# On algorithms to solve Quadratic Diophantine equations

Yuto Nakamura *

Japan Advanced Institute of Science and Technology

## 1 Introduction

A constraint using a finite number of $n$-variable integer-coefficient polynomials $f_1, \cdots, f_r$:

$$\bigwedge_{1 \le i \le r} f_i(x_1, \cdots, x_m) = 0$$

is called a Diophantine equation. Determining the existence of integer solutions $(x_1, \cdots, x_m) \in \mathbb{Z}^m$ satisfying this is an important problem in number theory and computational theory. If an algorithm exists for this determination, it's called decidable; if not, it's undecidable. It has been shown by [MATI 1970] and [MATI 1971] that when there are no restrictions on the degree of the polynomials or the number of variables, the problem is undecidable, even for a single polynomial. This result is known as the negative solution to Hilbert's Tenth Problem.

One the other hand, It has been shown by Grunwald [GRUN 1981] that the problem is decidable when the constraint consists of only a single quadratic Diophantine equation. The auther surveyed the details of the algorithm presented in [GRUN 1981] in their master's thesis [Nakamura 2024].

Of course, the problem is undecidable for systems of multiple quadratic polynomials.Any polynomial constraint can reduce the apparent degree within the equation by introducing new variables and quadratic expressions (e.g., a new variable $z$ and quadratic expression $xy = z$). This means that, without loss of generality, each polynomial can be assumed to be at most quadratic. However, even in this undecidable case, the speaker showed that the number of natural number solutions $(x_1, \cdots, x_m) \in \mathbb{N}^m$ satisfying the constraint can be expressed by an explicit formula combining real integrals and infinite series([nakamura 2025]).

Chapter 2 of this paper will provide an overview of the survey content from [Nakamura 2024], and Chapter 3 will present a little extension of it. Chapter 4 will provide the counting formula for the number of natural number solutions $(x_1, \cdots, x_m) \in \mathbb{N}^m$ satisfying the constraint $\bigwedge_{1 \le i \le r} f_i(x_1, \cdots, x_m) = 0$, where $f_i$ are quadratic polynomials.

*yewtoe@yahoo.co.jp

## 2 Overview of the algorithm to solve a single quadratic Diophantine equation

Consider the equation

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \tag{1}$$

where $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ represents the quadratic form for the quadratic terms of a single quadratic Diophantine equation, and $L(\boldsymbol{x}) = \boldsymbol{b}^\top \boldsymbol{x}$ represents the linear form for the linear terms.

First, we would like to summarize some simple cases.

- In the case of one variable, solutions can be directly obtained using the quadratic formula for quadratic equations.
- If $A = O$, equation (1) becomes a linear Diophantine equation. Linear Diophantine equations can be solved by an generalized argument of the Euclidean algorithm. The condition for a linear Diophantine equation $b_1x_1 + \cdots + b_mx_m = c$ to have integer solutions is that $c$ must be a multiple of $\mathrm{g.c.d}(b_1, \cdots, b_m)$, which makes it easy to determine the existence of integer solutions. Furthermore, analogous to the Euclidean algorithm, a parametric representation of the solutions can also be obtained (see [Nakamura 2024] 10.1).
- If $\det A = 0$, the number of variables can be reduced by a basis transformation using eigenvectors corresponding to the 0 eigenvalue (see [Nakamura 2024] 10.2).
- If $A$ is positive definite or negative definite, it is easy to narrow down the candidate solutions to a finite number using the spectral norm of the basis transformation $T$ that diagonalizes the quadratic form, such that $Q(T\boldsymbol{x}) = g(\boldsymbol{x}) = \sum_{i=1}^{m} \lambda_i x_i^2$ (see [Nakamura 2024] 10.3).

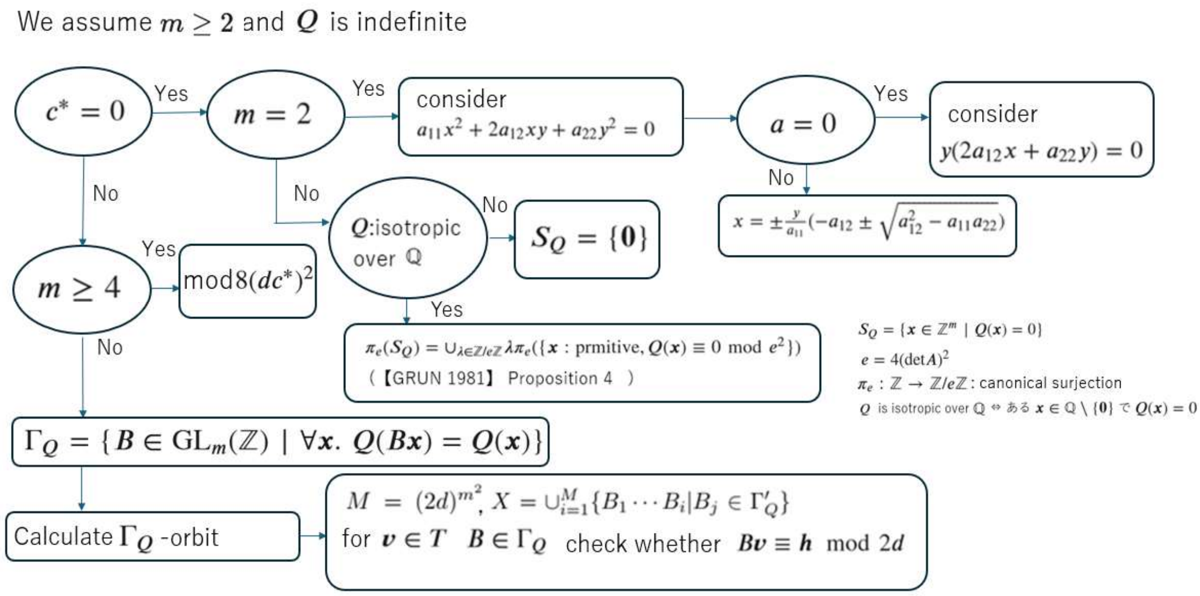
Henceforth, we can assume that the quadratic form has two or more variables, $A$ is regular (non-singular), and $A$ is neither positive definite nor negative definite. The algorithm for determining solvability is described based on the following proposition shown by Grunewald.

**Propositon 2.1.** ([GRUN 1981】]roposition 1 )
Put $d = \det A, \boldsymbol{h} = \tilde{A}\boldsymbol{b}, c^* = 4d^2c + Q(\boldsymbol{h})$,
then the equation (1) has a integer solution $\boldsymbol{x} \in \mathbb{Z}^m \Leftrightarrow \exists \boldsymbol{z} \in \mathbb{Z}^m\, (Q(\boldsymbol{z}) = c^* \wedge \boldsymbol{z} = \boldsymbol{h} \pmod{2d})$
($\tilde{A}$ is the adjugate matrix of $A$ )

*Proof.* $\boldsymbol{x}^\top A\boldsymbol{h} = \boldsymbol{x}^\top A\tilde{A}\boldsymbol{b} = dL(\boldsymbol{x})$, $Q(2d\boldsymbol{x} + \boldsymbol{h}) = 4d^2(Q(\boldsymbol{x}) + L(\boldsymbol{x})) + Q(\boldsymbol{h})$,so
$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \Leftrightarrow Q(2d\boldsymbol{x} + \boldsymbol{h}) = c^*$

□

Here below, we present the rough flow-chart of the decision algorithm.




Obviously, whether $c^* = 0$ is most important.

**$c^* = 0$ case**

We will solve the equation $Q(\boldsymbol{x}) = 0$. In the case of 2 variables, we can obtain a parametric representation of the solutions to the equation by using the quadratic formula and elementary number theory calculations. By projecting this onto mod 2det$A$, we can apply Proposition 2.1. For 3 or more variables, we set $e = 4(\det A)^2$ and compute the projected image $\pi_e(S_Q)$ of the zero set of $Q(\boldsymbol{x})$ modulo $e$. If $Q$ is $\mathbb{Q}$-anisotropic, then $\pi_e(S_Q)$ is only the origin, so we determine whether the quadratic form is $\mathbb{Q}$-isotropic ([Nakamura 2024] Definition 3.35). By Hasse's principle, to make this determination, it suffices to check whether it is isotropic over the real numbers $\mathbb{R}$ and over the $p$-adic numbers $\mathbb{Q}_p$ for each prime $p$ ([CASS 1978] Chapter 6 Theorem 1.1). For the determination over $\mathbb{R}$, we can use the quantifier elimination algorithms proposed in [TAR 1951] and [COLL 1975]. Regular quadratic forms with 5 or more variables are $\mathbb{Q}_p$-isotropic ([CASS 1978] Chapter 6 Corollary 1). In the case of 3 or 4 variables, this can be determined by diagonalizing the quadratic form via basis transformation and calculating Hilbert symbols ([Nakamura 2024] Section 5.3). If $Q(\boldsymbol{x})$ is $\mathbb{Q}$-isotropic, then: $\pi_e(S_Q) = \cup_{\lambda \in \mathbb{Z}/e\mathbb{Z}} \pi_e(\{\boldsymbol{x} \in \mathbb{Z}^m | \boldsymbol{x} : \text{primitive}, Q(\boldsymbol{x}) \equiv 0 \bmod e^2\})$ ([GRUN 1981] Proposition 4).

**$c^* \neq 0$ case**

We compute a finite set of generators $\Gamma'_Q$ for the orthogonal group $\Gamma_Q = \{B \in \mathrm{GL}_m(\mathbb{Z}) | Q(B\mathbf{x}) = Q(\mathbf{x})$ for all $\mathbf{x}\}$, and a subset $T'_Q = \{\mathbf{v} \in T_Q | Q(\mathbf{v}) = c^*\}$ of a complete system of representatives $T_Q$ for the $\Gamma_Q$-orbits. Let $X = \cup_{i=0}^{(2d)^{m^2}+1}\{g_1 \cdots g_i \mid g_1, \ldots, g_i \in \Gamma'_Q\}$. Let $\pi_{2d} : \mathrm{M}_m(\mathbb{Z}) \to \mathrm{M}_m(\mathbb{Z}/2d\mathbb{Z})$ be the natural projection. Then, by the pigeonhole principle, $\pi_{2d}(X) = \pi_{2d}(\Gamma_Q)$. Thus, for each element $g \in X$ and each element $\boldsymbol{v} \in T'_Q$, by checking whether $\boldsymbol{gv}$ is congruent to $\boldsymbol{h}$ modulo $2d$, the solvability of equation (1) can be determined. The orthogonal group $\Gamma_Q$ is an arithmetic subgroup of a $\mathbb{Q}$-group (an algebraic group defined over $\mathbb{Q}$). Therefore, according to the discussions in [BHC 1962] and [GRUN 1980], a finite set of generators can be computed ([Nakamura 2024], Chapters 6-9). In the process of computing the generators of $\Gamma_Q$, it is important to decompose the $\mathbb{Q}$-group $G_Q = \{B \in \mathrm{GL}_m(\mathbb{C}) | Q(B\mathbf{x}) = Q(\mathbf{x}) \text{ for all } \mathbf{x}\}$ into a semidirect product of its unipotent part and its reductive part. This decomposition corresponds to factoring the matrix group into a product of a subgroup of the form $\left\{\begin{pmatrix} 1 & * & * & * \\ 0 & 1 & \ddots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}\right\}$ (a group consisting only of upper triangular matrices with all diagonal entries equal to 1) and a subgroup of the form $\left\{\begin{pmatrix} \mathrm{GL}_{r_1}(\mathbb{C}) & O & O & O \\ O & \mathrm{GL}_{r_2}(\mathbb{C}) & \ddots & O \\ \vdots & \vdots & \vdots & \vdots \\ O & O & \cdots & \mathrm{GL}_{r_k}(\mathbb{C}) \end{pmatrix}\right\}$. Assuming $G_Q$ can be decomposed into a unipotent part $N$ and a reductive part $H$, a finite set of generators can be computed for each of $N \cap \mathrm{GL}_m(\mathbb{Z})$ and $H \cap \mathrm{GL}_m(\mathbb{Z})$. Using these, a set of generators for $\Gamma_Q$ can be computed. $T'_Q$ can be computed according to the discussion in Chapter 5 of [GRUN 1981]. In this process, an algorithm that determines whether two quadratic forms are equivalent under a change of basis by a matrix in $\mathrm{GL}_m(\mathbb{Z})$ is essentially used ([Nakamura 2024], Algorithm 4.25).

## 3 A little extension

If you want to solve quadratic inequality

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) \leq c \tag{2}$$

you can use Lagrange's four square theorem.

**Propositon 3.1.** every natural number can be represented as a sum of four non-negative integer squares

All you have to do is to solve quadratic Diophantine equation

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) + u_1^2 + u_2^2 + u_3^2 + u_4^2 = c \tag{3}$$

You can also solve quadratic Diophantine equation equipped with linear equations.

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \wedge l_1(\boldsymbol{x}) = 0 \wedge \cdots \wedge l_k(\boldsymbol{x}) = 0 \ \ (l_i : \text{linear})$$

As discussed in $A = O$ case,solutions of a linear Diophantine equation is represented in linear form of parameters. So you can substitute solution of each linear equation step by step and you can get a single quadratic Diophantine equation.

# 4 Counting natural number solutions

Consider the system of quadratic Diophantine equations

$$\begin{cases} \sum_{i,j} a_{ij}^{(1)} x_i x_j + \sum_{k=1}^{n} b_k^{(1)} x_k = c^{(1)} \\ \vdots \\ \sum_{i,j} a_{ij}^{(m)} x_i x_j + \sum_{k=1}^{n} b_k^{(m)} x_k = c^{(m)} \end{cases} \tag{4}$$

According to the undecidability of the Hilbert's 10th problem, of course, you cannot solve the Diophantine equations (4) in general. Howevwer, [Nakamura 2025] showed that if using real integrals and infinite series is admitted, you can count the number of natural number solution $\boldsymbol{x} \in \mathbb{N}^n$.

**Theorem 4.1.** ([Nakamura 2025])
Choose $\alpha_{ij}^{(l)}, \beta_k^{(l)}$ s.t. $a_{ij}'^{(l)} = a_{ij}^{(l)} + \alpha_{ij}^{(l)} > 0, b_k'^{(l)} = b_k^{(l)} + \beta_k^{(l)} > 0$. Then, the number of number solution of (4) is

$$\sum_{k_1 \dots k_n, u^{(1)} \dots u^{(m)} \in \mathbb{N}} [\frac{1}{(2\pi)^{2m+n}} \int_0^{2\pi} \cdots \int_0^{2\pi}$$

$$\frac{r^{\sum_{i=l}^m (2c^{(l)} + u^{(l)}) + \sum_{j=1}^n k_j}}{\prod_{k=1}^n \sqrt{\{1 + r^{-2(\sum_{l=1}^m (g_{lk} + h_{lk}) + 1)} (1 - 2r^{(\sum_{l=1}^m (g_{lk} + h_{lk}) + 1)} \cos(\sum_{l=1}^m (g_{lk} t_l + h_{lk} t_{m+n+l}) + t_{m+k}))\}}}$$

$$\times (\cos\{\sum_{l=1}^m \{(c^{(l)} + u^{(l)}) t_l + u^{(l)} t_{m+n+l}\} + \sum_{j=1}^n k_j t_{m+j}$$

$$- \sum_{k=1}^n \arcsin(\frac{r^{-(\sum_{l=1}^m (g_{lk} + h_{lk}) + 1)} \sin(\sum_{l=1}^m (g_{lk} t_l + h_{lk} t_{m+n+l}) + t_{m+k})}{\sqrt{\{1 + r^{-2(\sum_{l=1}^m (g_{lk} + h_{lk}) + 1)} (1 - 2r^{(\sum_{l=1}^m (g_{lk} + h_{lk}) + 1)} \cos(\sum_{l=1}^m (g_{lk} t_l + h_{lk} t_{m+n+l}) + t_{m+k}))\}}})\})$$

$$dt_1 \cdots dt_{2m+n}]$$

where $g_{lj} = \sum_{i=1}^n a_{ij}'^{(l)} k_i + b_j'^{(l)}, h_{lj} = \sum_{i=1}^n \alpha_{ij}^{(l)} k_i + \beta_j^{(l)}$

# 5 Future works

It doesn't seem that you can apply the result mentioned earlier to the case quadratic Diophantine equation equipped with linear constraints including linear inequalities.

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \wedge l_1(\boldsymbol{x}) = 0 \wedge \cdots \wedge l_k(\boldsymbol{x}) = 0 \wedge \wedge l_1'(\boldsymbol{x}) \leq 0 \wedge \cdots \wedge l_{k'}'(\boldsymbol{x}) \leq 0 \ \ (l_i, l_j' : \text{linear})$$

Theory of convex polytope shows that the solution of system of linear inequality is represented in the form $\boldsymbol{x} = \sum_{i=1}^l = \alpha_i \boldsymbol{v}_i$ where $\boldsymbol{v}_i$ are constant vectors and $\alpha_i \mathbb{N}$ are parameters([Loera 2013]). We want to construct an algorithm to solve single quadratic equation in natural number. [Pia 2017] showed that quadratic inequality case

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) \leq c \wedge l_1(\boldsymbol{x}) = 0 \wedge \cdots \wedge l_k(\boldsymbol{x}) = 0 \wedge \wedge l_1'(\boldsymbol{x}) \leq 0 \wedge \cdots \wedge l_{k'}'(\boldsymbol{x}) \leq 0 \ \ (l_i, l_j' : \text{linear})$$

is decidable. Pia combines algorithms to solve QP(continuous relaxation of (2)) and linear integer programing. We want to explore extension of Pia's result to the case with two quadratic inequalities since there exists a concise algorithm to solve continuous relaxation of this. If we succeed in this extension, this become alternative solution to $c^* \neq 0, m = 2, 3$ case in a single Diophantine equation.
Decidability of cubic Diophantine equations is one of the most difficult open problems. Since cubic polynomials don't satisfy Hasse principle, even specific cases (e.g. elliptic curves) demands high-level knowledge of number theory.This is one example of big result in cubic Diophantine equations

**Propositon 5.1.** (Siegel's theorem)
Let $C : F(x, y) = 0$ be non-singular curve defined by a cubic polynomial. Then $C$ has has at most finite integer points.

If $\nu$ variable $\delta$ th-degree Diophantine equations are undecidable, such $(\nu, \delta)$ is called "universal pair". In general, there is a trade-off between $\nu$ and $\delta$. A major method to explore universal pairs is to explore Diophantine equation that can simulate universal Turing machine. [JONE 1982] surveys about universal pairs.

# Reference

[GRUN 1981] Grunewald et.al. "How to solve a quadratic equation in integers" Mathematical Proceedings of the Cambridge Philosophical Society 89 (1) pp 1-5, 1981
[CASS 1978] Cassels "RATIONAL QUADRATIC FORMS" Academic Press London, 1978
[Nakamura 2024]Nakamura "On algorithms to solve Quadratic Diophantine equation" Master thesis, Japan Advanced Institute of Science and Technology 2024
(https://dspace02.jaist.ac.jp/dspace/handle/10119/19420)
[GRUN 1980] Grunewald et.al. "Some General Algorithms. I: Arithmetic Groups" Annals of Mathematics 112 (3) pp 531-583 , 1980
[MATI 1970] Matijasevic J.V. "Enumerable sets are Diophantine" English translation: Soviet Math. Doklady, 11 pp 354-357,1970
[MATI 1971] Matijasevic J.V. "Diophantine representation of enumerable predicates" (Russian) Izv. Akad. Nauk SSSR, Ser. Mat. 35 pp 3-30,1971
[TAR 1951]Tarski "Decision Methods for Elementary Algebra and Geometry." Berkeley: Univ.of California Press, 1951.
[COLL 19753] Collins "Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition" ,LNCS 32. Springer Verlag, 1975.
[DAVI 1973] M.Davis "Hilbert's Tenth Problem is Unsolvable" The American Mathematical Monthly, 80 (3) 233-269, 1973
[BHC 1962] Borel, Chandra "Arithmetic subgroups of algebraic groups" Ann of Math, 75, pp485-535,
[SIL 1992] Silverman, Tate "Rational Points on Elliptic Curves" springer, 1992
[JONE 1982] Jones "Universal Diophantine equation". THE JOURNAL OF SYMBOLIC LOGIC Volume 47 Number 3, 1982

[Lasserre 2001] Lasserre, Zeron, 2001 ”On counting integral points in a convex rational polytope”, Mathematics of Operations Research Vol. 28, No. 4 (Nov., 2003), pp. 853-870

[Pia 2017] Pia et.al. ”Mixed-integer Quadratic Programming is in NP”. Mathematical Programming 162 225-240, 2017

[Loera 2013] De Loera, Hemmecke, Köppe ”Algebraic and Geometric Ideas in the Theory of Discrete Optimization” , SIAM, 2013

[Nakamura 2025] 中村 ”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
(On algorithms to solve Quadratic Diophantine equations)” Proceedings of MATHSCI FRESHMAN SEMINAR 2025, forthcoming