THE CONSTRUCTION OF POSITIVE TERNARY QUADRATIC FORMS[1]

GORDON PALL

1. **Binary quadratic forms.** A positive, binary quadratic form $f=(a, t, b)=ax^2+2txy+by^2$ (a, t, and b real numbers) is equivalent to one and only one form in which

$$(1) \qquad |2t| \leqq a \leqq b, \quad t \geqq 0 \text{ if } a = b \text{ or } a = |2t|.$$

Such a form is called *reduced*, and has the further properties that: (i) a is the least number properly represented by f; (ii) $ab \leqq 4\Delta/3$, where $\Delta=ab-t^2$; (iii) among all forms equivalent to f with the minimum a as first coefficient, b is the least possible.

To obtain all reduced, classical, binary quadratic forms of a given determinant Δ, we have the following well known algorithm: factor $\Delta+t^2$ ($\pm t=0, 1, \cdots, (\Delta/3)^{1/2}$) as ab, with $|2t| \leqq a \leqq b$, in all possible ways; but discard forms with $t<0$ if $a=b$ or $|2t|$.

2. **Ternaries.** We develop in this article a similar method of finding a unique form in every class of integral ternary quadratic forms of a *given* determinant, or in a given order or genus. The methods of reduction hitherto devised (Seeber [1], Eisenstein [2], Selling [3]) are entirely adequate if one wishes to calculate all reduced forms of determinant less than a certain fixed value, but are not connected closely enough with the invariants to make the computation of forms with given values for their invariants practicable. By the method of this article one can obtain the reduced forms in a given genus of determinant around 1000 in fifteen minutes.

Our reduced form is not the same as that of Eisenstein or Selling, but we shall see how to pass from our form to that of Eisenstein.

Eisenstein found that within every class of real, positive, ternary quadratic forms $f=(a, b, c, r, s, t)=ax^2+by^2+cz^2+2ryz+2sxz+2txy$ there is a unique form (to be called *E-reduced*) satisfying the following inequalities:

$$(2) \qquad r, s, t \text{ all } > 0, \text{ or all } \leqq 0;$$

$$(3) \qquad a \geqq 2|s|, \quad a \geqq 2|t|, \quad b \geqq 2|r|;$$

$$(4) \qquad a \leqq b \leqq c; \; a+b+2r+2s+2t \geqq 0;$$

$$(5) \qquad \text{if } a = b, \; |r| \leqq |s|; \text{ if } b = c, \; |s| \leqq |t|;$$

[1] Presented to the Society, May 2, 1941.

(6) $$\text{if } a + b + 2r + 2s + 2t = 0,\ a + 2s + t \leqq 0;$$

(7) $$\text{if } a = 2t,\ s \leqq 2r;\ \text{if } a = 2s,\ t \leqq 2r;\ \text{if } b = 2r,\ t \leqq 2s;$$

(8) $$\text{if } a = -2t,\ s = 0;\ \text{if } a = -2s,\ t = 0;\ \text{if } b = -2r,\ t = 0.$$

Here the conditions (2), (3), and (4) are to be regarded as the principal inequalities, and determine the planar boundaries of the fundamental cell of reduced forms. From the principal inequalities readily follows Seeber's inequality $abc \leqq 2d$, where d is the determinant of f.

The number of possibilities for a given d is greatly limited; but no procedure is indicated for sifting out forms of a given determinant.

It may be observed that in an E-reduced form a is the minimum, and, among all forms equivalent to f, b is as small as it can be for the predetermined a, and c as small as it can be for the preceding a and b.

Eisenstein used two methods in constructing his table of integral ternaries. One was to write down sequences of forms satisfying (2)–(8), and to calculate their determinants. The other produced all forms of a given determinant with minimum $a = 1$, 2, or 3; but (2)–(8) are ill adapted to extend this method to $a > 3$. This article provides such an extension.

Let $F = (A, B, C, R, S, T)$ be the adjoint of f. On account of the rarity of Seeber's book it is worth noting that Seeber's conditions differ from Eisenstein's only in having (6), (7), and (8) replaced by

$$\text{if } a + b + 2r + 2s + 2t = 0,\ 2\,|\,R\,| \leqq C;\ \text{if } a = \pm 2t,\ 2\,|\,T\,| \leqq B;$$
$$\text{if } a = \pm 2s,\ 2\,|\,S\,| \leqq C;\ \text{if } b = \pm 2r,\ 2\,|\,R\,| \leqq C.$$

The equivalence of these conditions to (6)–(8) is obvious from identities like those we use in §4. It may be worth noting in regard to our method that while certain coefficients of F start off our process of construction (§7), only linear expressions in the coefficients of f need to be formed in testing for duplicates.

3. **A new reduced form.** We call the real, positive ternary quadratic form $f = (a, b, c, r, s, t)$ *reduced*, if the following inequalities hold:

(2) $$r, s, t \text{ all } > 0, \text{ or all } \leqq 0;$$

(9) $$a \leqq b,\ a \leqq c,\ a \leqq b + c - 2r,\ 0 \leqq b + c + 2r + 2s + 2t;$$

(10) $$a \geqq 2\,|\,s\,|,\ a \geqq 2\,|\,t\,|\ ;$$

(11) $$2\,|\,R\,| \leqq C \leqq B, \text{ where } R = st - ar,\ C = ab - t^2,\ B = ac - s^2;$$

(12) $$\text{if } a = -2s \text{ or } -2t, \text{ then } t \text{ or } s = 0;$$

(13) $$\text{if } a = 2s \text{ or } 2t, \text{ then } R \leqq 0 \text{ (i.e., } t \text{ or } s \leqq 2r, \text{ resp.});$$

(14) if $C = B$, $b \leqq c$ (hence $s^2 \geqq t^2$); if $C = -2R$, $b \geqq 2r$; if $C = 2R$, $a + 2s + t \geqq 0$;

(15) if $a = b$, $|r| \leqq |s|$; if $a = c$, $|r| \leqq |t|$;

(16) if $a = b$ or c, then $a + r + s + t \geqq 0$;

(17) if $a = b + c - 2r$ then $b \leqq r + t$;

(18) if $b + c + 2r + 2s + 2t = 0$, then $b + 2t + r \leqq 0$ and $b \leqq c$.

It should be observed that (9_4), (12), (14_3), (16), and (18) are trivial if (2_1) holds; and (9_3), (13), (14_2), and (17) are trivial if (2_2) holds.

THEOREM 1. *Every class of real, positive, ternary quadratic forms contains one and only one reduced form.*

We prove in this section that every class contains a reduced form. Denote the adjoint of f by $F=(A, B, C, R, S, T)$, so that $C=ab-t^2$ and $BC-R^2=ad$. We can replace f by an equivalent form in which:

(19) a is the minimum of f; C is the least possible with the aforesaid a; and B is the least possible with the predetermined a and C.

We have $2|R| \leqq C \leqq B$ by (19_2) and (19_3). For replacing y by $y \mp z$ in f replaces a by a, C by C, B by $C \pm 2R + B$.

Replacing x by $x+hy+kz$ in f corresponds in the adjoint transformation to replacing y by $y-hx$ and z by $z-kx$ in F, hence leaves C, R, and B unchanged but replaces s by $s+ak$, t by $t+ah$. We thus secure (10) and (11).

We get (2) by changing signs of an even number of x, y, z.

We next show that conditions (9) and (15)–(18) all follow from (19). First notice that (19_1) implies (9): $a \leqq f(0, 1, 0), \cdots, f(1, 1, 1)$.

Denote by (X, Y, Z) the unimodular transformation replacing x, y, z by X, Y, Z. If $a=b$, use $(-y, -x, -z)$ and get (a, a, c, s, r, t); if $a=c$, $(-z, -y, -x)$ and (a, b, a, t, s, r). Hence (19_3) and (19_2) imply that $ac-r^2 \geqq ac-s^2$, and $ab-r^2 \geqq ab-t^2$, or (15).

If $a=b-2r+c$, the transformation $(z, -x, x-y)$ carries f into $(b-2r+c, c, a, -s, s-t, r-c)$. Hence $(b-2r+c)c-(r-c)^2=bc-r^2$ $=b(a+2r-b)-r^2=ab-(b-r)^2 \geqq ab-t^2$, giving (17).

If $a=b$, $(y-z, x-z, -z)$ replaces f by $(a, a, \sigma, -a-t-s, -a-t-r, t)$, where $\sigma=a+b+c+2r+2s+2t$; if $a=c$, $(-y+z, -y, x-y)$ replaces f by $(a, \sigma, a, -a-s-t, s, -a-r-s)$. Hence $a\sigma-(a+t+r)^2$ $\geqq ac-s^2$, or $(a+s)^2 \geqq (r+t)^2$; and $a\sigma-(a+r+s)^2 \geqq ab-t^2$, or $(a+t)^2$ $\geqq (r+s)^2$; giving (16).

Let $b+c+2r+2s+2t=0$. Applying $(-x+z, -x+y, -x)$ and

$(x, x-z, x+y)$, we get $(a, b, a, t, -a-t-s, -t-b-r)$ and $(a, c, b, -r, -b-r-t, c+r+s)$. By (19_2), $ab-(t+b+r)^2 \geqq ab-t^2$, or $b+2t+r \leqq 0$. Also, $ac-(c+r+s)^2 \geqq ab-t^2$, or $t^2-(c+r+s)^2 \geqq a(b-c) = a(-2c-2r-2s-2t)$; if b could exceed c, then $-c-r-s-t = b+r+s+t>0$, whence $c+r+s-t \geqq 2a$, while $c<-r-s-t$; thus $-r-s-t>2a-r-s+t$, $-2t>2a$, contrary to (10). This gives (18).

If $a=-2s$ and $t\neq 0$, $(x-z, y, -z)$ carries f into $f_1=(a, b, c, -t-r, -s, -t)$, with $R_1=-R$, $C_1=C$, $B_1=B$. Here $(-s)(-t)<-2s(-t-r)$. Hence (13) holds for f_1. If $a=-2t$ and $s\neq 0$, use $(-x-y, -y, z)$ and $(a, b, c, -r-s, -s, -t)$.

If $a=2s$ and $R=s(t-2r)>0$, $(-x-z, -y, z)$ yields $(a, b, c, t-r, s, t)$, with $t-2(t-r)<0$. If $a=2t$ and $R>0$, use $(-x-y, y, -z)$ and $(a, b, c, s-r, s, t)$.

If $C=B$, we may replace f by (a, c, b, r, t, s), and thus secure (14_1). This does not affect any conditions so far obtained.

If $C=-2R$ and $b<2r$, $(-x, -y-z, z)$ replaces f by $f_2=(a, b, b-2r+c, b-r, t-s, t) \sim (a, b, b-2r+c, r-b, t-s, -t)$, with $R_2=-R-C=R$, $B_2=B$, and $b \geqq 2(b-r)$. The minimal conditions (9) and (15)–(18) must hold in consequence of (19); and (10), (11) also hold, for f_2. If $a=2t$ and $s=t$ we have (12); if $a=2t$ and $s<t$, $R_2=R \leqq 0$ by (13) for f. If also $C=B$, and $c<2r$, we use $(a, b-2r+c, b, b-r, t, t-s)$, and have $b-2r+c \geqq 2(b-r)$ since $b \leqq c$ by (14_1) for f.

Finally let $C=2R$, $a+2s+t<0$. Then $(-x+z, -y+z, z)$ carries f into $(a, b, \sigma, -t-b-r, -a-t-s, t)$, with C, R, and B unchanged. Here $a \geqq 2(a+t+s)$ since $a+2s+2t<0$; and we cannot have $a=-2t$ since then $s=0$ by (12) for f. But $a+2(-a-t-s)+t=-(a+2s+t) >0$. If also $C=B$ and $a+c+2r+2s+2t<0$, use $(a, \sigma, b-t-b-r, t, -a-t-s)$, where $a+2t+(-a-t-s)=t-s \geqq 0$ by (14_1) for f.

4. **Some properties of a reduced form.** Before completing the proof of Theorem 1, we note further inequalities for a reduced form:

(20) if $b = 2r$, $t \leqq 2s$; if $b < 2r$, $t < 2s$

(21) if $c = 2r$, $s \leqq 2t$; if $c < 2r$, $s < 2t$

[for, $0 \leqq C + 2R = a(b - 2r) + t(2s - t)$, $B + 2R$ similarly];

if $r, s, t \leqq 0$, then $b \geqq -2r$ and $c \geqq -2r$;

(22) if $b = -2r$, $t = 0$; if $c = -2r$, $s = 0$

[for, $0 \leqq C - 2R = a(b + 2r) - t(t + 2s)$, $B - 2R$ similarly];

(23) if $r, s, t > 0$, then $5b > 8r$ and $5c > 8r$

[for, $C>-2R$ by (14_2), $s^2-(t-s)^2>a(2r-b)$, $ab\geqq 4s^2$, $b>4(2r-b)$; $B\geqq -2R$, $c\geqq 4(2r-c)$, equality implying $s=t$, $c\geqq b$];

$$c+|t|\geqq b+|s|\ ;\qquad \text{if } b=c,\ |s|\leqq|t|\ ;\ \text{if } b>c,\ |s|<|t| \tag{24}$$

[for, $0\leqq B-C=(t-s)(t+s)-a(b-c)\leqq a(c-b\pm(t-s))$];

$$\text{if } r, s, t>0,\ c\geqq r+s \tag{25}$$

[for, $a\leqq b-2r+c$, $c-b\geqq s-t$, $c-(a+2r-c)\geqq s-t$, $2c\geqq 2r+a+s-t\geqq 2r+2s$];

$$\text{if } r, s, t\leqq 0,\ c+2s+r\geqq \tfrac{1}{2}(b-c) \tag{26}$$

[for, by (9_4), $c+2s+r\geqq c+2s-\frac{1}{2}b-\frac{1}{2}c-s-t=s-t-\frac{1}{2}(b-c)$];

$$\text{if } a+b+2r+2s+2t=0, C=2R \text{ if and only if } a+2s+t=0,\ \text{and } C>2R \text{ if and only if } a+2s+t<0; \tag{27}$$

$$\text{if } a+b+2r+2s+2t<0, \text{ then } a+2s+t<0$$

[for, $C-2R=a(a+b+2r+2s+2t)-(a+t)(a+2s+t)$];

$$\text{if } a+c+2r+2s+2t=0,\ B\geqq 2R \text{ if and only if } a+2t+s\leqq 0 \tag{28}$$

[for, $B-2R=a(a+c+2r+2s+2t)-(a+s)(a+2t+s)$].

We note that we cannot have $C=2R$ if $r, s, t>0$, nor $C=-2R$ if $r, s, t\leqq 0$. Thus if $r, s, t>0$, $ab>\frac{1}{4}ab+\frac{1}{2}ab\geqq t^2+2st-2ar$.

5. **The equivalent Eisenstein-reduced form.** We shall now exhibit for any reduced $f=(a, b, c, r, s, t)$ the equivalent E-reduced form; and Theorem 1 will follow when we verify that no such E-reduced form is equivalent to two distinct reduced forms. Each of the following fourteen forms is obtained from f by an unimodular transformation, respectively: (x, y, z), $(-x, -z, -y)$, $(-x, -y-z, z)$, $(x, y+z, -y)$, $(x, -y+z, -z)$, $(-x, -y+z, +y)$, $(-x, z, y-z)$, $(x, -y, y-z)$, (x, y, z), $(-x, -z, -y)$, $(-x+z, -y+z, z)$, $(x-z, -z, y-z)$, $(x-y, -y+z, -y)$, $(-x+y, y, y-z)$.

	Case $r, s, t>0$	E-reduced form equivalent to f
1°	$2r\leqq b\leqq c$	(a, b, c, r, s, t)
2°	$2r\leqq c<b$	(a, c, b, r, t, s)

	Case $r, s, t>0$	E-reduced form equivalent to f
3°	$b<2r\leqq c,\ s<t$	$(a, b, b-2r+c, b-r, t-s, t)$
4°	$b\leqq c<2r,\ s<t$	$(a, b-2r+c, b, b-r, t, t-s)$
5°	$b<2r\leqq c,\ t\leqq s$	$(a, b, b-2r+c, r-b, t-s, -t)$
6°	$b\leqq c<2r,\ t\leqq s$	$(a, b-2r+c, b, r-b, -t, t-s)$
7°	$c<2r\leqq b$	$(a, c, b-2r+c, r-c, s-t, -s)$
8°	$c<b<2r$	$(a, b-2r+c, c, r-c, -s, s-t)$

Use the abbreviation $\sigma=a+b+c+2r+2s+2t$.

	Case $r, s, t\leqq 0$	E-reduced form equivalent to f
9°	$b\leqq c,\ \sigma-c\geqq 0$	(a, b, c, r, s, t)
10°	$c<b,\ \sigma-b\geqq 0$	(a, c, b, r, t, s)
11°	$\sigma-c<0,\ \sigma-b\geqq 0$	$(a, b, \sigma, -t-b-r, -a-t-s, t)$
12°	$\sigma-c\geqq 0,\ \sigma-b<0$	$(a, c, \sigma, -s-c-r, -a-t-s, s)$
13°	$b\leqq c,\ \sigma-c<0,\ \sigma-b<0$	$(a, \sigma, b, -t-b-r, t, -a-t-s)$
14°	$c<b,\ \sigma-c<0,\ \sigma-b<0$	$(a, \sigma, c, -c-r-s, s, -a-t-s)$

We first verify that the forms in the last column satisfy the conditions of E-reduction. We cannot have $a=b$ in 3°–6°, nor $a=c$ in 7°–8°, since then by (15) $r\leqq s\leqq \frac{1}{2}b$, or $r\leqq t\leqq \frac{1}{2}c$. Nor can $a=b-2r+c$ in 7°–8°, for then $c<b\leqq r+t$, $a<r+t-2r+r+t=2t$. We use (23) for (2) in 3°–8°; (10) for (3); (9) for (4_1); (10) for (4_2) in 5°–8°, (6) being vacuous in 5°, 7°, and 8°; (14) and (24) in 1°–2°, (16) in 3°–6°; as to (6) and (8) in 6°, if $b=c$, $s=t$ by (24); we use (13) and (20)–(21) for (7) in 1°–2°, (23) ($t-s<r<2b-2r$) in 3°–4°; if $a=2t$ in 5°–6°, or $a=2s$ in 7°–8°, then $a\geqq 2s\geqq 2t$ or $a\geqq 2t\geqq 2s$, $s=t$.

All of 9°–14° satisfy (2_2); for by (10) and (22), $b\geqq -r-t$, $c\geqq -r-s$, and $a\geqq -s-t$. All satisfy (3) by (11) and (22). For (4_1) we have (9). As to (4_2) the sum $a+b+\cdots$ is respectively $\sigma-c$, $\sigma-b$, $c-\sigma$, $b-\sigma$, $c-b$, and $b-c$; thus (6) follows for 9°–10° from (27)–(28), for 13° from (24_2), and is vacuous for the rest. As to (5), use: (14) and (24) in 9°–10°; (18) in 13°–14°; (27) or (28) in 11°–12°, noting that $a=b$ (or $a=c$) is excluded by (16). As to (8): use (12) and (22) in 9°–10°; if $a=-2t$ in 11°–12°, $s=0$ by (12), $b<-2r$, contrary to (22); if $a+2s+2t=0$ in 11°–14°, b (or c) $<-2r$, a contradiction; if $b+2t+2r=0$ in 11°, $a<-2s$; if $c+2r+2s=0$ in 12°, $a<-2t$; $a\neq -2s$ in 12° and 14°, since $-s<-t$ by (24); in 13°, $\sigma=2b+2t+2r$ implies $a+2s+c-b=0$, $s=t$ by (24), $a=-s-t$; and finally, in 14°, $\sigma=2c+2r+2s$ implies $a+2t+b-c=0$, a contradiction.

It is easy to verify that in terms of the quantities C, R, B of f, the values of C, R, B of the forms 1°–14° are as follows:

$$
\begin{gathered}
(C, R, B), \quad (B, R, C), \quad (C, -C-R, C+2R+B), \\
(C+2R+B, -C-R, C), \\
(C, R+C, C+2R+B), \quad (C+2R+B, R+C, C), \\
(B, R+B, C+2R+B), \quad (C+2R+B, R+B, B), \\
(C, R, B), \quad (B, R, C), \quad (C, C-R, C-2R+B), \\
(B, B-R, C-2R+B), \\
(C-2R+B, C-R, C), \quad (C-2R+B, B-R, B).
\end{gathered} \tag{29}
$$

6. **No two reduced forms are equivalent.** Denote two reduced forms by f and $f'=(a', b', c', r', s', t')$, the adjoint of f' by (A', B', C', R', S', T'), and let $i^{\circ\prime}$ denote i° for f'. A moment's examination shows that for any i $(1\leqq i\leqq 14)$ $i^\circ=i^{\circ\prime}$ implies in some order that $a=a'$, $b=b'$, $\cdots$, $t=t'$. We shall obtain a contradiction if $i^\circ=j^{\circ\prime}$ with $i\neq j$.

Clearly forms 1° to 4°, with all terms positive, cannot coincide with any of forms 5°′ to 14°′.

If $5^\circ=11^{\circ\prime}$ (or $6^\circ=13^{\circ\prime}$), $a=a'$, $-t=t'$, $t-s=-a'-t'-s'$; thus $-2s'\leqq a'=s-s'=a\geqq 2s$, $s=-s'$, $a'=-2s'$, $t'=0$, but $t>0$. Similarly by interchanging b and c, s and t, for $7^\circ=12^{\circ\prime}$ and $8^\circ=14^{\circ\prime}$.

In all other cases we shall obtain one of the contradictory conclusions (i) $B=C$ but $b>c$ or $s^2<t^2$; (ii) $C=-2R$ but $b<2r$; or (iii) $C=2R$ but $a+2s+t<0$; for either f or f'.

If $i^\circ=j^{\circ\prime}$ the ith and jth triples in (29) for f and f' respectively must coincide. Thus if $3^\circ=4^{\circ\prime}$, $C=C'+2R'+B'\geqq B'\geqq C'=C+2R+B\geqq B\geqq C$. In a similar way we find $B=C$ and $B'=C'$ for the pairs $(i, j)=(1, 2)$, $(1, 4)$, $(2, 3)$, $(3, 4)$, $(5, 7)$, $(5, 8)$, $(5, 10)$, $(5, 12)$, $(6, 8)$ $(6, 14)$, $(7, 11)$, $(7, 13)$, $(8, 13)$, $(9, 10)$, $(10, 11)$, $(11, 12)$, $(13, 14)$; all these cases give (i). The same method yields (ii) in the cases $(5, 13)$, $(5, 14)$, $(6, 7)$, $(6, 11)$, $(6, 12)$, $(7, 8)$, $(7, 10)$, $(8, 9)$, $(8, 11)$, $(8, 12)$.

If $1^\circ=3^{\circ\prime}$, (29) gives $C=C'$, $-R=C'+R'\geqq -R'=C'+R\geqq -R$, hence $C'=-2R'$, but $b'<2r'$; similarly for $(2, 4)$, $(5, 6)$, $(5, 9)$, $(6, 9)$, $(6, 10)$, $(8, 10)$. The same method leads to (i) in $(7, 9)$, $(9, 12)$ $[R=B'-R'\geqq R'=B'-R=C-R\geqq R$, $C=2R$, $B'=2R'$, $C'=B'$, but $b'>c']$, $(9, 14)$, $(10, 12)$, $(10, 14)$, and $(12, 13)$.

Finally, $(7, 14)$, $(9, 11)$, $(9, 13)$, $(10, 13)$, $(11, 13)$, $(11, 14)$, and $(12, 14)$ lead to (iii). Thus in $(7, 14)$, $B=C'-2R'+B'$, $R+B=B'-R'$, $C+2R+B=B'$, $B\geqq B'\geqq B$, $C'=2R'$, $a'+2s'+t'\geqq 0$ by (14_3), whereas in 14°′, $\sigma'-c'=a'+b'+2r'+2s'+2t'<0$, or by (27), $a'+2s'+t'<0$.

Several cases could have been contradicted in more than one way.

7. **Algorithm for forms of determinant** d. The minimum a of f, by Seeber's inequality, satisfies $a^3 \leqq 2d$. Further, a is the minimum of the binary form (a, t, b) of determinant C, so that $a^2 \leqq 4C/3$; and C is the minimum of (C, R, B) of determinant ad, whence $C^2 \leqq 4ad/3$.

We are now ready to state an extension to ternaries of the binary algorithm of §1. We shall confine the statement to classical forms although it is easy to include forms in which $2r$, $2s$, or $2t$ may be odd.

Algorithm. Give a the values $1, 2, \cdots, [(2d)^{1/3}]$, $\pm R$ the values $0, 1, \cdots, [(\frac{1}{3}ad)^{1/2}]$. For each a and R, factor $ad+R^2$ in all ways as a product CB of positive integers C, B for which the congruences

$$C \equiv -t^2, \qquad B \equiv -s^2 \pmod{a} \tag{30}$$

are solvable, $2|R| \leqq C \leqq B$, and $\frac{3}{4}a^2 \leqq C$. Give s and t all solutions of (30) such that $|s| \leqq \frac{1}{2}a$ and $|t| \leqq \frac{1}{2}a$, and construct the quotients $b=(C+t^2)/a$ and $c=(B+s^2)/a$, and $r=(st-R)/a$, discarding cases in which r is not an integer [r will usually be an integer by choice of the sign of R, since $R^2 \equiv (st)^2 \pmod{a}$]. Change signs of two of r, s, t if necessary to secure (2). Discard all the resulting forms (a, b, c, r, s, t) which do not satisfy (9) and (12)–(18), as they are duplicates.

The forms remaining comprise one and only one representative of every (classical) class of determinant d. The Eisenstein reduced forms, if desired, may be written down by means of 1° to 14° in §5.

8. **Contracted process for an order or genus.** If we desire only the properly or improperly primitive (p.p. or i.p.) forms of an order (Ω, Δ), then in §7, the values of C, B, R are multiples of Ω, and we can set

$$C = \theta\Omega C_1, \qquad B = \theta\Omega B_1, \qquad R = \Omega R_1, \tag{31}$$

where $\theta = 1$ or 2 according as the reciprocal forms are to be p.p. or i.p. If f is to be i.p., a, b, and c must be even.

There is not much lessening of labor over that for the whole determinant if $\Omega = 1$ (and, if $\Delta = 1$, it is best to use the reciprocal order). But if Ω and Δ exceed 1, the possible values of C within the limits $\frac{3}{4}a^2$ and $(4ad/3)^{1/2}$ (where $d = \Omega^2\Delta$), are comparatively few; and it is less work to write out the values of C for each a, using (31_1) and (30_1), and to construct the equations $ad+R^2 = CB$ by solving the congruences $a\Delta + R_1^2 \equiv 0 \pmod{\theta^2 C_1}$ and forming $a\Delta + R_1^2 = \theta^2 C_1 B_1$, with $2|R_1| \leqq \theta C_1 \leqq \theta B_1$ and with (30_2) solvable for $B = \theta\Omega B_1$. When a is not prime to 2Ω it is necessary to calculate the remaining cofactors A, S, and T, to test whether the form belongs to the desired order.

A specification of the numbers representable properly by the order, and the reciprocal order (and this is especially true within the nar-

rower confines of a genus) will diminish considerably the number of pairs of values of a and C to be considered. We shall not take the space here to list these numbers; however, compare Example 2.

9. **Example 1.** There are over 175 classical, reduced forms of determinant $d=600$. We shall find all with minimum $a=4$. Using a factor table we form $2400+R^2=CB$, for $\pm R=0, 1, \cdots, 28$, with $12\leqq C\leqq(3200)^{1/2}$ and $2|R|\leqq C\leqq B$, C and B congruent to 0 or 3 (mod 4). [For somewhat larger values of a it would be less work to write out the admissible values of C and to solve the congruences $-ad\equiv R^2$ (mod C) for R.] We may take $t=0$ or ± 2 if $C\equiv 0$, $t=\pm 1$ if $C\equiv 3$ (mod 4); and similarly for s and B. We thus obtain the following table:

$\pm R$	C	B	a	b	c	r	s	t	a	b	c	r	s	t	
0	12	200	4	4	50	0	0	−2	4	4	51	1	2	2	(α)
0	15	160	4	4	40	0	0	−1							(β)
0	20	120	4	5	30	0	0	0	4	5	31	0	−2	0	
			4	6	30	0	0	−2	4	6	31	1	2	2	
0	24	100	4	6	25	0	0	0	4	6	26	0	−2	0	
			4	7	25	0	0	−2	4	7	26	1	2	2	
0	32	75	4	8	19	0	−1	0							(γ)
0	40	60	4	10	15	0	0	0	4	10	16	0	−2	0	
			4	11	15	0	0	−2	4	11	16	1	2	2	
4	16	151	4	4	38	−1	−1	0							(γ)
6	12	103	[4	4	51	2	1	2]							(α), (γ), (δ)
6	28	87	4	8	22	2	1	2							(γ), (ϵ)
7	31	79	4	8	20	2	1	1							
8	28	88	4	7	22	−2	0	0	4	7	23	−2	−2	0	
			4	8	22	−2	0	−2	4	8	23	3	2	2	(γ)
8	44	56	4	11	14	−2	0	0	4	11	15	−2	−2	0	
			4	12	14	−2	0	−2	4	12	15	3	2	2	(γ)
14	44	59	4	12	15	4	1	2							(γ), (ϵ)
15	35	75	4	9	19	4	1	1							
16	32	83	4	8	21	−4	−1	0							(ζ)
25	55	55	4	14	14	−6	−1	−1							

We have here omitted: (α) $t=0$ since $(12+0^2)/4<4$; (β) $s=-2$ ($a=-2s$) if $t\neq 0$; (γ) $t=-2$ ($a=-2t$) if $s\neq 0$; (δ) the bracketed form, by (15_1); (ϵ) $t=0$ since $4\nmid 0-R$; (ζ) $t=\pm 2$ since $4\nmid 2-R$. There remain 31 reduced forms, and all of them happen to be also E-reduced.

Example 2. To find the reduced forms in the genus of (7, 7, 7, 1, 1, 1), of determinant 324. Here $\Omega=6$, $\Delta=9$, and the reciprocal forms are i.p., so that $C_1=C/12$ is an integer (and also $B/12$); the numbers

represented by the genus of f are the positive integers not of the forms $3^{2q}(3n+2)$ $(q \geqq 0)$, $3(3n+2)$, or $4n+1$, 2; while C_1 in the reciprocal genus cannot be of the forms $3(3n \pm 1)$, $3n+2$, or $3^{2q+1}(3n+2)$ $(q \geqq 1)$. Since $a^3 \leqq 2d$, $a \leqq 8$. By §7 we have only the possibilities $(a, C) = (3, 12)$, (4, 12), (7, 48). If $a=3$ we solve $-972 \equiv R^2 \pmod{12}$, whence $6 \mid R$, and we form $972+0^2 = 12 \cdot 81$ (discarded since $12 \nmid 81$), $972+6^2 = 12 \cdot 84$, $12+0^2 = 3 \cdot 4$, $84+0^2 = 3 \cdot 28$; we thus write down the form (3, 4, 28 −2, 0, 0). If $a=4$ we obtain $1296+0^2 = 12 \cdot 108$, $1296+6^2 = 12 \cdot 111$ (discarded), $12+0^2 = 4 \cdot 3$ (discarded since $3<4$), $12+2^2 = 4 \cdot 4$, $108 +0^2 = 4 \cdot 27$, $108 = 2^2 = 4 \cdot 28$; and have the forms (4, 4, 27, 0, 0, −2), (4, 4, 28, 1, 2, 2); but discard the latter as i.p. If $a=7$, $2268+6^2 = 48 \cdot 48$, $2268+18^2 = 48 \cdot 54$ (discarded), $48+1^2 = 7 \cdot 7$; and we have (7, 7, 7, 1, 1, 1). Thus there are three reduced forms in this genus: (3, 4, 28, −2, 0, 0), (4, 4, 27, 0, 0, −2), and (7, 7, 7, 1, 1, 1). As a check, the mass of the genus should be $1/4+1/12+1/6 = 1/2$, and this agrees with the Eisenstein-Smith [4] formula.

10. **Some remarks about minima.** The invariance of (19) in §3 proves that among all forms within a class, (19) holds if the coefficients satisfy the inequalities (2) and (9)–(18). An examination of the last part of §3 allows us to drop some of these inequalities, and still assure the validity of (19).

Examples of reduced forms, and of E-reduced forms, in which C is not the minimum of the adjoint form, are easily found; C is, in a reduced form, only the minimum simultaneous with the minimum a.

In an E-reduced form, b is (if it exceeds a) the least number properly represented except for a; the corresponding number for a reduced form is readily deduced from the list of fourteen forms in §5. Conversely, if the least number represented by F simultaneously with the minimum a by f is desired for an E-reduced form, it can be deduced by inverting the transformations of §5 to obtain the corresponding reduced form.

References

1. L. A. Seeber, *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen*, Freiburg, 1831, 248 pp.

2. G. Eisenstein, Journal für die reine und angewandte Mathematik, vol. 41 (1851), pp. 141–190. See also L. E. Dickson's *History of the Theory of Numbers*, vol. 3, pp. 212–213, and B. W. Jones' table of Eisenstein-reduced positive ternary quadratic forms of determinant $\leqq 200$, Bulletin of the National Research Council, no. 97, 1935, pp. 3–5.

3. E. Selling, Journal de Mathématiques, (3), vol. 3 (1877), pp. 21–153.

4. H. J. S. Smith, *Collected Mathematical Papers*, vol. 1, p. 499.

Institute for Advanced Study