ACTA ARITHMETICA
V (1959)

The construction of perfect and extreme forms II

by

E. S. Barnes (Sydney)

1. Introduction. This article continues the work of Part I, (Acta Arithmetica, this volume, p. 57-79) and describes another general method of constructing perfect and extreme forms, by "extending" a known form. Although this method is independent of that given in Part I, the reader is referred to that article for the basic definitions and notations, and for a description of some general classes of forms.

If

$$f(\boldsymbol{x}) = \sum_{1}^{n} a_{ij}x_i x_j \qquad (a_{ij} = a_{ji})$$

is positive definite, with determinant D, and minimum M for integral $\boldsymbol{x} \neq \boldsymbol{O}$, we shall call $g(x_1, \ldots, x_n, x_{n+1}) = g(\boldsymbol{x}, x_{n+1})$ an *extension* of f, and f a *section* of g, if

$$f(\boldsymbol{x}) = g(\boldsymbol{x}, 0).$$

Starting with a perfect form f, we attempt to find an extension g which shall be perfect, with minimum M. That such an extension always exists is proved in Lemma 2.1.

A method of this type has been used by Chaundy [4], who attempted to find an absolutely extreme form in $n+1$ variables by extending an absolutely extreme form in n variables. Since, as we shall show, a perfect extension of an extreme form need not even be extreme, we shall adopt a less restricted approach, and give in Theorem 2.1 a criterion which ensures merely that the extension g is perfect whenever f is.

Our construction, which is based on Voronoi's concept of the "polyhedron of points nearest the origin", normally yields large numbers of perfect extensions of a given f; an independent test is then necessary to determine which of these are extreme.

As in Part I, we set

$$\Delta = \Delta(f) = \left(\frac{2}{M}\right)^n D, \qquad \Delta_n = \min_f \Delta(f),$$

so that $\Delta(f) = \Delta_n$ when f is an absolutely extreme form in n variables. Mordell [9] proved the inequality

$$\Delta_n \geqslant (\tfrac{1}{2}\Delta_{n-1})^{n/(n-2)}, \tag{1.1}$$

which is known to be precise for $n = 4$ and $n = 8$. Published results give

$$\begin{gathered}\Delta_1 = 2,\ \Delta_2 = 3,\ \Delta_3 = 4,\ \Delta_4 = 4,\ \Delta_5 = 4,\ \Delta_6 = 3,\\ \Delta_7 = 2,\ \Delta_8 = 1,\ \Delta_9 \leqslant 1,\ \Delta_{10} \leqslant \tfrac{3}{4},\ \Delta_{12} \leqslant (\tfrac{3}{4})^6;\end{gathered} \tag{1.2}$$

the inequalities for Δ_9, Δ_{10} arising from the extreme forms Φ_9, Φ_{10} of Chaundy [4], and that for Δ_{12} from the form K_{12} of Coxeter and Todd [6]. We shall exhibit in § 5 an 11-variable form, K_{11}, with $\Delta(K_{11}) = 3^5/2^9$, which establishes the new inequality

$$\Delta_{11} \leqslant \frac{3^5}{2^9}. \tag{1.3}$$

It is of interest to observe that Mordell's inequality (1.1) for $n = 12$ would hold with equality if these bounds were precise.

An inequality in the opposite direction to (1.1),

$$\Delta_n \leqslant \frac{n+1}{n}\,\Delta_{n-1}, \tag{1.4}$$

will be established in § 3 (the inequality $\Delta_n < 2\Delta_{n-1}$ being well-known and trivial). The above results show that this inequality is precise for $n = 2$ or 3.

The final sections 4 and 5 contain some applications of the method to particular forms f. The choice of these is to a large extent arbitrary; the form A_n alone exhibits all aspects of the method, and in particular its extensions include all the (known) absolutely extreme forms in $n+1$ variables for $n \leqslant 7$. I give also some extensions of L_n^r, which are of special interest in that they include the forms K_{11}, K_{12} mentioned above; they also include 13 perfect forms in 7, 8 or 9 variables distinct from those listed at the conclusion of Part I.

2. Description of the method. Beginning with a perfect form $f(\boldsymbol{x}) = \sum_1^n a_{ij}x_ix_j$, we attempt to find a perfect extension

$$g(\boldsymbol{x}, x_{n+1}) = f(\boldsymbol{x}) + 2x_{n+1}\sum_1^n a_ix_i + bx_{n+1}^2 \tag{2.1}$$

with

$$M(g) = M(f) = M. \tag{2.2}$$

We may write (2.1) in the alternative form

$$\begin{aligned} g(\boldsymbol{x}, x_{n+1}) &= f(\boldsymbol{x}+x_{n+1}\lambda) + cx_{n+1}^2 = \\ &= f(x_1+\lambda_1x_{n+1}, \ldots, x_n+\lambda_nx_{n+1}) + cx_{n+1}^2 \end{aligned} \tag{2.3}$$

where

$$a_i = \sum_j a_{ij}\lambda_j, \qquad b = c + f(\lambda), \qquad D(g) = cD(f). \tag{2.4}$$

To justify this aim, we prove:

LEMMA 2.1. *Any perfect form has a perfect extension with the same minimum.*

Proof. Let $f(\boldsymbol{x})$ be perfect, with minimum M, and consider the extension

$$g_1(\boldsymbol{x}, x_{n+1}) = f(\boldsymbol{x}) + Mx_{n+1}^2.$$

g_1 has minimum M and minimal vectors $(\boldsymbol{O}, 1)$, and $(\boldsymbol{m}, 0)$, where $\boldsymbol{m}$ runs through the minimal vectors of f. Clearly g_1 is imperfect, and any quadratic relation satisfied by all its minimal vectors is of the form

$$\psi \equiv x_{n+1}(p_1x_1 + \ldots + p_nx_n) = 0 \tag{2.5}$$

(since f is perfect).

For any such $\psi \neq 0$ we consider the form

$$g_2 = g_1 + \varrho\psi$$

(which is still an extension of f). The argument used by Voronoi ([10], p. 104-108) shows that g_2 is positive definite, with minimum M (obviously attained at all the minimal vectors of g_1) for a range of values of ϱ; and that, for a unique positive ϱ, g_2 has at least one more minimal vector: explicitly

$$\varrho = \min_{\psi<0} \frac{M - g_1}{\psi} > 0.$$

If now g_2 is not perfect, its minimal vectors satisfy a non-trivial relation of the same form (2.5) and the process may be repeated, yielding an extension of f with more minimal vectors than g_2.

Proceeding thus, we eventually obtain a perfect extension g as required, since the possible number of minimal vectors is bounded.

Let now Π_x be the set of points $\boldsymbol{x}$ which, with the metric defined by $f(\boldsymbol{x})$, are at least as near to the origin as to any other point of the integral lattice Γ. Thus Π_x is defined by the system of linear inequalities

$$f(\boldsymbol{x}) \leqslant f(\boldsymbol{x}\pm\boldsymbol{l}), \quad \boldsymbol{l} \in \Gamma.$$

It is easily shown in [11] that a finite number σ of these inequalities imply all the rest, and so suffice to define Π_x. Thus Π_x is a convex polytope with σ pairs of parallel faces, defined by

$$\pm 2 \sum a_{ij} l_{ik} x_j \leqslant f(\boldsymbol{l}_k) \quad (k = 1, 2, \ldots, \sigma). \tag{2.6}$$

Voronoi [11] shows, more precisely, that a point $\boldsymbol{l} \neq \boldsymbol{O}$ of Γ belongs to the defining set $\pm\boldsymbol{l}_1, \ldots, \pm\boldsymbol{l}_\sigma$ if and only if the minimum of $f(\boldsymbol{x})$ for integral $\boldsymbol{x} \equiv \boldsymbol{l} \pmod 2$ is attained only at $\boldsymbol{x} = \pm\boldsymbol{l}$. Hence $\sigma \leqslant 2^n - 1$, where the equality sign holds in general.

For any real λ, we define

$$\mathcal{M}(\lambda) = \mathcal{M}(f; \lambda) = \min_{\boldsymbol{x}\in\Gamma} f(\boldsymbol{x}+\lambda),$$

so that $\mathcal{M}(\lambda) = f(\lambda)$ if and only if $\lambda \in \Pi_x$. Clearly $\mathcal{M}(\lambda) = \mathcal{M}(\mu)$ if $\lambda - \mu \in \Gamma$, in which case we say that λ und μ are *congruent*. Also, if the integral unimodular matrix T is an automorph of f, we have

$$\mathcal{M}(f; \lambda) = \mathcal{M}(Tf; T\lambda) = \mathcal{M}(f; T\lambda);$$

we call the points λ and $T\lambda$ *equivalent* (for f).

We note here the obvious but useful result:

LEMMA 2.2. *The extensions $g(\boldsymbol{x}, x_{n+1})$ of $f(\boldsymbol{x})$ given by (2.3) which correspond to congruent or equivalent λ and the same c are equivalent.*

For any positive extension (2.3) of f, we set for convenience

$$M_k(g) = \min_{\boldsymbol{x}\in\Gamma} g(\boldsymbol{x}, \pm k) \quad (k = 0, 1, 2, \ldots), \quad (\boldsymbol{x}, k) \neq (\boldsymbol{O}, 0).$$

Thus

$$M_0(g) = M(f) = M,$$
$$M_k(g) = \mathcal{M}(f; k\lambda) + k^2 c,$$
$$M(g) = \min_k M_k(g) \leqslant M.$$

A vertex $\boldsymbol{v}$ of Π_x is a point of Π_x lying on n linearly independent faces. Thus we may say that $\boldsymbol{v}$ is a vertex if and only if its coordinates are determined by those of the relations (2.6) which it satisfies with equality.

Our construction of a perfect extension g rests on the following result:

THEOREM 2.1. *Suppose that $f(\boldsymbol{x})$ is perfect with minimum M, and that, for some integral $t \geqslant 1$, the point $t\lambda$ is congruent to a vertex $\boldsymbol{v}$ of Π_x and satisfies*

$$\mathcal{M}(t\lambda) = \mathcal{M}(\boldsymbol{v}) < M. \tag{2.7}$$

Then the extension $g(\boldsymbol{x}, x_{n+1})$ defined by (2.3) with

$$t^2 c = M - \mathcal{M}(t\lambda) \tag{2.8}$$

has $M_t(g) = M$; and g is perfect if its minimum is M.

Proof. We have, using (2.8),

$$M_t(g) = \mathcal{M}(f; t\lambda) + t^2 c = M.$$

By hypothesis, $t\lambda = \boldsymbol{v} - \boldsymbol{a}$ for some vertex $\boldsymbol{v}$ of Π_x and some integral $\boldsymbol{a}$. If now in fact $M(g) = M$, the minimal vectors $(\boldsymbol{x}, x_{n+1})$ of g certainly include (i) $(\boldsymbol{m}, 0)$, where $\boldsymbol{m}$ is any minimal vector of f; (ii) $(\boldsymbol{l}+\boldsymbol{a}, t)$, where $\boldsymbol{l}$ is any one of $\pm\boldsymbol{l}_1, \ldots, \pm\boldsymbol{l}_\sigma$ satisfying

$$f(\boldsymbol{l}+\boldsymbol{v}) = f(\boldsymbol{v}) \ (= \mathcal{M}(t\lambda)); \tag{2.9}$$

(iii) $(\boldsymbol{a}, t)$.

Now the equations $g(\boldsymbol{m}, 0) = M$ determine the coefficients a_{ij} of f, since the equations are just $f(\boldsymbol{m}) = M$ and f is perfect. From the minimal vectors (ii) and (iii) we have the equations

$$g(\boldsymbol{l}+\boldsymbol{a}, t) = M, \quad g(\boldsymbol{a}, t) = M$$

for the remaining $n+1$ coefficients of g. These may be written

$$f(\boldsymbol{l}+\boldsymbol{a}+t\lambda) = f(\boldsymbol{a}+t\lambda) = M - t^2 c,$$

which are just (2.9), with $\boldsymbol{v} = \boldsymbol{a}+t\lambda$. Since $\boldsymbol{v}$ is a vertex of Π_x, (2.9) yield n independent linear equations determining $\boldsymbol{v}$, and so λ. The remaining equation $g(\boldsymbol{a}, t) = M$ now determines c, as given by (2.8).

This shows that g is perfect, and the theorem is proved.

We conclude this section with some notes on the method.

(1) The construction used by Chaundy [4] is easily shown to be equivalent to taking in the above theorem: f absolutely extreme, $t = 1$, and λ a vertex of Π_x for which $f(\lambda)$ is greatest. In all cases considered in

[4], the inequality (2.7) is satisfied, so that the construction then gives the extension g of f with least $D(g) = cD(f)$. Since f is here chosen to be absolutely extreme, i. e. to have least D for minimum M, the resulting extension g is certainly a good candidate for the title of absolutely extreme.

(2) The construction clearly fails if $f(\boldsymbol{v}) \geqslant M$ for all vertices $\boldsymbol{v}$ of Π_x. Although this phenomenon can occur for imperfect forms, every perfect form examined has at least one vertex satisfying $f(\boldsymbol{v}) < M$. Lemma 2.1, while asserting the existence of a perfect extension, unfortunately does not guarantee that it can be constructed by the method of Theorem 2.1.

(3) For all forms examined, the method always yields an extension with $t = 1$. In this case, the corresponding vertex often satisfies the condition

$$\mathcal{M}(\boldsymbol{v}) = f(\boldsymbol{v}) \leqslant \tfrac{3}{4}M,$$

from which it follows easily that g has minimum M (and is therefore perfect). For then $M_0(g) = M_1(g) = M$, while, for $k \geqslant 2$,

$$M_k(g) = \mathcal{M}(f; k\boldsymbol{v}) + k^2 c \geqslant 4c = 4\big(M - \mathcal{M}(\boldsymbol{v})\big) \geqslant M.$$

(4) Theorem 2.1 becomes false if "perfect" is replaced by "extreme". Thus L_n^r has the extension L_{n+1}^r; if $n = 2r+1$, L_n^r is extreme and L_{n+1}^r is not. Conversely, we can obtain extreme extensions of non-extreme forms; e. g. M_{2r+3}^r is an extension of L_{2r+2}^r $(r \geqslant 3)$.

(5) We shall usually find it convenient to work with the contragredient coordinates $y_1, \ldots, y_n$ defined by

$$y_i = \sum_j a_{ij} x_j. \tag{2.10}$$

The polytope Π_x then becomes, more simply,

$$\Pi_y: \quad \pm 2 \sum l_{ik} y_i \leqslant f(\boldsymbol{l}_k) \quad (k = 1, 2, \ldots, \sigma), \tag{2.11}$$

and a vertex $\boldsymbol{\lambda}$ of Π_x transforms into a vertex $\boldsymbol{\alpha}$ of Π_y where, as in (2.4), $\alpha_i = \sum a_{ij}\lambda_j$. We have also

$$f(\boldsymbol{x}) = f^*(\boldsymbol{y}), \tag{2.12}$$

where f^* is the reciprocal of f; hence the second relation (2.4) may be written

$$b = c + f^*(\boldsymbol{\alpha}). \tag{2.13}$$

3. An inequality for Δ_n. We establish here the inequality (1.4). We need first the following general result:

LEMMA 3.1. *If $f(\boldsymbol{x})$ is positive definite with minimum M, there exists a $\boldsymbol{\lambda}$ with*

$$\mathcal{M}(f; \lambda) \geqslant \frac{nM}{2(n+1)}. \tag{3.1}$$

Proof. Expressing $f(\boldsymbol{x})$ as a sum of squares, we may write

$$\frac{4}{M} f(\boldsymbol{x}) = \sum_1^n \xi_i^2;$$

then, for integral $\boldsymbol{x}$, $\boldsymbol{\xi}$ belongs to a lattice Λ, and $\sum_1^n \xi_i^2 \geqslant 4$ for all $\boldsymbol{\xi} \in \Lambda$, $\boldsymbol{\xi} \neq \boldsymbol{O}$.

Hence the unit spheres centred at the points of Λ do not overlap. If now $P_1, \ldots, P_k$ are any points of Λ, P is any point, and $|PP_i| = r_i$, Blichfeldt's well-known inequality gives

$$\sum_1^k r_i^2 \geqslant 2(k-1). \tag{3.2}$$

Let $\boldsymbol{\lambda}$ be any vertex of the polytope Π_x of $f(\boldsymbol{x})$, and $P = \boldsymbol{\xi}$ the corresponding point in $\boldsymbol{\xi}$-coordinates. Then

$$\frac{4}{M}\mathcal{M}(f; \lambda) = \frac{4}{M} f(\lambda) = \sum_1^n \xi_i^2 = r^2,$$

say. By definition of a vertex, $\boldsymbol{\xi}$ is equidistant from 0 and at least n further lattice-points; hence (3.2) holds with $k = n+1$, $r_i = r$, giving

$$r^2 \geqslant \frac{2n}{n+1}, \qquad \mathcal{M}(f; \lambda) = \frac{M}{4} r^2 \geqslant \frac{nM}{2(n+1)},$$

as required.

Note. The inequality (3.1) is the best that can be asserted for an arbitrary *vertex* $\boldsymbol{\lambda}$ of $\Pi_x(f)$, since, as will be shown in the following section, A_n has a vertex $\boldsymbol{\lambda}$ satisfying (3.1) with equality, for all n. The result of the lemma is best possible for $n = 2$ or 3, but probably not for larger n.

LEMMA 3.2. *Any positive form $f(x_1, \ldots, x_n)$ has an extension $g(x_1, \ldots, x_{n+1})$ satisfying*

$$\Delta(g) \leqslant \frac{n+2}{n+1} \Delta(f).$$

Proof. We may assume that $M(f) = 2$, so that $\Delta(f) = D(f)$. Choose $\boldsymbol{\lambda}$ to satisfy (3.1), so that

$$\mathcal{M}(f; \lambda) \geqslant \frac{n}{n+1},$$

and define

$$g(x_1, \ldots, x_{n+1}) = f(\boldsymbol{x}+\lambda x_{n+1}) + \frac{n+2}{n+1} x_{n+1}^2.$$

Then $M(g) = 2$; for

$$M_0(g) = M(f) = 2;$$

$$M_1(g) = \mathcal{M}(f; \lambda) + \frac{n+2}{n+1} \geqslant 2;$$

$$M_k(g) = k^2 \frac{n+2}{n+1} > 2 \quad \text{for} \quad k \geqslant 2.$$

Hence

$$\Delta(g) = D(g) = \frac{n+2}{n+1} D(f) = \frac{n+2}{n+1} \Delta(f).$$

COROLLARY. $\Delta_{n+1} \leqslant \frac{n+2}{n+1} \Delta_n$.

This follows at once from Lemma 3.2 by choosing f as absolutely extreme, so that $\Delta(f) = \Delta_n$.

4. Extensions of A_n. We may write, as in I § 3,

$$A_n(\boldsymbol{x}) = \Big(\sum_1^n x_i\Big)^2 + \sum_1^n x_i^2,$$

with

$$M = 2, \quad s = \tfrac{1}{2}n(n+1), \quad D = \Delta = n+1.$$

The reciprocal of A_n is

$$A_n^*(\boldsymbol{y}) = \sum_1^n y_i^2 - \frac{1}{n+1}\Big(\sum_1^n y_i\Big)^2.$$

The contragredient lattice, defined in (2.10), is given by

$$y_i = \sum_1^n x_j + x_i,$$

so that, for integral $\boldsymbol{x}$, $\boldsymbol{y}$ runs through the sublattice Λ^* of Γ_n defined by

$$\sum_1^n y_i \equiv 0 \pmod{n+1}.$$

The integral vectors defining Π_x are simply the $\frac{1}{2}n(n+1)$ minimal vectors of A_n: $\boldsymbol{e}_i$ $(1 \leqslant i \leqslant n)$, $\boldsymbol{e}_i - \boldsymbol{e}_j$ $(1 \leqslant i < j \leqslant n)$. Thus Π_y is defined by

$$|y_i| \leqslant 1 \quad (1 \leqslant i \leqslant n), \qquad |y_i - y_j| \leqslant 1 \quad (1 \leqslant i < j \leqslant n),$$

and its vertices $\boldsymbol{w}$ are easily found to be the $2^n - 1$ points with all coordinates 0 or 1 (other than $\boldsymbol{O}$) and their negatives. Since $A_n^*(\boldsymbol{y})$ is invariant under an arbitrary permutation of the coordinates, any vertex is equivalent to one of

$$\boldsymbol{w}_k = (1_k, 0_{n-k}) \qquad (1 \leqslant k \leqslant n)$$

(where a symbol such as 1_k denotes a sequence of k coordinates 1). $A_n^*(\boldsymbol{y})$ is also invariant under the transformation: $y_1 \to y_1$, $y_i \to y_1 - y_i$ $(i = 2, 3, \ldots, n)$, under which

$$\boldsymbol{w}_k \sim (1, 0_{k-1}, 1_{n-k}) \sim \boldsymbol{w}_{n+1-k}.$$

Hence any vertex of Π_y is equivalent to some $\boldsymbol{w}_k$ with $1 \leqslant k \leqslant \frac{1}{2}(n+1)$; and, if $\boldsymbol{v}_k$ denotes the corresponding vertex of Π_x,

$$A_n(\boldsymbol{v}_k) = A_n^*(\boldsymbol{w}_k) = \frac{k}{n+1}(n+1-k).$$

We note first that

$$A_n(\boldsymbol{v}_1) = \frac{n}{n+1} < M = 2 \quad \text{for all } n,$$

$$A_n(\boldsymbol{v}_2) = \frac{2(n-1)}{n+1} < 2 \quad \text{for all } n,$$

$$A_n(\boldsymbol{v}_3) = \frac{3(n-2)}{n+1} < 2 \quad \text{only for } n \leqslant 7,$$

$$A_n(\boldsymbol{v}_k) \geqslant 2 \quad \text{for} \quad 4 \leqslant k \leqslant \tfrac{1}{2}(n+1).$$

Hence the method of Theorem 2.1 can be applied only with $\boldsymbol{v} \sim \boldsymbol{v}_k$ for $k = 1$, 2, or 3, and with $\boldsymbol{v} \sim \boldsymbol{v}_3$ only for $n \leqslant 7$. We consider in turn the various possible values of k and t.

I. $k = 1, t = 1$. Following Theorem 2.1, we take

$$\boldsymbol{a} = \boldsymbol{w}_1 = (1, 0_{n-1}), \qquad c = M - A_n^*(\boldsymbol{w}_1) = \frac{n+2}{n+1}.$$

The corresponding extension g_m therefore has $M = 2$, $D = n+2 = m+1$, and is easily verified to be equivalent to A_m.

II. $k = 2$, $t = 1$. Here

$$\boldsymbol{a} = \boldsymbol{w}_2 = (1, 1, 0_{n-2}), \qquad c = \frac{4}{n+1},$$

whence $D(g_m) = 4$; and we find that $g_m \sim B_m$.

III. $k=3$, $t=1$. Here we require $n \leqslant 7$ (and $n \geqslant 2k-1=5$), with

$$\boldsymbol{a} = \boldsymbol{w}_3 = (1_3, 0_{n-3}), \qquad c = M - A_n^*(\boldsymbol{w}_3) = \frac{8-n}{n+1}.$$

Thus for $m = n+1 = 6$, 7 or 8 we obtain an extension g_m with $D(g_m) = 9-m$. It is easily verified that these forms have minimum 2, and so must be equivalent to the absolutely extreme forms E_6, E_7 and E_8 in the notation of [5].

IV. $k=1$, $t \geqslant 2$. Taking the equivalent vertex $\boldsymbol{w}_n$ in place of $\boldsymbol{w}_1$, we require

$$t\boldsymbol{a} \equiv \boldsymbol{w}_n = (1_n) \,(\mathrm{mod}\, \Lambda^*),$$
$$t^2 c = M - A_n^*(\boldsymbol{w}_n) = \frac{n+2}{n+1} \tag{4.1}$$

(the condition (4.1) being the same as $t\lambda \equiv \boldsymbol{v}_n (\mathrm{mod}\, \Gamma_n)$). Any corresponding extension g_m therefore has

$$D(g_m) = cD(A_n) = \frac{m+1}{t^2}.$$

We have already described in Part I some forms with minimum 2 and this value of D, namely A_m^t and $A_m^{t,q,2}$ (with suitable restrictions on the parameters m, t, q), and all these are easily shown to correspond to various choices of $\boldsymbol{a}$ satisfying (4.1).

Thus if we take

$$t\boldsymbol{a} = (1_n) + (n+1, n+1, \ldots, n+1),$$
$$\boldsymbol{a} = \left(\frac{n+2}{t}, \frac{n+2}{t}, \ldots, \frac{n+2}{t}\right),$$

we obtain

$$g_m = \Big(\sum_1^n x_i\Big)^2 + \sum_1^n x_i^2 + \frac{2n+4}{t} x_m \Big(\sum_1^n x_i\Big) + \frac{(n+1)(n+2)}{t^2} x_m^2,$$

$$t^2 g_m = (tx_1 + \ldots + tx_n + mx_m)^2 + \sum_1^n (tx_i + x_m)^2 + x_m^2$$
$$= \Big(\sum_1^m z_i\Big)^2 + \sum_1^m z_i^2$$

with

$$z_i = tx_i + x_m \quad (i = 1, \ldots, n), \qquad z_m = x_m;$$

this shows at once that $t^2 g_m$ is the form A_m^t of I, § 7. (Of course, the results of Part I show that g_m is now not only perfect, but extreme, when its minimum is 2).

Similarly, taking

$$t\boldsymbol{a} = (1_n) + (1_{q-1}, -1_{q-1}, 0_{n-2q+2}) \qquad (1 \leqslant q \leqslant \tfrac{1}{2}n+1),$$

i. e.

$$\boldsymbol{a} = \frac{1}{t}(2_{q-1}, 0_{q-1}, 1_{n-2q+2}),$$

we obtain an extension equivalent to $A_m^{t,q,2}$ of I, § 6 (known to be in fact extreme when $q \geqslant t^2$, $m \geqslant 2q$, which are the necessary conditions for the extension to have minimum 2).

Many other (inequivalent) choices of $\boldsymbol{a}$ are available if n is sufficiently large; a discussion of these in any generality would take us too far here.

V. $k=2$, $t \geqslant 2$. Using $\boldsymbol{w}_{n-1}$ in place of $\boldsymbol{w}_2$, we take

$$t\boldsymbol{a} \equiv \boldsymbol{w}_{n-1} = (1_{n-1}, 0) \,(\mathrm{mod}\, \Lambda^*).$$
$$t^2 c = M - A_n^*(\boldsymbol{w}_{n-1}) = \frac{4}{n+1};$$

any extension g_m therefore has $D(g_m) = 4/t^2$.

An analysis closely parallel to that of IV now applies, and we are led in particular to the forms $B_m^{t,q,2}$, B_m^t described in Part I. These forms may in fact be more conveniently obtained as extensions of B_n which, for $n \geqslant 4$, has just one class of vertices satisfying $B_n(\boldsymbol{v}) < M(B_n) = 2$. The analysis is so close to that of I and IV above that we omit the details here.

Summarizing these results, we see that the perfect extensions of A_n include a large number of the general classes of forms examined in Part I, namely A_n, B_n, A_n^t, B_n^t, $A_n^{t,q,2}$, $B_n^{t,q,2}$ and E_6. These in turn include all known absolutely extreme forms, viz. A_2, A_3, B_4, B_5, E_6, A_7^2 ($\sim E_7$), B_8^2 ($\sim E_8 \sim A_8^3$), and the conjectured absolutely extreme form B_9^2 ($\sim \Phi_9$ of [4]) in 9 variables.

5. Extensions of L_n^r. In Part I, § 4, L_n^r was defined to be the form

$$f(\boldsymbol{x}) = \sum_{i=1}^{r} (x_i^2 - x_i x_{i+r} + x_{i+r}^2) + \sum_{k=2r+1}^{n} x_k^2 \quad (n \geqslant 2r) \tag{5.1}$$

with lattice Λ the sublattice of the integral lattice specified by

$$\sum_1^n x_i \equiv 0 \,(\mathrm{mod}\, 3). \tag{5.2}$$

Then L_n^r is perfect for $r \geqslant 3$ and for $r = 2$, $n \geqslant 5$, with

$$M = 2, \quad D = 3^{r+2}/2^{2r}, \quad s = \tfrac{1}{2}n(n-1)+\tfrac{1}{2}r(2n+r-7). \tag{5.3}$$

The contragredient variables y_i are given by

$$\left.\begin{aligned} y_i &= x_i - \tfrac{1}{2}x_{i+r} \\ y_{i+r} &= -\tfrac{1}{2}x_i + x_{i+r} \end{aligned}\right\} \quad (1 \leqslant i \leqslant r),$$
$$y_k = x_k \quad (2r+1 \leqslant k \leqslant n),$$

so that Λ^* is the lattice of points $\boldsymbol{y}$ for which $2y_1, \ldots, 2y_{2r}, y_{2r+1}, \ldots, y_n$ are integral and satisfy

$$\begin{aligned} &2y_i \equiv 2y_{i+r} \pmod 3 \quad (1 \leqslant i \leqslant r), \\ &\sum_{i=1}^{r}(2y_i+2y_{i+r}) + \sum_{2r+1}^{n} y_k \equiv 0 \pmod 3. \end{aligned} \tag{5.4}$$

The inverse of f is

$$f^*(\boldsymbol{y}) = \tfrac{4}{3}\sum_{i=1}^{r}(y_i^2+y_iy_{i+r}+y_{i+r}^2) + \sum_{2r+1}^{n} y_k^2.$$

The vectors defining Π are easily found to be the representatives of $f(\boldsymbol{x}) = 2$ and $f(\boldsymbol{x}) = 3$; thus Π_y is specified by the inequalities

$$\begin{aligned} |y_i - y_j| &\leqslant 1, \\ |y_i + y_{i+r} - y_j - y_{j+r}| &\leqslant 1, \\ |y_i + y_{i+r} + y_j| &\leqslant 1, \\ |y_i - y_{i+r}| &\leqslant \tfrac{3}{2}, \\ |y_i + 2y_{i+r}| &\leqslant \tfrac{3}{2}, \\ |2y_i + y_{i+r}| &\leqslant \tfrac{3}{2}, \\ |y_i + y_j + y_k| &\leqslant \tfrac{3}{2}, \\ |y_i + y_{i+r} - y_j - y_k| &\leqslant \tfrac{3}{2}, \\ |y_i + y_{i+r} + y_j + y_{j+r} - y_k| &\leqslant \tfrac{3}{2}, \\ |y_i + y_{i+r} + y_j + y_{j+r} + y_k + y_{k+r}| &\leqslant \tfrac{3}{4}. \end{aligned}$$

Here the suffixes in each inequality are supposed to be distinct and otherwise arbitrary, subject to the two restrictions: (i) no two suffixes are of the form i, $i+r$ $(1 \leqslant i \leqslant r)$ unless this is explicitly shown; (ii) in any pair i, $i+r$ the range of i is $1 \leqslant i \leqslant r$. The last inequality is of course vacuous if $r = 2$.

The number and form of the vertices of Π depend on the values of n and r, and we cannot attempt a complete analysis here. We therefore give a selection of vertices whose form may be specified for general n and r (subject always to the restrictions $n \geqslant 2r$, and either $r \geqslant 3$ or $r = 2$, $n \geqslant 5$). The verification that the given points $\boldsymbol{w}$ are in fact vertices of Π_y is in all cases straightforward.

(a) $\boldsymbol{w}_1 = (\frac{1}{2}, 0_{r-1}, \frac{1}{2}, 0_{r-1}, 0_{n-2r})$, $f^*(\boldsymbol{w}_1) = 1$. Taking $t = 1$ in Theorem 2.1, we have $\boldsymbol{a} = \boldsymbol{w}_1$, $c = M - f^*(\boldsymbol{w}_1) = 1$. Since $c < \frac{3}{4}M$, the resulting extension g_m has minimum 2, and so is perfect with $D(g_m) = 3^{r+2}/2^{2r}$. This extension is easily identified with L_m^r; explicitly it is

$$g_m = f(x_1+x_m, x_2, \ldots, x_r, x_{r+1}+x_m, x_{r+2}, \ldots, x_n) + x_m^2.$$

with integral $x_1, \ldots, x_n, x_m$ subject to (5.2).

(b) Using the same vertex $\boldsymbol{w}_1$ with $t = 2$ in Theorem 2.1, we have $4c = M - f^*(\boldsymbol{w}_1) = 1$, $c = \frac{1}{4}$,

$$2\boldsymbol{a} \equiv \boldsymbol{w}_1 \pmod{\Lambda^*}.$$

For any such choice of $\boldsymbol{a}$, the corresponding extension g_m will have

$$M_0(g) = M_2(g) = M(L_n^r) = 2,$$

by Theorem 2.1; and, for $k \geqslant 3$,

$$M_k(g) \geqslant k^2 c \geqslant \tfrac{9}{4} > 2.$$

Hence g will be perfect with minimum 2 if and only if

$$M_1(g) = \mathcal{M}(f; \lambda) + c \geqslant 2. \tag{5.6}$$

We shall show that $\boldsymbol{a}$ may be chosen to satisfy (5.5) and (5.6) whenever

$$n \geqslant r+7. \tag{5.7}$$

Thus, provided

$$m \geqslant 2r+1, \quad m \geqslant r+8, \tag{5.8}$$

the extension g_m will be perfect with

$$M(g_m) = 2, \quad \Delta(g_m) = D(g_m) = 3^{r+2}/2^{2r+2}. \tag{5.9}$$

(i) Set

$$2\boldsymbol{a} - \boldsymbol{w}_1 = \boldsymbol{l} = \big(0, (\tfrac{1}{2})_{r-1}, 0, (\tfrac{1}{2})_{r-1}; \varepsilon_{2r+1}, \ldots, \varepsilon_n\big), \tag{5.10}$$

where each ε_k is 0 or ± 1; $\boldsymbol{l}$ is then a point of Λ^* provided

$$\sum_{2r+1}^{n} \varepsilon_k \equiv r-1 \pmod 3. \tag{5.11}$$

This gives

$$\boldsymbol{a} = \left((\tfrac{1}{2})_{2r}; \tfrac{1}{2}\varepsilon_{2r+1}, \cdots, \tfrac{1}{2}\varepsilon_n\right),$$

which is easily seen to be a point of Π_y, so that

$$\mathcal{M}(f; \lambda) + c = f^*(\boldsymbol{a}) + \tfrac{1}{4} = \tfrac{1}{4}\left(r+1+\sum \varepsilon_k^2\right);$$

thus (5.6) is also satisfied provided

$$\sum_{2r+1}^{n} \varepsilon_k^2 \geqslant 7-r. \tag{5.12}$$

If now $2 \leqslant r \leqslant 6$, and (5.7) holds, we take

$$\varepsilon_k = -1 \quad (2r+1 \leqslant k \leqslant r+7), \qquad \varepsilon_k = 0 \quad (k > r+7),$$

giving $\sum \varepsilon_k = r-7$, $\sum \varepsilon_k^2 = 7-r$, so that (5.11), (5.12) are satisfied.

If $r \geqslant 7$ and $n \geqslant 2r+1$, we take $\varepsilon_k = 0$ for $k > 2r+1$ and $\varepsilon_{2r+1} = 0$ or ± 1 to satisfy (5.11); (5.12) is then satisfied trivially.

(ii) If $r \geqslant 7$ and $n = 2r$, the ε_k are vacuous and (5.10) will not always be a point of Λ^*. We therefore now choose

$$2\boldsymbol{a} - \boldsymbol{w}_1 = \boldsymbol{l} = \begin{cases} \left(0, (\tfrac{1}{2})_{r-1}; 0, (\tfrac{1}{2})_{r-1}\right) & \text{if} \quad r \equiv 1 \pmod 3, \\ \left(0, (\tfrac{1}{2})_{r-2}, 0; 0, (\tfrac{1}{2})_{r-2}, 0\right) & \text{if} \quad r \equiv 2 \pmod 3, \\ \left(0, (\tfrac{1}{2})_{r-3}, 0, 0; 0, (\tfrac{1}{2})_{r-3}, 0, 0\right) & \text{if} \quad r \equiv 0 \pmod 3. \end{cases}$$

Then (5.5) is satisfied, $\boldsymbol{a} \in \Pi_y$, and

$$M_1(g) = f^*(\boldsymbol{a}) + \tfrac{1}{4} = \tfrac{1}{4}(r+1),\ \tfrac{1}{4}r,\ \tfrac{1}{4}(r-1) \text{ respectively;}$$

since $r \geqslant 7$, $M_1(g) \geqslant 2$ in all cases and (5.6) therefore holds.

(c) $\boldsymbol{w}_2 = \left((\tfrac{1}{2})_r, 0_r; (-\tfrac{1}{2})_{n-2r}\right)$ is a vertex of Π_y with $f^*(\boldsymbol{w}_2) = \frac{1}{12}(3n-2r)$. Taking $t = 1$ in Theorem 2.1, we have

$$\boldsymbol{a} = \boldsymbol{w}_2, \qquad c = M - f^*(\boldsymbol{w}_2) = \tfrac{1}{12}(24+2r-3n). \tag{5.13}$$

We shall show that the corresponding extension g_m has minimum 2, and so is perfect, if and only if

$$r \leqslant 5, \qquad n \leqslant r+6 \tag{5.14}$$

(where, as always, we assume that L_n^r is perfect, so that $r \geqslant 3$ or $r = 2$, $n \geqslant 5$). We shall then have

$$M(g_m) = 2, \qquad \Delta(g_m) = D(g_m) = (\tfrac{3}{4})^{r+1}(27+2r-3m)$$

when

$$r \leqslant 5, \qquad 2r+1 \leqslant m \leqslant r+7.$$

The corresponding vertex λ of Π_x is

$$\lambda = \left((\tfrac{2}{3})_r, (\tfrac{1}{3})_r; (-\tfrac{1}{2})_{n-2r}\right)$$

so that, writing $\psi(x, y) = x^2 - xy + y^2$, we have

$$g = g_m = \sum_{i=1}^{r} \psi(x_i + \tfrac{2}{3}x_m, x_{i+r} + \tfrac{1}{3}x_m) + \sum_{2r+1}^{n} (x_k - \tfrac{1}{2}x_m)^2 + cx_m^2.$$

By choice of c,

$$M_0(g) = M_1(g) = M(L_n^r) = 2.$$

The necessary condition $c > 0$ gives at once

$$24+2r > 3n \geqslant 6r, \qquad r < 6.$$

Next,

$$g(\boldsymbol{x}, 2) = \sum_{i=1}^{r} \psi(x_i + \tfrac{4}{3}, x_{i+r} + \tfrac{2}{3}) + \sum (x_k - 1)^2 + 4c,$$

and each form ψ occurring here is easily seen to have minimum $\frac{1}{3}$ for integral x_i, x_{i+r}, attained when $(x_i, x_{i+r}) = (-1, 0), (-1, -1)$ or $(-2, -1)$, Since we can take all $x_k = 1$ $(k > 2r)$ and choose each pair x_i, x_{i+r} as above to satisfy (5.2), we therefore have

$$M_2(g) = \min g(\boldsymbol{x}, 2) = \tfrac{1}{3}r + 4c = 8 + r - n.$$

Thus $M_2(g) \geqslant 2$ if and only if $n \leqslant r+6$.

It remains for us now only to consider $M_k(g)$ for $k \geqslant 3$, assuming that (5.14) holds. Now

$$g(\boldsymbol{x}, 3) = \sum_{i=1}^{r} \psi(x_i + 2, x_{i+r} + 1) + \sum_{2r+1}^{n} (x_k - \tfrac{3}{2})^2 + 9c,$$

whence, since $n \leqslant r+6$,

$$M_3(g) \geqslant \tfrac{1}{4}(n-2r) + 9c = 18 + r - 2n \geqslant 6 - r.$$

This shows that $M_3(g) \geqslant 2$ if $r \leqslant 4$, or if $r = 5$, $n \leqslant 10$. The only other possibility allowed by (5.14) is that $r = 5$, $n = 11$, and in this case also $M_3(g) = 2$, since the values $x_i = -2$, $x_{i+r} = -1$ $(i = 1, \ldots, r)$, $x_{11} = 1$ or 2 do not satisfy (5.2).

Since $c \geqslant \frac{1}{6}$ unless $r = 5$, $n = 11$, we obtain

$$M_k(g) \geqslant k^2 c \geqslant \tfrac{16}{6} > 2 \quad \text{for} \quad k \geqslant 4.$$

If however $r = 5$, $n = 11$, then $c = \frac{1}{12}$ and $M_k(g) > 2$ for $k \geqslant 5$; a direct argument shows easily that also $M_4(g) > 2$.

(d) $\boldsymbol{w}_3 = \left((\frac{1}{6})_{2r}, -\frac{5}{6}, (\frac{1}{3})_{n-2r+1}\right)$, for $n \geqslant 2r+1$, is a vertex of Π_y with $f^*(\boldsymbol{w}_3) = \frac{1}{36}(4n+21-4r)$. Taking $t = 1$ in Theorem 2.1, we have

$$\boldsymbol{a} = \boldsymbol{w}_3, \quad c = M - f^*(\boldsymbol{w}_3) = \tfrac{1}{36}(4r+51-4n).$$

The corresponding extension g_m, if it has minimum 2, will then be perfect with

$$M(g_m) = 2, \quad \Delta(g_m) = D(g_m) = \frac{3^r}{2^{2r+2}}(4r+55-4m). \tag{5.15}$$

For a positive extension g_m we require $c > 0$, whence $n \leqslant r+12$; thus necessary conditions are

$$2r+1 \leqslant n \leqslant r+12, \quad r \leqslant 11.$$

It is easy to show, by arguments similar to those used above, that these conditions are also sufficient to ensure that $M(g_m) = 2$; thus we obtain a perfect form satisfying (5.15) whenever $2r+2 \leqslant m \leqslant r+13$.

(e) $\boldsymbol{w}_4 = \left(\frac{1}{3}, \frac{1}{3}, (-\frac{1}{6})_{r-2}, \frac{1}{3}, \frac{1}{3}, (-\frac{1}{6})_{r-2}; (\frac{1}{3})_{n-2r}\right)$ is a vertex of Π_y with $f^*(\boldsymbol{w}_4) = \frac{1}{9}(n-r+6)$. Taking $t = 1$ in Theorem 2.1 we have

$$\boldsymbol{a} = \boldsymbol{w}_4, \quad c = M - f^*(\boldsymbol{w}_4) = \tfrac{1}{9}(12+r-n).$$

The corresponding extension g_m, if it has minimum 2, will be perfect with

$$M(g_m) = 2, \quad \Delta(g_m) = D(g_m) = \frac{3^r}{2^{2r}}(13+r-m).$$

From the conditions $n \geqslant 2r$, $c > 0$, we obtain

$$2r+1 \leqslant m \leqslant r+12, \quad r \leqslant 11,$$

and these conditions are easily found to be sufficient to ensure that $M(g_m) = 2$.

Summarizing the above results, we have found a large number of perfect forms, most of them new; we tabulate here the new forms with $m = 7$, 8 or 9, giving the value of r in the original form L_n^r, the paragraph (a)-(e) above in which the form appears, the number s of pairs of minimal vectors and the value of $\Delta(g_m)$.

m	r	Para.	s	$\Delta(g_m)$	m	r	Para.	s	$\Delta(g_m)$
7	2	(c)	34	$3^3\cdot 5/2^5$	9	2	(c)	90	$3^3/2^4$
7	2	(d)	30	$3^2\cdot 5\cdot 7/2^6$	9	3	(c)	82	$3^5/2^7$
7	2	(e)	32	$3^2/2$	9	4	(c)	81	$3^5/2^7$
8	2	(c)	54	$3^3\cdot 7/2^6$	9	2	(d)	64	$3^5/2^6$
8	2	(d)	41	$3^2\cdot 31/2^6$	9	3	(d)	67	$3^3\cdot 31/2^8$
8	3	(d)	46	$3^3\cdot 5\cdot 7/2^8$	9	2	(e)	58	$3^3/2^3$
8	2	(e)	44	$3^2\cdot 7/2^4$	9	3	(e)	62	$3^3\cdot 7/2^6$
8	3	(e)	48	$3^3/2^3$					

From (c), with $n = 11$, $r = 5$ we obtain a perfect form g_{12} with $M = 2$, $\Delta = 3^6/2^{12}$, $s = 378$; this may be identified with the extreme form K_{12} of [6], which is most simply represented as the form

$$f(\boldsymbol{x}) = \sum_{i=1}^{6}(x_i^2 + x_i x_{i+6} + x_{i+6}^2)$$

with integral $\boldsymbol{x}$ satisfying

$$x_1 - x_7 \equiv x_2 - x_8 \equiv \ldots \equiv x_6 - x_{12} \pmod 3,$$

$$\sum_1^{12} x_j \equiv 0 \pmod 3.$$

From (c), with $n = 10$, $r = 4$ we obtain an extension g_{11} with $M = 2$, $\Delta = 3^5/2^9$, $s = 216$. This form was mentioned in § 1, where we called it K_{11}; it may be represented as the section of K_{12} above by $\sum_{j=1}^{12} x_j = 0$, and in this form it may easily be proved extreme by Voronoi's criterion.

References

[1] E. S. Barnes, *Note on extreme forms*, Can. J. Math. 7 (1955), p. 150-154.

[2] — *The complete enumeration of extreme senary forms*, Phil. Trans. Roy. Soc. (A) 249 (1957), p. 461-506.

[3] — *The perfect and extreme senary forms*, Can. J. Math. 9 (1957), p. 235-242.

[4] T. W. Chaundy, *The arithmetic minima of positive quadratic forms*, Quart. J. Math. (Oxford) 17 (1946), p. 166-192.

[5] H. S. M. Coxeter, *Extreme forms*, Can. J. Math. 3 (1951), p. 391-441.
[6] — and J. A. Todd, *An extreme duodenary form*, Can. J. Math. 5 (1951), p. 384-392.
[7] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. 11 (1877), p. 242-292.
[8] H. Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. reine angew. Math. 129 (1905), p. 220-274.
[9] L. J. Mordell, *Observation on the minimum of a positive quadratic form in eight variables*, J. Lond. Math. Soc. 19 (1944), p. 3-6.
[10] G. Voronoi, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. 133 (1908), p. 97-178.
[11] — *Recherches sur les paralléloèdres primitifs* (Part 1), ibid. 134 (1908), p. 198-287.

UNIVERSITY OF SYDNEY, AUSTRALIA

Reçu par la Rédaction le 10. 11. 1958

ACTA ARITHMETICA
V (1959)

Zur Theorie der algebraischen Gleichungen über endlichen Körpern

von

L. Rédei (Szeged) und P. Turán (Budapest)

Dem Andenken von S. Lubelski, des ersten Herausgebers der Acta Arithmetica gewidmet.

1. Einer der schönsten Sätze der Theorie der Kongruenzen höheren Grades (welche Lubelski selbst mit vielen schönen Forschungen bereichert hat) ist der folgende Satz von König-Rados [2]:

Es sei eine Kongruenz

$$a_0+a_1x+\ldots+a_{p-2}x^{p-2} \equiv 0 \pmod p \qquad (p \nmid a_0) \tag{1.1}$$

vorgelegt (p *Primzahl*, a_ν *ganze rationale Zahl*). *Dann ist die Anzahl der verschiedenen inkongruenten Lösungen von* (1.1) *gleich*

$$p-1-r_p;$$

r_p *bedeutet den Rang* mod p *der zyklischen Matrix*

$$Z_1 = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{p-2} \\ a_{p-2} & a_0 & a_1 & \ldots & a_{p-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}. \tag{1.2}$$

Ein vereinfachter Beweis dieses Satzes ist in Kronecker's Vorlesungen über die Zahlentheorie ([1], p. 389) gegeben; ein viel einfacherer Beweis und die Erweiterung auf endliche Körper war von dem ersten von uns gefunden ([3]). Er bewies den folgenden Satz:

In einem endlichen Körper K mit q Elementen sei eine Gleichung

$$a_0+a_1x+\ldots+a_{q-2}x^{q-2} = 0 \qquad (a_0 \neq 0) \tag{1.3}$$

vorgelegt ($a_\nu \in K$). *Dann ist die Anzahl der verschiedenen Lösungen von* (1.3) *gleich*

$$q-1-r;$$