Правительство Российской Федерации

**Федеральное государственное автономное
образовательное учреждение
высшего профессионального образования
“Национальный исследовательский университет
Высшая школа экономики ”**

Факультет математики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему

“Умножение кватернионных решеток”

Студент группы 4.11.1
Дурьев Эдуард Сергеевич

Руководитель ВКР
Доктор физико-математических наук, профессор,
Тиморин Владлен Анатольевич

Москва, 2013

Abstract

This paper considers sets values of integer quadratic forms and integer lattices. We start with discussing Gauss composition for integer positive definite quadratic forms of two variables and show its equivalence to the lattice multiplication. Our main goal is to generalize this theory to quadratic forms of four variables using the structure of quaternions.

Contents

Introduction

The initial question is to describe the set of values of a given integer positive definite quadratic form of two integer variables? It happens that for some forms this set can be easily described explicitly, but more frequently one faces difficulties in finding this set. Gauss proposed an approach that makes the answer to the question feasible. The structure of complex numbers and lattices lie in the core of this approach. Fortunately, the skew field of quaternions has a similar structure, and one can expect that the result of Gauss can be generalized with their use.

The main purpose of this paper is pointing out to the existing results in this subject and research of their generalizations. We are going to introduce Gauss approach, give the lattice representation of the problem, and make basic definitions and notions.

Structure of the paper. We start the paper from the general description of the initial problem. The first section is divided into three subsections. The first and the second subsections, mainly, present basic definitions and notions, the third one is dedicated to the Gauss composition. In the last section we present the main question of the research and approaches used to deal with it. Final part summarizes the main points of the reasearch and introduces the strategy which is expected to be helpful in achieving the goal of the investigation.

Keywords. Integer quadratic forms, integer lattices, complex numbers, quaternions, Gauss composition, lattice multiplication, quadratic forms of four variables.

1 The main problem

This paper presents the results of the research dedicated to the search of the multiplication structure on the classes of integer positive definite quadratic forms of four variables.

1.1 Quadratic Forms

We start with giving basic definitions. The main object we are going to work with is *integer quadratic form.* The *integer quadratic form* is a form

$f(x,y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. The *discriminant* of the form is an integer number $b^2 - 4ac$. The *Gramian matrix* of such form is the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. We will write (a, b, c) instead of the form $ax^2 + bxy + cy^2$.

We are going to consider only *positive definite* quadratic forms, i.e. such forms that for any $(x, y) \in \mathbb{Z}^2 \backslash (0, 0)$ $f(x, y) > 0$. The discriminant of such forms is necessarily negative. The original question is what integer values can we get by placing integers instead of x and y in our quadratic form $f(x, y)$. We will call such set *the set of values.*

It happens that some different forms have the same set of values. Thus we have no reason to differ such forms, which brings us to the notion of *equivalence.*

Definition 1.1. Two quadratic forms are said to be *equivalent* if one is obtained from the other by an invertible integer linear change of variables, i.e. if $G_2 = A^T G_1 A$, where G_1 and G_2 are the Gramian matrices of the forms, $A \in GL(2, \mathbb{Z})$ and $\det A = \pm 1$.

1.2 Integer Lattices

Another useful way of understanding quadratic forms is representing them as lattices in the Euclidian plane. Suppose we have the standard Euclidian plane $\mathbb{R}^2$ with a standard *length* and *inner product*. Given the vector (x_1, y_1), we say that its *length* is $|(x_1, y_1)| = \sqrt{x_1^2 + y_1^2}$ and the *inner product* of (x_1, y_1) and (x_2, y_2) is $\langle (x_1, y_1), (x_2, y_2) \rangle = x_1x_2 + y_1y_2 = |(x_1, y_1)||(x_2, y_2)| cos\phi$, where ϕ is the angle between the vectors. Let us call the set of values of the lattice L the set of the square lengths of the vectors from L.

Given two noncollinear vectors $\vec{u}$ and $\vec{v}$ on the Euclidian plane we can use them to generate the *integer lattice*, which consists of all vectors $m\vec{u} + n\vec{v}$, where $m, n \in \mathbb{Z}$, i.e. of all integer linear combinations of $\vec{u}$ and $\vec{v}$. Rank of the lattice is the minimal number of vectors which span the lattice. The rank of the described lattice is two. The following theorem shows the correspondence between quadratic forms and integer lattices.

Theorem 1.1. *For any integer positive definite quadratic form (a, b, c), there exists a pair of vectors $\vec{u}$ and $\vec{v}$ in the Euclidian plane such that*

$$\langle \vec{u}, \vec{u} \rangle = a, \quad 2\langle \vec{u}, \vec{v} \rangle = b, \quad \langle \vec{v}, \vec{v} \rangle = c. \tag{1}$$

If, on the other hand, the coefficients of a quadratic form (a, b, c) are given by the equations (1) for some noncollinear vectors $\vec{u}$ and $\vec{v}$ from the Euclidian plane, then the form (a, b, c) is positive definite.

Proof. Note that since quadratic form (a, b, c) is positively definite looking at its values on $(1, 0)$ and $(0, 1)$ we get that a and c are positive. Since the discriminant is negative, i.e. $b^2 - 4ac < 0$, we get $-1 \leq \frac{b}{2\sqrt{ac}} \leq 1$. Thus there exists ϕ such that $cos\phi = \dfrac{b}{2\sqrt{ac}}$. Let's take vectors $\vec{u}$ and $\vec{v}$ of length $\sqrt{a}$ and $\sqrt{c}$ and angle ϕ between them. Then $\langle \vec{u}, \vec{v} \rangle = \sqrt{a} \cdot \sqrt{c} \cdot \dfrac{b}{2\sqrt{ac}} = \dfrac{b}{2}$. To prove the second part note that:

$$ax^2 + bxy + cy^2 = \langle x\vec{u} + y\vec{v}, x\vec{u} + y\vec{v} \rangle.$$

On the right hand side we have the square of the length of the vector $x\vec{u}+y\vec{v}$. This number is positive for all x and y not equal simultaneously to zero. □

This brings us to a very important corollary.

Corollary 1.1. *The set of values of a given integer positive definite quadratic form (a, b, c) coincides with the set of values of the lattice generated by the vectors $\vec{v}$ and $\vec{u}$, where a, b, c, u and v satisfy equations (1) from Theorem 1.1.*

This corollary allows us to think about quadratic forms and their values in terms of integer lattices and their vector lengths. Note that lattices corresponding to equivalent quadratic forms are isometric. There is a relation between the area of the fundamental triangle of the lattice and the discriminant of the corresponding form, which implies that two lattices with equal areas of the fundamental triangles correspond to two quadratic forms of the same discriminant, and vice versa. The relation it the following:

Proposition 1.1. *Suppose S is the area of the fundamental triangle of the lattice L and Δ is the discriminant of the form (a, b, c) corresponding to that lattice by Theorem 1. Then $S^2 = -\dfrac{\Delta}{16}$.*

Proof. Discriminant Δ is equal to $b^2 - 4ac$ by the definition. Let $\vec{u}$ and $\vec{v}$ be the generating vectors of the lattice L and let ϕ be the angle between them. Then $S^2 = \dfrac{1}{4}|\vec{u}|^2|\vec{v}|^2 sin^2(\phi) = \dfrac{1}{4}ac(1 - \dfrac{b^2}{4ac}) = \dfrac{4ac - b^2}{16} = -\dfrac{\Delta}{16}$ □

1.3 Complex Numbers

The next step of understanding the set of values of the positive definite quadratic form is putting the corresponding lattice in the field of complex numbers. In order to obtain a complex structure on the lattice we replace the vectors from the Euclidian plane with the corresponding complex numbers, i.e. a vector $(x, y) \in \mathbb{R}^2$ turns into $x + iy \in \mathbb{C}$. The length (resp. square length) turns into the absolute value (resp. square absolute value), and our integer lattice now linearly spanned by the complex numbers instead of the vectors.

Proposition 1.2. *Let (a, b, c) be a positive definite quadratic form and consider the lattice $L \subset \mathbb{C}$ spanned by the complex numbers*

$$z_1 = \sqrt{a}, \quad z_2 = \frac{b + \sqrt{b^2 - 4ac}}{2\sqrt{a}}.$$

Then such a lattice corresponds to the form (a, b, c), i.e. the set of values of the quadratic form is equal to the set of square absolute values of the numbers in $L \subset \mathbb{C}$.

Proof. It is enough to check that $|z_1| = a$, $|z_2| = c$ and $cos\phi = \dfrac{b}{2\sqrt{ac}}$, where ϕ is the angle between z_1 and z_2. Recall that a and c are positive since the quadratic form is positive definite. That follows that $\sqrt{a}$ is a real number and the square of its absolutely value is a. Since $b^2 - 4ac < 0$, $\sqrt{b^2 - 4ac} = i\sqrt{4ac - b^2}$, thus $\mathrm{Re}(z_2) = \dfrac{b}{2\sqrt{a}}$ and $\mathrm{Im}(z_2) = \dfrac{\sqrt{b^2 - 4ac}}{2\sqrt{a}}$. Therefore:

$$|z_2|^2 = \left| \frac{b + \sqrt{b^2 - 4ac}}{2\sqrt{a}} \right|^2 = \frac{b^2}{4a} + \frac{4ac - b^2}{4a} = c$$

Since $\sqrt{a}$ is a real number the angle between two given numbers is the angle of the second with the real line. Let this angle be ϕ, then $cos\phi = \dfrac{\frac{b}{2\sqrt{a}}}{\sqrt{c}} = \dfrac{b}{2\sqrt{ac}}$ □

1.4 Gauss Composition

Recall that the initial question was to describe the set of values of the integer quadratic form. More precisely we are interested in the set of values of the forms in the equivalence class, which we will call integer class. The Gauss composition is the principal approach to answering the question. It helps to obtain a multiplication structure on the classes of the quadratic forms of fixed discriminant.

The multiplication, called composition, can be easily observed on the set of values of the form. The set of values of the product of two forms is exactly the set consisting of all pairwise products of values of the first and the second forms. In other words, this multiplication corresponds to the actual complex multiplication of integer lattices as subsets of $\mathbb{C}$.

Definition 1.2. The *product* or *multiplication* of two lattices $L_1, L_2 \subset \mathbb{C}$, corresponding to the integer quadratics forms, with equal areas of fundamental triangles is a lattice $L = \{z \in \mathbb{C} | z = z_1 z_2, \ where \ z_1 \in L_1 \ and \ z_2 \in L_2\}$.

To be correct this definition requires the following theorem to be true:

Theorem 1.2. *Let $L_1, L_2 \subset \mathbb{C}$ be integer lattices of rank two with equal ares of fundamental triangles. Then the set $L = \{z \in \mathbb{C} | z = z_1 z_2, \ where \ z_1 \in L_1 \ and \ z_2 \in L_2\} \subset \mathbb{C}$ is an integer lattice or rank two and the same square of the fundamental triangle.*

In the end of the section it will be clear why the theorem is true. The multiplication can be expressed in terms of quadratic forms. For this purpose, we need to define a *Dirichlet pair*.

Definition 1.3. Two integer positive definite quadratic forms (a, B, c) and (a', B, c') of the same discriminant Δ are said to form a *Dirichlet pair* if $B^2 - \Delta$ is divisible by $4aa'$, and the numbers a and a' are relatively prime.

Considering the fact that any two classes of integer positive definite quadratic forms of the same discriminant contain a *Dirichlet pair*, the following theorem presents the structure of a group (with an operation called *composition*) on the classes of integer positive definite quadratic forms of fixed discriminant.

Theorem 1.3. *Let the positive definite quadratic forms (a, B, c) and (a', B, c') form a Dirichlet pair. Then the composition of the classes of (a, B, c) and*

(a', B, c') is the class of the quadratic form

$$aa'x^2 + Bxy + \frac{B^2 - \Delta}{4aa'}y^2$$

Proof. For the proof we need lemma from [1]. Consider the lattices L and L' corresponding to the forms (a, B, c) and (a', B, c'), which form a Dirichlet pair. By Proposition 1.2 we may assume that L is spanned by the complex numbers

$$\sqrt{a}, \quad \frac{B + \sqrt{\Delta}}{2\sqrt{a}},$$

and L' is spanned by the complex numbers

$$\sqrt{a'}, \quad \frac{B + \sqrt{\Delta}}{2\sqrt{a'}}.$$

Then the product LL' is spanned by the following complex numbers:

$$e_{11} = \sqrt{aa'}, \quad e_{12} = (B + \sqrt{\Delta})\frac{\sqrt{a}}{2\sqrt{a'}},$$

$$e_{21} = (B + \sqrt{\Delta})\frac{\sqrt{a'}}{2\sqrt{a}}, \quad e_{22} = \frac{B^2 + 2B\sqrt{\Delta} + \Delta}{4\sqrt{aa'}}.$$

A priori lattice LL' can be not a rank 2 lattice. But the following lemma states it is.

Lemma 1.1. *Lattice LL' is spanned by just two complex numbers*

$$\sqrt{aa'}, \quad \frac{B + \sqrt{\Delta}}{2\sqrt{aa'}}.$$

See [1] for the proof. Now take the quadratic form corresponding to the lattice spanned by $\sqrt{aa'}$ and $\frac{B + \sqrt{\Delta}}{2\sqrt{aa'}}$. This simple exercise shows that this form is exactly the quadratic form from Theorem 1.3. □

Note that Lemma 1.1 also proves Theorem 1.2. Having such a structure on the group of classes of quadratic forms is a great help in understanding the set of values of a certain form. Suppose we know the set of values of some classes of forms of fixed discriminant. Decomposing the form we are in question into a product of other forms, we can extract information about the new set of values, using what we know about the other forms.

2 Direction of research

Complex numbers play an essential role in the method of the Gauss composition. An important property that they have is multiplicativity of the absolute value, which means that $|z_1||z_2| = |z_1 z_2|$. One can remember *quaternions*, i.e. the skew field with the absolute value which is multiplicative as well. We will recall its definition.

Definition 2.1. *Quaternions* $\mathbb{H}$ *are vectors* $(a, b, c, d) \in \mathbb{R}^4$ *or a set of all linear combinations* $a + bi + cj + dk$ *of four elements* $1, i, j, k$*, with real coefficients with the following operations of addition and multiplication. Addition is the same as addition of vectors in* $\mathbb{R}^4$*. The multiplication is defined by the following relations between* $1, i, j, k$ *and properties of distributivity and associativity:*

$$i^2 = j^2 = k^2 = 1,\ ij = -ji - k,\ jk = -kj = i,\ ki = -ik = j.$$

Absolute value of quaternion $q = a + bi + cj + dk$ is defined as $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$. One can check that $|q_1||q_2| = |q_1 q_2|$. This leads to the idea of using quaternions to generalize the result of Gauss.

Indeed, suppose we are interested in the set of values of the *integer quadratic form of four variables* $ax^2+by^2+cz^2+dw^2+exy+fxz+gxw+hyz+lyw+rwz$. The corresponding lattice L is a $\mathbb{Z}$-span of the set $\{e_1, e_2, e_3, e_4\} \subset \mathbb{H} \approx \mathbb{R}^4$, given by the following relations:

$$\begin{gathered} ||e_1|| = a,\ ||e_2|| = b,\ ||e_3|| = c,\ ||e_4|| = d, \\ \langle e_1, e_2 \rangle = e/2,\ \langle e_1, e_3 \rangle = f/2,\ \langle e_1, e_4 \rangle = g/2, \\ \langle e_2, e_3 \rangle = h/2,\ \langle e_2, e_4 \rangle = l/2,\ \langle e_3, e_4 \rangle = r/2. \end{gathered}$$

The set of values of the form can be presented as the set of square lengths of the vectors from L, lattice of rank 4. Two forms are called *equivalent*, when one can be obtained from another by a $\mathbb{Z}$-invertible change of variables. Note that, as in case of two variables, two equivalent forms have isometric lattices in $\mathbb{R}^4$.

We call $L_1 L_2 = \operatorname{span}_{\mathbb{Z}}\{l_1 l_2 | l_1 \in L_1, l_2 \in L_2\} \subset \mathbb{H}$ the *product* of L_1 and L_2. The question we face is whether or not it is true that the product of two rank 4 lattices L_1 and L_2 is a rank 4 lattice.

Unfortunately, it turns out that it is not true for most of lattices. Our goal is to find out for which lattices their product is a lattice of rank 4. Here we come up with the idea of considering linear spaces over $\mathbb{Q}$ instead of lattices over $\mathbb{Z}$.

Definition 2.2. Let us call linear space $L \subset \mathbb{H}$ a *quaternionic* $\mathbb{Q}$*-space* if there exists the basis vectors $q_1, q_2, q_3, q_4 \in \mathbb{H}$ such that

$$L = \{a_1q_1 + a_2q_2 + a_3q_3 + a_4q_4 \mid a_1, a_2, a_3, a_4 \in \mathbb{Q}\}.$$

Now that we have linear spaces over $\mathbb{Q}$, we have to define the equivalence relation between them.

Definition 2.3. Two quaternionic $\mathbb{Q}$-spaces L_1 and L_2 are said to be *equivalent* if one is obtained from the other by an invertible rational linear change of variables, i.e. if there exists a matrix $A \in GL(4, \mathbb{Q})$ such that $AL_1 = L_2$.

This will simplify our task of multiplication of classes but we will not be able to differentiate some integer classes since they will merge in one.

Another strategy of dealing with the question is to weaken the definition of multiplication of lattices.

Definition 2.4. We will say that quaternionic $\mathbb{Q}$-space $L \subset \mathbb{H}$ is *almost a product* of two quaternionic $\mathbb{Q}$-spaces L_1 and L_2, if there exists a quaternion $q : |q| = 1$ such that $L_1qL_2 = L$.

Note that multiplying one of the $\mathbb{Q}$-spaces on the unit quaternion we don't change the set of values of this space. Thus it is enough for L to be an almost a product of L_1 and L_2 in order to help us to answer the initial question.

The following theorem from [4] shows that understanding $\mathbb{Q}$ case is very important for further investigation of the $\mathbb{Z}$ case. We also introduce the proof from [4] by A. Pakharev.

Theorem 2.1. *Suppose that L_1 and L_2 are lattices. Then L_1L_2 is a rank 4 lattice $\iff$ $(\mathbb{Q}L_1)(\mathbb{Q}L_2)$ is a quaternionic $\mathbb{Q}$-space*

Proof. $\Rightarrow$: $(\mathbb{Q}L_1)(\mathbb{Q}L_2) = \mathbb{Q}(L_1L_2)$ is a quaternionic $\mathbb{Q}$-space, since L_1L_2 is a rank 4 lattice.

$\Leftarrow$: Let $\{u_i\}$ be a $\mathbb{Z}$-basis of L_1 and $\{v_i\}$ be a $\mathbb{Z}$-basis of L_2. Denote by $\{w_i\}$ a $\mathbb{Q}$-basis of $(\mathbb{Q}L_1)(\mathbb{Q}L_2)$. u_iv_j are in $(\mathbb{Q}L_1)(\mathbb{Q}L_2)$, so there exist such rational a_{ijk} that $u_iv_j = \sum_k a_{ijk}w_k$. Let n be the least common multiple of the denominators of a_{ijk}. Then $L_0 = \sum_i w_i\mathbb{Z}/n$ is a $\mathbb{Z}$-module of rank 4 and a lattice, which contain L_1L_2 as a $\mathbb{Z}$-submodule. Thus rank of L_1L_2 is at most 4. But $\mathbb{Q}L_1L_2 \supset L_0$, then L_1L_2 is a rank 4 lattice. □

Now we will demonstrate usefulness of this theorem focusing on a special case. We will consider lattices $L \subset \mathbb{H}$, which are rank 4 sublattices of the standard lattice:

$$L_0 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \subset \mathbb{H}.$$

We call L *primitive* if there is no integer $m > 1$ such that $L \subset m\mathbb{Z}^4$.

Note that for any such L, L_1 and L_2: $\mathbb{Q}L = \mathbb{Q}L_0$ and $(\mathbb{Q}L_1)(\mathbb{Q}L_2) = (\mathbb{Q}L_0)^2 = (\mathbb{Q}L_0)$. By Theorem 2.1 that means that the product of L_1 and L_2 is a lattice of rank 4. Now taking the product of primitive lattices L_1 and L_2 we will take the lattice $m^{-1}L_1L_2$ instead of L_1L_2, where m is the largest integer, such that $L_1L_2 \subset m\mathbb{R}^4$. In this part we will show a constructive way to take product of such lattices as the subsets of $\mathbb{H}$. Take a lattice $L \subset L_0 \subset \mathbb{H}$ and take $\{e_1, e_2, e_3, e_4\}$ – the $\mathbb{Z}$-basis of L. Suppose:

$$\begin{gathered}
e_1 = a_{11} + a_{12}i + a_{13}j + a_{14}k \\
e_2 = a_{21} + a_{22}i + a_{23}j + a_{24}k \\
e_3 = a_{31} + a_{32}i + a_{33}j + a_{34}k \\
e_4 = a_{41} + a_{42}i + a_{43}j + a_{44}k.
\end{gathered}$$

We will call the matrix A:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

the *generating matrix* of L. Integer operations on the rows of the matrix change the basis of the lattice, but preserve the lattice. Thus we can simplify the matrix making a reduction to so-called *Hermite normal form.*

Definition 2.5. A non-degenerate matrix H is in *Hermite normal form* if it is upper triangular with non-negative entries and the entries above the diagonal are strictly less than the diagonal entries in the same column.

Theorem 2.2. *Let $L \subset \mathbb{H}$ be the rank 4 sublattice of the standard lattice L_0. There exists unique matrix H – generating matrix of L, such that H is in Hermite normal form.*

Proof. First we prove the existence part. Take any $A = (a_{ij})$ – generating matrix of L. We will show that making only integer operations on the rows of A we can get a Hermit normal form matrix. Suppose a is the greatest common divisor of the first column. Then by the Euclidean algorithm making integer operation on all four rows we can reduce the first column to the column with all entries equal to a. Subtracting the first row from all others we get:

$$\begin{pmatrix} a & a'_{12} & a'_{13} & a'_{14} \\ 0 & a'_{22} & a'_{23} & a'_{24} \\ 0 & a'_{32} & a'_{33} & a'_{34} \\ 0 & a'_{42} & a'_{43} & a'_{44} \end{pmatrix}$$

Now make the same with the lower right corner 3×3 matrix and at last with the lower right corner 2×2 matrix. We get:

$$\begin{pmatrix} a & a'_{12} & a'_{13} & a'_{14} \\ 0 & b & a''_{23} & a''_{24} \\ 0 & 0 & c & a''_{34} \\ 0 & 0 & 0 & d \end{pmatrix}$$

Subtracting the multiplicities of the second, third and fourth rows from the first row we can make a'_{12}, a'_{13} and a'_{14} respectively less than b, c and d. Similarly make a''_{23} less than c, a''_{24} less than d and a''_{34} less than d. Finally we get the Hermite normal form matrix:

$$\begin{pmatrix} a & b_1 & c_1 & d_1 \\ 0 & b & c_2 & d_2 \\ 0 & 0 & c & d_3 \\ 0 & 0 & 0 & d \end{pmatrix}$$

Now we prove the uniqueness of such generating matrix. Note that a is the greatest common divisor of the set $\{\mathrm{Re}(z) | z \in L\}$. Similarly b is the GCD of $\{\mathrm{Re}(z \cdot i) | z \in L \cap \mathbb{R}^{\perp}\}$, where $\mathbb{R}^{\perp}$ is an orthogonal complement of $\mathbb{R}$ in $\mathbb{H}$. Finally, $c = GCD(\{\mathrm{Re}(z \cdot j) | z \in L \cap (\mathbb{R} + i\mathbb{R})^{\perp}\})$ and $d = GCD(\{\mathrm{Re}(z \cdot k) | z \in L \cap (\mathbb{R} + i\mathbb{R} + j\mathbb{R})^{\perp}\})$. That means that a, b, c, d are invariantly defined and don't depend on the transformations of the matrix. It remains to prove that $b_1, c_1, c_2, d_1, d_2, d_3$ are invariantly defined as well.

Suppose $H = (h_{ij})$ and $H' = (h'_{ij})$ are two Hermite normal form generating matrices of L. Let h_1, h_2, h_3, h_4 and h'_1, h'_2, h'_3, h'_4 be the rows of H and H' respectively. Since h'_1, h'_2, h'_3, h'_4 is a basis of L then $h_3 = \lambda_1 h'_1 + \lambda_2 h'_2 + \lambda_3 h'_3 + \lambda_4 h'_4$. Considering that our matrices are in Hermite normal form, we have $\lambda_1 = \lambda_2 = 0$, hence $h_3 = \lambda_3 h'_3 + \lambda_4 h'_4$. Since $h_{33} = h'_{33}$ we get $\lambda_3 = 1$, so $h_3 = h'_3 + \lambda_4 h'_4$. Thus $h'_{34} + \lambda_4 h'_{44} = h_{34} < h_{44} = h'_{44} \Rightarrow \lambda_4 = 0$. We get that $h_3 = h'_3$. Similarly $h_2 = h'_2$ and $h_1 = h'_1$. □

Now take L_1 and L_2 – primitive sublattices of L_0. Let A and B be the reduced (Hermite normal form) generating matrices of L_1 and L_2 respectively. Let C denote the 16×4 matrix with the rows $a_i \cdot b_j$, where $i, j = 14$ and a_i, b_j are the rows of A and B respectively. We write $a_i \cdot b_j$ here, meaning that we take $q_{ij} \in \mathbb{H}$ – the product of two quaternions corresponding to the rows a_i and b_j – and write q_{ij} as a row of matrix C. By Theorem 2.1 the rows of C span the rank 4 lattice, thus applying the Hermite reduction to C and permuting the rows we get a new matrix, whose first four rows form a Hermite normal form and all the other rows are zeros. Let $A \cdot B$ denote the matrix formed by the first rows. This is the generating matrix of $L_1 L_2$. One should also divide $A \cdot B$ by the largest common divisor of its entries to obtain the generating matrix of the the primitive product of L_1 and L_2.

The process described in this subsection gives a constructive way to take primitive products of certain lattices. The next results are based on the computer computations made with a program, which realizes this process. We present two conjectures that were obtained experimentally.

Definition 2.6. Lattice L is *periodic* if there exist $p \in \mathbb{Z}$, called *period*, such that $L^p = L$.

Conjecture 2.1. *Consider primitive rank 4 lattices $L \subset \mathbb{H}$, which are sublattices of a standard lattice L_0, with one of the following reduced generating matrices:*

$$\begin{pmatrix} n & 0 & 0 & 0 \\ 0 & 1 & m & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix}, \begin{pmatrix} n & 0 & 0 & 0 \\ 0 & 1 & 0 & m \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix}, \begin{pmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ 0 & 0 & 1 & m \\ 0 & 0 & 0 & n \end{pmatrix},$$

Such lattices are periodic with period 2 for all m, n such that $0 < m < n$.

Conjecture 2.2. *Consider primitive rank 4 lattices $L \subset \mathbb{H}$, which are sublattices of a standard lattice L_0, with one of the following reduced generating matrices:*

$$\begin{pmatrix} 1 & m & 0 & 0 \\ 0 & n & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix}, \begin{pmatrix} 1 & 0 & m & 0 \\ 0 & n & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & m \\ 0 & n & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix},$$

Such lattices are periodic with period 2 if and only if m and n are such that $0 < m < n$ and any prime factor of n is not equal to 1 modulus 4.

Conclusion

This paper presents the method of Gauss composition which denotes a structure of group on the classes of equivalence of integer positive definite quadratic forms of two variables and fixed discriminant. This method makes the question of describing the set of values of a given quadratic form more approachable.

Generalization of this method for quadratic forms of four variables is the main goal of the research. The structure of quaternions which is similar to the structure of complex numbers is very helpful in this endeavor, however a straight generalization faces some obstacles. It doesn't always happen that the product of lattices of rank 4 is a lattice of rank 4. However we can simplify the question in several ways.

The first way is to consider rational lattices and rational equivalence instead of integer. The second is to multiply lattices with a correction factor, the quaternion q of unit length, i.e. multiply L_1qL_2 instead of L_1L_2. The third is to restrict the set of considered lattice and try to find and understand the multiplication structures in it.

The further goal of the investigation is to describe which classes of forms or quaternionic lattices can be multiplied.

References

[1] Aicardi, F. & Timorin, V. (n.d.). *Quadratic Arithmetics in Problems.* Unpublished manuscript.

[2] Conway, J.H. & Sloane, N.J.A. (1993). *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag.

[3] Conway, J.H. & Smith, D.A. (2003). *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry.* Natick: A K Peters.

[4] Duryev, E. & Pakharev, A. & Timorin V. (n.d.). *Quaternionic Multiplication of Lattices.* Unpublished manuscript.