other sporadic simple groups). Its theta series is the unique modular form of weight 12 on Γ_1 with Fourier expansion starting $1 + 0q + \cdots$, so it must equal $E_{12}(z) - \frac{21736}{691}\Delta(z)$, i.e., the number $r_{\mathrm{Leech}}(n)$ of vectors of length $2n$ in the Leech lattice equals $\frac{21736}{691}\bigl(\sigma_{11}(n) - \tau(n)\bigr)$ for every positive integer n. This gives another proof and an interpretation of Ramanujan's congruence (28).

In rank 32, things become even more interesting: here the complete classification is not known, and we know that we cannot expect it very soon, because there are more than 80 million isomorphism classes! This, too, is a consequence of the theory of modular forms, but of a much more sophisticated part than we are presenting here. Specifically, there is a fundamental theorem of Siegel saying that the average value of the theta series associated to the quadratic forms in a single genus (we omit the definition) is always an Eisenstein series. Specialized to the particular case of even unimodular forms of rank $m = 2k \equiv 0 \pmod 8$, which form a single genus, this theorem says that there are only finitely many such forms up to equivalence for each k and that, if we number them $Q_1, \ldots, Q_I$, then we have the relation

$$\sum_{i=1}^{I} \frac{1}{w_i}\, \Theta_{Q_i}(z) \;=\; \mathsf{m}_k\, E_k(z)\,, \tag{39}$$

where w_i is the number of automorphisms of the form Q_i (i.e., the number of matrices $\gamma \in \mathrm{SL}(m,\mathbb{Z})$ such that $Q_i(\gamma x) = Q_i(x)$ for all $x \in \mathbb{Z}^m$) and m_k is the positive rational number given by the formula

$$\mathsf{m}_k \;=\; \frac{B_k}{2k}\,\frac{B_2}{4}\,\frac{B_4}{8}\,\cdots\,\frac{B_{2k-2}}{4k-4}\,,$$

where B_i denotes the ith Bernoulli number. In particular, by comparing the constant terms on the left- and right-hand sides of (39), we see that $\sum_{i=1}^{I} 1/w_i = \mathsf{m}_k$, the *Minkowski-Siegel mass formula.* The numbers $\mathsf{m}_4 \approx 1.44 \times 10^{-9}$, $\mathsf{m}_8 \approx 2.49 \times 10^{-18}$ and $\mathsf{m}_{12} \approx 7{,}94 \times 10^{-15}$ are small, but $\mathsf{m}_{16} \approx 4{,}03 \times 10^{7}$ (the next two values are $\mathsf{m}_{20} \approx 4.39 \times 10^{51}$ and $\mathsf{m}_{24} \approx 1.53 \times 10^{121}$), and since $w_i \ge 2$ for every i (one has at the very least the automorphisms $\pm\mathrm{Id}_m$), this shows that $I > 80000000$ for $m = 32$ as asserted.

A further consequence of the fact that $\Theta_Q \in M_k(\Gamma_1)$ for Q even and unimodular of rank $m = 2k$ is that the minimal value of $Q(x)$ for non-zero $x \in \Lambda$ is bounded by $r = \dim M_k(\Gamma_1) = [k/12] + 1$. The lattice L is called *extremal* if this bound is attained. The three lattices of rank 8 and 16 are extremal for trivial reasons. (Here $r = 1$.) For $m = 24$ we have $r = 2$ and the only extremal lattice is the Leech lattice. Extremal unimodular lattices are also known to exist for $m = 32$, 40, 48, 56, 64 and 80, while the case $m = 72$ is open. Surprisingly, however, there are no examples of large rank:

Theorem (Mallows–Odlyzko–Sloane). *There are only finitely many non-isomorphic extremal even unimodular lattices.*

We sketch the proof, which, not surprisingly, is completely modular. Since there are only finitely many non-isomorphic even unimodular lattices of any given rank, the theorem is equivalent to saying that there is an absolute bound on the value of the rank m for extremal lattices. For simplicity, let us suppose that $m = 24n$. (The cases $m = 24n + 8$ and $m = 24n + 16$ are similar.) The theta series of any extremal unimodular lattice of this rank must be equal to the unique modular form $f_n \in M_{12n}(\mathrm{SL}(2,\mathbb{Z}))$ whose q-development has the form $1 + \mathrm{O}(q^{n+1})$. By an elementary argument which we omit but which the reader may want to look for, we find that this q-development has the form

$$f_n(z) \;=\; 1 \;+\; n\,a_n\,q^{n+1} \;+\; \left(\frac{nb_n}{2} \;-\; 24\,n\,(n+31)\,a_n\right)\,q^{n+2} \;+\; \cdots$$

where a_n and b_n are the coefficients of $\Delta(z)^n$ in the modular functions $j(z)$ and $j(z)^2$, respectively, when these are expressed (locally, for small q) as Laurent series in the modular form $\Delta(z) = q - 24q^2 + 252q^3 - \cdots$. It is not hard to show that a_n has the asymptotic behavior $a_n \sim An^{-3/2}C^n$ for some constants $A = 225153.793389\cdots$ and $C = 1/\Delta(z_0) = 69.1164201716\cdots$, where $z_0 = 0.52352170017992\cdots i$ is the unique zero on the imaginary axis of the function $E_2(z)$ defined in (17) (this is because $E_2(z)$ is the logarithmic derivative of $\Delta(z)$), while b_n has a similar expansion but with A replaced by $2\lambda A$ with $\lambda = j(z_0) - 720 = 163067.793145\cdots$. It follows that the coefficient $\frac{1}{2}nb_n - 24n(n+31)a_n$ of q^{n+2} in f_n is negative for n larger than roughly 6800, corresponding to $m \approx 163000$, and that therefore extremal lattices of rank larger than this cannot exist. ♡

♠ Drums Whose Shape One Cannot Hear

Marc Kac asked a famous question, “Can one hear the shape of a drum?” Expressed more mathematically, this means: can there be two riemannian manifolds (in the case of real “drums” these would presumably be two-dimensional manifolds with boundary) which are not isometric but have the same spectra of eigenvalues of their Laplace operators? The first example of such a pair of manifolds to be found was given by Milnor, and involved 16-dimensional closed “drums.” More drum-like examples consisting of domains in $\mathbb{R}^2$ with polygonal boundary are now also known, but they are difficult to construct, whereas Milnor's example is very easy. It goes as follows. As we already mentioned, there are two non-isomorphic even unimodular lattices $\Lambda_1 = \Gamma_8 \oplus \Gamma_8$ and $\Lambda_2 = \Gamma_{16}$ in dimension 16. The fact that they are non-isomorphic means that the two Riemannian manifolds $M_1 = \mathbb{R}^{16}/\Lambda_1$ and $M_2 = \mathbb{R}^{16}/\Lambda_2$, which are topologically both just tori $(S^1)^{16}$, are not isometric to each other. But the spectrum of the Laplace operator on any torus $\mathbb{R}^n/\Lambda$ is just the set of norms $\|\lambda\|^2$ ($\lambda \in \Lambda$), counted with multiplicities, and these spectra agree for M_1 and M_2 because the theta series $\sum_{\lambda\in\Lambda_1} q^{\|\lambda\|^2}$ and $\sum_{\lambda\in\Lambda_2} q^{\|\lambda\|^2}$ coincide. ♡

$$\sharp(L_{24}, 2m) = \frac{65\,520}{691}(\sigma_{11}(m) - \tau(m)) \quad \textit{für alle} \quad m \geq 1.$$

Aus Korollar A, Korollar 6A, Satz III.4.3 und 1(4) folgert man direkt das

Korollar B. *Für positives $k \equiv 0 \pmod 4$ ist jedes $f \in \mathbb{M}_k$ eine Linearkombination von Theta–Reihen zu geraden, unimodularen, positiv definiten $2k \times 2k$ Matrizen.*

Bemerkung. Das zur Matrix L_{24} gehörige Gitter wurde von J. Leech im Jahre 1967 (Canadian J. Math. **19**, 251–265) im Zusammenhang mit der dichtesten Kugelpackung im $\mathbb{R}^{24}$ konstruiert. Aus der in Bemerkung 5b) erwähnten Klassifikation von H. Niemeier ergibt sich, dass es nur eine Klasse $\langle\, S\rangle$ von geraden, unimodularen Matrizen in $\mathrm{Pos}\,(24;\mathbb{Z})$ mit $\mu(S) > 2$ gibt. Also ist die Klasse $\langle\, L_{24}\rangle$ durch die Bedingung (3) eindeutig bestimmt. Zur Konstruktion und Klassifikation von Gittern vergleiche man J.H. Conway und N.J.A. Sloane [1999]. Insbesondere findet man dort eine Konstruktion des Leech–Gitteriss.–Vs mit Hilfe von Codes und mit der Kneserschen Nachbarschaftsmethode

8*. Extremale Gitter. Das Minimum $\mu(S)$ (vgl. 1.5(1)) einer unimodularen Matrix $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ kann nicht beliebig groß werden. Aus der Ungleichung von Hermite in Korollar 1.5A folgt

$$\mu(S) \leq \left(\tfrac{4}{3}\right)^{(n-1)/2}.$$

Ist S gerade, so kann man diese Abschätzung wesentlich verbessern.

Satz. *Sei $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ gerade und unimodular. Dann gilt*

$$\mu(S) \leq 2\left[\tfrac{n}{24}\right] + 2.$$

Beweis. Wir führen den Beweis indirekt und nehmen an, dass $\mu(S) > 2\left[\frac{n}{24}\right] + 2$ gilt. Man betrachte die Theta–Reihe

$$\Theta(\cdot\,; S) \in \mathbb{M}_k\,,\ k = n/2,$$

nach Satz 6. Die Fourier–Koeffizienten erfüllen dann

$$\sharp(S, 0) = 1\,,\ \sharp(S, 2m) = 0\,,\ 1 \leq m \leq \left[\tfrac{k}{12}\right] + 1.$$

Wegen $\dim \mathbb{M}_k = \left[\frac{k}{12}\right] + 1$ nach III.4.1 für $k \equiv 0 \pmod 4$ erhalten wir einen Widerspruch zu Korollar III.6.5. □

Eine gerade, unimodulare Matrix $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ mit $\mu(S) = 2\left[\frac{n}{24}\right] + 2$ nennen wir *extremal*. Ist G ein gerades, selbstduales Gitter in einem euklidischen Vektorraum (V, σ), so heißt G *extremal*, wenn die zugehörige Gram–Matrix extremal ist, d. h.

$$\sigma(g, g) \geq 2\left[\tfrac{n}{24}\right] + 2 \text{ für alle } g \in G\,,\ g \neq 0.$$

Es ist nun wesentlich zu zeigen, dass $\beta_k(0) \neq 0$ gilt.

Satz. *Für gerades $k \geq 4$ gilt*

$$(-1)^{k/2}\beta_k(0) < 0.$$

Beweis. (i) Sei $k \equiv 2 \pmod 4$. Dann gilt

$$G^*_{12t-k+2} = G_4^{*\nu}\ ,\ \nu \in \{0,1,2\},$$

wenn man 4.2(2) und 2.1(10) beachtet. Aus (3) und (5) folgt dann

$$\beta_k(m) > 0 \quad \text{für alle} \quad m \geq -t.$$

(ii) Sei $k \equiv 0 \pmod 4$, $k \equiv 4\nu \pmod{12}$ mit $\nu \in \{0,1,2\}$. Dann gilt

$$G^*_{k-12t+12} = G_4^{*\nu}.$$

Verwendet man (4) und 2.4(1), so liefert eine einfache Rechnung

$$\begin{aligned} 2\pi i \cdot g_k &= -G_4^{*-\nu} \cdot \Delta^{*1-t} \cdot \frac{dj}{d\tau} = \frac{3}{\nu-3}\Delta^{*1-t-\nu/3} \cdot \frac{dj^{1-\nu/3}}{d\tau} \\ &= \frac{3}{\nu-3}\frac{d(G_4^{*3-\nu}\cdot\Delta^{*-t})}{d\tau} + \frac{3t+\nu-3}{(3-\nu)t}G_4^{*3-\nu}\cdot\frac{d\Delta^{*-t}}{d\tau}\ . \end{aligned}$$

Der letzten Darstellung entnimmt man, dass $\beta_k(0)$ auch der konstante Koeffizient in der FOURIER–Entwicklung von

$$\frac{1}{2\pi i}\cdot\frac{3t+\nu-3}{(3-\nu)t}\cdot G_4^{*3-\nu}\cdot\frac{d}{d\tau}\Delta^{*-t}$$

ist. Alle FOURIER–Koeffizienten $\alpha(m)$, $m \geq 0$, von $G_4^{*3-\nu}$ sind positiv. Aus (5) schließt man, dass für die FOURIER–Koeffizienten $\gamma(m)$ von $\frac{1}{2\pi i}\cdot\frac{d\Delta^{*-t}}{d\tau}$ gilt

$$\gamma(m) < 0 \quad \text{für} \quad -t \leq m < 0 \quad \text{und} \quad \gamma(0) = 0.$$

Daraus folgt

$$\beta_k(0) < 0. \qquad \square$$

Wir beschreiben nun die „extremale“ Modulform.

Korollar. *Sei $k \geq 4$ gerade. Es gibt genau eine ganze Modulform $f \in \mathbb{M}_k$ mit der Eigenschaft*

(9) $$\alpha_f(0) = 1 \quad \textit{und} \quad \alpha_f(m) = 0 \quad \textit{für}\ \ 0 < m < t.$$

Dann gilt

$$(-1)^{k/2}\alpha_f(t) > 0.$$

Beweis. Der Fall $t = 1$ ist klar. Im Fall $t > 1$ folgt aus der Betrachtung der FOURIER–Reihen, dass man $\gamma_\nu \in \mathbb{Q}$ finden kann, so dass

JOURNAL OF ALGEBRA 36, 68–76 (1975)

Upper Bounds for Modular Forms, Lattices, and Codes

C. L. MALLOWS

Bell Laboratories, Murray Hill, New Jersey 07974

A. M. ODLYZKO*

Mathematics Department, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

AND

N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by Walter Feit

Received March 12, 1974

Let $W(z) = 1 + A_d\, e^{2\pi i d z} + A_{d+1}\, e^{2\pi i (d+1) z} + \cdots$ be a modular form of weight n for the full modular group. Then for every constant b there exists an $n_0 = n_0(b)$ such that if $d \geqslant n/6 - b$ and $n \geqslant n_0$, then one of $A_d, A_{d+1}, \ldots,$ has a negative real part. This implies that there is no even unimodular lattice in E^n, for $n \geqslant n_0$, having minimum nonzero squared length $\geqslant n/12 - b$. A similar argument shows that there is no binary self-dual code of length $n \geqslant n_0$ having all weights divisible by 4 and minimum nonzero weight $\geqslant n/6 - b$. A corresponding result holds for ternary codes.

1. MODULAR FORMS

Let $E_2(z) = 1 + 240 \sum_{r=1}^{\infty} \sigma_3(r)\, q^r$, $E_3(z) = 1 - 504 \sum_{r=1}^{\infty} \sigma_5(r)\, q^r$, $\Delta(z) = q \prod_1^{\infty} (1 - q^r)^{24}$, where $q = e^{2\pi i z}$, $\sigma_\lambda(r) = \sum_{d|r} d^\lambda$. Then E_2, E_3, Δ are modular forms (for the full modular group) of weights 2, 3, 6, respectively. Furthermore any modular form of weight n can be written as

$$W(z) = \sum_{2s+3t=n} c_s E_2{}^s E_3{}^t, \tag{1}$$

* Research supported by the Hertz Foundation.

where there are $\mu + 1$ complex constants c_s in the sum, and $\mu = [n/6] - 1$ if $n \equiv 1 \pmod 6$, $\mu = [n/6]$ if $n \not\equiv 1 \pmod 6$ [8, 13].

THEOREM 1. *Let b be any constant. Then there exists a constant $n_0(b)$ such that if*

$$W(q) = 1 + A_d q^d + A_{d+1} q^{d+1} + \cdots$$

is a modular form of weight $n \geqslant n_0(b)$ with $d \geqslant \mu + 1 - b$, then one of the coefficients A_d, A_{d+1},... has a negative real part.

Remark. An explicit bound for $n_0(b)$ could also be obtained by our methods.

2. Lattices

Let Λ be an even unimodular lattice in Euclidean space E^n, where n is a multiple of 8. Let A_r be the number of lattice points of squared length $2r$, let d be the smallest nonzero squared length of any lattice point, and let

$$W(z) = \sum_{r=0}^{\infty} A_r q^r = 1 + A_{d/2} q^{d/2} + A_{d/2+1} q^{d/2+1} + \cdots .$$

Then $W(z)$ is a modular form of weight $n/4$ [8, 13]. Lattices with $d = 2[n/24] + 2$ are known for small n [9, 10], and have connections with simple groups [4, 5]. However, Theorem 1 implies:

COROLLARY. *If b is any constant, an even unimodular lattice with $d \geqslant 2[n/24] + 2 - 2b$ does not exist for $n \geqslant n_0(b)$.*

[The proof shows that for $d = 2[n/24] + 2$, the coefficient $A_{d/2+1}$ first goes negative when n is about 41,000. But other coefficients may go negative before this.]

3. Codes

Let $n = 8j = 24\mu + 8\nu$, $\nu = 0$, 1 or 2. Let $\mathscr{C}$ be a binary self-dual code of length n (i.e., a self-dual subspace of $GF(2)^n$) with the property that the weight of every codeword is a multiple of 4. Let A_r be the number of codewords of weight $4r$, and let $W(q) = \sum_{r=0}^{n/4} A_r q^r$. Then $W(q)$ can be written as

$$W(q) = \sum_{s=0}^{\mu} c_s f^{j-3s} g^s \tag{2}$$

for suitable real constants c_s, where $f = 1 + 14q + q^2$, $g = q(1-q)^4$ [6, 2, 11]. Codes with minimum nonzero weight $4[n/24] + 4$ are known for small n [12]. Besides having high error-correcting capability, such codes are of combinatorial interest because they contain 5-designs [1]. However, we show:

THEOREM 2. *Let b be any constant. Suppose the c_s in (2) are chosen so that $W(q) = 1 + A_{d/4}q^{d/4} + A_{d/4+1}q^{d/4+1} + \cdots$, where $d \geqslant 4[n/24] + 4 - 4b$. Then one of the coefficients $A_{d/4}, A_{d/4+1}, \ldots$ is negative, for all sufficiently large n.*

COROLLARY. *If b is any constant, then a binary self-dual code of length n with all weights divisible by 4 and with minimum nonzero weight $d \geqslant 4[n/24] + 4 - 4b$ does not exist, for all sufficiently large n.*

This result was proved for $b < 0$ in [12], and for $b = 0$ by Goethals, MacWilliams, and Mallows [7] using a different method.

When $b = 0$, $d = 4[n/24] + 4$, the proof shows that $A_{d/4+1}$ first goes negative when n is about 3720. We have confirmed this by computer: for $n = 3720$, $b = 0$, $d = 624$, we find $W(q) = 1 + A_{156}q^{156} + A_{157}q^{157} + \cdots + A_{774}q^{774} + q^{930}$, with $A_{156} = 1.16\ldots \cdot 10^{170}$, $A_{157} = -5.84\ldots \cdot 10^{170}$, $A_i > 0$ for $158 \leqslant i \leqslant 465$, and $A_{930-i} = A_i$ for all i.

A similar argument establishes the corresponding result for self-dual codes over $GF(3)$:

THEOREM 3. *If b is any constant, then a ternary self-dual code of length n with minimum nonzero weight $\geqslant 3[n/12] + 3 - 3b$ does not exist, for all sufficiently large n.*

This result was proved for $b \leqslant 0$ in [12]. For $b = 0$, the first negative coefficient in $W(q)$ occurs when $n = 72$, as found by J. N. Pierce (see [6]).

4. TWO LEMMAS

LEMMA 1. *Suppose $G(q)$, $H(q)$ are analytic inside the circle $|q| = 1$ and satisfy:* (i) *$H(q) = \sum_{s=0}^{\infty} H_s q^s$ with $H_0 > 0$, $H_1 > 0$, and $H_s \geqslant 0$ for $s \geqslant 2$;* (ii) *if $F(y) = e^{2\pi y}H(e^{-2\pi y})$, then $F'(y) = 0$ has a solution $y = y_0$ in the range $y > 0$, with $F(y_0) = c_1 > 0$, $F''(y_0)/F(y_0) = c_2 > 0$, $G(e^{-2\pi y_0}) \neq 0$. Then β_r, the coefficient of q_r in $G(q)\,H(q)^r$, satisfies*

$$\beta_r \sim \frac{2\pi}{(rc_2)^{1/2}}\, G(e^{-2\pi y_0})\, c_1^{\ r}, \qquad as \quad r \to \infty.$$

Proof. From Cauchy's formula

$$\beta_r = \int e^{-2\pi i z r} G(e^{2\pi i z})\, H(e^{2\pi i z})^r \, dz$$

where the integral is along the path $z = x + iy$, $-\frac{1}{2} \leqslant x \leqslant \frac{1}{2}$, y fixed >0. We estimate this integral by the saddle-point method. From (i), $| e^{-2\pi i z} H(e^{2\pi i z})| \leqslant e^{2\pi y} H(e^{-2\pi y})$, with equality for $-\frac{1}{2} \leqslant x \leqslant \frac{1}{2}$ only at $x = 0$. Thus the saddle point is at $\xi = 0 + iy_0$, and we choose $y = y_0$ in the integral. Let $f(z) = e^{-2\pi i z} H(e^{2\pi i z})$. Since H is analytic,

$$\frac{\partial}{\partial x} \ln f(z) \Big|_{z=\xi} = \frac{1}{i} \frac{\partial}{\partial y} \ln f(z) \Big|_{z=\xi} = \frac{F'(y_0)}{iF(y_0)} = 0,$$

$$\frac{\partial^2}{\partial x^2} \ln f(z) \Big|_{z=\xi} = -\frac{\partial^2}{\partial y^2} \ln f(z) \Big|_{z=\xi} = -\frac{F''(y_0)}{F(y_0)} = -c_2\,.$$

The result now follows by standard techniques [3, Section 4.4]. (Note that in that reference a_3, a_4 ,... do not have to be real for the result to hold.)

LEMMA 2. *Let $\beta_{s,t}$ $(0 \leqslant t \leqslant s \leqslant n)$ be numbers such that $1/c \leqslant |\beta_{st}| \leqslant c$ for some constant $c > 0$. Then there exists a constant $d = d(c, n) > 0$, such that*

$$\sum_{s=0}^{n} \Big| \sum_{t=0}^{s} \beta_{st} X_t \Big| \geqslant d \sum_{t=0}^{n} | X_t | \,.$$

Proof. By induction on n. The result is true for $n = 0$. Now suppose $n > 0$ and the result is true for $n - 1$. Let Q denote the expression on the left. By the induction hypothesis, there exists $d_1 > 0$ such that

$$Q \geqslant d_1 \sum_{0}^{n-1} | X_t | + | \beta_{n0} X_0 + \cdots + \beta_{nn} X_n |$$

$$= d_1 \left(\sum_{0}^{n-1} | X_t | + | B_0 X_0 + \cdots + B_n X_n | \right),$$

where $B_t = \beta_{nt}/d_1$. Note that $1/cd_1 \leqslant | B_t | \leqslant c/d_1$.

Case (i). Suppose $| X_n | \geqslant 2c^2 \sum_0^{n-1} | X_t |$. Then

$$\Big| \sum_{0}^{n-1} B_t X_t \Big| \leqslant \frac{c}{d_1} \sum_{0}^{n-1} | X_t | \leqslant \frac{1}{2cd_1} | X_n | \leqslant \frac{1}{2} | B_n X_n |,$$

$$\Big| \sum_{0}^{n} B_t X_t \Big| \geqslant | B_n X_n | - \Big| \sum_{0}^{n-1} B_t X_t \Big| \geqslant \frac{1}{2} | B_n X_n | \geqslant \frac{1}{2cd_1} | X_n |,$$

and so

$$Q \geqslant d_1 \min \left\{1, \frac{1}{2cd_1}\right\} \sum_0^n |X_t|.$$

Case (ii). On the other hand, if $|X_n| < 2c^2 \sum_0^{n-1} |X_t|$, then

$$\sum_0^n |X_t| \leqslant (1 + 2c^2) \sum_0^{n-1} |X_t|$$

and so

$$Q \geqslant d_1 \sum_0^{n-1} |X_t| \geqslant \frac{d_1}{1 + 2c^2} \sum_0^n |X_t|.$$

In either case, $Q \geqslant d \sum_0^n |X_t|$, where $d = \min\{d_1, 1/2c, d_1/(1 + 2c^2)\}$.

5. The Proofs of Theorems 1, 2 and 3

Proof of Theorem 1

Part (I), *n even.* Let $n = 2j = 6\mu + 2\nu$, $\nu = 0$, 1 or 2. Since $\Delta = (1/1728)(E_2^3 - E_3^2)$, we can express $W(z)$ in terms of E_2 and Δ. We first treat the case $b \leqslant 0$, $d \geqslant \mu + 1$. Suppose

$$W(z) = \sum_{s=0}^{\mu} a_s E_2^{j-3s} \Delta^s, \tag{3}$$

where the a_s are chosen so that

$$W(z) = 1 + \sum_{r=\mu+1}^{\infty} A_r q^r. \tag{4}$$

Since both E_2 and Δ have real coefficients in their q-expansions, both the a_s and the A_r are real. We will show $A_{\mu+1} > 0$ for all n, and $A_{\mu+2} = -A_{\mu+1}(24\mu + O(1)) < 0$ as $n \to \infty$.

Let $\varphi = \varphi(q) = \Delta / E_2^3$. We expand E_2^{-j} in powers of φ using Bürmann's theorem [14, p. 128]:

$$E_2^{-j} = \sum_{s=0}^{\infty} \alpha_s \varphi^s, \tag{5}$$

where

$$\begin{aligned} \alpha_s &= \frac{1}{s!} \frac{d^{s-1}}{dq^{s-1}} \left\{ \frac{dE_2^{-j}}{dq} \left(\frac{q}{\varphi} \right)^s \right\}_{q=0} \\ &= \frac{-j}{s!} \frac{d^{s-1}}{dq^{s-1}} \{E_2' E_2^{3s-j-1} h^s\}_{q=0} \end{aligned} \tag{6}$$

where $h(q) = \prod_{r=1}^{\infty} (1 - q^r)^{-24}$. In particular,

$$\alpha_{\mu+1} = \frac{-j}{(\mu+1)!} \frac{d^{\mu}}{dq^{\mu}} \{E_2' E_2^{2-\nu} h^{\mu+1}\}_{q=0}, \tag{7}$$

$$\alpha_{\mu+2} = \frac{-j}{(\mu+2)!} \frac{d^{\mu+1}}{dq^{\mu+1}} \{E_2' E_2^{5-\nu} h^{\mu+2}\}_{q=0}. \tag{8}$$

From (3), (4), (5) we see that $a_s = \alpha_s$ $(0 \leqslant s \leqslant \mu)$ and that the $\alpha_s (s > \mu)$ and A_r are related by

$$\sum_{r=\mu+1}^{\infty} A_r q^r = -\sum_{s=\mu+1}^{\infty} \alpha_s E_2^{j-3s} \Delta^s.$$

Equating coefficients of $q^{\mu+1}$, $q^{\mu+2}$ we find

$$A_{\mu+1} = -\alpha_{\mu+1}, \tag{9}$$

$$A_{\mu+2} = -\alpha_{\mu+2} + \alpha_{\mu+1}(24\mu - 240\nu + 744). \tag{10}$$

That $\alpha_{\mu+1} < 0$ and $A_{\mu+1} > 0$ follows immediately from (7) and (9) since E_2 and h have positive coefficients. We now show that $|\alpha_{\mu+2}/\alpha_{\mu+1}|$ is bounded, which implies using (10) that $A_{\mu+2} = -A_{\mu+1}(24\mu + O(1)) < 0$ as $n \to \infty$.

We apply Lemma 1 with $G(q) = G_1(q) = E_2'(q)\, E_2^{2-\nu}(q)\, h(q)$, $H(q) = h(q)$. Now

$$\frac{F'(y)}{F(y)} = 2\pi - 48\pi \sum_{r=1}^{\infty} \frac{r}{e^{2\pi r y} - 1},$$

$$\frac{F''(y)}{F(y)} = \left(\frac{F'(y)}{F(y)}\right)^2 + 96\pi^2 \sum_{r=1}^{\infty} \frac{r^2 e^{2\pi r y}}{(e^{2\pi r y} - 1)^2}.$$

Thus for $y > 0$, $F(y) > 0$ and $F''(y) > 0$. Also $F'(y)/F(y)$ is a monotonic increasing function of y, which is negative for small y and positive for large y. Therefore $F'(y) = 0$ has a unique solution for $y > 0$ (at $y = y_0 = 0.52352\ldots$). Thus hypothesis (ii) of the lemma is satisfied. Then, from (7),

$$\alpha_{\mu+1} \sim -2\pi j c_2^{-1/2} \mu^{-3/2} G_1(e^{-2\pi y_0})\, c_1^{\mu}, \qquad \text{as} \quad \mu \to \infty,$$

where c_1 $(= 69.1\ldots)$, c_2 are constants. Similarly from (8), with $G_2(q) = E_2'(q)\, E_2^{5-\nu}(q)\, h(q)$, $H(q) = h(q)$,

$$\alpha_{\mu+2} \sim -2\pi j c_2^{-1/2} \mu^{-3/2} G_2(e^{-2\pi y_0})\, c_1^{\mu+1}, \qquad \text{as} \quad \mu \to \infty.$$

Hence $|\alpha_{\mu+2}/\alpha_{\mu+1}|$ is bounded. (In fact it approaches a limit of about 1.64×10^5 as $\mu \to \infty$.)

We now treat the case $b > 0$, $d = \mu + 1 - b$. Let $W_{\text{ext}}(z)$ denote the extremal $W(z)$ defined by (3), (4). We complete part (I) of the proof by showing that no matter how the coefficients $x_0, \ldots, x_{b-1}$ are chosen,

$$\begin{aligned} W(z) &= W_{\text{ext}}(z) + \sum_{s=0}^{b-1} x_{b-1-s} E_2^{\nu+3s} \Delta^{\mu-s} \\ &= 1 + \sum_{r=d}^{\infty} A_r' q^r \qquad \text{(say)} \end{aligned} \tag{11}$$

always contains a coefficient A_r' with negative real part when n is sufficiently large. Since E_2 and Δ have real coefficients, we may assume that the x_i are real (otherwise replace the x_i by their real parts). In fact, we show that the assumptions

$$A_d' \geqslant 0, A_{d+1}' \geqslant 0, \ldots, A_{\mu+2}' \geqslant 0, \tag{12}$$

lead to a contradiction for large n. Upon expanding (11), the $b + 2$ inequalities (12) become, with $m = 24\mu$,

$$x_0 \geqslant 0,$$

$$\sum_{t=0}^{s} x_t \left(\frac{(-m)^{s-t}}{(s-t)!} + O(m^{s-t-1}) \right) \geqslant 0, \qquad s = 1, \ldots, b-1,$$

$$A_{\mu+1} + \sum_{t=0}^{b-1} x_t \left(\frac{(-m)^{b-t}}{(b-t)!} + O(m^{b-t-1}) \right) \geqslant 0,$$

$$-mA_{\mu+1} \left(1 + O\left(\frac{1}{m}\right) \right) + \sum_{t=0}^{b-1} x_t \left(\frac{(-m)^{b+1-t}}{(b+1-t)!} + O(m^{b-t}) \right) \geqslant 0.$$

Set

$$X_t = \frac{x_t}{m^t} \qquad (0 \leqslant t \leqslant b-1), \qquad X_b = \frac{A_{\mu+1}}{m^b}, \qquad X_{b+1} = 0,$$

and

$$\beta_{s,t} = \frac{(-1)^{s-t}}{(s-t)!} \qquad \text{for} \quad 0 \leqslant t \leqslant s \leqslant b+1.$$

The inequalities now reduce to

$$\sum_{t=0}^{s} \left(\beta_{s,t} + O\left(\frac{1}{m}\right) \right) X_t \geqslant 0, \qquad s = 0, \ldots, b+1. \tag{13}$$

Let $\gamma_s = (b+1)!/(b+1-s)!$, and observe that $\sum_{s=t}^{b+1} \beta_{s,t}\gamma_s = 0$ for $t = 0,\dots, b$. We obtain the contradiction by evaluating in two ways the sum

$$\sum_{t=0}^{b+1} X_t \sum_{s=t}^{b+1} \left(\beta_{s,t} + O\left(\frac{1}{m}\right)\right) \gamma_s .$$

On the one hand it equals

$$\sum_{t=0}^{b+1} X_t \sum_{s=t}^{b+1} O\left(\frac{1}{m}\right) \gamma_s \leqslant \frac{c_3(b)}{m} \sum_{t=0}^{b+1} | X_t |,$$

while on the other hand it is equal to (from (13))

$$\sum_{s=0}^{b+1} \gamma_s \sum_{t=0}^{s} \left(\beta_{s,t} + O\left(\frac{1}{m}\right)\right) X_t = \sum_{s=0}^{b+1} \gamma_s \left| \sum_{t=0}^{s} \left(\beta_{s,t} + O\left(\frac{1}{m}\right)\right) X_t \right|,$$

and for m sufficiently large,

$$\left| \beta_{s,t} + O\left(\frac{1}{m}\right)\right| \geqslant c_4(b) > 0.$$

It now follows from Lemma 2, with $\beta_{s,t}$ in the lemma replaced by $\beta_{s,t} + O(1/m)$, that the sum is

$$\geqslant c_5(b) \sum_{t=0}^{b+1} | X_t |.$$

This is a contradiction for large m, since X_b is nonzero.

Part (II), *n odd*. Let $n = 2j + 3 = 6\mu + 2\nu + 3$, $\nu = 0$, 1 or 2. Instead of (3) we write

$$W(z) = \sum_{s=0}^{\mu} a_s E_2^{j-3s} E_3 \Delta^s,$$

and expand $E_2^{-j}E_3^{-1}$ in powers of φ. The proof is now parallel to Part (I) and we omit the details.

Proof of Theorem 2. This is also parallel to Part (I), with E_2, Δ and $m = 24\mu$ replaced by f, g, and $m = 4\mu$. Again the details are omitted.

Proof of Theorem 3. This is again parallel to Part (I), with E_2, Δ and $m = 24\mu$ replaced by $1 + 8q$, $q(1-q)^3$, and $m = 3\mu$.

ACKNOWLEDGMENTS

We thank Harold M. Stark for several helpful discussions.

REFERENCES

1. E. F. ASSMUS, JR., AND H. F. MATTSON, JR., New 5-Designs, *J. Combinatorial Theory*, **6** (1969), 122–151.
2. E. R. BERLEKAMP, F. J. MACWILLIAMS, AND N. J. A. SLOANE, Gleason's Theorem on Self-Dual Codes, *IEEE Trans. Info. Theory* **IT-18**, (1972), 409–414.
3. N. G. DE BRUIJN, "Asymptotic Methods in Analysis," 3rd edition, North-Holland, Amsterdam, Netherlands, 1970.
4. J. H. CONWAY, A Characterization of Leech's Lattice, *Inventiones math.* **7** (1969), 137–142.
5. J. H. CONWAY, Groups, lattices, and quadratic forms, *in* "Computers in Algebra and Number Theory," (G. Birkhoff and M. Hall, Jr., Eds.), pp. 135–139, American Math. Soc., Providence, RI, 1971.
6. A. M. GLEASON, Weight polynomials of self-dual codes and the MacWilliams identities, *in* "Actes, Congr. Int. Math.," pp. 211–215, Vol. 3, 1970, Gauthier-Villars, Paris, 1971.
7. J.-M. GOETHALS, F. J. MACWILLIAMS, AND C. L. MALLOWS, 1973, unpublished.
8. R. C. GUNNING, "Lectures on Modular Forms," Princeton University Press, Princeton, NJ, 1962.
9. J. LEECH, Notes on sphere packings, *Can. J. Math.* **19** (1967), 251–267.
10. J. LEECH AND N. J. A. SLOANE, Sphere packings and error-correcting codes, *Can. J. Math.* **23** (1971), 718–745.
11. F. J. MACWILLIAMS, C. L. MALLOWS, AND N. J. A. SLOANE, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Info. Theory*, **IT-18** (1972), 794–805.
12. C. L. MALLOWS, AND N. J. A. SLOANE, An upper bound for self-dual codes, *Information and Control* **22** (1973), 188–200.
13. J.-P. SERRE, "Cours d'Arithmetique," Presses Universitaires de France, Paris, 1970. (English translation, Springer, New York, 1973.)
14. E. T. WHITTAKER AND G. N. WATSON, A Course of Modern Analysis, 4th edition, Cambridge University Press, Cambridge, 1963.