Quadratic Forms with Semigroup Property

F. Aicardi and V. Timorin

August 22, 2007

Binary quadratic forms

Definition

A binary quadratic form is a function

$$f(x, y) = ax^2 + bxy + cy^2.$$

Notation

A quadratic form f is sometimes represented as a triple (a, b, c) of coefficients.

Definition

We say that a number A is represented by f is $A = f(x, y)$ for some $x, y \in \mathbb{Z}$.

Binary quadratic forms

Definition

A binary quadratic form is a function

$$f(x, y) = ax^2 + bxy + cy^2.$$

Notation

A quadratic form f is sometimes represented as a triple (a, b, c) of coefficients.

Definition

We say that a number A is represented by f is $A = f(x, y)$ for some $x, y \in \mathbb{Z}$.

Binary quadratic forms

Definition

A binary quadratic form is a function

$$f(x, y) = ax^2 + bxy + cy^2.$$

Notation

A quadratic form f is sometimes represented as a triple (a, b, c) of coefficients.

Definition

We say that a number A is represented by f is $A = f(x, y)$ for some $x, y \in \mathbb{Z}$.

Example: sum of squares

Example

The product of two integers represented by $x^2 + y^2$ is also represented by this quadratic form.

Explanation

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2.$$

This is equivalent to

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|, \quad z_1 = x_1 + iy_1, \; z_2 = x_2 + iy_2.$$

Example: sum of squares

Example

The product of two integers represented by $x^2 + y^2$ is also represented by this quadratic form.

Explanation

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2.$$

This is equivalent to

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|, \quad z_1 = x_1 + iy_1,\ z_2 = x_2 + iy_2.$$

Semigroup property

Definition

A quadratic form f is said to have semigroup property if the product of any two integers represented by f is also represented by f.

Fact

Among quadratic forms with small (say, < 100) coefficients, most forms have semigroup property.

Example

Every quadratic form $(1, b, c)$ has semigroup property.

Semigroup property

Definition

A quadratic form f is said to have semigroup property if the product of any two integers represented by f is also represented by f.

Fact

Among quadratic forms with small (say, < 100) coefficients, most forms have semigroup property.

Example

Every quadratic form $(1, b, c)$ has semigroup property.

Semigroup property

Definition

A quadratic form f is said to have semigroup property if the product of any two integers represented by f is also represented by f.

Fact

Among quadratic forms with small (say, < 100) coefficients, most forms have semigroup property.

Example

Every quadratic form $(1, b, c)$ has semigroup property.

Trigroup property

Theorem (Gauss, Arnold)

The product of any three integers represented by a quadratic form f is also represented by f.

Corollary

If f represents 1, then it has semigroup property.

Problem (Arnold)

Describe all quadratic forms with semigroup property.

Trigroup property

Theorem (Gauss, Arnold)

The product of any three integers represented by a quadratic form f is also represented by f.

Corollary

If f represents 1, then it has semigroup property.

Problem (Arnold)

Describe all quadratic forms with semigroup property.

Trigroup property

Theorem (Gauss, Arnold)

The product of any three integers represented by a quadratic form f is also represented by f.

Corollary

If f represents 1, then it has semigroup property.

Problem (Arnold)

Describe all quadratic forms with semigroup property.

Integer normed pairings

Definition

A bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ is called an integer normed pairing for a quadratic form f if

$$f(s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x}) \cdot f(\mathbf{y})$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$.

Remark

If a quadratic form f admits an integer normed pairing, then it has semigroup property.

Remark

We do not know any other examples of quadratic forms with semigroup property.

Integer normed pairings

Definition

A bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ is called an integer normed pairing for a quadratic form f if

$$f(s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x}) \cdot f(\mathbf{y})$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$.

Remark

If a quadratic form f admits an integer normed pairing, then it has semigroup property.

Remark

We do not know any other examples of quadratic forms with semigroup property.

Integer normed pairings

Definition

A bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ is called an integer normed pairing for a quadratic form f if

$$f(s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x}) \cdot f(\mathbf{y})$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^2$.

Remark

If a quadratic form f admits an integer normed pairing, then it has semigroup property.

Remark

We do not know any other examples of quadratic forms with semigroup property.

The main result

The main result

We give explicit integer parameterization for all integer normed pairings and the corresponding quadratic forms.

Remark

Integer normed pairings are intimately related to Gauss composition law. There are four types of integer normed pairings.

Notation

An integer normed pairing $\mathbf{z} = s(\mathbf{x}, \mathbf{y})$ can be given by a pair of matrices A_1, A_2:

$$z_j = \mathbf{x} A_j \mathbf{y}^t, \quad j = 1, 2.$$

We write $s = (A_1 | A_2)$.

The main result

The main result

We give explicit integer parameterization for all integer normed pairings and the corresponding quadratic forms.

Remark

Integer normed pairings are intimately related to Gauss composition law. There are four types of integer normed pairings.

Notation

An integer normed pairing $\mathbf{z} = s(\mathbf{x}, \mathbf{y})$ can be given by a pair of matrices A_1, A_2:

$$z_j = \mathbf{x} A_j \mathbf{y}^t, \quad j = 1, 2.$$

We write $s = (A_1 | A_2)$.

The main result

The main result

We give explicit integer parameterization for all integer normed pairings and the corresponding quadratic forms.

Remark

Integer normed pairings are intimately related to Gauss composition law. There are four types of integer normed pairings.

Notation

An integer normed pairing $\mathbf{z} = s(\mathbf{x}, \mathbf{y})$ can be given by a pair of matrices A_1, A_2:

$$z_j = \mathbf{x} A_j \mathbf{y}^t, \quad j = 1, 2.$$

We write $s = (A_1 | A_2)$.

The formulas

The explicit integer parameterization for all integer normed pairings and the corresponding quadratic forms:

$$s_1 = \left(\begin{array}{cc|cc} mp + kq & nq & -mq & mp \\ nq & -np & mp & nq + kp \end{array} \right), \quad \begin{array}{c} f_1 = (rm, rk, rn), \\ r := mp^2 + kpq + nq^2. \end{array}$$

$$s_2 = \left(\begin{array}{cc|cc} mp & nq + kp & mq & -mp \\ -nq & np & mp + kq & nq \end{array} \right), \quad \begin{array}{c} f_2 = (rm, rk, rn), \\ r := mp^2 + kpq + nq^2. \end{array}$$

$$s_3 = \left(\begin{array}{cc|cc} mp & -nq & mq & mp + kq \\ nq + kp & np & -mp & nq \end{array} \right), \quad \begin{array}{c} f_3 = (rm, rk, rn), \\ r := mp^2 + kpq + nq^2. \end{array}$$

$$s_4 = \left(\begin{array}{cc|cc} a & c & -d & -a \\ c & b & -a & -c \end{array} \right), \; f_4 = (a^2 - cd, \; ac - bd, \; c^2 - ab)$$

Quadratic forms vs lattices

Correspondence

There is a correspondence between positive definite quadratic forms and lattices in $\mathbb{C}$.

Theorem

Suppose that a quadratic form f admits an integer normed pairing. Then the corresponding lattice is stable under one of the following operations:

$$\sigma_1 : (z, w) \mapsto zw,$$
$$\sigma_2 : (z, w) \mapsto \bar{z}w,$$
$$\sigma_3 : (z, w) \mapsto z\overline{w},$$
$$\sigma_4 : (z, w) \mapsto \overline{zw}.$$

Quadratic forms vs lattices

Correspondence

There is a correspondence between positive definite quadratic forms and lattices in $\mathbb{C}$.

Theorem

Suppose that a quadratic form f admits an integer normed pairing. Then the corresponding lattice is stable under one of the following operations:

$$\begin{aligned} \sigma_1 &: (z, w) \mapsto zw, \\ \sigma_2 &: (z, w) \mapsto \bar{z}w, \\ \sigma_3 &: (z, w) \mapsto z\overline{w}, \\ \sigma_4 &: (z, w) \mapsto \overline{zw}. \end{aligned}$$

High-school algebra

Definition

The discriminant of a quadratic form (a, b, c) is defined as $\Delta = b^2 - 4ac$.

Definition

A quadratic form is called definite (respectively, indefinite, degenerate) if $\Delta < 0$ (respectively, $\Delta > 0$, $\Delta = 0$).

Definition

A quadratic form f is called positive definite if $f > 0$ except at the origin (equivalently, (a, b, c) is positive definite if $a > 0$ and $\Delta < 0$).

High-school algebra

Definition

The discriminant of a quadratic form (a, b, c) is defined as $\Delta = b^2 - 4ac$.

Definition

A quadratic form is called definite (respectively, indefinite, degenerate) if $\Delta < 0$ (respectively, $\Delta > 0$, $\Delta = 0$).

Definition

A quadratic form f is called positive definite if $f > 0$ except at the origin (equivalently, (a, b, c) is positive definite if $a > 0$ and $\Delta < 0$).

High-school algebra

Definition

The discriminant of a quadratic form (a, b, c) is defined as $\Delta = b^2 - 4ac$.

Definition

A quadratic form is called definite (respectively, indefinite, degenerate) if $\Delta < 0$ (respectively, $\Delta > 0$, $\Delta = 0$).

Definition

A quadratic form f is called positive definite if $f > 0$ except at the origin (equivalently, (a, b, c) is positive definite if $a > 0$ and $\Delta < 0$).

Indefinite forms

Definition

Define the ring $\mathbb{H}$ of hyperbolic numbers as $\mathbb{R}[x]/(x^2 - 1)$. In other terms $\mathbb{H}$ is spanned (as an $\mathbb{R}$-linear space) by 1 and j, where $j^2 = 1$.

Correspondence

There is a correspondence between indefinite quadratic forms and lattices in $\mathbb{H}$. This correspondence has many of the same properties as that for positive definite forms.

Indefinite forms

Definition

Define the ring $\mathbb{H}$ of hyperbolic numbers as $\mathbb{R}[x]/(x^2 - 1)$. In other terms $\mathbb{H}$ is spanned (as an $\mathbb{R}$-linear space) by 1 and j, where $j^2 = 1$.

Correspondence

There is a correspondence between indefinite quadratic forms and lattices in $\mathbb{H}$. This correspondence has many of the same properties as that for positive definite forms.

Class groups

Definition

Two quadratic forms f and g are called *equivalent* if there is $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = g \circ A$.

Gauss composition

The set of all classes with a given discriminant has a natural commutative group structure.

Theorem

If a quadratic form f admits an integer normed pairing, then the class α of f satisfies $\alpha = 1$ or $\alpha^3 = 1$ in the class group.

Class groups

Definition

Two quadratic forms f and g are called *equivalent* if there is $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = g \circ A$.

Gauss composition

The set of all classes with a given discriminant has a natural commutative group structure.

Theorem

If a quadratic form f admits an integer normed pairing, then the class α of f satisfies $\alpha = 1$ or $\alpha^3 = 1$ in the class group.

Class groups

Definition

Two quadratic forms f and g are called *equivalent* if there is $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $f = g \circ A$.

Gauss composition

The set of all classes with a given discriminant has a natural commutative group structure.

Theorem

If a quadratic form f admits an integer normed pairing, then the class α of f satisfies $\alpha = 1$ or $\alpha^3 = 1$ in the class group.

Integer normed lattices

Definition

Lattices L corresponding to integer quadratic forms are integer normed, i.e. $|z|^2 \in \mathbb{Z}$ for all $z \in L$.

Theorem

For any binary integer quadratic form f, there exists a lattice L and a linear orientation preserving isomorphism $\phi : \mathbb{Z}^2 \to L$ such that $f(\mathbf{x}) = |\phi(\mathbf{x})|^2$ for all $\mathbf{x} \in \mathbb{Z}^2$. The lattice L depends only on the class of f, and is unique up to a Euclidean rotation.

Definition

An integer normed lattice L is said to be *primitive* if $L/\sqrt{n}$ is not integer normed for integer $n > 0$.

Integer normed lattices

Definition

Lattices L corresponding to integer quadratic forms are integer normed, i.e. $|z|^2 \in \mathbb{Z}$ for all $z \in L$.

Theorem

For any binary integer quadratic form f, there exists a lattice L and a linear orientation preserving isomorphism $\phi : \mathbb{Z}^2 \to L$ such that $f(\mathbf{x}) = |\phi(\mathbf{x})|^2$ for all $\mathbf{x} \in \mathbb{Z}^2$. The lattice L depends only on the class of f, and is unique up to a Euclidean rotation.

Definition

An integer normed lattice L is said to be *primitive* if $L/\sqrt{n}$ is not integer normed for integer $n > 0$.

Integer normed lattices

Definition

Lattices L corresponding to integer quadratic forms are integer normed, i.e. $|z|^2 \in \mathbb{Z}$ for all $z \in L$.

Theorem

For any binary integer quadratic form f, there exists a lattice L and a linear orientation preserving isomorphism $\phi : \mathbb{Z}^2 \to L$ such that $f(\mathbf{x}) = |\phi(\mathbf{x})|^2$ for all $\mathbf{x} \in \mathbb{Z}^2$. The lattice L depends only on the class of f, and is unique up to a Euclidean rotation.

Definition

An integer normed lattice L is said to be *primitive* if $L/\sqrt{n}$ is not integer normed for integer $n > 0$.

Class groups via lattices

Definition

The product of two lattices $L_1, L_2 \subset \mathbb{C}$ is defined as

$$L_1 L_2 = \{z_1 z_2 \mid z_1 \in L_1,\ z_2 \in L_2\}.$$

In general, this is not a lattice.

Theorem (Gauss?)

Let L_1 and L_2 be two integer normed lattices of the same discriminant Δ. Then $L_1 L_2$ is also an integer normed lattice of discriminant Δ.

Definition

The product of two classes represented by lattices L_1 and L_2 is the class represented by $L_1 L_2$.

Class groups via lattices

Definition

The product of two lattices $L_1, L_2 \subset \mathbb{C}$ is defined as

$$L_1 L_2 = \{z_1 z_2 \mid z_1 \in L_1,\ z_2 \in L_2\}.$$

In general, this is not a lattice.

Theorem (Gauss?)

Let L_1 and L_2 be two integer normed lattices of the same discriminant Δ. Then $L_1 L_2$ is also an integer normed lattice of discriminant Δ.

Definition

The product of two classes represented by lattices L_1 and L_2 is the class represented by $L_1 L_2$.

Class groups via lattices

Definition

The product of two lattices $L_1, L_2 \subset \mathbb{C}$ is defined as

$$L_1 L_2 = \{z_1 z_2 \mid z_1 \in L_1,\ z_2 \in L_2\}.$$

In general, this is not a lattice.

Theorem (Gauss?)

Let L_1 and L_2 be two integer normed lattices of the same discriminant Δ. Then $L_1 L_2$ is also an integer normed lattice of discriminant Δ.

Definition

The product of two classes represented by lattices L_1 and L_2 is the class represented by $L_1 L_2$.

Integer normed pairings of type 4

Recall that an integer normed pairing of type 4 is that corresponding to $\sigma_4 : (z, w) \mapsto \overline{zw}$. The class α of the corresponding quadratic form satisfies $\alpha^3 = 1$.

Commutative traceless pairings

Consider an integer normed pairing $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ that is

- commutative: $s(\mathbf{x}, \mathbf{y}) = s(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$,
- traceless, i.e. for any $\mathbf{x} \in \mathbb{R}^2$ the operator $M_{\mathbf{x}} : \mathbf{y} \mapsto s(\mathbf{x}, \mathbf{y})$ has trace zero.

Theorem

An integer normed pairing is of type 4 iff it is commutative and traceless. The corresponding quadratic form f is recovered from the relation

$$s(\mathbf{x}, s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x})\mathbf{y}, \quad \mathbf{x}, \mathbf{y} \in \mathbb{R}^2$$

Integer normed pairings of type 4

Recall that an integer normed pairing of type 4 is that corresponding to $\sigma_4 : (z, w) \mapsto \overline{zw}$. The class α of the corresponding quadratic form satisfies $\alpha^3 = 1$.

Commutative traceless pairings

Consider an integer normed pairing $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ that is

- commutative: $s(\mathbf{x}, \mathbf{y}) = s(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$,
- traceless, i.e. for any $\mathbf{x} \in \mathbb{R}^2$ the operator $M_{\mathbf{x}} : \mathbf{y} \mapsto s(\mathbf{x}, \mathbf{y})$ has trace zero.

Theorem

An integer normed pairing is of type 4 iff it is commutative and traceless. The corresponding quadratic form f is recovered from the relation

$$s(\mathbf{x}, s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x})\mathbf{y}, \quad \mathbf{x}, \mathbf{y} \in \mathbb{R}^2$$

Integer normed pairings of type 4

Recall that an integer normed pairing of type 4 is that corresponding to $\sigma_4 : (z, w) \mapsto \overline{zw}$. The class α of the corresponding quadratic form satisfies $\alpha^3 = 1$.

Commutative traceless pairings

Consider an integer normed pairing $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ that is

- commutative: $s(\mathbf{x}, \mathbf{y}) = s(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$,
- traceless, i.e. for any $\mathbf{x} \in \mathbb{R}^2$ the operator $M_{\mathbf{x}} : \mathbf{y} \mapsto s(\mathbf{x}, \mathbf{y})$ has trace zero.

Theorem

An integer normed pairing is of type 4 iff it is commutative and traceless. The corresponding quadratic form f is recovered from the relation

$$s(\mathbf{x}, s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x})\mathbf{y}, \quad \mathbf{x}, \mathbf{y} \in \mathbb{R}^2$$

Integer normed pairings of type 4

Recall that an integer normed pairing of type 4 is that corresponding to $\sigma_4 : (z, w) \mapsto \overline{zw}$. The class α of the corresponding quadratic form satisfies $\alpha^3 = 1$.

Commutative traceless pairings

Consider an integer normed pairing $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ that is

- commutative: $s(\mathbf{x}, \mathbf{y}) = s(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$,
- traceless, i.e. for any $\mathbf{x} \in \mathbb{R}^2$ the operator $M_{\mathbf{x}} : \mathbf{y} \mapsto s(\mathbf{x}, \mathbf{y})$ has trace zero.

Theorem

An integer normed pairing is of type 4 iff it is commutative and traceless. The corresponding quadratic form f is recovered from the relation

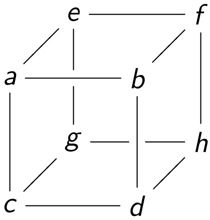
$$s(\mathbf{x}, s(\mathbf{x}, \mathbf{y})) = f(\mathbf{x})\mathbf{y}, \quad \mathbf{x}, \mathbf{y} \in \mathbb{R}^2$$

Bhargava cubes

- The coefficients of a bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ can be arranged in the form of a cube:
-

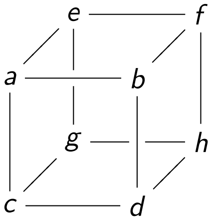
- From the pairs of opposite faces, one reads three classes α, β and γ such that $\alpha + \beta + \gamma = 0$.
- Integer normed pairings of type 4 correspond to cubes with a rotational 3-fold symmetry.

Bhargava cubes

- The coefficients of a bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ can be arranged in the form of a cube:
- 

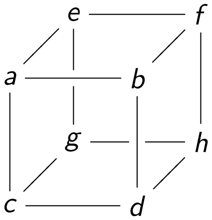
- From the pairs of opposite faces, one reads three classes α, β and γ such that $\alpha + \beta + \gamma = 0$.
- Integer normed pairings of type 4 correspond to cubes with a rotational 3-fold symmetry.

Bhargava cubes

- The coefficients of a bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ can be arranged in the form of a cube:
- 

- From the pairs of opposite faces, one reads three classes α, β and γ such that $\alpha + \beta + \gamma = 0$.
- Integer normed pairings of type 4 correspond to cubes with a rotational 3-fold symmetry.

Bhargava cubes

- The coefficients of a bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ can be arranged in the form of a cube:
- 

- From the pairs of opposite faces, one reads three classes α, β and γ such that $\alpha + \beta + \gamma = 0$.
- Integer normed pairings of type 4 correspond to cubes with a rotational 3-fold symmetry.