MULTIPLICATIVE PROPERTIES OF INTEGRAL BINARY QUADRATIC FORMS

A.G. Earnest

Department of Mathematics

Southern Illinois University Carbondale

Presentation at the International Conference on the Algebraic and Arithmetic Theory of Quadratic Forms

Lake Llanquihue, Chile

December 13-19, 2007

I. INTRODUCTION

V. I. Arnold *"Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world"*, *Bull. Braz. Math. Soc.* **34 (2003), 1-41.**

The product of three values represented by an integral binary quadratic form is again a value represented by the form; Arnold refers to this as the "trigroup property".

It is not always the case that products of two values represented by such a form is again a value represented by the form; a form for which this property does hold is said to be "perfect" by Arnold.

Problem: In a large cube in $\mathbb{R}^3$, what is the expected proportion of integral lattice points (a, b, c) for which the set of values represented by $ax^2 + bxy + cy^2$ is closed under multiplication?

Problem: Characterize the integral binary quadratic forms for which the set of represented values is closed under multiplication.

Example 1: Forms of the type $x^2 + dy^2$ have this property, as can be seen from the classical identity

$$(u^2 + dv^2)(z^2 + dw^2) = (uz + dvw)^2 + d(uw - vz)^2.$$

Example 2: The form $2x^2 + 3xy + 4y^2$ has this property, but does not represent 1.

II. NOTATION AND TERMINOLOGY

Throughout this talk, the term "form" will always refer to a nondegenerate integral binary quadratic form $ax^2+bxy+cy^2$, which will be denoted simply by (a,b,c). For a form f, let $D(f)$ denote the set of values represented by f. The discriminant of $f=(a,b,c)$ is $\Delta_f = b^2-4ac \neq 0$. It will be assumed here that all forms under consideration are either positive definite (if $\Delta_f < 0$) or indefinite (if $\Delta_f > 0$). A form (a,b,c) is said to be primitive if g.c.d.$(a,b,c)=1$.

<u>Definition</u>: A form f will be said to be "multiplicative" if $D(f)$ is closed under multiplication.

<u>Definition</u>: The form f is said to admit an integer normed pairing (or simply that f is "normed") if there exists a bilinear map $s : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ such that

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

for all $\vec{x},\vec{y} \in \mathbb{Z}^2$. [F. Aicardi & V. Timorin, 2007]

<u>Definition</u>: A form f will be said to be "parametrizable" if there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that

$$f = (\alpha^2 - \gamma\delta, \alpha\gamma - \beta\delta, \gamma^2 - \alpha\beta).$$

<u>Note</u>: If f is parametrizable, then f admits an integer normed pairing, which can be given explicitly by the equations

$$s(\vec{x}, \vec{y})_1 = \alpha x_1 y_1 + \gamma x_1 y_2 + \gamma x_2 y_1 + \beta x_2 y_2$$
$$s(\vec{x}, \vec{y})_2 = -\delta x_1 y_1 - \alpha x_1 y_2 - \alpha x_2 y_1 - \gamma x_2 y_2.$$

Therefore:

$$\boxed{\textbf{parametrizable} \implies \textbf{normed} \implies \textbf{multiplicative}}$$

<u>Conjecture 1</u>: If f is multiplicative, then f admits an integer normed pairing [F. Aicardi & V. Timorin, 2007].

<u>Conjecture 2</u>: If f is multiplicative, then f is parametrizable [F. Aicardi, 2004].

III. PRIMITIVE FORMS

Two forms f and g are equivalent, denoted $f \sim g$, if there is an integral transformation of determinant $+1$ taking one form to the other. For a form f, $[f]$ will denote the set of all forms equivalent to f. The set of equivalence classes of primitive forms of a fixed discriminant Δ has the structure of a finite abelian group, which will be denoted by $\mathfrak{C}_\Delta$, under the operation induced by Gaussian composition. The identity element of $\mathfrak{C}_\Delta$ is the class id_Δ consisting of the forms that represent 1. If $f = (a, b, c)$, then $[f]^{-1} = [f^{op}]$, where $f^{op} = (a, -b, c)$.

The notation $D([f])$ will be used to denote the set $D(g)$ for any $g \in [f]$. If f and g represent the integers k and ℓ, respectively, then the forms in the equivalence class $[f][g]$ represent the product $k\ell$; that is, $D(f)D(g) \subset D([f][g])$. Note also that $D(f^{op}) = D(f)$ since $f^{op}(x_1, x_2) = f(x_1, -x_2)$.

Proposition: For a primitive integral binary quadratic form f of discriminant Δ, the following are equivalent:

(a) f is multiplicative.

(b) $[f]^3 = 1$ in $\mathfrak{C}_\Delta$.

(c) f is parametrizable.

(d) f is normed.

Proof:

($a \Rightarrow b$) [A.G. Earnest & R.W. Fitzgerald, 2007]

($b \Rightarrow a$) Suppose that $[f]^3 = 1$. Let $k, \ell \in D(f)$. Then

$$k\ell \in D(f)D(f) \subset D([f]^2) = D([f]^{\pm 1}) = D(f).$$

($b \Rightarrow c$) Can be deduced as a special case of the description of composition given in [M. Bhargava, 2004].

IV. IMPRIMITIVE FORMS

Example 3: If $r \in D(f)$, then rf is multiplicative.

[Proof: Let $k, \ell \in D(rf)$; so $k = rk_0, \ell = r\ell_0$ for some $k_0, \ell_0 \in D(f)$. Then $k\ell = r(rk_0\ell_0) \in D(rf)$, since $rk_0\ell_0 \in D(f)$ by the trigroup property for f.]

Example 4: The form $(6, -3, 18)$ is multiplicative, but $(2, -1, 6)$ does not represent 3.

Write $f = c_f f_0$, where c_f denotes the g.c.d. of the coefficients of f and f_0 is primitive.

Theorem 1: For an integral binary quadratic form f, the following are equivalent:

(a) f is multiplicative.

(b) $c_f \in D(f_0)$ or $c_f \in D([f_0]^3)$.

(c) f is normed.

Therefore: Conjecture 1 is true.

<u>Main Lemma</u>: Let g and h be primitive integral binary quadratic forms of the same discriminant Δ, let p be an odd prime and n an integer. If $p \in D(g)$ and $np \in D(h)$, then either $n \in D([g][h])$ or $n \in D([g^{op}][h])$.

($a \Rightarrow b$) By a classical theorem due to Weber, there exists an odd prime p such that $p \in D(f_0)$. Then $c_f p \in D(f)$, and so $c_f^2 p^2 \in D(f)$ since f is multiplicative. Hence, $c_f p^2 \in D(f_0)$. It then follows from the lemma, with $g = h = f_0$ and $n = c_f p$, that either $c_f p \in D(id_\Delta)$ or $c_f p \in D([f_0]^2)$. In the first case, the lemma (with $g = f_0$, $h = id_\Delta$ and $n = c_f$) implies that $c_f \in D(f_0)$. In the second case, the lemma (with $g = f_0$, $[h] = [f_0]^2$ and $n = c_f$) implies that either $c_f \in D(f_0)$ or $c_f \in D([f_0]^3)$.

<u>Example 4 revisited</u>: The form $(6, -3, 18)$ is multiplicative. Here $c_f = 3$ and $f_0 = (2, -1, 6)$ is an element of order 5 in the class group of discriminant -47, $3 \notin D(f_0)$, and $3 \in D([f_0]^3) = D((3, -1, 4))$. Note that $(6, -3, 18)$ is parametrizable, with $\alpha = 2, \beta = -7, \gamma = 2, \delta = -1$.

Corollary: For a diagonal form f, the following are equivalent:

(a) f is multiplicative.

(b) $c_f \in D(f_0)$.

(c) f is parametrizable.

(d) f is normed.

Proof: ($b \Rightarrow c$) Since $c_f \in D(f_0)$, there exist $x, y \in \mathbb{Z}$ such that $c_f = ax^2 + cy^2$. Taking $\alpha = ax, \beta = -cx, \gamma = cy, \delta = -ay$ produces the desired parametrization.

Example 4: The form $(4, -2, 12)$ is multiplicative, but not parametrizable.

Therefore: Conjecture 2 is false in general.

<u>General setting</u>: Let $f = (a, b, c)$ be a primitive form and consider forms of the type rf. Suppose that rf is parametrizable. Then there exists $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ for which the following equations hold:

$$ra = \alpha^2 - \gamma\delta \tag{1}$$

$$rb = \alpha\gamma - \beta\delta \tag{2}$$

$$rc = \gamma^2 - \alpha\beta. \tag{3}$$

Multiplying (2) by γ and substituting for γ^2 from (3) and for $\gamma\delta$ from (1) yields:

$$\begin{aligned} rb\gamma &= \alpha\gamma^2 - \beta\gamma\delta \\ &= \alpha(rc + \alpha\beta) - \beta(\alpha^2 - ra) \\ &= \alpha rc + \beta ra. \end{aligned}$$

Dividing by r then gives

$$b\gamma = \alpha c + \beta a. \tag{4}$$

Multiplying both sides of (3) by b^2 and substituting (4)

then gives:

$$\begin{aligned} b^2rc &= (b\gamma)^2 - b^2\alpha\beta \\ &= (\alpha c + \beta a)^2 - b^2\alpha\beta \\ &= c^2\alpha^2 + (2ac - b^2)\alpha\beta + a^2\beta^2. \end{aligned}$$

Let

$$\hat{f} = c^2X^2 + (2ac - b^2)XY + a^2Y^2.$$

Thus, a necessary condition for the the form rf to be parametrizable is that

$$\exists\ \alpha, \beta \in \mathbb{Z} \quad \textbf{s.t. } b^2rc = \hat{f}(\alpha, \beta).$$

The form $\hat{f}$ is a primitive form of discriminant $b^2\Delta_f$.

In the particular case of the form $(4, -2, 12)$, we have $f = (2, -1, 6)$ and $r = 2$. The only representations of $rc = 12$ by $\hat{f} = (36, 23, 4) \sim (3, -1, 4) \in [f]^3$ are $(2, -6)$ and $(-2, 6)$. So $\alpha = \pm 2$ and $\beta = \mp 6$, and it follows from (3) that $\gamma = 0$. But then (2) becomes $-2 = \pm 6\delta$; hence, there is no integral solution for δ and the original form is not parametrizable.

<u>Remark</u>: If f is multiplicative and $c_f \notin D(f_0)$, then f is parametrizable [F. Aicardi & V. Timorin, 2007, Theorem 1.1].

<u>Question</u>: Let f be primitive, nondiagonal. For which $r \in D(f)$ is rf parametrizable?

V. k-MULTIPLICATIVITY

Definition: Let k be a non-negative integer. A form f is "k-multiplicative" if

$$a_1, a_2, ..., a_k \in D(f) \implies a_1 a_2 \cdots a_k \in D(f).$$

Theorem 2: Let f be a primitive form of discriminant Δ and let k be a non-negative even integer. Then f is k-multiplicative if and only if the order of $[f]$ in $\mathfrak{C}_\Delta$ is odd and at most $k+1$.

Definition: Let k be a non-negative even integer. A form f is "strictly k-multiplicative" if f is k-multiplicative but not ℓ-multiplicative for any even integer ℓ, $0 \leq \ell < k$.

Corollary: Let f be a primitive form of discriminant Δ and let k be a non-negative even integer. Then f is strictly k-multiplicative if and only if the order of $[f]$ in $\mathfrak{C}_\Delta$ is $k+1$.

REFERENCES

F. Aicardi, *"On the number of perfect binary quadratic forms"*, *Experiment. Math.* **13 (2004), 451-457.**

F. Aicardi, *"On trigroups and semigroups of binary quadratic forms values and of their associated linear operators"*, *Moscow Math. J.* **6 (2006), 589-627.**

F. Aicardi & V. Timorin, *"On binary quadratic forms with semigroup property"*, *Proceedings of Steklov Institute (Dedicated to the 70th birthday of V.I. Arnold)* **258 (2007), 23-43.**

V.I. Arnold, *"Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world"*, *Bull. Braz. Math. Soc.* **34 (2003), 1-41.**

M. Bhargava, *"Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations"*, *Ann. of Math.* **159 (2004), 217-250.**

A.G. Earnest & R.W. Fitzgerald, *"Represented value sets of integral binary quadratic forms"*, *Proc. Amer. Math. Soc.* **135 (2007), 3765-3770.**