



A mesh algorithm for principal quadratic forms

Agnieszka Polak^{1*}

¹*Faculty of Mathematics and Computer Science, Nicolaus Copernicus University,
Chopina 12/18, 87-100 Toruń, Poland*

Abstract – In 1970 a negative solution to the tenth Hilbert problem, concerning the determination of integral solutions of diophantine equations, was published by Y. W. Matiyasevich. Despite this result, we can present algorithms to compute integral solutions (roots) to a wide class of quadratic diophantine equations of the form $q(x) = d$, where $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is a homogeneous quadratic form. We will focus on the roots of one (i.e., $d = 1$) of quadratic unit forms ($q_{11} = \dots = q_{nn} = 1$). In particular, we will describe the set of roots \mathcal{R}_q of positive definite quadratic forms and the set of roots of quadratic forms that are principal. The algorithms and results presented here are successfully used in the representation theory of finite groups and algebras. If q is principal (q is positive semi-definite and $\text{Ker } q = \{v \in \mathbb{Z}^n ; q(v) = 0\} = \mathbb{Z} \cdot \mathbf{h}$) then $|\mathcal{R}_q| = \infty$.

For a given unit quadratic form q (or its bigraph), which is positive semi-definite or is principal, we present an algorithm which aligns roots \mathcal{R}_q in a Φ -mesh. If q is principal ($|\mathcal{R}_q| < \infty$), then our algorithm produces consecutive roots in \mathcal{R}_q from finite subset of \mathcal{R}_q , determined in an initial step of the algorithm.

1 Introduction

In 1900 during the International Congress of Mathematicians in Paris David Hilbert presented 23 problems, known today as Hilbert problems. One of those problems was The Tenth Hilbert Problem, which consists in finding a general procedure for solving any diophantine equation, i.e., a polynomial with the integral coefficients in which only integral variables are allowed. This problem had been open for many years until Y. W. Matiyasevich published its negative solution in 1970 [1]. Despite the result of Matiyasevich, it is possible to algorithmically describe the roots for selected classes of diophantine equations.

*apolak@mat.umk.pl

We denote by \mathbb{Z} the ring of integers, by \mathbb{N} the set of non-negative integers. Given $n \geq 1$, we denote by $\mathbb{M}_n(\mathbb{Z})$ the \mathbb{Z} -algebra of all square n by n matrices with coefficients in \mathbb{Z} .

In our paper we consider quadratic diophantine equations, i.e., those of the form $q(x) = d$, where $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is an integral quadratic form and $d \in \mathbb{Z}$. The problem of deciding if a quadratic diophantine equation has solution in \mathbb{Z}^n or not is NP-complete for $n \geq 2$, as shown by Manders and Adleman in 1978 [2]. We focus on unit forms, i.e., quadratic integral forms, in which $q_{11} = \dots = q_{nn} = 1$.

In Sections 2 and 3 an integral quadratic form, positive definite forms and positive semi-definite forms are defined. A number of criteria coupled with algorithms is recalled, which allows to decide if a given form q is positive definite or positive semi-definite. These criteria are utilized in a mesh algorithm for the principal form in Section 5. We show how to encode q using a non-symmetric Gram matrix or a bigraph of q . By a poset $I=(I, \preceq)$ we mean a finite set I together with a partial order relation \preceq . Given a finite poset I we study an integral quadratic form of I defined by the incidence matrix $C_I \in \mathbb{M}_n(\mathbb{Z})$. In Section 4 the set of roots of a unit form is defined. We present a theorem which allows to check if the set of all roots \mathcal{R}_q of a unit form q is finite. If q is principal (i.e., q is semi positive-definite and $\text{Ker } q = \{v \in \mathbb{Z}^n; q(v) = 0\} = \mathbb{Z} \cdot \mathbf{h}$) then \mathcal{R}_q is infinite. Next Φ -mesh, Φ -orbit and Φ -mesh graph are defined.

The aim of this paper is to present a Φ -mesh algorithm which, for a given principal quadratic form (or its bigraph), returns a part of the Φ -mesh graph. The vertices of this graph are labelled by the roots of \mathcal{R}_q . From the part of a Φ -mesh graph one can generate a complete Φ -mesh graph by means of simple operations (i.e., adding or subtracting the roots) and as a results the whole set \mathcal{R}_q of all roots can be produced.

2 Integral quadratic forms

By an integral quadratic form we mean a map $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ defined by the formula $q(x) = \sum_{i=1}^n q_{ii}x_i^2 + \sum_{1 \leq i < j \leq n} q_{ij}x_ix_j$, where $q_{ij} \in \mathbb{Z}$ and $i, j \in \mathbb{N}$. We are mainly concerned with unit forms, i.e., forms satisfying $q_{11} = \dots = q_{nn} = 1$. One way of unique encoding of an integral quadratic form is by the non-symmetric Gram matrix. The quadratic form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$, defined by the formula $q(x) = q(x_1, \dots, x_n) = \sum_{i=1}^n q_{ii}x_i^2 + \sum_{1 \leq i < j \leq n} q_{ij}x_ix_j$, $q_{ij} \in \mathbb{Z}$, is associated with the non-symmetric Gram matrix

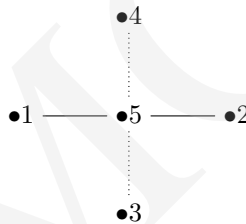
$$\tilde{G}_q = \begin{pmatrix} q_{11} & q_{12} & \dots & q_{1n} \\ 0 & q_{22} & \dots & q_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & q_{nn} \end{pmatrix} \in \mathbb{M}_n(\mathbb{Z}),$$

in which $q_{ij} \in \mathbb{Z}$ for $j = 1, \dots, n$. Note that $q(x) = x \cdot \check{G}_q \cdot x^{tr} = x \cdot G_q \cdot x^{tr}$, where $G_q = \frac{1}{2}[\check{G}_q + \check{G}_q^{tr}]$ is the symmetric Gram matrix of q . Another way of unique encoding of a unit form is by the so-called bigraph.

Definition 1. Let $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be a unit quadratic form given by $q(x) = \sum_{i=1}^n q_{ii}x_i^2 + \sum_{1 \leq i < j \leq n} q_{ij}x_ix_j$. By a bigraph we understand a graph $B = (B_0, B_1)$, where B_1 contains both solid and dashed edges. A bigraph for q contains n vertices and satisfies:

- (a) $|q_{ij}|$ is the number of solid edges connecting i and j , if $q_{ij} < 0$,
- (b) $|q_{ij}|$ is the number of dashed edges connecting i and j , if $q_{ij} > 0$,
- (c) $1 - q_t$ is the number of loops in a vertex t .

Example 1. For a given bigraph



its integral quadratic form is

$$q(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - x_1x_5 - x_2x_5 + x_4x_5 + x_3x_5,$$

and its non-symmetric Gram matrix is as follows: $\check{G}_q = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. The

reader may verify that $q(x) = x \cdot \check{G}_q \cdot x^{tr}$.

Definition 2. By a finite partially ordered set (or a poset) we mean a pair (I, \preceq) where $I = \{a_1, \dots, a_n\}$ is a finite set and \preceq is a binary relation on I with the following properties:

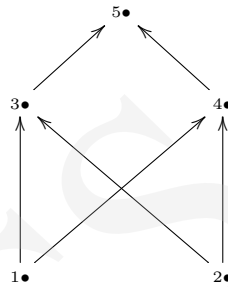
- (a) $j \preceq j$, for any $j \in I$ (reflexivity),
- (b) if $i \preceq j$ and $j \preceq k$, then $i \preceq k$ (transitivity),
- (c) if $i \preceq j$ and $j \preceq i$, then $i = j$ (antisymmetry).

Various quadratic forms can be investigated for posets [3], [4]. In this work we are concerned with one of them, the so-called quadratic form of a poset. Let $I \equiv (I, \preceq)$ denote a poset, for which $|I| = n$. An incidence matrix of I is defined as

$$C_I = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix} \in \mathbb{M}_n(\mathbb{Z}), \text{ where } n = |I| \text{ and } c_{ij} = \begin{cases} 0, & \text{if } i \not\preceq j \\ 1, & \text{if } i \preceq j \end{cases}$$

for any $i, j \in I$. An integral quadratic form of a poset $q_I : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ of a given poset I is defined with the formula $q_I(x) = x \cdot C_I \cdot x^{tr}$, where $C_I = [c_{ij}] \in \mathbb{M}_n(\mathbb{Z})$.

Example 2. Let I be the following poset:



The incidence matrix of I is then

$$C_I = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and the quadratic form of this poset is $q_I(x) = x \cdot C_I \cdot x^{tr} = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_1x_5 + x_2x_5 + x_3x_5 + x_4x_5$.

3 Positive definite forms and positive semi-definite forms

In this section we define the notions of a positive definite quadratic form, a positive semi-definite quadratic form, and we present the algorithms to decide if a given form is positive definite (positive semi-definite), or not.

Definition 3. A form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is called:

- (a) positive definite, if $q(v) > 0$ for every $0 \neq v \in \mathbb{Z}^n$,
- (b) positive semi-definite, if $q(v) \geq 0$ for every $v \in \mathbb{Z}^n$.

We now recall the Sylvester criterion, from which there follows an algorithm that can be used to verify if a given form is positive definite, or not.

Theorem 1. A quadratic and symmetric form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is positive definite if and only if its symmetric Gram matrix $G_q = [\hat{q}_{ij}]$ satisfies the following conditions of Sylvester:

$$\hat{q}_{11} > 0, \det \begin{pmatrix} \hat{q}_{11} & \hat{q}_{12} \\ \hat{q}_{21} & \hat{q}_{22} \end{pmatrix} > 0, \dots, \det \begin{pmatrix} \hat{q}_{11} & \dots & \hat{q}_{1s} \\ \vdots & \dots & \vdots \\ \hat{q}_{s1} & \dots & \hat{q}_{ss} \end{pmatrix} > 0, \det G_q > 0, \text{ for } 2 \leq s \leq n.$$

As the reader will note, it suffices to check the sign of n determinants. We have therefore an algorithm that checks the positive definiteness of a form in $\mathcal{O}(n^4)$ steps.

Theorem 2. A quadratic form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is positive semi-definite if and only if the following inequality holds for the symmetric Gram matrix $G_q = [\widehat{q}_{ij}]$:

$$\det \begin{pmatrix} \widehat{q}_{i_1 i_1} & \cdots & \widehat{q}_{i_1 i_r} \\ \vdots & \ddots & \vdots \\ \widehat{q}_{i_r i_1} & \cdots & \widehat{q}_{i_r i_r} \end{pmatrix} \geq 0,$$

for every $r = \{1, \dots, n\}$ and $1 \leq i_1 < \dots < i_r \leq n$.

The following algorithm tests if a given \check{G}_q is positive semi-definite (see Appendix for explanation of the Maple procedures used).

Algorithm 1. Generalized Sylvester Criterion

Require: \check{G}_q – a non-symmetric Gram matrix of q .

Ensure: 1 if q is positive semi-definite; 0 otherwise.

1. $n \leftarrow \text{coldim}(\check{G}_q)$
2. $\text{Gram} \leftarrow (\check{G}_q + \check{G}_q^{tr})$
3. $L \leftarrow \text{choose}(n)$
4. **for** $i = 2$ to $\text{nops}(L)$ **do**
5. **if** $\det(\text{submatrix}(\text{Gram}, L[i], L[i])) < 0$ **then**
6. **return** 0
7. **end if**
8. **end for**
9. **return** 1

4 The set of all roots of a unit form

In this section we define an integral root of a given form q , a set of all roots of q , and we give a theorem which decides when this set is finite. It follows from this theorem that \mathcal{R}_q is infinite for q in a principal form. A possible application of integral quadratic forms can be introduced by a primitive economic model, where n manufacturers produce goods of values v_1, \dots, v_n , and interchange those goods between themselves when needed. A quadratic form q is therefore a profit function. One can consider a set of all vectors (roots) v for which there is no loss, i.e., $q(v) \geq 0$, or for which the profit equals d (i.e., $q(v) = d$). We are interested in the cases of $d = 1$ and $d = 0$.

Definition 4. Let $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be an integral quadratic form.

- (a) A root of q is a vector $v \in \mathbb{Z}^n$ such that $q(v) = 1$.
- (b) The set $\mathcal{R}_q = \{v \in \mathbb{Z}^n; q(v) = 1\}$ is a set of all roots of q .
- (c) The set $\mathcal{R}_q(0) = \{v \in \mathbb{Z}^n; q(v) = 0\}$ is a kernel of q , denoted by $\text{Ker } q$.

The kernel of q can be calculated by the Lagrange algorithm, described in detail in [5].

Definition 5. A form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ is called principal, if

- (a) q is positive semi-definite,
- (b) its kernel has the form $\text{Ker } q = \{v \in \mathbb{Z}^n ; q(v) = 0\} = \mathbb{Z} \cdot \mathbf{h}_q$, where $0 \neq \mathbf{h}_q \in \mathbb{Z}^n$.

If q is principal and $\text{Ker } q = \mathbb{Z} \cdot \mathbf{h}$, then there exists $s \in \{1, \dots, n\}$ such that $h_s = 1$ or $h_s = -1$ [5].

Theorem 3. Let $n \geq 2$ and $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be a unit form. The set \mathcal{R}_q is finite if and only if q is positive definite.

Proof Can be found in [6].

At follows from the above theorem $|\mathcal{R}_q| = \infty$ for q in a principal form (since it is not positive definite). In the case q is positive definite, the set \mathcal{R}_q is finite and can be obtained with a restrictively counted algorithm, see [7] for a detailed description.

5 Φ -mesh, Φ -orbit, and Φ -mesh graphs

In this section we define a Φ -mesh, a Φ -orbit and a Φ -mesh graph, and we present a mesh algorithm, which is the main purpose of this work.

Definition 6. Let $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be a unit form defined by the formula $q(x) = x \cdot \check{G}_q \cdot x^{tr}$, where \check{G}_q is a non-symmetrix Gram matrix and $\det \check{G}_q \neq 0$.

- The Coxeter matrix of q is defined as $\text{Cox}_q := -\check{G}_q \cdot \check{G}_q^{-tr} \in \mathbb{M}_n(\mathbb{Z})$,
- The Coxeter transformation of q is a homomorphism $\Phi_q : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ of the \mathbb{Z}^n group, defined by the formula $\Phi_q(x) = x \cdot \text{Cox}_q$.

Definition 7. Let $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be a unit form, $\Phi_q : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ be the Coxeter transformation of q . Let $\mathcal{R}_q = \{v \in \mathbb{Z}^n ; q(v) = 1\}$ be the set of integral roots of the form q . By the Φ_q -orbit of a vector $v \in \mathcal{R}_q$ we mean the set $\Phi_q\text{-Orb}(v) = \Phi_q\text{-}\mathcal{O}(v) = \{\Phi_q^m(v)\}_{m \in \mathbb{Z}}$.

A Φ_q -orbit of a vector $v \in \mathcal{R}_q$ will be visualised as an infinite planary graph

$$\dots \xrightarrow{\Phi(v)^{-2}} \Phi(v)^{-1} \xrightarrow{\Phi(v)^{-1}} v \xrightarrow{\Phi(v)} \Phi(v) \xrightarrow{\Phi(v)^2} \dots$$

in the Euclidean plane \mathbb{R}^2 . It can be shown that for q positive definite, a Φ_q -orbit is finite for arbitrary $v \in \mathcal{R}_q$.

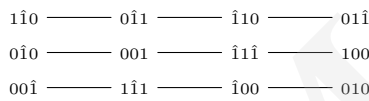
Example 3. Let I be the following poset:

$$\bullet_1 \longrightarrow \bullet_2 \longleftarrow \bullet_3 \dots$$

A quadratic form of I is of the form $q_I(x) = x \cdot C_I \cdot x^{tr} = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3$, and the Coxeter matrix is

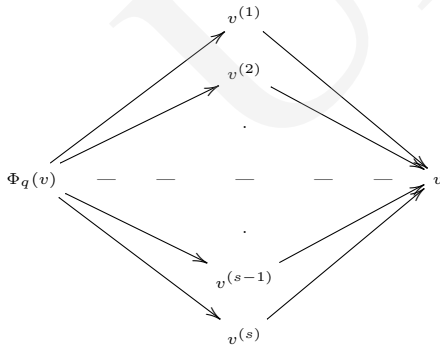
$$Cox = -C_I \cdot C_I^{-tr} = - \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ -1 & 1 & -1 \end{pmatrix}.$$

- Restriction on the coordinates: $|x_1| \leq 1, |x_2| \leq 1, |x_3| \leq 1$,
- $\mathcal{R}_{q_I} = \{[1,-1,0], [0,-1,1], [-1,1,0], [0,1,-1], [0,-1,0], [0,0,1], [-1,1,-1], [1,0,0], [0,0,-1], [1,-1,1], [-1,0,0], [0,1,0]\}$
- $|\mathcal{R}_{q_I}| = 12$,
- \mathcal{R}_q can be aligned in the following three orbits (each of which contains 4 roots):

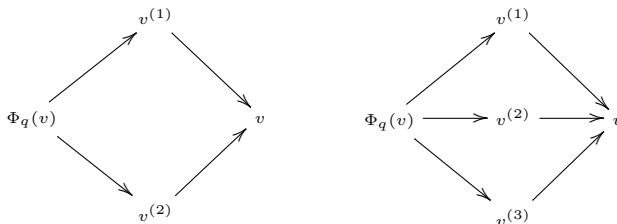


Definition 8. Let $\Phi_q : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ will be a non-trivial group automorphism. A Φ_q -mesh is composed of the set of vectors $v, \Phi_q(v), v^{(1)}, \dots, v^{(s)}$ for any $2 \leq s \in \mathbb{N}$, satisfying:

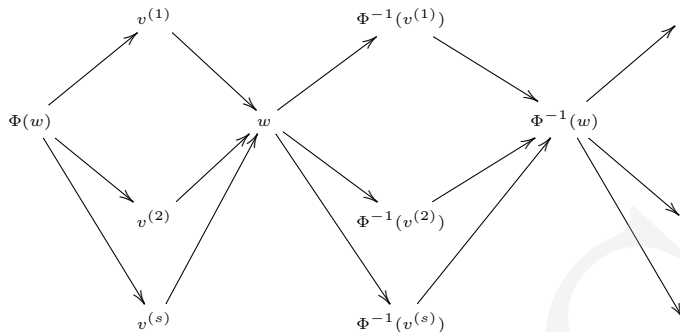
- (a) $v + \Phi_q(v) = v^{(1)} + \dots + v^{(s)}$.
- (b) Each of the vectors $v, v^{(1)}, \dots, v^{(s)}$ is situated in another Φ_q -orbit. The following picture is a way of visualizing a Φ_q -mesh:



In our work we are particularly interested in the meshes of orders two and three, i.e., the meshes of the following form



Then the Φ -mesh graph of \mathcal{R}_q consists of all Φ -orbits of vectors $w \in \mathcal{R}_q$ aligned in Φ -meshes in a way that a convex subgraph of the Φ -mesh graph, containing a Φ -orbit of any $w \in \mathcal{R}_q$, is composed of Φ -meshes and assumes the following shape:

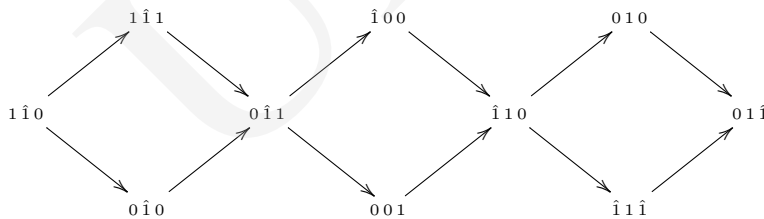


We refer the reader to [5] for a precise definition. It appears that if q is positive definite, then the Φ -mesh graph is connected and finite. On the other hand, if q is principal, then it splits into three connected mesh graphs.

Example 4. Let I be the following poset.



\mathcal{R}_q can be aligned in 3 orbits $\mathcal{O}_1 = [[0, 0, -1], [1, -1, 1], [-1, 0, 0], [0, 1, 0]]$, $\mathcal{O}_2 = [[0, -1, 0], [0, 0, 1], [-1, 1, -1], [1, 0, 0]]$, $\mathcal{O}_3 = [[1, -1, 0], [0, -1, 1], [-1, 1, 0], [0, 1, -1]]$, from which the following mesh graph can be composed:



Definition 9. Let $\check{G}_q \in \mathbb{M}_n(\mathbb{Z})$ be a non-symmetric Gram matrix of q , satisfying $\det \check{G}_q = 1$ or $\det \check{G}_q = -1$. Let $\Phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ be a Coxeter transformation defined by this matrix. If a quadratic form $q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$, defined with the formula $q(x) = x \cdot \check{G}_q \cdot x^{tr}$, is principal, and the kernel is of the form $\text{Ker } q = \mathbb{Z} \cdot \mathbf{h}$, then there exists a natural number $c \geq 1$ and a group homomorphism $\partial_q : \mathbb{Z}^n \longrightarrow \mathbb{Z}$, yielding

$$\Phi^c(x) = x + \partial_q(x) \cdot \mathbf{h}$$

for any $x \in \mathbb{Z}^n$. Minimal c will be called a reduced Coxeter number of q , and denoted by \check{c}_q . ∂_q will be called a defect of the Coxeter transformation Φ or a defect of q .

An algorithm to compute a defect of a given q can be found in [5]. If q is principal, then its Φ -mesh graph for \mathcal{R}_q is the union of three disjoint connected Φ -mesh graphs, consisting of negative-defect vectors, positive-defect vectors, and zero-defect vectors, respectively. A mesh graph for $w \in \mathcal{R}_q$ with a negative defect can be constructed from

the one for $v \in \mathcal{R}_q$ with a positive defect, replacing v with $-v$. The zero-defect roots of a principal quadratic form q , form a finite Φ -mesh graph together with a vector $\mathbf{h} \in \text{Ker } q$. We now present the mesh algorithm for principal forms.

Algorithm 2. The mesh algorithm for a principal form

Require: \check{G}_q - a non-symmetric Gram matrix of q and k - a numeric bound on the coordinate (for infinite orbits).

Ensure: A set of meshes for negative-defect roots, from which a whole Φ -mesh graph can be produced, labelled with all negative-defect roots.

1. Check if q is principal (generalized Sylvester criterion and the Lagrange algorithm [5]). If not, then stop.
2. Calculate $h = (h_1, \dots, h_n) \in \text{Ker } q$ by the Lagrange algorithm.
3. Calculate the defect ∂_q for q [5].
4. Find $s \in \{1, \dots, n\}$, for which $h_s \in \{-1, 1\}$.
5. Generate $\mathcal{R}_{q'}$ for $q'(x_1, \dots, x_n) = q(x_1, \dots, x_{s-1}, 0, x_{s+1}, \dots, x_n)$ (Restrictively counting algorithm [7]).
6. Take $w \in \mathcal{R}_{q'}$ such that $\partial_q(w) < 0$ and add to $\partial\mathcal{R}_q$. Let $O = \{\}$.
7. Calculate the Coxeter matrix $Cox = -\check{G}_q \cdot \check{G}_q^{-tr}$. {This gives the Φ .}
8. Align $v \in \partial\mathcal{R}_q$ in Φ -orbits taking into account the bound k on the coordinates.
9. Determine the meshes of orders two and three, and add them to O .
10. If necessary, move the meshes in O so that they border.
11. **return** O .

References

- [1] Matiyasevich Y., Enumerable sets are Diophantine, Doklady Akademii Nauk ZSSR (1970): 279.
- [2] Adleman L. and Manders K., Diophantine complexity (Proc. 17th IEEE Symposium on Foundations of Computer Science) Proc. IEEE (1976): 81.
- [3] Simson D., Linear Representations of Partially Ordered Sets and Vectors Space Categories, Algebra, Logic and Applications 4 (1992).
- [4] Simson D., Integral bilinear forms, Coxeter transformations and Coxeter polynomials of finite posets, Linear Algebra and its Applications (2010); doi:10.1016/j.laa.2010.03.041.
- [5] Simson D., Mesh algorithm for solving principal diophantine equations, preprint (2009).
- [6] Marczak G., Polak A., Simson D., P-critical integral quadratic forms and positive unit forms: An algorithmic approach, Linear Algebra and its Applications (2010); doi:10.1016/j.laa.2010.06.052.
- [7] Simson D., Mesh geometries of root orbits of integral quadratic forms, J. Pure Appl. Algebra (2010); doi:10.1016/j.jpaa.2010.02.029.