

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK

S. 7133.
[81]

DISSERTATIONES
MATHEMATICAE
(ROZPRAWY MATEMATYCZNE)

KOMITET REDAKCYJNY

KAROL BORSUK redaktor

ANDRZEJ BIAŁYNICKI-BIRULA, BOGDAN BOJARSKI,
ZBIGNIEW CIESIELSKI, JERZY ŁOŚ, ANDRZEJ MOSTOWSKI,
ZBIGNIEW SEMADENI, WANDA SZMIELEW

LXXXIV

G. L. WATSON

The number of minimum points of a positive quadratic form

38

WARSZAWA 1971

PAŃSTWOWE WYDAWNICTWO NAUKOWE

6.7133



PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

BUW-EO-71/ - /:

CONTENTS

Introduction	5
1. Definition of certain special forms	6
2. Statement of results	8
3. Proof of Theorem 2	9
4. Preliminaries for Theorem 1	10
5. Further preliminaries for Theorem 1	15
6. Construction for Theorem 1	18
7. The case $B_4 \not\subset f_n, C_5 \not\subset f_n$ of Theorem 1	21
8. The case $B_5 \not\subset f_n$ of Theorem 1	24
9. Further construction for the case $B_5 \subset f_n, n \geq 7$	26
10. The case $E_8 \not\subset f_n$	30
11. Preliminaries for the case $E_8 \not\subset f_n$	32
12. Proof of Theorem 1 for $E_8 \not\subset f_n$ and for $n \geq 10$	34
13. Completion of proof of Theorem 1	38
14. Conclusion	40
References	42

Introduction. Let $f_n = f_n(\mathbf{x}) = f_n(x_1, \dots, x_n)$ be an n -ary quadratic form, with real coefficients, such that:

(i) f_n is positive-definite, that is, $f_n(\mathbf{x}) > 0$ at all real points $\mathbf{x} = (x_1, \dots, x_n) \neq (0, \dots, 0)$; and

(ii) the values of $f_n(\mathbf{x})$ at integer points $(x_1, \dots, x_n) \neq (0, \dots, 0)$ have a positive greatest lower bound, which we denote by $\min f_n$.

It is easily proved that each of these properties implies the other, and also implies that the lower bound $\min f_n$ is attained. By a minimum point of f_n is meant a point $\mathbf{x} = (x_1, \dots, x_n)$, with integer coordinates, at which f_n takes the value $\min f_n$. The minimum points of f_n obviously occur in pairs $\pm \mathbf{x}$, and we denote the number of such pairs by $s(f_n)$.

We recall that the form f_n is said to be perfect if every f'_n with the same minimum points as f_n is a constant multiple of f_n . Further, denoting by $d(f_n), > 0$, the determinant of f_n , f_n is said to be *absolutely extreme* if $d(f'_n) \geq d(f_n)$ for every f'_n with $\min f'_n = \min f_n$. It is easily proved, as we shall see later, that, for given n , $s(f_n)$ is maximal only when f_n is perfect. It is plausible to conjecture that $s(f_n)$ is maximal only when f_n is absolutely extreme. So we shall refer to the work of Barnes [1], Blichfeldt [2], Korkine and Zolotareff [3], and earlier work quoted in these papers, on perfect and absolutely extreme forms.

From the work of Rankin [4] it follows, a little crudely, that

$$(1) \quad s(f_n) < 2^{4n(1+\varepsilon)} \quad \text{for} \quad \varepsilon > 0 \text{ and } n > n_0(\varepsilon).$$

Scott [5] has constructed numerous perfect forms, from which some possibilities for the pair $(s(f_n), n)$ can be found. Voronoi [6] showed that

$$(2) \quad s(f_n) \leq 2^n - 1.$$

The main object of the present paper is to prove that

$$(3) \quad s(f_n) \leq 3, 6, 12, 20, 36, 63, 120, 136 \quad \text{for} \quad n = 2, 3, 4, 5, 6, 7, 8, 9$$

respectively. For $n \leq 6$ this follows easily from [1] and [3], but for $n = 7, 8, 9$ it is new. For $n \geq 10$ I have not been able to obtain best possible results; I shall state just what follows without extra labour from the arguments needed for $n \leq 9$. It would not be possible, by my method, to prove the case $n = 9$ of (3) without doing considerably more for $n \leq 8$. We shall see that each of (3) is best possible; and that if the case of equality (which is essentially unique) is excluded then the bounds

12, ..., 136 can be replaced by 10, 16, 30, 46, 75, 135. These in turn are best possible for $n \leq 8$; the 135 is probably not best possible, but could not be improved below 129.

Excluding more special cases, some of the bounds will be lowered further. It will also be shown that if, for given positive integers s, n , $s(f_n) = s$ is impossible then $s > (n-1)^2$; and a little more is true for some n .

Barnes's paper [1] on 6-ary forms is very long and difficult, so in the hope of contributing to an easier proof of his result I shall here use only a weakened form of it, and I shall indicate that even this could be avoided.

Blichfeldt's paper [2] is also very difficult. I shall show how the proof could be shortened a little for $n = 6$, and I hope to do the same for $n = 7$ in a later paper. I shall not use [2] at all, except incidentally to prove for $n = 6, 7, 8$ that f_n is absolutely extreme when equality holds in (3).

I could shorten and simplify the very prolix arguments of [3], [6], but I refrain so as not to make this paper too long. I shall however give a proof of (2) which shows that the left member could be replaced by the number of pairs of integer points at which $0 < f_n < 2 \min f_n$.

1. Definition of certain special forms. A_n is defined for $n = 1, 2, \dots$ by

$$(1.1) \quad A_n(\mathbf{x}) = \sum \{x_i x_j \mid 1 \leq i \leq j \leq n\} = \frac{1}{2} \sum_{i=0}^n x_i^2,$$

with

$$(1.2) \quad x_0 = -(x_1 + \dots + x_n).$$

From this, $\min A_n = 1$ is clear, and the minimum points can be expressed conveniently, using the redundant coordinate x_0 , as the permutations of $(1, -1, 0, \dots, 0)$.

B_n is defined for $n \geq 3$ by

$$(1.3) \quad B_n(\mathbf{x}) = \frac{1}{2}(y_1^2 + y_2^2 + \dots + y_n^2),$$

where

$$(1.4) \quad y_i = \begin{cases} (x_1 + x_2 + \dots + x_n) - x_i & \text{for } i = 1, 2, 3; \\ x_i & \text{for } i > 3, \end{cases}$$

whence the x_i are all integers if and only if the y_i are so, and satisfy

$$(1.5) \quad y_1 + \dots + y_n \equiv 0 \pmod{2}.$$

Hence $\min B_n = 1$ and the minimum points are given by (1.4) and \mathbf{y} a permutation of $(\pm 1, \pm 1, 0, \dots, 0)$. We note that $A_3 = B_3$.

We next define E_n for $n \leq 8$ by

$$(1.6) \quad E_1, \dots, E_6 = A_1, A_2, A_3, B_4, B_5,$$

and

$$(1.7) \quad E_{n+1}(x) = \frac{1}{2} \sum_{i=1}^n (y_i - \frac{1}{2}x_{n+1})^2 + (1 - \frac{1}{8}n)x_{n+1}^2$$

for $n = 5, 6, 7$ and y_i as in (1.4). Hence $\min E_n = 1$ for $n = 6, 7, 8$ is easily verified; and the minimum points can be counted by taking $x_{n+1} = 0, 1, 2$ and choosing y subject to (1.5) so as to minimize the n -fold sum. Next,

$$(1.8) \quad E_9(x) = \frac{1}{2} \sum_{i=1}^7 (y_i - \frac{1}{2}x_8 - x_9)^2 + \frac{1}{8}x_8^2 + \frac{1}{2}x_9^2,$$

the y_i as in (1.4), with $n = 7$. By putting $(x_8, x_9) = (0, 0), (1, 0), (2, 0), (\pm 1, 1), (\pm 2, 1)$, and minimizing the sevenfold sum subject to (1.5), we verify $\min E_9 = 1$ and count the minimum points. From the definitions we have identically

$$(1.9) \quad E_n(x) = E_{n+1}(x_1, \dots, x_n, 0) \quad \text{for } n \leq 8,$$

which may be used to shorten the task of counting the minimum points.

We now define C_5, C_6, D_6 by

$$(1.10) \quad C_5(x_1, \dots, x_5) = \frac{1}{12} \sum_{i=0}^5 z_i^2,$$

$$(1.11) \quad C_6(x_1, \dots, x_6) = \frac{1}{12}(z_0 + \frac{5}{2}x_6)^2 + \frac{1}{12} \sum_{i=1}^5 (z_i - \frac{1}{2}x_6)^2 + \frac{3}{8}x_6^2,$$

$$(1.12) \quad D_6(x_1, \dots, x_6) = \frac{1}{12} \sum_{i=0}^2 (z_i - x_6)^2 + \frac{1}{12} \sum_{i=3}^5 (z_i + x_6)^2 + \frac{1}{2}x_6^2,$$

where in each case

$$(1.13) \quad z_i = \begin{cases} x_1 & \text{for } i = 1; \\ x_1 + 3x_i & \text{for } i = 2, \dots, 5; \\ -(z_1 + \dots + z_5) & \text{for } i = 0. \end{cases}$$

We notice that (1.13) makes the x_i all integers if and only if the z_i are so and satisfy

$$(1.14) \quad z_0 \equiv z_1 \equiv \dots \equiv z_5 \pmod{3}.$$

So we verify $\min C_5 = \min C_6 = \min D_6 = 1$, and count the minimum points, by minimizing the sixfold sum subject to (1.14) and $z_0 + \dots + z_5 = 0$, after putting $x_6 = 1$.

It is easy to calculate the determinant of E_n , for $n \leq 8$, from the foregoing definitions, and to see that it is equal to that of the known

absolutely extreme form, with minimum 1, see [2]. Hence E_1, \dots, E_8 are absolutely extreme; but we shall not use this property in what follows. We shall show that subject to (1.9), with $n = 8$, the definition (1.8) makes the determinant of E_8 as small as possible, whence it is plausible to conjecture that E_8 is also absolutely extreme.

2. Statement of results. It is easy to verify, as indicated in § 1, that the forms A_n, \dots, E_n are all perfect, with minimum 1, and satisfy

$$(2.1) \quad s(A_n) = \frac{1}{2}n(n+1) \quad \text{for all } n,$$

$$(2.2) \quad s(B_n) = n(n-1) \quad \text{for } n \geq 3,$$

$$(2.3) \quad s(C_n) = 15, 27 \quad \text{for } n = 5, 6,$$

$$(2.4) \quad s(D_8) = 22,$$

$$(2.5) \quad s(E_1), \dots, s(E_8) = 1, 3, 6, 12, 20, 36, 63, 120, 136.$$

Now our main result, implying (3), is:

THEOREM 1. *Let f_n be a positive-definite quadratic form, in $n \geq 2$ variables, with real coefficients. Suppose (vacuously if $n \geq 10$) that $f_n/\min f_n$ is not equivalent to any of the forms E_n, A_4, B_6, C_8 defined in (1.1)–(1.3). Then the number $s(f_n)$ of pairs of minimum points of f_n can (for imperfect but not for perfect f_n) take the values 28, 46 for $n = 6, 7$ respectively. Excluding these possibilities too, we have*

$$(2.6) \quad s(f_n) \leq 2, 5, 9, 16, 25, 42, 75 \quad \text{for } n = 2, 3, 4, 5, 6, 7, 8$$

respectively, each best possible and

$$(2.7) \quad s(f_n) < \begin{cases} 136 & \text{for } n = 9; \\ 2^{n-2} + 8 & \text{for } n \geq 10. \end{cases}$$

In the opposite direction, we prove:

THEOREM 2. *Let n, s be positive integers, $n > 1$. Then a sufficient condition for the existence of an imperfect positive-definite n -ary quadratic form f_n , with real coefficients, having exactly s pairs of minimum points, is*

$$(2.8) \quad s \leq \begin{cases} 2, 5 & \text{for } n = 2, 3; \\ (n-1)^2 & \text{for } n \geq 4; \\ 42, 50 & \text{for } n = 7, 8. \end{cases}$$

We shall prove Theorem 2 by induction on n , using:

THEOREM 3. *There exists f_n , imperfect and with $s(f_n) = s$, as in Theorem 2, if there exists an f_{n-1} , perfect or imperfect, with $s(f_{n-1}) = s$ or $s-1$.*

Proof. Take $f_n = f_{n-1}(x_1, \dots, x_{n-1}) + cx_n^2$, with $c \geq \min f_{n-1}$. Then obviously f_n is imperfect, $\min f_n = \min f_{n-1}$, and $s(f_n) - s(f_{n-1}) = 0$ or 1 according as $c >$ or $= \min f_{n-1}$.

Voronoi [6] proves (2) by showing that if \mathbf{x}, \mathbf{y} are two minimum points of f_n with $\mathbf{x} \equiv \mathbf{y} \pmod{2}$, then $\mathbf{x} = \pm \mathbf{y}$. (2) follows from this at once on noting that neither \mathbf{x} nor \mathbf{y} can be congruent modulo 2 to $\mathbf{0} = (0, \dots, 0)$. The improvement on (2) mentioned at the end of the Introduction follows at once from:

THEOREM 4. *If $\mathbf{x}, \mathbf{y} = (x_1, \dots, x_n), (y_1, \dots, y_n)$ satisfy $\mathbf{x} \equiv \mathbf{y} \pmod{2}$ but $\mathbf{x} \neq \pm \mathbf{y}$, then*

$$(2.9) \quad f_n(\mathbf{x}) + f_n(\mathbf{y}) \geq 4 \min f_n$$

for every positive-definite n -ary quadratic form f_n , and equality holds if and only if each of $\frac{1}{2}\mathbf{x} \pm \frac{1}{2}\mathbf{y}$ is a minimum point of f_n .

Proof. $\mathbf{u}, \mathbf{v} = \frac{1}{2}\mathbf{x} \pm \frac{1}{2}\mathbf{y}$ are integer points, neither $\mathbf{0}$. So the result follows from the well-known identity

$$(2.10) \quad f_n(\mathbf{u} + \mathbf{v}) + f_n(\mathbf{u} - \mathbf{v}) = 2f_n(\mathbf{u}) + 2f_n(\mathbf{v}).$$

It may be observed that Theorems 1, 2 determine completely all the possibilities for $s(f_n)$ with imperfect f_n for each $n \leq 7$.

3. Proof of Theorem 2. Theorem 2 follows from Theorem 3 and Lemma 1 below (which is needed also for Theorem 1), with a little further notation.

f_n, f'_n, φ_n will henceforth denote positive-definite quadratic forms with real coefficients, in n variables, φ_n being perfect but f_n, f'_n not necessarily imperfect. g_n denotes an n -ary quadratic form with real coefficients, not necessarily positive. The definition of perfection given above is equivalent to saying that f_n is perfect if and only if no g_n not identically 0 can satisfy

$$(3.1) \quad g_n(\mathbf{x}) = 0 \quad \text{for all integral } \mathbf{x} \text{ with } f_n(\mathbf{x}) = \min f_n.$$

We shall use the notation $f_n \rightarrow f'_n$ to mean that $\min f_n = \min f'_n$ and every minimum point of f_n is also a minimum point of f'_n , but not conversely, whence $s(f_n) < s(f'_n)$. We now state and prove:

LEMMA 1. *If f_n is imperfect there is at least one perfect φ_n with $f_n \rightarrow \varphi_n$, implying $s(f_n) < s(\varphi_n)$. For any such φ_n, g_n defined as $f_n - \varphi_n$ satisfies (3.1) and*

$$(3.2) \quad g_n(\mathbf{x}) \geq 0 \quad \text{for all integral } \mathbf{x} \text{ with } \varphi_n(\mathbf{x}) = \min \varphi_n.$$

Conversely, if φ_n (perfect) and g_n satisfy (3.2), with at least one case of equality and at least one case of strict inequality, and θ is positive and sufficiently small, then f_n defined as $\varphi_n + \theta g_n$ satisfies $f_n \rightarrow \varphi_n$; and $s(\varphi_n) - s(f_n)$ is the number of cases of strict inequality in (3.2).

Proof. The first assertion is proved in [6] and the rest follows easily. Instead of assuming that there is at least one case of strict inequality in (3.2), it would suffice since φ_n is perfect to assume g_n not identically 0.

COROLLARY TO LEMMA 1. *If $f_n \rightarrow \varphi_n$ and the form $f_{n-1} = f_{n-1}(x_1, \dots, x_{n-1})$ derived from f_n by putting $x_n = 0$ is perfect, with minimum = $\min f_n$, then the g_n of (3.1), (3.2) is necessarily of the shape $x_n l(\mathbf{x})$, l a linear form such that $l(\mathbf{x}) \geq 0$ at every minimum point of φ_n with $x_n > 0$. And $l(\mathbf{x}) > 0$ for just $s(\varphi_n) - s(f_n)$ such minimum points.*

Proof. This becomes clear on putting $x_n = 0$ in (3.1), (3.2) and using the perfection of f_{n-1} .

Proof of Theorem 2. For the case $s = 50$, $n = 8$ see [5]. For the rest we make several applications of the second part of Lemma 1. First,

$$(3.3) \quad \varphi_n = A_n \quad \text{and} \quad g_n = x_n(x_r + x_{r+1} + \dots + x_n),$$

with any r between 1 and n , gives an f_n with $s(A_n) - s(f_n) = \frac{1}{2}n(n+1) - s(f_n) = r$. The 'lost' minimum points, at which strict inequality holds in (3.2), are, see (1.2), the pairs $\pm(x_0, \dots, x_n)$ with $x_n = 1$, and (x_0, \dots, x_{n-1}) a permutation of $(-1, 0, \dots, 0)$, with the -1 in one of the first r places. This proves the sufficiency of $\frac{1}{2}n(n-1) \leq s < \frac{1}{2}n(n+1)$. Hence by induction on n , using Theorem 3, $s < \frac{1}{2}n(n+1)$ suffices, proving Theorem 2 for $n \leq 4$.

We now take $\varphi_n = B_n$ and $g_n = y_n(y_r + \dots + y_n)$, using the notation of (1.4). (3.2) clearly holds, and the cases of strict inequality are $\mathbf{y} = (\mathbf{u}, 1)$ and $\mathbf{y} = (-\mathbf{u}, 1)$, where \mathbf{u} is a permutation of $(1, 0, \dots, 0)$, with the 1 in one of the first $r-1$ places when $\mathbf{y} = (-\mathbf{u}, 1)$. So we lose $n-1+r-1$ pairs of minimum points, whence with $1 \leq r \leq n$ the f_n of the theorem exists if $(n-1)(n-2) \leq s \leq (n-1)^2$.

We next take $\varphi_n = B_n$ and

$$(3.4) \quad g_n = y_{n-1}(y_r + \dots + y_{n-1}) + y_n(y_1 + \dots + y_n), \quad 1 \leq r < n.$$

(3.2) again holds, and the number of pairs of minimum points lost is as above $n-1+n-2+r-1$. So the desired f_n exists if $(n-2)^2 < s \leq n^2 - 3n + 3$.

Combining these results we have by induction on n the sufficiency of $s \leq (n-1)^2$. This completes the proof for $n \neq 7$, so now we take $\varphi_n = E_7$, and we may suppose $36 < s \leq 42$. I leave it to the reader to verify that $g_7 = y_6(y_r + \dots + y_6)$, $1 \leq r \leq 6$, disposes of the case $s = 42 - r$. For $s = 42$, take $g_7 = y_6(-y_1 - y_2 - y_3 - y_4 - y_5 + y_6 + 4x_7)$.

This completes the proof; but it is convenient to notice at this point that for $n = 6, 7, 8$, $\varphi_n = E_n$ and $g_n = y_{n-1}x_n$ gives an imperfect f_n with $s(f_n) = 28, 46, 75$. This remark will shorten the proof of Theorem 1.

4. Preliminaries for Theorem 1. Henceforth, Λ_n is the standard lattice in n -dimensional space, whose points $\mathbf{x} = (x_1, \dots, x_n)$, with the x_i all integers, will be regarded as row vectors, or 1 by n matrices. By excluding from Λ_n the origin $\mathbf{0} = (0, \dots, 0)$ we define Λ'_n ; and Λ_n^+ is the set of $\mathbf{x} \in \Lambda'_n$ whose last non-zero element is positive. The rows \mathbf{e}_i of the n

by n identity matrix I_n form a basis for Λ_n . We note that $s(f_n)$ is the number of minimum points of f_n that are in Λ_n^+ .

We notice that the $\mathbf{y} \in \Lambda_n$ that satisfy (1.5) constitute a sublattice of Λ_n , which we denote by $\Lambda_n^{(2)}$, and which is put by (1.4) into 1-1 correspondence with Λ_n .

Latin capitals (except $A-E$ and L, N) will denote rectangular, say m by n , matrices, with integer elements, I_n being an identity matrix as above, and O null. If Y, Z have the same number of columns then $Y \supseteq Z$, or $Z \subseteq Y$, means the Z is a sub-matrix of some Y_1 derivable from Y by trivial row operations (permutations and changes of sign). $Y \supset Z$, or $Z \subset Y$, means the same thing, except that Z has fewer rows than Y . If Y is m by n , with $\min(m, n) = h \geq 1$, then $\Delta(Y) (\geq 0)$ is the g.c.d. of the determinants of all the h by h sub-matrices of Y . So $\Delta(Y) >, = 0$ for $\text{rank } Y = >, < h$. Thus $\Delta(\mathbf{x}), \mathbf{x} \in \Lambda_n^+$, is the g.c.d. of the x_i , and is 1 if and only if \mathbf{x} is primitive. In case $m = n$, $\Delta(Y) = |\det Y|$.

The positive-definite quadratic form f_n will henceforth be assumed to have minimum 1, without loss of generality since f_n and $f_n/\min f_n$ have the same minimum points. For $k < n$, $f_k \subset f_n$, or $f_n \supset f_k$, means that $\min f_k = 1$ and f_n represents f_k properly (that is, some $f'_n \sim f_n$, \sim denoting equivalence over the integers, reduces to f_k on putting $x_i = 0$ for $i = k + 1, \dots, n$). It will be convenient to use this notation also for $k = n$; if so, \subset means \sim .

By a minimal matrix of f_n is meant an $s(f_n)$ by n matrix, say $X(f_n)$, among whose rows is one and only one of each pair $\pm \mathbf{x}$ of minimum points of f_n . We thus have $\mathbf{x} \in X(f_n)$ if and only if \mathbf{x} is a minimum point of f_n ; and $f_n \rightarrow f'_n$ (with the convention that each form has minimum 1) may be redefined to mean $X(f_n) \subset X(f'_n)$. $X(f_n)$ may be normalized, if convenient, by using the trivial row operations mentioned above to arrange its rows in some convenient order, and choose them all from Λ_n^+ . If on the other hand we replace $X(f_n)$, using column operations, by $X(f_n)T$, T n by n , $\det T = \pm 1$, then we obtain a minimal matrix of a form $f'_n \sim f_n$, by the substitution $\mathbf{x} \rightarrow \mathbf{x}T$.

We now prove three lemmas.

LEMMA 2. Let $\varphi_n, n \leq 6$, be a perfect form, with $\min \varphi_n = 1$; and in case $n = 6$ assume $s(\varphi_n) \geq 22$. Then one and only one of the following must hold:

$$(4.1) \quad \varphi_n = \begin{cases} A_n \\ A_3 = B_3 \\ A_4 \text{ or } B_4 \\ A_5, C_5 \text{ or } B_5 \\ D_6, C_6, B_6 \text{ or } E_6 \end{cases} \quad \text{and} \quad s(\varphi_n) = \begin{cases} 1, 3 \\ 6 \\ 10 \text{ or } 12 \\ 15, 15 \text{ or } 20 \\ 22, 27, 30 \text{ or } 36 \end{cases}$$

for $n = 1$ or $2, 3, 4, 5, 6$ respectively.

Proof. Each case of (4.1) is possible, with the stated value of $s(\varphi_n)$, by § 1. A_5 and C_5 are inequivalent, since A_5 is integer-valued and C_5 ($= 3/2$ at the point $(3, -3, 0, 0, 0, 0)$ with the notation of (1.13)) is not so. A_5, C_5 being the only pair with the same s and n , the foregoing remark enables us to complete the proof by referring to [3] for $n \leq 5$, [1] for $n = 6$, to see that we have found the right number of possibilities for each n . C_5 and D_6 are clearly equivalent to certain forms defined in [3], [1] which there seem to have little or no symmetry.

LEMMA 3. Let $Y \subseteq X(f_n)$ have $m \leq n$ rows. Then

$$(4.2) \quad \Delta(Y) \leq \begin{cases} 1 & \text{for } m \leq 3 \\ 2 & \text{for } m = 4, 5 \\ 4, 8 & \text{for } m = 6, 7 \end{cases}$$

and

$$(4.3) \quad B_4 \subset f_n \quad \text{if } m = 4 \text{ and } \Delta(Y) = 2.$$

Further, if $m \leq 4$ and $\Delta(Y) = 0$, then every row of Y is a linear combination, with coefficients each 0 or ± 1 , of the rows of some $Y_1 \subset Y$ with $\Delta(Y_1) = 1$.

Proof. We notice first that by replacing $Y, X(f_n)$ by $YT, X(f_n)T$, with T n by n , $\det T = \pm 1$, we may suppose $Y = (Z, O)$, Z m by m , $\Delta(Y) = |\det Z|$. This means that it suffices to prove the lemma for $m = n$.

Now as observed in [7] we have $\Delta(Y) \leq \gamma_n^{4n}$, where γ_n is the Hermite constant; and (4.2) follows from classical results, without using the exact values of γ_6, γ_7 . From [7], 172, Lemma 1 we see that $m = n = 4$ and $\Delta(Y) = 2$ imply $s(f_4) \geq 12$, giving $f_4 \supset B_4$ by Lemmas 1, 2; whence (4.3).

For the last assertion, we do not need $m \leq n$, so we may assume $n = \text{rank } Y \leq 3$ and, by (4.2) with n for m , $I_n \subset Y$. Then (4.2), again with n for m , is contradicted if any element of Y is not 0 or ± 1 .

We notice that strict inequality in (4.2) is impossible for $m = 1, 2$; that is

$$(4.4) \quad \mathbf{x} \subseteq X(f_n) \Rightarrow \Delta(\mathbf{x}) = 1 \quad \text{and} \quad \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \subseteq X(f_n) \Rightarrow \Delta \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = 1.$$

The first of these is trivial, so if the second fails, with \mathbf{x}, \mathbf{y} then linearly dependent by (4.2), we have $\mathbf{x} = \pm \mathbf{y}$, contradicting the construction of $X(f_n)$.

We shall need to know, for certain f_4 , that there do not exist vectors $\mathbf{x}_1, \dots, \mathbf{x}_4$, in A_4 , such that

$$(4.5) \quad \mathbf{0} \neq \mathbf{x}_i \not\equiv \mathbf{x} \pmod{2} \quad \text{for } i = 1, \dots, 4 \text{ and all } \mathbf{x} \subseteq X(f_4),$$

$$(4.6) \quad \mathbf{x}_i \not\equiv \mathbf{x}_j \pmod{2} \quad \text{for } 1 \leq i < j \leq 4,$$

and

$$(4.7) \quad \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 + \mathbf{x}_4 \equiv \mathbf{0} \pmod{2}.$$

For $1 \leq k \leq n$ we define

$$(4.8) \quad s_k(f_n) = \max\{s(f_k) \mid f_k \subset f_n\}.$$

This implies obviously $s_n(f_n) = s(f_n)$. Further, since any $f_{n-1} \subset f_n$ can be obtained by transforming some linear form L into a multiple of x_n and then putting $x_n = 0$, we see that $s_{n-1}(f_n)$ can be found by counting the greatest number of rows of $X(f_n)$ at which such an L (not identically 0, and with integer coefficients) can vanish. That is,

$$(4.9) \quad s_{n-1}(f_n) = \max\{m \mid Y \text{ } m \text{ by } n, Y \subseteq X(f_n), \text{rank } Y < n\}.$$

It is clear from Lemmas 1, 2 that

$$(4.10) \quad 0 < s_k(f_n) \leq 1, 3, 6, 12, 20, 36 \quad \text{for } k = 1, \dots, 6,$$

and trivial that

$$(4.11) \quad s_k(f_n) \geq s_k(f_m) \quad \text{if } m \geq k \text{ and } f_m \subset f_n.$$

We now prove two more lemmas.

LEMMA 4. (i) $s(f_3) \geq 5$ implies $s_2(f_3) = 3$.

(ii) $s(f_4) \geq 7$ implies $s_2(f_4) = 3$.

(iii) $s(f_4) \geq 10$ implies $f_4 \sim A_4$ or B_4 , in which cases (4.5)–(4.7) are inconsistent.

(iv) $s(f_5) \geq 13$ implies $s_4(f_5) \geq 9$.

(v) $s(f_5) \geq 14$ implies $f_4 \subset f_5$ for some f_4 , with $s(f_4) \geq 9$, for which (4.5)–(4.7) are inconsistent.

(vi) $s(f_5) \geq 14$ and $f_5 \rightarrow 3$ or $\sim A_5$ imply $s(f_4) \geq 10$.

(vii) $s(f_5) \geq 15$ implies one of $f_5 \sim A_5, f_5 = C_5, B_4 \subset f_5$.

Proof. By Lemmas 1, 2 we may suppose $f_n \rightarrow 3$ or $= \varphi_n, \varphi_n = A_n, B_4, B_5$ or $C_5, n = 3, 4, \text{ or } 5$.

Since A_n goes into A_{n-1} when any one of the variables is put equal to 0, all that is asserted is trivial for $f_n = A_n$, except (iii), for which we consider the five possibilities modulo 2 for x_i satisfying (4.5), (4.6), and verify that no four of them satisfy (4.7). If $f_n \rightarrow 3$, we choose i such that as few as possible of the $s(A_n) - s(f_n)$ rows of $X(A_n)$ that are not minimum points of f_n satisfy $x_i = 0$; certainly at least one of them does not, for some i , and this gives all we need except (ii). For (ii), using the redundant x_0 of (1.2), there is a pair i, j for which none of the (at most 3) missing rows of $X(A_4)$ satisfies $x_i = x_j = 0$.

When $n = 5$ and $f_5 \rightarrow 3$ or $= C_5$, with $s(f_5) \geq 13$, we may suppose, with the notation of (1.13), that f_5 has as minimum points all the permutations of $(1, 1, 1, 1, -2, -2)$ except at most two, which may be taken by permuting the subscripts to be included among $(1, -2, -2, 1, 1, 1)$,

$(-2, 1, -2, 1, 1, 1), (1, 1, 1, 1, -2, -2)$. Among the others are nine may be written as (u, v) , each of u, v ranging over permutations of $(1, 1, -2)$. This gives (iv), and (v) is easily verified.

So we suppose $f_n \rightarrow B_n$, $n = 4$ or 5 , since the case $f_n = B_n$ is trivial. We denote by s_{ij} ($= 0, 1$ or 2) the number of pairs of points given by (1.4) and $y = \pm(e_i - e_j)$ that are minimum points of f_n . And if $s_{ij} = 1$, we write $\lambda_{ij} = \pm 1$ according as $e_i - e_j$ or $e_i + e_j$ is a minimum point of f_n .

We now permute the subscripts, as is easily seen to be possible, so that one of the following holds:

- (a) $s_{12} = s_{34} = 2$.
- (b) $s_{12} = s_{13} = s_{23} = 2$, all other $s_{ij} \leq 1$.
- (c) $s_{ij} = 2$ implies $\min(i, j) = 1$.

In case (a) above, the four points given by (1.4) and $y = e_1 \pm e_2, e_3 \pm e_4$ make up a 4 by n matrix $Y \subseteq X(f_n)$ with $\Delta(Y) = 2$, so $B_4 \subset f_n$ by (4.3), and all we need is clear. In case (b), we have $s(f_n) \leq 9, 13$, for $n = 4, 5$. (ii) is now clear, and (iv) is easily proved by putting one of the $y_i = 0$.

If $n = 4$ in case (c), we have trivially $s(f_4) \leq 9$. This disposes of (iii). To prove (ii), we permute the subscripts further so as to have $s_{12} = 2, s_{13} \geq 1, s_{23} \geq 1$. With $s(f_4) \geq 7$ this is easily seen to be possible; and it gives three minimum points whose sum is 0 .

Finally suppose $f_5 \rightarrow B_5$ and (c) holds. This implies $s(f_5) \leq 14$. If equality does not hold, all we need is (iv), and we prove it by putting one of the $y_i = 0$. So suppose $s(f_5) = 14$; then $s_{1j} = 2$ for $j = 2, \dots, 5, s_{ij} = 1$ for $2 \leq i < j \leq 5$.

It is easily seen to be possible, by permuting y_2, \dots, y_5 and changing their signs, to suppose that either every λ_{ij} ($2 \leq i < j \leq 5$) is 1, or that $\lambda_{ij} = -1$ for $2 \leq i < j \leq 4$. In the first case we obtain $f_4 \subset f_5$ with $s(f_4) = 10$ by putting $y_1 + \dots + y_5 = 0$, whence by (iii) we have (v). In the second case we obtain $f_4 \subset f_5$ with $s(f_4) \geq 9$ by putting $y_5 = 0$.

This $f_4 \rightarrow B_4$, has minimum points $y = e_1 \pm e_j, e_2 + e_3 + e_4 - e_j$, $j = 2, 3, 4$. All we need is that with it (4.5)–(4.7) are inconsistent. Working in $A_4^{(2)}/2A_4^{(2)}$, or alternatively using (1.4), this is easily verified.

LEMMA 5. *If $C_5 \subset f_6$ and $s(f_6) \geq 22$ then $f_6 \sim C_6$ or D_6 .*

Proof. By Lemma 2, we may suppose $f_6 \rightarrow$ or $= \varphi_6, \varphi_6$ one of C_6, B_6, E_6 . Now however, with $C_5 \subset f_6$, Lemma 1 and the Corollary, and the perfection of C_5 , give $C_5 \subset \varphi_6$. Since B_6 and E_6 are integer-valued, while C_5 is not, we clearly cannot have $\varphi_6 = B_6$ or E_6 . So we have $f_6 \rightarrow C_6$.

Now the linear form l of the Corollary to Lemma 1 can be expressed in the notation of (1.13) as

$$(4.12) \quad c_0(2z_0 + 5x_6) + \sum_{i=1}^5 c_i(2z_i - x_6) + c_6x_6,$$

where the constants c_i , not all 0 since l does not vanish identically, may be supposed because of $z_0 + \dots + z_5 = 0$ to satisfy $c_0 + \dots + c_5 = 0$.

The points at which l must be ≥ 0 are those with $x_0 = 1$ and the cofactors of c_0, \dots, c_5 in (4.12) a permutation of $\pm(1, 1, 1, 1, 1, -5)$. So we must have

$$(4.13) \quad c_6 \geq 6c_i \quad \text{and} \quad c_6 \geq -6c_i \quad \text{for} \quad i = 0, \dots, 5.$$

If $c_6 \leq 0$ this makes all the $c_i = 0$; so $c_6 > 0$. Now strict inequality holds in one at least of each of the pairs of inequalities (4.13). This gives $s(C_6) - s(f_6) = 27 - s(f_6) \geq 6$, which contradicts $s(f_6) \geq 22$ and completes the proof. [Instead to using the case $n = 6$ of Lemma 2, and thereby depending on [1], we could have proved, as for $B_{n-1} \subset f_n$ in the next section, that $C_5 \subset \varphi_6$ implies $\varphi_6 \sim C_6$ or D_6].

5. Further preliminaries for Theorem 1. In this section we shall prove Theorem 1 for $n \leq 5$ and investigate the cases $B_{n-1} \subset f_n$, $n = 5, \dots, 9$.

Proof of Theorem 1 for $n \leq 5$. We may by Lemmas 1, 2 assume $f_n \ni$ or $= A_n, B_4, B_5$ or C_5 . We necessarily have $f_1 = A_1 = E_1 = x_1^2$ in the trivial case $n = 1$, in which we have nothing to prove. By (1.6), we see that all the cases $f_n = A_2 = E_2, A_3 = E_3, A_4, B_4 = E_4, B_5$ are among those excluded in Theorem 1.

So we suppose $f_n \ni \varphi_n = A_2, A_3, A_4, B_4, A_5, B_5$ or C_5 . With this $s(f_n) < s(\varphi_n)$ gives (2.6) except in the cases $\varphi_n = B_4, B_5$, see (4.1). $f_4 \ni B_4$ gives (2.6) by Lemma 4 (iii).

So we suppose $n = 5$, $f_5 \ni B_5$. Then by (4.1) and Lemma 4 (vii), we have (2.6) unless $B_4 \subset f_5$. With this, all we need is $s(f_5) - s(B_4) = s(f_5) - 12 \leq 4$. This could be proved easily by using Lemma 1 as in the proof of Lemma 5; but instead we shall prove something more precise that will be needed later.

We now consider the possibilities for $s(f_n)$, and for the minimum points of f_n , when $B_{n-1} \subset f_n$. Clearly we may suppose, for some constants r_i, c , that

$$(5.1) \quad f_n(x) = \frac{1}{2} \sum_{i=1}^{n-1} (y_i - r_i x_n)^2 + c x_n^2,$$

with the y_i as in (1.4), with $n-1 (\geq 3)$ for n . That is, we work as in the definition of E_6, E_7, E_8 in the lattice $A_{n-1}^{(2)} \times A_1, A_1$ being the integers.

With the usual notation $\|a\| = \inf\{|x - a| \mid x \in A_1\}$, for real a , it will be convenient to write $\beta_i = \|r_i\|, \beta = \max(\beta_1, \dots, \beta_{n-1})$. It is clearly possible, with $x_n = 1$ and y_i satisfying, see (1.5),

$$(5.2) \quad y_1 + \dots + y_{n-1} \equiv 0 \pmod{2},$$

to make the $(n-1)$ fold sum in (5.1) $\leq (n-2)\beta^2 + (1-\beta)^2$, and this expression takes its greatest value $(n-1)/4$, for $0 \leq \beta \leq \frac{1}{2}$, when $\beta = \frac{1}{2}$.

So we must have (since we assume $\min f_n = 1$)

$$(5.3) \quad c \geq (9-n)/8.$$

Conversely, with $n \leq 7$, as we shall assume for the present, (5.3) gives $c \geq \frac{1}{4}$, and so $f_n \geq 1$ is implied by $x_n \geq 2$.

We shall now assume without loss of generality that the $(n-1)$ fold sum in (5.1) is least, for $x_n = 1$, when $\mathbf{y} = \mathbf{0}$. With this, we shall assume further that

$$(5.4) \quad c = 1 - \frac{1}{2}(r_1^2 + \dots + r_{n-1}^2).$$

For $\min f_n = 1$ implies that (5.4) holds with \geq for $=$, and with $>$ we should clearly have the uninteresting case $s(f_n) = s(B_{n-1})$. As assumed above we have

$$(5.5) \quad \sum_{i=1}^{n-1} (y_i - r_i)^2 \geq (r_1^2 + \dots + r_{n-1}^2),$$

whenever the integers y_i satisfy (5.2). Let the \mathbf{y} for which equality holds in (5.5) be called the minimal \mathbf{y} . Then clearly the number of minimal \mathbf{y} is $s(f_n) - s(B_{n-1}) - \varepsilon$, where $\varepsilon = 1$ in case $c = \frac{1}{4}$, $n = 7$, 0 otherwise. Now we consider three cases.

Case 1: $\beta = \frac{1}{2}$. The cases of equality in (5.5) are clearly just those in which each $\|y_i - r_i\| = \beta_i$, which gives 1 or 2 choices for y_i according as $\beta_i <$ or $= \frac{1}{2}$, and so, by (5.2), the number of minimal \mathbf{y} is 2^{h-1} , where $h, \geq 1, \leq n-1$, is the number of $\beta_i = \frac{1}{2}$. The set of minimal \mathbf{y} is thus determined; for example, when $h = n-1$, in which case $f_n = E_n$ for $n = 6, 7$, it may be taken to be the set of \mathbf{y} with each $y_i = 0$ or 1, with evenly many 1's.

Case 2: $\beta = 0$; that is, each r_i is an integer. Here by (5.5) we may suppose the r_i to be 0, ..., 0 or 1, 0, ..., 0. In the first case we have only one minimal \mathbf{y} ; in the second we have $f_n \sim B_n$ (because the $2y_i - r_i x_n$ and x_n are integers with even sum) and $2n-2$ minimal \mathbf{y} (with one $y_i - r_i = \pm 1$, the others 0).

Case 3: $0 < \beta < \frac{1}{2}$. Here a minimal \mathbf{y} clearly has each $|y_i - r_i| = \beta_i$ or $1 - \beta_i$. The latter choice, if unavoidable because of (5.2), must be made in one case only, and that with $\beta_i = \beta$, since trivially $0 \leq a < \beta < \frac{1}{2}$ implies $(1-a)^2 + \beta^2 > a^2 + (1-\beta)^2$. So we have 1 or h minimal \mathbf{y} , with h as in case 1. And in the latter case a change of origin (with possibly some changes of sign) would take the minimal \mathbf{y} into h permutations of $(1, 0, \dots, 0)$.

We now notice that the lattice $A_4^{(2)}$ has an automorphism

$$(5.6) \quad \mathbf{y} \rightarrow (L, L - y_3 - y_4, L - y_2 - y_4, L - y_2 - y_3),$$

$$2L = y_1 + y_2 + y_3 + y_4,$$

which takes B_4 into itself. This automorphism interchanges the two cases $(r_1, \dots, r_4) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}), (1, 0, 0, 0)$ in which $c = \frac{1}{2}, n = 5$; whence in each of these cases we have $f_5 \sim B_5$.

We can now complete the foregoing proof of Theorem 1 for $n = 5$ by noting that except in these two cases we have at most four minimal y , giving $s(f_5) \leq s(B_4) + 4 = 16$. Later however we shall need to note that equality holds when and only when either $h = 3$ in case 1, or $h = 4$ in case 3.

We shall return later to the case $n = 6$ of (5.1), and we now consider the cases $n = 7, 8, 9$. We notice first that (5.3) is useless for $n = 9$. But the argument leading to (5.3) shows that, for $n = 9$, $\min f_9 = 1$ implies

$$(5.7) \quad 1 \leq \frac{1}{2} \|r_1\|^2 + \dots + \frac{1}{2} \|r_4\|^2 + \frac{1}{2} + c,$$

and similarly, taking $x_9 = 2$,

$$(5.8) \quad 1 \leq \frac{1}{2} \|2r_1\|^2 + \dots + \frac{1}{2} \|2r_4\|^2 + \frac{1}{2} + 4c.$$

Multiplying (5.7), (5.8) by 4, 3 and adding,

$$(5.9) \quad \frac{7}{2} \leq 2 \max \{4a^2 + 3|2a|^2 \mid 0 \leq a \leq \frac{1}{2}\} + 16c.$$

The maximum is easily seen to be 1, attained only for $a = \frac{1}{4}, \frac{1}{2}$. So $c \geq \frac{3}{32}$. Equality is possible only if, with every $\|r_i\| = \frac{1}{4}$ or $\frac{1}{2}$, we have equality in each of (5.7), (5.8). This implies that just one of the $\|r_i\|, i = 1, 2, 3, 4$, is $\frac{1}{4}$, the rest all $\frac{1}{2}$. Avoiding this case by permuting the subscripts 1-8,

$$(5.10) \quad c > \frac{3}{32} \quad \text{if} \quad n = 9.$$

Now we can prove:

LEMMA 6. For $n = 7, 8, 9$, Theorem 1 is true if $B_{n-1} \subset f_n$.

Proof. For $u = 1, 2, \dots$ denote by $s(u)$ the number of minimum points of f_n with $x_n = u$. Then $s(u) = 0$ for $u \geq 4$ by (5.3), (5.10), the former of which gives also $s(3) = 0$. In case $n = 7$ we may suppose also $s(2) = 0$; for otherwise equality must hold in (5.3), whence each $\|r_i\| = \frac{1}{2}$, giving $f_7 \sim E_7$. Hence, assuming (2.6) or (2.7) false, we have

$$(5.11) \quad s(1) \geq 13, \quad s(1) + s(2) \geq 34, \quad s(1) + s(2) + s(3) \geq 80$$

for $n = 7, 8, 9$ respectively.

Now for $n = 7$, looking at cases 1-3 above, we see that (5.11) implies $s(1) = 2^{h-1} = 16$ or 32 , with just $h = 5$ or 6 of the $\|r_i\| = \frac{1}{2}$. For $h = 6$ this is the case excluded above, and for $h = 5$ it gives $s(f_7) = s(B_6) + 16 = 46$, which is excluded in Theorem 1.

If for $n = 8$ or 9 and $u = 2$ or 3 , Case 1 above gives $s(u) = 2^{h-1}$, $h \geq 5$, then h of the $\|ur_i\|$ are $= \frac{1}{2}$, and so, cf (5.4), $s(u) > 0$ implies $u^2c + h/8 \leq 1$, implying $c \leq \frac{3}{8}u^2 \leq \frac{3}{32}$, and contradicting (5.3) or (5.10). Similarly, if Case 2 leads to $s(u) = 2n - 2$, with $u = 2$ or 3 , then $u^2c = \frac{1}{2}$.



This for $n = 8$, $u = 2$ gives equality in (5.3), and $f_8 \sim E_8$; and for $n = 9$, $u = 3$ it contradicts (5.10). So we assume $s(u) \leq 8$ for $u = n-6$, and $s(2) \leq 16$ for $n = 9$.

Now if $n = 8$ (5.11) gives $s(1) \geq 26$, so $s(1) = 2^{h-1}$, $h = 6$ or 7 , with h of the $\|r_i\| = \frac{1}{2}$. With $h = 7$ this is the case of equality in (5.3), and so $f_8 \sim E_8$; we therefore suppose $h = 6$. Now exactly 6 of the $2r_i$ are integers and this gives $s(2) \leq 1$, contradicting (5.11).

With $n = 9$, (5.11) gives $s(1) \geq 56 = 2^{h-1}$, $h = 7$ or 8 . But $h = 8$ will not do; for with eight $\|r_i\| = \frac{1}{2}$ we cannot have $f_n = 1$ when $x_9 = 1$. So $h = 7$, $s(1) = 64$. With seven of the $\|3r_i\| = \frac{1}{2}$, $s(3) > 0$ is possible only if $9c \leq \frac{1}{9}$, contradicting (5.10); so $s(3) = 0$, and we need $s(2) = 16$ to satisfy (5.11). And with seven of the $\|2r_i\| = 0$, this is possible only if the eighth $\|2r_i\| = 0$, making the corresponding $\|r_i\| = 0$ because of the impossibility of $h = 8$. This is easily seen to give $f_9 \sim E_9$ which completes the proof.

6. Construction for Theorem 1. In this section we suppose that $1 \leq k \leq n-2$, $k \leq 5$, and $f_k \subset f_n$, with $s(f_k)$ maximal, that is, $= s_k(f_n)$. Without loss of generality we may suppose that f_n goes into f_k by putting $x_i = 0$ for $i = k+1, \dots, n$. Then we have an identity of the shape

$$(6.1) \quad f_n(\mathbf{x}) = f_k\left(x_1 - \sum r_{1j}x_j, \dots, x_k - \sum r_{kj}x_j\right) + \psi(x_{k+1}, \dots, x_n),$$

where the r_{ij} , $i \leq k < j$, are real constants, the summation is over $j = k+1, \dots, n$, and ψ is a positive-definite $(n-k)$ ary quadratic form, whose minimum may be < 1 . It follows at once, with suitable normalization of $X(f_n)$, that

$$(6.2) \quad X(f_n) = \begin{pmatrix} X_{11} & O \\ X_{21} & X_{22} \end{pmatrix}, \quad \text{with} \quad X_{11} = X(f_k) \text{ and } \mathbf{0} \notin X_{22}.$$

We may indeed suppose that every row of X_{22} is in A_{n-k}^+ .

It is clear that if f_n has not n linearly independent minimum points, then $s(f_n) = s(f_{n-1})$ for some $f_{n-1} \subset f_n$. Excluding such f_n , as we clearly may, it is clear that $s(f_k) = s_k(f_n)$ implies

$$(6.3) \quad \Delta(X_{11}) \neq 0.$$

For $\mathbf{a} \in A_{n-k}'$, we define $N(\mathbf{a})$ as the number of rows of X_{22} that are $= \pm \mathbf{a}$; we ought to write $N(f_k, \mathbf{a}, f_n)$, but the simpler notation should cause no confusion. Clearly, see (4.4), $N(\mathbf{a})$ is the number of possibilities modulo 2 for a $u \in A_k$ with $(u, \mathbf{a}) \in X(f_n)$; and

$$(6.4) \quad s(f_n) - s(f_k) = \sum \{N(\mathbf{a}) \mid \mathbf{a} \in A_{n-k}^+\}.$$

If we replace (x_{k+1}, \dots, x_n) by $x_n \mathbf{a}$, for primitive \mathbf{a} , we obtain a form $f_{k+1} \subset f_n$; so

$$(6.5) \quad s_{k+1}(f_n) - s(f_k) \geq \max \{N(\mathbf{a}) \mid \mathbf{a} \text{ primitive}\}.$$

Next, for $\mathbf{b} \in A_{n-k}$, we define

$$(6.6) \quad N'(\mathbf{b}) = \sum \{N(\mathbf{a}) \mid \mathbf{a} \in A_{n-k}^+, \mathbf{a} \equiv \mathbf{b} \pmod{2}\},$$

which with (6.4) gives

$$(6.7) \quad s(f_n) - s(f_k) = \sum \{N'(\mathbf{b}) \mid \mathbf{b} \pmod{2}\},$$

the summation being over 2^{n-k} values of $\mathbf{b} \in A_{n-k}$, pairwise incongruent modulo 2.

Now supposing for the moment that $N(\mathbf{a}) = 0$ for imprimitive \mathbf{a} , each $N(\mathbf{a})$, by the argument leading to (6.5) is $s(f_{k+1}) - s(f_k)$, for some $f_{k+1} \supset f_k$; whence, e.g. from Lemma 5 or § 5, we may be able to determine the possibilities for $N(\mathbf{a})$. This may enable us to deduce (2.6) or (2.7) from (6.4), or alternatively, to deduce a good lower bound for $s_{k+1}(f_n)$ from (6.5) and $s_k(f_n) = s(f_k)$.

This argument will not work unless we know a good upper bound for the number of positive terms on the right of (6.4). Here Theorem 4 may help. If not, we note that the number of positive terms in (6.7) is trivially bounded; so we have the alternative of trying to show that the sum in (6.6) either always has just one positive term, or that if not it is small.

We now outline what is needed to make the argument work. First, we wish to show that $N(\mathbf{a}) = 0$ for imprimitive \mathbf{a} . If not, we have, for some $\mathbf{u} \in A_k$ and some prime p ,

$$(6.8) \quad (\mathbf{u}, \mathbf{a}) \subset X(f_n), \quad p \mid \Delta(\mathbf{a}) \neq 0.$$

This is trivially impossible if we know that $\min \psi > \frac{1}{4}$. If not, then (6.3), (6.8) imply the existence of Y with

$$(6.9) \quad Y \subseteq X(f_n), \quad Y \text{ } k+1 \text{ by } n, \quad \Delta(Y) \geq p.$$

For $p \geq 5$ this will always contradict Lemma 3 if $k \leq 5$. For $p = 3$, (6.9) contradicts Lemma 3 if $k \leq 4$; also if $k = 5$ and $\Delta(Y_1) \geq 2$, for some 5×5 $Y_1 \subseteq X_{11}$, in which case (6.9) holds with 6 for p on the right. So the case $p > 2$ of (6.8) will not present any difficulty for any f_k with which we shall be concerned.

If (6.8) holds with $p = 2$, we try to contradict Lemma 3 with $m \geq 2$, even, by solving one of the congruences

$$(6.10) \quad \mathbf{u} \equiv \mathbf{0}, \mathbf{x}, \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} + \mathbf{z} \pmod{2},$$

where $\mathbf{x}, \mathbf{y}, \mathbf{z}$ denote rows of $X_{11} = X(f_k)$. If we can solve one of the first three of these, then we appeal to Lemma 3 with $m \leq 3$, the rows of Y being the first m of $(\mathbf{u}, \mathbf{a}), (\mathbf{x}, \mathbf{0}), (\mathbf{y}, \mathbf{0})$. By (6.10) we have $2 \mid \Delta(Y)$, and with m minimal and $\mathbf{a} \neq \mathbf{0}$, $\Delta(Y) \neq \mathbf{0}$, giving the contradiction. Similarly if we suppose $B_4 \notin f_n$, all four of (6.10) must be impossible, with $N(\mathbf{a})$ choices for \mathbf{u} .

Assuming it established that $N(\mathbf{a}) = 0$ for imprimitive \mathbf{a} , the sum in (6.7) has at most $2^{n-k} - 1$ positive terms, and we should like to know that we cannot have

$$(6.11) \quad \begin{pmatrix} \mathbf{u}_1 & \mathbf{a}_1 \\ \mathbf{u}_2 & \mathbf{a}_2 \end{pmatrix} \subseteq X(f_n), \quad p \mid \Delta \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \end{pmatrix} \neq 0.$$

We shall have no difficulty in proving this impossible for odd p ; then any $\mathbf{a}_1, \mathbf{a}_2$ with $\mathbf{a}_2 \not\equiv \mathbf{a}_1 \pmod{2}$ can be simultaneously transformed into the first two base points of \mathcal{A}_{n-k} by an integral unimodular transformation of x_{k+1}, \dots, x_n .

The sum in (6.6) has two or more non-zero terms when (6.11) is possible with $p = 2$, and $\mathbf{a}_1 \equiv \mathbf{a}_2 \equiv \mathbf{b} \pmod{2}$. If so, cf (6.10), the first two of

$$(6.12) \quad \mathbf{u}_1 + \mathbf{u}_2 \equiv \mathbf{0}, \mathbf{x}, \mathbf{x} + \mathbf{y} \pmod{2},$$

\mathbf{x}, \mathbf{y} any rows of X_{11} , have to be impossible; and the third too if $B_4 \notin f_n$.

Now suppose that there exist $\mathbf{a}_i \in \mathcal{A}_{n-k}$ satisfying

$$(6.13) \quad \mathbf{a}_1 \not\equiv \mathbf{a}_2 \not\equiv \mathbf{a}_3 \not\equiv \mathbf{a}_1, \quad \mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 \equiv \mathbf{0} \pmod{2},$$

and that each $N(\mathbf{a}_i)$ is positive, whence for some $\mathbf{u}_i \in \mathcal{A}_k$

$$(6.14) \quad (\mathbf{u}_i, \mathbf{a}_i) \subset (X_{21}, X_{22}) \quad \text{for } i = 1, 2, 3.$$

Further suppose that by choice of the \mathbf{u}_i and \mathbf{x} we have

$$(6.15) \quad \mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3 \equiv \mathbf{0} \text{ or } \mathbf{x} \pmod{2}, \quad \mathbf{x} \subseteq X_{11}.$$

LEMMA 7. *Suppose that (6.13), (6.14), and either the first of (6.15), or $B_4 \notin f_n$ and the second of (6.15), are satisfied. Then $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$ for some choice of the signs.*

Proof. In the first case the $(\mathbf{u}_i, \mathbf{a}_i)$ have sum $\mathbf{0} \pmod{2}$ and so are the rows of a 3 by n $Y \subseteq X(f_n)$ with $\Delta(Y) \equiv 0 \pmod{2}$, whence $\Delta(Y) = 0$ by (4.2). Using the last part of Lemma 3, $(\mathbf{u}_1, \mathbf{a}_1) \pm (\mathbf{u}_2, \mathbf{a}_2) \pm (\mathbf{u}_3, \mathbf{a}_3) = \mathbf{0}$ easily follows, giving the result.

With $B_4 \notin f_n$, in the second case, Lemma 3, with a 4 by n Y having rows $(\mathbf{x}, \mathbf{0})$ and $(\mathbf{u}_i, \mathbf{a}_i)$, gives $\Delta(Y) = 0$ and one row of Y is a linear combination, with coefficients each 0 or ± 1 , of the other three. Looking at (6.13), (6.15) we see that each coefficients is ± 1 , and the result follows.

COROLLARY TO LEMMA 7. *If (6.13), (6.14) and the second of (6.15) hold, but $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$ is false for all choices of the signs, then all the eight points*

$$(6.16) \quad \frac{1}{2}(\mathbf{x}, \mathbf{0}) \pm \frac{1}{2}(\mathbf{u}_1, \mathbf{a}_1) \pm \frac{1}{2}(\mathbf{u}_2, \mathbf{a}_2) \pm \frac{1}{2}(\mathbf{u}_3, \mathbf{a}_3)$$

are minimum points of f_n . Further, if s' is the number of rows \mathbf{x} of X_{11} for which the foregoing hypotheses hold, with given \mathbf{a}_i and suitably chosen \mathbf{u}_i , $i = 1, 2, 3$, the \mathbf{u}_i possibly depending on \mathbf{x} , then for some f_m with $m \leq k+3$ we have

$$(6.17) \quad f_m \subset f_n, \quad s(f_m) \geq s(f_k) + 8s' + N(\mathbf{a}_1) + N(\mathbf{a}_2) + N(\mathbf{a}_3).$$

Proof. For the first assertion see [7], p. 172, Lemma 1. For the second, we count the $8s'$ points (6.16), the $s(f_k)$ rows of X_{11} , and the $N(\mathbf{a}_i)$ points $(\mathbf{u}_i, \mathbf{a}_i)$. Evidently, using $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 \neq \mathbf{0}$, and (6.13), which implies $\mathbf{a}_i \neq \pm \mathbf{a}_j$ for $i \neq j$, these points are all different and no two differ only in sign. And they clearly span a space of dimension $\leq k+3$.

To make effective use of Lemma 7 we need also:

LEMMA 8. *Suppose that (6.13) holds and that $\mathbf{a}_4, \dots, \mathbf{a}_7$, each in Λ_{n-k} and linearly independent of $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ modulo 2, satisfy $\mathbf{a}_{4+i} \equiv \mathbf{a}_4 + \mathbf{a}_i \pmod{2}$, $i = 1, 2, 3$; whence trivially (6.13) remains valid if the triplet $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$ is replaced by $\{\mathbf{a}_h, \mathbf{a}_i, \mathbf{a}_j\}$ with $\{h, i, j\} = \{h, 4, 4+h\}$, $h = 1, 2$, or 3, or one of $\{1, 6, 7\}$, $\{2, 5, 7\}$, $\{3, 5, 6\}$. Then at least one of the seven triplets so obtained fails to satisfy $\mathbf{a}_h \pm \mathbf{a}_i \pm \mathbf{a}_j = \mathbf{0}$, for all four choices of the signs.*

Proof. If not, we may clearly suppose without loss of generality that $\mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 = \mathbf{0}$ and $\mathbf{a}_7 = \mathbf{a}_4 + \mathbf{a}_1 + \mathbf{a}_2$. Now we have to have

$$\mathbf{a}_5 = \pm \mathbf{a}_1 \pm \mathbf{a}_4 = \pm \mathbf{a}_2 \pm \mathbf{a}_7 = \pm \mathbf{a}_2 \pm (\mathbf{a}_4 + \mathbf{a}_1 + \mathbf{a}_2) = \pm (\mathbf{a}_1 + \mathbf{a}_4)$$

and so we may suppose $\mathbf{a}_5 = \mathbf{a}_1 + \mathbf{a}_4$; and similarly $\mathbf{a}_6 = \mathbf{a}_2 + \mathbf{a}_4$. Now however neither of $\mathbf{a}_5 \pm \mathbf{a}_6 = \pm \mathbf{a}_3$.

7. The case $B_4 \not\subset f_n, C_5 \not\subset f_n$ of Theorem 1. We use the construction of § 6 to prove;

LEMMA 9. *If $k \leq \min(4, n-2)$, $B_4 \not\subset f_n$, and $s_k(f_n) \geq 2^{k-1}$ then either*

$$(7.1) \quad s_{k+1}(f_n) - s_k(f_n) \geq 2^{k-2} + 1$$

or

$$(7.2) \quad s(f_n) \leq s_k(f_n) + 2^{n-2} - 2^{k-2}.$$

Proof. With f_k such that $s(f_k) = s_k(f_n)$, we see that (7.2) follows from (6.7) if we assume $N'(\mathbf{b}) \leq 2^{k-2}$ for all \mathbf{b} , and $N'(\mathbf{0}) = 0$, so we assume that one of these is false. It is clear from Lemma 3, with $m = k+1 \leq 5$, and (6.3), that $N(\mathbf{a}) = 0$ for imprimitive \mathbf{a} with $\Delta(\mathbf{a}) \geq 3$. We consider

the possibility $N(\mathbf{a}) > 0$ with $\Delta(\mathbf{a}) = 2$, see (6.8), (6.10). It suffices to show, without at this step using the assumption $B_4 \not\subset f_n$, that one of the first three of (6.10) is soluble, for some $\mathbf{x}, \mathbf{y} \in X_{11}$ and every $u \in \Lambda_k$.

Now the number of possibilities for \mathbf{u} or $\mathbf{u} + \mathbf{x}$, modulo 2, is at least 1 plus the number of rows of $X_{11} = X(f_k)$, and this is $s(f_k) + 1 = s_k(f_n) + 1 > 2^{k-1}$, by (4.4), and $s_k(f_n) \geq 2^{k-1}$. Hence, again using the last inequality, one of these possibilities for \mathbf{u} or $\mathbf{u} + \mathbf{x}$ is also a possibility for \mathbf{y} . So one at least of the first three of (6.10) is soluble as asserted, which completes the proof that $N(\mathbf{a}) > 0$ only for primitive \mathbf{a} .

With this we have $N'(\mathbf{0}) = 0$ and so assume $N'(\mathbf{b}) > 2^{k-2}$ for some $\mathbf{b} \not\equiv \mathbf{0} \pmod{2}$. Now (7.1) will follow if, for this \mathbf{b} , we can find $\mathbf{a} \equiv \mathbf{b} \pmod{2}$ with $N(\mathbf{a}) = N'(\mathbf{b}) > 2^{k-2}$, since for such an \mathbf{a} , primitive as we have proved, we can appeal to (6.5). We have therefore to exclude the possibility that the sum in (6.7) has two or more positive terms, say $N(\mathbf{a}_1)N(\mathbf{a}_2) > 0$, $\mathbf{a}_1, \mathbf{a}_2$ each congruent to $\mathbf{b} \pmod{2}$ and in Λ_{n-k}^+ , and $\mathbf{a}_1 \neq \mathbf{a}_2$: and trivially $\mathbf{a}_1 \neq -\mathbf{a}_2$.

With $\mathbf{a}_1, \mathbf{a}_2$ primitive this makes them linearly independent, so we have (6.11) with $p = 2$. With this, and $B_4 \not\subset f_n$, all three of (6.12) have to be impossible, for $\mathbf{x}, \mathbf{y} \in X_{11}$ and some $\mathbf{u}_1, \mathbf{u}_2$. The argument used for (6.10) shows that this is not so, giving a contradiction which completes the proof.

COROLLARY TO LEMMA 9. *If $A_2 \not\subset f_n$ then $s(f_n) \leq 2^{n-2} + 2$.*

Proof. We note that trivially $A_2 \subset f_n$ (for $\min f_n = 1$) if and only if $s_2(f_n) = 3$; also that $A_2 \subset B_4$, so we may assume $B_4 \not\subset f_n$ and appeal to the lemma. We may suppose $n \geq 5$ by Lemma 4 (i), (ii) and so take $k = 1, 2, 3$.

With $k = 1$ we trivially have $s(f_n) = 1$ or $s_2(f_n) \geq 2$, so we assume $s_2(f_n) = 2$ and take $k = 2$. Then either (7.1) gives $s_3(f_n) \geq 4$, or (7.1) gives $s(f_n) \leq 2^{n-2}$. So we suppose $s_3(f_n) \geq 4$, with equality since otherwise $s_2(f_n) = 3$ by Lemma 4 (i) and (4.11). Now the lemma, with $k = 3$, gives either $s_4(f_n) \geq 7$ or $s(f_n) \leq 2^{n-2} + 2$. So we assume $s_4(f_n) \geq 7$, giving $s_2(f_n) = 3$ by Lemma 4 (ii) and (4.11), and this contradiction completes the proof.

We need a slight improvement on Lemma 9 for $k = 4$.

LEMMA 10. *Let the hypotheses of Lemma 8 hold, with $k = 4$, and suppose that $s_5(f_n) \geq 14$. Then either*

$$(7.3) \quad s_5(f_n) \geq s_4(f_n) + 6$$

or

$$(7.4) \quad s(f_n) \leq 25, 40, 7 + 2^{n-2}$$

for $n = 6, n = 7, n \geq 8$ respectively.

Proof. By (4.11), Lemma 4 (v), and $s_5(f_n) \geq 14$, we have $f_4 \subset f_n$ for an f_4 , with $s(f_4) = s_4(f_n) \geq 9$, such that (4.5)–(4.7) are inconsistent. We use the construction of § 6 with an f_4 satisfying these conditions. And we notice that $s(f_4) = 9$ or 10 , and $s_5(f_n) = 14$ or 15 , since otherwise either (iii) or (vii) of Lemma 4 would give the contradiction $B_4 \subset f_n$.

Just as in Lemma 9 we see that $N(\mathbf{a}) = 0$ for imprimitive \mathbf{a} , and $N'(\mathbf{b})$ is always equal to $N(\mathbf{a})$ for some $\mathbf{a} \equiv \mathbf{b} \pmod{2}$, so we have, see (6.7)

$$(7.5) \quad s(f_n) - s_4(f_n) = \sum N(\mathbf{a}), \quad s_4(f_n) \geq 10,$$

with summation over at most $2^{n-4} - 1$ values of $\mathbf{a} \in A_{n-4}$, all primitive and pairwise incongruent modulo 2. Further, see (6.5), we have (7.3) unless $N(\mathbf{a}) \leq 5$ for every \mathbf{a} , which we therefore assume.

If on the other hand $N(\mathbf{a}) \leq 4$ always, then (7.5) gives (7.4), so we choose \mathbf{a}_1 with $N(\mathbf{a}_1) = 5$. We next choose $\mathbf{a}_2, \mathbf{a}_3$ so that (6.13) holds and $N(\mathbf{a}_2) + N(\mathbf{a}_3) \geq 9$, whence we may suppose $N(\mathbf{a}_2) = 5$, $N(\mathbf{a}_3) = 4$ or 5 . If this is impossible, (7.5) again gives (7.4).

With this choice of $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ we already have (7.4) if $n = 6$, so we suppose $n \geq 7$. We choose $\mathbf{a}_4, \dots, \mathbf{a}_7$ as in Lemma 7, so that $N(\mathbf{a}_4) + \dots + N(\mathbf{a}_7) \geq 16$. If this is not possible, (7.5) again gives (7.4). Each of these $N(\mathbf{a}_i)$ being ≤ 5 , all are positive, and at most one is ≤ 2 .

Now, appealing to Lemma 8, we can renumber the \mathbf{a}_i so that $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ satisfy (6.13), $N(\mathbf{a}_1) \geq 4$, $N(\mathbf{a}_2) \geq 3$, $N(\mathbf{a}_3) \geq 1$, and $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$ is false for all four choices of the signs.

Appealing now to Lemma 7, and using $B_4 \not\subset f_n$, both of (6.15) are impossible, for every $\mathbf{x} \in X(f_4)$, and with $N(\mathbf{a}_i)$ possibilities modulo 2 for each \mathbf{u}_i . Now using only $N(\mathbf{a}_i) \geq 3, 2, 1$ for $i = 1, 2, 3$, we see that there exist $\mathbf{u}, \mathbf{v}, \mathbf{w}$ in A_4 with $\mathbf{0} \not\equiv \mathbf{v} \not\equiv \mathbf{w} \not\equiv \mathbf{0} \pmod{2}$ such that with \mathbf{u}_i satisfying (6.14) we can have $\mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3$ congruent modulo 2 to any one of $\mathbf{u}, \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{w}, \mathbf{u} + \mathbf{v} + \mathbf{w}$. These four vectors, pairwise incongruent, with sum $\mathbf{0}$, modulo 2, are such that none them is congruent modulo 2 to $\mathbf{0}$ or to any $\mathbf{x} \in X(f_4)$, since (6.15) is impossible. That is, taking them to be $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4$, (4.5)–(4.7) are consistent. This contradiction with our choice of f_4 completes the proof.

From Lemmas 9, 10 we deduce

LEMMA 11. *If $n \geq 6$ and (2.6) (for $n \leq 8$) or (2.7) (for $n \geq 9$) is false then either $B_4 \subset f_n$ or $C_5 \subset f_n$.*

Proof. We assume $B_4 \not\subset f_n$. We notice that (7.2), with $s_k(f_n) = s(f_k) \leq 1, 3, 6$ or 12 by (4.10), implies (2.6) or (2.7). So Lemma 9 may be taken to assert that if $s_k(f_n) \geq 2^{k-1}$ then $s_{k+1}(f_n) - s_k(f_n) \geq 2^{k-2} + 1$. Similarly, by the corollary to Lemma 9, we may suppose $A_2 \subset f_n$, $s_2(f_n) = 3$; and if we can appeal to Lemma 10, we need only consider the case (7.3).

Now taking $k = 2, 3, 4$ in Lemma 9 we find $s_{k+1}(f_n) \geq 5, 8, 13$ for $k+1 = 3, 4, 5$. With this, (4.11) and Lemma 4 (iv) give $s_4(f_n) \geq 9$; so Lemma 9 gives $s_5(f_n) \geq 14$. With this, Lemma 10 gives $s_5(f_n) \geq 15$; and so by Lemma 4 (vii) we have either the desired result or $A_5 \subset f_n$. With this however Lemma 4 (vi) gives $s_4(f_n) \geq 10$, and then Lemma 10 gives $s_5(f_n) \geq 16 > s(A_5)$. Now Lemma 4 (vii) clearly gives $B_4 \subset f_n$, so the lemma is proved.

8. The case $B_5 \not\subset f_n$ of Theorem 1. We dispose of this case in two lemmas.

LEMMA 12. *If $n \geq 6$, $B_4 \not\subset f_n$, and (2.6) or (2.7) fails, according as $n \leq 8$ or $n \geq 9$, then $n = 6$ and $f_6 \sim C_6$.*

Proof. By Lemmas 5, 11 we may suppose $n \geq 7$ and $C_5 \subset f_n$. So we use the construction of § 6 with $k = 5$ and $f_5 = C_5$, $X_{11} = X(C_5)$. It is easily seen there exists Y , 5 by 5, $\subseteq X_{11}$, with $\Delta(Y) > 1$, = 2 by (4.2). To avoid verifying this statement by calculation, we may appeal to a result proved in [3] that if, for n by n Y , and perfect φ_n , $Y \subseteq X(\varphi_n)$ implies $\Delta(Y) \leq 1$ then $\varphi_n \sim A_n$.

It follows that (6.8) is impossible for $p \geq 3$. To prove it so for $p = 2$, it suffices, using $B_4 \not\subset f_n$, to verify that one at least of the congruences (6.10) is soluble. We thus have $N(\mathbf{a}) > 0$ only for primitive \mathbf{a} .

We next verify that if all three of the congruences (6.12) are impossible then $\mathbf{u}_1 + \mathbf{u}_2$, and consequently each of $\mathbf{u}_1, \mathbf{u}_2$, are determined uniquely modulo 2. In verifying this statement, we may work with the notation of (1.13), which can be written as $(z_1, \dots, z_5) = (x_1, \dots, x_5)M$, $2 \nmid \det M$. It follows that if the sum on the right of (6.6) has more than one positive term, then $N'(\mathbf{b}) = 2$.

We thus have at most $2^{n-5} - 1$ positive terms on the right of (6.7), each of which, if $\neq 2$, is equal to $N(\mathbf{a})$ for some $\mathbf{a} \equiv \mathbf{b} \pmod{2}$. And Lemma 5 gives us $N(\mathbf{a}) \leq 7$ unless $N(\mathbf{a}) = 12 = s(C_6) - s(C_5)$. Unless there are at least two 12's in the sum, (6.7) gives $s(f_n) \leq s(C_5) + 5 + 7(2^{n-5} - 1)$, from which with $s(C_5) = 15$ and $n \geq 7$ (2.6) or (2.7) follows.

With two 12's in the sum (6.7), we have $N(\mathbf{a}_1) = N(\mathbf{a}_2) = 12$, for $\mathbf{a}_1 \neq \mathbf{a}_2$, $\mathbf{a}_1, \mathbf{a}_2$ primitive and in A_{n-5}^+ , so linearly independent, and incongruent modulo 2.

We seek a contradiction.

We consider forms f_6 of the shape, with z_i as in (1.13),

$$(8.1) \quad \frac{1}{12} \sum_{i=0}^5 (z_i - r_i x_6)^2 + c x_6^2, \quad r_0 + \dots + r_5 = 0.$$

Obviously every $f_6 \supset C_5$ is equivalent to a form of this shape. I assume for the moment that if f_6 , of the shape (8.1), is equivalent to C_6 then $c = \frac{3}{8}$

and $\mathbf{r} = (r_0, \dots, r_5)$ satisfies $\mathbf{r} \equiv \frac{1}{2}\mathbf{u} \equiv -\frac{1}{2}\mathbf{u} \pmod{\Lambda}$, where Λ is the lattice of \mathbf{z} satisfying (1.13) for $\mathbf{x} \in \Lambda_5$, and $\mathbf{u} = (-5, 1, 1, 1, 1, 1)$.

Now we are concerned, see (6.1) with C_5 for f_k , with f_n , $n \geq 7$, such that every substitution $(x_6, \dots, x_n) \rightarrow x_6 \mathbf{a}, \mathbf{a} \in \Lambda'_{n-5}$, takes f_n into an f_6 of the shape (8.1), with $c = \psi(\mathbf{a})$ and a value of \mathbf{r} which we denote by $\mathbf{r}(\mathbf{a})$. And Lemma 5 tells us that this f_6 has $s(f_6) = 12 = s(C_6) - s(C_5)$ if and only if it is equivalent to C_6 , which by the result assumed above gives $\psi(\mathbf{a}) = \frac{3}{8}$ and $\mathbf{r}(\mathbf{a}) \equiv \frac{1}{2}\mathbf{u} \pmod{\Lambda}$. With $\mathbf{a}_1, \mathbf{a}_2$ as above, this gives $\psi(\mathbf{a}_1) = \psi(\mathbf{a}_2) = \frac{3}{8}$, and $\mathbf{r}(\mathbf{a}_1) \equiv \mathbf{r}(\mathbf{a}_2) \equiv \frac{1}{2}\mathbf{u} \pmod{2}$. It follows that for either sign we have $\mathbf{r}(\mathbf{a}_1 \pm \mathbf{a}_2) \equiv \mathbf{0} \pmod{\Lambda}$. So either of the substitutions $(x_6, \dots, x_n) \rightarrow x_6(\mathbf{a}_1 \pm \mathbf{a}_2)$ takes f_n into a form of the shape (8.1) with $\mathbf{r} \in \Lambda$, and $c = \psi(\mathbf{a}_1 \pm \mathbf{a}_2)$. Putting $x_6 = 1$ and $\mathbf{z} = \mathbf{r}$ and so making the sixfold sum zero, we have $\min f_n = 1 \leq \psi(\mathbf{a}_1 \pm \mathbf{a}_2)$ with either sign. Adding, and using (2.10), we have the contradiction $2 \leq 2\psi(\mathbf{a}_1) + 2\psi(\mathbf{a}_2) = \frac{3}{2}$.

It remains only to prove the assertion italicised above. As far as $c = \frac{3}{8}$ is concerned it follows easily from its trivial converse, see (1.11), on comparing determinants. As regards \mathbf{r} , we note that since $2C_6$ is integer-valued it easily follows that all the $r_i \pm r_j$ are integers, and then because of $c = \frac{3}{8}$ that each r_i is congruent to $\frac{1}{2} \pmod{1}$. Reducing modulo Λ , we may suppose each of $2r_1, \dots, 2r_5 = \pm 1$; then $|2r_0| \leq 5$, with equality since (8.1) has to have minimum 1, and now the result is clear.

LEMMA 13. *Theorem 1 is true (for $\min f_n = 1$) if $B_5 \not\subset f_n$.*

Proof. As we have disposed of the case $n \leq 5$, we may by Lemma 12 suppose $n \geq 6$ and $B_4 \subset f_n$. We use the construction of § 6 with $k = 4$ and $f_k = B_4$. So (6.7) takes the shape

$$(8.2) \quad s(f_n) = 12 + \sum \{N'(\mathbf{b}) \mid \mathbf{b} \pmod{2}\}.$$

And (6.1) may be replaced by

$$(8.3) \quad f_n = \frac{1}{2} \sum_{i=1}^4 \left(y_i - \sum_{j=5}^n r_{ij} x_j \right)^2 + \psi(x_5, \dots, x_n),$$

with the y_i as in the case $n = 4$ of (1.4), (1.5). We consider the forms of the shape (5.1), with 5 for n , derivable from (8.3) by $(x_5, \dots, x_n) \rightarrow x_5 \mathbf{a}$, and use the results of § 5.

It is clear, see (5.3), that we must have $\psi(\mathbf{a}) \geq \frac{1}{2}$ always, and that if equality occurs the above-mentioned substitution gives $f_5 \subset f_n$, $f_5 \sim B_5$, which is excluded. So we have $\min \psi > \frac{1}{2}$. This implies obviously $\psi(\mathbf{a}) > 1$, $N(\mathbf{a}) = 0$, if \mathbf{a} is imprimitive, whence in particular there are at most $2^{n-4} - 1$ non-zero terms in (8.2).

We next notice that $N'(\mathbf{b})$ cannot be the sum of two or more non-zero terms, see (6.6). For if $\mathbf{a}_1 \equiv \mathbf{a}_2 \pmod{2}$, then Theorem 4 and $\min \psi > \frac{1}{2}$

give $\psi(\mathbf{a}_1) + \psi(\mathbf{a}_2) > 2$, whence one term is > 1 , unless $\mathbf{a}_1 = \pm \mathbf{a}_2$. So each $N'(\mathbf{b}) = N(\mathbf{a})$, for some $\mathbf{a} \equiv \mathbf{b} \pmod{2}$. Further, we see from § 5 that with $\min \psi > \frac{1}{2}$ we have $N(\mathbf{a}) \leq 4$ always.

With the foregoing, (8.2) implies (2.6) in any case, and (2.7) unless for every $\mathbf{b} \not\equiv \mathbf{0} \pmod{2}$ in Λ_{n-4} there is an $\mathbf{a} \equiv \mathbf{b} \pmod{2}$ with $N(\mathbf{a}) = 4$. So we assume this, and $n \geq 9$.

Looking at cases 1–3 of § 5, we see that $N(\mathbf{a}) = 4$ is possible only in cases 1, 3; and then implies $\psi(\mathbf{a}) \leq 1 - \frac{3}{2}(\frac{1}{2})^2$ in case 1, and $\psi(\mathbf{a}) \leq 1 - \frac{3}{2}\beta^2 - \frac{1}{2}(1 - \beta)^2$, $0 < \beta < \frac{1}{2}$, in case 3. In either case we find $\psi(\mathbf{a}) \leq \frac{5}{8}$.

We now chose any triplet $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$ satisfying (6.13), and $N(\mathbf{a}_i) = 4$, $\psi(\mathbf{a}_i) \leq \frac{5}{8}$, $i = 1, 2, 3$. By choice of the sign, $\psi(\mathbf{a}_1 \pm \mathbf{a}_2) \leq \frac{5}{4}$. So we must have $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$; for otherwise $\mathbf{a}_1 + \mathbf{a}_2 \equiv \mathbf{a}_3 \pmod{2}$, by (6.13), and Theorem 4, with $\min \psi > \frac{1}{2}$, would give

$$2 < \psi(\mathbf{a}_1 \pm \mathbf{a}_2) + \psi(\mathbf{a}_3) \leq \frac{5}{4} + \frac{5}{8} < 2.$$

We now vary the choice of the triplet $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$, as in Lemma 8, and that lemma shows that for some choice of the residue classes of the \mathbf{a}_i modulo 2, $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$ is false, whence some $N(\mathbf{a}_i) < 4$. This gives the result for $n \geq 9$.

COROLLARY TO LEMMA 13. *Theorem 1 is true for $n \leq 6$.*

Proof. Since we have disposed of the case $n \leq 5$, we may by the lemma assume $n = 6$ and $B_5 \subset f_6$. So we take $n = 6$ in § 5. $s(f_6) - s(B_5) = s(f_6) - 20$ may be supposed ≥ 6 , otherwise we have (2.6), and is the number of choices of \mathbf{y} discussed in cases 1–3 of § 5.

This number can be 16 in case 1, but if so we clearly have $f_6 \sim E_6$. In case 3 it can be 10, and if so $f_6 \sim B_6$. It may be 8 in case 1, but this possibility has been dealt with in the proof of Theorem 2. It is ≤ 5 in all other cases.

9. Further construction for the case $B_5 \subset f_n$, $n \geq 7$. For this case we replace (6.1) by

$$(9.1) \quad f_n(\mathbf{x}) = \frac{1}{2} \sum_{i=1}^5 \left(y_i - \sum_{j=6}^n r_{ij} x_j \right)^2 + \psi(x_6, \dots, x_n),$$

with the y_i as in the case $n = 5$ of (1.4) and so

$$(9.2) \quad y_1 + \dots + y_5 \equiv 0 \pmod{2}.$$

We correspondingly modify (6.2) by multiplying each of $X_{11} = X(B_5)$ and X_{21} by the matrix of (1.4). So X_{11} is replaced by a matrix with 20 rows $\pm \mathbf{e}_i + \mathbf{e}_j$, $1 \leq i < j \leq 5$. And for every $\mathbf{a} \in \Lambda_{n-5}^+$ we have just $N(\mathbf{a})$ rows (\mathbf{v}, \mathbf{a}) in the transform of $X(f_n)$, with the $\mathbf{v} = \mathbf{v}(\mathbf{a})$ all in $\Lambda_5^{(2)}$ and pairwise incongruent modulo $2\Lambda_5^{(2)}$.

It is clear from § 5 that $\min f_n = 1$ implies $\min \psi \geq \frac{3}{8}$ and so if \mathbf{a} is imprimitive we have $\psi(\mathbf{a}) > 1, N(\mathbf{a}) = 0$. For any primitive \mathbf{a} , the substitution $(x_6, \dots, x_n) \rightarrow x_6 \mathbf{a}$ takes f_n into a form $f_6 \subset f_n$, which is given by

$$(9.3) \quad f_6 = \frac{1}{2} \sum_{i=1}^5 (y_i - r_i x_6)^2 + \psi(\mathbf{a}) x_6^2, \quad r_i = \sum_{j=5}^n r_{ij} a_j,$$

where $\mathbf{a} = (a_6, \dots, a_n)$ and we write for brevity $\mathbf{r} = (r_1, \dots, r_5) = \mathbf{r}(\mathbf{a})$. And we have $s(f_6) = s(B_5) + N(\mathbf{a}) = 20 + N(\mathbf{a})$.

$N'(\mathbf{b})$ is defined by (6.6), and if it is not equal to one of the terms in the sum on the right we know, see (6.12), that

$$(9.4) \quad N(\mathbf{a}_1) N(\mathbf{a}_2) > 0, \quad \mathbf{a}_1 \equiv \mathbf{a}_2 \pmod{2} \quad \text{and} \quad \mathbf{a}_1 \neq \pm \mathbf{a}_2$$

imply

$$(9.5) \quad \mathbf{v}(\mathbf{a}_1) + \mathbf{v}(\mathbf{a}_2) \not\equiv \mathbf{0} \quad \text{or} \quad \mathbf{e}_i \pm \mathbf{e}_j \pmod{2 A_5^{(2)}},$$

for any pair i, j with $i \neq j$. Using $\min \psi \geq \frac{3}{8}$ and Theorem 4, we see that (9.4) also implies that *either*

$$(9.6) \quad \psi(\mathbf{a}_1) + \psi(\mathbf{a}_2) > \frac{3}{2},$$

or

$$(9.7) \quad \psi(\frac{1}{2} \mathbf{a}_1 + \frac{1}{2} \mathbf{a}_2) = \psi(\frac{1}{2} \mathbf{a}_1 - \frac{1}{2} \mathbf{a}_2) = \min \psi = \frac{3}{8}.$$

If $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$, in A_{n-5} , satisfy (6.12) but $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 \neq \mathbf{0}$ for all four choices of these signs then by Theorem 4, with one of $\mathbf{a}_1 \pm \mathbf{a}_2$ for \mathbf{x} and \mathbf{a}_3 for \mathbf{y} , we have

$$(9.8) \quad \psi(\mathbf{a}_1) + \psi(\mathbf{a}_2) + \psi(\mathbf{a}_3) \geq 4 \min \psi \geq \frac{3}{2},$$

with equality throughout only when $\min \psi = \frac{3}{8}, s(\psi) \geq 2$, and $\psi(\frac{1}{2} \mathbf{a}_1 \pm \frac{1}{2} \mathbf{a}_2 \pm \frac{1}{2} \mathbf{a}_3) = \frac{3}{8}$ for at least two choices of the signs. We have also, see (6.15),

$$(9.9) \quad \mathbf{v}(\mathbf{a}_1) + \mathbf{v}(\mathbf{a}_2) + \mathbf{v}(\mathbf{a}_3) \not\equiv \mathbf{0} \pmod{2 A_5^{(2)}}.$$

It will be convenient to define $\mu(x_6, \dots, x_n)$ as the minimum value of the fivefold sum in (9.1), for integers y_i satisfying (9.2). Then $\min f_n = 1$ implies

$$(9.10) \quad \psi(\mathbf{a}) \geq 1 - \frac{1}{2} \mu(\mathbf{a}) \quad \text{for every } \mathbf{a} \in A'_{n-5},$$

with equality if and only if $N(\mathbf{a}) > 0$.

The possibilities for $N(\mathbf{a})$. These can be written down at once by referring to § 5.

(i) If just $h, 1 \leq h \leq 5$, of the $\|r_i(\mathbf{a})\|$ are $= \frac{1}{2}$, then $N(\mathbf{a}) = 0$ or 2^{h-1} .

(ii) If all the $r_i(\mathbf{a})$ are integers then $N(\mathbf{a}) = 0$ or 1 if the sum of the $r_i(\mathbf{a})$ is even 0, or 10 if the sum is odd.

(iii) If $\beta = \max \|r_i(\mathbf{a})\|$ satisfies $0 < \beta < \frac{1}{2}$, and $\|r_i(\mathbf{a})\| = \beta$ for just h values of i , and $N(\mathbf{a}) \neq 0$, then $N(\mathbf{a}) = 1$ or h according as $|y_i - r_i(\mathbf{a})| = \|r_i(\mathbf{a})\|$ for all i is or is not consistent with (9.2).

We note that $N(\mathbf{a}) = 16$ in case (i) above implies that the $f_6 \subset f_n$ of (9.3) is equivalent to E_6 , while $N(\mathbf{a}) = 10$ in case (ii) gives $f_6 \sim B_6$. Using (9.10), we have inequalities for $\psi(\mathbf{a})$; trivially $\psi(\mathbf{a}) \leq 1$ when $N(\mathbf{a}) \geq 1$ and for $N(\mathbf{a}) \geq 2$ we have, in the three cases above:

- (i) $\psi(\mathbf{a}) = \frac{3}{8}, \leq \frac{1}{2}, \leq \frac{5}{8}, \leq \frac{3}{4}$ for $N(\mathbf{a}) = 16, 8, 4, 2$.
- (ii) $\psi(\mathbf{a}) = \frac{1}{2}$ when $N(\mathbf{a}) = 10$.
- (iii) $\psi(\mathbf{a}) \leq 1 - \frac{1}{2}(h-1)\beta^2 - \frac{1}{2}(1-\beta)^2$ when $N(\mathbf{a}) = h \geq 2$, giving $\psi(\mathbf{a}) \leq \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{3}{4}$ for $N(\mathbf{a}) = 5, 4, 3, 2$.

We now consider $N'(\mathbf{b})$; we need rather more than $N'(\mathbf{b}) \leq N(\mathbf{a}) + 2$ for some $\mathbf{a} \equiv \mathbf{b} \pmod{2}$;

LEMMA 14. *Suppose that $N'(\mathbf{b}) \geq 5$ and that the sum in (6.6) has $\nu \geq 2$ positive terms $N(\mathbf{a}_i)$, $i = 1, \dots, \nu$, the greatest being $N(\mathbf{a}_1)$. Then $\nu \leq 3$, $N(\mathbf{a}_i) = 1$ for $i > 1$, and either $N(\mathbf{a}_1) \leq 5$ or $N(\mathbf{a}_1) = 10$. In the latter case (9.7) holds.*

Proof. We prove all except $\nu \leq 3$ by considering the two possibilities $N(\mathbf{a}_1) \geq 6$, $N(\mathbf{a}_2) \geq 1$ and $N(\mathbf{a}_1) \geq N(\mathbf{a}_2) \geq 2$. In either of these cases, by (i)–(iii) above, the left member of (9.6) is $\leq \frac{3}{2}$ and so (9.7) must hold.

Now the $\|r_i(\frac{1}{2}\mathbf{a}_1 \pm \frac{1}{2}\mathbf{a}_2)\|$ are all $= \frac{1}{2}$, with either sign, so the $r_i(\mathbf{a}_1)$ and the $r_i(\mathbf{a}_2)$ are all integers, with sum even for \mathbf{a}_1 , odd for \mathbf{a}_2 , or vice versa. So one of $N(\mathbf{a}_1)$, $N(\mathbf{a}_2)$ is either 0 or 1, the other either 0 or 10.

When $\nu \geq 4$, we shall obtain a contradiction by permuting the \mathbf{a}_i so that the second of the congruences (9.5) can be satisfied. The modulus of this congruence may be replaced by $2A_5$, since $e_i + e_j$ and $e_i - e_j$ are congruent modulo $2A_5$ but incongruent modulo $2A_5^{(2)}$. So what we need is $v(\mathbf{a}_i) + v(\mathbf{a}_j)$ congruent modulo $2A_5$ to a permutation of $(1, 1, 0, 0, 0)$, for some pair i, j with $1 \leq i < j \leq \nu$.

If this is impossible we see easily that $v(\mathbf{a}_i) + v(\mathbf{a}_j)$ does not take four incongruent values whose sum is congruent to 0, modulo $2A_5$. It follows easily that $v(\mathbf{a}_i)$ does not take 3 different values modulo $2A_5$; and consequently that it does not take 5 different values modulo $2A_5^{(2)}$. So $\nu \leq 4$. But if $\nu = 4$, we use $N'(\mathbf{b}) \geq 5$ and so have two different choices for $v(\mathbf{a}_1)$ modulo $2A_5^{(2)}$, and the argument goes through.

With the foregoing construction, we shall prove step by step that if (2.6) or (2.7) is false then $\min \psi = \frac{3}{8}$, $s(\psi) \geq 2$, $s(\psi) > 2$, and that these imply respectively $E_6, E_7, E_8 \subset f_n$. At the first step the \mathbf{a} with $N(\mathbf{a}) = 10$ are troublesome, and we need:

LEMMA 15. *Let q be the number of $\mathbf{a} \in \Lambda_{n-5}^+$ with $N(\mathbf{a}) = 10$. Then $q \leq n - 5$; and $q \geq k - 5$ implies for $k = 6, 7$ that $B_k \subset f_n$, and for $k = 8$ that either $E_6 \subset f_n$ or $B_6 \subset f_n$.*

Proof. Suppose first that $\mathbf{a}_1, \mathbf{a}_2$ satisfy $N(\mathbf{a}_1) = N(\mathbf{a}_2) = 10$ and are unequal elements of A_{n-5}^+ whence $\mathbf{a}_1 \neq \pm \mathbf{a}_2$. We prove that they are orthogonal when $\psi^{1/2}$ is taken as distance function in $(n-5)$ dimensional space; this will give $q \leq n-5$. Now from (ii) above we see that $\psi(\mathbf{a}_1) = \psi(\mathbf{a}_2) = \frac{1}{2}$ and $\mathbf{r}(\mathbf{a}_1) \equiv \mathbf{r}(\mathbf{a}_2) \equiv (1, 1, 1, 1, 1) \pmod{2A_5^{(2)}}$. For either sign, it follows that $\mathbf{r}(\mathbf{a}_1 \pm \mathbf{a}_2) \equiv \mathbf{0} \pmod{2A_5^{(2)}}$, giving $\mu(\mathbf{a}_1 \pm \mathbf{a}_2) = 0$, obviously, whence $\psi(\mathbf{a}_1 \pm \mathbf{a}_2) \geq 1$ by (9.10). But by the identity (2.10), $\psi(\mathbf{a}_1 + \mathbf{a}_2) + \psi(\mathbf{a}_1 - \mathbf{a}_2) = 2\psi(\mathbf{a}_1) + 2\psi(\mathbf{a}_2) = 2$. So $\psi(\mathbf{a}_1 + \mathbf{a}_2) = \psi(\mathbf{a}_1 - \mathbf{a}_2)$ giving the desired orthogonality.

For the second assertion we suppose without loss of generality that $k = n$ and $q = k-5 \leq 8$. We consider the case $k = 8, q = 3$, since the other cases are similar but simpler. We choose $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$, pairwise orthogonal and with $\psi(\mathbf{a}_i) = \frac{1}{2}, N(\mathbf{a}_i) \equiv 10, \mathbf{r}(\mathbf{a}_i) \equiv (1, 1, 1, 1, 1) \pmod{2A_5^{(2)}}$ for $i = 1, 2, 3$.

With this, if the \mathbf{a}_i are the first three base points of A_3 , we have $B_8 \sim f_n$, since the $y_i - r_{ij}x_j$ and x_6, x_7, x_8 are integers with sum even. If we cannot reduce the general case to this one by transforming x_6, x_7, x_8 , we see that 2ψ must represent the diagonal form $x_6^2 + x_7^2 + x_8^2$ improperly; let the determinant of the transformation taking 2ψ into the diagonal form be $m \geq 2$. Crudely $m = 2$; for if $m \geq 3$ then the determinant of 2ψ , in the usual Gaussian notation, is at most $\frac{1}{9}$, making its minimum $\leq (\frac{2}{9})^{1/3} < \frac{3}{4}$ and contradicting $\min \psi \geq \frac{3}{8}$.

Now obviously we must have

$$(9.11) \quad 2\psi \sim (x_6 - \frac{1}{2}t_1x_8)^2 + (x_7 - \frac{1}{2}t_2x_8)^2 + \frac{1}{4}x_8^2,$$

each t_i 0 or 1. (9.11) clearly implies $\min \psi \leq \frac{3}{8}$; but now equality must hold, and $E_8 \subset f_n$ follows. (For $k = 6, 7, m = 2$ is also impossible).

LEMMA 16. Suppose that $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ satisfy (6.13), $N(\mathbf{a}_1) = 16, N(\mathbf{a}_2)N(\mathbf{a}_3) > 0$, and that none of the four vectors $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3$ is $\mathbf{0}$. Then for some f_m with $m \leq 8$ we have

$$(9.12) \quad f_m \subset f_n, \quad s(f_m) \geq 118.$$

Proof. We appeal to the Corollary to Lemma 7, rewriting (6.15) as

$$(9.13) \quad \mathbf{e}_i \pm \mathbf{e}_j + \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 \equiv \mathbf{0} \pmod{2A_5^{(2)}}.$$

(9.12) will follow on taking $k = 5, s(f_k) = s(B_5) = 20, s' \geq 10$, with the $N(\mathbf{a}_i) \geq 16, 1, 1$, in (6.17), if we can prove that for each of the ten pairs i, j with $1 \leq i < j \leq 5$ one at least of the congruences (9.13) is soluble by choice of the \mathbf{v} . To prove that this is so it suffices to deduce from $N(\mathbf{a}_1) = 16$ that $(\mathbf{v}_1, \mathbf{a}_1)$ is a minimum point of f_n for 16 different \mathbf{v}_1 in $A_5^{(2)}$ that are pairwise incongruent modulo $2A_5$. This is clear since, see § 5, Case 1, the possibilities for \mathbf{v}_1 can be taken to be $\mathbf{0}$ and all permutations of $(1, 1, 0, 0, 0)$ and of $(1, 1, 1, 1, 0)$.

10. The case $E_8 \notin f_n$. With the construction of the last section, we shall in this section show that Theorem 1 follows if we assume $E_8 \notin f_n$, or equivalently $\min \psi > \frac{3}{8}$. (For if $\psi(\mathbf{a}) = \frac{3}{8}$ then (9.10) gives $\mu(\mathbf{a}) \geq \frac{5}{4}$, which by the argument leading to (5.3) is possible (with equality) only if every $\|r_i(\mathbf{a})\| = \frac{1}{2}$, with which see (i) of § 9.)

We choose \mathbf{a}_1 (in A_{n-5}^+), if possible, so that $\psi(\mathbf{a}_1) = \min \psi$ and $N(\mathbf{a}_1) = 8$; if not, we choose \mathbf{a}_1 with $\psi(\mathbf{a}_1) = \min \psi$ and $N(\mathbf{a}_1)$ maximal. Now we rewrite (6.7), with $k = 5$ and $s(f_k) = s(B_5) = 20$, as

$$(10.1) \quad s(f_n) = 20 + N'(\mathbf{a}_1) + \sum \{N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})\},$$

where the sum has $2^{n-6} - 1$ terms, none with $\mathbf{b} \equiv \mathbf{0}$ or $\mathbf{a}_1 \pmod{2}$, no two with $\mathbf{b}_1 + \mathbf{b}_2 \equiv \mathbf{0}$ or $\mathbf{a}_1 \pmod{2}$. We suppose the range of summation so chosen that always

$$(10.2) \quad N'(\mathbf{b}) \geq N'(\mathbf{a}_1 + \mathbf{b}).$$

For each \mathbf{b} , we choose $\mathbf{a}_2 = \mathbf{a}_2(\mathbf{b})$ as the $\mathbf{a} \equiv \mathbf{b} \pmod{2}$ with greatest $N(\mathbf{a})$. Similarly, $\mathbf{a}_3 = \mathbf{a}_3(\mathbf{b})$ is the $\mathbf{a} \equiv \mathbf{a}_1 + \mathbf{b} \pmod{2}$ with maximal $N(\mathbf{a})$. Now from (i)–(iii) of § 9, using Lemma 14, and $\min \psi > \frac{3}{8}$, we have

$$(10.3) \quad N'(\mathbf{b}) \begin{cases} = N(\mathbf{a}_2) = 8 \text{ or } 10 & \text{if } N(\mathbf{a}_2) > 5, \\ \leq \max\{N(\mathbf{a}_2) + 2, 4\} & \text{if } N(\mathbf{a}_2) \leq 5. \end{cases}$$

Clearly (10.3) remains valid if \mathbf{b}, \mathbf{a}_2 are replaced by $\mathbf{a}_1 + \mathbf{b}, \mathbf{a}_3$, or by $\mathbf{a}_1, \mathbf{a}_1$.

In order to deduce (2.6) or (2.7) from (10.1)–(10.3), we need to estimate $N(\mathbf{a}_2) + N(\mathbf{a}_3)$. We note that the triplet $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$ always satisfies (6.13), and we consider two cases.

Case 1. $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 \neq \mathbf{0}$ (for all choices of the signs). Here (9.8) gives, with our choice of \mathbf{a}_1 , $\psi(\mathbf{a}_2) + \psi(\mathbf{a}_3) > \frac{9}{8}$. If we suppose $N'(\mathbf{b}) \leq 7$ then (10.2) gives $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b}) \leq 14$; if not, then (i)–(ii) of § 9 and (10.3) give $\psi(\mathbf{a}_2) \leq \frac{1}{2}$, so $\psi(\mathbf{a}_3) > \frac{5}{8}$ and this gives $N(\mathbf{a}_3) \leq 3$, $N'(\mathbf{a}_1 + \mathbf{b}) \leq 5$. So we have

$$(10.4) \quad N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b}) \leq \begin{cases} 15 & \text{if } N(\mathbf{a}_2) = 10, \\ 14 & \text{otherwise.} \end{cases}$$

Case 2. $\mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}$; say $\mathbf{a}_1 = \mathbf{a}_2 + \mathbf{a}_3$. We investigate the cases in which (10.4) fails; clearly these are given by $N(\mathbf{a}_2) = 10$ with $N(\mathbf{a}_3) = 10, 8, 5, 4$ and $N(\mathbf{a}_2) = 8$ with $N(\mathbf{a}_3) = 8, 5$. These are obviously all impossible unless $\min \psi \leq \frac{1}{2}$. By (9.10) we have

$$(10.5) \quad \psi(\mathbf{a}_1) = \psi(\mathbf{a}_2 + \mathbf{a}_3) \geq 1 - \frac{1}{2}\mu(\mathbf{a}_2 + \mathbf{a}_3),$$

and with $N(\mathbf{a}_3) > 0$, also

$$(10.6) \quad \psi(\mathbf{a}_3) = 1 - \frac{1}{2}\mu(\mathbf{a}_3).$$

(i) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 10, 10$ is impossible. For it gives $\mathbf{r}(\mathbf{a}_2) \equiv \mathbf{r}(\mathbf{a}_3) \equiv \mathbf{u} \pmod{\mathcal{A}_5^{(2)}}$, where $\mathbf{u} = (1, \dots, 1)$. With this, $\mathbf{r}(\mathbf{a}_2 + \mathbf{a}_3) \equiv \mathbf{0}$, $\mu(\mathbf{a}_2 + \mathbf{a}_3) = 0$, and (10.5) gives $\psi(\mathbf{a}_1) \geq 1 > \min \psi$.

(ii) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 10, 5$ is impossible. For it gives, with some $\beta > 0, < \frac{1}{2}$, $\mathbf{r}(\mathbf{a}_3) \equiv (\beta, \beta, \beta, \beta, \beta - 1)$, $\mathbf{r}(\mathbf{a}_2)$ as above, and $\mathbf{r}(\mathbf{a}_2 + \mathbf{a}_3) \equiv \beta \mathbf{u}$, modulo $2\mathcal{A}_5^{(2)}$. With this, $\mu(\mathbf{a}_3) = 4\beta^2 + (1 - \beta)^2 > 5\beta^2 = \mu(\mathbf{a}_2 + \mathbf{a}_3)$, whence (10.5), (10.6) give $\psi(\mathbf{a}_1) > \psi(\mathbf{a}_3) \geq \min \psi$.

(iii) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 8, 8$ is impossible. For with 4 of the $\|r_i(\mathbf{a}_2)\|$ and 4 of the $\|r_i(\mathbf{a}_3)\| = \frac{1}{2}$, 3 of the $\|r_i(\mathbf{a}_2 + \mathbf{a}_3)\|$ are 0. Now obviously $N(\mathbf{a}_1) \neq 8$; on the other hand $\mu(\mathbf{a}_2 + \mathbf{a}_3) \leq 1$ is fairly obvious, so (10.5) gives $\psi(\mathbf{a}_1) = \min \psi \geq \frac{1}{2}$. This implies that \mathbf{a}_1 could have been chosen with $N(\mathbf{a}_1) = 8$, since $N(\mathbf{a}) = 8$ implies $\psi(\mathbf{a}) \leq \frac{1}{2}$.

(iv) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 10, 8$ is possible only if $N(\mathbf{a}_1) = 8$, by the choice of \mathbf{a}_1 , since it makes four of the $\|r_i(\mathbf{a}_1)\| = \frac{1}{2}$.

(v) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 10, 4$ is possible only if $N(\mathbf{a}_1) \leq 4$. In this case we have a contradiction as in (ii) if four of the $\|r_i(\mathbf{a}_3)\|$ have the same value β ; and if three of them are $= \frac{1}{2}$, then so too are the corresponding three of the $\|r_i(\mathbf{a}_2 + \mathbf{a}_3)\|$, giving $N(\mathbf{a}_1) \leq 4$.

(vi) $N(\mathbf{a}_2), N(\mathbf{a}_3) = 8, 5$ is possible only if $N(\mathbf{a}_1) \leq 4$. For we have $\mathbf{r}(\mathbf{a}_2)$ as in (iii), $\mathbf{r}(\mathbf{a}_3)$ as in (ii); then at most one of the $\|r_i(\mathbf{a}_2 + \mathbf{a}_3)\|$ is $\frac{1}{2}$, and at most four are equal.

From the foregoing we see that if $N(\mathbf{a}_1) = 8$ then (10.4) is valid with 18 in place of 15, whence (10.1) gives

$$(10.7) \quad s(f_n) \leq 28 + 14(2^{n-6} - 1) + 4q,$$

with $q \leq n - 5$ as in Lemma 15. If $N(\mathbf{a}_1) \leq 4$, then (10.4) is valid with 16, 15 for 15, 14, and so

$$(10.8) \quad s(f_n) \leq 26 + 15(2^{n-6} - 1) + q.$$

In other cases (10.4) as it stands is valid always, so if $N(\mathbf{a}_1) = 10$ we have

$$(10.9) \quad s(f_n) \leq 30 + 14(2^{n-6} - 1) + q - 1,$$

and if $N(\mathbf{a}_1) \neq 10$, then $N(\mathbf{a}_1) \leq 5$, $N'(\mathbf{a}_1) \leq 7$, and

$$(10.10) \quad s(f_n) \leq 27 + 14(2^{n-6} - 1) + q.$$

Now if $n \geq 10$ we find that any one of (10.7)–(10.10), with $q \leq n - 5$, implies (2.7); so we suppose $n \leq 9$. With this, if $q \geq n - 6$ we have $B_{n-1} \subset f_n$ by Lemma 15, and we may appeal to Lemma 6. So we suppose $q \leq n - 7$; and with this, any of (10.7)–(10.10) gives (2.6) or (2.7). This disposes of the case $E_6 \not\subset f_n$.

11. Preliminaries for the case $E_6 \subset f_n$. We may clearly suppose $n \geq 7$ and

$$(11.1) \quad f_n(x_1, \dots, x_7, 0, \dots, 0) = \frac{1}{2} \sum_{i=1}^5 (y_i - \frac{1}{2}x_6 - r_i x_7)^2 + \psi_2(x_6, x_7),$$

$$(11.2) \quad \psi \supset \psi_2 = \frac{3}{8}x_6^2 + \alpha x_6 x_7 + \beta x_7^2.$$

Here, and throughout this section, the y_i are as in the case $n = 5$ of (1.4), ψ is as in (9.1), and the left member of (11.1) means f_7 if $n = 7$.

LEMMA 17. *If $s(\psi) > 1$ then f_n is equivalent to a form satisfying (11.1), (11.2) and*

$$(11.3) \quad \beta = \frac{3}{8}, \quad r_1 = \dots = r_5 = \frac{1}{2}, \quad \alpha = -\frac{1}{4}.$$

(11.1)–(11.3) imply $E_7 \subset f_n$, $N'(e_6) = N'(e_7) = 16$, and $N'(e_6 + e_7) \geq 11$, with equality if $s(\psi) = 2$, where e_6, e_7, \dots are the base points of Λ_{n-5} .

Proof. $s(\psi) > 1$ implies that $\psi(\mathbf{a}) = \min \psi = \frac{3}{8}$ for some $\mathbf{a} \neq \pm e_6$; plainly we may suppose that ψ_2 has the same property. Now if we take ψ_2 to be a reduced form, we must have $\psi_2(e_7) = \beta = \frac{3}{8}$. Then $\min f_n = 1$ implies (§ 5) that each $\|r_i\|$ is $\frac{1}{2}$; and we may trivially suppose each $r_i = \frac{1}{2}$. Now by choice of \mathbf{y} in $\Lambda_5^{(2)}$ it is possible to make the fivefold sum in (11.1) = $\frac{1}{2}, 0$ for $x_7 = 1$ and $x_6 = 1, -1$. So $\min f_n = 1$ implies $\frac{3}{8} \mp \alpha + \beta \geq \frac{1}{2}, 1$ respectively, whence $\alpha = -\frac{1}{4}$.

Using (11.3), we transform by putting $x_6 + x_7$ for x_7 . It then becomes clear that the form (11.1) is equivalent to E_7 , and so $E_7 \subset f_n$.

By construction, we have $N(e_i) = 16$, whence $N'(e_i) = 16$, by Lemma 14, for $i = 6, 7$; we also have $N(e_6 + e_7) = 10$ and $N(-e_6 + e_7) = 1$. This gives $N'(e_6 + e_7) \geq 11$. If equality does not hold, Lemma 14 shows that $e_6 + e_7$ is expressible in another way as a sum of two minimum points of ψ , whence $s(\psi) > 2$. This completes the proof.

In the case $s(\psi) > 1$, using Lemma 17, we change the notation and replace (11.1), (11.2) by (11.4), (11.5) below, assuming $n \geq 8$ since for $n = 7$ we have $f_7 \sim E_7$ and so have nothing to prove.

$$(11.4) \quad f_n(x_1, \dots, x_8, 0, \dots, 0) = \frac{1}{2} \sum_{i=1}^5 (y_i - \frac{1}{2}x_6 - \frac{1}{2}x_7 - r_i x_8)^2 + \psi_3(x_6, x_7, x_8),$$

$$(11.5) \quad \psi \supset \psi_3 = \frac{3}{8}x_6^2 - \frac{1}{4}x_6 x_7 + \frac{3}{8}x_7^2 + x_8(a'x_6 + a''x_7 + \beta x_8).$$

LEMMA 18. *If $s(\psi) > 2$ then f_n is equivalent to a form satisfying (11.4), (11.5) and*

$$(11.6) \quad \beta = \frac{3}{8}, \quad r_1 = \dots = r_5 = \frac{1}{2}, \quad a' = a'' = -\frac{1}{4}.$$

(11.4)–(11.6) imply $E_8 \subset f_n$, $s(\psi) = 4$,

$$(11.7) \quad N'(\mathbf{a}) = 16 \quad \text{for} \quad \mathbf{a} = e_6, e_7, e_8, e_6 + e_7 + e_8,$$

and

$$(11.8) \quad N'(\mathbf{a}) = 12 \quad \text{for} \quad \mathbf{a} = \mathbf{e}_6 + \mathbf{e}_7, \mathbf{e}_6 + \mathbf{e}_8, \mathbf{e}_7 + \mathbf{e}_8.$$

Proof. $s(\psi) > 2$ implies that there is an $\mathbf{a} \neq \pm \mathbf{e}_6, \pm \mathbf{e}_7$ with $\psi(\mathbf{a}) = \frac{3}{8}$. If we take this \mathbf{a} to be \mathbf{e}_8 , then the argument for (11.6) is like that in Lemma 17 for (11.3). This assumption is legitimate unless some $\psi'_3 \subset \psi$ goes into the ψ_3 of (11.5), (11.6) by a transformation with determinant $m \geq 2$. If so, the determinant of ψ'_3 , in the usual Gaussian notation, can be calculated easily; it is $\frac{1}{32} m^2 \leq \frac{1}{128} < \frac{1}{2} \left(\frac{3}{8}\right)^3$. Using a classical result for the minimum of a positive ternary form, this gives $\min \psi \leq \min \psi'_3 < \frac{3}{8}$, which is impossible.

Assuming (11.4)–(11.6), $E_8 \subset f_n$ becomes clear on putting $x_6 + x_7 + x_8$ for x_8 . For the \mathbf{a} in (11.7) it is easily seen that $N(\mathbf{a}) = 16$, whence $N'(\mathbf{a}) = 16$ by Lemma 14; so we have $s(\psi) \geq 4$. For the \mathbf{a} in (11.8), $N(\mathbf{a}) = 10$ is easily verified, whence $N'(\mathbf{a}) \leq 12$ by Lemma 14. To show that equality holds, we need only consider $\mathbf{a} = \mathbf{e}_6 + \mathbf{e}_7$ and find two other \mathbf{a} , each $\equiv \mathbf{e}_6 + \mathbf{e}_7$ modulo 2, with $N(\mathbf{a}) = 1$; $\mathbf{a} = \mathbf{e}_7 - \mathbf{e}_8, \mathbf{e}_6 + \mathbf{e}_7 + 2\mathbf{e}_8$ does what is wanted.

It remains only to exclude the possibility $s(\psi) > 4$. If this holds there is an \mathbf{a} , linearly independent of those in (11.7), with $\psi(\mathbf{a}) = \frac{3}{8}$. So $n \geq 9$ and ψ represents, properly or improperly, the form

$$(11.9) \quad \frac{3}{8}(x_6^2 + \dots + x_9^2) - \frac{1}{4}(x_6 x_7 + \dots + x_8 x_9).$$

Now we have a contradiction since the form (11.9) is not positive-definite; it vanishes at (1, 1, 1, 1). This completes the proof.

Using Lemmas 17, 18, we modify (10.1) by choosing an \mathbf{a}_1 with $\psi(\mathbf{a}_1) = \frac{3}{8}$, $N'(\mathbf{a}_1) = N(\mathbf{a}_1) = 16$. We further pick out the summands $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})$ that have one term = 16; for $s(\psi) = 1$ there is no such summand, for $s(\psi) = 2$ Lemma 17 shows that there is just one, whose value is 27, and in the remaining case Lemma 18 shows that there are three, each = 28. So we have

$$(11.10) \quad s(f_n) - \sum \{N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})\} = \begin{cases} 36 & \text{if } E_8 \subset f_n, E_7 \not\subset f_n, \\ 63 & \text{if } E_7 \subset f_n, E_8 \not\subset f_n, \\ 120 & \text{if } E_8 \subset f_n \end{cases}$$

for any \mathbf{a}_1 with $N(\mathbf{a}_1) = 16$. Here \mathbf{b} and $\mathbf{a}_1 + \mathbf{b}$ together range over the residue classes of A_{n-5} modulo 2 that are linearly independent modulo 2 of the minimum points of ψ . So the number of summands in the sum on the left of (11.10) is $2^{n-6} - 1, 2^{n-6} - 2, 2^{n-6} - 4$ in the three cases.

Now for \mathbf{b} in the range of summation in (11.10) Lemma 14 gives $N'(\mathbf{b}) \leq 10$; and similarly $N'(\mathbf{a}_1 + \mathbf{b}) \leq 10$. So from (11.10) we find

$$(11.11) \quad s(f_n) \leq \begin{cases} 63 & \text{if } n = 7, \\ 83 & \text{if } n = 8 \text{ and } f_8 \not\sim E_8. \end{cases}$$

We investigate $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})$, when neither of its terms is 0, by choosing $\mathbf{a}_2, \mathbf{a}_3$ so that

$$(11.12) \quad \mathbf{a}_2, \mathbf{a}_3 \equiv \mathbf{b}, \mathbf{a}_1 + \mathbf{b} \pmod{2}, \quad N(\mathbf{a}_2)N(\mathbf{a}_3) \neq 0.$$

The crude inequalities (11.11) enable us to prove that (11.12) implies, for some choice of the signs,

$$(11.13) \quad \mathbf{a}_1 \pm \mathbf{a}_2 \pm \mathbf{a}_3 = \mathbf{0}.$$

To see this, we appeal to Lemma 16, noting that (11.12) implies $\mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 \equiv \mathbf{0} \pmod{2}$. So from (2), (9.12) and (11.11) we have (11.13) or $E_8 \subset f_n$, leaving nothing to prove unless $n \geq 9$. We may assume (11.4)–(11.6). Now \mathbf{b} is restricted in (11.10) to have its last $n-8$ elements not all even. Using this we see that Lemma 16 and the negation of (11.13) imply a representation of E_8 by f_n which does not coincide with the obvious one got by taking $x_9 = \dots = x_n = 0$. So one of the possibilities for \mathbf{a} with $\psi(\mathbf{a}) = \frac{3}{8}$ implied by this non-obvious representation of E_8 contradicts Lemma 18 by giving $s(\psi) > 4$. This completes the proof that (11.12) implies (11.13), for the \mathbf{b} of (11.10), and for any choice of \mathbf{a}_1 with $N(\mathbf{a}_1) = 16$.

12. Proof of Theorem 1 for $E_8 \not\subset f_n$ and for $n \geq 10$. We investigate the possibility of choosing $\mathbf{a}_2, \mathbf{a}_3$ so that

$$(12.1) \quad N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b}) = N(\mathbf{a}_2) + N(\mathbf{a}_3), \quad \mathbf{a}_2, \mathbf{a}_3 \equiv \mathbf{b}, \mathbf{a}_1 + \mathbf{b} \pmod{2}$$

and prove:

LEMMA 19. *Let \mathbf{a}_1 satisfy $N(\mathbf{a}_1) = 16$, restrict \mathbf{b} as in (11.10), and suppose without loss of generality that $N'(\mathbf{b}) \geq N'(\mathbf{a}_1 + \mathbf{b})$. Then:*

(i) (12.1) is impossible only if $N'(\mathbf{b}) = 8$ and $N'(\mathbf{a}_1 + \mathbf{b}) = 2$; and conversely:

(ii) $N(\mathbf{b}) = 8$, implying by Lemma 14 that $N(\mathbf{a}_2) = 8$ for some $\mathbf{a}_2 \equiv \mathbf{b} \pmod{2}$, implies that (12.1) is impossible; and

(iii) if $N'(\mathbf{a}_1 + \mathbf{b})N(\mathbf{a}_3) > 0$ for some $\mathbf{a}_3 \equiv \mathbf{a}_1 + \mathbf{b} \pmod{2}$, then $N'(\mathbf{b}) = 8$ and (12.1) is impossible.

Proof. Choosing one of $\mathbf{a}_2, \mathbf{a}_3$ to be $\mathbf{a}_1 + \mathbf{a}_3$ or $\mathbf{a}_2 + \mathbf{a}_3$ if one of $N'(\mathbf{b}), N'(\mathbf{a}_1 + \mathbf{b}) = 0$, and using (11.13) if not, we see that \mathbf{a}_1 and the $\mathbf{a}_2, \mathbf{a}_3 \equiv \mathbf{b}, \mathbf{a}_1 + \mathbf{b}$ that we need to consider all lie in a sublattice of Λ_{n-8} of dimension 2. So it suffices to prove the lemma for $n = 7$. Using the notation of (11.1), (11.2) we may take $\mathbf{a}_1 = (1, 0)$ and suppose $\psi = \psi_2$ to be a reduced form, with second minimum = β , $\beta > \frac{5}{8}$ because of the restriction on \mathbf{b} in (11.10). So we may suppose

$$(12.2) \quad |\alpha| \leq \frac{5}{8} < \beta,$$

and trivially,

$$(12.3) \quad \|r_i\| \leq \|r_j\| \quad \text{for} \quad 1 \leq i < j \leq 5.$$

From (12.2) we see that for $\mathbf{a} \in A_2^+$ we can have $N(\mathbf{a}) \geq 1$, implying $\psi(\mathbf{a}) \leq 1$, only for $\mathbf{a} = (1, 0), (0, 1), (\pm 1, 1)$, so

$$(12.4) \quad N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b}) = N(0, 1) + N(1, 1) + N(-1, 1).$$

Hence (12.1) is impossible if and only if $N(1, 1)N(-1, 1) > 0$. We write for brevity

$$(12.5) \quad \mathbf{r} = (r_1, \dots, r_5), \quad \mathbf{u} = (1, \dots, 1),$$

whence, see (9.10), the three vectors $\mathbf{r}, \mathbf{r} \pm \frac{1}{2}\mathbf{u}$ have to satisfy certain inequalities (involving α, β) to make $\min f_7 = 1$ and in these inequalities the sign of equality is needed to make $N(0, 1)$ or $N(\pm 1, 1)$ positive.

More precisely, the $\mu(\mathbf{a})$ of (9.10), for $\mathbf{a} = (\pm 1, 1)$, is readily seen, using (12.3), to be

$$\left(\frac{1}{2} \pm \|r_1\|\right)^2 + \left(\frac{1}{2} - \|r_2\|\right)^2 + \dots + \left(\frac{1}{2} - \|r_5\|\right)^2,$$

with $+$ in one case and $-$ in the other. So adding these two cases of (9.10) we see that

$$(12.6) \quad 2\beta \geq \|r_2\| + \dots + \|r_5\| - \sum_{i=1}^5 \|r_i\|^2,$$

with equality if and only if $N(1, 1)N(-1, 1) > 0$. Taking $\mathbf{a} = (0, 1)$, we similarly find that one of

$$(12.7) \quad 2\beta \geq 2 - \|r_1\|^2 - \dots - \|r_4\|^2 - (\varepsilon - \|r_5\|)^2,$$

$\varepsilon = 0$ or 1 , must hold, with equality if and only if $N(0, 1) > 0$.

To prove (i) we assume equality in (12.6); then, using (12.3) and the trivial $\|r_i\| \leq \frac{1}{2}$, we find that

$$(12.8) \quad \|r_2\| = \dots = \|r_5\| = \frac{1}{2}$$

and that equality holds also in (12.7). With this we see, referring to § 5, cases 1-3, that $N(0, 1) = 8$ or 16 , according as $\|r_1\| < \text{or} = \frac{1}{2}$; the restriction on \mathbf{b} , or equivalently $\beta > \frac{3}{8}$, excludes the latter case, so $N(0, 1) = 8$, giving $N'(\mathbf{b}) = 8$ by Lemma 14. Further, (12.8) clearly implies that each of $N(\pm 1, 1)$ is ≤ 1 , so each, being positive, is 1 and (i) is proved.

To prove (ii), we may assume (12.8), with $\|r_1\| < \frac{1}{2}$, and equality in (12.7). Then equality holds also in (12.6). For (iii), we have only to note that equality in (12.6) is inconsistent with strict inequality in (12.7), as we have seen. This completes the proof. We also need to investigate the case in which (12.1) can be satisfied.

LEMMA 20. If $N(\mathbf{a}_1) = 16$, \mathbf{b} is as in (11.10), (12.1) holds, and $N'(\mathbf{b}) = N'(\mathbf{a}_1 + \mathbf{b})$, then we have one of

$$(12.9) \quad N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b}) \leq 6,$$

$$(12.10) \quad N'(\mathbf{b}) = N(\mathbf{a}_2) = 10 \quad \text{and} \quad N'(\mathbf{a}_1 + \mathbf{b}) = 0,$$

$$(12.11) \quad N(\mathbf{a}_2) = N(\mathbf{a}_3) = 5.$$

Proof. As in the proof of Lemma 19, we see that it suffices to suppose $n = 7$ and use the notation of (11.1), (11.2), $N(1, 1)N(-1, 1) = 0$, whence by choosing the sign of α we may suppose $N(-1, 1) = 0$. We investigate the possibilities for $N(\mathbf{a}_2)$, $N(\mathbf{a}_3)$ by considering, with the notation (12.5), the vectors $\mathbf{r}, \mathbf{r} + \frac{1}{2}\mathbf{u}$.

If all the elements of \mathbf{r} are integers, then all those of $\mathbf{r} + \frac{1}{2}\mathbf{u}$ are congruent to $\frac{1}{2}$ modulo 1 and we see (§ 5) that $N(0, 1) = 0, 1$, or 10 and $N(1, 1) = 0$ or 16, $= 0$ because of the restriction on \mathbf{b} ; so we have (12.9) or (12.10); and similarly if all the elements of \mathbf{r} are $\equiv \frac{1}{2} \pmod{1}$.

If exactly four of the $\|r_i\|$ are 0, or $\frac{1}{2}$, then Lemma 19 shows that (12.1) is possible only with $N'(\mathbf{b}) = N'(\mathbf{a}_1 + \mathbf{b}) = 0$.

Excluding these cases, let h be the number of maximal $\|r_i\|$, and h' the number of minimal $\|r_i\|$; then h' is also the number of maximal $\|r_i + \frac{1}{2}\|$. And, see again § 5, we have $N(0, 1) \leq h$ if $h \neq 3, 4$ if $h = 3$, and $N(1, 1) \leq h'$ if $h' = 3, 4$ if $h' = 3$. These inequalities, with (12.1), give (12.9) if $h + h' \leq 5$. So we assume $h + h' \geq 6$, implying obviously $h = h' = 5$.

Now however each of $N(0, 1)$, $N(1, 1)$ is 0, 1 or 5, so we have either (12.9) or (12.11), and the proof is complete.

Proof of Theorem 1 for $f_n \supset E_7$. By the first case of (11.10), with $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})$ always ≤ 10 by Lemmas 19, 20, we have for $n \geq 9$

$$s(f_n) \leq 36 + 10(2^{n-6} - 1) = 26 + 5 \cdot 2^{n-5} < 2^{n-2},$$

giving (2.7) with a good deal to spare. For $n = 8$ we have $s(f_8) \leq 66$, giving (2.6). For $n = 7$, with just one summand $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})$, either = 10 or ≤ 6 , we have either $s(f_7) \leq 42$ or $s(f_7) = 46$, which is just what we need. Since $f_7 \sim E_7$ is excluded in Theorem 1, we suppose henceforth $n \geq 8$.

Proof of Theorem 1 for $f_n \supset E_7, \not\supset E_8, n \geq 9$. By the second case of (11.10), with $2^{n-6} - 2$ summands each ≤ 10 as above, we have

$$s(f_n) \leq 63 + 10(2^{n-6} - 2) = 43 + 5 \cdot 2^{n-5} < 2^{n-2},$$

again giving (2.7) with much to spare.

Proof of Theorem 1 for $f_n \supset E_8, n \geq 10$. By the third case of (11.10) we find as above that

$$s(f_n) \leq 120 + 10(2^{n-6} - 4) = 80 + 5 \cdot 2^{n-5} < 2^{n-2},$$

again giving (2.7) with much to spare.

Proof of Theorem 1 for $n = 8$, $f_8 \supset E_7$. Since $f_8 \sim E_8$ is excluded, we are concerned with the second case of (11.10), with just two summands in the sum on the left. Using the notation of (11.4), (11.5), with $n = 8$, and noting that $N(\mathbf{e}_6) = N(\mathbf{e}_7) = 16$, we may rewrite (11.10) more explicitly as

$$(12.12) \quad s(f_8) - 63 = N'(\mathbf{e}_8) + N'(\mathbf{e}_6 + \mathbf{e}_8) + N'(\mathbf{e}_7 + \mathbf{e}_8) + N'(\mathbf{e}_6 + \mathbf{e}_7 + \mathbf{e}_8).$$

The right member of (12.12) can be broken up into two sums $N'(\mathbf{b}) + N'(\mathbf{a}_1 + \mathbf{b})$ in two different ways, with $\mathbf{a}_1 = \mathbf{e}_6, \mathbf{e}_7$. We first show that (12.1) holds in either case, for each of the two sums of two terms.

Assuming the contrary, Lemma 19 shows that $N(\mathbf{a}) = 8$ for some $\mathbf{a} = (a_6, a_7, a_8)$ with $a_8 \geq 1$, odd. The possibility $a_8 \geq 3$ is easily excluded by the argument used at the beginning of the proof of Lemma 18. So we may suppose $N(\mathbf{e}_8) = 8$. Now by Lemma 19, with $\mathbf{a}_1 = \mathbf{e}_6, \mathbf{e}_7$, we must have $N'(\mathbf{e}_6 + \mathbf{e}_8) = N'(\mathbf{e}_7 + \mathbf{e}_8) = 2$, with each of $N(\pm \mathbf{e}_6 + \mathbf{e}_8)$, $N(\pm \mathbf{e}_7 + \mathbf{e}_8) = 1$. Now (12.12) gives the desired result $s(f_8) \leq 75$ (with equality), unless the fourth term on the right is positive, and if so we see from (11.4) and § 5, with four of the $\|r_i\| = \frac{1}{2}$ because of $N(\mathbf{e}_8) = 8$, that this fourth term = 8. So we have $\mathbf{a} \equiv \mathbf{e}_6 + \mathbf{e}_7 + \mathbf{e}_8 \pmod{2}$, with $N(\mathbf{a}) = 8$.

By the argument leading to $N(\mathbf{e}_8) = 8$, we may take this \mathbf{a} to be $\lambda_6 \mathbf{e}_6 + \lambda_7 \mathbf{e}_7 + \mathbf{e}_8$, with $\lambda_6 \lambda_7$ odd. There are just four values of \mathbf{a} in A_3^+ with $N(\mathbf{a}) = 1$. These have been found above, and by the same argument they must also be $(\lambda_6 \pm 1) \mathbf{e}_6 + \lambda_7 \mathbf{e}_7 + \mathbf{e}_8$ and $\lambda_6 \mathbf{e}_6 + (\lambda_7 \pm 1) \mathbf{e}_7 + \mathbf{e}_8$. However we choose λ_6, λ_7 this gives a contradiction.

Now with (12.1) always applicable, we may rewrite (12.12) as

$$(12.13) \quad s(f_8) - 63 = N(\mathbf{b}_0) + N(\mathbf{b}_1) + N(\mathbf{b}_2) + N(\mathbf{b}_3),$$

with $\mathbf{b}_0, \dots, \mathbf{b}_3 \equiv \mathbf{e}_8, \dots, \mathbf{e}_6 + \mathbf{e}_7 + \mathbf{e}_8 \pmod{2}$. Again pairing the terms in two different ways, but now using Lemma 20, we see that one term in each pair must have sum 10, since otherwise $s(f_8) \leq 63 + 6 + 6 = 75$ would follow. If one of the four terms on the right of (12.13) is 10, then using also $N(\mathbf{e}_6 + \mathbf{e}_7) = 10$, see (11.4), we see that $q \geq 2$ in the notation of Lemma 15, whence by that lemma we have $B_7 \subset f_8$, and we appeal to Lemma 6. Lemma 20 shows, excluding this case, that if Theorem 1 fails three of the terms on the right of (12.13) must be equal to 5. We may clearly suppose $N(\mathbf{e}_8) = N(\mathbf{e}_8 \pm \mathbf{e}_6) = N(\mathbf{e}_8 \pm \mathbf{e}_7) = 5$.

We now see that all the $\|r_i\|$ in (11.4) are equal. With this, we can have (11.4), (11.5) with each $r_i = \gamma$, for some γ with $0 \leq \gamma \leq 1$. (For this, we make suitable changes of sign of the variables y_i, x_j , and then replace \mathbf{y} by $\mathbf{y} + x_6 \mathbf{u}_6 + x_7 \mathbf{u}_7 + x_8 \mathbf{u}_8$, with suitable $\mathbf{u}_i \in A_5^{(2)}$.) $N(\mathbf{e}_8) = 5$ now requires $\frac{1}{2} < \gamma < 1$ and $\beta = 1 - 2(1 - \gamma)^2 - \frac{1}{2}\gamma^2$. With this, $N(\mathbf{e}_8 - \mathbf{e}_i) = 5$, $i = 6$ or 7 , is impossible, and $N(\mathbf{e}_8 + \mathbf{e}_6) = N(\mathbf{e}_8 + \mathbf{e}_7) = 5$

gives $\alpha' = \alpha''$ and determines the value of $\frac{3}{8} + \alpha' + \beta$. With a little calculation we find $\alpha' = \alpha'' = \frac{1}{2}\gamma$.

Now we have a contradiction, for we find that at the point $(\mathbf{y}, 1, 1, 1)$ with $\mathbf{y} = (2, \dots, 2)$ f_8 takes the value $2 - 2\gamma < 1$.

13. Completion of proof of Theorem 1. It seems hopelessly difficult to sharpen the arguments of the last section sufficiently to prove the one remaining case $n = 9$, $E_8 \subset f_8$. Instead, we write

$$(13.1) \quad f_8 = f_8(\mathbf{x}, x_8) = E_8(\mathbf{x} - x_8 \mathbf{r}) + cx_8^2, \quad \mathbf{x} = (x_1, \dots, x_8),$$

with a constant c and an $\mathbf{r} = (r_1, \dots, r_8)$ to be determined. We may suppose without loss of generality that

$$(13.2) \quad E_8(\mathbf{x} - \mathbf{r}) \geq E_8(\mathbf{r}) \quad \text{for all } \mathbf{x} \in X(E_8).$$

We shall deduce from (13.2) that

$$(13.3) \quad E_8(\mathbf{r}) \leq \frac{1}{2}, \quad \text{whence} \quad c \geq \frac{1}{2},$$

since $\min f_8 = 1$ clearly implies $E_8(\mathbf{r}) + c \geq 1$. We shall also show that

$$(13.4) \quad \mathbf{x} \in \Lambda_8 \text{ and } E_8(\mathbf{x}) = 2 \quad \text{imply} \quad \mathbf{x} = \mathbf{y} + \mathbf{z}, \quad \mathbf{y}, \mathbf{z} \in X(E_8).$$

From (13.2) and (13.3) we shall deduce that

$$(13.5) \quad E_8(\mathbf{x} - \mathbf{r}) \geq E_8(\mathbf{r}) \quad \text{for all } \mathbf{x} \in \Lambda_8.$$

We notice that if $\mathbf{x} \in X(E_8)$ then we may reflect Λ_8 in the hyperplane through $\frac{1}{2}\mathbf{x}$ perpendicular to \mathbf{x} . We thereby obtain an automorph of E_8 which is easily to be an integral one, i.e. to take Λ_8 into itself, since E_8 is integer-valued; and to interchange \mathbf{y}, \mathbf{z} if \mathbf{y}, \mathbf{z} in Λ_8 satisfy $E_8(\mathbf{y}) = E_8(\mathbf{z})$ and $\mathbf{y} - \mathbf{z} = \pm \mathbf{x}$. This will shorten the arguments.

We shall also show that without loss of generality we may assume that

$$(13.6) \quad \mathbf{r} \text{ is determined uniquely by the cases of equality in (13.2)}$$

and

$$(13.7) \quad c = 1 - E_8(\mathbf{r}).$$

Assumptions (13.6), (13.7) are justified if (13.3) holds.

For if so, we obviously have $f_8(\mathbf{x}, x_8) > 1$ if $x_8 > 1$, and $f_8(\mathbf{x}, 1) > 1$ unless (13.5) fails, or holds with equality; here we use the obvious $c \geq 1 - E_8(\mathbf{r})$. Now using the triangle inequality we have $f_8(\mathbf{x}, 1) > 1$ unless

$$E_8^{1/2}(\mathbf{x}) \leq E_8^{1/2}(\mathbf{x} - \mathbf{r}) + E_8^{1/2}(\mathbf{r}) \leq 2E_8^{1/2}(\mathbf{r}) \leq 2^{1/2},$$

giving $E_8(\mathbf{x}) \leq 2$. Thus we see that (13.3) implies that $\min f_8 = 1$, and that $s(f_8) - s(E_8) = s(f_8) - 120$ is equal to the number of cases of equality

in (13.5) if (13.7) holds, but is 0 if $c > 1 - E_8(\mathbf{r})$. As we have nothing to prove in the latter case, we may assume (13.7).

We may moreover, by Lemma 1, assume that f_8 is perfect, since we are only interested in the maximum value of $s(f_8)$. By the definition of perfection, and the perfection of E_8 , f_8 can be perfect only if the (\mathbf{x}, x_8) with $x_8 > 0$ and $f_8(\mathbf{x}, x_8) = 1$ determine the coefficients of f_8 uniquely; and these \mathbf{x} are as we have seen just those for which equality holds in (13.5) with $E_8(\mathbf{x}) = 1$ or 2. So assumption (13.6) would be justified if in it we read (13.5) for (13.2). To justify (13.6) as it stands, we note that the cases of equality in (13.5) with $E_8(\mathbf{x}) = 2$ are trivial consequences, by (13.4), of cases of equality in (13.2).

Assumptions (13.6), (13.7) are justified if they imply (13.3).

This is trivial as far as (13.7) is concerned. To prove it for (13.6), note that (13.2) is a system of linear inequalities in r_1, \dots, r_8 , satisfied if and only if \mathbf{r} lies in a certain convex polytope; and the points of this polytope that are farthest from the origin are its vertices. So (13.3) is true if it is implied by (13.6).

It now suffices to assume (13.1), (13.2), (13.6), and (13.7) and prove (13.3), (13.4) and either $f_8 \sim E_8$ or $s(f_8) < 136$. To do this it is best to change the notation. We write, cf (1.8),

$$(13.8) \quad f_8 = \frac{1}{8} \sum_{i=1}^8 (w_i - t_i x_8)^2 + c x_8^2,$$

where $w_i = x_8 - 2y_i$ for $i = 1, \dots, 7$ and $w_8 = x_8$, whence \mathbf{w} ranges over the sub-lattice of A_8 defined by

$$(13.9) \quad w_1 \equiv \dots \equiv w_8 \pmod{2}, \quad w_1 + \dots + w_8 \equiv 0 \pmod{4}.$$

The minimum points of E_8 , in the \mathbf{w} -notation, are the permutations of

$$(13.10) \quad (\pm 2, \pm 2, 0, \dots, 0) \quad \text{and} \quad (\pm 1, \dots, \pm 1),$$

with evenly many + signs in the latter case; and so the inequalities (13.2) become

$$(13.11) \quad \pm t_i \pm t_j \leq 2, \quad i \leq 1 < j \leq 8,$$

$$(13.12) \quad \pm t_1 \pm \dots \pm t_8 \leq 4.$$

It is easy to write down the points where $E_8 = 2$, in terms of \mathbf{w} , and verify (13.4). It is easily seen, using the reflections mentioned above, that the group of automorphisms of E_8 is transitive on the $112 + 128$ points (13.10). Now to determine the t_i we need at least 8 cases of equality in (13.11), (13.12); for brevity we call these cases equations (13.11), or (13.12). And we may clearly suppose that we have at least 4 irredundant

equations (13.11). Further, we note that the lattice (13.9) is unaltered by permuting the w_i , or changing the signs of any two of them, so we may suppose

$$(13.13) \quad t_1 \geq t_2 \geq \dots \geq t_7 \geq |t_8|.$$

If among the four, or more, equations (13.11) there are two with the same i, j , we may clearly, by (13.13), suppose these two to be $t_1 \pm t_2 = 2$, giving $t_1 = 2, t_2 = \dots = t_8 = 0$. Changing the origin of t and looking at (1.8), this is easily seen to give $f_8 \sim E_8$, and $c = E_8(\mathbf{r}) = \frac{1}{8} \sum t_i^2 = \frac{1}{2}$.

If $t_1 = t_2$, then the equations (13.11) will give $t_1 = \dots = t_4 = 1$, whence (13.12) is easily seen to imply that the other t_i all vanish. Since the point $(2, 2, 2, 2, 0, \dots, 0)$ is easily seen to go into $(3, 1, 1, 1, 1, 1, 1, -1)$ and this into $(4, 0, \dots, 0)$, by reflections, we see from the preceding paragraph that in this case we again have $c = \frac{1}{2}, f_8 \sim E_8$.

There remains only the case in which the equations (13.11) are equivalent to $t_1 = 2 - \theta, t_2 = \dots = t_h = \theta, 0 < \theta < 1, h \geq 5$. Then the first five \pm signs in any equation (13.12) must all be $+$. So if we subtract one of these equations from each of the others, we obtain a system of equations $t_i \pm t_j = 0, h < i < j$, which must clearly suffice to determine all the t_i with $i > h$. It follows easily that all these t_i are zero. Then any one equation (13.12) gives $2 + (h-2)\theta = 4, \theta = 2/(h-2)$.

The case $h = 6$ may be excluded since in it the equations (13.12) give $t_7 + t_8 = 0$ but not $t_7 - t_8 = 0$; also $h = 7$, since it gives only one equation (13.12), from which $t_8 = 0$ does not follow. With $h = 5$ or 8 we find $c > \frac{1}{2}$. This excludes any possibility of equality in (13.5) except with $E_8(\mathbf{x}) = 1$; and we find $s(f_8) = 129$ by verifying that there are just 8 cases of equality in (13.11) and (13.12), hence in (13.2), and noting the trivial case $\mathbf{x} = \mathbf{0}$ of (13.5). This completes the proof of Theorem 1.

14. Conclusion. I note that (2.7) can be considerably improved for $n \geq 10$ if $E_8 \subset f_n$ is assumed; and this can be done very easily, because with $f_k = E_8$ in (6.1) we must by (13.3) have $\min \psi \geq \frac{1}{2}$. In particular, $E_8 \subset f_{10}$ implies $s(f_{10}) \leq 168$, and equality is possible. But at earlier stages of the argument, that is, without the assumption $E_8 \subset f_{10}$, it seems very difficult to do much better than (2.7), that is, $s(f_7) < 264$.

I note also that, by the Corollary to Lemma 9, if $\min f_n = 1$ and $A_2 \not\subset f_n$, then for $n \leq 6$ we have $s(f_n) < \frac{1}{2} n(n+1)$ and so f_n is not perfect, *a fortiori* not extreme, nor absolutely extreme. Consequently, for $n \leq 6$, in investigating the minimum of the determinant of f_n for $\min f_n = 1$, one may assume $A_2 \subset f_n$. This would simplify the argument of Blichfeldt [2] by getting rid of two parameters; it is equivalent to assuming the

intuitively obvious, but probably false, result that in a densest possible lattice packing of equal spheres, each sphere must touch two others that touch each other.

This simplification of [2] is possible also for $n = 7$. More precisely, suppose $\min f_7 = 1$ and $A_2 \not\subset f_7$; then in a paper under preparation I have proved that $s(f_7) \leq 28$, and if equality holds, as it must if f_7 is perfect, then there is just one possibility for f_7 up to equivalence. For this possibility see [8]; it is perfect, and extreme, but not absolutely extreme.

References

- [1] E. S. Barnes, *The complete enumeration of extreme senary forms*, Philos. Trans. Roy. Soc. London, Ser. A, 249 (1957), pp. 461–506.
- [2] H. F. Blichfeldt, *The minimum values of positive quadratic forms in six, seven and eight variables*, Math. Zeitschr. 39 (1935), pp. 1–15.
- [3] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. 11 (1877), pp. 242–292.
- [4] R. A. Rankin, *The closest packing of spherical caps in n dimensions*, Proc. Glasgow Math. Assoc. 2 (1955), pp. 139–144.
- [5] P. R. Scott, *On perfect and extreme forms*, J. Aust. Math. Soc. 4 (1964), pp. 56–77.
- [6] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. 133 (1908), pp. 97–178.
- [7] G. L. Watson, *On the minimal points of perfect septenary quadratic forms*, Mathematika 16 (1969), pp. 170–177.
- [8] — *The least common denominator of the coefficients of a perfect quadratic form*, Acta Arith. 18 (1971), pp. 29–36.

UNIVERSITY COLLEGE, London
