2008

Multiplicative Properties of Integral Binary Quadratic Forms

A. G. Earnest
Southern Illinois University Carbondale, aearnest@math.siu.edu

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

To appear in *Contemporary Mathematics*.

Contemporary Mathematics

Multiplicative Properties of Integral Binary Quadratic Forms

A.G. Earnest and Robert W. Fitzgerald

Abstract. In this paper, the integral binary quadratic forms for which the set of represented values is closed under k-fold products, for even positive integers k, will be characterized. This property will be seen to distinguish the elements of odd order in the form class group of a fixed discriminant. Further, it will be shown that this closure under k-fold products can always be expressed by a k-linear mapping from $(\mathbb{Z}^2)^k$ to $\mathbb{Z}^2$. In the case $k = 2$, this resolves a conjecture of Aicardi and Timorin.

1. Preliminaries

Throughout this paper, the term *form* will always refer to a nondegenerate integral binary quadratic form $ax_1^2 + bx_1x_2 + cx_2^2$, 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 $\Delta_f > 0$). 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.

A form (a, b, c) is said to be primitive if g.c.d.$(a, b, c) = 1$. Classical Gaussian composition induces a binary operation on the equivalence classes of primitive forms of a fixed discriminant. For our purposes, the salient feature of the composition operation is that for primitive forms f, g of the same discriminant Δ, there exist primitive forms $\hat{f}, \hat{g}$ and h of discriminant Δ, and a bilinear mapping $\sigma : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ such that there is an identity of the type

$$\hat{f}(x)\hat{g}(y) = h(\sigma(x, y)), \tag{1.1}$$

for all $x, y \in \mathbb{Z}^2$. In this case, we will write $[f][g] = [h]$. Under this operation, the set of equivalence classes of primitive forms of a fixed discriminant Δ is a finite abelian group, called the form class group of discriminant Δ, which will be denoted by $\mathfrak{C}_\Delta$. 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 $f^{op} = (a, -b, c)$. A detailed description of the composition operation can be found, for example, in [**6**]. A fresh

2000 *Mathematics Subject Classification.* Primary 11E16; Secondary 11E12, 11R29.

perspective is given in the pioneering work of Bhargava [**5**], which has opened up new directions for broad generalizations of the classical theory.

For a form f, the notation $D([f])$ will denote the set $D(g)$ for any $g \in [f]$. If f and g are primitive forms that represent the integers k and ℓ, respectively, then it can be seen from (1.1) that the forms in the equivalence class $[f][g]$ represent the product $k\ell$; that is,

$$D(f)D(g) \subset D([f][g]). \tag{1.2}$$

Let f be a primitive form. Note that $D(f^{op}) = D(f)$, since $f^{op}(x_1, x_2) = f(x_1, -x_2)$. So $D(f)D(f)D(f) = D(f)D(f^{\mathrm{op}})D(f) = D([f])D([f]^{-1})D([f]) \subseteq D([f])$, where the final containment follows from (1.2). So

$$D(f)D(f)D(f) \subseteq D(f) \tag{1.3}$$

for all primitive forms f. That is, the three-fold product of integers represented by f is again an integer represented by f. That this property extends to all, not necessarily primitive, forms can be seen by writing $f = c_f f_0$ where f_0 is primitive and applying (1.3) to f_0. This property was observed by Arnold [**4**], who refers to it as the *tri-group* property. In fact, this property appears in an earlier paper of Goins [**8**], where it is derived from a triple product formula for certain 2×2 matrices. Moreover, it is shown in both [**4**] and [**8**] that there exists a 3-linear mapping $\sigma : \mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ such that

$$f(x)f(y)f(z) = f(\sigma(x, y, z)) \tag{1.4}$$

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

2. Background

The classical identity

$$(x_1^2 + dx_2^2)(y_1^2 + dy_2^2) = (x_1y_1 + dx_2y_2)^2 + d(x_1y_2 - x_2y_1)^2 \tag{2.1}$$

shows that certain forms f (in this case, those of the type $f = (1, 0, d)$) have the property that their represented value set $D(f)$ is closed under products (that is, $D(f)$ forms a multiplicative semigroup). Arnold initiated the systematic study of forms with this property, which he referred to as *perfect* forms, in [**4**]. In subsequent papers [**1**], [**2**] and [**3**], Aicardi and Timorin have investigated several related conditions that produce such forms. In [**7**], we have shown that the primitive forms f for which $D(f)$ is closed under products are precisely those for which $[f]^3 = 1$ in $\mathfrak{C}_\Delta$. The results for primitive forms are summarized in the following statement.

Proposition 2.1. *Let f be a primitive form of discriminant Δ. The following are equivalent:*

1. *$D(f)$ is closed under products.*
2. *$[f]^3 = 1$ in $\mathfrak{C}_\Delta$.*
3. *There exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that*
$$f = (\alpha^2 - \gamma\delta, \alpha\gamma - \beta\delta, \gamma^2 - \alpha\beta).$$
4. *There exists a bilinear mapping $\sigma : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ such that*
$$f(x)f(y) = f(\sigma(x, y))$$
for all $x, y \in \mathbb{Z}^2$.

SKETCH OF PROOF. The equivalence of (1) and (2) appears in Corollary 2.4 of [**7**]. (2) $\Rightarrow$ (3) can be deduced by direct computation using the characterization of composition given by Bhargava [**5**]. (3) $\Rightarrow$ (4) follows by considering the mapping $\sigma : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}^2$ defined coordinatewise by the equations $\sigma(x,y)_1 = \alpha x_1 y_1 + \gamma x_1 y_2 + \gamma x_2 y_1 + \beta x_2 y_2$ and $\sigma(x,y)_2 = -\delta x_1 y_1 - \alpha x_1 y_2 - \alpha x_2 y_1 - \gamma x_2 y_2$. (4) $\Rightarrow$ (1) is clear. □

For convenience, we will refer to a (not necessarily primitive) form f as being *multiplicative*, *parametrizable* or *normed* if the condition (1), (3) or (4) of Proposition 2.1, respectively, is satisfied for f. As the argument for (3) $\Rightarrow$ (4) above does not depend on primitivity, the following implications hold in general:

$$\text{parametrizable} \Rightarrow \text{normed} \Rightarrow \text{multiplicative}. \tag{2.2}$$

Proposition 2.1 shows that the converses of both of these implications are also true when we restrict to primitive forms. We will see in section 4 that the converse of the second implication is always true (see Theorem 4.2), as conjectured by Aicardi and Timorin [**3**]. However, an example appearing in section 5 shows that the converse of the first implication is not true in general.

In the rest of this paper, a general form f will be written as $f = c_f f_0$, where c_f is the g.c.d. of the coefficients of f and f_0 is primitive. The main result of [**7**] is:

THEOREM 2.2. *f is multiplicative if and only if $c_f \in D(f_0) \cup D([f_0]^3)$.*

From this result, we obtain the equivalence of the three conditions in (2.2) for the case of diagonal forms.

COROLLARY 2.3. *Let f be a diagonal form. The following are equivalent:*

(1) *f is multiplicative.*
(2) *$c_f \in D(f_0)$.*
(3) *f is parametrizable.*
(4) *f is normed.*

PROOF. (1) $\Rightarrow$ (2): Since f_0 is diagonal, $f_0^{op} = f_0$ and so $[f_0]^3 = [f_0][f_0^{\mathrm{op}}][f_0] = [f_0][f_0]^{-1}[f_0] = [f_0]$. (2) $\Rightarrow$ (3): Let $f_0 = (a,0,c)$. Since $c_f \in D(f_0)$, there exist $u, v \in \mathbb{Z}$ such that $c_f = au^2 + cv^2$. Taking $\alpha = au, \beta = -cu, \gamma = cv, \delta = -av$ produces the desired parametrization of f. The remaining implications are clear. □

In the remaining three sections of this paper, we will consider each of the properties in (2.2) in more detail. The discussion of multiplicative and normed forms will be set in the more general context of k-fold products for arbitrary nonnegative even integers k.

3. Multiplicative forms

Throughout this section, k and ℓ will denote nonnegative integers.

DEFINITION. A form f is *k-multiplicative* if

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

When $k = 0$ we take the empty product to be 1. Thus 0-multiplicative simply means $1 \in D(f)$.

PROPOSITION 3.1. (1) *If f is k-multiplicative then f is $(k+2)$-multiplicative.*
(2) *Every form f is k-multiplicative for each odd k.*

PROOF. (1) For any $a_1, a_2, \dots, a_{k+2} \in D(f)$, $a_1 a_2 \cdots a_k \in D(f)$, since f is k-multiplicative. Then $(a_1 a_2 \cdots a_k) a_{k+1} a_{k+2}$ is a product of three elements of $D(f)$ and so is in $D(f)$ by (1.3).
(2) Each f is 1-multiplicative by definition. Apply (1). □

Thus, in the remainder of this paper we will only be interested in the property k-multiplicative when k is even. The main theorem characterizing forms with this property is the following, which generalizes Theorem 2.3 of our previous paper [**7**].

THEOREM 3.2. *Let k be even. The following are equivalent:*
(1) *f is k-multiplicative.*
(2) *There exists a prime p with $p \in D(f_0)$ and $c_f^k p^k \in D(f)$.*
(3) *$c_f^{k-1} \in D([f_0]^{\ell+1})$, for some even ℓ, $0 \le \ell \le k$.*

The main step in the proof of this theorem is contained in the following lemma.

LEMMA 3.3. *Let k be even. Suppose f_0 is a primitive form, p is a prime, and $d \in \mathbb{Z}$ with $p \in D(f_0)$ and $dp^k \in D(f_0)$. Then $d \in D([f_0]^{\ell+1})$ for some even ℓ, $0 \le \ell \le k$.*

For the proof of this lemma, it is convenient to recall the key lemma (Lemma 2.2) of our previous paper [**7**].

LEMMA 3.4. *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 $n \in D([g^{op}][h])$.*

PROOF OF LEMMA 3.3. The result is clear if $k = 0$ so suppose $k > 0$. We can assume that k is the least positive, even integer with $dp^k \in D(f_0)$.
Claim: $dp^{k-j} \in D([f_0]^{j+1})$, for $0 \le j \le k$.
We prove this by induction; the case $j = 0$ is our hypothesis. Say $j > 0$ and suppose $dp^{k-j} \in D([f_0]^{j+1})$. Lemma 3.4, with $g = f_0$, $[h] = [f_0]^{j+1}$ and $n = dp^{k-j-1}$, gives $dp^{k-j-1} \in D([f_0]^{j+2}) \cup D([f_0]^j)$. If $dp^{k-(j+1)} \in D([f_0]^{j+2})$ then we have completed the induction argument and we are done. So suppose

$$dp^{k-j-1} \in D([f_0]^j).$$

Let m be the least positive integer such that $dp^{k+m-2j-1} \in D([f_0]^m)$. Note that this occurs if $m = j$. And if $m = 1$ then we have contradicted the minimality of k (as $j > 0$). Hence $1 < m \le j$. Lemma 3.4, with $g = f_0$, $[h] = [f_0]^m$ and $n = dp^{k+m-2j-2}$, gives

$$dp^{k+m-2j-2} \in D([f_0]^{m+1}) \cup D([f_0]^{m-1}).$$

Now $dp^{k+(m-1)-2j-1} \in D([f_0]^{m-1})$ contradicts the minimality of m. Hence we have:

$$dp^{k-(j+1)} = dp^{j-m+1} \cdot p^{k+m-2j-2} \in D([f_0]^{j-m+1}) D([f_0]^{m+1}) \subset D([f_0]^{j+2}),$$

which completes the induction proof of the **Claim**.
Taking $j = k$ in the **Claim** gives $d \in D([f_0]^{k+1})$. □

PROOF OF THEOREM 3.2. (1) $\Rightarrow$ (2) is clear: f_0 represents a prime p since f_0 is primitive; take each $a_i = c_f p$ in the definition. (2) $\Rightarrow$ (3) is Lemma 3.3, as $c_f^{k-1} p^k \in D(f_0)$. For (3) $\Rightarrow$ (1), let $c_f a_i \in D(f)$ for $1 \leq i \leq k$. Let $2s = k - \ell$. Then

$$\prod_{i=1}^{k} a_i = (a_1 a_2 a_3) \cdots (a_{3s-2} a_{3s-1} a_{3s}) a_{3s+1} a_{3s+2} \cdots a_k$$

is in $D([f_0]^{s+(k-3s)}) = D([f_0]^{\ell}) = D([f_0]^{-\ell})$, where we have used (1.3) to conclude that each product of three a_i's is again in $D(f_0)$. Hence, by (3),

$$c_f^{k-1} \prod_{i=1}^{k} a_i \in D([f_0]^{\ell+1}) D([f_0]^{-\ell}) \subset D(f_0)$$

and so

$$\prod_{i=1}^{k} (c_f a_i) \in c_f D(f_0) = D(f).$$

This completes the proof. □

When f is primitive (and so $c_f = 1$), condition (3) says $[f]^{\ell+1} = 1$. We thus get:

COROLLARY 3.5. *Let f be a primitive form of discriminant Δ and let k be even. The following are equivalent:*

(1) *f is k-multiplicative.*
(2) *There is a prime $p \in D(f)$ with $p^k \in D(f)$.*
(3) *The order of $[f] \in \mathfrak{C}_\Delta$ is odd and at most $k+1$.*

DEFINITION. Let k be even. A form f is *strictly k-multiplicative* if f is k-multiplicative but not ℓ-multiplicative for any even ℓ, $0 \leq \ell < k$.

COROLLARY 3.6. *Let f be a primitive form of discriminant Δ and let k be even. The following are equivalent:*

(1) *f is strictly k-multiplicative.*
(2) *There is a prime $p \in D(f)$ such that $p^k \in D(f)$ but $p^\ell \notin D(f)$ for even ℓ, $0 \leq \ell < k$.*
(3) *The order of $[f] \in \mathfrak{C}_\Delta$ is $k+1$.*

4. Normed forms

Throughout this section, n will denote a positive integer. To simplify notation, let $V = \mathbb{Z} \times \mathbb{Z}$. A map $\sigma : V^n \to V$ is n-linear if it is linear in each coordinate.

DEFINITION. A form f is *n-normed* if there exists n-linear $\sigma : V^n \to V$ such that

$$f(v_1) f(v_2) \cdots f(v_n) = f(\sigma(v_1, v_2, \ldots, v_n)),$$

for all $v_1, v_2, \ldots, v_n \in V$.

Note that a form is 2-normed by this definition if and only if it is normed, in the terminology introduced in section 2. For example, the identity (2.1) shows that forms of the type $(1, 0, d)$ are 2-normed.

LEMMA 4.1. (1) *Every form f is 3-normed.*

(2) *Suppose $f_1, f_2, \dots, f_n, g$ are primitive forms of discriminant Δ. If $\prod_{i=1}^n [f_i] = [g]$ in $\mathfrak{C}_\Delta$ then there exists n-linear $\sigma : V^n \to V$ such that*

$$f_1(v_1)f_2(v_2)\cdots f_n(v_n) = g(\sigma(1, v_2, \dots, v_n)),$$

for all $v_1, v_2, \dots v_n \in V$.

PROOF. (1) This follows from (1.4).

(2) We use induction on n. When $n = 1$ we have $f_1 \sim g$. So there is $M \in SL_2(\mathbb{Z})$ such that $f_1(v) = g(Mv)$ for all $v \in \mathbb{Z}$ (viewed as a column vector). Set $\sigma(v) = Mv$.

Let h be a primitive form such that $\prod_{i=1}^{n-1}[f_i] = [h]$. By induction, there is $(n-1)$-linear τ such that

$$f_1(v_1)f_2(v_2)\cdots f_{n-1}(v_{n-1}) = h(\tau(v_1, v_2, \dots, v_{n-1})).$$

We have $[f_n][h] = [g]$ in $\mathfrak{C}_\Delta$. By (1.1) there exist forms $f_n' \in [f_n]$, $h' \in [h]$ and $g' \in [g]$ and a bilinear mapping $\gamma : V^2 \to V$ such that $f_n'(v_n)h'(w) = g'(\gamma(v_n, w))$. And there exist isometries $\beta_i : V \to V$ such that $f(v) = f_n'(\beta_1(v))$, $h(v) = h'(\beta_2(v))$ and $g(v) = g'(\beta_3(v))$, for all $v \in V$. Then

$$f_n(v_n)h(w) = g(\beta_3(\gamma(\beta_1(v_n), \beta_2(w)))).$$

Let $\nu : V^2 \to V$ be given by $\nu(v, w) = \beta_3(\gamma(\beta_1(v), \beta_2(w)))$. Clearly ν is bilinear. We obtain:

$$\begin{aligned} f_1(v_1)f_2(v_2)\cdots f_{n-1}(v_{n-1})f_n(v_n) &= f(v_n)h(\tau(v_1, v_2, \dots, v_{n-1})) \\ &= g(\nu(v_n, \tau(v_1, v_2, \dots, v_{n-1})). \end{aligned}$$

Clearly $\sigma(v_1, v_2, \dots, v_n) = \nu(v_n, \tau(v_1, \dots, v_{n-1}))$ is n-linear. □

THEOREM 4.2. *Let $k \geq 2$ be an even integer. A form f is k-multiplicative iff it is k-normed.*

PROOF. Clearly k-normed implies k-multiplicative. So suppose f is k-multiplicative. By Theorem 3.2, $c_f^{k-1} \in D([f_0]^{\ell+1})$, for some even $\ell \leq k$. Pick $g \in [f_0]^{\ell+1}$ and suppose $g(u) = c_f^{k-1}$, where $u \in V$. Write $k - \ell = 2s$.

Now by Lemma 4.1 (1), there exists 3-linear β such that

$$f_0(v_1)f_0(v_2)f_0(v_3) = f_0(\beta(v_1, v_2, v_3)).$$

For $v = (x, y) \in V$, let $v' = (x, -y)$. Now

$$[g^{op}][f_0]^s[f_0]^{k-3s} = [f_0]^{-(\ell+1)}[f_0]^\ell = [f_0^{op}],$$

in $\mathfrak{C}_\Delta$. Hence, by Lemma 4.1 (2), there exists $(k - 2s + 1)$-linear τ such that

$$g^{op}(z)\prod_{j=1}^{s} f_0(w_j)\prod_{i=3s+1}^{k}(v_i) = f_0^{op}(\tau(z, w_1, \dots w_s, v_{3s+1}, \dots v_k)).$$

We have:

$$\begin{aligned} c_f^{k-1}f(v_1)f(v_2)\cdots f(v_k) &= g^{op}(u')\prod_{j=1}^{s} f_0(\beta(v_{3j-2}, v_{3j-1}, v_{3j}))\prod_{i=3s+1}^{k} f_0(v_i) \\ &= f_0(\tau(u', \beta(v_1, v_2, v_3), \dots, \beta(v_{3s-2}, v_{3s-1}, v_{3s}), v_{3s+1}, \dots, v_k)'). \end{aligned}$$

Let σ map $(v_1, v_2, \ldots, v_k)$ to

$$\tau(u', \beta(v_1, v_2, v_3), \ldots, \beta(v_{3s-2}, v_{3s-1}, v_{3s}), v_{3s+1}, \ldots, v_k)'.$$

Clearly σ is k-linear. We have $c_f^{k-1} f_0(v_1) \cdots f_0(v_k) = f_0(\sigma(v_1, \ldots, v_k))$. Multiply by c_f to get:

$$f(v_1)f(v_2)\cdots f(v_k) = f(\sigma(v_1, v_2, \ldots, v_k)),$$

showing that f is k-normed. □

REMARK. Specialized to the case $k = 2$, Theorem 4.2 establishes the truth of the Conjecture 0.1 of [**3**].

5. Parametrizable forms

Aicardi and Timorin [**3**] characterize all the forms f and bilinear pairings σ for which the identity

$$f(x)f(y) = f(\sigma(x, y))$$

holds for all $x, y \in V$. These fall into four types, which are enumerated in Theorem 1.1 of [**3**]. An examination of this result shows that in the first three cases the forms are of the type rg where $r \in D(g)$, and in the remaining case the form f is parametrizable. From this we conclude that if a form is multiplicative but not parametrizable, then it must be of the type rg with $r \in D(g)$.

We are thus led to further investigate the parametrizability of forms of the type rf for $r \in D(f)$. For forms of this type, we give criteria for parametrizability in terms of the solutions of $f(u, v) = ra^2$.

PROPOSITION 5.1. *Let $f = (a, b, c)$ and $r \in D(f)$. Then rf is parametrizable if and only if there exist $\alpha, \delta \in \mathbb{Z}$ such that $f(\alpha, \delta) = ra^2$ and either:*

(1) *$\delta \neq 0$, $\delta \mid (\alpha^2 - ra)$, and $\delta^2 \mid (\alpha^3 - ra\alpha + rb\delta)$; or*
(2) *$\delta = 0$, $\alpha \mid rb$, and $\alpha^3 \mid (r^2b^2 - rc\alpha^2)$.*

PROOF. Suppose that rf is parametrizable. So there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that:

$$ra = \alpha^2 - \gamma\delta, rb = \alpha\gamma - \beta\delta \text{ and } rc = \gamma^2 - \alpha\beta. \tag{5.1}$$

Assume first that $\delta \neq 0$. Solving for γ in the first equation of (5.1) gives

$$\gamma = \frac{\alpha^2 - ra}{\delta},$$

and it follows that $\delta \mid (\alpha^2 - ra)$. The second equation gives

$$\beta = \frac{\alpha\gamma - rb}{\delta} = \frac{\alpha(\alpha^2 - ra) - rb\delta}{\delta^2} = \frac{\alpha^3 - ra\alpha - rb\delta}{\delta^2},$$

giving $\delta^2 \mid (\alpha^3 - ra\alpha - rb\delta)$. The third equation of (5.1) then becomes

$$rc = (\frac{\alpha^2 - ra}{\delta})^2 - \alpha(\frac{\alpha^3 - ra\alpha - rb\delta}{\delta^2}),$$

from which it follows that

$$ra^2 = a\alpha^2 = b\alpha\delta + c\delta^2 = f(\alpha, \delta).$$

For the converse, assume that $f(\alpha, \delta) = ra^2$ and use the above expressions for β and γ. It is straightforward to verify that the equations in (5.1) hold.

Now suppose that (5.1) holds with $\delta = 0$. The first equation of (5.1) gives

$$f(\alpha, \delta) = f(\alpha, 0) = a\alpha^2 = ra^2.$$

The second equation of (5.1) becomes $rb = \alpha\gamma$ and so $\alpha \mid rb$. Substituting this expression for γ into the third equation of (5.1) and solving for β yields

$$\beta = \frac{r^2b^2 - rc\alpha^2}{\alpha^3},$$

and hence $\alpha^3 \mid (r^2b^2 - rc\alpha^2)$, as claimed. The converse again follows by direct substitution of the above expressions for β and γ into (5.1) and using the condition that $f(\alpha, 0) = ra^2$. □

This proposition makes it easy to analyze the following example, which shows that the converse of the first implication in (2.2) does not hold in general.

Example. The form $(4, -2, 12)$ is not parametrizable. To see this, apply Proposition 5.1 with $r = 2$ and $f = (2, -1, 6)$. The only representations of $ra^2 = 8$ by the form f are $(\pm 2, 0)$. Condition (2) of Proposition 5.1 is not satisfied for either of these, since $\alpha^3 = \pm 8$ and $r^2b^2 - rc\alpha^2 = -44$.

When examining the multiples of a fixed primitve form f by represented values r, it generally happens that rf is parametrizable for some values of r but not others. However, it can never be the case that for a given primitive form f there exist no values of r for which rf is parametrizable.

Corollary 5.2. *For any form f, there exist infintely many $r \in D(f)$ such that rf is parametrizable.*

Proof. By replacing f with an equivalent form if necessary, we can assume that $f = (a, b, c)$ with $a \neq 0$. Take $r_0 = f(a, a)$. It is easily checked that the conditions of Proposition 5.1 (1) are satisfied. So $r_0 f$ is parametrizable. For any integers $s \neq 0$, $r_0 s^2 f$ is also parametrizable (replace each parameter ρ by $s\rho$). □

On the other hand, the following result shows that it can happen that rf is parametrizable for all $r \in D(f)$.

Corollary 5.3. *If $f = (a, b, c)$ and $a \mid b$, then rf is parametrizable for every $r \in D(f)$.*

Proof. For $r = f(u, v)$, take $\alpha = au$ and $\delta = av$.

Case 1: $v \neq 0$. In this case

$$\alpha^2 - ra = a^2u^2 - a(au^2 + buv + cv^2) = -av(bu + cv) = -\delta(bu + cv).$$

So $\delta \mid (\alpha^2 - ra)$. Further,

$$\begin{aligned}\alpha^3 - ra\alpha + rb\delta &= (au)^3 - (au^2 + buv + cv^2)a(au) + (au^2 + buv = cv^2)b(av) \\ &= -a^2cuv + abuv^2 + abcv^3.\end{aligned}$$

The last expression in the previous line is divisible by $\delta^2 = a^2v^2$ since $a \mid b$; hence, $\delta^2 \mid \alpha^3 - ra\alpha + rb\delta$ and the conditions of Proposition 5.1 (1) are satisfied.

Case 2: $v = 0$. In this case, $r = f(u, 0) = a\alpha^2$. So $rb = (a\alpha^2)b$ is divisible by α, and

$$r^2b^2 - rc\alpha^2 = (a\alpha^2)^2b^2 - (a\alpha^2)c\alpha^2 = \alpha^4(a^2\alpha b^2 - ac)$$

is divisible by α^3. Hence, the conditions of Proposition 5.1 (2) are satisfied. □

References

[1] F. Aicardi, *On the number of perfect binary quadratic forms*, Experiment. Math. **13** (2004), 451–457.

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

[3] F. Aicardi and V. Timorin, *On binary quadratic forms with semigroup property* Proc. Steklov Inst. (Dedicated to the 70th birthday of V.I. Arnold) **258** (2007), 23–43.

[4] 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.

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

[6] D. A. Cox, *Primes of the form x^2+ny^2. Fermat, class field theory and complex multiplication* John Wiley & Sons, New York, 1989.

[7] A.G. Earnest and R.W. Fitzgerald, *Represented value sets of integral binary quadratic forms* Proc. Amer. Math. Soc. **135** (2007), 3765–3770.

[8] E. Goins, *A ternary algebra with applications to binary quadratic forms* Contemp. Math. **284** (2001), 7–12.

Department of Mathematics, Southern Illinois University Carbondale
Current address: Department of Mathematics, Mailcode 4408, Southern Illinois University, 1245 Lincoln Drive, Carbondale, Illinois 62901
E-mail address: aearnest@math.siu.edu

Department of Mathematics, Southern Illinois University Carbondale
Current address: Department of Mathematics, Mailcode 4408, Southern Illinois University, 1245 Lincoln Drive, Carbondale, Illinois 62901
E-mail address: rfitzg@math.siu.edu