

二次ディオファントス方程式の求解アルゴリズムについて

中村 悠人[†] 小川 瑞史[†]

[†] 北陸先端科学技術大学院大学

〒923-1292 石川県能美市旭台 1-1

E-mail: [†]yuto.nakamura@jaist.ac.jp, ^{††}mizuhito@gmail.com

あらまし 整数係数多変数多項式制約解消は、実数解と整数解の場合に分かれ、SMT ソルバーにおいて、それぞれ Nonlinear Real number Arithmetic (NRA)、Nonlinear Integer Arithmetic (NIA) の背景理論に相当する。多項式制約の実数上の充足可能解は、1930 年前後に *Tarski* が Quantifier elimination に基づく決定可能性を示した。しかし、そのアルゴリズムは間接的に証明内に記述されており、アルゴリズムとして整理されるのは *Tarski* 自身によって 1951 年になってからであった。多項式制約の整数解に限る場合をディオファントス制約とよぶ。多項式制約には等式 (=) と不等式 (>) があるが、本稿では等式であるディオファントス方程式に注目する。ディオファントス方程式の決定可能性は *Hilbert* の第十問題として知られ、その否定的解決は *Matijasevic* により 1970 年に示された。決定可能な部分問題として *Grunwald* と *Segal* は 1981 年に単一の二次ディオファントス方程式を提示した。しかし、その証明は *Hasse* 原理を含む古典的二次形式の理論、*Hensel* 補題を含む可換環論・代数群・Lie 環の基礎理論に基づき、多岐にわたる背景知識と部分アルゴリズムは多くの関連文献に埋没する。本稿では、数学的証明は各文献への参照にとどめ、単一の二次ディオファントス方程式の充足可能性の決定アルゴリズムを整理し、その概要を紹介する。

キーワード 二次ディオファントス方程式、二次形式、整数解、決定可能性

On Solving Quadratic Diophantine Equation

Yuto NAKAMURA[†] and Mizuhito OGAWA[†]

[†] Japan Advanced Institute of Science and Technology

1-1 Asahidai Nomi, Ishikawa, 923-1292 Japan

E-mail: [†]yuto.nakamura@jaist.ac.jp, ^{††}mizuhito@gmail.com

Abstract Polynomial constraint solving are often either on Real numbers or on Integers, which correspond to Backend theories NRA (Nonlinear Real number Arithmetic) and NIA (Nonlinear Integer Arithmetic) of an SMT-solver, respectively. For the former, *Tarski* showed its decidability based on the quantifier elimination. However, the algorithm was shown rather implicit among the proofs, and an organized algorithm appeared later on 1951 by *Tarski* himself. The latter, i.e., solving on Integers, is called *Diophantine constraint*, which is either an equation (=) or an inequation (>). We focus on the former, which is called *Diophantine equation*. Its solution is known as *Hilbert's 10th problem*, and was negatively solved by *Matijasevic* on 1970. As a decidable subclass of a single Diophantine equation, *Grunwald* and *Segal* posed a quadratic Diophantine equation on 1981. Its proof crosses various areas of mathematics, e.g., classical quadratic form (including Hasse's principle), basic theories of commutative rings, algebraic groups, and Lie algebra. Hence, subroutines of the algorithm are buried in various literatures. In this report, the mathematical proofs are left to the references and we overview an organized self-contained algorithm to solve a single quadratic Diophantine equation.

Key words Quadratic Diophantine Equation, Quadratic form, Integral solution, Decidability

1. ま え が き

整数係数多変数多項式制約解消は、実数解と整数解の場合に分かれ、SMT ソルバーにおいて、それぞれ Nonlinear Real number

Arithmetic (NRA)、Nonlinear Integer Arithmetic (NIA) の背景理論に相当する。多項式制約の実数上の充足可能性は、1930 年前後に *Tarski* が Quantifier elimination に基づく決定可能性を示した。しかし、そのアルゴリズムは間接的に証明内に記述されて

おり、アルゴリズムとして整理されるのは *Tarski* 自身によって 1951 年になってからであった [21]。現在では、より効率の良い (二重指数関数) アルゴリズムである CAD (Cylindrical Algebraic Decomposition) [11] を用いた *Mathematica*, *Maple*, *Reduce* などの実装が知られている。

多項式制約の整数解に限る場合をディオファントス制約とよぶ。多項式制約には等式 (=) と不等式 (>) があるが、本稿では等式であるディオファントス方程式に注目する。ディオファントス方程式の決定可能性は *Hilbert* の第十問題として知られ、その否定的解決は *Matijasevic* により 1970 年に示された [13], [16]。方程式は次数に関わらず、新たな変数を導入することで複数の二次方程式に還元される。たとえば、 x^2yz などの項は $\alpha = x^2, \beta = yz$ により $\alpha\beta$ となる。さらに複数の二次方程式 $f_1 = 0, \dots, f_k = 0$ は単一の 4 次ディオファントス方程式 $\sum_{i=1}^k (f_i)^2 = 0$ に帰着される。単一のディオファントス方程式の決定可能性は 4 次以上は決定不能だが、3 次は未解決であり、2 次の場合は 1981 年に *Grunwald* と *Segal* は決定可能であることを示した [14]。その論文は数ページだが、整数行列のなす直交群が有限生成であること [9] の構成的証明を与えた [14] の系となっており、Hasse 原理を含む古典的二次形式の理論 [2]、行列表現上の *Hensel* 補題を含む可換環論 [6], [8]・代数群 [4], [5]・Lie 環 [3], [10] など多岐にわたる背景知識を用いている。そのため、サブルーチンとなる部分アルゴリズムは多くの参考文献に分散して埋没する。本稿では、数学的証明は各文献への参照にとどめ、単一の二次ディオファントス方程式の充足可能性の決定アルゴリズムを整理して包括的に紹介する。アルゴリズムの詳細は、第一著者の修士論文 [7] を参照されたい。

2. 求解アルゴリズムの概要

複素数、実数、有理数、整数の集合をそれぞれ $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ 、また逆元をもつ環 R 上の n 次行列の集合を $GL_n(R)$ 、直交行列の集合を $O_n(R)$ で表す。 $\mathbf{x} \in \mathbb{Z}^n$ の各要素が互いに素のとき、primitive という。

単一の n 変数 2 次ディオファントス方程式を、 $A \in O_n(\mathbb{Z}) \subseteq GL_n(\mathbb{Z})$, $\mathbf{b}, \mathbf{x} \in \mathbb{Z}^n, c \in \mathbb{Z}$ を用いて

$$\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} = c \quad (1)$$

により表現する。簡単に解ける場合として、

- (1) 1 変数のとき：線形方程式の解に帰着。
- (2) $\det(A) = 0$ のとき：変数がより少ない場合に帰着。
- (3) A が定値 (definite) なとき。つまり A の固有値が全て定符号のとき： $\mathbf{x}$ の各値が十分大きくなると $\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x}$ は定符号となり、その上界以下の有限探索に帰着する。

以下では、 $n \geq 2$, $\det(A) \neq 0$, A は非定値 (indefinite) を仮定する。その場合、一次項 $\mathbf{b}^\top \mathbf{x}$ の消去として、

命題 ([15]: Proposition 1) $\tilde{A} \in O_n(\mathbb{Z}) \subseteq GL_n(\mathbb{Z})$, $\mathbf{b}, \mathbf{x} \in \mathbb{Z}^n$, $c \in \mathbb{Z}$ に対し、 $d = \det(A)$, $\mathbf{h} = \tilde{A}\mathbf{b}$, $c^* = 4d^2c + \mathbf{h}^\top A \mathbf{h}$ とおくと、2 次ディオファントス方程式

$$\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} = c \text{ が整数解 } \mathbf{x} \in \mathbb{Z}^n \text{ を持つ}$$

$\Downarrow$

$$\mathbf{z}^\top A \mathbf{z} = c^* \text{ が } \mathbf{z} \equiv \mathbf{h} \pmod{2d} \text{ を満たす整数解 } \mathbf{z} \in \mathbb{Z}^n \text{ を持つ}$$

この命題により、2 次ディオファントス方程式 $\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} = c$ の解は二次形式 $\mathbf{z}^\top A \mathbf{z} = c^*$ の解の探索に帰着される。以下では二次形式では $\det(A) \neq 0$ と仮定する。

さらに変数の個数が 3 以外の場合は、簡単な手法に還元される。変数が 2 個のときは二次方程式のように式変形と初等的数論のみで平方数判定に帰着し、4 個以上の場合は自由度が大きいため判定が簡単になる。3 個の場合がもっとも難しい。

- 変数が 2 個のとき ($n = 2$) のときは、Fermat に帰属する古典的な二次形式の手法により、以下の判定条件に帰着する。

$$\mathbf{x}^\top A \mathbf{x} = px^2 + qxy + ry^2 = c \text{ が整数解を持つ}$$

$\Downarrow$

$$\text{判別式 } D = q^2 - 4pr \text{ が } \text{mod } 4c \text{ で平方数である}$$

- 変数が 4 個以上のとき ($n \geq 4$) のときは、

$$\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} = c \text{ が整数解を持つ}$$

$\Downarrow$

$$\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} \equiv c \pmod{8(\det(A)c^*)^2} \text{ が解を持つ}$$

により有限探索に帰着される ([15] Proposition 2)。

以下の章は 3 変数の場合 ($n = 3$) に特化するが、数学的手法 (Hasse の原理や整数行列直交群の有限生成元の計算など) は、基本的に $n \geq 3$ の場合に同様に成り立つ。解法は $c^* = 0$ と $c^* \neq 0$ の場合で手法が異なる。

(1) $c^* = 0$ の場合：二次形式 $Q(\mathbf{z}) = \mathbf{z}^\top A \mathbf{z}$ の isotropic 性とは、 $Q(\mathbf{z}) = 0$ となる整数ベクトルが $\mathbf{0}$ 以外に存在しないことをいう。二次形式の isotropic 性の判定は複雑であり章 3. で紹介する。(Hasse の原理を用いる。)

- (a) 二次形式 $\mathbf{z}^\top A \mathbf{z}$ が isotropic な場合： $\mathbf{z} = \mathbf{0}$ のみが解。
- (b) 二次形式 $\mathbf{z}^\top A \mathbf{z}$ が isotropic でない場合 ([15] Proposition 4)： $e = 4\det(A)^2$, $\pi_e: \mathbb{Z} \rightarrow \mathbb{Z}/e\mathbb{Z}$ を自然な射影とする。そのとき $S_Q = \{\mathbf{x} \in \mathbb{Z} \mid Q(\mathbf{x}) = 0\}$ に対し

$$\pi_e(S_Q) = \bigcup_{\lambda \in \mathbb{Z}/e\mathbb{Z}} \lambda \pi_e(\{\mathbf{x} \in \mathbb{Z}^n : \text{primitive} \mid \mathbf{x}^\top A \mathbf{x} \equiv 0 \pmod{e^2}\})$$

(2) $c^* \neq 0$ の場合：二次形式 $Q(\mathbf{x}) = \mathbf{x}^\top A \mathbf{x}$ において

- (a) Q の直交群 $\Gamma_Q = \{B \in GL_n(\mathbb{Z}) \mid \forall \mathbf{x} \in \mathbb{Z}^n. Q(B\mathbf{x}) = Q(\mathbf{x})\}$ の生成元の有限集合 Γ'_Q を計算する [9], [14]。
- (b) $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ において、 $\mathbf{x} \sim_Q \mathbf{y} \Leftrightarrow \exists B \in \Gamma_Q. \mathbf{y} = B\mathbf{x}$ とする。 Γ_Q -軌道 (つまり $\mathbb{Z}^n / \sim_Q$) の完全代表系 T_Q の部分集合 $T'_Q = \{\mathbf{v} \in T_Q \mid Q(\mathbf{v}) = c^*\}$ を算出する。([14] Ch.5)
- (c) 十分に大きい D に対し、 $X = \bigcup_{i=0}^D \{g_1 \cdots g_i \mid g_1, \dots, g_i \in \Gamma'_Q\}$ とする。自然な射影 $\pi_{2d}: M_m(\mathbb{Z}) \rightarrow M_m(\mathbb{Z}/2d\mathbb{Z})$ に対し、 $\pi_{2d}(\Gamma_G)$ は有限群 $GL_n(\mathbb{Z}/2d\mathbb{Z})$ の部分群をなし $\pi_{2d}(X) = \pi_{2d}(\Gamma_Q)$ となる。
- (d) $\mathbf{v} \in T'_Q, g \in X$ に対し $g\mathbf{v} \equiv \mathbf{h} \pmod{2d}$ が成り立つとき $\mathbf{x}^\top A \mathbf{x} + \mathbf{b}^\top \mathbf{x} = c$ の解に等価となる。

3. $c^* = 0$ の場合

3.1 Hasse の原理に基づく isotropic 性判定

問題となるのは、二次形式 $Q(x) = z^T A z$ の isotropic 性 $\exists z (\neq 0) \in \mathbb{Z}^n . Q(z) = 0$ の判定である。

$$\exists z (\neq 0) \in \mathbb{Z}^n . Q(z) = 0 \Leftrightarrow \exists x (\neq 0) \in \mathbb{Q}^n . Q(x) = 0$$

なので $\mathbb{Z}$ 上の議論は $\mathbb{Q}$ 上に帰着される。さらに Hasse の原理

$$\exists x (\neq 0) \in \mathbb{Q}^n . Q(x) = 0$$

$$\Updownarrow$$

$$\exists x (\neq 0) \in \mathbb{R}^n . Q(x) = 0 \wedge \bigwedge_{p:\text{prime}} \exists x (\neq 0) \in \mathbb{Q}_p^n . Q(x) = 0$$

により各 $\mathbb{Q}$ の各完備化 $\mathbb{R}, \mathbb{Q}_p$ 上の判定に帰着する。ここで $\mathbb{R}$ は $\mathbb{Q}$ のユークリッド距離による完備化であり、各素数 p に対し p 進体 $\mathbb{Q}_p$ は $\mathbb{Q}$ の p 進距離による完備化である。 $a, b \in \mathbb{Q}$ に対する p 進距離は、 $a - b = \frac{m}{n} p^k$ (ただし m, n, p は互いに素) となるとき $\|a - b\|_p = 2^{-k}$ による定義される。このとき、

- $\exists x \in \mathbb{R}^n . z^T A x$ の判定は CAD アルゴリズム [11]。
- 素数 p に対し、 $\exists x \in \mathbb{Q}_p^n . x^T A x$ については

$n \geq 5$ のとき 任意の二次形式 $Q(x)$ は $\mathbb{Q}_p$ で isotropic。

$n = 3, 4$ のとき $\mathbb{Q}_p$ 上の古典的な Hilbert 記号の計算に帰着。

二次形式 A を $(GL_n(\mathbb{Q}))$ による基底変換で対角化した A' による二次形式 $Q'(x) = \sum_{i=1}^n a_i x_i^2$ において $c_p(Q') = \prod_{i < j} (a_i, a_j)_p = (-1, -\det(A'))_p$ とする。 $n = 3, 4$ のときに以下が成り立つ。

Q' が isotropic $\Leftrightarrow$

$$\begin{cases} c_p(Q') = (-1, -\det(A'))_p & \text{if } n = 3 \\ \det(A') \notin (\mathbb{Q}_p^\times)^2 \text{ or } c_p(Q') \neq -(-1, -1)_p & \text{if } n = 4 \end{cases}$$

ただし体 K 上の Hilbert 記号とは、 $a, b \in K \setminus \{0\}$ に対し以下のように定義される。

$$(a, b)_K = \begin{cases} 1 & \text{if } \exists (x, y, z) \in K^3 \setminus \{0\} . z^2 = ax^2 + by^2 \\ -1 & \text{otherwise} \end{cases}$$

$K = \mathbb{Q}_p$ のとき $a = p^\alpha u, b = p^\beta v$ (ただし u, v は p と素) とする。奇数 x に対し $\epsilon(x) = (x-1)/2, \omega(x) = (x^2-1)$ とする。

$$(a, b)_p = \begin{cases} (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2 \end{cases}$$

ただし奇素数 p に対し、Legendre 記号は次で定義される。

$$\left(\frac{u}{p}\right) \equiv u^{(p-1)/2} \pmod{p}$$

3.2 二次形式 $z^T A z$ が isotropic でない場合

$A \in O_n(\mathbb{Z})$ かつ $n \geq 3$ のとき、二次形式 $Q(z) = z^T A z$ が isotropic ではないとする。

命題 ([15] : Proposition 4) $e = 4\det(A)^2, \pi_e : \mathbb{Z} \rightarrow \mathbb{Z}/e\mathbb{Z}$ を自然な射影とする。 $S_Q = \{x \in \mathbb{Z} \mid Q(x) = 0\}$ に対し、

$$\pi_e(S_Q) = \bigcup_{\lambda \in \mathbb{Z}/e\mathbb{Z}} \lambda \pi_e(\{x \in \mathbb{Z}^n : \text{primitive} \mid Q(x) \equiv 0 \pmod{e^2}\})$$

この証明には、以下の近似補題を用いる。近似補題は Hensel の補題 [6], [8] に基づく。

近似補題 ([2] Ch.3 Lemma 2.1) $A \in O_n(\mathbb{Z}), n \geq 3, P$ を素数の有限集合、 $\varepsilon (\in \mathbb{R}) > 0$ とする。二次形式 $Q(x) = x^T A x$ において、各 $p \in P$ に対し、 $x_p \in \mathbb{Q}_p^n$ が $Q(x_p) = 0$ を満たすとする。このとき、 $z \in \mathbb{Q}^n$ が存在して、 $Q(z) = 0$ かつ すべての $p \in P$ について $\|z - x_p\|_p < \varepsilon$ 。

$\|z - x_p\|_p < \varepsilon$ は、 z の取り方でいくらでも大きい p の累乗を x_p との公約数に持つことができることを示している。これにより、近似補題から以下の命題が示され、上記の $\pi_e(S_Q)$ の計算法が導かれる。

命題 $x \in \mathbb{Z}^n$ が primitive で $Q(x) \equiv 0 \pmod{e^2}$ ならば、 $Q(y) = 0$ かつ $y \equiv x \pmod{e}$ を満たす $y \in \mathbb{Z}^n$ が存在する。

4. $c^* \neq 0$ の場合 (1) : 二次形式 $Q(x)$ の直交群の生成元の計算

$GL_n(\mathbb{C})$ の部分群で、有限個の多項式の零点集合との共通部分で表わされる群を $\mathbf{Q}$ -群という ($\mathbf{Q}$ -群は代数群の一つである)。 $\mathbf{Q}$ -群 G に対し $G_{\mathbb{R}} = G \cap GL_n(\mathbb{R}), G_{\mathbb{Q}} = G \cap GL_n(\mathbb{Q}), G_{\mathbb{Z}} = G \cap GL_n(\mathbb{Z})$ とする。 $G_{\mathbb{Q}}$ の部分群 Γ で指数 $|G_{\mathbb{Z}} : G_{\mathbb{Z}} \cap \Gamma|, |\Gamma : G_{\mathbb{Z}} \cap \Gamma|$ がともに有限のとき、算術部分群 (Arithmetic subgroup) とよび、以下の性質が知られる。

定理 [9] 算術部分群は有限生成群である。

二次形式 $Q(x) = x^T A x$ の直交群

$$\begin{cases} G_Q &= \{B \in GL_n(\mathbb{C}) \mid \forall x \in \mathbb{Z}^n . Q(Bx) = Q(x)\} \\ \Gamma_Q &= \{B \in GL_n(\mathbb{Z}) \mid \forall x \in \mathbb{Z}^n . Q(Bx) = Q(x)\} \end{cases}$$

において G_Q は $\mathbf{Q}$ -群であり、 Γ_Q は G_Q の算術部分群である。(通常の直交群 $O_n(\mathbb{C})$ も $\mathbf{Q}$ -群であり、 $O_n(\mathbb{Z})$ はその算術部分群である。)

上記定理の原証明 [9] は古典的証明であり、有限生成であっても生成元の計算法は与えていない。さらに仮定として

- Γ が G_F の部分群である
- $g \in G_F$ が $g \in \Gamma$ が判定可能である
- $|G_F : \Gamma|$ の上界が与えられている

を追加した場合の構成的証明は [14] で与えられ、その系として [15] が導かれる。以下、 $\mathbf{Q}$ -群 G 、その算術部分群 Γ と参照して、有限生成系の計算ステップを示す。本章における存在は構成的存在の意味で用い、その計算アルゴリズムを前提とする。 $\mathbf{Q}$ -群の単位元の連結成分を考える際に二つの位相を想定する。Zariski 位相とは、多項式の有限集合の零点集合を閉集合とする位相であり、 $\mathbf{Q}$ -群 G の (Zariski 位相に関する) 単位元の連結成分を G^0 と書く。Euclid 位相とは通常の位相であり、 $\mathbf{Q}$ -群 G の (Euclid 位相に関する) 単位元の連結成分を K により参照する。Zariski 位相で閉集合であれば Euclid 位相でも閉集合であるが、逆は成り立たない。

Q-群は Lie 群 [3] とみなせる。本章では Lie 群においてよく知られる Jordan-Chevalley 分解に似た冪単根基と reductive complement の半直積とする分解を用いる。

以下では、**Q**-群 G の冪単根基 N と reductive component H による分解 $G = N \ltimes H$ の記法を用いる。冪単根基、reductive component については、それぞれ節 4.3、4.4 にて説明する。

4.1 Siegel set

正有理数 $\Delta > 0, t, u > 0$ に対し、 $GL_n(\mathbb{R})$ の部分集合

$$\begin{cases} B_\Delta &= \{g \in SL_n(\mathbb{R}) \mid |g_{ij} - \delta_{ij}| < \Delta\} \\ \mathfrak{S}_{t,u} &= O_n(\mathbb{R}) \cdot A_t \cdot N_u \end{cases}$$

で定義する。ただし、 A_t はすべての対角成分で $0 < a_{ii} < ta_{i+1,i+1}$ が成り立つ対角行列の集合、 N_u は対角成分がすべて 1 でその他の各成分が $|x_{ij}| \leq u$ となる上半三角行列の集合とする。(これは Lie 群の岩澤分解の近傍系に相当する。) $\mathfrak{S}_{t,u} \subset GL_n(\mathbb{R})$ を Siegel set とよび、対応する二次形式を $\mathfrak{S}(t, u)$ で表し Siegel domain とよぶ。Siegel set について次の特徴付けが成り立つ。

定理 ([14] Th.1.6.1)

- (1) $\{g \in GL_n(\mathbb{Z}) \mid \mathfrak{S}_{t,u}g = \mathfrak{S}_{t,u}\}$ は有限。
- (2) $t \geq 2/\sqrt{3}, u \geq 1/2$ ならば $\mathfrak{S}_{t,u} \cdot GL_n(\mathbb{Z}) = GL_n(\mathbb{R})$ 。

4.2 **Q**-群 G の Zariski 位相・Euclid 位相による単位元の連結成分 $G^0 \cdot K$

命題 ([14] Lemma 3.1.3) G を整数係数多項式環のイデアル α により定義される **Q**-群とする。 α の極小素イデアルは有限個であり $\mathfrak{p}_1 = \langle f_{11}, \dots, f_{1r_1} \rangle, \dots, \mathfrak{p}_s = \langle f_{s1}, \dots, f_{sr_s} \rangle$ と表わすとき、単位元を零点とする素イデアルが $\mathfrak{p}_i$ がちょうど一つ存在する。この $\mathfrak{p}_i$ の零点集合を G^0 となる。

したがって、 G^0 の特徴付けはそのような素イデアルを α の準素イデアル分解を計算することに帰着する。さらに $F = \mathbb{C}, \mathbb{R}$ において $|G_F : (G^0)_F|$ が有限であることを知られており、その代表元の計算は以下の方法で順に ℓ を枚挙することで得られる ([14] Algorithm 3.1.5)。

$P_\ell(t_1, \dots, t_\ell) \Leftrightarrow \forall x \in G_F \exists y \in (G^0)_F \cdot \bigvee_{i=1}^\ell x = yt_i$ としたとき、 $\exists t_1, \dots, t_\ell \cdot P_\ell(t_1, \dots, t_\ell)$ は算術的に記述可能であり CAD アルゴリズムにより判定可能である。

この手順で、 $|G_F : (G^0)_F| = \ell$ を得ると同時に、 $t_1, \dots, t_\ell$ の代表元を得る。 $\mathbb{R}$ 内で $\mathbb{Q}$ は稠密であるので、特に $t_i \in GL_n(\mathbb{Q})$ と取ることができる。

命題 ([14] Algorithm 1.4.2, 3.3.5) $G_{\mathbb{R}}$ を (Zariski 位相で) 連結とする。そのとき単位元の (Euclid 位相の) 連結成分 K に対し、指数 $|G_{\mathbb{R}} : K|$ は有界かつ計算可能である。さらに $G_{\mathbb{R}}$ の K による右剰余類の代表元も同時に計算される。

これは松本による以下の定理に基づく。

定理 ([14] Th.3.3.1) $G_{\mathbb{R}}$ は Zariski 位相で連結とする。 K を $G_{\mathbb{R}}$ の単位元の (Euclid 位相での) 連結成分、 D を $G_{\mathbb{R}}$ の (Zariski 位相で) 連結・(実数基底で) 対角化可能・代数的な極大部分群とする。このとき $G_{\mathbb{R}} = K \ltimes D$ 。

すなわち $D \cap GL_n(\mathbb{Z})$ の中で $G_{\mathbb{R}}$ の K に関する右剰余類の代

表元を探す手続きに帰着する。

4.3 G^0 の冪単根基 N に対し $N_{\mathbb{Z}}$ の有限生成系の計算

固有値がすべて 1 の行列を冪単とよび、冪単行列からなる **Q**-群 U を冪単群とよぶ。冪単群 U において以下が知られている ([14] Lemma 1.4.4)。

- $U_{\mathbb{Q}}, U_{\mathbb{Z}}$ は U において (Zariski 位相で) 稠密 (Rosenlicht の定理 [1])。
- $U_{\mathbb{Z}}$ は整数上の基底変換により対角成分が 1 となる上三角行列群とできる。

Q-群 G の冪単根基 $u(G)$ は、極大可解部分群における単位元の (Zariski 位相に関する) 連結成分と冪単行列の共通部分として定義される。冪単根基は定義から $u(G) = u(G^0)$ となる。

Q-群 G を Lie 群とみなしたとき、その Lie 環 $\mathcal{L}(G)$ に対し、

$$\mathcal{L}(u(G^0)) = n(\mathcal{L}(G^0))$$

の関係が知られている ([18] Th.7.1)。ただし、 $n(L)$ は Lie 環 L の冪零イデアルを表わす。これにより、行列の指数関数・対数関数により $u(G^0) = \exp(n(\mathcal{L}(G^0))), n(\mathcal{L}(G^0)) = \log(u(G^0))$ が成り立つ。このとき、Lie 環の冪零性・Lie 群の冪単性により、級数展開が有限の項で打ち切ることが可能なため $\exp, \log$ の計算が可能となる。

上記の性質から G^0 から $u(G)$ を計算するアルゴリズムが導かれる ([14] Algorithm 1.4.5, 3.4.4)。おおまかな手順は

- (1) $\mathcal{L}(u(G^0))$ は $M_n(\mathbb{Q})$ の部分空間なので、その基底から冪零イデアル $n(\mathcal{L}(G^0))$ の基底を計算する。これにより $n(\mathcal{L}(G^0))$ は一次多項式 $P_1, \dots, P_t$ の零点として表現される。
- (2) $n(\mathcal{L}(G^0)) = \mathcal{L}(u(G^0))$ から多項式 $\log^*(X) = -\sum_{i=1}^{n-1} i^{-1}(I_n - X)^i$ と定めると、 $u(G) = u(G^0)$ は $\{(X - 1)^n, P_1(\log^*(X)), \dots, P_t(\log^*(X))\}$ の零点集合と $GL_n(\mathbb{C})$ の共通部分となり、 $u(G)$ の定義多項式が得られる。

命題 ([14] Algorithm 1.5.1, 4.2.1) G を冪単群とする。 $G = G^0$ かつ、正有理数 $\Delta > 0$ が存在して、 $G_{\mathbb{R}} = (G \cap B_\Delta) \cdot G_{\mathbb{Z}}$ が成り立つ。

命題 ([14] Algorithm 1.5.2, 4.2.2) 任意の正有理数 $\delta > 0$ に対し、有限集合 $F_1(\delta) \subseteq GL_n(\mathbb{Z})$ が存在し、 $1 \in F_1(\delta) = F_1(\delta)^{-1}$ かつ $F_1 \supseteq B_\delta^{-1} B_\delta \cap GL_n(\mathbb{Z})$ が成り立つ。

これらに基づき $F_1(\Delta) \cap G_{\mathbb{Z}}$ は $G_{\mathbb{Z}}$ の有限生成系となる ([14] Proposition 1.5.4)。

4.4 G^0 の reductive complement $H_{\mathbb{Z}}$ の有限生成系の計算

Q-群 G が、冪単根基 $u(G) = \{1\}$ のとき reductive という。

Lie 環 $\mathcal{L}(G)$ の Wedderburn 分解に対応して、**Q**-群 G の分解 $G = N \ltimes H$ (ただし N は冪単根基、 H は reductive 部分群) は Borel-Serre による次の補題 ([14] Lemma 3.5.1) から得られる。このとき H を reductive complement という。

補題 **Q**-群 G の冪単根基を N とする。そのとき reductive 部分群 H が存在して、 $G = N \ltimes H$ となる。とくに任意の G の reductive 部分群は N の元により H の部分群と共役となる。

計算アルゴリズムは、[14] Algorithm 1.4.5, 3.5.3 に記述さ

れているが、そのアイデアは冪単根基 $N_{\mathbb{Z}}$ を対角成分が 1 の上三角行列となるように整数基底 $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ をとったとき、 $k_i < k_{i+1}$ かつ $k_j = n$ が存在し、 V_i を $\mathbf{e}_1, \dots, \mathbf{e}_{k_i}$ 、 W_i を $\mathbf{e}_{k_i+1}, \dots, \mathbf{e}_{k_{i+1}}$ がそれぞれはる部分空間で $u \in N_{\mathbb{Z}}$ が $u|_{W_i} = \mathbf{1}|_{W_i}$ 、 $k_j = n$ を満たすものとする。このとき、reductive complement は $G \cap (GL_{k_1}(\mathbb{C}) \times GL_{k_2-k_1}(\mathbb{C}) \times \dots \times GL_{k_j-k_{j-1}}(\mathbb{C}))$ に相当する。共役のための変換は行列計算を多項式として CAD アルゴリズムを用いることで得る。

この手続きに並行して、以下の命題も示される。(これは次節で用いられる。)

命題 ([14] Lemma 1.4.9) ある $\mu \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$ が存在して $(G_{\mathbb{Z}})^{\mu} \subseteq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \subseteq (G^{\mu})_{\mathbb{Z}}$ 。

$\mathbf{Q}$ -群 G の冪単根基はつねに (Zariski 位相で) 連結であるが、reductive complement H は一般には連結ではない。Siegel set $\mathfrak{S}_{t,u}$ に $H_{\mathbb{Z}}$ と有限集合 $F_5 \subseteq GL_n(\mathbb{Z})$ の元を作用させて $H_{\mathbb{R}}$ の被覆とする際、 $\mathfrak{S}_{t,u}$ は (Euclid 位相で) 連結なので、 $H_{\mathbb{R}}$ の (Euclid 位相の) 連結成分 K 、ならびにその右剰余類の代表元 $\{y_i\}$ を考える必要がある。これは節 4.2 にあるように H の H^0 による右剰余類、 H^0 の K の右剰余類の二段階で計算される。

以下に $H_{\mathbb{Z}}$ の有限生成系の計算方法を概説する。

命題 Reductive な $\mathbf{Q}$ -群 H に対し、ある $\xi \in GL_n(\mathbb{R})$ が存在して $\xi^{-1}H_{\mathbb{R}}\xi$ が行列の転置に関して閉じる。

命題 $F_3(t, u) = \{g \in GL_n(\mathbb{Z}) \mid \mathfrak{S}_{t,ug} \cap \mathfrak{S}_{t,u} \neq \emptyset\}$ は有限集合。

このような ξ 、ならびに正有理数 $t, u > 0$ に対する有限集合 $F_3(t, u)$ は CAD アルゴリズムにより計算することができる (それぞれ [14] Algorithm 1.4.3、ならびに 1.6.2 と 4.1.1)。

命題 ([14] Algorithm 1.7.1, 5.3.1) Reductive な $\mathbf{Q}$ -群 H 、正有理数 $t > 2/\sqrt{3}, u > 1/2$ に対し、有限集合 $F_5 \subseteq GL_n(\mathbb{Z})$ と $\xi^{-1}G_{\mathbb{R}}\xi$ を自己共役とする $\xi \in GL_n(\mathbb{R})$ が存在して、 $\Omega = \xi \mathfrak{S}_{t,u}^0 F_5 \cap H_{\mathbb{R}}$ が $\Omega \cdot H_{\mathbb{Z}} = H_{\mathbb{R}}$ を満たす。

命題 ([14] Proposition 5.4.1) Reductive な $\mathbf{Q}$ -群 H に対し $F_5^{-1}F_3F_5 \cap G_{\mathbb{Z}}$ は $H_{\mathbb{Z}}$ を生成する。

この F_5 の計算において、 H の K についての右剰余類の代表元 $\{y_i\}$ が用いられる。

4.5 $G_{\mathbb{Z}}$ の算術部分群 Γ の有限生成系の計算

G を $\mathbf{Q}$ -群、 Γ を G の算術部分群とする。 Γ の生成系の計算過程には以下のステップがある。

- (1) N を G の冪単根基、 H をその reductive complement とし、 $G_{\mathbb{Q}} = N \rtimes H$ と半直積分解し、 N, H を計算する (節 4.3)。
- (2) $N_{\mathbb{Z}}$ の有限生成系 X_1 を計算する (節 4.3)。
- (3) $H_{\mathbb{Z}}$ の有限生成系を X_2 計算する (節 4.4)。
- (4) $(G_{\mathbb{Z}})^{\mu} \subseteq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \subseteq (G^{\mu})_{\mathbb{Z}}$ を満たす $\mu \in GL_n(\mathbb{Q}) \cap M_n(\mathbb{Z})$ を計算する (節 4.4)。
- (5) $A = (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}}$ は有限集合 $Y = (X_1 \cup X_2)^{\mu^{-1}}$ で生成され、かつ $\Gamma^{\mu} \subseteq (G_{\mathbb{Z}})^{\mu} \subseteq A$ が成り立つ。 A の Γ^{μ} に関する右剰余類の集合を T とおくと、 $TYT^{-1} \cap \Gamma^{\mu}$ は Γ^{μ} を生成する ([5] Th.2.7)。

(6) $A \subseteq (G^{\mu})_{\mathbb{Z}}$ から $|T| = |A : (G_{\mathbb{Z}})^{\mu}| \leq |(G^{\mu})_{\mathbb{Z}} : (G_{\mathbb{Z}})^{\mu}|$ 。 $|(G^{\mu})_{\mathbb{Z}} : (G_{\mathbb{Z}})^{\mu}|$ の上界は、鳩の巣原理により $m\mu^{-1} \in M_n(\mathbb{Z})$ となる m に対し $D = m^{n^2} + 1$ (すなわち $GL_n(\mathbb{Z})$ の各要素の $\text{mod } m$ の場合の数) で与えられる。 $W_D(Y) = \bigcup_{i=1}^D Y^i$ とすると $T \subseteq W_D(Y)$ となり、 $W_D(Y) \cap \Gamma^{\mu}$ は Γ^{μ} を生成する。したがって $W_D(Y)\mu^{-1} \cap \Gamma$ は Γ を生成する。

5. $c^* \neq 0$ の場合 (2) : 二次形式 $Q(x)$ の直交群の軌道の計算

二次形式 $Q(x) = x^T A x$ に対し、 G_Q, Γ_Q をそれぞれ $\mathbb{C}, \mathbb{Z}$ 上の Q の直交群とする。 G_Q は $\mathbf{Q}$ -群、 Γ_Q は G_Q の算術部分群である。

$\mathbb{Z}^n$ に同値関係 $\sim_Q$ を $x \sim_Q y \Leftrightarrow \exists B \in \Gamma_Q. y = Bx$ で定める。同値類 $\mathbb{Z}^n / \sim_Q$ の元を Γ_Q -軌道といい、各 Γ_Q -軌道から代表元を 1 つずつとってきて作った集合 T_Q を完全代表系という。

章 4. では Γ_Q の有限生成系 Γ'_Q の計算法を与えた。本章では、 Γ_Q -軌道の完全代表系 T_Q の部分集合のうち

$$T'_Q = \{v \in T_Q \mid Q(v) = c^*\}$$

の計算アルゴリズムを示す ([15] Ch.5)。

5.1 二次形式の $\mathbb{Z}$ -同値性判定

ここで二つの (整数係数) 二次形式 Q, Q' が $\mathbb{Z}$ -同値とは、 $T \in GL_n(\mathbb{Z})$ が存在して、 $Q'(x) = Q(Tx)$ となることをいう。このとき、以下の性質が成り立つ。

定理 ([2] Ch.9 Th.1.1) 整数 $d \neq 0$ に対し、 $d(Q) = \det(A) = d$ となる二次形式 Q の $\mathbb{Z}$ -同値類は有限個、かつ代表元が計算可能。

$\mathbb{Z}$ -同値類の代表元として、ある種の標準形として、

- *Minkowski-reduced* ([2] pp.255) 二次形式：正定値な二次形式の標準形とみなせる。
 - *Hermite-reduced* ([2] pp.286) 二次形式：符号の変換により正定値にしたときに *Minkowski-reduced* な二次形式を含むことをいう。
- をとることができる。(それぞれの正確な定義は [2] にゆずる。)

命題 ([2] Ch.12 Th 1.1) 正定値な二次形式 Q と $\mathbb{Z}$ -同値な *Minkowski-reduced* な二次形式は存在し、かつ高々有限個。

命題 ([2] Ch.13 Lemma 2.1) 二次形式 Q はある *Hermite-reduced* な二次形式と $\mathbb{Z}$ -同値。

二次形式 $Q(x) = x^T A x$ に対し、 $d(Q) = \det(A)$ とする。上記の命題により、

- $d(Q)$ を固定すると、*Hermite-reduced* な二次形式の集合 T_d は有限集合で計算可能 ([2] Ch.13 Th.11.1)。
- 与えられた 2 つの $\mathbb{Z}$ 係数二次形式 Q, Q' が $\mathbb{Z}$ -同値性が判定可能 ($d(Q) \neq d(Q')$ ならば $\mathbb{Z}$ -同値でない。 $d(Q) = d(Q')$ ならば、それぞれ T_d 内の元に還元して比較。[2] Ch.12 Lemma 1.3 と上記の T_d の有限性を用いる)。

5.2 T'_Q の計算

二次形式 Q と整数 $a \neq 0$ に対して、

$$\begin{cases} R_Q(a) &= \{x \in \mathbb{Z}^n \mid Q(x) = a\} \\ R_Q^{(0)}(a) &= \{x \in \mathbb{Z}^n, \text{primitive} \mid Q(x) = a\} \end{cases}$$

と定義すると、 $R_Q(a) = \cup_{r^2|a} rR_Q^{(0)}(ar^{-2})$ が成り立つ。また a を固定したとき、 $R_Q(a)$ は有限個の Γ_Q 軌道からなることが知られている ([2] Ch.9 Lemma 6.1)。 $T \subseteq R_Q(a)$ を有限個の Γ_Q 軌道の代表元として計算する。

以下では $a = c^*$ とする。さらに $r^2|c^*$ なる r を固定して $h = c^*r^{-2}$ と定めて、最初に $T_Q^{(h)} = T_Q \cap R_Q^{(0)}(h)$ を計算する。

Step 1 以下の条件を満たす有限集合 T_1 を構成する。 ([2] Ch.9 Th.1.1 の証明 Ch.9.3 のアルゴリズムを用いる。)

- T_1 は $d(\phi) = h^{n-2}d(Q)$ を満たす $n-1$ 変数二次形式 ϕ からなる。

- 任意の $n-1$ 変数の二次形式 ϕ' に対して ϕ' と $\mathbb{Z}$ -同値な $\phi \in T_1$ が存在する。

Step 2 有限集合 T_2 を $\phi \in T_1, |v_j| \leq h$ に対し、

$$\psi(x) = (hx_1 + v_2x_2 + \cdots + v_nx_n)^2 + \phi(x_2, \dots, x_n)$$

の形をした ψ の集合とする。各 $\psi \in T_2$ に対して ψ が hQ と $\mathbb{Z}$ -同値性を判定する。 ([2] Ch.13.12 のアルゴリズムを用いる。)

Step 3 T_2 の要素のうち、 hQ と $\mathbb{Z}$ -同値なものたちの集合を T_3 とおく。 $\psi \in T_3$ に対して $hQ(B_\psi x) = \psi(x)$ となる $B_\psi \in GL_n(\mathbb{Z})$ を求める。 $T_Q^{(h)} = \{v \mid v \text{ はある } \psi \in T_3 \text{ に対し } B_\psi \text{ の } 1 \text{ 列目}\}$ とする。

以上の Step により $v \in T_Q^{(h)}$ は $Q(v) = h$ を満たすので、 $T'_Q = \cup_{r^2|c^*} rT_Q^{(h)}$ により $T'_Q = \{v \in T_Q \mid Q(v) = c^*\}$ となる。

6. $c^* \neq 0$ の場合 (3) : 求解アルゴリズム

章 4. で得た Γ_Q の有限生成系 Γ'_0 、および章 5. で得た $Q(v) = c^*$ を満たす Γ_Q 軌道の代表元の有限集合 T'_Q を用いて、以下の手順で解を決定する。このとき節 4.5 の手順 (6) と同じ議論で、 Γ_0 の元として長さ D 以下の Γ'_0 の語を考えれば十分である。そのような語の集合を X とする。全ての組み合わせに対し、

- $g \in X, v \in T'_Q$ に対し $gv \equiv h \pmod{2d}$ を判定する。

これが満たされれば解が発見され、なければ解は存在しないことが結論づけられる。

7. 未解決な問題・拡張

もっとも大きな未解決問題は、単一の三次ディオファントス方程式の決定可能性であるが、本稿の二次ディオファントス方程式は二次形式の理論に大きく基づいており、同様な手法の拡張は難しい。特に $x^T Ax$ という行列表現を用いた二次形式の等価変換を整数上の代数群 (整数上の直交行列) として扱う点 [9], [14] は本質的である。

また、二次ディオファントス方程式の求解アルゴリズムという点では、3 変数の場合のみ本質的な困難があり、アルゴリズムの単純化も挑戦すべき課題である。また同様に、計算量評価も課題である。本稿で紹介した求解アルゴリズムは、 $\mathbb{R}$ 上で多項式を解く CAD (Cylindrical Algebraic Decomposition) を多用す

る。CAD アルゴリズムは (変数の個数について) 二重指数関数的だが、用いるのは 3 変数の場合のみなので、二次形式 Q の $\det(A)$ などに関する計算量評価が必要になるであろう。

実用上は二次ディオファントス制約は形式手法において重要である。たとえば、整数上の線形制約 (背景理論が LIA = Linear Integer Arithmetic) を Hoare 論理のベースとする形式手法において、ループ不変式生成は (一般的には決定不能だが) Farkas 補題を用いたヒューリスティックな手法 [12] が一般的である。そのため、単一の二次ディオファントス等式のみならず、不等式制約や線形制約の追加、また制約の個数を変数の個数に基づき制限するなどで決定可能性を得ることができる場合は望ましい。

最後に以下に容易な拡張をあげる。

- 二次ディオファントス不等式制約は、たとえば Lagrange の四平方和定理

任意の自然数は 4 つの整数の平方和で表すことができる。

を用いると、 $x^T Ax + b^T x \geq c$ は、新たな四つの変数 u_1, u_2, u_3, u_4 を用いて $x^T Ax + b^T x + u_1^2 + u_2^2 + u_3^2 + u_4^2 = c$ に還元する。一般に、多項式制約において、等式 (=) より不等式 (>) の方が簡単であり、実際、二次ディオファントス不等式制約については、[19] で計算量評価がなされている。

- 単一の二次ディオファントス等式に (単一とは限らない) 線形等式制約を加えた場合は、線形等式制約に基づく媒介変数表示を用いて、単一の二次ディオファントス等式に帰着する。

文 献

- [1] Borel, A. *Linear Algebraic Groups*. Springer GTM (1969)
- [2] Cassels, J.W.S. *Rational Quadratic Forms*. Academic Press (1978)
- [3] Chevalley, C. *Theory of Lie Groups*. Princeton Univ Press (1947)
- [4] Hartshorne, R. *Algebraic Geometry*. Springer GTM 52 (2000)
- [5] Magnus, W., Karass, A., Solitar, D. *Combinatorial group theory*, Wiley (1966)
- [6] Nagata, M. *Local Rings*, Wiley (1962)
- [7] 中村悠人. 2 次ディオファントス方程式の整数解求解アルゴリズムについて. JAIST 修士論文、2024 年 12 月
- [8] Serre, J.-P. *A Course in Arithmetic*. Springer GTM 7 (1973)
- [9] Borel, A. Harish-Chandra. *Arithmetic subgroups of algebraic groups*. Annals of Math 75(3), 485-535 (1962)
- [10] Chevalley, C. *Algebraic Lie Algebras*. Annals of Math 48(1), 91-100 (1947)
- [11] Collins, G.E. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*. Springer LNCS 32 (1975)
- [12] Colon, M.A., Sankaranarayanan, S. Sipma, H.B. *Linear Invariant Generation Using Non-Linear Constraint Solving*. CAV 2003, Springer LNCS 2725, 420-432 (2003)
- [13] Davis, M. *Hilbert's Tenth Problem is Unsolvable*. AMS Monthly 80(3) 233-269 (1973)
- [14] Grunewald, F.J., Segal, D. *Some General Algorithms. I: Arithmetic Groups*. Annals of Math 112 (3) 531-583 (1980)
- [15] Grunewald, F.J., Segal, D. *How to solve a quadratic equation in integers*. Math Proc Cambridge Phil. Soc. 89(1) 1-5 (1981)
- [16] Matijasevic, J.V. *Enumerable sets are Diophantine*. English translation: Soviet Math. Doklady (11) 354-357 (1970)
- [17] Mostow, G.D. *Self-adjoint groups* Annals of Math 62, 44-55 (1955)
- [18] Mostow, G.D. *Fully reducible subgroups of algebraic groups*. Amer. J. Math. 78, 200-221 (1956)
- [19] Pia, A.D., Dey, S.S., Morinano, M. *Mixed-integer Quadratic Programming is in NP*. Mathematical Programming 162 225-240 (2017)
- [20] Seidenberg, A. *Constructions in algebra*. Trans. AMS 197, 273-313 (1974)

- [21] Tarski, A. *Decision Methods for Elementary Algebra and Geometry*.
University of California Press (1951)