$Y_k = (0, Y_{k-1}) \cup (-1, (0^k, 1^2)^P),$$

$$Z_k = (0, Z_{k-1}) \cup (-1, (0^k, 1^2)^P).$$

X_k, Y_k, Z_k が定理 2.1 の最大の元の個数を達成する集合であり, 成分の置換を除いて他には存在しない.

定理 2.1 は帰納法により証明される. 帰納法のステップにおいて, 次の補題が必要である.

補題 2.2. $k \geq 4$ とし, $X \subset L_{1k2}$ は $D(X) < D(L_{1k2})$ を満たすとする. そのとき, ある i に対して, $|\{(x_1, \dots, x_{k+3}) \in X \mid x_i = 0\}| \geq \binom{k+2}{2} + 2$ を満たす.

証明. この補題は, 0 の個数の平均を各成分に対して取ることで得られる. □

補題 2.3. $k \geq 2$ とする. $M_{1,k-1,2} = \binom{k+2}{2} + 2$ であり, $X_{k-1}, Y_{k-1}, Z_{k-1}$ が, 成分の置換を除いて, 最大な集合であると仮定する. $X \subset L_{1k2}$ が $D(X) < D(L_{1k2})$ を満たし, ある i に対して, $|\{(x_1, \dots, x_{k+3}) \in X \mid x_i = 0\}| = \binom{k+2}{2} + 2$ を満たすとする. そのとき, $|X| \leq \binom{k+3}{3} + 2$ であり, 等号を達成する集合は, 成分の置換を除いて, $X = X_k, Y_k, Z_k$ となる.

証明の概略. L_{1k2} に対して, 最大距離をもつ 2 点を辺で結ぶことにより得られるグラフ (直径グラフ) に, 完全マッチングまたは最大マッチングを与える. その最大マッチングから, グラフの最大独立集合 (孤立点の集合で最大なもの) の分類が得られる. 最大独立集合の分類を与えることは, 補題の最大集合を与えることを意味する. □

$k = 1, 2, 3$ の場合に対しては, 初等的ではあるが, 非常に煩雑な議論により, 最大なもの の分類を与えられる. 基本的には, 含まれる部分集合を決定し, それにどのような元が付け加えられるかを考察する. $k = 1, 2, 3$ において, ソフトウェア Magma を用いて分類することが可能であることを, 講演後に東北大学の宗政昭弘氏にご教授頂いた. $k \leq 3$ の場合が証明されれば, $k \geq 4$ に対して, 補題 2.2, 2.3 を用いることで, 定理 2.1 の証明を与えることは容易い.

3 距離集合への応用

$X \subset \mathbb{R}^n$ が s 距離集合であるとは, 互いに異なる 2 点間の距離の個数 $|\{d(x, y) \mid x, y \in X, x \neq y\}|$ が s であるときを言う. 距離集合の問題のひとつは, 距離の個数 s と次元 n を固定した時に, 最大な元の個数をもつ s 距離集合を決定することである. Bannai–Sato–Shigezumi [2] では, ジョンソンスキーム $J(n, m)$ の m 距離集合としての埋め込み, つまり

$$\tilde{J}(n, m) = (1^m, 0^{n-m})^P$$

を含む最大な m 距離集合を扱っている. ここで, $\tilde{J}(n, m)$ の元は, 成分和が一定であるので, \mathbb{R}^{n-1} の m 距離集合とみなすことが出来る. Bannai–Sato–Shigezumi [2] では, $m \leq 5$ において, $\tilde{J}(n, m)$ を含む最大な m 距離集合の分類を, $\tilde{J}(9, 4)$ 以外の部分で与えている. L_{162} の最大距離を避ける最大な部分集合の分類を用いることで, 未解決として残されていた, $\tilde{J}(9, 4)$ を含む 4 距離集合の分類を与えることができる.

以下の 4 つの集合の任意の元は, $\tilde{J}(9, 4) = (1^4, 0^5)^P$ に 4 距離集合を保ったまま加えるこ

とができる.

$$\begin{aligned} X^{(i)} &= \left(\left(\frac{2}{3} \right)^7, \left(-\frac{1}{3} \right)^2 \right)^P, & X^{(ii)} &= \left(\left(\frac{2}{3} \right)^8, -\frac{4}{3} \right)^P, \\ X^{(iii)} &= \left(\frac{4}{3}, \left(\frac{1}{3} \right)^8 \right)^P, & X^{(iv)} &= \left(\left(\frac{4}{3} \right)^2, \left(\frac{1}{3} \right)^6, -\frac{2}{3} \right)^P. \end{aligned}$$

$X^{(iv)}$ と $(-1^1, 0^6, 1^2)^P$ は距離集合として同型(等長写像が存在する)である. $(-1^1, 0^6, 1^2)^P$ の最大距離を避ける最大部分集合 X_6, Y_6, Z_6 に対応する $X^{(iv)}$ の部分集合を, それぞれ X'_6, Y'_6, Z'_6 とする. $\tilde{J}(9, 4)$ の距離の種類が $\sqrt{2}, \sqrt{4}, \sqrt{6}, \sqrt{8}$ であることに注意すると, 全ての元を同時に $\tilde{J}(9, 4)$ へ加えられる最大な $X^{(iv)}$ の部分集合は, X'_6, Y'_6, Z'_6 であることが分かる. そのことに注意し, さらに $X^{(i)}, X^{(ii)}, X^{(iii)}, X^{(iv)}$ の間の距離関係を調べることで, 次の定理を得る.

Theorem 3.1 ([1]). $X \subset \{(x_1, \dots, x_9) \in \mathbb{R}^9 \mid x_1 + \dots + x_9 = 1\}$ を $\tilde{J}(9, 4)$ を含む 4 距離集合であるとする. そのとき,

$$|X| \leq 258$$

が成り立つ. 等号が達成されるときは, 成分の置換を除いて, X は次のいずれかとなる.

- (1) $\tilde{J}(9, 4) \cup X^{(i)} \cup X^{(iii)} \cup \{(-4/3, (2/3)^8)\} \cup X'_6,$
- (2) $\tilde{J}(9, 4) \cup X^{(i)} \cup X^{(iii)} \cup \{(-4/3, (2/3)^8)\} \cup Y'_6,$
- (3) $\tilde{J}(9, 4) \cup X^{(i)} \cup X^{(iii)} \cup \{(-4/3, (2/3)^8)\} \cup Z'_6.$

定理 3.1(1) の集合は, [2] において最大であると予想されていた. ここでは, その予想の解決と, 新たに (2), (3) の集合を得ることが出来た. (1), (2), (3) の集合は, どの 2 つも距離集合として同型でない. それは, 例えば距離が $\sqrt{2}$ となる二頂点を結んで得られるグラフが, 非同型であることから確かめられる.

4 他の M_{mkl} について

著者たち [1] と同時期に Frankl–Kupavskii [7] は, 本稿で扱った問題 1.3 について, 独立に結果を得ている.

Theorem 4.1 ([7]). $m = 1$ のとき, 次が成立する.

$$M_{1kl} \leq \begin{cases} l \binom{n-1}{l}, & 2l \leq n \leq l^2 \text{ のとき,} \\ l \binom{l^2-1}{l} - \binom{l^2}{l+1} + \binom{n}{l+1}, & n > l^2 \text{ のとき.} \end{cases}$$

$n = l^2 + 1$ のとき, $l \binom{n-1}{l} = l \binom{l^2-1}{l} - \binom{l^2}{l+1} + \binom{n}{l+1}$ となることに注意されたい. 定理 4.1 の等号を達成する集合 X は, [7] で以下のように与えられているが, 成分の置換を除いての

分類は与えられていない.

$2l \leq n \leq l^2 + 1$ のとき:

$$X = \{(x_1, \dots, x_n) \in L_{1kl} \mid x_1 = 1\}.$$

$n \geq l^2 + 1$ のとき:

$$X = \mathcal{P}^{n-l^2}((1, (-1, 0^{l^2-l-1}, 1^{l-1})^P)). \quad (1)$$

$n \geq l^2 + 2$ のとき:

$$X = \mathcal{P}^{n-l^2-1}((1, (-1, 0^{l^2-l}, 1^{l-1})^P)). \quad (2)$$

ここで, $X \subset L_{1kl}$ に対して, $\mathcal{P}(X) = (0, X) \cup (-1, (0^{k+1}, 1^l)^P) \subset L_{1,k+1,l}$ と定義される. 定理 2.1 における最大な集合は, Y_k が (1) にあたり, Z_k が (2) にあたる.

参考文献

- [1] S. Adachi, and H. Nozaki, On the largest subsets avoiding the diameter of $(0, \pm 1)$ -vectors, to appear in *Ars Math. Contemp.*
- [2] E. Bannai, T. Sato, and J. Shigezumi, Maximal m -distance sets containing the representation of the Johnson graph $J(n, m)$, *Discrete Math.* **312** (2012), no. 22, 3283–3292.
- [3] P. Borg, Intersecting families of sets and permutations: a survey, *Int. J. Math. Game Theory Algebra* **21** (2012), 543–559.
- [4] M. Deza, and P. Frankl, The Erdős–Ko–Rado theorem - 22 years later, *SIAM J. Algebraic Discrete Methods* **4** (1983), 419–431.
- [5] P. Erdős, C. Ko, and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford Ser. (2)* **12** (1961), 313–320.
- [6] P. Frankl, The shifting technique in extremal set theory, in: C. Whitehead (Ed.), *Combinatorial Surveys*, Cambridge Univ. Press, London/New York, 1987, pp. 81–110.
- [7] P. Frankl, and A. Kupavskii, Erdős–Ko–Rado theorem for $\{0, \pm 1\}$ -vectors, preprint, arXiv:1510.03912.

On algebraic problems I worked on for development of
 crystallographic software *CONOGRAPH*
 (結晶学ソフトウェア *CONOGRAPH* の開発中に
 出会った代数学の諸問題について)

Ryoko Oishi-Tomiyasu*

April 17, 2016

Abstract

When the author developed crystallographic software called *CONOGRAPH*, it was necessary to resolve some algebraic problems concerning ternary positive-definite quadratic forms with real coefficients: (a) when a part of representations over \mathbb{Z} of an unknown quadratic form is given, determine the equivalence class of the quadratic form (powder indexing), (b) when observed values of $a_{ij} \in \mathbb{R}$ of a quadratic form $\sum_{1 \leq i < j \leq 3} a_{ij} x_i x_j$ are provided, determine the Bravais type of the quadratic form in as small a number of steps as possible, considering observational errors in a_{ij} (error-stable Bravais-lattice determination). The theorems used to solve these problems are introduced.

Introduction

“Powder indexing” and “error-stable Bravais-lattice determination” are the following problems discussed in mathematical crystallography to deal with some kind of experimental data:

- (a) powder indexing: when partial information about representations over \mathbb{Z} (*i.e.*, some elements of $\{f(x) : 0 \neq x \in \mathbb{Z}^n\}$) of an unknown positive-definite quadratic form f is given, determine the equivalence class of the quadratic form.
- (b) error-stable Bravais-lattice determination: when the coefficients $a_{ij} \in \mathbb{R}$ of a positive-definite quadratic form $\sum_{1 \leq i < j \leq 3} a_{ij} x_i x_j$ contain observational errors, determine the Bravais type of the original quadratic form in as small a number of steps as possible, under consideration for observational errors in a_{ij} ,

where the equivalence class of a quadratic form (over \mathbb{Z}) is defined from the equivalence relation: $f \sim g \stackrel{\text{def}}{\iff} f(x) = g(xw)$ for some $w \in GL_3(\mathbb{Z})$. The *isometry group* $\text{Isom}(f)$ of f consists of all the $w \in GL_3(\mathbb{Z})$ with $f(xw) = f(x)$. Two positive-definite quadratic forms f_1, f_2 belong to the same Bravais type, if $\text{Isom}(f_1)$ and $\text{Isom}(f_2)$ are conjugate in $GL_3(\mathbb{Z})$.

The above two problems have been mainly discussed in mathematical crystallography for an analysis of observed data (*e.g.*, Chap. 7, [6]; 9.2.5, 9.3.2, [13]). What follows, only the cases of ternary quadratic forms are discussed, although the cases of a general rank

*Yamagata University/JST PRESTO (ryoko.tomiyasu@sci.kj.yamagata-u.ac.jp)

has been also a scope of interest in the community of mathematical crystallography for analyses of quasicrystal samples. The differences of (a) and (b) from similar problems in pure mathematics (*e.g.*, [32], [33], [27]) are caused by the lack of information and the existence of observational errors.

In the following Sections 1, 2, the theorems in [22], [23] used by the author to provide new algorithms for (a) and (b) are introduced. Some reduction theory of quadratic forms is used to construct a framework for (a). Recall that when $\mathcal{S}_{>0}^n$ is the set of all the n -ary positive-definite quadratic forms, the reduction theories aim to provide a tessellation of $\mathcal{S}_{>0}^n/\mathbb{R}^\times$ by using a finite set of tiles $\mathcal{D}_i \subset \mathcal{S}_{>0}^n/\mathbb{R}^\times$, and its translations $\mathcal{D}_i[g] := \{gS^t g : S \in \mathcal{D}_i\}$ for some $g \in GL_3(\mathbb{Z})$.

Our study for (b) was originally motivated by a necessity to execute the determination multiple-times after powder indexing in short time. In general, observational errors contained in experimental data cannot be formulated accurately. However, if the following may be assumed, it is always possible to obtain a finite set of quadratic forms and its isometry group that contains the correct one:

- (A) Let $S^{obs} \in \mathcal{S}^3$ be the observed quadratic form of a positive-definite $S \in \mathcal{S}_{>0}^3$. If a parameter $p \in \mathbb{R}$ satisfies $p \geq S^{obs}(x)/2$ or $p \geq (S^{obs})^{-1}(x)/2$ theoretically for some $0 \neq x \in \mathbb{Z}^3$, the observed value p^{obs} is also positive.

Note that it is indicated from (A) that S^{obs} is also positive-definite, similarly to the original S . (A) is considered to be true in normal experimental data, although the propagation of overestimated errors may sometimes make (A) false. Any algorithms for Bravais-lattice determination require such an assumption, because infinitely many candidates for the true solution may be generated otherwise. This follows from the fact that \mathcal{T}_i intersects at the boundary of $\mathcal{S}_{>0}^n/\mathbb{R}^\times$ with infinitely many of $\mathcal{T}_j[g]$ ($g \in GL_3(\mathbb{Z})$).

Almost of all the proofs of the theorems and computational results are omitted herein. See the author's cited papers, if necessary. The algorithms are used in powder indexing software *CONOGRAPH* distributed at <https://z-code.kek.jp/zrg/> for users of neutron-source and synchrotron facilities.

What follows, notation and symbols used in this article are listed. A *lattice* $L \subset \mathbb{R}^N$ is a discrete \mathbb{Z} -submodule generated by linearly independent $l_1, \dots, l_N \in \mathbb{R}^N$ over \mathbb{R} . This $\langle l_1, \dots, l_N \rangle$ is called a *basis* of L . In this article, $2D$, $3D$ are used to represent the lattice rank $N = 2, 3$. If $\{k_1, \dots, k_i\} \subset L$ ($1 \leq i < N$) is a subset of some basis of L , the $\{k_1, \dots, k_i\}$ is called a *primitive set* of L . The Euclidean norm of \mathbb{R}^N is represented by $|\cdot|^2$.

If a lattice L has a basis $\langle l_1, \dots, l_N \rangle$, L is associated with the N -ary quadratic form $\sum_{i=1}^N |x_i l_i|^2$, which is called the *quadratic form* of L . Throughout this article, a quadratic form $\sum_{1 \leq i \leq j \leq N} a_{ij} x_i x_j$ is always identified with the N -by- N symmetric matrix with a_{ii} in the diagonal entries and $a_{ij}/2$ in the other entries.

On the space \mathcal{S}^N consisting of N -by- N symmetric matrices, an inner product is defined by

$$\langle S, T \rangle := \text{Trace}(ST) = \sum_{i=1}^N \sum_{j=1}^N s_{ij} t_{ij}. \quad (1)$$

The subset of \mathcal{S}^N consisting of positive-definite (*resp.* positive-semidefinite) symmetric matrices is denoted by $\mathcal{S}_{>0}^N$ (*resp.* $\mathcal{S}_{\geq 0}^N$). For any $S \in \mathcal{S}^N$ and $g \in GL_3(\mathbb{Z})$, $gS^t g$ is denoted by $S[g]$. For any subset $D \subset \mathcal{S}^N$ and a matrix g , a new domain $D[g]$ is defined as $\{S[g] : S \in D\}$. The identity matrix of size N is denoted by I_N .

1 Powder indexing

1.1 Outline of powder indexing

Powder indexing is a lattice determination problem in crystallography that aims to retrieve the crystal lattice from experimental data called powder diffraction patterns. Mathematically, powder indexing can be formulated as the lattice determination from an average theta series. The advantage of doing this is that it clarifies that problems in powder indexing such as “systematic absence” and “existence of more than one solutions” remain after all the experimental problems are removed.

First let $L \subset \mathbb{R}^N$ be a lattice of rank N . A *periodic point set* is a union of finite number of translations of L as follows:

$$P := \bigcup_{i=1}^m (x_i + L) \subset \mathbb{R}^N. \quad (2)$$

When $N = 3$, P can be regarded as a simple model of a crystal structure. In [5], the average theta series of P is defined by:

$$\Theta_P(z) := \frac{1}{m} \sum_{i=1}^m \sum_{j=1}^m \sum_{l \in L} e^{\pi\sqrt{-1}z|l+x_i-x_j|^2}. \quad (3)$$

The following is the functional equality of $\Theta_P(z)$ obtained from the Poisson summation formula:

$$\Theta_P(z) = \frac{1}{\text{mvol}(\mathbb{R}^N/L)} \left(\frac{\sqrt{-1}}{z} \right)^N \sum_{l^* \in L^*} \exp\left(-\frac{\pi\sqrt{-1}|l^*|^2}{z}\right) \left| \sum_{i=1}^m e^{-2\pi\sqrt{-1}x_i \cdot l^*} \right|^2,$$

where L^* is the reciprocal lattice of L defined by:

$$L^* := \{l^* \in \mathbb{R}^N : l \in L \Rightarrow l \cdot l^* \in \mathbb{Z}\}. \quad (4)$$

What follows, it is always assumed that L is the maximum lattice contained in P , *i.e.*, $l \in L \Leftrightarrow P = P + l$ holds for any $l \in \mathbb{R}^3$. The $\Theta_P(z)$ can be also written as follows:

$$\Theta_P(z) = \frac{1}{\text{mvol}(\mathbb{R}^N/L)} \left(\frac{\sqrt{-1}}{z} \right)^N \sum_{q \in \Lambda_P} \exp\left(-\frac{\pi\sqrt{-1}q}{z}\right) F_P(q), \quad (5)$$

$$\Lambda_P := \left\{ |l^*|^2 : 0 \neq l^* \in L^*, F_{P,l^*} \neq 0 \right\}, \quad (6)$$

$$F_P(q) := \sum_{l^* \in L^*, q=|l^*|^2} |F_{P,l^*}|^2, \quad (7)$$

$$F_{P,l^*} := \sum_{i=1}^m \exp(-2\pi\sqrt{-1}x_i \cdot l^*). \quad (8)$$

Therefore, the information contained in $\Theta_P(z)$ is same as that obtained from Λ_P and $F_P(q)$.

What follows, suppose that $N = 3$, and the quadratic form of L and x_i are parameters with unknown values. Information about $\Theta_P(z)$ is provided as observed data. Under this situation, the procedures to determine L is called “powder indexing”. The subsequent process to determine x_i is called “ab-initio powder crystal structure determination”. Normally, in powder indexing, L (or equivalently, L^*) is determined only from Λ_P , and x_i ($1 \leq i \leq m$) are subsequently determined from $F_P(q)$. The method to convert a powder diffraction pattern to an average theta series is explained in the Appendix of [20].

1.2 Systematic absence in crystallography

Systematic absence (SA) and existence of more than one solution are chief obstacles against the lattice determination, and may occur even if the completely accurate information about Θ_P is available. As explained in the following, SA is determined only from the group symmetry of a periodic point set. Although this is one of the achievements of applied mathematics widely recognized in crystallography, SA do not seem to have been defined in a mathematical style. Normally, SA is explained by providing a concrete example as in Example 1.

First, let Λ_L be the following set:

$$\Lambda_L := \{|l^*|^2 : 0 \neq l^* \in L^*\}. \quad (9)$$

From the definition (6), Λ_P is contained in Λ_L . However, how much difference exists between Λ_P and Λ_L ? It is possible to provide a simple algorithm to determine L from Λ_L , if the rank of L is less than 5 [24], although $\Lambda_P = \Lambda_L$ does not generally hold. (Here, “to determine” means to obtain all the possible solutions if the solution is not unique. Such an algorithm is possible as long as L has rank < 5 , because infinitely many solutions may exist otherwise.) In actual cases given by real crystals, it may be thought that $F_{P,l^*} = 0$ for many $l^* \in L^*$ generally happens owing to SA.

Before proceeding to the definition of SA, recall the definition of crystallographic groups; for any congruent transformation σ of \mathbb{R}^N , there exist $\tau \in O(N)$ and $\nu \in \mathbb{R}^N$ such that σ is represented as follows:

$$x^\sigma = x^\tau + \nu \quad (\forall x \in \mathbb{R}^N). \quad (10)$$

The σ is represented by $\{\tau|\nu\}$. From the decomposition, $O(N) \times \mathbb{R}^N$ may be regarded as the group of all the congruent transformation of \mathbb{R}^N .

A group G is a *crystallographic group*, if it is a discrete and cocompact subgroup of $O(N) \times \mathbb{R}^N$, where the topology of $O(N) \times \mathbb{R}^N$ is the product of the standard topology of $O(N)$ and \mathbb{R}^N . When $N = 2, 3$, G is also called a *wallpaper group* and a *space group*.

In general, G has a subgroup $L := G \cap (\{1\} \times \mathbb{R}^N)$ consisting of all the translations in G . As a group, $L \cong \mathbb{Z}^N$, and may be identified as a lattice in \mathbb{R}^N . The subgroup $R := G/L \subset O(N)$ is a finite group, and called the *point group* of G . From the definition of L , for any $\{\tau|\nu_\tau\} \in G$, the class $\nu_\tau + L \in \mathbb{R}^N/L$ is uniquely determined. Furthermore, the map $R_G \rightarrow \mathbb{R}^N/L : \tau \rightarrow \nu_\tau + L$ is a 1-cocycle, *i.e.*, it satisfies $\nu_{\sigma\tau} \equiv \nu_\sigma^\tau + \nu_\tau \pmod{L}$. In this way, G is assigned to the cohomology classes of $\tau \mapsto \nu_\tau + L$, which provides a well-known correspondence between group extensions of L by R_G and $H^2(R_G, L) \cong H^1(R_G, \mathbb{R}^N/L)$.

Let $(\mathbb{R}^N)^H \subset \mathbb{R}^N$ be the subset consisting of all the $x \in \mathbb{R}^N$ fixed by all of $h \in H$.

Definition 1.1. Let G be a crystallographic group with the translation subgroup L , $H \subset G$ be a subgroup with $(\mathbb{R}^N)^H \neq \emptyset$. Such a (G, H) is called a type of systematic absence (SA). Let L^* be the reciprocal lattice of L . If $l^* \in L^*$ is contained in the following $\Gamma_{ext}(G, H)$, we shall say that SA of type (G, H) holds for l^* :

$$\Gamma_{ext}(G, H) := \left\{ l^* \in L^* : \sum_{\sigma \in H \setminus G/L} \exp(2\pi\sqrt{-1}x^\sigma \cdot l^*) = 0 \text{ for any } x \in (\mathbb{R}^N)^H \right\}.$$

For any $x \in (\mathbb{R}^N)^H$, a periodic point set is defined by $P_{x,G} = \{x^\sigma : \sigma \in G\}$. From the definition, SA of type (G, H) holds for $l^* \in L^*$ if and only if $F_{P_{x,G},l^*} = 0$ holds for any $x \in (\mathbb{R}^N)^H$. In general, the value of such an $|l^*|^2$ cannot be extracted from Θ_P , if P is represented as $\bigcup_{i=1}^m P_{x_i,G}$ for some $x_i \in (\mathbb{R}^N)^H$. Contrarily, even if SA does not hold for $l^* \in L^*$, there is still possibility that $|l^*|^2$ cannot be obtained from

Θ_P , if $F_P(q) = 0$ occurs, due to some coincidence (under observational errors, this also happens for l^* with very small $|F_P(q)|$). Although the cases of SA are mainly discussed in the following sections, the algorithm in Section 1.4 can handle lack of information, due to a reason other than SA, if the assumptions (a)–(c) in Section 1.3 are assumed.

The following are general properties of SA. For the proof, several facts known in the theory of the Galois cohomology are used.

Lemma 1.1 (Lemma C.1, [25]). *Let R_H be the image of H by the natural onto map $G \rightarrow R_G : \{\sigma|\nu_\sigma\} \mapsto \sigma$. For fixed $l^* \in L^*$, the equivalence relation among the right cosets $R_H \backslash R_G$ is defined by:*

$$R_H \sigma_1 \stackrel{l^*}{\sim} R_H \sigma_2 \stackrel{def}{\iff} \sum_{\sigma \in R_H \sigma_1} \sigma l^* = \sum_{\sigma \in R_H \sigma_2} \sigma l^*. \quad (11)$$

For any $x \in \mathbb{R}^N$ stabilized by H , $l^* \in L^*$ belongs to $\Gamma_{ext}(G, H)$ if and only if for every $R_H \sigma_1 \in R_H \backslash R$, we have

$$\sum_{R_H \sigma_2 \stackrel{l^*}{\sim} R_H \sigma_1} e^{2\pi i x \cdot \{\sigma_2 | \nu_{\sigma_2}\} \cdot l^*} = 0. \quad (12)$$

The following are corollaries of the above Lemma:

Corollary 1.1 (Corollary 4.1, [21]). *Let L be the translation subgroup of a crystallographic group G , and M be the order of $R_G := G/L$. For any type (G, H) of SA, there exists a union $\mathcal{H}_{G,H} \subset \mathbb{R}^N$ of linear subspaces of \mathbb{R}^N of dimension $< N$ and a subset $\Omega \subset L^*/ML^*$ such that for any $l^* \in L^*$, $\notin \mathcal{H}_{G,H}$, the following holds:*

$$l^* \in \Gamma_{ext}(G, H) \iff l^* + ML^* \in \Omega \quad (13)$$

□

Corollary 1.2 (Proposition 3, [25]). *Let M be the index $[G : L]$ and ML^* be the set $\{Ml^* : l^* \in L^*\}$. Then $ML^* \cap \Gamma_{ext}(G, H) = \emptyset$ holds regardless of the choice of (G, H) .*

We already described that L can be retrieved from Λ_P , if $\Lambda_P = \Lambda_L$. This is true even if only $\Lambda_P \supset M\Lambda_L$ holds for some known integer M [25]. According to Corollary 1.2, $q \in M\Lambda_L$, $q \notin \Lambda_P$ happens, owing to a reason other than SA.

In $N = 2$, there are 17 isomorphism classes of wallpaper groups. In $N = 3$, there are 219 classes (or 230 if distinct chiral copies are counted.) In [13], 72 types of SA for wallpaper groups, and about 1700 types for space groups are listed, and $\Gamma_{ext}(G, H)$ for all the types (G, H) are described.

The following is an example of SA in the case of $F d d 2$ (Hermann-Mauguin symbol).

Example 1. *Let $L \subset \mathbb{R}^3$ be the lattice with the basis $(a, b, 0)$, $(a, 0, c)$, $(0, b, c) \in \mathbb{R}^3$ for some $0 \neq a, b, c \in \mathbb{R}$. L is a face-centered orthorhombic lattice, and fixed by the $\tau_1, \tau_2 \in O(3)$ with the following action on \mathbb{R}^3 :*

$$\begin{aligned} \tau_1 & : (x, y, z) \mapsto (-x, -y, z), \\ \tau_2 & : (x, y, z) \mapsto (-x, y, z). \end{aligned}$$

$F d d 2$ is the space group generated by $\sigma_1 := \{\tau_1 | (0, 0, 0)\}$, $\sigma_2 := \{\tau_2 | (a/2, b/2, c/2)\}$, in addition to all the elements of L . If H is the the group of order 2 generated by σ_1 , we have $(\mathbb{R}^3)^H = \{(0, 0, z) : z \in \mathbb{R}\}$. Any $l^* \in L^*$ is represented as follows, by using some integers h, k, l .

$$l^* = \left(\frac{h+k-l}{2a}, \frac{h-k+l}{2b}, \frac{-h+k+l}{2c} \right).$$

When h, k, l are fixed, for any $x := (0, 0, z) \in (\mathbb{R}^3)^H$,

$$\begin{aligned} F_{P_{x,G},l^*} &= \sum_{\sigma \in H \setminus G/L} \exp(2\pi\sqrt{-1}x^\sigma \cdot l^*) \\ &= \exp\left(\frac{2\pi\sqrt{-1}z(-h+k+l)}{2c}\right) + \exp\left(\frac{2\pi\sqrt{-1}(z+c/2)(-h+k+l)}{2c}\right) \\ &= \exp\left(\frac{2\pi\sqrt{-1}z(-h+k+l)}{2c}\right) \left(1 + \exp\left(2\pi\sqrt{-1} \cdot \frac{-h+k+l}{4}\right)\right). \end{aligned}$$

From this, $l^* \in \Gamma_{ext}(G, H)$ holds if and only if $-h+k+l \equiv 2 \pmod{4}$.

1.3 Idea of the algorithm for powder indexing using topographs

Herein, the background of Theorems 1–3 in the next section is explained; we shall start from the algorithm of the program *ITO* which was invented by a crystallographer Ito [14], improved by de Wolff [7], and implemented by Visser [29]. Ito's original idea is to obtain the binary quadratic forms of a sublattice contained in the solution L^* , by using the following identity called the parallelogram law:

$$2(|l_1|^2 + |l_2|^2) = |l_1 + l_2|^2 + |l_1 - l_2|^2. \quad (14)$$

If q_1, q_2, q_3, q_4 with $2(q_1 + q_2) = q_3 + q_4$ are found among observed elements of Λ_P , *ITO* assumes that there are some $l_1, l_2 \in L^*$ such that $q_1 = |l_1|^2$, $q_2 = |l_2|^2$, $q_3 = |l_1 + l_2|^2$ and $q_4 = |l_1 - l_2|^2$. Under the assumption, the binary quadratic form of the lattice expanded by l_1, l_2 is computable by:

$$\begin{pmatrix} q_1 & (q_1 + q_2 - q_4)/2 \\ (q_1 + q_2 - q_4)/2 & q_2 \end{pmatrix} \quad (15)$$

Although this estimation may seem to be no problem, it is known that *ITO* does not work well in particular when SA holds for some $l^* \in L^*$. This is because some assumptions used in *ITO* are not always true, or even never true in some cases (in this point, similarly to the other powder indexing algorithms, *ITO* cannot be regarded as a mathematical algorithm, because it is not based on mathematical reasoning.) For example, *ITO* assumes that the true solution L^* always contains a primitive set $\{l_1, l_2\}$ of L^* such that all of $|l_1|^2, |l_2|^2, |l_1 + l_2|^2, |l_1 - l_2|^2$ are observed as elements of Λ_P . However, in the cases some types of SA happen, L^* contains none of such primitive sets.

In Section 1.2, powder indexing is formulated as a lattice determination problem from Θ_P . If $\Lambda^{obs} \subset \Lambda_P$ is extracted from real observed data (*i.e.*, powder diffraction patterns), and the observational error $\text{Err}[q_{obs}]$ of $q^{obs} \in \Lambda^{obs}$ is ignored for simplicity (it is straightforward to reformulate all the discussions under consideration of $\text{Err}[q^{obs}]$, as in the original papers), the following may be assumed:

- (a) The range of Λ^{obs} is contained in a bounded interval $[q_{min}, q_{max}] \subset (0, \infty)$.
- (b) For any $q \in \Lambda_P \cap [q_{min}, q_{max}]$, $q \notin \Lambda^{obs}$ occurs with unknown small probability ϵ_1 . In addition, for any $q^{obs} \in \Lambda^{obs}$, $q \notin \Lambda_P$ occurs with unknown small probability ϵ_2 .
- (c) owing to repulsive forces between atoms, there exists a constant D ($\approx 2\text{\AA}$) such that $|l| > D$ holds for any $l \in L$ and all the existing crystal lattices L .

In the case of real powder diffraction data, the observed range $[q_{min}, q_{max}]$ is supposed to be adjusted to the size of considered L . In addition, larger elements in Λ^{obs} have less accuracy in their observed values, *e.g.*, the values of $|l^*| > 5\text{\AA}^{-1}$ of a reciprocal

lattice vector $l^* \in L^*$ are almost indistinguishable from observed data. Therefore, the last condition (c) is important for successful powder indexing; with regard to the third successive minimum D_3^* of L^* , the following is proved from (c) and an inequality in [16]:

$$D_3^* \leq 3 \cdot 2^{-1/3} D^{-2} \approx 0.6 \text{\AA}^{-2}. \quad (16)$$

The inequality indicates that even if $q_{max} < 5 \text{\AA}^{-1}$, Λ^{obs} normally contains sufficient information to obtain the quadratic form of L^* .

In the situation explained so far, our idea for the lattice determination is to use topographs defined in [4], as a sorting criterion of 2D lattices generated from Λ^{obs} . As a consequence, our algorithm can be explained in a picturesque way.

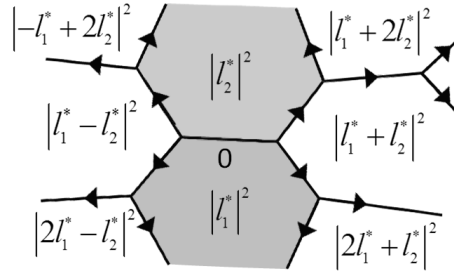


Figure 1: A topograph (at most one edge in a topograph can have orientation 0.)

As a property of the topograph, the following can be easily observed from Figure 1; for any fixed edge, if the two domains adjacent across the edge are labeled with $|l_1|^2$, $|l_2|^2$, the two other domains which touch an endpoint of the edge are labeled with $|l_1 + l_2|^2$, $|l_1 - l_2|^2$. Therefore, as stated in [4], every edge of a topograph is associated with a

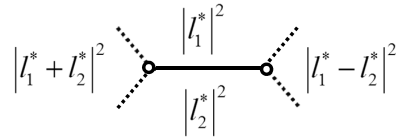


Figure 2: Four lattice-vector lengths associated with an edge of a topograph

set of four lattice-vector lengths satisfying the parallelogram law. In [4], topographs are used to explain the Selling reduction for 2D lattices. For a general rank $N > 0$, the fundamental domain $\mathcal{D}^N \subset \mathcal{S}_{>0}^N / \mathbb{R}_{>0}$ consists of $S \in \mathcal{S}_{>0}^N$ that satisfy:

$$\langle S, A_N \rangle \leq \langle S[g], A_N \rangle \text{ for any } g \in GL_3(\mathbb{Z}), \quad (17)$$

where $A_N \in \mathcal{S}_{>0}^N$ is the matrix with 2 in all the diagonal entries and 1 in the others.

If we put $St(A_N) := \{g \in GL(N, \mathbb{Z}) : {}^t g A_N g = A_N\}$, the right-hand domains are disjoint except for their boundaries, hence the following union provides a tessellation of $\mathcal{S}_{>0}^N / \mathbb{R}_{>0}$:

$$\mathcal{S}_{>0}^N / \mathbb{R}_{>0} = \bigcup_{g \in St(A_N) \backslash GL_N(\mathbb{Z})} \mathcal{D}^N[g] \quad (18)$$

The graph structure of a topograph is the same as the dual of the above tessellation, *i.e.*, it is the graph obtained by regarding $St(A_N) \backslash GL_N(\mathbb{Z})$ as the set of all the nodes,

and by connecting two nodes $St(A_N)g_1$ and $St(A_N)g_2$ if $\mathcal{D}^N[g_1]$ and $\mathcal{D}^N[g_2]$ have a common facet.

The first advantage of using topographs is that a method to verify the assumption mentioned after (14) is naturally provided; if some sets of q_1, q_2, q_3, q_4 satisfying $q_1 + q_2 = 2(q_3 + q_4)$ are found in Λ^{obs} , topographs can be formed from those sets; first, an edge of a topograph is formed for such q_1, q_2, q_3, q_4 as in Figure 2, by assuming as in *ITO* that there exist $l_1, l_2 \in L^*$ such that $q_1 = |l_1|^2$, $q_2 = |l_2|^2$, $q_3 = |l_1 + l_2|^2$, $q_4 = |l_1 - l_2|^2$. After multiple edges are obtained, by searching for edges that have a common node and joining them as in Figure 3, subgraphs of topographs are generated. If the assumption

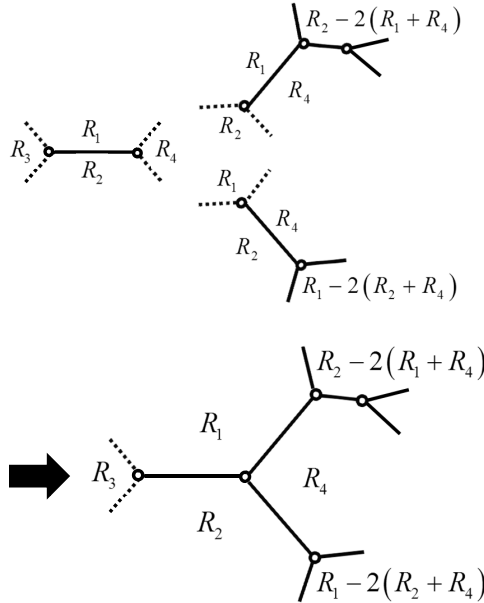


Figure 3: Connection of topographs with the same node

is false, and there do not exist $l_1, l_2 \in L^*$ such that $q_1 = |l_1|^2$, $q_2 = |l_2|^2$, $q_3 = |l_1 + l_2|^2$, $q_4 = |l_1 - l_2|^2$, the subgraph containing the edge will not have a number of edges, because the probability that all of the observed lengths accidentally satisfy the parallelogram law is rather small. Conversely, if such $l_1, l_2 \in L^*$ really exist, even if Λ^{obs} is a little different from Λ_P , the subgraph will grow. This estimation seems to work, at least unless SA happens. This is actually proved for any types of SA of wallpaper groups (Th. 1, [23]). Although the same thing does not hold for space groups, similar things can be proved if a different identity is used, instead of the parallelogram law.

As another advantage, topographs can be utilized as a framework to discuss common rules (distribution rules on topographs) of SA, as in Section 1.4. Although some types (G, H) of SA, have complex conditions for $l^* \in \Gamma_{ext}(G, H)$ when G is a space group, an algorithm that works regardless of the type of SA is provided by the distribution rules. However, our initial goal was to prove the rules by using properties of topographs generalized for 3D lattices, which has not been achieved in the *CONOGRAPH* software project. Therefore, all the theorems in this article were searched for by a computer. For the proof, Corollary 1.1, some properties of convex bodies in \mathbb{R}^3 and an exhaustive check by a computer were utilized. In $N = 3$, if M is taken as in Theorem 1.1, $\Gamma_{ext}(G, H)$ for some type (G, H) contains half of L^*/ML^* . Thus, before the search, it was not clear whether such common properties really exist.

In order to discuss the distribution rules, the definition of topographs should be generalized for ternary quadratic forms. With regard to the method of the generalization,

there seem to be two candidates (Section 1.4 is understandable, even if the following part is skipped):

1. (Well-rounded retract [26]) For any finite subset $\Phi \subset \mathbb{Z}^N$, define

$$\mathcal{D}(\Phi) := \{S \in \mathcal{S}_{>0}^N : \text{for any } v \in \Phi, {}^t v S v = \min\{{}^t u S u : 0 \neq u \in \mathbb{Z}^N\}\}.$$

In this case, $\mathcal{D}(\Phi)$ is convex in \mathcal{S}^N , and $\mathcal{S}_{>0}^N/\mathbb{R}_{>0} = \bigcup_{\mathcal{D}(\Phi) \neq \emptyset} \mathcal{D}(\Phi)/\mathbb{R}_{>0}$. When the cardinality of $\Phi = 1$ (resp. 2), $\mathcal{D}(\Phi) \neq \emptyset$, and has dimension $N(N+1)/2$ (resp. $N(N+1)/2 - 1$) if and only if Φ is a primitive set of \mathbb{Z}^N . A *well-rounded retract* of $\mathcal{S}_{>0}^N/\mathbb{R}_{>0}$ is defined as the subset $\aleph := \bigcup_{\substack{\mathcal{D}(\Phi) \neq \emptyset, \\ \Phi \text{ generate } \mathbb{Z}^N}} \mathcal{D}(\Phi)/\mathbb{R}_{>0}$ of $\mathcal{S}^N/\mathbb{R}_{>0}$. If $N = 2$, a topograph can be identified with \aleph , because they are homeomorphic, and the association of lattice vectors with edges and nodes of topographs are also provided by the natural map $\mathcal{D}(\Phi) \mapsto \Phi$.

2. (*C*-type reduction [28]) Let $[u]$ be the class of $u \in \mathbb{Z}$, when u and $-u$ are identified. Let Φ be a set of 2^N such classes, and assume that the natural map $\Phi \rightarrow \mathbb{Z}^N/2\mathbb{Z}^N$ is onto. For such a Φ , the convex cones $\mathcal{C}(\Phi)$ is defined by:

$$\mathcal{C}(\Phi) := \{S \in \mathcal{S}_{>0}^N : \text{for any } [v] \in \Phi, {}^t v S v = \min\{{}^t u S u : u \in v + 2\mathbb{Z}^N\}\}.$$

Only $\mathcal{C}(\Phi)$ containing interior points is used for the tessellation. Similarly to the Voronoi reduction of the first and the second kind [30], [31], the tessellation of the *C*-type reduction coincides with that of the Selling reduction if $N = 2$. Even if the definition of topographs is generalized to $N > 2$, the relation between the edges of a topograph and the parallelogram law naturally holds, *i.e.*, if two distinct *C*-type domains with interior points share a facet, the facet is naturally associated with the 4 vectors $\pm l_1^*, \pm l_2^*, \pm(l_1^* \pm l_2^*)$, because of the following proposition:

Proposition 1.1 (Proposition 5.1, [21]). *Suppose that two distinct C-type domains containing interior points have an $(\frac{N(N+1)}{2} - 1)$ -dimensional cone as their intersection. Then $\Phi_{S_1} \cap \Phi_{S_2}$ contains exactly $2^N - 1$ elements, and there exist $u, v \in \mathbb{Z}^N$ such that $\Phi_{S_1} \setminus \Phi_{S_2} = \{[u]\}$, $\Phi_{S_2} \setminus \Phi_{S_1} = \{[v]\}$, and $[\frac{v+u}{2}]$, $[\frac{v-u}{2}]$ are elements of $\Phi_{S_1} \cap \Phi_{S_2}$. $\{\frac{v+u}{2}, \frac{v-u}{2}\}$ is a primitive set of \mathbb{Z}^N .*

1.4 Theorems and algorithm for ternary case

In the sequel, for any fixed type (G, H) , let $L \subset G$ be the translation subgroup of G . $L^* \subset \mathbb{R}^3$ be the reciprocal lattice of L , by seeing L as a lattice in \mathbb{R}^3 . In powder indexing, the type (G, H) is normally unknown, and with regard to every element $q \in \Lambda_{ext}(G, H) := \{|l^*|^2 : 0 \neq l^* \in L^*, l^* \notin \Gamma_{ext}(G, H)\}$ extracted from Θ_P , it is unknown which $l^* \in L^*$ correspond to the q . Owing to this, properties of SA that hold for all the types (G, H) and most of $l^* \in L^*$ are required to establish a mathematical algorithm for powder indexing.

First, the following theorem can be used to obtain candidates for $2D$ sublattices of the true solution L^* .

Theorem 1 (Th. 2, [23]). *Regardless of the type (G, H) of SA , there exist infinitely many primitive sets $\{l_1^*, l_2^*\}$ of L^* such that none of $l_1^*, l_2^*, l_1^* + 2l_2^*, 2l_1^* + l_2^*$ is contained in $\Gamma_{ext}(G, H)$. \square*

Note that the same thing does not hold if $l_1^*, l_2^*, l_1^* + 2l_2^*, 2l_1^* + l_2^*$ in Theorem 1 are replaced by $l_1^*, l_2^*, l_1^* \pm l_2^*$. The 4 lattice vectors in the theorem satisfy the following identity:

$$3|l_1^*|^2 + |l_1^* + 2l_2^*|^2 = 3|l_2^*|^2 + |2l_1^* + l_2^*|^2. \quad (19)$$

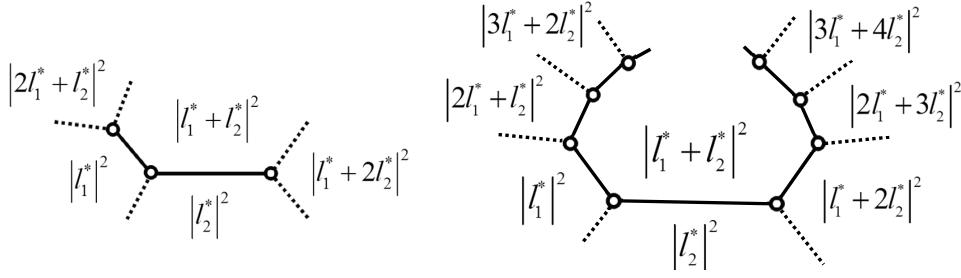


Figure 4: The subgraph of a topograph associated with the identity $3|l_1^*|^2 + |l_1^* + 2l_2^*|^2 = 3|l_2^*|^2 + |2l_1^* + l_2^*|^2$

The identity (19) may be considered to correspond to the left-hand subgraph in Figure 4. Furthermore, we have:

Theorem 2 (Th. 3, [23]). *Regardless of the type (G, H) of SA, there exist infinitely many primitive sets $\{l_1^*, l_2^*\}$ of L^* such that $ml_1^* + (m-1)l_2^* \notin \Gamma_{ext}(G, H)$ holds for any integer m . Furthermore, L^* contains infinitely many 2D sublattices whose bases are such primitive sets. \square*

From the following identity, it is seen that the lattice vectors $ml_1^* + (m-1)l_2^*$ ($m \in \mathbb{Z}$) in Theorem 2 provide four vectors satisfying the identity (19):

$$3|ml_1^* + (m-1)l_2^*|^2 + |(m+2)l_1^* + (m+1)l_2^*|^2 = 3|(m+1)l_1^* + ml_2^*|^2 + |(m-1)l_1^* + (m-2)l_2^*|^2. \quad (20)$$

Therefore, Theorem 2 leads to Theorem 1. By joining the subgraphs corresponding to (19) for each m , the right-hand graph in Figure 4 containing infinitely many edges is formed. In the graph of Figure 4, SA of the type (G, H) holds for none of all the reciprocal lattices, except for $\pm(l_1^* + l_2^*)$ in the centered domain. This indicates that if the identity (20) is used, instead of the parallelogram law, the estimation on the growth of topographs in the latter half of Section 1.3 works. That is, a number of topographs corresponding to 2D sublattices of the true solution L^* will have a number of edges, without being adversely affected by SA. Theorem 2 claims that “infinitely many” of topographs with infinitely many edges are generated, if $\Lambda_{ext}(G, H)$ is used, instead of the finite set Λ^{obs} of observed lengths.

The following theorem describe how to obtain the quadratic form of L^* from the lattice-vector lengths in Λ^{obs} , after well-grown topographs are obtained:

Theorem 3. [Th. 4, [23]] *Regardless of the type (G, H) of SA, L^* has infinitely many basis $\langle l_1^*, l_2^*, l_3^* \rangle$ satisfying the following:*

- (a) $\pm l_1^* + l_2^* + l_3^* \notin \Gamma_{ext}(G, H)$,
- (b) *the following holds for both $i = 2, 3$: $ml_1^* + (m-1)(-l_1^* + l_i^*) \notin \Gamma_{ext}(G, H)$ for any integer m , or $ml_i^* + (m-1)(l_1^* - l_i^*) \notin \Gamma_{ext}(G, H)$ for any integer $m \geq 0$.*

\square

Finally we shall explain the algorithm of *CONOGRAPH*, based on the above theorems. What follows, Λ^{obs} is a finite set, consisting of observed elements of $\Lambda_P \cap [q_{min}, q_{max}]$.

- (1) If $q_1, q_2, q_3, q_4 \in \Lambda^{obs}$ satisfying $2(q_1 + q_2) = q_3 + q_4$ are found, an edge as in Figure 2 is generated, by assuming $q_1 = |l_1|^2$, $q_2 = |l_2|^2$, $q_3 = |l_1 + l_2|^2$, $q_4 = |l_1 - l_2|^2$.

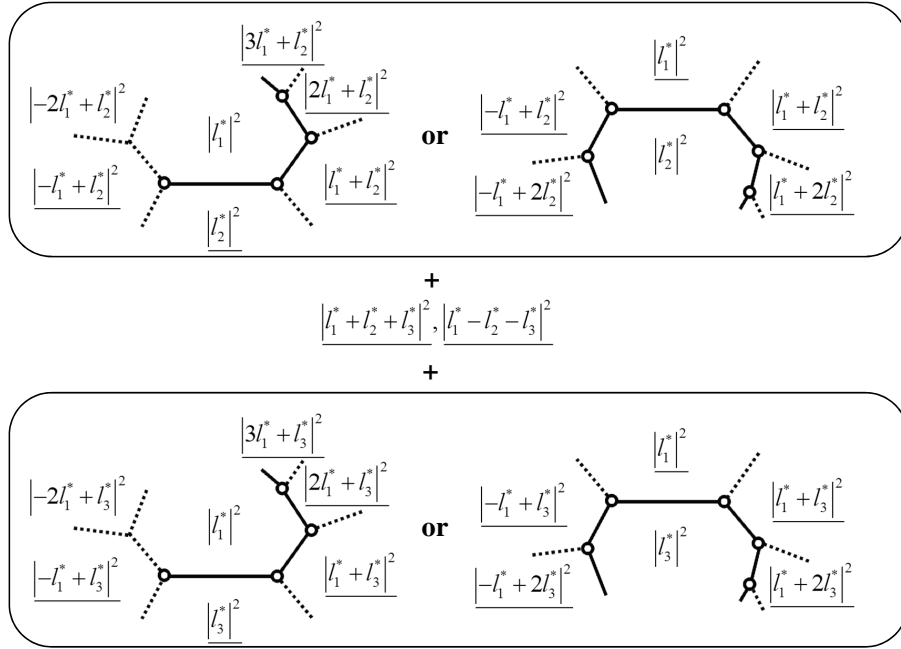


Figure 5: Lattice-vector lengths used for enumeration of 3D lattices (In the process of determining the ternary quadratic form of a lattice, it may be assumed from Theorem 3 that the lengths of all the underlined vectors are included in Λ^{obs} .)

- (2) If $q_1, q_2, q_3, q_4 \in \Lambda^{obs}$ satisfying $3q_1 + q_3 = 3q_2 + q_4$ are found, two edges as in Figure 6 are generated, by splitting the graph in Figure 4, where the value of q_7 is set to $(q_1 + q_3 - 2q_2)/2 = (q_2 + q_4 - 2q_1)/2$ so that they satisfy the parallelogram law. If this q_7 does not equal any of $q_i \in \Lambda^{obs}$, q_7 is supposed to be an element of Λ_L that has not been observed owing to some reason.

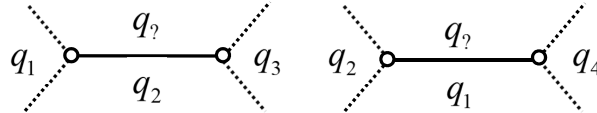


Figure 6: Edges obtained from $q_1, q_2, q_3, q_4 \in \Lambda^{obs}$ satisfying $3q_1 + q_3 = 3q_2 + q_4$ (q_7 may not belong to the set Λ^{obs} of observed lengths)

- (3) If two edges contain the same nodes (two nodes are the same, if the labels of the three domains surrounding the node coincide), the edges are connected as in Figure 3. For each obtained graph T , count the number of elements in Λ^{obs} that appear in T . Sort the subgraphs in descending order of the number. If two subgraphs T_1, T_2 have the same number, the sorting is done according to $T_1 < T_2 \iff \det S(T_1) < \det S(T_2)$, where $S(T) \in \mathcal{S}^2$ is the quadratic form of $2D$ lattices expanded by l_1^*, l_2^* , when T contains an edge as in Figure 2.
- (4) Starting from the subgraphs in higher order, insert all the edges in the subgraph in an array A_2 , until the number of entries of A_2 exceeds M .

- (5) For all the combinations of $q_6 \in \Lambda^{obs}$ and two edges in A_2 that commonly contain $q_1 \in \Lambda^{obs}$, the following is done ; if it is assumed that a basis (l_1^*, l_2^*, l_3^*) of L^* satisfies $|l_i^*|^2 = q_i$ ($1 \leq i \leq 3$) , $|l_1^* + l_2^*|^2 = q_4$, $|l_1^* + l_3^*|^2 = q_5$, $|l_1^* + l_2^* + l_3^*|^2 = q_6$, the quadratic form of L^* is provided by:

$$\begin{pmatrix} q_1 & \frac{q_4 - q_1 - q_2}{2} & \frac{q_5 - q_1 - q_3}{2} \\ \frac{q_4 - q_1 - q_2}{2} & q_2 & \frac{q_6 + q_1 - q_4 - q_5}{2} \\ \frac{q_5 - q_1 - q_3}{2} & \frac{q_6 + q_1 - q_4 - q_5}{2} & q_3 \end{pmatrix}.$$

Insert this quadratic form in an array as a candidate solution.

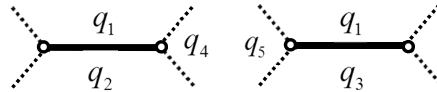


Figure 7: Two edges commonly containing q_1

- (6) The quadratic forms are sorted by the de Wolff figure of merit [8] and output.

The M in (4) is a parameter used to adjust the efficiency and exhaustiveness of the search for L^* in *CONOGRAPH*. Further discussions to rationalize the use of M and to determine whether the algorithm is practical or not are omitted herein, considering the scope of AC proceedings. See the author's cited papers, if necessary.

2 Error-stable Bravais-lattice determination

If the automorphism groups of lattices $L_1, L_2 \subset \mathbb{R}^N$ are conjugate in $GL_3(\mathbb{Z})$, L_1 and L_2 are said to belong to the same *Bravais type*. If the automorphism groups are conjugate in $GL_N(\mathbb{Q})$, L_1 and L_2 belong to the same *lattice system*. Since the study of Bravais [2], it has been well-known that there are 14 Bravais types for 3D lattices. With regard to N -dimensional lattices with $N = 1-6$, it is known that there are 1, 5, 14, 64, 189 and 826 Bravais types [27]. For $N = 3$, there are 7 lattice systems, and each system is divided into distinct Bravais types as in Table 1.

The centering type is another category to classify 3D lattices (Figure 8). Mathematically, the centering types may be considered to describe on the relation between the original lattice L and its sublattice expanded by all the $l \in L$ whose corresponding reflection $x \mapsto x - 2(x \cdot l / l \cdot l)l$ is an automorphism of L .

If triclinic is excluded, monoclinic (P, B), orthorhombic (I, F) and rhombohedral are Bravais types with the automorphism group minimal by inclusive order. If it is possible to determine whether a given 3D lattice has at least either of the above 5 symmetries, the check whether the lattice belongs to a higher-symmetry Bravais type is straightforward and can be conducted in a small number of steps (*cf.* Section 5.3, [22]). Therefore, it may be thought that the most complex part in the Bravais-lattice determination is the stage for centering-type determination. Theorem 4-7 in the following sections, prove the algorithms in Table 2-8 are error-stable. In particular, even if the distribution of the error is unknown, as long as the scale of the error is not extremely large and (A) described above is satisfied, it is possible to prove the algorithms are error-stable.

What follows, we shall briefly introduce the background of this problem in mathematical crystallography; error-stable Bravais-lattice determination algorithms have been discussed mainly for the cases of $N \leq 3$. A method that uses 44 lattice characters (*cf.* 9.2.5, [13]) was proposed for the case of $N = 3$. It was soon noticed that the method does not always work well when the coefficients of quadratic forms are real numbers and

Table 1: Lattice systems and Bravais types for 3D lattices

| Lattice system | Constraints on lattice vectors | Number of Bravais types (centering types ^a) |
|----------------|---|---|
| Triclinic | no conditions | 1 |
| Monoclinic | some $l_1, l_2 \neq 0$ satisfy $l_1 \cdot l_2 = 0$ | 2 (P, B) |
| Orthorhombic | some $l_1, l_2, l_3 \neq 0$ satisfy $l_i \cdot l_j = 0$ | 4 (P, B, I, F) |
| Tetragonal | some $l_1, l_2, l_3 \neq 0$ satisfy $l_i \cdot l_j = 0$, $l_1 \cdot l_1 = l_2 \cdot l_2$ | 2 (P, I) |
| Rhombohedral | some lattice basis $\langle l_1, l_2, l_3 \rangle$ satisfies $l_1 \cdot l_1 = l_2 \cdot l_2 = l_3 \cdot l_3$, $l_1 \cdot l_2 = l_1 \cdot l_3 = l_2 \cdot l_3$ | 1 |
| Hexagonal | some lattice basis $\langle l_1, l_2, l_3 \rangle$ satisfies $l_1 \cdot l_1 = l_2 \cdot l_2 = -2l_1 \cdot l_2$, $l_1 \cdot l_3 = l_2 \cdot l_3 = 0$ | 1 |
| Cubic | some $l_1, l_2, l_3 \neq 0$ satisfy $l_i \cdot l_j = 0$, $l_1 \cdot l_1 = l_2 \cdot l_2 = l_3 \cdot l_3$ | 3 (P, I, F) |

^a P : primitive centering, B : base-centered (also notated as A, C), I : body-centered, F : face-centered.

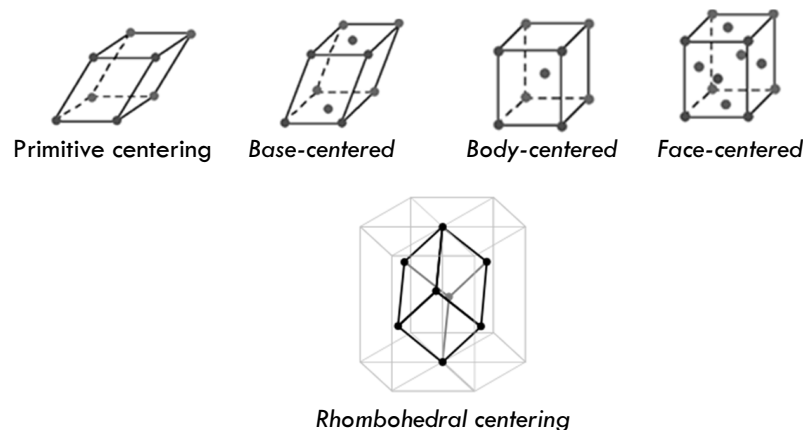


Figure 8: Centering types for 3D lattices; it is easily seen that all the rhombohedral lattices contains a hexagonal lattice as a sublattice. Similarly to the other centering types, rhombohedral centering (abbreviated by R) can be seen as a subcategory of the rhombohedral lattice system.

include small errors. In [3], [12], [15], [35] and [11], some improvements was proposed in order to handle the cases in which round-off errors are contained in the coefficients. Studies on Bravais lattice determination under experimental errors have been conducted by Clegg (1981), [17], [34], and [1]. Most of them use the Niggli reduction and the Buerger reduction, because they are standard in crystallography. In the method of [34], the Selling reduction (also called the Delaunay reduction [9]) is adopted. In [1], it is proposed to apply the above 44 lattice characters to all the nearly reduced lattices.

One of the problem of the existing methods is that they are not well-grounded by mathematical discussion. As a result, under large errors, they fail to obtain the correct solution in some cases, or need a number of iterations for computation. Another problem is that the Niggli and Buerger reductions clearly do not suit for efficient error-stable algorithms, because their fundamental domain is not connected, and many forms with high symmetry exist in the boundaries of their fundamental domain (also called reduced domain). For example, if the reduced domain of the Buerger reduction defined in (23) is denoted by $D_{Buerger}$, the following quadratic form of a cubic (F) lattice is in the intersection of 168 distinct $D_{Buerger}[g]$ ($g \in GL_3(\mathbb{Z})$).

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} \quad (21)$$

This indicates that if Buerger reduction used for the cubic (F) determination, the necessary time is almost proportional to the number 168. By a similar reason, if the Selling reduction is used, the time is proportional to 3 (the size of C_F in Table 3). The optimal reduction varies, depending on the considered Bravais types. Owing to this, our algorithm applies the Minkowski reduction to lattices with primitive centering, and the Selling-reduction to face-centered, body-centered, rhombohedral and base-centered lattices. In [21], it is explained by comparing the number of matrices required for the determination that our method is (in the best case, about 120 times) faster than the method of [1]. Our algorithm is optimal, in the sense that the number of matrices cannot be reduced, as long as the Minkowski, Selling, Niggli and Buerger reductions are utilized.

2.1 Definition of several kinds of reduced forms

The Niggli and Buerger reductions for ternary quadratic forms, which are standard in crystallography, were originated from the paper by Eisenstein [10]. Later Minkowski established reduction theory for lattices of general rank [18]. As seen in the following, the definitions of these three reductions are basically same if the boundary conditions are ignored.

Recall that $(s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3$ is *Minkowski-reduced* if and only if it belongs to the following D_{min} :

$$D_{min} := \left\{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : \begin{array}{l} 0 < s_{11} \leq s_{22} \leq s_{33}, \quad 2|s_{12}|, 2|s_{13}| \leq s_{11}, \quad 2|s_{23}| \leq s_{22}, \\ 2|s_{13} + s_{23}| \leq s_{11} + s_{22} + 2s_{12}, \\ 2|s_{13} - s_{23}| \leq s_{11} + s_{22} - 2s_{12} \end{array} \right\} \quad (22)$$

A quadratic form is *Buerger-reduced* if and only if it belongs to the following $D_{Buerger}$:

(Buerger-reduced domain)

$$D_{Buerger} := D_B^+ \cup D_B^-, \quad (23)$$

$$D_B^+ := \left\{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : 0 < s_{11} \leq s_{22} \leq s_{33}, \quad 0 \leq 2s_{12}, 2s_{13} \leq s_{11}, \quad 0 \leq 2s_{23} \leq s_{22} \right\}, \quad (24)$$

$$D_B^- := \left\{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : 0 < s_{11} \leq s_{22} \leq s_{33}, \quad 0 \leq -2s_{12}, -2s_{13} \leq s_{11}, \quad 0 \leq -2s_{23} \leq s_{22}, \right. \\ \left. -2(s_{12} + s_{13} + s_{23}) \leq s_{11} + s_{22} \right\} \quad (25)$$

The following boundary conditions are added in the definition of the Niggli-reduced cell (Niggli(1928), Hahn (1983)).

1. (Normalization)

$$(s_{ij}) \in D_B^+ \implies s_{12} > 0, s_{13} > 0, s_{23} > 0, \quad (26)$$

$$s_{11} = s_{22} \implies |s_{23}| \leq |s_{13}|, \quad (27)$$

$$s_{22} = s_{33} \implies |s_{13}| \leq |s_{12}|. \quad (28)$$

2. When $s_{12} > 0, s_{13} > 0, s_{23} > 0,$

$$s_{23} = \frac{s_{22}}{2} \implies s_{12} \leq 2s_{13}, \quad (29)$$

$$s_{13} = \frac{s_{11}}{2} \implies s_{12} \leq 2s_{23}, \quad (30)$$

$$s_{12} = \frac{s_{11}}{2} \implies s_{13} \leq 2s_{23}. \quad (31)$$

3. When $s_{12} \leq 0, s_{13} \leq 0, s_{23} \leq 0,$

$$|s_{23}| = \frac{s_{22}}{2} \implies s_{12} = 0, \quad (32)$$

$$|s_{13}| = \frac{s_{11}}{2} \implies s_{12} = 0, \quad (33)$$

$$|s_{12}| = \frac{s_{11}}{2} \implies s_{13} = 0, \quad (34)$$

$$|s_{12} + s_{13} + s_{23}| = \frac{s_{11} + s_{22}}{2} \implies s_{11} \leq |s_{12} + 2s_{13}|. \quad (35)$$

The Niggli reduction is defined so that the reduced form is uniquely determined for any $(s_{ij}) \in \mathcal{S}_{>0}^3$. Frequently, $s_{12} \leq 0, s_{23} \leq 0$ are added to the definition of the Minkowski-reduced form. Whichever definitions are used, the Minkowski-reduced domain D_{min} is connect, while neither of the Niggli and the Buerger-reduced domains has this property. As seen in the following sections, the efficiency of a given error-stable algorithm is almost determined by how far quadratic forms with the considered symmetry exist from the boundaries of the reduced domain. It is not to difficult to see that whichever Bravais types are chosen, the Niggli or the Buerger-reduced reductions have properties opposite to this.

In order to discuss the error-stableness of a given algorithm, it is convenient if the method of the Venkov reduction is adopted to define the Minkowski and Selling reductions (in a broad sense). Note that the following reduced domains are invariant by permutation matrices.

(Minkowski-reduced domain in a broad sense) Any $S \in \mathcal{S}_{>0}^3$ is *Minkowski-reduced in a broad sense* if and only if it is an element of the following set:

$$\begin{aligned} \tilde{D}_{min} &:= \left\{ S \in \mathcal{S}_{>0}^3 : \langle S, I_3 \rangle = \min_{g \in GL(3, \mathbb{Z})} \langle S[g], I_3 \rangle \right\} \\ &= \left\{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}_{>0}^3 : \begin{array}{l} 2|s_{ij}| \leq \min\{s_{ii}, s_{jj}\}, \\ 2|s_{ik} \pm s_{jk}| \leq s_{ii} + s_{jj} \pm 2s_{ij} \\ \text{for any distinct } 1 \leq i, j, k \leq 3 \end{array} \right\}. \end{aligned} \quad (36)$$

It is easily seen that \tilde{D}_{min} contains D_{min} in (22), and any $S \in \tilde{D}_{min}$ is transformed into an element of D_{min} by simply sorting its diagonal entries in ascending order.

(Selling-reduced domain in a broad sense) Any $S \in \mathcal{S}_{>0}^3$ is *Selling-reduced* (or *Delaunay-reduced*) in a broad sense if and only if it is in the following set:

$$\tilde{D}_{del} = \left\{ S \in \mathcal{S}_{>0}^3 : \langle S, A_3 \rangle = \min_{g \in GL(3, \mathbb{Z})} \langle S[g], A_3 \rangle \right\}, \quad (37)$$

$$A_3 := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}. \quad (38)$$

For reference, we shall also define the Selling-reduced (or Delaunay-reduced) domain in a narrow sense that is also used in [34]:

$$D_{del} = \left\{ (s_{ij} \in \tilde{D}_{del} : 1 \leq s_{11} \leq s_{22} \leq s_{33} \leq \sum_{1 \leq i, j \leq 3} s_{ij}) \right\}. \quad (39)$$

A Selling-reduced $S \in \mathcal{S}_{>0}^3$ is frequently represented as an element of $\mathcal{S}_{\geq 0}^4$; for any $(s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}_{>0}^3$, let $\tilde{S} \in \mathcal{S}_{\geq 0}^4$ be the quartic quadratic form given by:

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} & -\sum_{j=1}^3 s_{1j} \\ s_{21} & s_{22} & s_{23} & -\sum_{j=1}^3 s_{2j} \\ s_{31} & s_{32} & s_{33} & -\sum_{j=1}^3 s_{3j} \\ -\sum_{i=1}^3 s_{i1} & -\sum_{i=1}^3 s_{i2} & -\sum_{i=1}^3 s_{i3} & \sum_{i=1}^3 \sum_{j=1}^3 s_{ij} \end{pmatrix}. \quad (40)$$

For any $\tilde{S} \in \mathcal{S}_{\geq 0}^4$, there is some $S \in \mathcal{S}_{>0}^3$ corresponding to \tilde{S} as in (40) if and only if \tilde{S} belongs to the following set:

$$V_{del} := \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in \mathcal{S}^4 : \begin{array}{l} \sum_{i=1}^4 \sum_{j=1}^4 \tilde{s}_{ij} = 0, \\ (s_{k_i k_j})_{1 \leq i, j \leq 3} \succ 0 \text{ for any distinct } 1 \leq k_1, k_2, k_3 \leq 4 \end{array} \right\} \quad (41)$$

We shall also say $\tilde{S} \in V_{del}$ is *Selling-reduced in a broad sense*, if \tilde{S} belongs to the following set:

$$\begin{aligned} & \left\{ \tilde{S} \in V_{del} : \tilde{S} \succeq 0, \langle \tilde{S}, I_4 \rangle = \min_{g \in GL(3, \mathbb{Z})} \langle \tilde{S}[g], I_4 \rangle \right\} \\ & = \{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \tilde{s}_{ij} \leq 0 \ (1 \leq i < j \leq 4) \}. \end{aligned} \quad (42)$$

From the definition, the stabilizer subgroups of \tilde{D}_{min} , \tilde{D}_{del} of $GL(3, \mathbb{Z})$ are defined by:

$$St(I_3) := \{ g \in GL(3, \mathbb{Z}) : {}^t g I_3 g = I_3 \}, \quad (43)$$

$$St(A_3) := \{ g \in GL(3, \mathbb{Z}) : {}^t g A_3 g = A_3 \}. \quad (44)$$

2.2 Minkowski reduction for determination of monoclinic (P) cases

The error-stable determination of monoclinic (P) lattices might be the most straightforward case among all the centering types, although the discussions applied to the other centering-types are not much different from the following.

Any Minkowski-reduced $S \in \mathcal{S}_{>0}^3$ belongs to $V_{mono, p}$, if it precisely has monoclinic (P) symmetry.

$$V_{mono, p} := V_{mono, p, a} \cup V_{mono, p, b} \cup V_{mono, p, c}, \quad (45)$$

$$V_{mono, p, a} := \{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : s_{12} = s_{13} = 0 \}, \quad (46)$$

$$V_{mono, p, b} := \{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : s_{12} = s_{23} = 0 \}, \quad (47)$$

$$V_{mono, p, c} := \{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : s_{13} = s_{23} = 0 \}. \quad (48)$$

When the above union of linear space is for the determination, it is necessary to check if the observed quadratic form S^{obs} and the true quadratic form S become Minkowski-reduced with regard to the same basis. Fortunately, the following theorem holds (although it seems almost clear in this case). As a result, the algorithm in Table 2 is error-stable, as long as (A) is satisfied. Note that it is impossible to reduce the size of C_P used in Table 2, even if the input S^{obs} has precise coefficients (i.e., $\epsilon = 0$).

Theorem 4 (Th.1, [22]). *Let $S \in \mathcal{S}_{>0}^3$ be the true quadratic form of a lattice with monoclinic (P) symmetry, and let S^{obs} be an observed S corresponding to the same basis of \mathbb{Z}^3 . Under the assumption (A), if S^{obs} is Minkowski-reduced in a broad sense, S belongs to $V_{mono,p}$.*

From Theorem 4, it is concluded that the algorithm in Table 2 is error-stable. On output, S^{obs} is projected on each subspace, $V_{mono,p,a}$, $V_{mono,p,b}$ and $V_{mono,p,c}$ respectively, according to which of the three matrices in Table 2. The coefficients of S^{obs} containing errors, are modified by projecting S^{obs} onto the subspaces.

| Table 2: Algorithm for nearly monoclinic (P) lattices | |
|---|--|
| (Input) | $S^{obs} \in \mathcal{S}_{>0}^3$: Minkowski-reduced in a broad sense, $\epsilon > 0$: threshold, $\text{dist}(S, T)$: arbitrary distance function with arguments $S, T \in \mathcal{S}^3$. |
| (Output) | A : array of pairs of $g \in GL_3(\mathbb{Z})$ and $S \in V_{mono,p,b}$ with $\text{dist}(S, S^{obs}[g]) \leq \epsilon$. |
| 1: | Prepare the array C_P of size $I_{max} := 3$: $C_P := \left\{ I_3, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$ |
| 2: | for $i = 1$ to $I_{max} := 3$ do |
| 3: | Compute $S_{new} := C_P[i]S^{obs} {}^t C_P[i]$ and |
| 4: | $S := \begin{pmatrix} s_{11} & 0 & s_{13} \\ 0 & s_{22} & 0 \\ s_{13} & 0 & s_{33} \end{pmatrix}$, where s_{ij} is the (i, j) -entry of S_{new} . |
| 5: | If $\text{dist}(S_{new}, S) \leq \epsilon$, insert $(C_P[i], S)$ in A . |
| 6: | end for |

Proof of Theorem 4. Let g be an element of $GL_3(\mathbb{Z})$ such that $S \in \tilde{D}_{min}[g]$. Then, $S[g^{-1}]$ belongs to $V_{mono,p} \cap \tilde{D}_{min}$. By replacing g with gg_0 for some $g_0 \in St(I_3)$, it may be supposed that $S[g^{-1}]$ is also contained in the following subset of $V_{mono,p,b}$.

$$U_{mono,p,b} := \{(s_{ij})_{1 \leq i, j \leq 3} \in V_{mono,p,b} : s_{11} \leq s_{33}, -s_{11} \leq 2s_{13} \leq 0\}. \quad (49)$$

The (i, j) -entries of S and ${}^t g g$ are denoted by s_{ij} and a_{ij} , respectively. The following inequality is obtained from $S[g^{-1}] \in U_{mono,p,b}$:

$$\begin{aligned} \langle S, I_3 \rangle - \langle S[g^{-1}], I_3 \rangle &= \left\langle \begin{pmatrix} s_{11} & 0 & s_{13} \\ 0 & s_{22} & 0 \\ s_{13} & 0 & s_{33} \end{pmatrix}, g^T g - I_3 \right\rangle \\ &= (a_{11} - 1)s_{11} + 2a_{13}s_{13} + (a_{22} - 1)s_{22} + (a_{33} - 1)s_{33} \\ &\geq (a_{11} + a_{33} - 2 - |a_{13}|)s_{11} + (a_{22} - 1)s_{22} \\ &\geq \frac{1}{2}(a_{11} + a_{33} - 2)s_{11} + (a_{22} - 1)s_{22}. \end{aligned} \quad (50)$$

For the last inequality, $a_{11} + a_{33} \geq 2|a_{13}| + 1$ is used. Since tgg is an integer-valued positive definite symmetric matrix, a_{11} , a_{22} , and a_{33} are positive integers. Hence, the coefficients of s_{11} and s_{22} are not negative in the last line of (50).

On the other hand, $\langle S^{obs}, I_3 \rangle - \langle S^{obs}[g^{-1}], I_3 \rangle \leq 0$ also holds because $S^{obs} \in \tilde{D}_{min}$. Therefore, the coefficients of s_{11} and s_{22} must be less than $\frac{1}{2}$ from the assumption (A). Hence, we have

$$a_{11} = a_{22} = a_{33} = 1. \quad (51)$$

Thus, it is proved that g belongs to $U_{mono,p,b}$. From the assumption, $S[g^{-1}] \in U_{mono,p,b}$, therefore S is an element of $V_{mono,p}$. \square

2.3 Selling reduction for determination of face and body-centered cases

While the Minkowski reduction is suitable for lattices with monoclinic (P) symmetry, the Selling reduction is more suitable than the Minkowski and Buerger reductions to deal with the other centering types, *i.e.*, face-centered, body-centered, rhombohedral and base-centered. The distance defined on the linear space \mathcal{S}^3 was used in the proof of Theorem 4. All the following theorems are similarly proved.

In this case, the face-centered case seems to be the most straightforward. Any $\tilde{S} \in V_{del}$ Selling-reduced in a broad sense has face-centered symmetry if and only if it is an element of the following:

$$\begin{aligned} \tilde{V}_F &:= \bigcup_{1 \leq k_1 < k_2 \leq 3} \tilde{V}_{F,k_1,k_2}, \quad (52) \\ \tilde{V}_{F,k_1,k_2} &:= \left\{ (\tilde{s}_{ij})_{1 \leq i < j \leq 4} \in V_{del} : \begin{array}{l} \tilde{s}_{k_1 l_1} = \tilde{s}_{k_1 l_2} = \tilde{s}_{k_2 l_1} = \tilde{s}_{k_2 l_2} \\ \text{for } 1 \leq l_1 < l_2 \leq 4 \text{ distinct from } k_1, k_2 \end{array} \right\}. \quad (53) \end{aligned}$$

For example, as seen from the following, any elements of $\tilde{V}_{F,1,2}$ has a sublattice represented by a diagonal form.

$$h_F \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} {}^t h_F, h_F := \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \\ -1 & 0 & -1 \end{pmatrix}. \quad (54)$$

What follows, $v_1, v_2, v_3, v_4 \in \mathbb{Z}^3$ with $\sum_{i=1}^4 v_i = 0$ is called a *superbasis*, if they expand \mathbb{Z}^3 over \mathbb{Z} . The following theorem is proved similarly to Theorem 4.

Theorem 5 (Th.2, [22]). *Let $\tilde{S} \in V_{del}$ be the true quadratic form of a lattice with face-centered symmetry, and let $\tilde{S}^{obs} \in V_{del}$ be an observed \tilde{S} with regard to the same superbasis. Under the assumption (A), if \tilde{S}^{obs} is Selling-reduced in a broad sense, \tilde{S} belongs to \tilde{V}_F .*

As a result, the algorithm in Table 3 for face-centered lattices is proved to be error-stable. If $S \in \mathcal{S}_{>0}^3$ has orthorhombic (F) symmetry, S^{-1} has orthorhombic (I) symmetry. Hence, the algorithm for body-centered cases, is provided by Table 4.

2.4 Theorems and algorithms for rhombohedral and base-centered cases

If a lattice has rhombohedral symmetry, its quadratic form S is an element of V_R defined by

$$V_R := \left\{ (s_{ij})_{1 \leq i, j \leq 3} \in \mathcal{S}^3 : s_{11} = s_{22} = s_{33}, s_{12} = s_{13} = s_{23} \right\}. \quad (55)$$

Table 3: Algorithm for nearly orthorhombic (F) lattices

| | |
|----------|---|
| (Input) | $S^{obs} \in \mathcal{S}_{>0}^3$: Selling-reduced in a broad sense, $\epsilon > 0$, $\text{dist}(S, T)$: same as in Table 2, |
| (Output) | A : array of pairs of an integer matrix g with $h_F g \in GL(3, \mathbb{Z})$ and a diagonal matrix S with $\text{dist}(S, S^{obs}[g]) \leq \epsilon$. |
| 1: | Set the inverse of the following matrix h_F : $h_F := \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{pmatrix}, h_F^{-1} := \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 1 & 1 & 2 \end{pmatrix},$ |
| 2: | Set the array C_F of size $I_{max} := 3$: $C_F := \left\{ h_F^{-1}, h_F^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, h_F^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}.$ |
| 3: | for $i = 1$ to I_{max} do |
| 4: | Compute $S_{new} := C_F[i] S^{obs} {}^t C_F[i]$ and $S := \begin{pmatrix} s_{11} & 0 & 0 \\ 0 & s_{22} & 0 \\ 0 & 0 & s_{33} \end{pmatrix}$, |
| | where s_{ii} is the (i, i) -entry of S_{new} . |
| 5: | If $\text{dist}(S_{new}, S) \leq \epsilon$, insert $(C_F[i], S)$ in A . |
| 6: | end for |

^aThis algorithm outputs the diagonal S , because in crystallography, this S is conventionally used to parametrize face-centered lattice.

Table 4: Algorithm for nearly orthorhombic (I) lattices

| | |
|----------|---|
| (Input) | $S^{obs} \in \mathcal{S}_{>0}^3$: $(S^{obs})^{-1}$ is Selling-reduced in a broad sense, $\epsilon > 0$, $\text{dist}(S, T)$: same as in Table 2, |
| (Output) | A : array of pairs of an integer matrix g with $h_I g \in GL(3, \mathbb{Z})$ and a diagonal matrix S with $\text{dist}(S, S^{obs}[g]) \leq \epsilon$. |
| 1: | Set the inverse of the following matrix h_I : $h_I := \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 2 \end{pmatrix}, h_I^{-1} := \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$ |
| 2: | Set the array C_I of size $I_{max} := 3$: $C_I := \left\{ h_I^{-1}, h_I^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, h_I^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}.$ |
| 3: | for $i = 1$ to I_{max} do |
| 4: | Compute $S_{new} := C_I[i] S^{obs} {}^t C_I[i]$ and $S := \begin{pmatrix} s_{11} & 0 & 0 \\ 0 & s_{22} & 0 \\ 0 & 0 & s_{33} \end{pmatrix}$, |
| | where s_{ii} is the (i, i) -entry of S_{new} . |
| 5: | If $\text{dist}(S_{new}, S) \leq \epsilon$, insert $(C_I[i], S)$ in A . |
| 6: | end for |

When $-\frac{1}{2}s_{11} < s_{12} < -\frac{1}{3}s_{11}$ or $\frac{1}{2}s_{11} < s_{12} < s_{11}$, the elements of V_R are positive-definite but not Minkowski-reduced. However, the following linear space \tilde{V}_R contains all the Selling-reduced forms of rhombohedral lattices.

$$\begin{aligned} \tilde{V}_R &:= \bigcup_{\substack{1 \leq k_1 < k_2 \leq 4 \\ 1 \leq l_1 \leq 4, l_1 \neq k_1, k_2}} \tilde{V}_{R, k_1, k_2, l_1}^+ \cup \bigcup_{1 \leq l_1 < l_2 < l_3 \leq 4} \tilde{V}_{R, l_1, l_2, l_3}^-, \quad (56) \\ \tilde{V}_{R, k_1, k_2, l_1}^+ &:= \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \begin{array}{l} \tilde{s}_{k_1 l_2} = \tilde{s}_{k_2 l_1} = 0, \tilde{s}_{k_1 k_2} = \tilde{s}_{k_1 l_1} = \tilde{s}_{k_2 l_2} \\ \text{for } 1 \leq l_2 \leq 4 \text{ distinct from } k_1, k_2, l_1 \end{array} \right\}, \\ \tilde{V}_{R, l_1, l_2, l_3}^- &:= \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \tilde{s}_{l_1 l_1} = \tilde{s}_{l_2 l_2} = \tilde{s}_{l_3 l_3}, \tilde{s}_{l_1 l_2} = \tilde{s}_{l_1 l_3} = \tilde{s}_{l_2 l_3} \right\}. \end{aligned}$$

With regard to base-centered lattices, the following linear space \tilde{V}_B contains all the Selling-reduced quadratic forms:

$$\tilde{V}_B := \bigcup_{1 \leq k_1 < k_2 \leq 4} \tilde{V}_{B, k_1, k_2}^{(1)} \cup \bigcup_{1 \leq k_1 < k_2 \leq 3} \tilde{V}_{B, k_1, k_2}^{(2)} \cup \bigcup_{1 \leq k_1, k_2 \leq 4} \tilde{V}_{B, k_1, k_2}^{(3)}, \quad (57)$$

$$\tilde{V}_{B, k_1, k_2}^{(1)} := \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \tilde{s}_{k_1 l} = \tilde{s}_{k_2 l} \text{ for any } 1 \leq l \leq 4, l \neq k_1, k_2 \right\}, \quad (58)$$

$$\tilde{V}_{B, k_1, k_2}^{(2)} := \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \begin{array}{l} \tilde{s}_{k_1 l} = \tilde{s}_{k_2 4}, \tilde{s}_{k_1 4} = \tilde{s}_{k_2 l} \\ \text{for any } 1 \leq l \leq 3 \text{ distinct from } k_1, k_2 \end{array} \right\}, \quad (59)$$

$$\tilde{V}_{B, k_1, k_2}^{(3)} := \left\{ (\tilde{s}_{ij})_{1 \leq i, j \leq 4} \in V_{del} : \begin{array}{l} \tilde{s}_{k_1 k_2} = 0, \tilde{s}_{k_1 l_1} = \tilde{s}_{k_1 l_2} \\ \text{for any } 1 \leq l_1 < l_2 \leq 4 \text{ distinct from } k_1, k_2 \end{array} \right\}. \quad (60)$$

The above is seen from the following equality between $S \in S_{>0}^3$ and $\tilde{S} \in V_{del}$.

$$h_{del} T_R^+ \begin{pmatrix} a & d & d \\ d & a & d \\ d & d & a \end{pmatrix} {}^t(h_{del} T_R^+) = \begin{pmatrix} a & -d & -a+d & 0 \\ -d & a & 0 & -a+d \\ -a+d & 0 & 2(a-d) & -a+d \\ 0 & -a+d & -a+d & 2(a-d) \end{pmatrix}, \quad (61)$$

$$h_{del} h_B \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ d & 0 & c \end{pmatrix} {}^t(h_{del} h_B) = \begin{pmatrix} \frac{a+b}{4} & \frac{a-b}{4} & \frac{d}{2} & -\frac{a+d}{2} \\ \frac{a-b}{4} & \frac{a+b}{4} & \frac{d}{2} & -\frac{a+d}{2} \\ \frac{d}{2} & \frac{d}{2} & c & -c-d \\ -\frac{a+d}{2} & -\frac{a+d}{2} & -c-d & a+c+2d \end{pmatrix}, \quad (62)$$

$$h_{del} T_B^{(2)} h_B \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ d & 0 & c \end{pmatrix} {}^t(h_{del} T_B^{(2)} h_B) = \begin{pmatrix} \frac{a+b}{4} & \frac{-a+b}{4} & \frac{-a+b+2d}{4} & \frac{a-b+2d}{4} \\ \frac{-a+b}{4} & \frac{a+b}{4} & \frac{a-b+2d}{4} & \frac{-a+b+2d}{4} \\ \frac{-a+b+2d}{4} & \frac{a-b+2d}{4} & \frac{a+b}{4} + c + d & \frac{-a+b}{4} - c - d \\ \frac{a-b+2d}{4} & \frac{-a+b+2d}{4} & \frac{-a+b}{4} - c - d & \frac{a+b}{4} + c + d \end{pmatrix}, \quad (63)$$

$$h_{del} T_B^{(3)} h_B \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ d & 0 & c \end{pmatrix} {}^t(h_{del} T_B^{(3)} h_B) = \begin{pmatrix} \frac{a+b}{4} & \frac{d}{2} & -\frac{b}{2} & \frac{-a+b-2d}{4} \\ \frac{d}{2} & c & 0 & -c - \frac{d}{2} \\ -\frac{b}{2} & 0 & b & -\frac{b}{2} \\ \frac{-a+b-2d}{4} & -c - \frac{d}{2} & -\frac{b}{2} & \frac{a+b}{4} + c + d \end{pmatrix}, \quad (64)$$

where

$$h_{del} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}, \quad (65)$$

$$T_R^+ := \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}, \quad (66)$$

$$h_B := \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (67)$$

$$T_B^{(2)} := \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad (68)$$

$$T_B^{(3)} := \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}. \quad (69)$$

What follows, let $g \in GL_3(\mathbb{Z})$ also act on $\tilde{S} \in V_{del}$, $\tilde{D} \subset V_{del}$ by:

$$S[g] := \tilde{g} S^t \tilde{g}, \quad \tilde{g} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix} g \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (70)$$

$$D[g] := \{S[g] : S \in D\}. \quad (71)$$

For rhombohedral and base-centered forms, the following theorems are obtained:

Theorem 6 (Th.3, [22]). *Let $\tilde{S} \in V_{del}$ be the true quadratic form of a lattice with rhombohedral symmetry, and let $\tilde{S}^{obs} \in V_{del}$ be an observed \tilde{S} with regard to the same superbasis. Under the assumption (A), if \tilde{S}^{obs} is Selling-reduced in a broad sense, \tilde{S} belongs to the following subset of V_{del} :*

$$\tilde{V}_R \cup \bigcup_{g_0 \in St(A_3)} \tilde{V}_{R,1,2,3}^- [g_0 t_{001}] \cup \bigcup_{\substack{g_0 \in St(A_3), \\ h = t_{010}, t_{001}}} \tilde{V}_{R,1,2,3}^- [g_0 T_R^+ h], \quad (72)$$

where T_R^+ is the matrix defined by (66), and t_{001} , t_{010} are the following elements of $GL_3(\mathbb{Z})$:

$$t_{i_1 i_2 i_3} := \begin{pmatrix} (-1)^{i_1} & 0 & 0 \\ 0 & (-1)^{i_2} & 0 \\ 0 & 0 & (-1)^{i_3} \end{pmatrix}. \quad (73)$$

Theorem 7 (Th.4, [22]). *Let \tilde{S} be the true quadratic form of a lattice with base-centered symmetry, and \tilde{S}^{obs} be an observed \tilde{S} with regard to the same superbasis. Under the assumption (A), if \tilde{S}^{obs} is Delaunay-reduced in a broad sense, \tilde{S} belongs to the following union of linear subspaces of V_{del} :*

$$\tilde{V}_B \cup \bigcup_{g_0 \in St(A_3)} \tilde{V}_{B,1,2}^{(1)} [g_0 t_{010}] \cup \bigcup_{\substack{g_0 \in St(A_3), \\ i=2,3}} \tilde{V}_{B,1,2}^{(i)} [g_0 T_B^{(i)} \sigma_{23}], \quad (74)$$

where $T_B^{(2)}, T_B^{(3)}$ are the matrices defined by (68), (69) respectively and

$$\sigma_{23} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \quad (75)$$

The domains (72), (74) are decomposed into $\bigcup_{g \in C_R} \tilde{V}_{R,1,2,3}^-[g^{-1}]$, $\bigcup_{g \in C_B} \tilde{V}_{B,1,2}^{(1)}[g^{-1}]$, where C_R (resp. C_B) constitute the matrices in Table 5 (resp. Table 6).

Table 5: Matrices to search for nearly rhombohedral lattices; the matrices are chosen so that $\tilde{V}_{R,1,2,3}^-[g_1^{-1}] \neq \tilde{V}_{R,1,2,3}^-[g_2^{-1}]$ holds for any $g_1 \neq g_2$.

| | | | | | |
|--|--|--|--|--|--|
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^*$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & -1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}^*$ |
| $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}^*$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}^*$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$ |
| $\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 0 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix}$ |

*Matrices contained in C'_R .

However, it may be too prudent to use all the matrices for the determination, because Propositions 2.1, 2.2 hold.

By using the inner product $\text{Trace}(S, T)$, define the distance on \mathcal{S}^3 by:

$$\text{dist}(S, T) := \sqrt{\text{Trace}((S - T)^2)}. \quad (76)$$

More generally, the propositions hold, if the distance on \mathcal{S}^3 is represented as follows for some $r > 0$:

$$\text{dist}((s_{ij})_{1 \leq i, j \leq 3}, (t_{ij})_{1 \leq i, j \leq 3}) := \left(\sum_{i=1}^3 (s_{ii} - t_{ii})^2 + r \sum_{1 \leq i < j \leq 3} (s_{ij} - t_{ij})^2 \right)^{1/2}. \quad (77)$$

Proposition 2.1 (Prop.3, [22]). *By using the following projection map $P_R : \mathcal{S}^3 \rightarrow V_R$, $\delta_R(S) := \text{dist}(S, P_R(S))^2$ is defined as a measure of the displacement caused by the*

projection:

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} \\ s_{12} & s_{22} & s_{23} \\ s_{13} & s_{23} & s_{33} \end{pmatrix} \mapsto \frac{1}{3} \begin{pmatrix} a & d & d \\ d & a & d \\ d & d & a \end{pmatrix}, \quad a := \frac{s_{11} + s_{22} + s_{33}}{3}, \quad d := \frac{s_{12} + s_{13} + s_{23}}{3}.$$

This $\delta_R(S)$ satisfies the following inequalities for any $g \in St(A_3)$ and Selling-reduced $S^{obs} \in \mathcal{S}_{>0}^3$ in a broad sense:

$$\delta_R(S^{obs}[g^{-1}]) \leq \delta_R(S^{obs}[(gt_{001})^{-1}]), \quad (78)$$

$$\delta_R(S^{obs}[(gT_R^+)^{-1}]) \leq \delta_R(S^{obs}[(gT_R^+t_{001})^{-1}]) \leq \delta_R(S^{obs}[(gT_R^+t_{010})^{-1}]). \quad (79)$$

Proposition 2.2. By using the following projection map $P_B : \mathcal{S}^3 \rightarrow \tilde{V}_{B,1,2}^{(1)}$, $\delta_B(S) := \text{dist}(S, P_B(S))$ is defined:

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} \\ s_{12} & s_{22} & s_{23} \\ s_{13} & s_{23} & s_{33} \end{pmatrix} \mapsto \begin{pmatrix} a & s_{12} & d \\ s_{12} & a & d \\ d & d & s_{33} \end{pmatrix}, \quad a := \frac{s_{11} + s_{22}}{2}, \quad d := \frac{s_{13} + s_{23}}{2}.$$

The following inequalities hold for any $g \in St(A_3)$ and Selling-reduced $S^{obs} \in \mathcal{S}_{>0}^3$ in a broad sense:

$$\delta_B(S^{obs}[g^{-1}]) \leq \delta_B(S^{obs}[(gt_{010})^{-1}]), \quad (80)$$

$$\delta_B(S^{obs}[(gT_B^{(2)})^{-1}]) \leq \delta_B(S^{obs}[(gT_B^{(3)}\sigma_{23})^{-1}]), \quad (81)$$

$$\delta_B(S^{obs}[(gT_B^{(3)})^{-1}]) \leq \delta_B(S^{obs}[(gT_B^{(2)}\sigma_{23})^{-1}]). \quad (82)$$

From Proposition 2.1, $P_R(S^{obs}[g^{-1}])$ and $P_R(S^{obs}[(gT_R^+)^{-1}])$ are prioritized over $P_R(S^{obs}[(gt_{001})^{-1}])$, $P_R(S^{obs}[(gT_R^+t_{010})^{-1}])$ and $P_R(S^{obs}[(gT_R^+t_{001})^{-1}])$, if the most feasible candidate for the Bravais type is determined by the distance between the observed quadratic form and its projection on V_R . Therefore, the algorithm in Table 7 uses only the matrices belonging to the right cosets $St(A_3)$ and $St(A_3)T_R^+$ (the first 16 matrices in Table 5). From (66), $\tilde{V}_{R,1,2,3}^-[T_R^+] = \tilde{V}_{R,3,4,1}^+$, and $\tilde{V}_R = \bigcup_{g \in C'_R} \tilde{V}_{R,1,2,3}^-[g^{-1}]$ are obtained. This indicates that the algorithm is optimal, in the sense that it is impossible to reduce the size of C'_R , even if the coefficients of S^{obs} have precise values. With regard to base-centered forms, $\tilde{V}_B = \bigcup_{g \in C'_B} \tilde{V}_{B,1,2}^{(1)}[g^{-1}]$ holds, hence the same conclusion is obtained.

References

- [1] L. C. Andrews and H. J. Bernstein. Lattices and reduced cells as points in 6-space and selection of bravais lattice type by projections. *Acta Cryst.*, A44:1009–1018, 1988.
- [2] A. Bravais. Mémoire sur les systèmes formés par les points distribués régulièrement sur un plan ou dans l'espace. *J. Ecole Polytech.*, 19:1–731, 1850.
- [3] M. J. Buerger. Reduced cells. *Z. Kristallogr.*, 109:42–60, 1957.
- [4] J. H. Conway. *The sensual (quadratic) form* (邦題: 素数が香り、形がきこえる: 目で見る 2次形式からはじまる数学). Carus Mathematical Monographs 26, Mathematical Association of America, 2006.
- [5] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups (3rd ed.)*, volume 290 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1998.

Table 7: Algorithm for nearly rhombohedral lattices

| | |
|----------|--|
| (Input) | $S^{obs} \in \mathcal{S}_{>0}^3$: Selling-reduced in a broad sense, $\epsilon > 0$, $\text{dist}(S, T)$: same as in Table 2, |
| (Output) | A : array of pairs of $g \in GL_3(\mathbb{Z})$ and $S \in V_R$ satisfying $\text{dist}(S, S^{obs}[g]) \leq \epsilon$. |
| <hr/> | |
| 1: | Prepare the array C'_R of size $I_{max} := 16$ presented in Table 5. |
| 2: | for $i = 1$ to I_{max} do |
| 3: | Compute $S_{new} := C'_R[i] S^{obs} {}^t C'_R[i]$. |
| 4: | Set $a := \frac{1}{3}(s_{11} + s_{22} + s_{33})$ and $d := \frac{1}{3}(s_{12} + s_{13} + s_{23})$, using the (i, j) -entry s_{ij} of S_{new} . |
| 5: | Set $S := \begin{pmatrix} a & d & d \\ d & a & d \\ d & d & a \end{pmatrix}$. |
| 6: | If $\text{dist}(S_{new}, S) \leq \epsilon$, insert $(C'_R[i], S)$ in A . |
| 7: | end for |

Table 8: Algorithm for nearly base-centered lattices.

| | |
|----------|---|
| (Input) | $S^{obs} \in \mathcal{S}_{>0}^3$: Selling-reduced in a broad sense, $\epsilon > 0$, $\text{dist}(S, T)$: same as in Table 2, |
| (Output) | A : array of pairs of an integer matrix g with $h_B g \in GL(3, \mathbb{Z})$ and $S \in V_B$ satisfying $\text{dist}(S, S^{obs}[g]) \leq \epsilon$. |
| <hr/> | |
| 1: | Prepare the array C'_B of size $I_{max} := 21$ presented in Table 5. |
| 2: | for $i = 1$ to I_{max} do |
| 3: | Compute $S_{new} := C'_B[i] S^{obs} {}^t C'_B[i]$, |
| 4: | Set $S := \begin{pmatrix} s_{11} & 0 & s_{13} \\ 0 & s_{22} & 0 \\ s_{13} & 0 & s_{33} \end{pmatrix}$, using the (i, j) -entry s_{ij} of S_{new} . |
| 5: | If $\text{dist}(S_{new}, S) \leq \epsilon$, insert $(C'_B[i], S)$ in A . |
| 6: | end for |

- [6] W. I. F. David, K. Shankland, L. B. McCusker, and Ch. Baerlocher. *Structure determination from powder diffraction data (IUCr Monographs on crystallography 13)*. Oxford Science publications, 2002.
- [7] P. M. de Wolff. On the determination of unit-cell dimensions from powder diffraction patterns. *Acta Cryst.*, 10:590–595, 1957.
- [8] P. M. de Wolff. A simplified criterion for the reliability of a powder pattern indexing. *J. Appl. Cryst.*, 1:108–113, 1968.
- [9] B. Delaunay. Neue darstellung der geometrischen kristallographie. *Z. Kristallogr.*, 84:109–149, 1933.
- [10] G. Eisenstein. Tabelle der reducirten positiven quadratischen former nebst den resultaten neuerer forschungen. *J. Reine Angew. Math.*, 41:141–189, 1851.
- [11] R. W. Gross-Kunstleve, N. K. Sauter, and P. D. Adams. Numerically stable algorithms for the computation of reduced unit cells. *Acta Cryst.*, A60:1–6, 2004.
- [12] B. Gruber. The relationship between reduced cells in a general bravais lattice. *Acta Cryst.*, A29:433–440, 1973.
- [13] T. Hahn. *International tables for crystallography*, volume A. Dordrecht:Kluwer, 1983.
- [14] T. Ito. A general powder X-ray photography. *Nature*, 164:755–756, 1949.
- [15] I. Křivý and B. Gruber. A unified algorithm for determining the reduced (niggli) cell. *Acta Cryst.*, A32:297–298, 1976.
- [16] J. C. Lagarias, H. W. Lenstra, JR., and C. P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.
- [17] Y. Le Page. The derivation of the axis of the conventional unit cell from the dimensions of the buerger reduced cell. *J. Appl. Cryst.*, 15:255–259, 1982.
- [18] H. Minkowski. Diskontinuitätsbereich für arithmetische äquivalenz. *J. Reine Angew. Math.*, 129:220–274, 1905.
- [19] P. Niggli. *Kristallographische und strukturtheoretische grundbegriffe. Handbuch der experimentalphysik*, volume 7. Leipzig: Akademische Verlagsgesellschaft, 1928.
- [20] R. Oishi-Tomiyasu. 結晶学におけるある 3 次元格子の決定問題への格子基底簡約理論の迅しい応用, accepted. 応用数理.
- [21] R. Oishi-Tomiyasu. Distribution rules of systematic absences on the conway topograph and their application to powder auto-indexing. *arXiv:1211.3926*, 2012. (different article from [23], although the title is same).
- [22] R. Oishi-Tomiyasu. Rapid bravais-lattice determination algorithm for lattice parameters containing large observation errors. *Acta Cryst. A.*, 68:525–535, 2012.
- [23] R. Oishi-Tomiyasu. Distribution rules of systematic absences on the conway topograph and their application to powder auto-indexing. *Acta Cryst. A.*, 68:603–610, 2013.
- [24] R. Oishi-Tomiyasu. Method to generate all the geometrical ambiguities of powder indexing solutions. *J. Appl. Cryst.*, 47:2055–2059, 2014.

- [25] R. Oishi-Tomiyasu. A table of geometrical ambiguities in powder indexing obtained by exhaustive search. *Acta Cryst. A.*, 72:73–80, 2016.
- [26] A. Pettet and J. Souto. Minimality of the well-rounded retract. *Geometry and Topology*, 12:1543–1556, 2008.
- [27] W. Plesken and W. Hanrath. The lattices of six-dimensional euclidean space. *MATHEMATICS OF COMPUTATION*, 243:573–587, 1984.
- [28] S. S. Ryshkov and E. P. Baranovskii. C-types of n-dimensional lattices and 5-dimensional primitive parallelohedra (with application to the theory of coverings). *Proceedings of the Steklov Institute of Mathematics*, 137, 1976.
- [29] J. W. Visser. A fully automatic program for finding the unit cell from powder data. *J. Appl. Cryst.*, 2:89–95, 1969.
- [30] G. F. Voronoi. Sur quelques proprietes des formes quadratiques positives parfaites. *J. Reine Angew. Math.*, 133:97–178, 1907.
- [31] G. F. Voronoi. Nouvelles applications des parametres continus a la theorie des formes quadratiques. *J. Reine Angew. Math.*, 134:198–287, 1908.
- [32] G. L. Watson. Determination of a binary quadratic form by its values at integer points. *Mathematika*, 26:72–75, 1979.
- [33] G. L. Watson. Determination of a binary quadratic form by its values at integer points: acknowledgement. *Mathematika*, 27:188, 1980.
- [34] H. Zimmermann and H. Burzlaff. Delos—a computer program for the determination of a unique conventional cell. *Z. Kristallogr.*, 170:241–246, 1985.
- [35] L. Zuo, J. Muller, M. J. Philippe, and C. Esling. A refined algorithm for the reduced-cell determination. *Acta Cryst.*, A51:943–945, 1995.

A summation formula for polynomials in binary variables

Norichika Matsuki

Let $I_n = (x_1^2 - 1, \dots, x_n^2 - 1)$ be an ideal of $\mathbb{Q}[x_1, \dots, x_n]$. For $f \in \mathbb{Q}[x_1, \dots, x_n]$, we define \bar{f} as the right-hand side of the congruence

$$f \equiv a_\emptyset + \sum_{S \subseteq \{1, \dots, n\}} a_S x^S \pmod{I_n},$$

where x^S is a multilinear monomial that has factor x_i if and only if $i \in S$. Note that $f(b_1, \dots, b_n) = \bar{f}(b_1, \dots, b_n)$ for $b_1, \dots, b_n \in \{-1, 1\}$. Denote by S_i the i -th subset of the graded lexicographically ordered subsets

$$\emptyset < \{1\} < \{n\} < \{1, 2\} < \dots < \{n-1, n\} < \dots < \{1, \dots, n\}.$$

We define $T(\bar{f}) = (T(\bar{f})_{ij})$ to be the matrix whose (i, j) entry is $a_{S_i \Delta S_j}$, where $S_i \Delta S_j$ is the symmetric difference of S_i and S_j . Then the following property [2, Theorem 3.3] holds.¹

Theorem 1 *Let $n(f)$ be the zero points in $\{-1, 1\}^n$ of $f \in \mathbb{Q}[x_1, \dots, x_n]$. Then $n(f) = 2^n - \text{rank } T(\bar{f})$.*

In this article, we calculate the trace and determinant of $T(\bar{f})$. Our tool is the following summation formula.

Lemma 2

$$\sum_{b_1, \dots, b_n \in \{-1, 1\}} f(b_1, \dots, b_n) = 2^n \bar{f}(0, \dots, 0).$$

Proof. We use induction on n . It is obvious for $n = 1$. Suppose that it is true for $n = k$. Since

$$\bar{f}(x_1, \dots, x_k, -1) + \bar{f}(x_1, \dots, x_k, 1) = 2\bar{f}(x_1, \dots, x_k, 0),$$

¹For the number of solutions in \mathbb{F}_q^n of a Diophantine equation in n variables over \mathbb{F}_q , the similar property also holds [3].

we have

$$\begin{aligned} \sum_{b_1, \dots, b_{k+1} \in \{-1, 1\}} f(b_1, \dots, b_{k+1}) &= 2^k \bar{f}(0, \dots, 0, -1) + 2^k \bar{f}(0, \dots, 0, 1) \\ &= 2^{k+1} \bar{f}(0, \dots, 0). \end{aligned}$$

Hence it is also true for $n = k + 1$. \square

Theorem 3

$$\text{tr } T(\bar{f}) = \sum_{b_1, \dots, b_n \in \{-1, 1\}} f(b_1, \dots, b_n), \quad (1)$$

$$\det T(\bar{f}) = \prod_{b_1, \dots, b_n \in \{-1, 1\}} f(b_1, \dots, b_n). \quad (2)$$

Proof. From the definition, we have $T(\bar{f})_{ii} = \bar{f}(0, \dots, 0)$. By Lemma 2, (1) follows.

Since $f(b_1, \dots, b_n)$ is an eigenvalue of $T(\bar{f})$ [2, the proof of Lemma 3.2], (2) follows. \square

Lemma 2 is applicable to combinatorial problems. Given a set of integer and an integer m , the subset sum problem is to decide whether there is a subset whose sum equals m . Li and Wan [1] gave a formula for the number of solutions of the subset sum problem over a finite field. The problem is reduced to deciding whether $l_n = a_1 x_1 + \dots + a_n x_n = 0$, where $a_1, \dots, a_n \in \mathbb{Z}$, has a solution in $\{-1, 1\}^n$. We calculate the number $n(l_n)$ of the solutions.

Proposition 4 Let $a = |a_1| + \dots + |a_n|$ and $\Gamma = \{1^2, \dots, a^2\}$. Then we have

$$n(l_n) = \frac{2^n}{(a!)^2} \sum_{\substack{1 \leq i \leq a \\ k_1, \dots, k_{a-i} \in \Gamma}} \sum_{\substack{j_1 + \dots + j_n = i \\ j_1 \geq 0, \dots, j_n \geq 0}} \frac{(-1)^i (2i)! k_1 \dots k_{a-i} a_1^{2j_1} \dots a_n^{2j_n}}{(2j_1)! \dots (2j_n)!}.$$

Proof. Setting

$$\begin{aligned} L(x_1, \dots, x_n) &= \frac{(-1)^a}{(a!)^2} \prod_{1 \leq |k| \leq a} (a_1 x_1 + \dots + a_n x_n - k) \\ &= \frac{1}{(a!)^2} \sum_{\substack{1 \leq i \leq a \\ k_1, \dots, k_{a-i} \in \Gamma}} (-1)^i k_1 \dots k_{a-i} (a_1 x_1 + \dots + a_n x_n)^{2i}, \end{aligned}$$

it follows that

$$L(x_1, \dots, x_n) = \begin{cases} 1 & \text{if } a_1 x_1 + \dots + a_n x_n = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Since

$$\overline{L}(0, \dots, 0) = \frac{1}{(a!)^2} \sum_{\substack{1 \leq i \leq a \\ k_1, \dots, k_{a-i} \in \Gamma}} (-1)^i k_1 \cdots k_{a-i} \times \left(\sum_{\substack{2j_1 + \dots + 2j_n = 2i \\ 2j_1 \geq 0, \dots, 2j_n \geq 0}} \frac{(2i)!}{(2j_1)! \cdots (2j_n)!} a_1^{2j_1} \cdots a_n^{2j_n} \right),$$

the proposition follows. \square

Next consider

$$h_n = \prod_{\substack{1 \leq i < j \leq n \\ 1 \leq l \leq n/2}} \left(\left(\sum_{k=1}^n x_{ik} x_{jk} \right)^2 - 4l^2 \right).$$

Since a matrix (c_{ij}) is an Hadamard matrix if and only if $|c_{ij}| = 1$ and $\sum_{k=1}^n c_{ik} c_{jk} = 0$ for $1 \leq i < j \leq n$, we see that there is an Hadamard matrix of order n if and only if $\overline{h}_n(0, \dots, 0) \neq 0$.

References

- [1] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Fields Appl.* 14 (2008) 911–929.
- [2] N. Matsuki, Counting problems and ranks of matrices, *Linear Algebra Appl.* 465 (2015) 104–106.
- [3] N. Matsuki, On the number of solutions of a Diophantine equation over a finite field, submitted for publication.

ペアリング暗号に適した楕円曲線族が 理想的条件をもつ可能性について

岡野 恵司 (都留文科大学)¹⁾

1 主結果

Koblitz [13], Miller [15] によって独立に提唱された楕円 ElGamal 暗号とは別に, 曲線のペアリングに基づいた暗号方式が 2000 年を前後して Boneh-Franklin [4], 柏原-大岸-境 [11], [12] によって (これもまた独立に) 提唱された. この暗号方式は ID-情報に基づく公開鍵暗号や三者間鍵共有などへの応用に適していると考えられている. この暗号方式の最も大きな特徴の一つは, “ペアリングに適した (pairing-friendly) 楕円曲線 (以下 PF 楕円曲線と略す)” とよばれる特別な性質をもつ曲線を必要とする, ということである. そしてこの曲線を構成することがこの分野の大きな課題の一つとなっている. よく知られた構成法で実際に広く応用されているものとしては, 例えば Cocks-Pinch による構成 [7], Brezing-Weng による構成 [6] や, 宮地-中林-高野による MNT-曲線 [16], Barreto-Naehrig による BN-曲線 [2], Kachisa-Schaefer-Scott による KSS-曲線 [10] などがある.

さて, このような曲線のペアリングに基づいた暗号方式では, 構成した PF 楕円曲線 E/\mathbb{F}_q の部分群を暗号に用いるのであるが, この部分群の位数 r と定義体の位数 q に関して指標となる値 ρ を定義する: $\rho(E) = (\log q)/(\log r)$. この値が大きいくほど, 曲線の定義体が r に比べて大きいということであり, 計算に時間がかかってしまうことを意味する. 様々な埋め込み次数に対し, この値が 1 に近い (1 となるのが最良であるといえる) 曲線を構成することが大きな目標である. しかし ρ が 1 に近い曲線の構成は現在も盛んに研究されているにもかかわらず, ちょうど $\rho = 1$ となるものは非常に少ない. 特に本稿の考察対象である楕円曲線の完全族については, (ρ の定義は少し異なるが) $\rho = 1$ となる族は BN-曲線のたった一つしか知られていない. 近年ではゼロ知識証明に $\rho = 1$ である MNT-曲線や BN-曲線のもつ性質が応用されている ([3], [8] 参照) ということや, 数学的興味からも, $\rho = 1$ となる曲線を求めることは興味深い問題といえる. しかし上記のようになかなか見つからないのであるから, そもそも存在するための必要条件も考える必要があると思われる. 例えば, 埋め込み次数 1, 2 に対しては $\rho = 1$ となる PF 楕円曲線の完全族は存在しない ([9, Proposition 2.9]). そこで本稿ではこのような理想的な PF 楕円曲線の完全族が存在するための条件を考察する.

k を自然数, D を平方因子をもたない自然数とする. 有理数係数多項式の組 $(t(x), r(x), q(x), y(x))$ が CM-判別式 D , 埋め込み次数 k をもつ PF 楕円曲線の完全族を生成するとする (各述語は後で改めて定義する).

$$\rho(t, r, q, y) := \lim_{x \rightarrow \infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}$$

¹⁾E-mail: okano@tsuru.ac.jp

とおく. 以下 $\varphi(x)$ は Euler 関数, $\Phi_k(x)$ は k 次円分多項式とする. このとき主結果は次のようになる. 最初の 2 つは小さい埋め込み次数 k に関するものである.

定理 1.1. $k = 3, 4, 6$ のとき, $\rho(t, r, q, y) \neq 1$, すなわちどのような PF 楕円曲線の完全族も理想的条件は満たさない.

定理 1.2. $k = 8$ または $k = 12$ とする. $\sqrt{-D}$ が k 次円分体に含まれかつ

$$\deg r(x) \neq 2 \deg t(x)$$

であれば, $\rho(t, r, q, y) \neq 1$ である.

注 1.3. MNT-曲線は埋め込み次数 3, 4, 6 の $\rho = 1$ を満たす族であるが, 完全族ではない. また BN-曲線は埋め込み次数 12 をもつが, 定理 1.2 の仮定 $\deg r(x) \neq 2 \deg t(x)$ は満たしていないので, 既存の結果とは矛盾しない.

次の 2 つは部分群の位数を生成する多項式 $r(x)$ として円分多項式を選んだ場合の結果である.

定理 1.4. [17]. $r(x) = \Phi_k(x)$ とき, 次のいずれかを満たしているならば $\rho(t, r, q, y) \neq 1$.

- (i) k は p および $2p$ のいずれか. ただし p は奇素数.
- (ii) k は $pQ, 2pQ$ のいずれかであって次が成り立つ:

$$(p-2)Q + 1 < \varphi(k), \quad D = p, \quad t(x) = x + 1.$$

ここで $p \geq 7$ は $p \equiv 3 \pmod{4}$ なる奇素数であり, $Q \geq 2$ は整数である.

注 1.5. 定理 1.4 (i) は Sha [18] によりさらに拡張されている. 定理 1.4 (ii) の条件は (i) の証明方法を k が合成数の場合にも適用できるようにするための技術的条件である. 例えば 2 つの奇素数 p, q ($p \leq q$) により $k = pq$ と表せるのであれば, $(p-2)Q + 1 < \varphi(k)$ は満たされる.

定理 1.6. [17]. $r(x), t(x)$ が

$$r(x) = \Phi_{dk}(x), \quad t(x) = x^{dg} + 1 \quad (\gcd(g, k) = 1)$$

であるとする (d は任意の自然数). このとき埋め込み次数 k が平方因子をもつならば $\rho(t, r, q, y) \neq 1$ である.

2 ペアリングに適した楕円曲線とその族

この節ではペアリングに適した楕円曲線の定義と, Brezing-Weng [6] によるその完全族の構成法を簡単に解説する. 詳しい解説は Freeman-Scott-Teske [9] を参照.

有限体 \mathbb{F}_q 上の楕円曲線を E とする. その \mathbb{F}_q -有理点の個数は Frobenius 写像のトレース t を用いて

$$E(\mathbb{F}_q) = q + 1 - t$$

と表せる. E の部分群に関する埋め込み次数を次のように定義する.

定義 2.1. $E(\mathbb{F}_q)$ が素数位数 r ($\gcd(r, q) = 1$) の部分群 G をもつとする. r に関する埋め込み次数を, G 上の非退化ペアリング $G \times G \rightarrow \overline{\mathbb{F}_q}^\times$ の像を含む最小の体の \mathbb{F}_q 上の拡大次数と定める. ただし $\overline{\mathbb{F}_q}$ は \mathbb{F}_q の代数閉包. もし $r \nmid kq$ であれば, これは

$$r \mid \Phi_k(t-1)$$

と同値 ([9, Proposition 2.4]).

[9] に倣い, 次の (i)(ii) を満たす楕円曲線をペアリングに適した楕円曲線 (以下 PF 楕円曲線と略す) とよぶ:

- (i) 素数 r は $r \geq \sqrt{q}$ かつ $r \mid \#E(\mathbb{F}_q)$ を満たす.
- (ii) r に関する埋め込み次数 k は $(\log_2 r)/8$ より小さい.

PF 楕円曲線とは, 簡単に言えば, ペアリングが効率的に計算可能であって任意のセキュリティレベルを確保した暗号系に利用可能な楕円曲線のことである. また冒頭で述べたように $\rho(E) = (\log q)/(\log r)$ を定める. この値が大きいほど, 計算に時間がかかってしまうことを意味する.

暗号実装の際には, 安全性に合わせて様々な埋め込み次数 k に対する PF 楕円曲線が必要になる. E が超特異であれば $k \leq 6$ であることが分かっているから, 超特異でない (ordinary) 楕円曲線を作る必要がある. 与えられた素数を位数とする部分群をもつ楕円曲線の構成には, Atkin-Morain [1] による CM-法が使われる:

定理 2.2. (Atkin-Morain [1]) k を自然数とする. 次を満たす整数 t, r, q が与えられたとする:

- (i) r は $r \nmid kq$ なる素数.
- (ii) q は素数の冪.
- (iii) $r \mid q + 1 - t$ かつ $\gcd(t, q) = 1$.
- (iv) $r \mid \Phi_k(t-1)$
- (v) ある $y \in \mathbb{Z}$ と平方因子をもたない自然数 $D < 10^4$ が存在して $Dy^2 = 4q - t^2$ が成り立つ (D は CM-判別式とよばれる).

このとき, \mathbb{F}_q 上の超特異でない楕円曲線であって次の性質を満たすものが存在する:

- (a) $\#E(\mathbb{F}_q) = q + 1 - t$ であり, $E(\mathbb{F}_q)$ は位数 r の部分群をもつ.
- (b) r に関する埋め込み次数は k .

以上より問題は, 様々な埋め込み次数 k と素数 r に対し, 定理 2.2 を満たす t, q, D および y を見つければよい, ということになる. これらパラメータを実際に求めるアルゴリズムとして, 例えば Cocks-Pinch 法 [7] が知られている. しかし, この方法で実際に楕円曲線を構成してみるとほとんどが $\rho \approx 2$ であって, ρ が 1 に十分近い値をとることはなかなかない. また実装のためには必要とするビット長の曲線を構成できるようにしたほうが良い. そのため定理 2.2 の t, r, q, y をパラメータ x の多項式にして, 楕円曲線の族を構成する.

定義 2.3. $f(x) \in \mathbb{Q}[x]$ とする.

- (i) ある $a \in \mathbb{Z}$ があって $f(a) \in \mathbb{Z}$ となるとき $f(x)$ は整数生成系であるという.
- (ii) 整数表現をもつ定数でない既約多項式 $f(x)$ について, $f(x)$ の最高次係数が正であって

$$\gcd(f(x) \mid x \text{ は } f(x) \in \mathbb{Z} \text{ を満たす}) = 1$$

を満たすとき, $f(x)$ は素数生成系であるという.

Bouniakowski, Schinzel 等により, 素数生成系である多項式は無数個の素数値を取り得ると予想されているので ([14, p.323]), ここではそれを利用する.

定義 2.4. k を自然数, D を平方因子をもたない自然数とする. 4つの0でない多項式の組 $(t(x), r(x), q(x), y(x)) \in \mathbb{Q}[x]^4$ が次を満たすとする:

- (i) $r(x)$ は素数生成系²⁾.
- (ii) $q(x)$ は素数生成系.
- (iii) $r(x) \mid q(x) + 1 - t(x)$, 即ちある $h(x) \in \mathbb{Q}[x]$ が存在して $h(x)r(x) = q(x) + 1 - t(x)$.
- (iv) $r(x) \mid \Phi_k(t(x) - 1)$.
- (v) $Dy(x)^2 = 4q(x) - t(x)^2 (= 4h(x)r(x) - (t(x) - 2)^2)$.

このとき $(t(x), r(x), q(x), y(x))$ は埋め込み次数 k , CM-判別式 D の **PF** 楕円曲線の完全族を生成するという. さらにこのとき

$$\rho(t, r, q, y) := \lim_{x \rightarrow \infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}$$

と定める.

以下, $\rho = \rho(t, r, q, y)$ と略記する. $\rho = 2 \max\{\deg y(x), \deg t(x)\} / \deg r(x)$ とも表せる. 前述のように $\rho = 1$ のときが最良のものといえ, このとき $h(x)$ は定数である.

$(t(x), r(x), q(x), y(x))$ は埋め込み次数 k , CM-判別式 D の PF 楕円曲線の完全族を生成するとする. このとき定義 2.4 より, $\mathbb{Q}[x]/(r(x))$ は k 次円分体と虚二次体 $\mathbb{Q}(\sqrt{-D})$ を含む体を成し, $t(x) - 1$ が 1 の原始 k 乗根の 1 つになっていることがわかる. 逆にこのような代数体から PF 楕円曲線の完全族を生成する多項式を構成するのが Brezing-Weng のアルゴリズムである:

定理 2.5 (Brezing-Weng [6]). k を自然数, D を平方因子をもたない自然数とする. 以下のステップを実行する:

1. k 次円分体と虚二次体 $\mathbb{Q}(\sqrt{-D})$ を含む体 K をとる.
2. 素数生成系である多項式 $r(x) \in \mathbb{Z}[x]$ であって $\mathbb{Q}[x]/(r(x)) \xrightarrow{\sim} K$ となるものを取り, この同型を固定する.
3. K 内の 1 の原始 k 乗根 ξ_k を 1 つ固定し, $t(x) - 1 \in \mathbb{Q}[x]$ をこの同型により ξ_k に対応する多項式とする.

²⁾(i), (ii) の条件を多少弱めた定義もある [9, Definition 2.7], [10, Definition 2.2].

4. $y(x) \in \mathbb{Q}[x]$ をこの同型によって $\frac{(\xi_{k-1})\sqrt{-D}}{-D} \in K$ に対応する多項式とする.

5. $q(x) := \frac{1}{4}(t(x)^2 + Dy(x)^2)$ とおく.

もし $q(x)$ が素数生成系ならば, $(t(x), r(x), q(x), y(x))$ は埋め込み次数 k , CM-判別式 D の PF 楕円曲線の完全族を生成する.

Brezing-Weng の方法では $t(x), y(x)$ は $r(x)$ を法として定まるので, 生成した楕円曲線族の多くは $\rho < 2$ を満たすことができる. この方法の最も重要な部分は $r(x)$ の取り方であり, $r(x)$ として円分多項式をとるのが古典的かつ標準的である. [9], [10] では円分多項式でない場合を数多く扱っている. また $t(x)$ の取り方も 1 の原始 k 乗根の取り方の分だけある. この方法により, $\rho < 2$ の完全族の構成が保証され, より小さい ρ をもつ族を構成する研究が進められているが, 現在においても $\rho = 1$ を満たす完全族の例は Barreto-Naehrig [2] による以下の例しか知られていない:

$$\begin{cases} t(x) = 6x^2 + 1, \\ r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ y(x) = 6x^2 + 4x + 1 \end{cases}$$

とすると, これらは埋め込み次数 12, CM-判別式 3, $\rho = 1$ の PF 楕円曲線の完全族を生成する.

3 定理 1.1 の概略

$k = 4$ のときのみ示す (他も同様). $\deg t(x) < \deg r(x)$, $\deg y(x) < \deg r(x)$ と仮定してよい. まず $\sqrt{-D}$ が k 次円分体に含まれる場合は容易である: ζ_4 を 1 の原始 4 乗根であって, 固定した同型 $\mathbb{Q}[x]/(r(x)) \simeq K \supset \mathbb{Q}(\zeta_4)$ により $X := t(x) - 1$ と対応するものとする. $\sqrt{-1}$ は $s(x) = \pm X$ と対応するから, $\Phi_4(X) = X^2 + 1$ により

$$\begin{aligned} y(x) &\equiv \frac{(X-1)s(x)}{-1} = \mp(X^2 - X) \\ &\equiv \pm(X+1) \pmod{r(x)} \end{aligned}$$

となる. よって $q(x) = \frac{1}{2}(X+1)^2$ を得るが, これは $q(x)$ が素数生成系であることに矛盾.

次に $\sqrt{-D}$ が k 次円分体に含まれず, かつ $\rho = 1$ とする. $X = t(x) - 1$, $m := \deg t(x)$ とおくと, 仮定より $m > 1$ である. $r(x) \mid \Phi_4(X)$ かつ $1 = \rho \geq \frac{2 \deg t(x)}{\deg r(x)}$ より, $r(x)$ は

$$r(x) = \Phi_4(X)$$

という表示をもつ. $r(x)$ の具体的表示が得られたので, あとは地道に $y(x) \bmod r(x)$ を計算すればよい: まず

$$\deg y(x) = \frac{m}{2}$$

を導く. 次数が $2m$ 未満の多項式よりなる \mathbb{Q} -ベクトル空間 $\mathbb{Q}[x]_{2m-1}$ の基底として

$$\begin{aligned} & x^{m-1}X, \quad x^{m-2}X, \quad \dots, \quad xX, \quad X, \\ & x^{m-1}, \quad x^{m-2}, \quad \dots, \quad x, \quad 1 \end{aligned}$$

をとり, $s(x) \in \mathbb{Q}[x]_{2m-1}$ を

$$s(x) = (F_1(x)x+a_1)X + (F_2(x)x+a_2) \quad (a_i \in \mathbb{Q}, \deg F_i(x) \leq m-2 \ (i=1,2))$$

と表せば

$$\begin{aligned} & (X-1)s(x) \\ & = F_1(x)xX^2 + a_1X^2 + (F_2(x) - F_1(x))xX + (a_2 - a_1)X - (F_2(x)x + a_2) \end{aligned}$$

となる. $F_1(x)xX^2, a_1X^2, (F_1(x) - F_2(x))xX$ はどれも同じ次数の項はもたないことに注意する. 一方で $\deg((X-1)s(x)) < 3m$ と $\deg y(x) < 2m$ より

$$(X-1)s(x) = -Dy(x) + (G(x)x+b)\Phi_4(X) \quad (b \in \mathbb{Q}, \deg G(x) \leq m-2) \quad (3.2)$$

と表せる. $\deg y(x) \leq m$ だから (3.1), (3.2) の両者を比較して

$$-Dy(x) = (a_2 - a_1)X - 2F_1(x)x - (a_2 + a_1).$$

故に

$$\begin{aligned} D^2y(x)^2 & = -4(a_2 - a_1)F_1(x)xX \\ & \quad + 4F_1(x)^2x^2 + 4(a_2 + a_1)F_1(x)x + (X \text{ のみの項}). \end{aligned} \quad (3.3)$$

ここで $Dy(x)^2 = 4h\Phi_4(X) - (X-1)^2 \in \mathbb{Q}[X]$ なので, (3.3) と $\deg X \geq 2$ とを合わせて

$$F_1(x) = 0 \quad \text{または} \quad a_1 = a_2$$

である. $\sqrt{-D} \notin \mathbb{Q}(\zeta_4)$ より容易に $F_1(x) \neq 0$ かつ $a_1 = a_2 = b$ がわかるので, 結局 $-Dy(x) = -2F_1(x)x - 2a_1$ となる. 以上より $\deg(y(x)^2) \leq 2(m-1)$ が得られ, $y(x)^2 \in \mathbb{Q}[X]$ と $\deg X = m$ より $\deg y(x) = m/2$ を得る.

この結果より $Dy(x)^2 = 2X$ となって $q(x) = \frac{1}{4}(X^2 + 4X + 1)$ となる. 確かに $\deg q(x) = \deg r(x)$ であるが, これは $q(x)$ が整数生成系であることに矛盾する. 故に $\rho \neq 1$.

4 定理 1.2 の証明の概略

証明は単純である. 再び $m = \deg t(x)$ とおく. $r(x) \mid \Phi_k(t(x) - 1)$ かつ $\varphi(k) \mid \deg r(x)$ だから ([9, Theorem 5.1] 参照), ある整数 $n \leq m$ があって $\deg r(x) = 4n$ と書ける. もし $4n < 2m$ なら $\rho > 1$ なので $m \leq 2n$ としてよく, 仮定と合わせて

$$n \leq m < 2n \quad (4.1)$$

が成り立っている. また $\deg y(x) < \deg r(x)$ としてよい. 定理 1.1 の証明のときと同様に $\zeta = \zeta_k$ を 1 の原始 k 乗根であって, 同型 $\mathbb{Q}[x]/(r(x)) \simeq K$ により $t(x) - 1$ と対応するものとする.

$\alpha \in \mathbb{Q}(\zeta)$ に対し, この同型によって対応する次数 $4n$ 未満の代表元を $P(\alpha) = P(\alpha; x) \in \mathbb{Q}[x]$ とおく. 例えば $P(\zeta) = t(x) - 1$, $P((\zeta - 1)\sqrt{-D}) = -Dy(x)$ である. これは \mathbb{Q} -線型写像 $\mathbb{Q}(\zeta) \rightarrow \mathbb{Q}[x]$ になっている.

ここで $\rho = 1$ と仮定する. (4.1) より $2 \deg t(x) < \deg r(x)$ だから

$$\deg y(x) = 2n \quad (4.2)$$

を得る. さらに $\deg (P(\zeta)^2) = 2m < 4n$ もわかるから, $P(\zeta^2) = P(\zeta)^2$ も得られる. 以上を使って $(\zeta - 1)\sqrt{-D}$ と $\zeta(\zeta - 1)\sqrt{-D}$ の次数をみる. ここでは $k = 8$, $D = 1$ のときを扱う (他の場合も同様). $\sqrt{-1} = \pm\zeta^2$ より

$$\begin{aligned} -Dy(x) &= P(\pm(\zeta - 1)\zeta^2) = P(\pm(\zeta^3 - \zeta^2)) \\ &= \pm P(\zeta^3) \mp P(\zeta^2). \end{aligned}$$

(4.1), (4.2) と合わせると

$$\deg P(\zeta^3) \leq 2m$$

を得る. 一方 (4.1) から $\deg (P(\zeta)P((\zeta - 1)\sqrt{-1})) = m + 2n < 4n$ なので

$$P(\mp(\zeta^3 + 1)) = P(\zeta(\zeta - 1)\sqrt{-1}) = P(\zeta)P((\zeta - 1)\sqrt{-1})$$

となる. 特に $P(\zeta^3)$ は次数 $m + 2n$ をもつ. しかし $\deg P(\zeta^3) \leq 2m$ であったから $2n \leq m$ である. これは (4.1) に矛盾し, 従って $\rho \neq 1$ である.

5 定理 1.4 の証明の概略

$k = p$ のときのみ扱う (他も同様である). $r(x) = \Phi_p(x)$ とする. 定理 1.1 より $m := \varphi(k)/2 \geq 2$ のときのみ調べればよい. x に対応する 1 の原始 p 乗根 ζ_p を固定する³⁾. このとき, $\deg r(x) = p - 1$ だから $t(x)$ はある整数 g

³⁾ この ζ_k のとり方は 定理 1.1, 1.2 のときとは異なる. ζ_k は $t(x) - 1$ に対応しているとは限らない.

($1 \leq g < k$, $\gcd(g, k) = 1$) を用いて $t(x) = x^g + 1$ と表せる. $\deg y > m$ を示せばよい. 円分体の理論より $p = D \equiv 3 \pmod{4}$ であり, $m \geq 2$ より $p \geq 7$ である. 例えば [5, Theorem 7 on p.349, Problem 8 on p.354]などを参照すると

$$\sqrt{-p} = \sum_{a=0}^{p-1} \chi_p(a) \zeta_p^a$$

と表せる. ここで $\chi_p(a)$ は p を法とする位数 2 の Dirichlet 指標. さて $y(x)$ に対応する元は $(\zeta_p^g - 1)\sqrt{-p}/(-p)$ であり, これに上式を代入すると

$$(\zeta_p^g - 1)\sqrt{-p} = \sum_{a=0}^{p-2} (\chi_p(a-g) - \chi_p(a)) \zeta_p^a + (1 - \chi_p(1+g)) \zeta_p^{p-1} \quad (5.1)$$

となる.

$\chi_p(1+g) = 1$ とする. このときある $\frac{p+1}{2} \leq b \leq p-2$ が存在して $\chi_p(b-g) - \chi_p(b) \neq 0$ が成り立つことを示す. そうでないと仮定すると

$$\begin{cases} \chi_p(1) = \chi_p(1+g), \\ \chi_p(a) = \chi_p(a-g) \quad \left(\frac{p+1}{2} \leq a \leq p-2\right) \end{cases}$$

となるので, $\chi_p(p-1) = -1 = \chi_p(-1-g) = \chi_p((p-1)-g)$ が成り立ち, 従って

$$\chi_p(a) = -\chi_p(p-a) = -\chi_p(p-a-g) = \chi_p(a+g)$$

がすべての $2 \leq a \leq \frac{p-1}{2}$ で成り立つ. よって χ_p は法 g で定義されることになり $g = p$ となる. これは $\gcd(g, p) = 1$ に矛盾である. この主張より (5.1) の ζ_p^b の項は消えないから $y(x)$ の次数は $m = \frac{p-1}{2}$ より大きい.

次に $\chi_p(1+g) = 0$, すなわち $g = p-1$ なら, $\deg t = g = p-1$ だから $\rho \neq 1$ である.

最後に $\chi_p(1+g) = -1$ とすると (5.1) は

$$(\zeta_p^g - 1)\sqrt{-p} = \sum_{a=0}^{p-2} (\chi_p(a-g) - \chi_p(a) - 2) \zeta_p^a$$

となる. そこである整数 $2 \leq a \leq \frac{p-1}{2}$ が存在して $\chi_p(p-a-g) - \chi_p(p-a) \neq 2$ が成り立つことを示せばよい. そうでないと仮定すると,

$$\begin{cases} \chi_p(2) = \cdots = \chi_p(\frac{p-1}{2}) = 1 \\ \chi_p(\frac{p+1}{2}) = \cdots = \chi_p(p-1) = -1 \end{cases}$$

かつ $g = \frac{p-1}{2}$. これは矛盾. 実際 $p = 7, 11$ なら $\chi_7(4) = 1, \chi_{11}(9) = 1$ であり, $p \geq 19$ なら $\sqrt{\frac{p}{2}} < c < \sqrt{p}$ なる c をとれば $\chi_p(c^2) = 1$ かつ $\frac{p+1}{2} \leq c^2 \leq p-1$ だからである. 以上より $\deg y > m$ となって主張がいえたとことになる.

6 定理 1.6 の証明

この証明が4つの定理の中で最もややこしい。基本的な考え方は、 $\rho = 1$ として定義 2.4(v) の式を見ると、対称性をもつ円分多項式が x^a ($k = a^2 k'$) の多項式でもあるとき $(t(x) - 2)^2 = (x^{dg} - 1)^2$ という僅か3項を引くことで $Dy(x)^2$ という完全平方を作るのは難しかろうということである。そこでまずは余計な平方因子を取り除いた上で $r(x)$ の次数と $t(x)$ の次数の大小を詳しく調べ(補題 6.3)、このことを正当化する。恥ずかしながら [17] の証明にはギャップがあるので、修正したものを記しておく。まず次の補題が帰納法を使って証明できる：

補題 6.1. $f(x) \in \mathbb{Q}[x]$ を次数 m の多項式とする。 $f(x)^2$ の項のうち次数が m 以上のものがすべて $\mathbb{Q}[x^a]$ ($a \mid m$) に含まれるとすると、 $f(x)$ についても $f(x) \in \mathbb{Q}[x^a]$ が成り立つ。

$r(x) := \Phi_{dk}(x)$ とし、定理 1.6 の仮定が成り立っているとす。 $\rho = 1$ と仮定して矛盾を導く。 $D > 0$ かつ $Dy(x)^2 = 4h\Phi_{dk}(x) - (x^{dg} - 1)^2$ (h は定数) であるから、次数をみて $2dg \leq \varphi(dk)$ となる。まず $\gcd(d, k) = 1$ の場合に帰着させる。

補題 6.2. 必要なら x の適当なべきを改めて x に置きなおすことにより、 $\gcd(d, k) = 1$ かつ d が平方因子をもたない場合に帰着できる。

証明. $\gcd(d, k) =: e \geq 2$ と仮定して $d = ed'$ とおくと、円分多項式の性質より

$$Dy(x)^2 = 4h\Phi_{d'k}(x^e) - ((x^e)^{d'g} - 1)^2 \quad (6.1)$$

となる。 $\deg y(x) < e$ と仮定して矛盾を導く⁴⁾。このとき $\rho = 1$ より $\varphi(dk) = 2dg$ かつ $h = 1/4$ である。もし $d'g = 1$ であれば、 $e\varphi(k) = 2e$ となって、 $k = 3, 4$ または 6 でなければならない。しかし定理 1.1 によってこれは矛盾。故に $d'g \geq 2$ 。 $\Phi_{d'k}(x^e)$ の中の次数 dg の項が $-2x^{dg}$ でなければ

$$2 \deg y(x) \geq dg = ed'g \geq 2e$$

となって矛盾であるから、 $\Phi_{d'k}(x^e)$ の中の次数 dg の項は $-2x^{dg}$ であり、(6.1) の $((x^e)^{d'g} - 1)^2$ のすべての項は $\Phi_{d'k}(x^e)$ の項と打ち消しあうことになる。 $dg = \varphi(dk)/2$ と円分多項式の対称性によって (6.1) の右辺の次数は dg より大きくなり、この場合も $2 \deg y(x) > ed'g \geq 2e$ が得られ矛盾する。以上より

$$\deg y(x) \geq e$$

としてよい。(6.1) の右辺は $\mathbb{Q}[x^e]$ に含まれるから、補題 6.2 を適用して $y(x) \in \mathbb{Q}[x^e]$ を得る。よって x^e を改めて x に置きなおすことで $\gcd(d, k) = 1$ としてよいことになる。

⁴⁾[17] はこの考察を行っていない。

次に d が平方因子をもつとして $d = a^2 d''$ ($a \geq 2$) とおく. このとき

$$Dy(x)^2 = 4h\Phi_{ad''k}(x^a) - ((x^a)^{ad''g} - 1)^2$$

である. 上とまったく同様にして $\deg y(x) \geq a$ が導ける. 故に再び補題 6.2 を適用して x^a を x と改めて置きなおすことができ, d は平方因子をもたない (かつ $\gcd(d, k) = 1$) として考えればよいことになる. \square

補題のような状況のもとで, k が平方因子をもち, かつ $\rho = 1$ であるとして矛盾を導く. $k = a^2 k'$ ($a \geq 2$, k' は平方因子をもたない) と表示しておく. $\gcd(d, k) = \gcd(g, k) = 1$ より $\gcd(dg, a) = 1$ であることに注意. $m := \varphi(dk)/2 = a\varphi(d)\varphi(ak')/2$ とおくと, $2dg \leq 2m$ である. 再び $Dy(x)^2$ の式を見ると

$$Dy(x)^2 = 4h\Phi_{dak'}(x^a) - (x^{dg} - 1)^2. \quad (6.2)$$

補題 6.3. $a \neq 2$ および $m < 2dg < 2m$ が成り立つ.

証明. (i) $dg < m$, (ii) $a \neq 2$, (iii) $m < 2dg$ の順に証明する.

(i) $a \geq 2$ に注意. まず

$$\frac{\varphi(d)\varphi(ak')}{2} \in \mathbb{Z}. \quad (6.3)$$

が成り立つことを示す. まず $d = 1$ かつ (6.3) が成り立たないとする. このとき $a = 2$, $k' = 1$ である. 故にこの場合は $r(x) = \Phi_4(x)$ かつ $k = 4$ であって, この場合は $\rho \neq 1$ であったから, 今の仮定 $\rho = 1$ に矛盾. 次に $d \geq 2$ であれば $\gcd(d, a) = 1$ より $a \neq 2$ または $d \neq 2$ であるが, いずれの場合も $\varphi(d)\varphi(ak')$ は偶数だから (6.3) が成り立つ. 以上より (6.3) がいえた.

$dg = m$ なら $m = a\varphi(d)\varphi(ak')/2 \in a\mathbb{Z}$ より $a \mid dg$ となって $\gcd(dg, a) = 1$ に矛盾. よって $dg < m$ が得られた. 特に (6.2) の右辺の次数は $2m$ となって

$$\deg y = m$$

が得られる.

(ii) $a = 2$ と仮定して再び背理法を用いる. このとき

$$Dy(x)^2 = 4h\Phi_{2dk'}(x^2) - (x^2)^{dg} + 2x^{dg} - 1$$

であって, $2x^{dg}$ 以外の右辺のすべての項は $\mathbb{Q}[x^2]$ に含まれる. また $dg < m = \deg y$ だから, 補題 6.2 を $a = 2$ として適用して $y(x) \in \mathbb{Q}[x^2]$ を得る. しかし右辺の x^{dg} の項は $\gcd(dg, a) = 1$ より奇数次だから, これは矛盾である. 故に $a \neq 2$ となる.

(iii) 上記 (ii) と同様に $m \leq 2dg$ が得られる. 実際 (6.2) の右辺の x^{2dg} , $2x^{dg}$ 以外の項は $\mathbb{Q}[x^a]$ の元であり, $2dg < m = \deg y$ とすると補題 6.2 と $a \nmid dg$ から矛盾が生じるからである. さらに

$$2dg \neq m = a\varphi(d)\frac{\varphi(ak')}{2}$$

がいえる。実際そうでないとすると、 $\varphi(d)\varphi(ak')/2 \in \mathbb{Z}$ より $a \mid 2dg$ となって $a = 2$ を得るが、これは矛盾であるからである。故に $dg < m < 2dg$ となる。 \square

(6.2) の両辺を帰納的に比較していく。 $\deg y = m$ であった。

$$y(x) = y_m x^m + \cdots + y_0 \quad (y_i \in \mathbb{Q}, y_m \neq 0)$$

と表示しておく。まず補題 6.3 によって $m < 2dg$ であったことに注意して、最高次の項から x^{2dg+1} の項へと帰納法を用いると

$$y_i = 0 \quad (2dg - m + 1 \leq i < m, a \nmid i) \quad (6.4)$$

となることが導かれる。

$y_0 \neq 0$ のとき：この場合、今度は定数項から x^{dg-1} の項に向かって帰納法を用いると

$$y_i = 0 \quad (0 < i \leq dg - 1, a \nmid i)$$

となることがわかる。 $dg \leq m - 1$ より $2dg - m + 1 \leq dg$ であるから、この式と (6.4) を比較して $y(x) \in \mathbb{Q}[x^a]$ が導かれる。(6.2) の両辺の x^{dg} を比較すれば、これは矛盾である。

$y_0 = 0$ のとき：この場合、(6.2) の定数項をみて $4h = 1$ 。 $\deg r = 2m > 2dg$ だからこれは $Dy_m^2 = 1$ を意味する。さらに $y_m \in \mathbb{Q}$ と $D > 0$ が平方因子をもたないことより $D = 1$ となる。よって円分体の性質から $4 \mid dk$ である。 $\gcd(d, k) = 1$ と d が平方因子をもたないという仮定より、 $2 \nmid d$ 、したがって $4 \mid a^2 k'$ でなければならない。さらに $\gcd(dg, a) = 1$ と k' も平方因子をもたないことから、 a は偶数であり dg は奇数。最後に (6.2) の $x^2, x^4, \dots, x^{2dg-2}$ の項を昇降順に比較していくと

$$y_i = 0 \quad (0 < i \leq dg - 1, a \nmid i)$$

が導かれ、上記と同様にこれから矛盾が導かれる。

本研究は JSPS 科研費 26870486 の助成を受けたものです。

参考文献

- [1] A.O.L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comput. **61**, (1993) 29–68.
- [2] P.S.L.M. Barreto, M. Naehrig, *Pairing-friendly elliptic curves of prime order*, Selected Areas in Cryptography-SAC 2005. Lecture Notes in Computer Science, **3897** (Springer, Berlin, 2006), 319–331.
- [3] E. Ben-Sasson, A. Chiesa, E. Tromer, M. Virza *Scalable zero knowledge via cycles of elliptic curves*, CRYPTO 2014 (34th IACR International Cryptology Conference), (2014) 276–294.

- [4] D. Boneh, M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 2001. Lecture Notes in Computer Science, **2139** (Springer, Berlin, 2001), 213–229. Full version: SIAM J. Comput. **32**, (2003) 586–615.
- [5] A.I. Borevich, I.R. Shafarevich, *Number theory*, Academic Press (New York-London, 1966)
- [6] F. Brezing, A. Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37**, (2005) 133–141.
- [7] C. Cocks, R.G.E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, Unpublished manuscript (2001).
- [8] C. Costello, C. Fournet, J. Howell, M. Kohlweiss, B. Kreuter, M. Naehrig, B. Parno, S. Zahur, *Geppetto: Versatile Verifiable Computation*, IEEE Symp. Security and Privacy 2015, (2015) 253–270.
- [9] D. Freeman, M. Scott, E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*, Journal of Cryptology **23** (2010), 224–280.
- [10] E. Kachisa, E. Schaefer, M. Scott, *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*, Pairing-Based Cryptography-Pairing 2008. Lecture Notes in Computer Science, **5209** (Springer, Berlin, 2008), 126–135.
- [11] M. Kasahara, K. Ohgishi, R. Sakai, *Notes on ID-based key sharing systems on elliptic curve*, IEICE Japan Tech. Rep., **ISEC99-57** (1999-11), 37–42.
- [12] M. Kasahara, K. Ohgishi, R. Sakai, *Cryptosystems based on pairings*, Symposium on Cryptography and Information Security 2000, SCIS 2000, Okinawa, Japan (2000).
- [13] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, **48** (1987), 203–209.
- [14] S. Lang, *Algebra*, revised 3rd edition (Springer, Berlin, 2002).
- [15] V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science, **218** (Springer-Verlag, 1986), 417–426.
- [16] A. Miyaji, M. Nakabayashi, S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundam. **E84-A**, (2001) 1234–1243.
- [17] K. Okano, *On the rho-values of complete families of pairing-friendly elliptic curves*, J. Math. Cryptol. **6**, (2012) 249–268.
- [18] M. Sha, *A kind of non-ideal cyclotomic families of pairing-friendly elliptic curves*, J. Math. Cryptol. **8**, (2014) 417–440.

数論データベース LMFDB の開発について

Development of LMFDB: a database in number theory

横山 俊一¹ (Shun'ichi Yokoyama)
九州大学大学院 数理学研究院

概要 LMFDB (the database of L -functions, Modular forms, and related objects) は、整数論における巨大データベースの一つ、およびその開発・運営プロジェクトである。筆者もデータベースの提供を行っているが、本稿ではこの取り組みについて簡単に紹介する。

1 LMFDB とは

整数論において、拡大体や Galois 群、楕円曲線やモジュラー形式などをデータベース化する営みは長く行われている。その中でも、近年活発に開発が進んでいるものの一つに LMFDB (the database of L -functions, Modular forms, and related objects) がある。

LMFDB は、David Farmer がチェアを務める大型数論データベース、およびそのプロジェクトの名称である。現在は “the database of L -functions, modular forms, and related objects” という呼称が使われているが、稼働当初は “the L -functions, Modular forms, and their Friends Data Base” と呼ばれており、このイニシャルをとって LMFDB と略記された (この名残が今も残っている)。現在は John Cremona が PI となって、2013 年から 2019 年までの 6 年間の EPSRC² プログラムの予算を確保し運営が進んでいる。これに伴い、当初は米ワシントン大学に設置されていたサーバは、2013 年に英ウォーリック大学³に移設された。

データベースの管理は、原則として GitHub を用いて行われている。基本的には誰でもデータベースの提供によって LMFDB に貢献出来るようになっている。

The screenshot shows the GitHub interface for the LMFDB repository. At the top, it says 'LMFDB / lmfdb' with 22 watches, 29 stars, and 68 forks. Below that, it lists repository statistics: 4,844 commits, 5 branches, 0 releases, and 48 contributors. A table of recent commits is shown, with columns for the commit message and the time since the commit. The most recent commit is 'remove spurious app.debug = True' by user 'jwbober', made 4 days ago. Other recent commits include 'updated authentication code for elliptic_curves, ecnf and hmfs' (3 months ago) and 'Updating the contributor list' (4 months ago).

LMFDB GitHub <https://github.com/LMFDB/lmfdb>

¹s-yokoyama@math.kyushu-u.ac.jp

²Engineering and Physical Sciences Research Council.

³PI の John Cremona が所属している。

2 LMFDB の使い方

それでは実際に利用してみよう．LMFDB のトップページにアクセスすると，以下のような画面が確認出来る．

LMFDB <http://www.lmfdb.org/>⁴

ここでは \mathbb{Q} 上の楕円曲線のデータベース（これも John Cremona による）にアクセスしてみる．左側のツールバーから“Varieties”の項目にある“Curves - Elliptic $/\mathbb{Q}$ ”をクリックすると，検索画面に切り替わる．

本稿執筆（2016年1月）時点では階数4以下，導手369,999以下の全ての \mathbb{Q} 上の楕円曲線（2,306,461個存在する）を網羅している． \mathbb{Q} 上の楕円曲線には，所謂“Cremona’s index”と呼ばれる記号が割り振られ，導手と isogeny 類別が分かるようになっているが，この記法が LMFDB にも踏襲されている．

⁴ベータ版（主に開発者向け）のページは <http://beta.lmfdb.org/> からアクセス出来る．

Elliptic Curve 389.a1 (Cremona label 389a1)

Show commands using: `sagemath, pari/gp, Magma`

This elliptic curve has smallest conductor among those of rank 2.

Minimal Weierstrass equation

$$y^2 + y = x^3 + x^2 - 2x$$

Mordell-Weil group structure

$$\mathbb{Z}^2$$

Infinite order Mordell-Weil generators and heights

| | | |
|--------|-------------------|-------------------|
| P | $(-1, 1)$ | $(0, 0)$ |
| $h(P)$ | 0.686667083305587 | 0.327000773651605 |

Integral points

$$(-2, 0), (-1, 1), (0, 0), (1, 0), (3, 5), (4, 8), (6, 15), (39, 246), (133, 1539), (188, 2584)$$

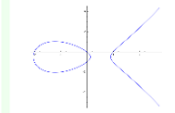
Note: only one of each pair $\pm P$ is listed.

Invariants

$$N = 389 = 389$$

Properties

Label: 389.a1



Conductor: 389
 Discriminant: 389
 j-invariant: $\frac{1404928}{389}$
 CM: no
 Rank: 2
 Torsion Structure: Trivial

Related objects

Isogeny class 389.a
 Minimal quadratic twist (itself) 389.a1
 All twists
 L-function
 Symmetric square L-function
 Symmetric 4th power L-function
 Modular form 389.2a

例えば上は導手 389 の \mathbb{Q} 上の楕円曲線 389a1 : $y^2 + y = x^3 + x^2 - 2x$ である。LMFDB の特徴の一つとして、一つ対象物を選択すると LMFDB サーバ上で即時に計算を行い、関連する様々な情報（不変量、グラフ、整数論的性質）を同時に表示する機能が挙げられる。ここでは楕円曲線のグラフはもちろんのこと、判別式や j 不変量、更に CM 曲線か否か（389a1 は CM 曲線ではない）や、階数が 2 であって Mordell-Weil 群の torsion part は自明であることなども分かる。

LMFDB では、Sage [6], Pari/GP [5], Magma [1] の 3 つのフォーマットに限り、表示された各種データを求めるためのソースコードを表示させることも出来る⁵。画面上の “Show commands using:” の右から選択すればよい。

Invariants

```
sage: E.conductor().factor()
N = 389 = 389
sage: E.discriminant().factor()
Delta = 389 = 389
sage: E.j_invariant().factor()
j = 1404928/389 = 2^12 * 7^3 * 389^-1
End(E) = Z (no Complex Multiplication)
```

Complex multiplication

An elliptic curve whose **endomorphism ring** is larger than \mathbb{Z} is said to have **complex multiplication**. In this case, for curves defined over fields of characteristic zero, the endomorphism ring is isomorphic to an order in an imaginary quadratic field.

This is a special case of an **abelian variety** with complex multiplication.

[permalink](#)

更に `permalink` の機能を使えば、使われている数学用語の簡単な説明を読むことが出来る。例えばこのページの “complex multiplication” の項目をクリックすると、上記のようなポップアップ画面が現れる。

次に画面右側にある “Related objects” の項目に注目してみよう。例えば楕円曲線の場合、それに付随するモジュラー形式の情報が有用である。LMFDB ではこの情報を 1 クリックで引き出すことが出来る。

⁵基本的には計算には Sage が用いられている。「Sage では計算出来るが Magma では計算出来ない」という情報については、Magma のソースコードを選択しても表示されない。

Newforms of weight 2 for $\Gamma_1(389)$

The character number should be a positive integer less than or equal to and coprime to the level 389. You gave: 0

The space of Newforms of weight 2 on $\Gamma_1(389)$ decomposes as

$$S_2^{\text{new}}(\Gamma_1(389)) = \bigoplus_{\chi \bmod 389} S_2^{\text{new}}(\Gamma_0(389), \chi)$$

where the direct sum is over all Dirichlet characters mod 389. If χ and χ' are in the same Galois orbit, then $S_2^{\text{new}}(\Gamma_0(389), \chi)$ and $S_2^{\text{new}}(\Gamma_0(389), \chi')$ are Galois conjugate, so in particular they have the same dimension.

The table below gives the dimensions of the spaces of newforms for $\Gamma_0(389)$ of weight 2 and characters in each Galois orbit, with links to each space.

| Dimension of $S_2^{\text{new}}(\Gamma_0(389), \chi)$ | $S_2(\chi_{389}(n, \cdot)) := S_2^{\text{new}}(\Gamma_0(389), \chi_{389}(n, \cdot))$ for characters χ grouped by Galois orbit | | | | | | |
|--|--|--|---|---|---|---|---|
| 32 | S₂(χ₃₈₉(1, ·)) | | | | | | |
| 0 | S₂(χ₃₈₉(2, ·)) | | | | | | |
| 32 | S₂(χ₃₈₉(3, ·)) | S₂(χ₃₈₉(8, ·)) | S₂(χ₃₈₉(10, ·)) | S₂(χ₃₈₉(12, ·)) | S₂(χ₃₈₉(14, ·)) | S₂(χ₃₈₉(15, ·)) | S₂(χ₃₈₉(19, ·)) |
| 31 | S₂(χ₃₈₉(5, ·)) | S₂(χ₃₈₉(6, ·)) | S₂(χ₃₈₉(7, ·)) | S₂(χ₃₈₉(11, ·)) | S₂(χ₃₈₉(13, ·)) | S₂(χ₃₈₉(16, ·)) | S₂(χ₃₈₉(17, ·)) |
| 0 | S₂(χ₃₈₉(115, ·)) | | | | | | |
| 32 | S₂(χ₃₈₉(274, ·)) | | | | | | |

The space is clickable whenever the Hecke orbits are stored for that space.

ここでは重さ 2, レベル 389 のモジュラー形式とその分解が与えられている。更に L 関数の情報も確認してみる。

L-function $L(s, E)$ for the Elliptic Curve Isogeny Class 389.a

Dirichlet series

$$L(s, E) = 1 - 1.414 \cdot 2^{-s} - 1.154 \cdot 3^{-s} + 4^{-s} - 1.341 \cdot 5^{-s} + 1.632 \cdot 6^{-s} - 1.889 \cdot 7^{-s} + 0.333 \cdot 9^{-s} + 1.897 \cdot 10^{-s} - 1.206 \cdot 11^{-s} - 1.154 \cdot 12^{-s} - 0.832 \cdot 13^{-s} + 2.672 \cdot 14^{-s} + 1.549 \cdot 15^{-s} - 16^{-s} - 1.455 \cdot 17^{-s} - 0.471 \cdot 18^{-s} + 1.147 \cdot 19^{-s} - 1.341 \cdot 20^{-s} + 2.182 \cdot 21^{-s} + 1.705 \cdot 22^{-s} - 0.834 \cdot 23^{-s}$$

Functional equation

$$\Lambda(s, E) = 389^{s/2} \Gamma_{\mathbb{C}}(s + 1/2) \cdot L(s, E) = \Lambda(1 - s, E)$$

Invariants

- d = 2
- N = 389
- ϵ = 1
- Primitive : yes
- Self-dual : yes
- Selberg data = (2, 389, (: 1/2), 1)

Euler product

$$L(s, E) = \prod_{p \text{ bad}} (1 - a(p)p^{-s})^{-1} \prod_{p \text{ good}} (1 - a(p)p^{-s} + p^{-2s})^{-1}$$

Properties

- Degree 2
- Conductor 389
- Sign 1
- Self-dual yes
- Motivic weight 1

Related objects

- [Isogeny class 389.a](#)
- [Elliptic curve 389.a1](#)
- [Symmetric square L-function](#)
- [Symmetric cube L-function](#)

Downloads

- [Lcalcfile](#)

これは楕円曲線 389a1 に付随する L 関数 $L(s, E)$ に関する情報である。Dirichlet 級数や関数等式の情報, 不変量といった基本的事項から始まり, 零点の分布などの情報も得ることが出来る。このように, 互いに付随する整数論的構造物, とくに「保型性」(modularity) に関する情報に手軽にアクセス出来ることも, LMFDB の長所である。

3 LMFDB を引用するには

詳細は “How to cite LMFDB” のページ <http://www.lmfdb.org/citation> を参照されたい。BibTeX の形式も指定されているので, [3] という形で引用すればよい (参考文献の箇所を参照のこと)。但し幾つかのデータベースを単独で用いた場合は, 引用の文面を変更することも可能である。例えば [4] と引用すればよい。

4 LMFDB に貢献するには

筆者は, AC2011 で紹介した話題 [7] に関するデータベースを LMFDB に提供している. 具体的には, 次数の低い代数体上至る所良い還元を持つような楕円曲線の存在・非存在を網羅したデータベースを作成している. この作業に関しては John Cremona の他, Haluk Sengun (University of Sheffield) から協力をして頂き, GitHub で指定されているフォーマットへの変換を行った. なお要約した表については, 筆者のウェブページにある

“Elliptic Curves with Everywhere Good Reduction over Number Fields”

<http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECtable.html>

から見る事が出来る.

先述の通り, 基本的には誰でも LMFDB へ貢献することが可能である. とくにデータベースを作成したが公開する機会が得られていないもの, また部分的であっても非常に計算コストが大きなデータベースなどをお持ちの場合は, 是非 LMFDB への提供をお願いしたい.

より詳しい情報を得たい場合, 今のところ LMFDB について詳細に解説した和文の解説は(恐らく)存在しないが, 英文であれば PI の John Cremona による解説論文 [2] が公開されている. 興味を持った方は, ぜひこちらを御一読頂きたい. また定期的に LMFDB の開発に関するワークショップがヨーロッパを中心として開催されている.

参考文献

- [1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation, **24** (1997), 235-265.
- [2] J. Cremona, The L -functions and modular forms database project, ArXiv 1511.04289 (2015), 14pp.
- [3] The LMFDB Collaboration, *The L -functions and Modular Forms Database*, <http://www.lmfdb.org>, 2013, [Online; accessed 26 January 2016].
- [4] The LMFDB Collaboration, *The L -functions and Modular Forms Database*, Home page of the L -function $L(s,E)$ for the Elliptic Curve Isogeny Class 234446.a, <http://www.lmfdb.org/L/EllipticCurve/Q/234446.a/>, 2013, [Online; accessed 26 January 2016].
- [5] *Pari/GP* (Version 2.7.5), 2015, <http://pari.math.u-bordeaux.fr/>.
- [6] *Sage Mathematics Software* (Version 6.10), 2015, <http://www.sagemath.org>.
- [7] 横山俊一, 至る所良い還元を持つ楕円曲線について: 計算機的手法とその最近の進展, 第9回「代数学と計算」(AC2011)報告集(2012), 21-31.

Shun'ichi Yokoyama

Faculty of Mathematics, Kyushu University

744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

E-mail Address: s-yokoyama@math.kyushu-u.ac.jp

High-speed computation of the dimensions of coherent cohomology by computer algebra systems

Momonari Kudo*

April 26, 2016

Abstract

A number of invariants to classify algebraic varieties are computed from the dimensions of the cohomology groups of coherent sheaves. J.-P. Serre theoretically proved a possibility to compute the dimensions of the cohomology groups $H^q(\mathbb{P}^r, \mathcal{F})$ for a projective space \mathbb{P}^r over a field K and a coherent sheaf \mathcal{F} . After that, some algorithms for the computation have been proposed and implemented over computer algebra systems. Computer algebra system Magma has a function to compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$, which adopts an algorithm proposed by W. Decker and D. Eisenbud. Their algorithm is based on the free resolution computation over exterior algebra, the Beilinson–Gelfand–Gelfand correspondence and Tate resolutions. On the other hand, M. Maruyama showed an alternative method to compute the dimensions in his textbook. Different from Decker–Eisenbud’s algorithm, his method can compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ by directly computing a locally free resolution of \mathcal{F} . However, Maruyama’s method has not been described in an algorithmic format, and it has not been implemented yet. In this paper, we first write down his method as an explicit algorithm, and give some remarks for efficient implementations of the algorithm over mathematical softwares. We also give an analysis on the algorithm, whose complexity is estimated. Furthermore we implemented it over Magma, and compare our function with Magma’s one in order to investigate pros/cons between the two algorithms.

Key words— Computational algebraic geometry, Sheaf cohomology, Free resolution

1 Introduction

Throughout this paper, let K be a field and $S = K[X_0, \dots, X_r]$ the polynomial ring with $(r + 1)$ variables over K . The polynomial ring S can be represented as the graded ring $S = \bigoplus_{d \geq 0} S_d$, by taking S_d for each $d \geq 0$ to be the set of all linear combinations of monomials with total degree d in X_0, \dots, X_r . Let $\mathbb{P}^r = \text{Proj}(S)$ denote the projective r -space, and $\mathcal{O}_{\mathbb{P}^r}$ its structure sheaf. For a coherent $\mathcal{O}_{\mathbb{P}^r}$ -module \mathcal{F} and $q \in \mathbb{Z}$, we denote by $H^q(\mathbb{P}^r, \mathcal{F})$ (or $H^q(\mathcal{F})$) its q -th cohomology group. Computing the dimension $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ allows us to compute a number of invariants such as Hilbert functions, Euler characteristics, and arithmetic genera of algebraic varieties (see [6] for details). Thus the computation of $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ is one of the most important topics in computational algebraic geometry.

Since Serre [10] theoretically showed a possibility to compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$, some algorithms to compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ have been proposed by Eisenbud [4], Smith [11] and Decker–Eisenbud [3].

*Graduate School of Mathematics, Kyushu University. E-mail: m-kudo@math.kyushu-u.ac.jp

In particular, the algorithm proposed by Decker-Eisenbud is based on the free resolution computation over exterior algebra, the Beilinson-Gelfand-Gelfand correspondence and Tate resolutions, and it has been implemented over computer algebra systems such as Macaulay2 [5] and Magma [1]. On the other hand, M. Maruyama showed an alternative method to compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ in his textbook [9] (unfortunately, it is written in Japanese). Different from Decker-Eisenbud's algorithm, Maruyama's method can compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$ by directly computing a locally free resolution of \mathcal{F} and the Čech cohomology via Gröbner bases for free modules and linear algebra.

In this paper, we focus on Maruyama's method to compute the dimensions of the cohomology groups $H^q(\mathbb{P}^r, \mathcal{F})$. His method is not described in an algorithmic format, and it has not been implemented yet over computer algebra systems. Then our main contributions are as follows:

Contributions: We write down Maruyama's method as an explicit algorithm (Algorithm 2.2.2 in Section 2.2), and then we analyze it. More concretely, we analyze the complexity in order to prove that the algorithm terminates in polynomial time under some assumptions, and also show a pruning technique for efficiency. We implemented the algorithm over Magma as a new function “newCohomologyDimension” (cf. Magma already has the function “CohomologyDimension”, in which Decker-Eisenbud's algorithm is adopted)¹. We compare the two functions by experiments, and investigate pros/cons between the two algorithms.

Organization of this paper: In Section 2, we first introduce Maruyama's method to compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F})$, and then we write down an explicit algorithm of the method. In Section 3, we give some remarks for exact and efficient implementations of the algorithm. In Section 4, we first analyze its complexity under some assumptions. Then we show experimental results obtained from our implementation of the algorithm over Magma, which shows practical behavior in performance of our function.

Notation

- $\text{rk}F$: the rank of a linear map $F : V \rightarrow W$,
- $\Lambda(f)$: the support of $f \in K[X_0, \dots, X_r] \setminus \{0\}$,
- $M(m)$: the m -th twisted graded R -module $\bigoplus_{t \in \mathbb{Z}} M_{m+t}$ of a graded R -module $M = \bigoplus_{t \in \mathbb{Z}} M_t$, where each M_t is the homogeneous part with degree t of M ,
- M^h : the set of homogeneous elements for a graded module M ,
- M^\sim : the sheaf associated with an S -module M ,
- $\mathcal{F}(m)$: the m -th Serre twist of a sheaf \mathcal{F} of $\mathcal{O}_{\mathbb{P}^r}$ -modules,
- $R_{(f)}$: the localization of a ring R by an element $f \in R$,
- R_d : the homogeneous part with degree d of a graded ring R ,
- $\binom{m}{n}$: the binomial coefficient of two non-negative integers m and n with $m \geq n$.

¹The source code of our implementation and the computation results for this paper are available at <http://www2.math.kyushu-u.ac.jp/~m-kudo/> (our source code is in the file `newCohomologyDimension.txt`).

2 Maruyama's method and its algorithm

In this section, we introduce Maruyama's method given in [9, Chapter 6] to compute the dimensions of the cohomology groups of coherent sheaves on a projective space.

2.1 Bases of $H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$

In this subsection, we give a brief review on the bases of $H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$.

Theorem 2.1.1 ([6], Theorem 5.1) We have the following:

- (1) For all $m \in \mathbb{Z}$, there exist isomorphisms of K -vector spaces as follows:

$$H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \cong \begin{cases} S_m & \text{for } m \geq 0, \\ 0 & \text{for } m < 0. \end{cases}$$

Hence for every $m \geq 0$, the set

$$\{X_0^{\ell_0} \cdots X_r^{\ell_r} ; \ell_i \geq 0 \text{ for } 0 \leq i \leq r, \text{ and } \ell_0 + \cdots + \ell_r = m\}$$

of monomials of total degree m is a basis of $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$.

- (2) $H^q(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) = 0$ for $0 < q < r$ and arbitrary m .

- (3) Let $S(m)$ denote the m -th twisted graded ring of S . Denote by $\left(S(m)_{(X_0 \cdots X_r)}\right)_0$ the homogeneous part with degree 0 of the localization $S(m)_{(X_0 \cdots X_r)}$ by $X_0 \cdots X_r$. Note that $\left(S(m)_{(X_0 \cdots X_r)}\right)_0$ is the K -vector space spanned by the set

$$\{aX_0^{\ell_0} \cdots X_r^{\ell_r} ; a \in K, \ell_i \in \mathbb{Z} \text{ for } 0 \leq i \leq r, \text{ and } \ell_0 + \cdots + \ell_r = m\}.$$

Let W be the K -vector subspace of $\left(S(m)_{(X_0 \cdots X_r)}\right)_0$ spanned by

$$\{X_0^{\ell_0} \cdots X_r^{\ell_r} ; \ell_i \geq 0 \text{ for some } i, \text{ and } \ell_0 + \cdots + \ell_r = m\}.$$

Then we have the following isomorphism of K -vector spaces:

$$H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \cong \left(S(m)_{(X_0 \cdots X_r)}\right)_0 / W. \quad (2.1.1)$$

Hence for every $m < 0$, the set

$$\{X_0^{\ell_0} \cdots X_r^{\ell_r} ; \ell_i < 0 \text{ for } 0 \leq i \leq r, \text{ and } \ell_0 + \cdots + \ell_r = m\}$$

gives rise to a basis of $H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m))$ via the above isomorphism (2.1.1).

Corollary 2.1.2 ([6], Theorem 5.1) For all $m \in \mathbb{Z}$, we have the following:

$$\begin{aligned} \dim_K H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) &= \begin{cases} \binom{m+r}{r} & \text{for } m \geq 0, \\ 0 & \text{for } m < 0. \end{cases} \\ \dim_K H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) &= \begin{cases} \binom{-m-1}{r} & \text{for } m \leq -r-1, \\ 0 & \text{for } m > -r-1. \end{cases} \end{aligned}$$

2.2 Interpretation on Maruyama's method and explicit algorithm

In this subsection, we give explicit formulae (Theorem 2.2.1) on the dimensions of the cohomology groups of coherent sheaves on \mathbb{P}^r . As we will give an algorithm (Algorithm 2.2.2), with the formulae, the dimensions can be computed algorithmically. To simplify the notations, we denote $H^q(\mathbb{P}^r, \mathcal{H})$ by $H^q(\mathcal{H})$ for a coherent sheaf \mathcal{H} on \mathbb{P}^r . As only a sketch of a proof of the formulae is given in [9, Chapter 6], we here give a complete proof. A coherent sheaf \mathcal{F} on \mathbb{P}^r has the following locally free resolution:

$$0 \rightarrow \bigoplus_{j=1}^{t_{r+1}} \mathcal{O}_{\mathbb{P}^r} \left(m_j^{(r+1)} \right) \xrightarrow{f_{r+1}} \dots \xrightarrow{f_1} \bigoplus_{j=1}^{t_0} \mathcal{O}_{\mathbb{P}^r} \left(m_j^{(0)} \right) \xrightarrow{f_0} \mathcal{F} \rightarrow 0 \quad (2.2.1)$$

for some t_i and $m_j^{(i)}$ with $0 \leq i \leq r + 1$ and $1 \leq j \leq t_i$. For an index i with $t_i = 0$, we identify $\bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbb{P}^r} \left(m_j^{(i)} \right) = 0$. Put

$$\mathcal{G}_i := \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbb{P}^r} \left(m_j^{(i)} \right), \quad \mathcal{K}_i := \text{Ker}(f_i), \quad \mathcal{K}_{-1} := \mathcal{F}. \quad (2.2.2)$$

Then we have the following theorem (for the proof, see also [9, Chapter 6] and [7, Theorem 4.2.1]).

Theorem 2.2.1 ([9], Chapter 6) Let \mathcal{F} be a coherent sheaf on \mathbb{P}^r with a resolution of the form (2.2.1). Put \mathcal{G}_i and \mathcal{K}_i as in (2.2.2). Then we have the following formulae:

- (1) $\dim_K H^0(\mathcal{F}) = \dim_K H^0(\mathcal{G}_0) - \dim_K H^r(\mathcal{G}_{r+1}) + \dim_K H^r(\mathcal{G}_r) - \text{rk} H^0(f_1) - \text{rk} H^r(f_r)$.
- (2) $\dim_K H^q(\mathcal{F}) = \dim_K H^r(\mathcal{G}_{r-q}) - \text{rk} H^r(f_{r-q}) - \text{rk} H^r(f_{r-q+1})$ for $r \geq 2$ and $1 \leq q \leq r - 1$.
- (3) $\dim_K H^r(\mathcal{F}) = \dim_K H^r(\mathcal{G}_0) - \text{rk} H^r(f_1)$.

Here $H^r(f_i)$ denotes the morphism $H^r(\mathcal{G}_i) \rightarrow H^r(\mathcal{G}_{i-1})$ induced by f_i for each $0 \leq i \leq r + 1$.

Proof. We first show (2). Suppose $r \geq 2$. It suffice to show

$$H^q(\mathcal{F}) \cong \text{Ker}(H^r(f_{r-q})) / \text{Im}(H^r(f_{r-q+1})) \text{ for } 1 \leq q \leq r - 1. \quad (2.2.3)$$

For each $0 \leq i \leq r + 1$, the following sequence of coherent sheaves is exact:

$$0 \rightarrow \mathcal{K}_i \rightarrow \mathcal{G}_i \rightarrow \mathcal{K}_{i-1} \rightarrow 0. \quad (E_i)$$

Each (E_i) induces a long exact sequence of cohomology groups

$$\begin{array}{ccccccc} 0 & \rightarrow & H^0(\mathcal{K}_i) & \rightarrow & H^0(\mathcal{G}_i) & \rightarrow & H^0(\mathcal{K}_{i-1}) \\ & & \rightarrow & & H^1(\mathcal{K}_i) & \rightarrow & H^1(\mathcal{G}_i) \rightarrow H^1(\mathcal{K}_{i-1}) \\ & & \rightarrow & & \dots & & \\ & & \rightarrow & & H^{r-1}(\mathcal{K}_i) & \rightarrow & H^{r-1}(\mathcal{G}_i) \rightarrow H^{r-1}(\mathcal{K}_{i-1}) \\ & & \rightarrow & & H^r(\mathcal{K}_i) & \rightarrow & H^r(\mathcal{G}_i) \rightarrow H^r(\mathcal{K}_{i-1}) \rightarrow 0. \end{array} \quad (L_i)$$

Note here that $H^q(\mathcal{G}_i) = 0$ for $1 \leq q \leq r - 1$ since

$$H^q(\mathcal{G}_i) = H^q \left(\bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbb{P}^r} \left(m_j^{(i)} \right) \right) \cong \bigoplus_{j=1}^{t_i} H^q \left(\mathcal{O}_{\mathbb{P}^r} \left(m_j^{(i)} \right) \right)$$

and $H^q\left(\mathcal{O}_{\mathbb{P}^r}\left(m_j^{(i)}\right)\right) = 0$ for all indexes i, j and $1 \leq q \leq r-1$. It follows from (L_i) 's that

$$H^q(\mathcal{F}) \cong H^{q+1}(\mathcal{K}_0) \cong \dots \cong H^{r-1}(\mathcal{K}_{r-q-2}). \quad (2.2.4)$$

The sequence

$$0 \rightarrow H^q(\mathcal{F}) \cong H^{r-1}(\mathcal{K}_{r-q-2}) \rightarrow H^r(\mathcal{K}_{r-q-1}) \rightarrow H^r(\mathcal{G}_{r-q-1})$$

is exact, and thus we have $H^q(\mathcal{F}) \cong \text{Ker}(\sigma_q)$, where σ_q denotes $H^r(\mathcal{K}_{r-q-1}) \rightarrow H^r(\mathcal{G}_{r-q-1})$ in the above exact sequence. Note that the following diagram of morphisms of coherent sheaves commutes and its horizontal sequence is exact:

$$\begin{array}{ccccccc} \mathcal{G}_{r-q+1} & \xrightarrow{f_{r-q+1}} & \mathcal{G}_{r-q} & \longrightarrow & \mathcal{K}_{r-q-1} & \longrightarrow & 0 \\ & & & \searrow f_{r-q} & \downarrow & & \\ & & & & \mathcal{G}_{r-q-1} & & \end{array}$$

Since the functor $H^r(\cdot)$ is right exact, the horizontal sequence of the following commutative diagram is also exact:

$$\begin{array}{ccccccc} H^r(\mathcal{G}_{r-q+1}) & \xrightarrow{H^r(f_{r-q+1})} & H^r(\mathcal{G}_{r-q}) & \longrightarrow & H^r(\mathcal{K}_{r-q-1}) & \longrightarrow & 0 \\ & & & \searrow H^r(f_{r-q}) & \downarrow \sigma_q & & \\ & & & & H^r(\mathcal{G}_{r-q-1}) & & \end{array}$$

Hence we have $H^q(\mathcal{F}) \cong \text{Ker}(\sigma_q) \cong \text{Ker}(H^r(f_{r-q})) / \text{Im}(H^r(f_{r-q+1}))$ as K -vector spaces.

We next show (3). It suffices to show that $H^r(\mathcal{F})$ is isomorphic to $\text{Coker}(H^r(f_1))$. The sequence of coherent $\mathcal{O}_{\mathbb{P}^r}$ -modules $\mathcal{G}_1 \rightarrow \mathcal{G}_0 \rightarrow \mathcal{F} \rightarrow 0$ is exact, and the functor $H^r(\cdot)$ is right exact. Hence the sequence

$$H^r(\mathcal{G}_1) \xrightarrow{H^r(f_1)} H^r(\mathcal{G}_0) \xrightarrow{H^r(f_0)} H^r(\mathcal{F}) \longrightarrow 0$$

is also exact, and thus $H^r(\mathcal{F}) \cong \text{Coker}(H^r(f_1))$.

We finally show (1). Note that $\mathcal{K}_r \cong \mathcal{G}_{r+1}$ because of the exactness of (2.2.1). In a similar way to show (2), we have $H^1(\mathcal{K}_1) \cong H^{r-1}(\mathcal{K}_{r-1})$ for $r \geq 2$ and

$$\dim_K H^1(\mathcal{K}_1) = \begin{cases} \dim_K H^r(\mathcal{G}_{r+1}) & (r=1), \\ \dim_K H^r(\mathcal{G}_{r+1}) - \text{rk} H^r(f_{r+1}) & (r \geq 2). \end{cases} \quad (2.2.5)$$

In the long exact sequence (L_0) of cohomology groups, specifically the following sequence is also exact:

$$H^0(\mathcal{G}_0) \rightarrow H^0(\mathcal{F}) \rightarrow H^1(\mathcal{K}_0) \rightarrow H^1(\mathcal{G}_0) \rightarrow H^1(\mathcal{F}). \quad (L'_0)$$

We denote by κ_0 the linear map $H^1(\mathcal{K}_0) \rightarrow H^1(\mathcal{G}_0)$. It follows from the exactness of (L'_0) that

$$\dim_K H^0(\mathcal{F}) = \dim_K \text{Im}(H^0(f_0)) + \dim_K \text{Ker}(\kappa_0). \quad (2.2.6)$$

The K linear map $H^0(f_0) : H^0(\mathcal{G}_0) \rightarrow H^0(\mathcal{F})$ induces the isomorphism

$$\text{Im}(H^0(f_0)) \cong H^0(\mathcal{G}_0) / \text{Ker}(H^0(f_0)).$$

Since $\text{Ker}(H^0(f_0))$ is isomorphic to $H^0(\mathcal{K}_0)$, we have

$$\dim_K \text{Im}(H^0(f_0)) = \dim_K H^0(\mathcal{G}_0) - \dim_K H^0(\mathcal{K}_0). \quad (2.2.7)$$

In the long exact sequence (L_1) of cohomology groups, specifically

$$H^0(\mathcal{G}_1) \rightarrow H^0(\mathcal{K}_0) \rightarrow H^1(\mathcal{K}_1) \rightarrow H^1(\mathcal{G}_1) \rightarrow H^1(\mathcal{K}_0) \quad (L'_1)$$

is exact. We denote by τ and κ_1 the K -linear maps $H^0(\mathcal{G}_1) \rightarrow H^0(\mathcal{K}_0)$ and $H^1(\mathcal{K}_1) \rightarrow H^1(\mathcal{G}_1)$, respectively. The exactness of (L'_1) implies

$$\dim_K H^0(\mathcal{K}_0) = \dim_K \text{Im}(\tau) + \dim_K \text{Ker}(\kappa_1). \quad (2.2.8)$$

Let us determine $\dim_K \text{Im}(\tau)$. Since $H^0(\mathcal{K}_0) \rightarrow H^0(\mathcal{G}_0)$ is injective in the commutative diagram

$$\begin{array}{ccc} H^0(\mathcal{G}_1) & \xrightarrow{H^0(f_1)} & H^0(\mathcal{G}_0) \\ & \searrow \tau & \nearrow \\ & H^0(\mathcal{K}_0) & \end{array}$$

we have $\text{Ker}(H^0(f_1)) = \text{Ker}(\tau)$. Thus,

$$\text{Im}(\tau) \cong H^0(\mathcal{G}_1)/\text{Ker}(\tau) = H^0(\mathcal{G}_1)/\text{Ker}(H^0(f_1)) \cong \text{Im}(H^0(f_1))$$

and hence

$$\dim_K \text{Im}(\tau) = \dim_K \text{Im}(H^0(f_1)) = \text{rk} H^0(f_1). \quad (2.2.9)$$

Now we show the equality (1) by (2.2.5)–(2.2.9) in each case of $r = 1$ and $r \geq 2$.

Case of $r = 1$: In this case, $H^1(\mathcal{G}_0) \rightarrow H^1(\mathcal{K}_{-1})$ and $H^1(\mathcal{G}_1) \rightarrow H^1(\mathcal{K}_0)$ are surjective in the exact sequences (L'_0) and (L'_1) , respectively. Thus we have

$$\dim_K \text{Ker}(\kappa_0) = \dim_K H^1(\mathcal{K}_0) - \dim_K H^1(\mathcal{G}_0) + \dim_K H^1(\mathcal{K}_{-1}), \quad (2.2.10)$$

$$\dim_K \text{Ker}(\kappa_1) = \dim_K H^1(\mathcal{K}_1) - \dim_K H^1(\mathcal{G}_1) + \dim_K H^1(\mathcal{K}_0), \quad (2.2.11)$$

where we recall $\mathcal{K}_{-1} = \mathcal{F}$. By the equations (2.2.5)–(2.2.11) and (3), the equation (1) holds.

Case of $r \geq 2$: In this case, since $H^1(\mathcal{G}_i) = 0$, it follows from (L'_i) that $\text{Ker}(\kappa_i) = H^1(\mathcal{K}_i)$ for $i = 0$ and 1. In a similar way to (2.2.4), we have $H^1(\mathcal{K}_0) \cong H^{r-1}(\mathcal{K}_{r-2})$, and a similar strategy to the proof of (2) shows

$$\dim_K H^1(\mathcal{K}_0) = \dim_K H^r(\mathcal{G}_r) - \text{rk} H^r(f_r) - \text{rk} H^r(f_{r+1}). \quad (2.2.12)$$

Thus (1) follows from (2.2.5)–(2.2.9) and (2.2.12). \square

Maruyama's method Let \mathcal{F} be a coherent $\mathcal{O}_{\mathbb{P}^r}$ -module. In the following, we write down Maruyama's method to compute $\dim_K H^q(\mathcal{F}(n))$ as an explicit algorithm, where $\mathcal{F}(n)$ denotes the n -th Serre twist of the coherent sheaf \mathcal{F} . It is known that \mathcal{F} (resp. $\mathcal{F}(n)$) is isomorphic to M^\sim (resp. $M(n)^\sim$) for some finitely generated graded S -module M of the form

$$M \cong \left(\bigoplus_{j=1}^t S(-d_j) \right) / \langle \mathbf{u}_1, \dots, \mathbf{u}_{t_0} \rangle_S, \quad (2.2.13)$$

where $\mathbf{u}_j \in \left(\bigoplus_{j=1}^t S(-d_j) \right)^h$ for $1 \leq j \leq t_0$. We take integers $t > 0$, q , d_j for $1 \leq j \leq t$ and finite homogeneous elements $\mathbf{u}_1, \dots, \mathbf{u}_{t_0}$ in $\bigoplus_{j=1}^t S(-d_j)$ as inputs.

Algorithm 2.2.2 Let $\mathbf{u}_1, \dots, \mathbf{u}_{t_0}$ be homogeneous elements in the S -module $\bigoplus_{j=1}^t S(-d_j)$, and M the finitely generated graded S -module given in (2.2.13) with $\mathcal{F} := M^\sim$. For given $t > 0$, q , d_j for $1 \leq j \leq t$ and $\mathbf{u}_1, \dots, \mathbf{u}_{t_0}$, one can compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F}(n))$ as follows.

Step 1. Compute a (graded) free resolution of M (for the free resolution computation, see [2, Chapter 6]):

$$0 \rightarrow \bigoplus_{j=1}^{t_{r+1}} S(-d_j^{(r+1)}) \xrightarrow{\varphi_{r+1}} \dots \xrightarrow{\varphi_1} \bigoplus_{j=1}^{t_0} S(-d_j^{(0)}) \xrightarrow{\varphi_0} M \rightarrow 0. \quad (2.2.14)$$

The above exact sequence (2.2.14) induces an exact sequence of coherent $\mathcal{O}_{\mathbb{P}^r}$ -modules, that is of the form

$$0 \rightarrow \bigoplus_{j=1}^{t_{r+1}} \mathcal{O}_{\mathbb{P}^r}(n - d_j^{(r+1)}) \xrightarrow{\varphi_{r+1}^{(n)^\sim}} \dots \xrightarrow{\varphi_1^{(n)^\sim}} \bigoplus_{j=1}^{t_0} \mathcal{O}_{\mathbb{P}^r}(n - d_j^{(0)}) \xrightarrow{\varphi_0^{(n)^\sim}} \mathcal{F}(n) \rightarrow 0, \quad (2.2.15)$$

where each $\varphi_i(n)$ denotes the n -th twisted morphism of φ_i . We here set

$$\mathcal{G}_i := \bigoplus_{j=1}^{t_i} \mathcal{O}_{\mathbb{P}^r}(n - d_j^{(i)}) \quad \text{and} \quad f_i := \varphi_i(n)^\sim \quad \text{for} \quad 0 \leq i \leq r+1. \quad (2.2.16)$$

Step 2. If $q < r$ (resp. $q = r$), generate bases of $H^r(\mathcal{G}_i)$ for $r - q - 1 \leq i \leq r - q + 1$ (resp. $r - q \leq i \leq r - q + 1$) by Theorem 2.1.1 (3). If $q = 0$, additionally generate bases of $H^0(\mathcal{G}_0)$ and $H^0(\mathcal{G}_1)$ by Theorem 2.1.1 (1).

Step 3. If $1 \leq q \leq r - 1$ (resp. $q = 0$), compute the representation matrices of $H^r(f_{r-q+1})$ and $H^r(f_{r-q})$ (resp. $H^0(f_1)$ and $H^r(f_{r-q})$) via the bases obtained in Step 2 and compute their ranks. If $q = r$, compute the representation matrix of $H^r(f_{r-q+1})$. Finally output $\dim_K H^q(\mathcal{F}(n))$ by the formulae given in Theorem 2.2.1.

3 Remarks for exact and efficient implementations

In this section, we first concretely describe Step 3 in Algorithm 2.2.2. We also give a technique to prune unnecessary operations in the implementations, by which one's implementation is expected to become more efficient.

3.1 Detail of sub-procedures

Step 3 has the computation of $\text{rk}H^r(f_i)$ or $\text{rk}H^0(f_i)$ for some i . In the computation, explicit bases of $H^r(\mathcal{G}_i)$ or $H^0(\mathcal{G}_i)$ and explicit representation matrices of the morphisms are computed. We here give such explicit representations, by which the algorithm shall be implemented more exactly.

Computing $H^r(f_i)$: Let $t > 0$ and $t' > 0$, and let m_ℓ and m'_k be integers for $1 \leq \ell \leq t$ and $1 \leq k \leq t'$. Let $A = (g_{k,\ell})_{k,\ell}$ be a $(t' \times t)$ matrix such that each (k, ℓ) -entry $g_{k,\ell}$ is a homogeneous polynomial in S with degree $(m'_k - m_\ell)$. Then A defines the following graded homomorphism φ of degree zero:

$$\varphi : \bigoplus_{j=1}^t S(m_j) \longrightarrow \bigoplus_{j=1}^{t'} S(m'_j) ; \mathbf{u} \mapsto \mathbf{u} \cdot A. \quad (3.1.1)$$

Clearly φ induces a morphism φ^\sim of coherent $\mathcal{O}_{\mathbb{P}^r}$ -modules

$$\varphi^\sim : \bigoplus_{j=1}^t \mathcal{O}_{\mathbb{P}^r}(m_j) \longrightarrow \bigoplus_{j=1}^{t'} \mathcal{O}_{\mathbb{P}^r}(m'_j) \quad (3.1.2)$$

and the following K -linear map of the cohomology groups:

$$H^r(f) : H^r(\mathbb{P}^r, \mathcal{G}) \longrightarrow H^r(\mathbb{P}^r, \mathcal{G}') ; w \mapsto w \cdot A, \quad (3.1.3)$$

where we set

$$f := \varphi^\sim, \quad \mathcal{G} := \bigoplus_{j=1}^t \mathcal{O}_{\mathbb{P}^r}(m_j) \text{ and } \mathcal{G}' := \bigoplus_{j=1}^{t'} \mathcal{O}_{\mathbb{P}^r}(m'_j) \quad (3.1.4)$$

For an element $v \in H^r(\mathcal{O}_{\mathbb{P}^r}(m_i))$, denote by $\eta_i(v)$ an element $(0, \dots, 0, v, \dots, 0)$ in $H^r(\mathcal{G})$. Namely, define the map η_i as the following embedding:

$$\eta_i : H^r(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m_i)) \hookrightarrow H^r(\mathbb{P}^r, \mathcal{G}) ; v \mapsto (0, \dots, 0, v, 0, \dots, 0) \quad (3.1.5)$$

We here describe how to compute $\text{rk}H^r(f)$.

Step 3-1. Note first that $H^r(\mathcal{G})$ and $H^r(\mathcal{G}')$ are represented as follows:

$$H^r(\mathcal{G}) = \bigoplus_{j=1}^t H^r(\mathcal{O}_{\mathbb{P}^r}(m_j)) \text{ and } H^r(\mathcal{G}') = \bigoplus_{j=1}^{t'} H^r(\mathcal{O}_{\mathbb{P}^r}(m'_j)). \quad (3.1.6)$$

Thus the set

$$\mathcal{V} := \left\{ \eta_j \left(X_0^{\ell_0} \cdots X_r^{\ell_r} \right) ; 1 \leq j \leq t, \ell_k < 0 \text{ for } 0 \leq k \leq r, \text{ and } \ell_0 + \cdots + \ell_r = m_j \right\} \quad (3.1.7)$$

gives rise to a basis of the K -vector space $H^r(\mathcal{G})$. (Similarly, a basis \mathcal{V}' of $H^r(\mathcal{G}')$ is constructed.)

Step 3-2. Compute the image of \mathcal{V} by $H^r(f)$. Each $v \in \mathcal{V}$ is of the form $v = \eta_j \left(X_0^{\ell_0} \cdots X_r^{\ell_r} \right)$ for some $1 \leq j \leq t$ and $(\ell_0, \dots, \ell_r) \in \mathbb{Z}_{<0}^{r+1}$ with $\ell_0 + \cdots + \ell_r = m_j$. Then we have

$$\begin{aligned} (H^r(f))(v) &= \sum_{k=1}^{t'} g_{j,k} \eta_k(X_0^{\ell_0} \cdots X_r^{\ell_r}) \\ &= \sum_{k=1}^{t'} \sum_{(k_0, \dots, k_r) \in \Lambda(g_{j,k})} c_{k_0, \dots, k_r}(g_{j,k}) X_0^{k_0} \cdots X_r^{k_r} \eta_k(X_0^{\ell_0} \cdots X_r^{\ell_r}) \\ &= \sum_{k=1}^{t'} \sum_{(k_0, \dots, k_r) \in \Lambda(g_{j,k})} c_{k_0, \dots, k_r}(g_{j,k}) \eta_k(X_0^{\ell_0+k_0} \cdots X_r^{\ell_r+k_r}), \end{aligned} \quad (3.1.8)$$

where $c_{k_0, \dots, k_r}(g)$ denotes the coefficient of $X_0^{k_0} \cdots X_r^{k_r}$ in g for each polynomial $g \in S$. Note from Theorem 2.1.1 (3) that $\eta_k(X_0^{\ell_0+k_0} \cdots X_r^{\ell_r+k_r})$ is regarded as $\mathbf{0}$ if $\ell_i + k_i \geq 0$ for some i . Comparing the representation (3.1.8) with the basis \mathcal{V}' of $H^r(\mathcal{G}')$, the representation matrix of $H^r(f)$ is computed.

Step 3-3. The rank of $H^r(f)$ is computed by techniques in linear algebra, e.g., the Gaussian elimination, the LU decomposition.

Computing $H^0(f_i)$: This computation can be done in a similar way to the case of $\text{rk} H^r(f_i)$, which we described in the previous paragraph.

3.2 Pruning unnecessary operations

For efficient implementations, note that we can prune unnecessary operations in the computation of $H^r(f_i)$. We here give a brief description on the pruning, which we adopt in our implementation. In Step 3-2, we have

$$(H^r(f))(v) = \sum_{k=1}^{t'} \sum_{(k_0, \dots, k_r) \in \Lambda(g_{j,k})'} c_{k_0, \dots, k_r}(g_{j,k}) \eta_k(X_0^{\ell_0+k_0} \cdots X_r^{\ell_r+k_r}), \quad (3.2.1)$$

where we set

$$\Lambda(g_{j,k})' := \{(k_0, \dots, k_r) \in \Lambda(g_{j,k}) : k_i + \ell_i < 0 \text{ for all } 0 \leq i \leq r\}. \quad (3.2.2)$$

Considering (3.2.1) and (3.2.2), for each basis element $v = \eta_j \left(X_0^{\ell_0} \cdots X_r^{\ell_r} \right) \in H^r(\mathcal{G})$, we first determine the coefficients $c_{k_0, \dots, k_r}(g_{j,k})$ such that for all $0 \leq i \leq r$, $k_i + \ell_i < 0$ and write $(H^r(f))(v)$ as the form (3.2.1). Then we obtain the representation matrix of $H^r(f)$. By this procedure, we can prune at most $t' \cdot \alpha \cdot \dim_K H^r(\mathcal{G})$ operations, where we set $\alpha := \max_{j,k} \#(\Lambda(g_{j,k})')$. Moreover, the representation matrix obtained as above can be a sparse matrix, which can make computing $\text{rk} H^r(f)$ more efficient.

4 Analysis on the proposed algorithm

In this section, we analyze Algorithm 2.2.2. In our analysis, we first determine the complexity of the algorithm under some assumptions. We also implemented the algorithm over Magma, and examine

the efficiency of the algorithm and our implementation by experiments. Magma already has a function `CohomologyDimension` in which Decker-Eisenbud's algorithm [3] is adopted. Comparing our function with Magma's one, we investigate pros/cons between the two algorithms.

4.1 Complexity

Let M be a finitely generated graded S -module, where we recall $S := K[X_0, \dots, X_r]$. Maruyama's method can be divided to the following two steps: (A) computing a (graded) free resolution of the form (2.2.14), (B) computing the bases of $H^q(\mathcal{G}_i)$ and the morphisms $H^q(f_i)$ for $q = 0$ or $q = r$ and some i , where \mathcal{G}_i and f_i are given in (2.2.16). Note here that the complexity of the free resolution computation has been estimated only for the worst case. Mathematical objects such as the cohomology groups are determined by mathematical invariants for the inputs. In this case, the output $\dim_K H^q(\mathbb{P}^r, \mathcal{F}(n))$ is determined by $n, t_i, d_j^{(i)}$ and $g_{k,\ell}^{(i)}$, which are invariants with respect to the (minimal) free resolution of M . In addition,

$$D := \max\{\dim_K H^q(\mathbb{P}^r, \mathcal{G}_i) ; 0 \leq i \leq r+1 \text{ and } q = 0, r\} \quad (4.1.1)$$

is determined by $n, t_i, d_j^{(i)}$, and thus it is also an invariant with respect to the (minimal) free resolution of M . From this, we estimate the complexity with respect to the parameters D and

$$\alpha := \max_{1 \leq i \leq r+1} \left\{ \# \left(\Lambda \left(g_{k,\ell}^{(i)} \right) \right) ; 1 \leq k \leq t_i \text{ and } 1 \leq \ell \leq t_{i-1} \right\}. \quad (4.1.2)$$

In other words, we determine the complexity of the computation (B).

Remark 4.1.1 In our analysis, we fix r and do not count the computation of the bases of $H^q(\mathcal{G}_i)$ in Algorithm 2.2.2. This computation depends on the method to compute partition numbers.

Case of $q = 0$: In this case, we first compute the image of a basis of $H^r(\mathcal{G}_r)$ by $H^r(f_r)$. For a simplicity, suppose $H^r \left(\mathcal{O}_{\mathbb{P}^r} \left(n - d_j^{(i)} \right) \right) \neq 0$ for each pair of i and j . Since $\dim_K H^r(\mathcal{G}_r) = O(D)$ and since $A_r = \left(g_{k,\ell}^{(r)} \right)_{k,\ell}$ is a $(t_r \times t_{r-1})$ matrix over S , this computation runs in $O(\alpha t_{r-1} D) = O(\alpha D^2)$ arithmetic operations over K . We then construct the representation matrix of $H^r(f_r)$ and compute its rank. Clearly the computation of the representation matrix terminates in $O(\alpha D^2)$ arithmetic operations over K . Assume that $\text{rk} H^r(f_r)$ is computed by the Gaussian elimination. This computation can be done in $O(D^3)$ arithmetic operations over K . Thus the arithmetic complexity of computing $\text{rk} H^r(f_r)$ is estimated to be $O(\alpha D^2) + O(D^3)$.

We next compute $\text{rk} H^0(f_1)$. In a similar way to $\text{rk} H^r(f_r)$, the arithmetic complexity of computing $\text{rk} H^0(f_1)$ is estimated to be $O(\alpha D^2) + O(D^3)$.

Case of $q \neq 0$: In a similar way to the case of $q = 0$, it is estimated that this computation can be done in $O(\alpha D^2) + O(D^3)$ arithmetic operations over K .

To summarize, we estimate that the complexity of the computation of $\dim_K H^q(\mathbb{P}^r, \mathcal{F}(n))$ by Maruyama's method is $O(\alpha D^2) + O(D^3)$ when r is fixed,

4.2 Implementation and experiments

In this subsection, we show experimental results on our implementation of Algorithm 2.2.2. We implemented Algorithm 2.2.2 over Magma V2.20-10 [1]². Our aim in this subsection is to examine practicality in performance of our function, and we observe that our function performs more efficiently than the complexity estimated in Section 4.1. In the following, we first describe the form of the (minimal) free resolutions in our experiments.

Case 1 Choose three homogeneous polynomials f_1, f_2 and f_3 in $\mathbb{Q}[X_0, X_1, X_2, X_3]$ so that the minimal free resolution of $M := S/\langle f_1, f_2, f_3 \rangle$ forms

$$0 \rightarrow S(-9) \xrightarrow{\varphi_3} \bigoplus_{j=1}^3 S(-6) \xrightarrow{\varphi_2} \bigoplus_{j=1}^3 S(-3) \xrightarrow{\varphi_1} S \xrightarrow{\varphi_0} M \rightarrow 0.$$

Case 2 Choose four homogeneous polynomials f_1, f_2, f_3 and f_4 in $\mathbb{Q}[X_0, X_1, X_2, X_3, X_4, X_5]$ so that the minimal free resolution of $M := S/\langle f_1, f_2, f_3, f_4 \rangle$ forms

$$0 \rightarrow S(-8) \xrightarrow{\varphi_4} \bigoplus_{j=1}^4 S(-6) \xrightarrow{\varphi_3} \bigoplus_{j=1}^6 S(-4) \xrightarrow{\varphi_2} \bigoplus_{j=1}^4 S(-2) \xrightarrow{\varphi_1} S \xrightarrow{\varphi_0} M \rightarrow 0.$$

Table 1: The results of experiments to compare our implementation of Algorithm 2.2.2 with Magma's function. The parameters α and D are defined as in (4.1.1) and (4.1.2), respectively.

| Case | Parameters independent of resolutions | | Parameters dependent on resolutions | | Output and Timing of each function | | |
|------|---------------------------------------|-----|-------------------------------------|------|------------------------------------|--------------|------------------|
| | r | n | α | D | $\dim_K H^1(\mathcal{F}(n))$ | Our function | Magma's function |
| 1 | 3 | 0 | 3 | 56 | 0 | 0.047s | 0.109s |
| | | -3 | 3 | 165 | 0 | 0.110s | 0.110s |
| | | -7 | 3 | 455 | 0 | 0.937s | 0.109s |
| 2 | 5 | 0 | 3 | 21 | 17 | 0.031s | 3.172s |
| | | -3 | 3 | 252 | 64 | 0.156s | 5.907s |
| | | -7 | 3 | 3168 | 128 | 13.703s | 13.188s |

Performance: Table 1 implies that our function performs more efficiently than $O(\alpha D^2) + O(D^3)$ which is the complexity estimated in Section 4.1. For instance, in Case 1 of Table 1, when $D = 56$, our function terminates in 0.047 seconds. Note that $\alpha = 3$ is fixed in Case 1. Since $455/56 = 8.125$, we predict from the estimated complexity $O(\alpha D^2) + O(D^3)$ that it takes $0.047 \times (8.125)^3 \approx 25.210$ seconds for our function to terminate when $D = 455$. However, our function actually performs in 0.937 seconds, which implies that an actual complexity of Algorithm 2.2.2 is not as expensive as $O(\alpha D^2) + O(D^3)$. We observe the reason why our function performs more efficiently than $O(\alpha D^2) + O(D^3)$ as follows: In Case 1, we have

²We use a computer with 2.60GHz CPU (Intel Corei5) and 8GB memory. The OS is Windows 8.1 Pro, 64bit. The source code of our implementation and the computation results for this section are available at <http://www2.math.kyushu-u.ac.jp/~m-kudo/> (our source code is in the file `newCohomologyDimension.txt`).

$\dim_K H^r(\mathcal{G}_{r-q+1}) = 455$ and $\dim_K H^r(\mathcal{G}_{r-q}) = 660$, and the size of the representation matrix of $H^r(f_{r-q+1})$ is 660×455 . We here denote by B the representation matrix, and then B has $660 \times 455 = 300300$ entries. In our computation, the number of zero entries of B is equal to 298320. We see that B is so-called *sparse*, i.e., most of the entries of B are zero, which causes that the computation of $\text{rk}H^r(f_{r-q+1}) = \text{rank}B$ becomes more efficient. The sparsity of B is considered to be due to our pruning technique given in Section 3.2.

Table 1 also shows that performance of Magma's function mainly depends on the size of r while ours depends on the size of D , and thus it is implied that Magma's function performs more efficiently for large D , whereas ours performs more efficiently for large r when D is fixed. Specifically, we see from the timing data of Case 2 that when $r = 5$, Magma's function performs more efficiently for $D \geq 3000$ while ours performs more efficiently for $D \leq 3000$.

Merits on Ours: Once one gets a free resolution, one can obtain explicit bases of $H^q(\mathcal{G}_i)$ and explicit representations of $H^q(f_i)$ by our function. As in [8, Chapter 5], those explicit representations can lead further computation of mathematical objects such as an explicit basis of $H^q(\mathcal{F}(n))$ (cf. the current Magma's function does not support the computation).

5 Conclusion and future works

In this paper we first introduced Maruyama's method to compute the dimensions of the cohomology groups of coherent sheaves, and then proposed an explicit algorithm in order to implement his method over mathematical softwares. Maruyama's method is mainly based on the free resolution computation over modules, the Čech cohomology and linear algebra. In more detail, for a given finitely generated graded S -module M with $S = K[X_0, \dots, X_r]$, Maruyama's method takes the following three procedures: *Step 1:* Compute a free resolution of the form (2.2.14). *Step 2:* Generate the bases of the K -linear spaces $H^q(\mathcal{G}_i)$ for $q = 0$ or r and some i , where each \mathcal{G}_i is given as a locally free sheaf of the form (2.2.16). *Step 3:* Compute the representation matrices of $H^q(f_i)$ for some q and i , and their ranks. Moreover, we gave a pruning technique which is adopted in our implementation. Main idea of the technique is to focus on the algebraic structure of $H^q(\mathcal{G}_i)$ which are defined by the Čech cohomology. By the technique, the operations to compute the representation matrices of $H^q(f_i)$ can be reduced, and then the representation matrices shall become sparse. In such cases, computing the ranks of $H^q(f_i)$ becomes more efficient.

We then analyzed the proposed algorithm. In our analysis, the complexity of the algorithm was determined to be polynomial-bounded as $O(\alpha D^2) + O(D^3)$ under some assumptions, where α and D are parameters determined from the form of the free resolution. We implemented the algorithm over computer algebra system Magma and conducted experiments, by which we examined a practicality in performance of the algorithm. Our experimental results show that our function performs more efficiently than the complexity estimated in Section 4.1. In our experiments, we also compared our function with Magma's one. Magma's function adopts Decker-Eisenbud's algorithm which based on the free resolution computation over exterior algebra, the Beilinson-Gelfand-Gelfand correspondence and Tate resolutions. By our experimental results, we observed that performance of Magma's function mainly depends on the size of r while ours depends on the size of D , and thus it is implied that Magma's function performs more efficiently for large D , whereas ours performs more efficiently for large r when D is fixed. Aside from this, the algorithm based on Maruyama's method has an advantage that once one gets a free resolution of the input module, one can obtain

explicit bases of $H^q(\mathcal{G}_i)$ and explicit representations of $H^q(f_i)$ for all q and i . Thus it is concluded that those explicit representations can lead further computation of mathematical objects such as an explicit basis of $H^q(\mathbb{P}^r, \mathcal{F}(n))$.

However, the algorithm proposed in this paper deeply depends on the free resolution computation over modules, and thus without efficient computation of the free resolution, one cannot compute $\dim_K H^q(\mathbb{P}^r, \mathcal{F}(n))$ efficiently. For instance, if M has a long free resolution, the proposed algorithm might be costly. In order to realize more high-speed computation for large r or D and for the case that M has more long free resolutions, it needs to improve the free resolution computation over finitely generated S -modules. This is our future work.

Acknowledgements The author dedicates this paper to the late Masaki Maruyama, and would like to offer the author's deepest sympathy. The author thanks the committee of AC2015 for giving an opportunity to talk about this research at the conference. The author also thanks Masaya Yasuda and Shun'ichi Yokoyama for helpful comments and corrections on this paper.

References

- [1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. of Symbolic Comput., **24**, 235–265 (1997).
- [2] D. Cox, J. Little and D. O'shea, *Using Algebraic Geometry*, GTM, **185**, Springer-Verlag, New York-Berlin (1998).
- [3] W. Decker and D. Eisenbud, *Sheaf algorithms using the Exterior algebra*, In: *Computations in Algebraic Geometry with Macaulay2*, Algorithms and Computation in Mathematics, **8**, 215–247, Springer-Verlag (2002).
- [4] D. Eisenbud, Chapter 8: Computation of Cohomology, pp. 219–226: In Vasconcelos (1998).
- [5] D. Eisenbud, D. Grayson and M. Stillman, Appendix C: Using Macaulay 2, pp. 355–379: In Vasconcelos (1998).
- [6] R. Hartshorne, *Algebraic Geometry*, GTM, **52**, Springer-Verlag (1977).
- [7] M. Kudo, *On the computation of the dimensions of the cohomology groups of coherent sheaves on a projective space*, Master thesis, Kyushu University (2015) available at http://www2.math.kyushu-u.ac.jp/~m-kudo/Master.Thesis_20150206.Kudo.pdf.
- [8] M. Kudo, *Analysis of an algorithm to compute the cohomology groups of coherent sheaves and its applications*, MI Preprints, 2016-1 (2016) available at http://www.imi.kyushu-u.ac.jp/eng/files/imipublishattachment/file/math_56f1fd1e23f2c.pdf.
- [9] M. Maruyama, [*Gröbner Bases and the Application*] (in Japanese), Kyoritsu Publisher (2002).
- [10] J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math., **61**, 197–278 (1955).
- [11] G. G. Smith, *Computing Global Extension Module*, J. of Symbolic Comput., **29**, 729–746 (2000).
- [12] W. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics, **2**, Springer (1998).