wenn f irreduzibel über $K(N_{s-1})$ ist. Wäre das Polynom reduzibel, so hätte es als Binom von Primzahlgrad in $K(N_{s-1})$ eine Nullstelle b, und es folgte $a = be$ mit einer p-ten Einheitswurzel e; weiter $b^p = a^p \in N_{s-1}$, also $b \in N_{s-1}$ nach Induktionsannahme, $e \in N_s$ und damit $e \in K^\times$ nach Voraussetzung; dann wäre aber $a \in N_{s-1}$, im Widerspruch zu $[N_s : N_{s-1}] = p > 1$.

Nun sei $c \in K(N_s)$, $c^p \in N_s$ (und $c \in K^\times M$, falls $p = 2$ und $i \in K(N_s)$ ist), also $c^p = a^q d$ mit $0 \leqslant q < p$, $d \in N_{s-1}$. Wir nehmen zunächst $q > 0$, also prim zu p an und zeigen, daß das zu einem Widerspruch führt. Mit N bezeichnen wir die Norm von $K(N_s)$ nach $K(N_{s-1})$. Wegen $Na = (-1)^{p-1} a^p$ ergibt sich $((-1)^{p-1} a^p)^q = (Nc)^p d^{-p}$. Für ungerades p ist a^p demnach p-te Potenz eines Elements aus $K(N_{s-1})$, im Widerspruch zu

$$[K(N_s) : K(N_{s-1})] = p.$$

Im Fall $p = 2$ wird $-a^2 = f^2$ mit $f \in K(N_{s-1})$, also $i \in K(N_s)$, $i \notin K(N_{s-1})$, $c^2 = ad = \pm ifd$. Schreibt man $c = g + ih$ mit $g, h \in K(N_{s-1})$, so folgt $g^2 = h^2$, d.h. $c = (1 \pm i)g$. Daraus folgt $g^4 = -c^4/4 \in N_{s-1}$, weiter durch zweimalige Anwendung der Induktionsannahme $g \in N_{s-1}$ und damit $1 \pm i \in K^\times M$, was zusammen mit $i \notin K(N_{s-1})$ der anfangs gemachten Voraussetzung widerspricht.

Wir haben hiernach $c^p \in N_{s-1}$. Ist S ein Isomorphismus von $K(N_s)$ in einen Oberkörper, der alle Elemente aus $K(N_{s-1})$, nicht aber a fest lässt, also $Sa = ae$ mit einer primitiven p-ten Einheitswurzel e, so gilt $Sc^p = c^p$, also $Sc = ce^r$, und daraus folgt $c = a^r b$ mit $b \in K(N_{s-1})$; weiter $b^p \in N_{s-1}$ (und $b \in K^\times M$, falls $c \in K^\times M$), also $b \in N_{s-1}$, nach Induktionsannahme und damit $c \in N_s$.

Literaturverzeichnis

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), S. 3–6.

[2] L. J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. 3 (1953), S. 625–630.

[3] C. L. Siegel, *Algebraische Abhängigkeit von Wurzeln*, Acta Arith. 21 (1972), S. 59–64.

Eingegangen 22. 12. 1973 (512)

ACTA ARITHMETICA
XXVI (1975)

One-class genera of positive quadratic forms in at least five variables

by

G. L. Watson (London)

1. Introduction. Let f be a positive-definite quadratic form, with integer coefficients, in any number n of variables; and denote by $c(f)$ the number of classes in the genus of f. I showed in [1] and [2] that there exists an f with $c(f) = 1$ if and only if $n \leqslant 10$. Now it would be of interest to find all the one-class genera of positive n-ary forms for any n with $2 \leqslant n \leqslant 10$ ($n = 1$ is trivial); especially for $n = 2$, which however seems hopeless.

Using a method based on the results of [3], I break the problem up into two parts. The second of these, which I defer to a later paper, involves a great deal of calculation, but is considerably simplified by using the results of [4]. The first part, done for $n = 3, 4$ in [5], [6], and for $5 \leqslant n \leqslant 10$ in this paper, consists in finding all the one-class positive genera that have certain simple arithmetic properties explained in the next section. The number of such genera is 1 for $n = 1$ and 20, 27, 14, 14, 7, 5, 1, 1 for $n = 3, \ldots, 10$; and considerably greater for $n = 2$.

On choosing reduced representatives of the $42 = 14 + \ldots + 1$ of these genera that have $n \geqslant 5$, and putting in $10 = 1 + 1 + 2 + 6$ forms with $n \leqslant 4$, we obtain a list of 52 forms $F_1, \ldots, F_{52}$ each of which, except $F_1 = x_1^2$, has one of the others as its leading $(n-1)$-ary section. This feature of the result shortens both the statement (see Table 1, below) and the proof of the main result.

2. Strongly primitive (SP) and square-free (SF) forms. We use the notation

$$\sum \{a_{ij} x_i x_j : 1 \leqslant i \leqslant j \leqslant n\} \tag{2.1}$$

for a quadratic form (with integer coefficients a_{ij}); and for $j < i$ we write $a_{ij} = a_{ji}$. For n-ary f and prime p we define $r_p(f)$ as the least of the integers r $(0 \leqslant r \leqslant n)$ for which a form (2.1) equivalent to f can satisfy

$$p \mid a_{ij} \quad \text{whenever} \quad j > r. \tag{2.2}$$

Then f is said to be *strongly primitive* (SP) if $r_p(f) \geqslant \frac{1}{2}n$ for every p.

Now, from the set of forms (2.1) that are equivalent to f and satisfy (2.2) with $r = r_p(f)$, we choose one satisfying

$$p^2 \mid a_{ij} \quad \text{whenever} \quad i > r \text{ and } j > k, \tag{2.3}$$

with k least possible, but $\geqslant r$. Then f is p-adically square-free if $f \sim (2.1)$, (2.2) with $r = r_p(f)$, and (2.3) with $k < n$, are inconsistent. And f is *square-free* (SF) if it is p-adically SF for every p.

With these definitions, which are taken from [3] with a slight change of notation, we can state precisely the object of the present paper; it is to investigate positive-definite n-ary quadratic forms f that are SP and SF and satisfy the conditions $n \geqslant 5$ and $c(f) = 1$.

If the form f is expressed as in (2.1) then its matrix $A = A(f)$ is the $n \times n$ symmetric matrix whose (i, j) element is a_{ij} if $i \neq j$, $2a_{ii}$ if $i = j$. Then the discriminant of f is

$$d = d(f) = \begin{cases} (-1)^{\frac{1}{2}n} \det A & \text{if} \quad 2 \mid n, \\ \frac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}} \det A & \text{if} \quad 2 \nmid n. \end{cases} \tag{2.4}$$

Since A is congruent modulo 2 to a skew matrix, this definition makes d an integer always, and see, e.g. [7], p. 21, (52),

$$d \equiv 0 \text{ or } 1 \pmod 4 \quad \text{if} \quad 2 \mid n. \tag{2.5}$$

The $\frac{1}{2}$ in (2.4) is in some ways inconvenient, but it gives us, see [3], p. 583, Lemma 4,

$$r_p(f) = n \Leftrightarrow p \nmid d(f). \tag{2.6}$$

Now let f be a form chosen from its class so as to satisfy (2.2) with $r = r_p(f)$ and (2.3) with minimal k; and define two forms g, h, each obviously with integer coefficients, by

$$g(x_1, \ldots, x_n) = p^{-1} f(px_1, \ldots, px_r, x_{r+1}, \ldots, x_n), \tag{2.7}$$

$$\begin{aligned} h(x_1, \ldots, x_n) &= p^{-1} g(x_1, \ldots, x_r, px_{r+1}, \ldots, px_k, x_{k+1}, \ldots, x_n) \\ &= f(x_1, \ldots, x_k, p^{-1}x_{k+1}, \ldots, p^{-1}x_n). \end{aligned} \tag{2.8}$$

It is shown in [3] that the classes of g and h are uniquely determined by p and the class of f, and that

$$c(f) \geqslant c(g) \geqslant c(h). \tag{2.9}$$

Obviously there is equality in (2.9) if f is p-adically SF, for then (2.8) gives $h = f$; and we also have that one of $r_p(f)$, $r_p(g)$ is $\geqslant \frac{1}{2}n$, since their sum is n. Other possibilities for equality in (2.9) are investigated in [4].

If f is not p-adically SF then $k < n$ and (2.8) gives

$$d(h) = p^{2k-2n} d(f),$$

whence crudely $|d(h)| < |d(f)|$. So by repeating the construction, with suitable choice of p at each step, we see that starting with any given f we come in finitely many steps to a form F which is SP and SF and satisfies $c(F) \leqslant c(f)$; further, F can be taken into a multiple of f by a substitution with integer coefficients and determinant $\geqslant 1$.

3. The forms $F_1, \ldots, F_{52}$. These forms are listed in Table 1, below.

Table 1

n	i	j	border	$d(F_i)$
1	1	—	1	1
2	2	1	1, 1	−3
3	3,	2	1, 1, 1	−2
	4		0, 0, 1	−3
4	5–	3	0, 1, 1, 1	4
	8		1, 1, 1, 1	5
			0, 0, 0, 1	8
			0, 1, 1, 2	12
4	9,	4	0, 0, 1, 1	9
	10		0, 0, 0, 1	12
5	11–	5	1, 1, 1, 1, 1	2
	13		0, 0, 0, 0, 1	4
			1, 1, 1, 1, 2	6
5	14–	6	1, 1, 1, 1, 1	3
	16		0, 0, 0, 0, 1	5
			0, 0, 1, 1, 2	7
5	17–	7	0, 0, 0, 1, 1	6
	20		0, 1, 1, 1, 2	10
			0, 0, 1, 1, 2	11
			0, 1, 1, 0, 2	12
5	21	8	1, 1, 1, −1, 2	15
5	22	9	0, 0, 0, 0, 1	9
5	23,	10	1, 1, 1, 1, 2	14
	24		0, 0, 1, 1, 2	18
6	25–	11	0, 1, 1, 1, 1, 1	−3
	29		1, 1, 1, 1, 1, 1	−4
			0, 0, 0, 0, 0, 1	−8
			0, 1, 1, 1, 1, 2	−11
			1, 1, 1, 1, 1, 2	−12
6	30,	12	0, 0, 0, 0, 1, 1	−12
	31		0, 0, 0, 0, 0, 1	−16
6	32,	14	1, 1, 1, 1, 1, 1	−7
	33		0, 0, 1, 1, 1, 2	−15
6	34,	15	0, 0, 0, 0, 1, 1	−15
	35		0, 0, 1, 1, 1, 2	−23
6	36	17	0, 1, 1, 1, 1, 2	−28
6	37	22	0, 0, 0, 0, 1, 1	−27
6	38	24	0, 0, 1, −1, 0, 2	−108
7	39,	25	0, 1, 1, 1, 1, 1, 1	−1
	40		0, 0, 0, 0, 0, 0, 1	−3
7	41–	26	1, 1, 1, 1, 1, 1, 1,	−2
	43		0, 0, 0, 0, 0, 0, 1	−4
			1, 0, 0, 0, 0, 0, 2	−5
7	44	27	0, 0, 0, 0, 0, 1, 1	−6
7	45	30	0, 0, 0, 0, 1, 1, 1	−8
8	46,	39	0, 0, 0, 0, 0, 0, 1, 1	1
	47		0, 0, 0, 0, 0, 0, 1, 2	5
8	48	40	0, 0, 0, 0, 0, 0, 1, 1	9
8	49	41	1, 1, 1, 1, 1, 1, 1, 1	4
8	50	45	0, 0, 0, 0, 0, 1, 1, 1	16
9	51	46	0, 0, 0, 0, 0, 0, 0, 0, 1	1
10	52	51	0, 0, 0, 0, 0, 0, 0, 0, 1, 1	−3

The table needs a little explanation. Except for $F_1 = x_1^2$, each F_i is a form of rank $n = n(i) \geqslant 2$ which reduces on putting $x_n = 0$ to F_j, for some $j < i$, with $n(j) = n(i)-1$, shown in column 3. To complete the definition of F_i we need only the coefficients of $x_1x_n, x_2x_n, \ldots, x_n^2$ and these are shown in column 4.

4. Notation; and two lemmas. The letters $f, g, h, F, \varphi, \psi, \theta$, plain or embellished, denote quadratic forms, with integer coefficients unless otherwise stated. Except in dealing with p-adic properties, all quadratic forms are assumed to be positive-definite. $f \sim g$, $f \underset{p}{\sim} g$ mean that f is equivalent to g over the rational, p-adic integers respectively, p any prime. $f \supset g$, $f \underset{p}{\supset} g$ mean that f represents g over the rational, p-adic integers; we shall be concerned mostly with cases in which the representation is proper. We recall that two forms f, g in the same number of variables (and so, since both are positive-definite, equivalent over the real field) are in the same genus, in symbols $f \simeq g$, if $f \underset{p}{\sim} g$ for every p. $c(f) = 1$ means that $f \simeq g$ implies $f \sim g$.

An n-ary form with discriminant d will often, for brevity, be denoted by (n, d); a disjoint form, say $g(x_1, \ldots, x_k)+\psi(x_{k+1}, \ldots, x_n)$, $0 < k < n$, by $g+\psi$. Combining these abbreviations, for example, F_{17} is $(3, -2)+$ $+(2, -3)$. Using this notation, and (2.6), we may redefine $r_p(f)$ by

$$r_p(f) = \max\{r\colon f \supset (r, d_r) \nRightarrow p|d_r\}. \tag{4.1}$$

We note also, see [7], pp. 51–52, Theorems 29, 30, that

(4.2) if dd' is the square of a p-adic unit then $(n, d) \underset{p}{\sim} (n, d')$.

The hypothesis means $(dd'|p) = 1$ (Legendre symbol) if $p > 2$, dd' $\equiv 1 \pmod 8$ if $p = 2$.

If f is an n-ary form, p-adically SF and with $r_p(f) = r$, then (see [1], pp. 552–553) we have

$$f \underset{p}{\sim} (r, d')+p(n-r, d''), \quad p\nmid d'd'', \tag{4.3}$$

except possibly if

$$p = 2, \quad 2\,|\,n, \quad \text{and} \quad 2\nmid r, \tag{4.4}$$

in which case

$$f \underset{2}{\sim} (r-1, 1)+[a, 2b, 2c]+2(n-r-2, 1), \quad 2\nmid ac. \tag{4.5}$$

It is to be understood that $(0, d)$ is meaningless unless $d = 1$, in which case it is identically 0. In (4.5), and later, we write $[a_{11}, a_{12}, a_{22}]$ for the case $n = 2$ of (2.1). In case $2\nmid b$, in (4.5), we may if we please replace $[a, 2b, 2c]$ by $[a, 0, c']$, $ac' \equiv 1 \pmod 4$.

Now we define, for n-ary f and $k = 1, \ldots, n$,

$$f_k = f_k(x_1, \ldots, x_k) = f(x_1, \ldots, x_k, 0, \ldots, 0), \tag{4.6}$$

$$d_k = d_k(f) = d(f_k); \tag{4.7}$$

$f_n, d_n = f, d(f)$. We shall consider f as Hermite-reduced if it has the property (for $k = 1, \ldots, n-1$)

$$|d_k(f)| = \min\{|d_k(f')|\colon f' \sim f,\ d_m(f') = d_m(f) \text{ for all } m < k\}. \tag{4.8}$$

Whether f is reduced or not, if f_k is given (up to equivalence) then in general d_{k+1} is restricted to satisfy certain congruence conditions. These will be needed later, so we prove:

LEMMA 1. *With the foregoing notation, if $2 \leqslant k < n$, then f_k represents a $(k-1)$-ary form $(k-1, d'_{k-1})$ with*

$$d'_{k-1} \equiv d_{k+1} \begin{cases} \pmod{d_k} & \text{if} \quad 2\,|\,k, \\ \pmod{4d_k} & \text{if} \quad 2\nmid k. \end{cases} \tag{4.9}$$

Proof. By suitably transforming the variables $x_1, \ldots, x_k$ we may suppose that the last row of $A_{k+1} = A(f_{k+1})$ is $0, \ldots, 0, a, 2b$, where a and b are integers; transposition gives the last column. In $\det A_{k+1}$, the cofactor of $2b$ is $\det A_k$; so on reducing modulo $2\det A_k$ we find $\det A_{k+1}$ $\equiv -a^2 \det A_{k-1}$. Referring to (2.4), we have (4.9) with $a^2 d_{k-1}$ for d'_{k-1}. Obviously $f_k \supset (k-1, a^2 d_{k-1})$ (properly if $a = \pm 1$); the lemma follows.

Another lemma restricts f_{n-2} but not d_{n-2}.

LEMMA 2. *Suppose $n \geqslant 3$ and let a be an integer with $a \equiv 0$ or $1 \pmod 4$, $(a|p) = -1$ if $p > 2$, $a \equiv -3 \pmod 8$ if $p = 2$. Suppose also that the disjoint form*

$$f(x_1, \ldots, x_n)-g(x_{n+1}, \ldots, x_{2n-2}) \tag{4.10}$$

is equivalent over the p-adic rationals to

$$x_1x_2+x_3x_4+\ldots+x_{2n-7}x_{2n-6}+(2, a)+p(2, a). \tag{4.11}$$

Then $f \underset{p}{\supset} g$ is false.

Proof. Temporarily, let $\sim$ denote equivalence over the p-adic rationals; and note that (4.11) means $(2, a)+p(2, a)$ if $n = 3$. From (4.10) $\sim$ (4.11) it follows that $d(f)d(g)$ is a p-adic square. Now suppose $f \underset{p}{\supset} g$; then $f \sim g+\theta$ for some 2-ary θ with $d(\theta)$ a p-adic square, so $\theta \sim (2, 1)$, $= x_1x_2$. By diagonalizing g and using the obvious $cx_1^2-cx_2^2$ $\sim x_1x_2$ for $c \neq 0$, $g-g \sim (2, 1)+(2, 1) \ldots$, (4.10) $\sim$

$$x_1x_2+x_3x_4+\ldots+x_{2n-3}x_{2n-2}. \tag{4.12}$$

We now have (4.11) $\sim$ (4.12); and by a well known theorem, due to Witt, we can cancel (if $n \geqslant 4$), and so obtain $(2, a)+p(2, a) \sim x_1x_2+x_3x_4$, which however is false since the left member is not a zero form. This contradiction completes the proof.

5. Statement of results. The forms $F_1, \ldots, F_{52}$ in Table 1 represent 52 different genera. To see this we need only consider pairs with the same n, d; there are just four such pairs, all with $d \equiv \pm 3 \pmod 9$. That implies, taking $p, r = 3, n-1$ in (4.3), that one of $d_{n-1} \equiv 1, -1 \pmod 3$ is inconsistent with $(n, d) \supset (n-1, d_{n-1})$. Looking at column 3 of Table 1, or putting $x_1 = 0$ in F_{10}, F_{33}, we find each pair 3-adically inequivalent.

The forms $F_1, \ldots, F_{10}$ are all SP and SF, with class-number 1. This is trivial for $n = 2$ and proved for $n = 3, 4$ in [5], [6]. $F_{11}, \ldots, F_{52}$ are all SP and SF. To see this, use (4.3)–(4.5). It is trivial that $r_p(f) = n$ or $n-1$, and f is p-adically SF, unless $p^2 \mid d(f)$, which for $f = F_i$ $(11 \leqslant i \leqslant 52)$ gives $p \leqslant 3$; and the proof is easily completed. Now we state the main result.

THEOREM 1. *Let f be a positive-definite n-ary quadratic form with integer coefficients, $n \geqslant 5$, which is square-free and strongly primitive. Then f has class-number* 1 *if and only if f is equivalent to one of the last* 42 *of the forms listed in Table* 1 *above.*

For the 'if' of Theorem 1 we shall need

THEOREM 2. *With the notation of* (4.6), (4.7), *let F_i be the form defined in the i-th row of Table* 1; *and let f be a form with the same number n of variables as F_i, satisfying the condition*

$$(5.1) \qquad d_k(f) = d_k(F_i) \quad \text{for} \quad k = 1, 2, \ldots, n.$$

Suppose also that f is SF; then $f \sim F_i$.

The forms F_i have been chosen from their classes so as to be Hermite-reduced; but it turns out that they have the following property, stronger and simpler than (4.8):

$$(5.2) \qquad f \simeq F_i \Rightarrow |d_k(f)| \geqslant |d_k(F_i)| \quad \text{for} \quad k = 1, \ldots, n.$$

Since Table 1 shows that $d_k(F_i) = 1, -3$ for $k = 1, 2$, and all i, we see, using (2.5), that (5.2) is trivial for $k = 1, 2$. For $k = 3$, we note that $(3, -1)$ does not exist (its minimum would be less than 1), and $d_3(F_i)$ is always either -2 or -3, so we have only to find a p with $F_i \not\supset_p (3, -2)$ in each case in which $d_3(F_i) = -3$. To do this for $F_{23} = (5, 14)$, we use Lemma 2 with $p = 2$ and $g = (3, -2)$. Other cases are easier; for example, $F_{24} = (5, 18) \supset F_{10} \supset (3, -4)$, so, by (4.3) with $p = r = 3$, $F_{24} \not\supset_3 (3, -2)$. The argument is similar for $k = 4, 5, \ldots$

6. Proof of Theorem 2. We shall deduce $f \sim F_i$ from (5.1) and

$$(6.1) \qquad \text{either } f \text{ is SF or } F_i = F_l(x_1, \ldots, x_n, 0) \text{ for some } l > i.$$

We notice also, see Table 1, that $F_i(x_1, \ldots, x_{n-1}, 0) = F_j$ for some $j < i$.

Now we can use induction on n; the case $n = 1$ is trivial. For $n \geqslant 2$ the inductive hypothesis permits us to replace (5.1) by

$$(6.2) \qquad f_{n-1} \sim F_j = F_i(x_1, \ldots, x_{n-1}, 0); \quad d(f) = d(F_i);$$

and it suffices to prove that (6.1) and (6.2) determine f uniquely up to equivalence.

Denote by A, B the matrices of f, f_{n-1}, with $f_{n-1} \sim F_j$ to be chosen later. Write $\mathrm{col}\{\boldsymbol{a}, 2b\}$, $(\boldsymbol{a}', 2b)$ for the last column and the last row of A, where b is an integer and the column vector $\boldsymbol{a}$ and its transpose $\boldsymbol{a}'$ have integer elements. Then (6.2) gives

$$(6.3) \qquad A = \begin{pmatrix} B & \boldsymbol{a} \\ \boldsymbol{a}' & 2b \end{pmatrix}, \quad 2b \det B - \boldsymbol{a}'(\mathrm{adj}\, B)\boldsymbol{a} = \det A = \det A(F_i),$$

whence b is determined if $\boldsymbol{a}$ is given, and $\boldsymbol{a}$ has to satisfy

$$(6.4) \qquad \boldsymbol{a}'(\mathrm{adj}\, B)\boldsymbol{a} \equiv -\det A(F_i) \pmod{2 \det B}.$$

What we need therefore is to show that with suitable normalization $\boldsymbol{a}$ is determined uniquely by (6.1) and (6.4). As in Lemma 1, (6.4) is a congruence modulo $4d(F_j)$ if n is even, but 2 cancels out and the modulus becomes $d(F_j)$ if $n-1$ is even.

Normalization of $\boldsymbol{a}$ can be done in two stages. First, we may, without altering the class of f, replace $\boldsymbol{a}$ by $\boldsymbol{a} + B\boldsymbol{t}$, for any $\boldsymbol{t}$ with integer elements. Secondly, if S is any integral automorph of f_{n-1}, we may transform f by $\mathrm{diag}[S, 1]$ and so replace $\boldsymbol{a}$ by $S'\boldsymbol{a}$ (S' being the transpose of S). Often $S = -I$ (I for identity) is all we need; but when F_j is disjoint (and we choose $f_{n-1} \sim F_j$ so as to preserve the disjointness) there are other obvious possibilities, with S either a permutation matrix or diagonal, with elements ± 1.

As an example, take $n = 5$, $F_j = (4, 5) = F_6$, whence as noted above 2 cancels from (6.4). We may choose $f_4 \sim F_6$ so as to have $B \equiv \mathrm{diag}[C, 0]$, for some C, $5 \nmid \det C$, $\mathrm{adj}\, B \equiv \mathrm{diag}[0, 0, 0, c] \pmod 5$, where $c = \det C$. Now (6.4) reduces, writing $\boldsymbol{a} = \mathrm{col}\{a_1, \ldots, a_4\}$, to a congruence of the shape $a_4^2 \equiv e \pmod 5$. Normalization of $\boldsymbol{a}$ by $\boldsymbol{a} \to \boldsymbol{a} + B\boldsymbol{t}$ with $\boldsymbol{t} = (\mathrm{adj}\, B)\boldsymbol{u}$, $B\boldsymbol{t} = 5\boldsymbol{u}$ permits us to reduce the a_i modulo 5. Then obviously, with other choices of $\boldsymbol{t}$, we can have $a_1 = a_2 = a_3 = 0$. So we have at most two possibilities for $\boldsymbol{a}$ when $d(F_i)$ is given; and $S = -I$ removes the ambiguity.

Now take $F_j = (5, 18) = F_{24}$. F_i can only be $(6, -108) = F_{38}$, and f is SF since the second part of (6.1) is impossible. Choosing B suitably, we can normalize so as to have $a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 3$, with (6.4) implying $a_4^2 \equiv a_5^2 \pmod 3$. Now to make f SF we need $r_3(f) = 3$, which is false if $3 \nmid a_4 a_5$, so $3 \mid \boldsymbol{a}$ and (6.4) simplifies to a congruence modulo 8.

It may next be noted that a disjoint F_j presents no difficulty when its summands have been dealt with, so we need only (see column 3 of Table 1) consider the 14 possible F_j that are not disjoint. Of these, one is F_{18}, see above, and ten others can be dealt with just like (4, 5). The three that remain are $F_5 = (4, 4)$, $F_8 = (4, 12)$, and $F_{26} = (6, -4)$. F_5 and F_{26} are well known forms with numerous automorphs, and F_8 has leading section (3, −2), also with numerous automorphs. So these three cases can be dealt with by suitable choice of S; the details are left to the reader.

7. Representation by SF forms. We shall prove three lemmas.

LEMMA 3. *Let f, g be positive-definite forms, and suppose $f \underset{p}{\supset} g$ for every p, then $f' \supset g$ for some $f' \simeq f$; whence, if $c(f) = 1$, $f \supset g$.*

Proof. The result is well known; see, e.g., [5], p. 101, Lemma 6 (for a reference).

LEMMA 4. *Suppose f, g, in n, s variables respectively, are both p-adically SF. Then any one of the following conditions implies $f \underset{p}{\supset} g$:*

(i) $s < \min(n-2, r)$ $(r = r_p(f))$;

(ii) $p \nmid d(g)$ *and* $s < r$;

(iii) $s \leqslant n-3$, $r_p(g) < r$ *and* $s - r_p(g) < n-r$;

(iv) $s = n-2$, $r_p(g) < r$ *and* $d(f)d(g)$ *not a p-adic square*;

(v) $p = 2$, $s = 3$, $n = 6$, $r = 3$.

Proof. For the sufficiency of (i), (ii), (iii) see [1], p. 555, Lemma 2, (4.13), (4.14). Using the sufficiency of (i) and (iii) we may for (v) suppose $r = 3$, and $2 \nmid d(g)$. Then we may suppose, see (4.3), that $g = x_1x_2 + ex_3^2$, $2 \nmid e$; which with f satisfying (4.5) gives the result.

It remains to prove the sufficiency of (iv). As in the proof of the lemma quoted above, if $r \geqslant 3$ we have, for some f',

$$f \underset{p}{\simeq} x_1x_2 + f' \underset{p}{\supset} px_1x_2 + f',$$

so we may suppose $r - r_p(g) \leqslant 2$. If $f \underset{p}{\simeq} h + f'$ and $g \underset{p}{\simeq} h + g'$ then $d(f')d(h')$ is not a p-adic square, so we may use induction on n. For $p = 2$, taking $h = x_1x_2$ or (2, −3), this tells us that we may suppose $r_p(g) \leqslant 1$. But for $p > 2$, taking $h = ax_1^2$, $p \nmid a$, we may suppose $r_p(g) = 0$. Similarly using a suitable h with divisor p, we suppose $\min(n-r, n-2-r_p(g)) \leqslant 2$ if $p = 2$, $\leqslant 1$ if $p > 2$. For $p > 2$ this gives $n \leqslant 3$, for which see [5], Lemma 4. So suppose $p = 2$, and $n \leqslant 5$, with $r = 3$, $r_2(g) = 1$ in the case $n = 5$. I now omit some details.

With $n = 5$, see (4.3), we have $f \underset{2}{\simeq} x_1x_2 + f' \underset{2}{\supset} ax_1^2 - ax_2^2$, for any odd a, so by taking $h = ax_1^2$ for suitable a we have an induction from $n = 4$. A similar argument, using also $(2, -3) \underset{2}{\supset} ax_1^2 + ax_2^2$, $2 \nmid a$, can be used if $n = 4$ and $r_2(g) = 1$. If $n = 4$ and $r_2(g) = 0$, then $r = 2$ and $f, g \underset{2}{\simeq} (2, a) + 2(2, b), 2(2, c)$ with a, b, c each 1 or −3, and $abc \not\equiv 1 \pmod 8$. So $a = 1$ or $b = c$, and in either case $f \underset{2}{\supset} g$. The case $n = 3$ is straightforward.

LEMMA 5. *With the notation of (4.6), (4.7), suppose $f \supset g$, $f_k \not\supset g$, for some g the greatest of whose successive minima is m. Then after suitable transformation of $x_{k+1}, \ldots, x_k$*

$$(7.1)\qquad |d_{k+1}| \leqslant \begin{cases} m\,|d_k| & \text{for even } k, \\ 4m\,|d_k| & \text{for odd } k. \end{cases}$$

Suppose that $k \geqslant n-3$ and equality holds in (7.1). Then for some t-ary form h, $t \leqslant 3$, whose successive minima are all equal to m,

$$(7.2)\qquad f \supset f_k + h \supset g.$$

Proof. (4.6) gives

$$(7.3)\qquad f = f_k(x_1 + L_1, \ldots, x_k + L_k) + \psi(x_{k+1}, \ldots, x_n),$$

where ψ is a rational quadratic and the L_i are rational linear forms in $x_{k+1}, \ldots, x_k$. We may suppose that the leading coefficient of ψ is its minimum, $\min\psi$, and

$$(7.4)\qquad f_{k+1} = f_k(x_1 + c_1x_{k+1}, \ldots, x_k + c_kx_{k+1}) + (\min\psi)x_{k+1}^2,$$

with rational constants c_i.

Using (2.4), we have (7.1) with strict inequality if $\min\psi < m$. So we suppose $\min\psi \geqslant m$. Now by hypothesis, if g has s variables, g takes values $\leqslant m$ at s linearly independent points (with integer coordinates). Since $f \supset g$, f takes values $\leqslant m$ at s linearly independent points. One of these points has $x_{k+1}, \ldots, x_n \neq 0, \ldots, 0$; otherwise $f \supset g$ would imply $f_k \supset g$. So there are integers $x_1, \ldots, x_n$ satisfying $f \leqslant m$ and $x_i \neq 0$ for some $i > k$. With $\min\psi \geqslant m$, this is possible only if $\min\psi = m$ and the integers $x_{k+1}, \ldots, x_n$ satisfy

$$(7.5)\qquad \psi(x_{k+1}, \ldots, x_n) = m \quad\text{and}\quad L_i(x_{k+1}, \ldots, x_n) \equiv 0 \pmod 1 \quad\text{for}\quad i = 1, \ldots, k.$$

Further, $\min\psi = m$ gives us (7.1), with =, so we may suppose $k \geqslant n-3$.

If (7.5) has fewer than $n-k$ linearly independent solutions we may suppose that it implies $x_n = 0$; then all the hypotheses hold good with $f(x_1, \ldots, x_{n-1}, 0)$ in place of f. We may therefore suppose that (7.5) holds at $n-k$ points with determinant $D > 0$. It is well known that a positive form in three or fewer variables cannot take its minimum value at a set of points with determinant > 1. So $D = 1$.

Now each linear form L_i takes an integral value at $n-k$ points with determinant 1; so the coefficients of L_i must be integers. A trivial transformation now takes the right member of (7.3) into the disjoint form $f_k+\psi$ (and so ψ has to have integer coefficients). This gives (7.2).

COROLLARY TO LEMMA 5. *With the hypotheses of the second part of the lemma, $g \sim g'+h'$, with $g' \subset f_k$ and $h' \subset h$, where h', in 1, 2, or 3 variables, has all its successive minima $\leqslant m$.*

Proof. f_k+h has to take values $\leqslant m$ at integer points $(x_1, \ldots, x_{r+l})$ corresponding to a set of linearly independent solutions of $g \leqslant m$. Since $\min h = m$, any such point $(x_1, \ldots, x_n)$ has to have either all the variables of f_k, or all those of h, equal to 0. The result follows.

8. Disjoint and perfect forms. We need three lemmas.

LEMMA 6. *A disjoint form $g+h$ cannot represent a perfect form φ, with minimum 1, unless either $g \supset \varphi$ or $h \supset \varphi$. If $g+h$ represents the disjoint form $\varphi'+\varphi''$, each of φ', φ'' perfect with minimum 1, then either one of g, h represents $\varphi'+\varphi''$, or one of them represents φ' and the other φ''.*

Proof. [1], p. 556–557, Lemmas 3, 4.

LEMMA 7. *Let f be positive, SF and SP, with $n \geqslant 7$ and $r_p(f) \leqslant n-3$ for at least one prime p. Denote by q the product of the p for which $r_p(f)$ is minimal. Then there exist a 4-ary form g and an $(n-4)$-ary form h, each SF and SP, such that*

(8.1) $$d(g) = q^2, \quad r_p(g) = 2 \text{ if } p \mid q, \quad 4 \text{ if } p \nmid q;$$

(8.2) $$d(h) = q^{-2}d(f), \quad r_p(h) = \begin{cases} r_p(f)-2 & \text{if } p \mid q, \\ r_p(f)-4 & \text{if } p \nmid q, \end{cases}$$

and

(8.3) $$f \simeq g+h.$$

Proof. See [1], p. 560, Lemma 9, for the existence of g satisfying (8.1); then [1], p. 554, Lemma 1, for h satisfying (8.2), (8.3).

LEMMA 8. *With hypotheses of Lemma 7, suppose further that $c(f) = 1$. Then $n \leqslant 8$, $q = 2$, $r_2(f) = 4$, and $h \supset (2, -3)$.*

Proof. If $n \geqslant 11$ then for $c(f) > 1$ see [1], p. 549, Theorem 1. For $n \geqslant 9$ and f of the shape (8.1)–(8.3), $c(f) > 1$ by [1], p. 562, Lemma 12. So $n \leqslant 8$. Now suppose $r_p(f) \geqslant 5$ for $p \mid q$. Then Lemma 4 gives $f \underset{p}{\supset} \varphi$ for every 4-ary φ, and so by $c(f) = 1$, Lemma 3, and (8.3), $g+h \supset \varphi$. In particular we may take $\varphi = (4, 4)$ or $(4, 5)$ $(= F_5$ or $F_6)$, each of which is well known to be perfect with minimum 1. Then by Lemma 6, either g or $h \supset (4, 4)$ and either g or $h \supset (4, 5)$, so $g+h \supset (4, 4)+(4, 5)$ which gives $r_p(f) \geqslant 6 \geqslant n-2$ for every p. This contradiction proves $r_p(f) = 4$ for $p \mid q$.

Again appealing to Lemmas 3, 4, 6 with (8.3), and noting that $(3, -2)$ is also perfect with minimum 1, either g or $h \supset (3, -2)$. In either case, (8.1) and (8.2) give $r_p(g+h) \geqslant 5$ for $p > 2$, so with $r_p(f) = 4$ when $p \mid q$ we have $q = 2$.

Now $r_p(g+h) > 4$ for $p > 2$ shows that $f \supset \varphi$ is true for every 4-ary φ with $f \underset{2}{\supset} \varphi$. So either $f \supset (4, 5)$ or $f \supset (4, 9)$. The first of these gives a contradiction as above; so $f \sim g+h \supset (4, 9) = (2, -3)+(2, -3)$. Applying Lemma 6 with $\varphi' = \varphi'' = (2, -3)$, if $h \not\supset (2, -3)$ then $g = (4, 4) \supset (4, 9)$, which is impossible. So $h \supset (2, -3)$ and the proof is complete.

9. Inequalities for reduced forms. In this section f is a positive form which is Hermite-reduced, and we make use of (4.6)–(4.8). We express f in the shape (7.3), and (2.4) gives

(9.1) $$(d_k d(\psi))^{-1}d(f) = 1, \ -4 \quad \text{for} \quad k(n-k) \text{ even, odd.}$$

We also have (7.4), and this gives

(9.2) $$d_k^{-1}d_{k+1} = \min\psi, \ -4\min\psi \quad \text{for} \quad k \text{ even, odd.}$$

We have a bound for d_{k+1} in terms of k, d_k, n, d if we can estimate $\min\psi$; for this the following two formulae will suffice:

(9.3) $$(\min\psi)^{k-n}|d(\psi)| \geqslant 3, 2, 4, 2, 3, 1, 1 \quad \text{for } n-k = 2, 3, 4, 5, 6, 7, 8;$$

(9.4) $$3(\min\psi)^2 \leqslant |d_k^{-1}d_{k+2}| \quad \text{for} \quad n \geqslant k+2.$$

The first of these is well known, and (9.4) follows on using $\min\psi \leqslant \min\psi_2$, where $\psi_2 = \psi(x_{k+1}, x_{k+2}, 0, \ldots, 0)$.

The labour of proving the 'if' of Theorem 1 by calculation, using the foregoing and Theorem 2, can be shortened in three ways. First, [2] gives

(9.5) $$c(F_{51}) = c(F_{52}) = 1,$$

so we may suppose $n \leqslant 8$. Next, reference to [8] would dispose of many of the easier cases. More usefully, since the small k give most trouble, we make use of the table of reduced quaternary forms given in [9]. From that table we find

(9.6) $$d \leqslant 21 \Rightarrow c(4, d) = 1,$$

which is best possible since

(9.7) $$(3, -2)+3x_4^2 \simeq (2, -3)+x_3^2+2x_4^2,$$

as is easily verified by means of (4.2) (for $p > 3$), (4.3), (4.5). We shall prove, using [9]:

Lemma 9. *Suppose $f \simeq F_i$ ($11 \leqslant i \leqslant 52$, see Table 1), and let f be Hermite-reduced; then f_4 is equivalent to one of $F_5, \ldots, F_{10}$.*

Proof. Using (9.5) and (9.3) (with $k = 0$, $\psi = f$), we find $d_1 = \min f < 2$, $= 1$. Then by (9.1)–(9.3), with $k = 1$, $|d_2| < 7$ in all cases; so with $d_2 \equiv 0$ or $1 \pmod 4$, $d_2 < 0$, we have $d_2 = -3$ or -4. Then (9.1)–(9.3) give $|d_3| \leqslant 6$, $d_4 \leqslant 29$, $d_5 < 36$. In the troublesome case $f = (6, -108) \simeq F_{38}$, we have $18 \mid d_5$, so $d_5 = 18$; whence a sharper estimate for d_4 can be had by using (9.4) instead of (9.3). Thus we find $d_4 \leqslant 25$, which referring to [9] gives $|d_3| \leqslant 4$, whence on calculating we find $d_4 < 20$. From [9] this gives either $2 \leqslant |d_3| \leqslant 3$ or $d_3 = -4$, $d_4 = 16$, $4 \mid d_5$. The latter case, in which f_4 is a sum of four squares, contradicts (9.1)–(9.3) for $n \geqslant 6$ or $d \leqslant 12$, leaving one case ($i = 20$) in which it contradicts $f \simeq F_i$. So $|d_3| \leqslant 3$.

Supposing first $d_3 = -3$, we calculate $d_4 \leqslant 16$ but besides $d_4 \equiv 0$ or $1 \pmod 4$, see (2.5), we have $d_4 \not\equiv 1 \pmod 3$ by Lemma 1, so $d_4 \leqslant 12$. If $d_3 = -2$ we calculate $d_4 \leqslant 13$, with equality only for $(5, 18)$, for which obviously $3 \mid d_4$. So again $d_4 \leqslant 12$; and this, by [9], gives the result.

10. Proof of the 'if' of Theorem 1. We assume f to be reduced and in the genus of one of the forms $F_{11}, \ldots, F_{52}$ of Table 1, say F_i, and we have to prove $f \sim F_i$. We may by (9.5) suppose $n \leqslant 8$, $i \leqslant 50$; and we take first $n = 5$, $i \leqslant 24$. By Lemma 9, we have six cases to consider.

First, $f_4 = F_5 = (4, 4)$. In this case $d \equiv 0 \pmod 2$ by Lemma 1, Theorem 2 gives $f \sim F_{11}, F_{12}$ or F_{13} if $d \leqslant 6$, and other d are excluded by (5.2).

Next, $f_4 = F_6 = (4, 5)$. Here $d \geqslant 3$ by (9.2) and (9.4), with $k = 3$, and $d \not\equiv \pm 1 \pmod 5$ by Lemma 1. Of the possibilities for $d = d(F_i)$, these restrictions exclude all but 3, 5, 7, giving $f \sim F_{14}, F_{15}$ or F_{16} by Theorem 2, and 9, 10, 12, 15, 18, excluded by (5.2).

The next two cases are similar. The case $f_4 = (2, -3) + (2, -3) = F_9$ needs a little more than one can get from (9.1)–(9.4); we have $3 \mid d$, $d \geqslant 6$, $d \neq 12, 15$ by (5.2), $f \sim F_{22}$ if $d = 9$. We need to exclude the case $d = 6$. Bordering $(2, -3) + (2, -3)$ as in the proof of Theorem 2 to give $(5, 6)$, we easily find $(5, 6) \sim (2, -3) + (3, -2) \supset (4, 8)$. Similarly for $f_4 = (2, -3) + (2, -4)$. So we have

$$(10.1) \qquad d_3 = -3 \quad \text{and} \quad d_4 = 9,\ 12 \Rightarrow d_5 \geqslant 9,\ 12 \ \text{respectively}.$$

As in the proof of Lemma 9, and using (5.2), we find $d_1, \ldots, d_5 = 1$, -3, -3, -12, 18 in case $f = (6, -108)$, whence $f \sim F_{38}$ by Theorem 2. We may therefore suppose $n \geqslant 6$ and $d \neq -108$, and we need to prove that f_5 is equivalent to one of

$$F_{11}, F_{12}, F_{14}, F_{15}, F_{17}, F_{22} = (5, 2), (5, 4), (5, 3), (5, 5), (3, -2) + (2, -3).$$

With n, d as above we find that $d_3 = -2$ implies $d_4 = 8$. $d_3 = -3$, $d_4 = 12$ is impossible, for using (9.3) it gives $d_5 < 12$, contradicting (10.1). So $d_4 \leqslant 9$. If $d_4 = 9$ we find $d_5 \leqslant 9$ by (9.3), with equality by (10.1), and so $f_5 \sim F_{22}$, and we may suppose $d_3 = -2$, $d_4 \leqslant 8$. If $d_4 = 4$, (5.2) gives us $|d| \leqslant 16$, whence we calculate $d_5 < 6$, and with $2 \mid d_5$ by Lemma 1 we have $d_5 = 2$ or 4 as required. If $d_4 = 5$, then $d_5 \geqslant 3$ and $\not\equiv \pm 1 \pmod 5$, as for $n = 5$; we calculate $d_5 < 7$ and have $d_5 = 3$ or 5 as required. If $d_4 = 8$ then $d_5 \geqslant 6$, $\not\equiv \pm 1 \pmod 8$, so $d_5 = 6$, as required, if we use (5.2) to exclude $n = 6$, $|d| \geqslant 24$ by considering the p-adic behaviour of $(6, -27)$, $(6, -28)$ for $p = 3, 7$.

We now finish the argument for $n = 6$ as for $n = 5$. So we assume $n = 7$ or 8, which gives better bounds for $\min \psi$ and so excludes some of the foregoing possibilities for f_5, leaving only $(5, 2)$, $(5, 4)$, $(5, 3)$, $(3, -2) + (2, -3)$. We next show that f_6 is equivalent to one of $F_{25} = (6, -3)$, $F_{27} = (6, -8)$, $F_{30} = (4, 4) + (2, -3)$.

For $d_5 = 2$ we have $d_6 \not\equiv \pmod 8$, so on calculating $|d_6| \leqslant 8$ we have what is required. For $d_5 = 4$, we note that (9.4), with $k = 4$, $d_4 = 4$, gives $|d_6| \geqslant 12$. On the other hand (9.3), with $k = 5$, gives $|d_6| < 16$, and Lemma 1 gives $2 \mid d_6$, so $d_6 = -12$, $f_6 \sim F_{30}$. With $d_5 = 3$ we find $d_6 \not\equiv 1 \pmod 3$, $|d_6| \geqslant 7$, < 12, $= 7$; and then $|d_7| \geqslant 4$, $d_8 = 16$ (if $n = 8$); otherwise $|d_6| < 7$. In the five remaining cases, $F_i \underset{p}{\supset} (6, -7)$ is false for $p = 2, 5, 2, 2, 2$.

So $d_5 \neq 3$. If $f_5 = (3, -2) + (2, -3)$ we have to have $|d_6| > 12$, $\leqslant 16$, $d_6 \not\equiv 1 \pmod 3$, $d_6 = -15$. Then we find $f_6 \sim (4, 5) + (2, -3)$, $d_4 \leqslant 5$, contradiction. Now the possibilities for f_6 are as stated; so we can finish the proof for $n = 7$, and also for $n \geqslant 8$ (for $n = 9, 10$, see (9.5)), if we can show that for $n = 8$ f_7 must be one of $F_{39} = (7, -1)$, $F_{40} = (7, -3)$, $F_{41} = (7, -2)$, $F_{45} = (7, -8)$. We can exclude $d_6 = -8$, because $d_5 = 2$ gives $|d_6| < 8$ unless $d_8 = 16$, and $F_{50} \underset{2}{\not\supset} (5, 2)$. Similarly, we avoid $d_6 = -12$ unless $d_8 = 16$, and then $|d_7| < 16$, $\equiv 0 \pmod 8$. Now $(8, 16) \underset{2}{\not\supset} (6, -3)$, $(6, -4)$ is easily verified, and by using $|d_8| \leqslant 9$ when $d_6 = -3$ or -4 the proof is easily completed.

11. Possibilities for $d_1, \ldots, d_5$ when $c(f) = 1$. From now on, since we have only to prove the 'only if' of Theorem 1, f is assumed to be SP and SF, with $n \geqslant 5$, $c(f) = 1$, and so $n \leqslant 10$ by [1]. With $r_p(f) \geqslant \frac{1}{2}n$, so $\geqslant 3$, for every p, and $n \geqslant 5$, Lemmas 3 and 4 (i) give $f \supset g$ for every 2-ary g. In particular, $f \supset (2, -3)$, whence, taking f to be reduced, $d_1 = 1$ and $d_2 = -3$.

Next, we have $f \supset (2, -4) = x_1^2 + x_2^2$. So we can appeal to Lemma 5 with $k = 2$, $f_2 = (2, -3)$, and $g = (2, -4)$, $m = 1$. Now (7.1) gives $|d_3| \leqslant 3$, and $d_3 \not\equiv -1 \pmod 3$ by Lemma 1, so $d_3 = -2$ or -3, and Theorem 2 gives $f_3 \sim F_3 = (3, -2)$ or $F_4 = (2, -3) + x_3^2$.

In the case $f_3 = (3, -2)$, f_3 cannot represent the 2-adic zero form $(2, -7) = x_1^2+x_1x_2+2x_2^2$. So we can appeal again to Lemma 5, with $f_k = (3, -2)$, $g = (2, -7)$, $m = 2$. From (7.1), with strict inequality by the Corollary to Lemma 5, $d_4 < 16$. By Lemma 1, $d_4 \not\equiv 1 \pmod 8$, so $d_4 = 4, 5, 8, 12$ or 13. For d_5, see Table 2, below.

In the other case, $f_3 = (3, -3) \not\supset (2, -8)$, which is a 3-adic zero form. So Lemma 5, with $m = 2$, gives $d_4 \leqslant 24$. We may however exclude $d_4 = 24$ by using (9.7), and $c(f) = 1$, to see that $f \supset (4, 24) \supset (3, -3) \Rightarrow d_3 = -2$. We have moreover $d_4 \not\equiv 1 \pmod 3$ by Lemma 1, and $d_4 \geqslant 9$, otherwise (9.4) with $k = 2$ would give $|d_3| < 3$. So $d_4 = 9, 12, 17, 20$, or 21. For d_5, again see Table 2.

Table 2

d_3	d_4	$f_4 \not\supset$	p	$d_5 \leqslant$	$d_5 \not\equiv$	$d_5 \geqslant$
-2	4	[1, 1, 2]	2	7	1 (2)	2
	5	[2, 2, 2]	2	9	± 1 (5)	3
	8	[3, 0, 3]	3	24	± 1 (8)	6
	12	[2, 1, 2]	3	23	-1 (3), 1 (4)	14
	13	[3, 3, 4]	13	51	—	16
-3	9	[1, 0, 2]	3	18	± 1 (3)	9, see (10.1)
	12	[2, 2, 3]	2	35	1 (3), -1 (4)	12, see (10.1)
	17	[2, 2, 9]	17	153	—	—
	20	[2, 2, 2]	2	40	—	25
	21	[2, 2, 2]	2	42	—	28

If g is the binary form shown in column 3 of Table 2, then $f \supset g$ as noted above, but $f_4 \not\supset g$ because Lemma 2 shows that $f_4 \underset{p}{\supset} g$ is false for the p of column 4. So on appealing to Lemma 5, with $m = g(0, 1)$, we have $d_5 \leqslant d_4 g(0, 1)$; in some cases there is strict inequality by the Corollary to Lemma 5. Hence the entries in column 5. $a(b)$, under $d_5 \not\equiv$, means $d_5 \not\equiv a \pmod b$ and is proved by Lemma 1. The lower bound for d_5 in column 7 comes from (9.4) with $k = 3$, unless otherwise stated.

Studying the table, and noting that if $r_p(f) = 3$ then $p \mid d_4$ and $p^2 \mid d_5$, we see that

(11.1) $$r_p(f) \geqslant 4 \quad \text{for all } p \geqslant 5.$$

For the only possible exception, by the inequalities in the table, is $d_3 = -3$, $d_4 = 20$, $d_5 = 20$. If so, however, by using Lemma 4 (ii), (iv) and $(3, -3) \underset{5}{\sim} (3, -2)$, see (4.2), we have the contradiction $d_3 = -2$.

We next show that

(11.2) $$r_3(f) = 3 \Rightarrow d_3 = -3 \quad \text{and} \quad d_4 = 9 \text{ or } 12.$$

For when $r_3 \leqslant n-2$ we can find h so that $f \simeq (2, -3)+h$, see the references given for Lemma 7. And then if $f \not\supset (3, -2)$ Lemma 6 gives $h \supset (3, -2)$, whence $f \supset x_1^2+(3, -2) = (4, 8)$ and so $r_3(f) \geqslant 4$. This gives the first implication. For the second, exclude $d_4 = 21$, with $9 \mid d_5$ giving $d_5 = 36$, by using $f_4 \supset (3, -7) \underset{3}{\sim} (3, -4)$. With this, Lemma 4 gives $f \supset (3, -4)$ and by using $(3, -4)$ instead of $(2, -8)$ in Lemma 5 we find the contradiction $d_4 \leqslant 4|d_3|$.

Consider the cases $d_3 = -2$, $d_4 = -12$, 13. In each, $f \supset (3, -4) = x_1^2+x_2^2+x_3^2$ would, using Lemma 5 with $f_k = (3, -2)$, give the contradiction $d_4 \leqslant 8$. So $f \not\supset (3, -4)$, and by Lemma 3 and $c(f) = 1$, $f \underset{p}{\supset} (3, -4)$ is false for some p; but not for odd p, for which we can use (11.1) or (11.2) and Lemma 4 (ii). So $f \underset{2}{\not\supset} (3, -4)$; and by Lemma 4 (iv), (v), $n = 5$ and $-d_5$ is a 2-adic square. A similar argument, using $(3, -3)$, 3 in place of $(3, -4)$, 2, shows that $-3d_5$ is a 3-adic square. It follows that either $d_5 \equiv 15 \pmod{72}$ or $d_5 \equiv 60 \pmod{288}$, giving $d_5 = 15$ or 60; but $d_5 = 60$ only if $r_2(f) = 3$, implying $2 \mid d_4$, $d_4 \neq 13$. So from the inequalities in the table we must have $d_4 = 12$, $d_5 = 15$, $n = 5$, then $f \sim F_{21}$ by Theorem 2.

A similar but simpler argument, involving the forms $(3, -2)$ and $(3, -4)$, and leading to the contradiction that $-d_5$ and $-2d_5$ are both 2-adic squares, shows that $d_4 \leqslant 12$ in case $d_3 = -3$. Now five rows of Table 2 have been disposed of, and the others need to be dealt with one by one.

$d_4 = 4$ gives $d_5 = 2, 4$, or 6 and so $f \sim F_{11}, F_{12}$ or F_{13} if $n = 5$. In case $n = 6$, $f \supset (3, -3)$ as above, $f_4 \not\supset (3, -3)$ since $r_2(4, 4) = 2$, so Lemma 5 with $f_k = (4, 4)$ gives $d_5 \leqslant 4$, $= 2$ or 4.

If $d_4 = 5$ then $f_4 \not\supset (3, -4)$ and so we find either $f \supset (3, -4)$ and $d_5 \leqslant 5$, or $n = 5$ and $-d_5$ a 2-adic square. So $d_5 = 3, 5$, or 7, $f_5 \sim F_{14}$, F_{15} or F_{16}, with $d_5 = 3$ or 5 when $n = 6$.

If $d_4 = 8$ and $f \not\supset (3, -7)$, $= x_1^2+(2, -7)$, then $n = 5$, $d_5 = 21$, $f_5 = (5, 21) \underset{p}{\supset} (4, 9)$ for all p is easily verified, and Lemma 5 with $g = (4, 9) = (2, -3)+(2, -3)$ gives the contradiction $d_5 \leqslant 8$. So $f \supset (3, -7)$ and Lemma 5 with $g = (3, -7)$ gives $d_5 < 16$. Excluding $d_5 = 13$, 14 by calculating that $f_5 \underset{p}{\supset} (4, 5)$, or $(4, 4)$, for all p, $d_5 = 6, 8, 10, 11$ or 12. This gives what we need for $n = 5$, since then f SF and SP implies obviously $8 \nmid d$. So suppose $n \geqslant 6$ (then d_5 must be 6, but the other possibilities can be excluded more easily later).

When $d_4 = 9$ we have $d_5 = 9, 12, 15$ or 18. For $d_5 = 12$ or 15 it is easily seen that $f \underset{p}{\supset} (3, -2)$ for every p, giving the contradiction $d_3 = -2$. With $d_5 = 18$, $f_5(x_1, 0, x_3, 0, x_5) = x_1^2+x_3^2+2x_5^2 = (3, -8) \underset{3}{\sim} (3, -2)$ leads to the same contradiction. So $d_5 = 9$ and $f_5 \sim F_{22}$.

Now suppose $d_3 = -3$, $d_4 = 12$. If $9 \nmid d_5$ then $f \not\supset (3, -2)$ gives $n = 5$ and $d_5 \equiv -2 \pmod{16}$; so the table gives $d_5 = 14$, 30, 18 or 27. But we see now that $f \supset (3, -7)$, so $d_5 \leqslant 2d_4$ and we have $d_5 = 14$ or 18, $f_5 \sim F_{23}$ or F_{24}. If $n = 6$, $d_5 = 18$ is the only possibility.

We have now completed the proof of Theorem 1 for $n = 5$.

12. Table 3, below, is constructed on the lines of Table 2 to give, for $n = 6$, a fairly small number of possibilities for $d = d_6$, for each of the possible f_5 found in § 11. Let g be the ternary form shown in column 4; in each case, $g = [a_{11}, a_{12}, a_{22}; a_{33}]$ is disjoint, with no terms in x_1x_3 or x_2x_3; and $f_5 \not\supset g$ comes from Lemma 2, with the p of column 5.

Table 3

d_3	d_4	d_5	$f_5 \not\supset$	p	$\|d\| \leqslant$	$d \not\equiv$	$\|d\| \geqslant$
-2	4	2	[1, 1, 2; 2]	2	16	1 (8)	3
		4	[1, 1, 2; 1]	2	31	1 (2)	12
-2	5	3	[1, 1, 1; 2]	3	24	1 (3)	7
		5	[2, 2, 2; 1]	2	39	± 1 (5)	15
-2	8	6	[2, 2, 2; 1]	3	47	1 (3), 5 (8)	15
		8	[1, 1, 2; 2]	2	64	1 (2)	24
		10	[1, 1, 1; 2]	2	80	± 1 (5), 5 (8)	39
		11	[3, 0, 3; 1]	3	132	1, 3, 4, 5, 9 (11)	47
		12	[1, 1, 1; 2]	3	96	1 (3), 1 (2)	55
-3	9	9	[1, 1, 4; 3]	3	144	$27 \mid d$	27
-3	12	18	[1, 1, 1; 3]	3	216	$27 \mid d$	80

The only point that needs explanation is that with the chosen g's we have always $f \underset{p}{\supset} g$ for every p. Supposing the contrary, we seek a contradiction. Referring to Lemma 4, we have $p > 2$ by (v), $p \nmid d(g)$ by (iii), and $r_p(f) \leqslant 3$ (obviously with equality) by (ii); so (11.1) gives $p = 3$. Now (11.2) gives $d_4 = 9$ or 18, whence the table gives $3 \mid d(g)$, a contradiction. We note also that $r_3(f) = 3$ implies $27 \nmid d$. In the last two rows, $27 \nmid d$ would give the contradiction $f \supset (3, -2)$.

We can cut down the number of possibilities in the table as in § 11. For example, in rows 3–11 we have to have $f \not\supset (4, 4)$, and we see from Lemmas 3, 4 and $c(f) = 1$ that $f \not\supset (4, 4)$ implies either $r_p(f) = 4$, $p^2 \mid d$, $p \mid d_5$, for some odd p, or d is a 2-adic square. In the latter case either $d \equiv 1 \pmod 8$ or $r_2(f) = 4$ and $d \equiv 4 \pmod{32}$, which implies $2 \mid d_5$. It will be convenient to put these arguments too into tabular form, see Table 4.

When column 3 of Table 4 asserts $f \not\supset g$, g 4-ary, we must assume $f \supset g$ and deduce a contradiction. $d(g) < d_4$, for the d_4 in column 1, gives an obvious contradiction; in other cases we have $d(g) > d_4$. Now in many cases Lemma 5, with $k = 4$, would contradict the value of d_5 shown in column 2. In three cases in which no such contradiction arises, we verify that $f_5 \not\supset g$ and use Lemma 5 with $k = 5$, giving a bound for $|d|$; and in column 3 we make the further assumption that $|d|$ exceeds this bound. Then in using Lemmas 3, 4 to exclude some d when $f \not\supset g$, we argue as above.

Table 4

d_4	d_5	$f \not\supset$	Restriction on d
4	2	(4, 9) if $d = -16$	$d \neq -16$
	4	(4, 8) if $\|d\| > 16$	$2d$ a 2-adic square
5	3	(4, 4)	$9 \mid d$ or $d \equiv 1 \pmod 8$
	5	(4, 4)	$25 \mid d$ or $d \equiv 1 \pmod 8$
8	6	(4, 4)	$9 \mid d$ or d a 2-adic square;
		(4, 5)	$9 \mid d$, $d \equiv 4 \pmod{16}$,
			or $d \equiv \pm 5 \pmod{25}$,
	8	(4, 4), (5, 4)	d a 2-adic square, $d \neq -28$,
	10	(4, 5), (4, 4), (4, 9)	$d \equiv 4 \pmod{16}$ or $\pm 5 \pmod{25}$,
		[use $f_5 \underset{2}{\not\supset} (4, 9)$]	$\Rightarrow 25 \nmid d$; d a 2-adic square;
			$d \equiv 1 \pmod 3$
	11	(4, 4), (4, 9), (4, 5)	$11^2 \mid d$ or $d \equiv 1 \pmod 8$,
			$1 \pmod 3$, and $\pm 5 \pmod{25}$
	12	(4, 4),	$9 \mid d$ or d a 2-adic square;
		$(2, -3) + (2, -4)$,	$d \neq -72, -92$, so $d = -60$;
		(4, 5), (4, 9)	$d \equiv 1 \pmod 3$ or $\pm 5 \pmod{25}$
9	9	$(2, -3) + 2(2, -3)$ if $\|d\| > 72$	$d \not\equiv 1 \pmod 8$ (Lemma 2)
12	18	(4, 9)	$d \equiv 4 \pmod{16}$

In dealing with the case $d_4 = 8$, $d_5 = 12$, we do not need the forms (4, 5), (4, 9) except for $r_2(f) = 4$, in which case $f \underset{2}{\supset} (4, 5)$, (4, 9) are both false.

Now there are 14 sets $(d_1, \ldots, d_5, d)$ for which Theorem 2 gives us $f \sim F_i$ for some i $(25 \leqslant i \leqslant 38)$. If we exclude these, Tables 3 and 4 show that there remain only a few cases, e.g. d_5, $d = 9, -108$, in which f is not SF. So the proof of Theorem 1 is complete for $n = 6$.

13. Completion of the argument for $n = 7, 8, 9, 10$. We first dispose of the case $r_p(f) \leqslant n - 3$ for some p, in which, by Lemmas 7, 8 and $c(f) = 1$, we have $n \leqslant 8$ and

$$f \sim (4, 4) + h, \quad h \supset (2, -3). \tag{13.1}$$

We see from (13.1), and $(4, 4) \supset (2, -3)$, that $f \underset{2}{\supset} (4, 9)$, whence $f \underset{2}{\supset} (4, 49) = (2, -7) + (2, -7)$; and since $r_p(f) \geqslant 5$ for all $p \neq 2$, we have $f \underset{p}{\supset} (4, 49)$ for all p by Lemma 4, $f \supset (4, 49)$ by Lemma 3. But $(4, 4) + (2, -3)$

$\underset{7}{\not\supset}$ (4, 49), by Lemma 2; so we can appeal to Lemma 5 with $f_k = (4, 4) + (2, -3)$, $g = (4, 49)$, and $m = 2$, since $(2, -7) \sim [1, 1, 2]$. (7.1), with equality excluded by the corollary to Lemma 5, gives $|d_7| < 24$.

We must have $8 \mid d_7$, since $r_2(f) = 4$, and we cannot have $d_7 \equiv -1 \pmod 3$, by Lemma 1, so $d_7 = -8$. This, by Theorem 2, gives $f_7 \sim F_{45}$, so we may suppose $n = 8$; and $h \supset (3, -2)$. The foregoing argument can be repeated, with $f_k = (4, 4) + (3, -2)$ and $g = (4, 49) + x_5^2$; and it gives $d = d_8 < 64$. $r_2(f) = 4$ gives $16 \mid d$, so $d = 16$, 32, or 48. In the first case we find $f \sim F_{50}$. In each of the others, using (4.3)–(4.5), we find the contradiction $r_2(f) > 4$.

Now we assume $r_p(f) \geqslant n-2$ for all p; whence $c(f) = 1$ and Lemmas 3, 4 give $f \supset g$ for every $(n-3)$-ary (positive) g. The argument is like that for $n = 5$, 6, but simpler, and is condensed into Table 5 below.

Table 5

n	k	d_k	$f_k \not\supset$	$d_{k+1} \not\equiv$	$<$ in (7.1), $d_{k+1} =$	$=$ in (7.1), $f \supset$
7	4	4	(4, 5)	1 (2)	2	—
	5	2	(2, −3) + (2, −3)	1 (8)	−3, −4	(5, 2) + (2, −3)
	6	−3	(2, −7) + 2(2, −3)	1 (3)	−1, −3, (−4)	—
	6	−4	(2, −7) + (2, −4)	1 (4)	{−1}, −2, −4, −5, −6	—
8	5	2	(5, 3)	1 (8)	−3, −4	—
	6	−3	(5, 4)	1 (3)	−1	(7, −3)
	6	−4	(5, 5)	1 (4)	{−1}, −2	(7, −4)
	7	−1	(3, −4) + (2, 7)	—	1, (4), 5	—
	7	−2	(3, −2) + (2, −7)	5 (8)	{1}, 4	—
	7	−3	(3, −2) + (2, −3)	−1 (3)	{1, 4}, 9	—
	7	−4	(3, −4) + (2, −7)	1 (2)	{4, 8}, 12, ..., 28	
9	6	−3	(6, −4)	1 (3)	−1	—
	7	−1	(4, 4) + (2, −3)	—	1	(7, −1) + (2, −3)
	8	1	(4, 4) + (2, −7)	—	1	—
10	7	−1	(7, −2)	—	1	—
	8	1	(4, 4) + (3, −7)	—	1	—
	9	1	(4, 4) + (3, −7)	—	−3, −4, −7	(8, 1) + (2, −8)

If g is the form shown in column 4, then we have $f \supset g$, g being $(n-3)$-ary, and $f \supset (n-3, d_{n-3})$, as explained above. $f_k \not\supset g$ follows from $f_k \underset{p}{\not\supset} g$ with $p = 3$ for $n = 8$, $k = 6$, 7, $d_k = -3$, $p = 2$ otherwise. $f_k \underset{p}{\not\supset} g$ is either straightforward, or proved by Lemma 2. Lemma 5 is applied with $m = 1$ or 2; it is easy to see which. Values of d_{k+1} that f can be excluded by the reduction inequalities or, for $k = n-1$, make not SF, are enclosed in { }, ( ) respectively in column 6. Blank entries in column 7 are justified by either Lemma 6 or the corollary to Lemma 5. The forms $(7, d_7)$, $d_7 = -3$, -4, in column 7, and columns 2, 3, are $(6, d_7) + x_7^2$, by Lemma 5.

Studying the table, we see at once that the 'only if' of Theorem 1 is true for $n = 7$. For $n = 9$, all we need is to notice that $(7, -1) + (2, -3) \simeq (8, 1) + 3x_9^2$; for this we may use Lemma 4. For $n = 10$, note that in the cases $d = -4$, -7, -8 that we have to exclude $f \supset (8, 1) + 2x_9^2$. With $c(f) = 1$ this gives $f \supset \Phi_9$, where $\Phi_9 = (9, 2) \simeq (8, 1) + 2x_9^2$ is perfect with minimum 1. See [1], p. 559, Lemma 8, and p. 563, Theorem 3. With $g = \Phi_9$ and $m = 1$, Lemma 5 gives $|d| < 4$.

Finally, for $n = 8$ we have to exclude $d = 12, \ldots, 28$ when $f_7 = (6, -4) + x_7^2$. We can do so by using Lemmas 3, 4 and $c(f) = 1$ to show that f represents in each case at least one of the perfect forms $(6, -3)$, $(6, -7)$, except for $d = 16$, which however makes f not SF.

References

[1] G. L. Watson, *The class-number of a positive quadratic form*, Proc. London Math. Soc. (3) 13 (1963), pp. 549–576.

[2] — *One-class genera of positive quadratic forms*, Journal London Math. Soc. 38 (1963), pp. 387–392.

[3] — *Transformations of a quadratic form which do not increase the class-number*, Proc. London Math. Soc. (3) 12 (1962), pp. 577–587.

[4] — *Transformations of a quadratic form which do not increase the class-number, II*, Acta Arith. 27 (1975), pp. 171–189.

[5] — *One-class genera of positive ternary quadratic forms*, Mathematika 19 (1972), pp. 96–104.

[6] — *One-class genera of positive quaternary quadratic forms*, Acta Arith. 24 (1973), pp. 461–475.

[7] — *Integral Quadratic Forms*, Cambridge 1960.

[8] — *Positive quadratic forms with class-numbers*, Proc. London Math. Soc. (3) 13 (1963), pp. 577–592.

[9] Kurt Germann, *Tabellen reduzierter, Positiver, quaternarer quadratischer Formen*, Commentarii Mathematici Helvetici 38 (1963–4), pp. 56–83.

UNIVERSITY COLLEGE
London, England

Received on 27. 12. 1973 (511)