$\mathbb{R}^{13}$ への区分線形埋め込みを用いた rank 3 の格子の高速同一性判定

Efficient comparison of rank-3 lattices via piecewise-linear embeddings into $\mathbb{R}^{13}$

富安 亮子 (Ryoko Oishi-Tomiyasu)[1]
[1] 九州大学 (Kyushu University)
e-mail : tomiyasu@imi.kyushu-u.ac.jp

1 概要

Rank 3 の格子パラメータの同一性判定・比較は，ユークリッド計量を含む $\mathbb{R}^{13}$ の計量での 13 次元ベクトルの比較に還元できることを紹介する．通常，(rank n でも) 同一性判定は 2 次形式の簡約理論を用いて行われるが，格子の摂動に対し，簡約形は不連続に変化することがあり，丸め誤差や観測誤差を考慮すると rank の指数関数で増大する回数の反復計算が必要となる．Voronoi 第 2 簡約などが与える一部の格子の不変量の例外を除いて，格子パラメータの簡約形は格子の摂動に対して常に連続に変化するわけではない．これは昔から知られている問題だが，深層学習を用いた結晶構造生成といった応用で，格子や結晶構造といった周期性を持つ構造をうまく（連続に）パラメトライズする (= $\mathbb{R}^m$ に埋め込む) 需要が急増している．生成されたパラメータ $p \in \mathbb{R}^m$ から $\mathcal{L}S_n$ の元を復元する逆写像の計算が容易で，p に含まれる数値誤差が結果に大きく影響しないことも必要である．

そこで，ランク 3 の格子のパラメータ（モジュライ）空間を連続かつ区分線形に 13 次元ユークリッド空間へ埋め込む 2 つの方法を提案する．1 つめは Conway vonorm および conorm の新しい応用，2 つめは Ryškov C-type 簡約理論の modulo 3 への自然な拡張による．

2 誤差を含む格子パラメータを比較するための既存手法

複数の格子の比較・同一性判定は，$\mathcal{L}S_n := GL_n(\mathbb{Z})\backslash\mathcal{S}^n_{\succ 0}$ 上の距離（計量）を与えれば行える．応用分野でアフィン不変リーマン計量と呼ばれる正定値錐 $\mathcal{S}^n_{\succ 0}$ 上の標準的な不変計量が定める距離 d を用いた場合，誘導される $\mathcal{L}S_n$ 上の距離 $d_{\mathcal{L}S_n}$ を求めるには以下の最小化問題を解く必要がある．

$$d_{\mathcal{L}S_n}([S_1],[S_2]) := \min_{g\in GL_n(\mathbb{Z})} d(S_1, gS_2\,{}^t g).$$

最適解 g を得るための反復は Voronoi 第 2 簡約を用いても生じる．任意の $S \in \mathcal{S}^n_{\succ 0}$ に対し，*vonorm* 写像 $\Lambda_n := (\mathbb{Z}^n/2\mathbb{Z}^n) \setminus \{2\mathbb{Z}^n\} \to \mathbb{R}$ は以下で定義される（$2\mathbb{Z}^n$ を定義域から除いた）．

$$\mathrm{vo}_S(u + 2\mathbb{Z}^n) := \min\{vS\,{}^t v : v \in u + 2\mathbb{Z}^n\}.$$

$S \mapsto \mathrm{vo}_S$ が連続写像 $\mathcal{S}^n_{\succ 0} \to \mathbb{R}^{\Lambda_n}$ を与えること，商位相を考えれば連続写像 $f_n : \mathcal{L}S_n \to GL_n(\mathbb{Z}/2\mathbb{Z})\backslash\mathbb{R}^{\Lambda_n}$ を誘導することは明らか． 以下の予想は f_n が単射であることと同値で，$n \le 5$ までの成立が示されている．([1] for $n = 4$; [2] for $n = 5$)．

予想 1 (Conway-Sloane)．$S \in \mathcal{S}^n_{\succ 0}$ が属す $\mathcal{LS}_n$ の軌道は，vo_S の値から一意に定まる．

予想が成立する任意の n に対し，以下の同一性判定アルゴリズムは適切に動く:

入力: グラム行列 $S_1, S_2 \in \mathcal{S}^n_{\succ 0}$, $\mathbb{R}^{\Lambda_n}$ $(= \mathbb{R}^{2^n-1})$ の距離 d.

出力: d によって誘導される，$[S_1], [S_2] \in \mathcal{L}S_n$ の距離.

1: Fincke-Pohst アルゴリズムなどを用いて，$\mathrm{vo}_{S_i} \in \mathbb{R}^{\Lambda_n}$ $(i = 1, 2)$ を計算.

2: 各 $g \in GL_n(\mathbb{Z}/2\mathbb{Z})$ に対して $d(\mathrm{vo}_{S_1}, g \cdot \mathrm{vo}_{S_2})$ を計算．ただし $(g \cdot f)(u) := f(ug^{-1})$ $(\forall u \in \Lambda_n)$.

3: 2 で得られた距離の最小値を返す.

$GL_2(\mathbb{Z}/2\mathbb{Z})$ の位数は $\prod_{k=1}^{n}(2^n - 2^{k-1})$ に等しく，rank 2–5 では 6, 168, 20160, 9999360 となる．大量の格子パラメータを扱う実際の解析では 168 回の比較もボトルネックになり得る．[3] など他のアプローチでも状況は変わらないが，次節の ι_s (or ι_m) による像を $\mathbb{R}^{13}$ の計量により比較すると，$gS_1\,{}^t g \approx S_2$ となる $g \in GL_3(\mathbb{Z})$ の情報は直ちに得られない分，比較回数を 1 とできる.

3　2 つの埋め込み $\iota_* : \mathcal{L}S_3 \hookrightarrow \mathbb{R}^{13}$ の定義と性質

Rank 2 では，埋め込み $\mathcal{L}S_2 \hookrightarrow \mathbb{R}^3$ が，3 つの vonorm の値 (or conorms p_{ij} or root invariants in $\sqrt{p_{ij}}$ [4]) から得られることは容易に示せる．以下の [5] の結果はその rank 3 への拡張である.

定義 1. 任意の $S \in \mathcal{S}^3_{\succ 0}$ に対し，$\iota_s(S) := (f_1(S), f_2(S)) \in \mathbb{R}^{13}$ を以下の $f_1(S) \in \mathbb{R}^7$, $f_2(S) \in \mathbb{R}^6$（ともに寄与の順序でソートされているとする）の結合とする.

$$f_1(S) := [\,\mathrm{vo}_S(g) : g \in \Lambda_3\,],$$
$$f_2(S) := \left[\,\sum_{g \in \Lambda_3} \chi(g)\mathrm{vo}_S(g) : \begin{array}{c}\chi((1,0,0)) = \chi((0,1,0)) = \chi((0,0,1)) \text{ が} \\ \text{成立しない指標} \chi(\mathbb{Z}/2\mathbb{Z})^3 \to \{\pm 1\}\end{array}\right].$$

$f_1(S)$, $f_2(S)$ の元は非零の vonorm, conorm で，S が Selling 簡約なら容易に計算できる.

定義 2. 任意の $S \in \mathcal{S}^n_{\succ 0}$ と整数 $r \geq 2$ に対し *modulo* r の *vonorm* 写像 $\Lambda_{n,r} := (\mathbb{Z}^n/r\mathbb{Z}^n)\backslash\{r\mathbb{Z}^n\} \to \mathbb{R}$ を

$$\mathrm{vo}_{S,r}(u + r\mathbb{Z}^n) := \min\{vS\,{}^t v : v \in u + r\mathbb{Z}^n\},$$

で定義する．$\mathrm{vo}_{S,r}(u + r\mathbb{Z}^n) = \mathrm{vo}_{S,r}(-u + r\mathbb{Z}^n)$ より，*13* 個の各類 $\{\pm 1\}\backslash\Lambda_{3,3}$ に対する $\mathrm{vo}_{S,3}$ の値を寄与の順序でソートしたベクトルを $\iota_m(S)$ とする．すなわち，

$$\iota_m(S) := \left[\mathrm{vo}_{S,3}(u + 3\mathbb{Z}^3) : \pm u + 3\mathbb{Z}^3 \in \{\pm 1\}\backslash\Lambda_{3,3}\right].$$

定義より，ι_s and ι_m は区分線形な連続写像 $\mathcal{L}S_3 \to \mathbb{R}^{13}$ である．証明は [5] を参照.

定理 1. *S が Minkowski 簡約なら，$\iota_m(S)$ は以下の 13 個の値を寄与の順序で並べたベクトルに等しく，容易に計算できる: 各 $v = (1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,0)$, $(1,0,1)$, $(0,1,1)$, $(1,1,1)$, $(1,-1,0)$, $(1,0,-1)$, $(0,1,-1)$) に対する $vS\,{}^t v$, および，$\min\{vS\,{}^t v : v = (-1,1,1), (2,1,1)\}$, $\min\{vS\,{}^t v : v = (1,1,-1), (1,1,2)\}$, $\min\{vS\,{}^t v : v = (1,-1,1), (1,2,1), (-2,-1,1), (1,-1,-2)\}$.*

定理 2. *ι_s, ι_m が誘導する写像 $\mathcal{L}S_3 \to \mathbb{R}^{13}$ はそれぞれ単射である.*

参考文献

[1] F. Vallentin, Ph. D. thesis (2003), Technical University Munich.

[2] M. D. Sikirić, M. Kummer, Expositiones Mathematicae, 40 (2022), 302–314.

[3] B. Gruber, Acta Cryst. A29 (1973), 433–440.

[4] V. Kurlin, Foundations of Computational Mathematics, 24 (2022), 805–863.

[5] R. Oishi-Tomiyasu, https://arxiv.org/abs/2506.08934 (2025).

楕円曲線の直積を定義域とする高次数同種写像計算の効率化

Improving the Efficiency of Odd Degree Isogeny Computations with the Domain as a Product of Elliptic Curves

吉住 峻 (Ryo Yoshizumi)[1]
[1] 九州大学 (Kyushu University)
e-mail : yoshizumi.ryo.483@s.kyushu-u.ac.jp

1　概要

2 次元の同種写像を効率的に計算することは, 数論アルゴリズムや同種写像暗号の観点から興味深い問題である. 特に, Kani の補題 [1] という定理を利用する場合, 次のような問題を効率的に計算することが重要である:

問題.　E_1, E_2, F_1, F_2 を楕円曲線, $\Phi : E_1 \times E_2 \to F_1 \times F_2$ を (D, D)-同種写像とする. $\operatorname{Ker}\Phi \simeq (\mathbb{Z}/D\mathbb{Z})^2$ の基底 $((P_1, P_2), (Q_1, Q_2))$ が与えられているとする. また, $x_1, \ldots, x_m \in E_1$ を任意の点とする $(m \geq 1)$. $E_1, E_2, P_1, P_2, Q_1, Q_2, x_1, \ldots, x_m$ が与えられたとき, F_1, F_2 と $\Phi((x_1, 0_{E_2})), \ldots, \Phi((x_m, 0_{E_2})) \in F_1 \times F_2$ を効率的に求めよ.

暗号応用上, D が 2 冪であるケースが多いが, 本稿では D が 2 冪ではない, すなわち, D が奇素因数を含む場合を考える. 既存手法としては, 与えられたデータから $E_1 \times E_2, (P_1, P_2), (Q_1, Q_2), (x_1, 0_{E_2}), \ldots, (x_m, 0_{E_2})$ を計算し, その後 2 次元の同種写像のアルゴリズムを用いて $F_1, F_2, \Phi((x_1, 0_{E_2})), \ldots, \Phi((x_m, 0_{E_2}))$ を求める. 2 次元の同種写像を計算する方法の一つとして, テータ関数を用いる方法が知られている. 特に, テータ関数を用いた奇数次数同種写像の効率的な計算方法としては, Lubicz–Robert [2] によって公式が与えられている. また, この公式は [3] によって, 効率的なアルゴリズムが与えられている. 本稿では, 上記の問題に対して, 既存手法より効率化した公式, アルゴリズムを提案する. また, その提案手法を SageMath 上で実装し, 既存手法と実行時間を比較した結果についても紹介する.

2　提案公式

基本的なアイデアは, 計算する点が $(x_i, 0_{E_2}) \in E_1 \times E_2$ $(x_i \in E_1)$ の形であるため, $E_1 \times E_2$ 上で行われる計算を出来る限り E_1, E_2 それぞれの上で計算を行うことで, 第 2 成分が $0_{E_2} \in E_2$ であることにより計算量を減らすということである. $f : E_1 \times E_2 \to A_2$ を (ℓ, ℓ)-同種写像とする. $0_{A_2} \in A_2$ と $f((x, 0_{E_2}))$ $(x \in E_1)$ の計算手法について, 提案手法の公式について紹介する. 正確には, それらのテータ座標を用いて計算する. 以下, $\ell = \sum_{1 \leq u \leq r} a_u^2$ を平方和, (e_1, e_2) を $\operatorname{Ker}(f_1) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ の基底, $e_i = (e_i^{(1)}, e_i^{(2)}) \in E_1 \times E_2$ $(i = 1, 2)$, $\mathbf{x} = (x, 0_{E_2})$ とする. このとき, 以下の式 (1) で 0_{A_2} のテータ座標を, 式 (2) で $(x, 0_{E_2})$ のテータ座標を計算できる. ただし, $c^{(1)}_{m_1,m_2}, c^{(2)}_{m_1,m_2}, c'^{(1)}_{m_1,m_2}$ の定義は省略.

$$\theta_i(0_{A_2}) = \prod_{1 \leq t \leq 2} \left(\sum_{0 \leq m_1, m_2 < \ell} c^{(t)}_{m_1,m_2} \prod_{1 \leq u \leq r} \theta_{a_u i}(a_u m_1 e_1^{(t)} + a_u m_2 e_2^{(t)}) \right). \tag{1}$$

	既存手法 [3]	提案手法 (Sec.2)
(i)	18.17	12.63
(ii)	15.79	<u>12.24</u>

表 1. 1 点 $(x_1, 0_{E_2})$ を計算する場合に必要な f_1 の平均実行時間 (秒)

	既存手法 [3]	提案手法 (Sec.2)
(i)	25.22	14.55
(ii)	20.50	<u>13.95</u>

表 2. 2 点 $(x_1, 0_{E_2}), (x_2, 0_{E_2})$ を計算する場合に必要な f_1 の平均実行時間 (秒)

$$\theta_i(f((x, 0_{E_2}))) = \left(\sum_{0 \le m_1, m_2 < \ell} c'^{(1)}_{m_1, m_2} \prod_{1 \le u \le r} \theta_{a_u i}(a_u x + a_u m_1 e_1^{(1)} + a_u m_2 e_2^{(1)}) \right) \tag{2}$$
$$\times \left(\sum_{0 \le m_1, m_2 < \ell} c^{(2)}_{m_1, m_2} \prod_{1 \le u \le r} \theta_{a_u i}(a_u m_1 e_1^{(2)} + a_u m_2 e_2^{(2)}) \right)$$

このとき, 式 (2) の 2 項目は式 (1) の 2 項目 ($t = 2$) で現れた式と全く同じであるため, 計算結果が再利用可能である. この点で提案手法は既存手法 [3] より効率的である.

3 実装結果

以下の 67 ビット素数 p と D に関して, $\mathbb{F}_{p^2}$ 上の (D, D)-同種写像 $\Phi : E_1 \times E_2 \to F_1 \times F_2$ を考える: $p = 110564446907225951023$, $D = 7^3 \cdot 11 \cdot 19 \cdot 23^2 \cdot 53 \cdot 137$. D の素因数分解を $D = \ell_1 \cdots \ell_m$ とする. ただし, $\ell_1 = 137$ とする. この Φ を次数 ℓ_i の同種写像に分解して計算する方法が最も効率的である. この Φ を $E_1 \times E_2 \overset{f_1}{\to} A_2 \overset{f_2}{\to} \cdots \to A_n \overset{f_n}{\to} F_1 \times F_2$ に分解する. ただし, $\deg(f_i) = \ell_i$. 今, 各 (ℓ_i, ℓ_i)-同種写像 f_i の計算量は $O(\ell_i^2)$ であるため, f_1 の計算が支配的なステップである.

上のパラメータに関して, 既存手法 [3] と提案手法 (Section 2) を計算機代数システム SageMath で実装した. 表 1, 2は, その f_1 の計算の平均実行時間 (秒) を表したものである. 表 1は 1 点 $x_1 \in E_1$ に関して, $f_1(0_{E_1 \times E_2}), f((P_1, P_2)), f((Q_1, Q_2)), f((x_1, 0_{E_2}))$ を計算に関して, 10 回実行したときの平均実行時間を表している. 表 2は 2 点 $x_1, x_2 \in E_1$ に関して, 同様の平均実行時間を表したものである. 表 1, 2から, いずれも提案手法が効率的であることが分かる. 計算する点 $x_1, x_2, \ldots$ の数が増えれば増えるほど効率化の影響は大きくなる. 提案手法を実装したコードは GitHub リポジトリ (https://github.com/Yoshizumi-Ryo/isogeny-product-sage) で公開している.

謝辞 本研究は九州大学マス・フォア・イノベーション卓越大学院プログラムの支援を受けています.

参考文献

[1] Ernst Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.*, 485:93–121, 1997.

[2] David Lubicz and Damien Robert. Fast change of level and applications to isogenies. *Res. Number Theory*, 9(1):Paper No. 7, 28, 2023.

[3] Ryo Yoshizumi, Hiroshi Onuki, Ryo Ohashi, Momonari Kudo, and Koji Nuida. Efficient theta-based algorithms for computing (ℓ, ℓ)-isogenies on kummer surfaces for arbitrary odd ℓ. In Ruben Niederhagen and Markku-Juhani O. Saarinen, editors, *Post-Quantum Cryptography*, pages 3–37, Cham, 2025. Springer Nature Switzerland.

多重次数付けされた連立代数方程式の求解について

Solving systems of multi-graded equations via Macaulay matrices

中村 周平 (Shuhei Nakamura)[1]
[1] 茨城大学 (Ibaraki University)
e-mail : shuhei.nakamura.fs71@vc.ibaraki.ac.jp

1　はじめに

近年, 多変数多項式暗号から連立代数方程式に帰着する攻撃で, さらに連立代数方程式問題の定義多項式が多重次数付け可能な場合のものがいくつか見つかっており, 本講演ではそのような連立代数方程式問題を対象とする. また, 連立代数方程式の求解アルゴリズムは様々なものがあるが, 暗号の安全性解析にしばしば想定される Macaulay 行列を用いた XL (eXtended Linearization) 手法について調べる. この手法は, グレブナー基底を求める方法と Macaulay 行列の右カーネルから解を求める方法の主に二つに分かれる. 既存の暗号解析では, 具体的な方式から得られる多重次数付け可能な代数方程式系に対して, 後者の方法で解くことのみが考えられてきた. 本講演では, まず両方の手法に対応する多重次数付け可能な代数方程式系を入力としたアルゴリズムを提案する. 次に, これらのアルゴリズムから解を求めることが可能となるいくつかの入力の次数について特徴付けを行う. 本講演の一部は, すでに [1] において発表されている.

2　準備 (多重次数付けされた Macaulay 行列)

変数集合 $\underline{X}$ における有限体 $\mathbb{F}$ 上の多項式環 $A = \mathbb{F}[\underline{X}]$ に対して, $Mon(\underline{X})$ をその単項式集合とする. 変数集合 $\underline{X} = \{x_{ji}\}_{1\le i\le s, 1\le j\le n_i}$ を $\underline{X}_i = \{x_{1,i}, \dots, x_{n_i,i}\}$ として s 個の変数集合 $\underline{X} = \underline{X}_1 \cup \cdots \cup \underline{X}_s$ に分ける. 多項式 f に対して多重次数 $\deg_{\mathbb{Z}^s_{\ge 0}}$ を $\deg_{\mathbb{Z}^s_{\ge 0}} f = (\deg_{\underline{X}_1} f, \dots, \deg_{\underline{X}_s} f)$ により定め, $Mon_{(d_1,\dots,d_s)}(\underline{X}) = \{u \in Mon(\underline{X}) \mid \deg_{\mathbb{Z}^s_{\ge 0}} u = (d_1, \dots, d_s)\}$, $Mon_{\le(d_1,\dots,d_s)}(\underline{X}) = \bigcup_{i_j \le d_j} Mon_{(i_1,\dots,i_s)}(\underline{X})$ を定義する. このとき, 次のように Macaulay 行列は導入される:

定義 1　$F \subset A = \mathbb{F}[\underline{X}_1, \cdots, \underline{X}_s]$ を有限集合, $\succ$ を全順序とする. $\boldsymbol{d} \in \mathbb{Z}^s_{\ge 0}$ に対して有限集合 $XM_{\boldsymbol{d}}(F) := \{u \cdot f \mid f \in F, u \in Mon_{\le \boldsymbol{d} - \deg_{\mathbb{Z}^s_{\ge 0}} f}(\underline{X})\}$ を定める. F の次数 $\boldsymbol{d}$ の Macaulay 行列 $Mac^{\succ}_{\boldsymbol{d}}(F)$ とは, $XM_{\boldsymbol{d}}(F)$ の各元 f に $(\mathrm{Coeff}(f, u_1), \dots, \mathrm{Coeff}(f, u_N))$ が対応している行列をいう. ただし, $Mon_{\le \boldsymbol{d}}(\underline{X}) = \{u_1, \dots, u_N\}$ で, $u_i \succ u_{i+1}$ となる.

3　主結果

本講演では, 連立代数方程式 $\{f_i = 0\}_{i=1}^m$ を定める多項式系 $F = \{f_1, \dots, f_m\} \subset \mathbb{F}[\underline{X}]$ は $c_{RM} := \dim_{\mathbb{F}} \mathbb{F}[\underline{X}]/\langle F\rangle_A < \infty$ を満たしているとする.

■ グレブナー基底を利用した求解　単項式集合 $Mon(\underline{X})$ 上の全順序 $\succ$ で次を満たすものを単項式順序と呼ぶ: i) $u_1 \succ u_2 \Rightarrow u_3u_1 \succ u_3u_2$ $(u_i \in Mon(\underline{X}))$ ii) $\forall u \in Mon(\underline{X}), u \succeq 1$. また, 単項式順序を固定したとき, $f \in \mathbb{F}[\underline{X}]$ に対して先頭項 $LM_{\succ}(f) := \max_{\succ}\{u \in Mon(\underline{X}) \mid \mathrm{Coeff}(f, u) \ne 0\}$ が定まる. イデアル I に対して次の条件を満たすその部分集合 G はグレブナー基底と呼ばれる: $\forall f \in I, \exists g \in G$ s.t. $LM_{\succ}(g) \mid LM_{\succ}(f)$. $c_R < \infty$ を満たすような, 有限個の解を持つ連立代数方程式 $F = \mathbf{0}$ において, イデアル $\langle F\rangle_A$ の辞書式単項式順序に関するグレブナー基底は一変数多項式を含

む. これは $F = \mathbf{0}$ の解が満たす方程式を定めることから, 一変数の求解を繰り返すことで解を決定することが可能となる.

有限集合 F の生成するイデアル $\langle F\rangle_A$ に含まれる次の部分空間を考える:

$$\langle [A \cdot F]_{\leq \boldsymbol{d}} \rangle_{\mathbb{F}} := \langle XM_{\boldsymbol{d}}(F) \rangle_{\mathbb{F}} \subseteq A_{\leq \boldsymbol{d}}.$$

ただし, $A_{\leq \boldsymbol{d}} = \langle Mon_{\leq \boldsymbol{d}}(\underline{X}) \rangle_{\mathbb{F}}$ である. このとき, 次が成り立つことをみた.

命題 2（Proposition 8 [2]） 単項式順序 $\succ$ を固定する. 集合 $\{\boldsymbol{d} = (d_1, \ldots, d_s) \mid \dim A_{\leq \boldsymbol{d}}/\langle [A \cdot F]_{\leq \boldsymbol{d}} \rangle_{\mathbb{F}} \leq c_{RM} \leq d_i, 1 \leq \forall i \leq s\}$ の元 $\boldsymbol{D}$ が存在するとき, $Mac^{\succ}_{\boldsymbol{D}}(F)$ の行階段行列に対応する多項式集合はグレブナー基底である.

■ Macaulay 行列の右カーネルを利用した求解 多項式 $f \in A = \mathbb{F}[\underline{X}]$ に対して $\boldsymbol{a} \in \mathbb{F}^n$ はその根であるとする. つまり, $f(\boldsymbol{a}) = 0$ である. このとき, $(\mathrm{Coeff}(f, u_1), \ldots, \mathrm{Coeff}(f, u_{N_{\boldsymbol{d}}}))$ と $(u_1(\boldsymbol{a}), \ldots, u_{N_{\boldsymbol{d}}}(\boldsymbol{a}))$ の内積は 0 である. ただし, $\boldsymbol{d} = \deg_{\mathbb{Z}^s_{\geq 0}} f$, $Mon_{\leq \boldsymbol{d}}(\underline{X}) = \{u_1, \ldots, u_{N_{\boldsymbol{d}}}\}$ である. f に単項式倍をしても $\boldsymbol{a} \in \mathbb{F}^n$ は再びその根となる. したがって, 方程式系 $F = \mathbf{0}$ が共通解 $\boldsymbol{a}$ をもつとき, $Mac^{\succ}_{\boldsymbol{D}}(F)$ の右カーネルには $(u_1(\boldsymbol{a}), \ldots, u_{N_{\boldsymbol{D}}}(\boldsymbol{a}))$ が含まれる. ただし, $Mon_{\leq \boldsymbol{D}}(\underline{X}) = \{u_1, \ldots, u_{N_{\boldsymbol{D}}}\}$ である. ゆえに, Macaulay 行列のカーネルには解に対応するベクトルが存在し, 有限体上の求解アルゴリズムとして Algorithm 1 を考えることはできる.

Algorithm 1 Multi-Degree Macaulay Matrix Generation and Kernel Vector Computation

Input: $\boldsymbol{d} \in \mathbb{Z}^s_{\geq 1}$, $q < \infty$, $\succ$: 単項式順序, F: 多項式集合で方程式 $F = \mathbf{0}$ は $\mathbb{F}_q$ 上で解を持つ.

1: F の各元 f に対して $Mon_{\leq \boldsymbol{d} - \deg_{\mathbb{Z}^s_{\geq 0}} f}(\underline{X})$ の元をかけて $XM_{\boldsymbol{d}}(F)$ を計算し, Macaulay 行列 $Mac^{\succ}_{\boldsymbol{d}}(F)$ を生成する.

2: ガウスの消去法により $Mac^{\succ}_{\boldsymbol{d}}(F)$ の右カーネルの基底を計算する.

3: $v_1 \neq 0$ となるカーネルベクトル $\boldsymbol{v}$ に対して, $(v_{x_1}/v_1, \ldots, v_{x_n}/v_1)$ が $F = \mathbf{0}$ の解ならばそれを返す. ただし, v_u は単項式 $u \in Mon_{\leq \boldsymbol{d}}(\underline{X})$ に対応する $\boldsymbol{v}$ の成分である.

$\mathrm{Rank}(Mac^{\succ}_{\boldsymbol{D}}(F)) = \dim_{\mathbb{F}} \langle [A \cdot F]_{\leq \boldsymbol{D}} \rangle_{\mathbb{F}}$ であるから, $\dim \mathrm{Ker}(Mac^{\succ}_{\boldsymbol{D}}(F)) = \dim_{\mathbb{F}} A_{\leq \boldsymbol{D}}/\langle [A \cdot F]_{\leq \boldsymbol{D}} \rangle_{\mathbb{F}}$ が成り立つ. 特に, $\dim_{\mathbb{F}} A/\langle F\rangle_A = 1$ のとき, $\dim \mathrm{Ker}(Mac^{\succ}_{\boldsymbol{D}}(F)) = 1$ を満たす $\boldsymbol{D}$ において Algorithm 1 でのステップ 3 の反復を避ける.

命題 3（Proposition 12. [2]） $\dim_{\mathbb{F}} A/\langle F\rangle = 1$ とする. 集合 $\{\boldsymbol{d} = (d_1, \ldots, d_s) \in \mathbb{Z}^s_{\geq 1} \mid \dim_{\mathbb{F}} A_{\leq \boldsymbol{d}}/\langle [A \cdot F]_{\leq \boldsymbol{d}} \rangle_{\mathbb{F}} = 1\}$ が空でないとき, その集合の元において Algorithm 1 は $F = \mathbf{0}$ の解を返す.

謝辞 本講演は JST CREST JPMJCR2113, 科研費 JP23K16885 の助成を受けたものです.

参考文献

[1] 中村周平, Macaulay 行列を利用した連立代数方程式の求解について, 2025 年 暗号と情報セキュリティに関するシンポジウム, 数論応用セッション, 2D2-4 (2025).

[2] Shuhei Nakamura, Solving systems of polynomial equations via Macaulay matrices, IACR e-print archive 2025/793 (2025), https://eprint.iacr.org/2025/793

On Diffie-Hellman key exchange algorithm based on a real quadratic analogue of ideal class group action of CM elliptic curves

木村 巖 (Iwao KIMURA)[1]
[1] 富山大学学術研究部理学系 (Faculty of Science, Academic Assembly, University of Toyama)
e-mail : iwao@sci.u-toyama.ac.jp

1　イントロダクション

本講演では，Darmon-Dasgupta [DD06] により提案された，「実 2 次体上の楕円単数」への実 2 次体の整環のイデアル類群の作用を利用した Diffie-Hellman 鍵交換アルゴリズムの実現について議論する．

2　本論

■暗号学的群作用　G を群，X を G 作用を持つ群とする．Alamati et al. [ADFMP20, §1.1] らに従い，一方向性などの何らかの困難性をもつ群作用を総称して暗号学的群作用と呼ぶことにする．X 自身が素数 p 位数の群，$G = (\mathbb{Z}/p\mathbb{Z})^\times$ を法 p の既約剰余類の群とすると，$g \in G$, $x \in X$ に対して $g \cdot x \coloneqq x^g$ により群作用が定まるが，Diffie-Hellman 仮定が成り立てば，この群作用は暗号学的群作用である．

■古典的な虚数乗法論とイデアル類群作用　この節については上掲 [DD06, §1] 参照．正の整数 N を固定する．複素数体 $\mathbb{C}$ 内の格子の対で，包含関係があり，剰余群が位数 N の巡回群となるもののhomothety に関する同値類の集合を Ω_N とする：

$$\Omega_N \coloneqq \{\, (\Lambda_1, \Lambda_2) \mid \Lambda_i \subset \mathbb{C} \text{ (lattice)}, \Lambda_1 \supset \Lambda_2, \Lambda_1/\Lambda_2 \cong \mathbb{Z}/N\mathbb{Z} \,\} /\text{homothety}.$$

格子 Λ_1 の基底 ω_1, ω_2 を適切にとって，$\Lambda_1 = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\Lambda_2 = N\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\Im(\omega_1\omega_2' - \omega_1'\omega_2) > 0$ とできる．このとき，次の全単射が存在する：

$$\underline{\tau} \colon \Omega_N \ni (\lambda_1, \Lambda_2) \mapsto \frac{\omega_1}{\omega_2} \in \mathfrak{h}/\Gamma_0(N),$$

ただし $\mathfrak{h}$ は複素上半平面，$\Gamma_0(N)$ はレベル N の主合同部分群である．さらに，K を虚 2 次体（複素数体 $\mathbb{C}$ 内の部分体と考える）に対して

$$\Omega_N(K) \coloneqq \{\, (\Lambda_1, \Lambda_2) \in \Omega_N \mid \Lambda_i \subset K \ (i = 1, 2) \,\} / K^\times$$

とすると，$\tau \in \mathfrak{h} \cap K$ なら $\tau \in \underline{\tau}(\Omega_N(K))$ である．$O \subset K$ を K の整環とするとき，

$$\Omega_N(O) \coloneqq \{\, (\Lambda_1, \Lambda_2) \in \Omega_N(K) \mid O \text{ は } \Lambda_i \text{ を保つ最大の整環}, (i = 1, 2) \,\}$$

とすると，

$$\underline{\tau}(\Omega_N(O)) = \mathfrak{h}^O/\Gamma_0(N),$$

ただし，$\mathfrak{h}^O = \{\, \tau \in \mathfrak{h} \mid O_\tau \cong O \,\}$, $O_\tau = \{\, \left(\begin{smallmatrix} a & b \\ c & Nd \end{smallmatrix}\right) \mid a\tau + b = c\tau^2 + Nd\tau \,\}$ である．以上の状況は，$\mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_1$ という，O に虚数乗法を持つ CM 楕円曲線の位数 N 巡回同種写像と，それに対応する開モジュラー曲線 $Y_0(N) = \mathfrak{h}/\Gamma_0(N)$ の O 値点の対応に他ならない．

このとき，O のイデアル類群 $\mathrm{Pic}(O)$ が $\Omega_N(O)$ に，$[\mathfrak{a}] \in \mathrm{Pic}(O)$, $(\Lambda_1, \Lambda_2) \in \Omega_N(O)$ に対して

$$[\mathfrak{a}] \cdot (\Lambda_1, \Lambda_2) \coloneqq (\mathfrak{a}\Lambda_1, \mathfrak{a}\Lambda_2)$$

により作用し，同様に $\mathrm{Pic}(O)$ は $\mathfrak{h}^O/\Gamma_0(N)$ にも作用する．このとき，$\tau \in \mathfrak{h}^O$ ならば，O についての環類体 H_O の零でない元 $u(\alpha, \tau)$ が存在して，次の性質を満たす：

$$u(\alpha, [\mathfrak{a}] \cdot \tau) = \left(\frac{H_O/K}{[\mathfrak{a}]^{-1}}\right) u(\alpha, \tau), \tag{1}$$

ここで，$\left(\frac{H_O/K}{[\mathfrak{a}]^{-1}}\right)$ は Abel 拡大 H_O/K の Artin 記号である．

有限次代数体の有限次 Abel 拡大 L/K に対して，その Galois 群 $\mathrm{Gal}(L/K)$ は，類体論により K の（一般化された）イデアル類群の部分群と同型になる．よって $\mathrm{Gal}(L/K)$ の作用を受ける集合は，K の（一般化された）イデアル類群の作用を持つと見なすことができる．この観点と虚数乗法論を組み合わせて暗号学的群作用をもつ集合を構成し，Diffie-Hellman 型鍵共有アルゴリズムを得る可能性については，すでに Couveigne [Cou06, §5.7] で指摘されている．

■実 2 次体類似　Darmon-Dasgupta 上掲論文の §2 では，以上の状況を実 2 次体上に移植するために，K を実 2 次体，p を K で惰性する有理素数，Λ_1, Λ_2 を K 内の $\mathbb{Z}[1/p]$ 格子（K 内の階数 2 自由 $\mathbb{Z}[1/p]$ 加群），などとして，それらの対の homothety 類 $\Omega_N(K)$, さらに O が Λ_1, Λ_2 を保つ最大の整環となる部分集合 $\Omega_N(O)$ を定義した．これらの上に，K の $\mathbb{Z}[1/p]$ 整環 O の狭義イデアル類群 $\mathrm{Pic}^+(O)$ の作用が定まり，また，p 進上半平面のモジュラー群による商への $\mathrm{Pic}^+(O)$ 作用も定まる．このとき，上記の $u(\alpha, \tau)$ に相当するものが O に対応する環類体 H_O の零でない元として定まり，次を満たすことを**予想**した：

$$u(\alpha, \tau) \in O_H[\frac{1}{p}]^\times/\{1 \text{ の冪根 }\}, \quad u(\alpha, [\mathfrak{a}] \cdot \tau) = \left(\frac{H_O/K}{[\mathfrak{a}]^{-1}}\right) u(\alpha, \tau) \pmod{\{1 \text{ の冪根 }\}}. \tag{2}$$

この予想は未解決だが，数値的な検証は可能である．Dasgupta [Das07] 参照.

本講演では，上記の実 2 次体の整環のイデアル類群作用を持つ K 内の $\mathbb{Z}[1/p]$ 格子のペアの集合上での，Diffie-Hellman 型鍵共有アルゴリズムについて考察する．

参考文献

[ADFMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis, *Cryptographic group actions and applications*, Advances in cryptology—ASIACRYPT 2020. Part II, Lecture Notes in Comput. Sci., vol. 12492, Springer, Cham, [2020] ©2020, pp. 411–439. MR 4210345

[Cou06] Jean-Marc Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive, Paper 2006/291, 2006.

[Das07] Samit Dasgupta, *Computations of elliptic units for real quadratic fields*, Canad. J. Math. **59** (2007), no. 3, 553–574. MR 2319158

[DD06] Henri Darmon and Samit Dasgupta, *Elliptic units for real quadratic fields*, Ann. of Math. (2) **163** (2006), no. 1, 301–346. MR 2195136