Sphere-packings, codes, lattices and theta-functions

MATHEMATICAL CENTRE TRACTS 106 (1979) 141-160.

10

SPHERE-PACKINGS, CODES, LATTICES AND THETA-FUNCTIONS

J.H. VAN LINT

INTRODUCTION

During the year 1977-1978 the Combinatorial Theory Seminar Eindhoven discussed several connections between the topics mentioned in the title of this chapter. We shall now give a brief survey of the ideas, concepts, and theorems which were treated. Obviously much will have to be skipped and our proofs will generally be sketchy. The reader who decides to become interested in this subject can find several excellent treatments in the literature. Our main sources are C.A. ROGERS, *Packing and Covering* [4] for the classical theory of sphere-packings, T.M. APOSTOL, *Modular Functions and Dirichlet Series* [1] for the theory of modular forms, N.J.A. SLOANE, *Binary Codes, Lattices, and Sphere-packings* [6]. For a short treatment of modular forms, lattices and quadratic forms we also refer the reader to J.P. SERRE, *A Course in Arithmetic* [5].

1. SPHERE-PACKING

In the following K denotes a sphere in $\mathbb{R}^n$. The volume of a subset A of $\mathbb{R}^n$ is denoted by $\mu(A)$. If $(\underline{a}_i)_{i\in\mathbb{N}}$ is a sequence of points in $\mathbb{R}^n$ we denote the set of translates $\{\underline{a}_i + K \mid i \in \mathbb{N}\}$ of K by $\mathcal{K}$. If no point of $\mathbb{R}^n$ is an interior point of more than one of these translated spheres we call $\mathcal{K}$ a *sphere-packing*. Let C_s be the cube $\{\underline{x} \in \mathbb{R}^n \mid -\tfrac{1}{2}s \le x_i \le \tfrac{1}{2}s,\ 1 \le i \le n\}$. For a set A we define $s(A) := \min\{s \mid A \subset C_s\}$.

DEFINITIONS 1.1.

$$\rho_+(\mathcal{K},C_s) := \mu(C_s)^{-1} \sum_{i:K+\underline{a}_i\cap C_s\neq\emptyset} \mu(K+\underline{a}_i)$$

$$\rho_-(K,C_s) := \mu(C_s)^{-1} \sum_{i:K+\underline{a}_i \subset C_s} \mu(K+\underline{a}_i),$$

$$\rho_+(K) := \limsup_{s\to\infty} \rho_+(K,C_s),$$

$$\rho_-(K) := \liminf_{s\to\infty} \rho_-(K,C_s).$$

$\rho_+(K)$ and $\rho_-(K)$ are called the *upper density* and *lower density* of K.

THEOREM 1.2. $\rho_+(K) \leq 1$.

PROOF. Choose b such that $K \subset C_b$. Then $\rho_+(K,C_s) \leq (s+2b)^n/s^n$. □

We are interested in the *packing density* $\Delta_n = \Delta(K)$ of spheres in $\mathbb{R}^n$ which is defined to be the supremum of $\rho_+(K)$ over all sphere-packings K. Clearly Δ_n depends only on n and not on the radius of K. If $\underline{e}_1,\ldots,\underline{e}_n$ is a basis for $\mathbb{R}^n$ we call the set $\Lambda := \mathbb{Z}\underline{e}_1 \oplus \mathbb{Z}\underline{e}_2 \oplus \ldots \oplus \mathbb{Z}\underline{e}_n$ a *lattice* in $\mathbb{R}^n$ and the vectors $\underline{e}_i$ a *basis* for Λ.

The matrix M with the vectors $\underline{e}_i$ as columns is called a *generator matrix* for the lattice. The *determinant* of Λ is defined to be

$$\det \Lambda = |\det M|.$$

If in (1.1) we make the restriction that the sequence $(\underline{a}_i)_{i\in\mathbb{N}}$ consists of the points of some lattice then the corresponding *lattice packing density* is denoted by $\Delta_L(K)$. If we allow the set $\{\underline{a}_i \mid i \in \mathbb{N}\}$ to be a union of a finite number of translates of a lattice we obtain in the same way $\Delta_p(K)$, the *periodic packing density*.

THEOREM 1.3. $\Delta_L(K) \leq \Delta_p(K) \leq \Delta(K)$.

PROOF. Trivial. □

The definitions and theorems given above can immediately be generalized to other sets than the sphere K (e.g. ellipsoids). Let T be a nonsingular affine transformation of $\mathbb{R}^n$. Let Λ be the lattice $(s\mathbb{Z})^n$ and let $\{\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_N\}$ be a set of points. We consider a sphere-packing $K := \{K+\underline{a}_i+\underline{b}_j \mid 1 \leq i \leq N,\ j \in \mathbb{N}\}$ where $\underline{b}_j$ runs through the lattice Λ. We also consider TK.

THEOREM 1.4. $\rho_+(TK) = \rho_-(TK) = \rho_+(K) = \rho_-(K) = N\mu(K)/\mu(C_s)$.

PROOF.

(i) W.l.o.g. we may assume that each $K+\underline{a}_i$ has a point in C_s.

(ii) TK is obtained by translating TK over all $T(\underline{a}_i+\underline{b}_j) - T(\underline{0})$.

(iii) Let $G_1 := C_{s_1}$ where $s_1 > 2s(TC_s) + 2s(TK)$, $G_2 := C_{s_1-2s(TK)}$, $G_3 := C_{s_1-2s(TC_s)-2s(TK)}$. For each $\underline{p} \in G_3$ there is a j such that $\underline{p} \in T(C_s+\underline{b}_j) \subset G_2$. Number the vectors $\underline{b}_j$ in such a way that $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_M$ correspond to points $\underline{p} \in G_3$ as described above. Then we have

(a) $$M\mu(TC) \geq \mu(G_3) = (s_1-2s(TC_s) - 2s(TK))^n.$$

Clearly all the $T(K+\underline{a}_i+\underline{b}_j)$, $1 \leq i \leq N$, $1 \leq j \leq M$ are contained in G_1. Therefore

(b) $$\rho_-(TK,G_1) \geq NM\mu(TK)/\mu(G_1).$$

From (a) and (b) we find

(c) $$\rho_-(TK,G_1) \geq N \cdot \frac{\mu(TK)}{\mu(TC_s)} \cdot \left(1 - 2\,\frac{s(TC_s)+s(TK)}{s_1}\right)^n.$$

Observe that $\mu(TK)/\mu(TC_s) = \mu(K)/\mu(C_s)$ and let $s_1 \to \infty$. Then (c) implies

$$\rho_-(TK) \geq N\mu(K)/\mu(C_s).$$

(iv) In the same way we have $\rho_+(TK) \leq N\mu(K)/\mu(C_s)$ and then the theorem follows from the fact that we may take T to be the identity mapping. □

THEOREM 1.5. *If K is a sphere-packing corresponding to the lattice Λ then* $\rho_+(K) = \rho_-(K) = \mu(K)/\det \Lambda$.

PROOF. Let T be the transformation which maps $\mathbb{Z}^n$ onto Λ. In Theorem 1.4 replace K by $T^{-1}K$ and take $s = 1$. □

THEOREM 1.6. *Let T be a nonsingular affine transformation of $\mathbb{R}^n$. We have*

$$\Delta(TK) = \Delta_P(K) = \Delta(K), \qquad \Delta_L(TK) = \Delta_L(K).$$

PROOF. The second part is trivial. For the first part we only have to show that $\Delta_p(K) = \Delta(K)$ and apply Theorem 1.4. For every $\varepsilon > 0$ there is a system K_ε of translates of K such that $\rho_+(K_\varepsilon) > (1-\varepsilon)\Delta(K)$. Choose s so large that $\{s/(s+2s(K))\}^n > (1-\varepsilon)$ and $\rho_+(K_\varepsilon, C_s) > (1-\varepsilon)\,\rho_+(K_\varepsilon)$. The sets of K_ε which have a point in C_s are completely contained in $C_{s'}$, where $s' := s+2s(K)$. Let these sets be $\underline{a}_1+K,\ldots,\underline{a}_N+K$ and let $\underline{b}_j$ run through the lattice $(s'\mathbb{Z})^n$. The corresponding periodic packing K' has

$$\rho_+(K') = \rho_-(K') \geq (1-\varepsilon)^3\Delta(K).$$

The theorem now follows from Theorem 1.3. □

We now wish to establish a bound for Δ_n due to C.A. ROGERS (cf. [3]). Consider a sequence of points $\underline{a}_1,\underline{a}_2,\ldots$ in $\mathbb{R}^n$ with finite covering radius and mutual distances ≥ 2 (the *covering radius* equals, by definition, inf $\{R \in \mathbb{R} \mid \min_i d(\underline{a}_i,\underline{x}) \leq R$ for all $\underline{x} \in \mathbb{R}^n\}$). With each point $\underline{a}$ of this sequence we associate a *Voronoi-polyhedron* $\Pi(\underline{a})$ consisting of the points $\underline{x}$ such that $d(\underline{a},\underline{x}) = \min_i d(\underline{a}_i,\underline{x})$. Subsequently each polyhedron is dissected in the following canonical way. Components will be simplices $\underline{c}_0\underline{c}_1\ldots\underline{c}_n$ where $\underline{c}_0 := \underline{a}$, $\underline{c}_1$ is the point closest to $\underline{a}$ on some (n-1)-dimensional face of $\Pi(\underline{a})$ and all other $\underline{c}_i$ are on this same face, $\underline{c}_2$ is the point closest to $\underline{a}$ on some (n-2)-dimensional face of the previous face, etc.. Clearly the angle between $\underline{c}_i - \underline{c}_0$ and $\underline{c}_j - \underline{c}_i$ (at $\underline{c}_i$) is not acute if $j > i$, i.e. if we take $\underline{c}_0$ as origin we have $\langle\underline{c}_j,\underline{c}_i\rangle \geq \langle\underline{c}_i,\underline{c}_i\rangle$. We now need a lemma known as *Blichfeldt's inequality* (cf. [4]).

LEMMA 1.7. *If* $\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_{k+1}$ *all have distance* d *to* $\underline{0}$ *and mutual distances at least* 2 *then* $d \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

PROOF. $2k(k+1) \leq \sum_{1\leq i<j\leq k+1} \langle\underline{a}_i-\underline{a}_j,\underline{a}_i-\underline{a}_j\rangle = (k+1)\sum_{i=1}^{k+1}\langle\underline{a}_i,\underline{a}_i\rangle - \langle\sum\underline{a}_i,\sum\underline{a}_i\rangle$
$\leq (k+1)^2d^2$. □

COROLLARY. *If* $\underline{x}$ *is on an* (n-k)*-dimensional face of* $\Pi(a)$ *then* $d(\underline{x},\underline{a}) \geq (\frac{2k}{k+1})^{\frac{1}{2}}$.

This corollary and our observation above concerning $\langle\underline{c}_i,\underline{c}_j\rangle$ establish the following lemma.

LEMMA 1.8. *For each simplex* $\underline{c}_0\underline{c}_1\underline{c}_2\ldots\underline{c}_n$ $(\underline{c}_0 = \underline{0})$ *in the dissection of a Voronoi-polyhedron we have*

$$\langle \underline{c}_i, \underline{c}_j \rangle \geq \frac{2i}{i+1} \quad \textit{if} \quad j \geq i.$$

DEFINITION 1.9. Consider a regular simplex S in $\mathbb{R}^n$ with side 2 and the n+1 spheres of radius 1 centered at the vertices of the simplex. Let S_0 be the intersection of S with the union of the spheres. We define $\sigma_n := \mu(S_0)/\mu(S)$.

Let us look at such a simplex S, say with vertices $(\sqrt{2},0,0,\ldots,0)$, $(0,\sqrt{2},0,\ldots,0),\ldots,(0,0,\ldots,0,\sqrt{2})$ where these n+1 points are in the hyperplane defined by $\sum_{i=1}^{n+1} x_i = \sqrt{2}$ in $\mathbb{R}^{n+1}$. We divide S into n! congruent simplices as follows. Start with the centroid of S, next take the centroid of an (n-1)-face, the centroid of one of its (n-2)-faces, etc.,...,vertex. A typical subsimplex G has vertices $\underline{g}_i = (\frac{\sqrt{2}}{i+1}, \frac{\sqrt{2}}{i+1},\ldots,\frac{\sqrt{2}}{i+1}, 0,0,\ldots,0)$, (n-i coordinates 0), $(0 \leq i \leq n)$. We then have

(a) $$\langle g_i - g_0, g_j - g_0 \rangle = \frac{2i}{i+1} \quad \text{if } i \leq j$$

and furthermore if B is a sphere of radius 1 centered at $\underline{g}_0$ then

(b) $$\mu(B \cap G)/\mu(G) = \sigma_n.$$

THEOREM 1.10. $\Delta_n \leq \sigma_n$.

PROOF. Suppose $\Delta(K) > \sigma_n$. We assume K has radius 1. It follows from Theorem 1.6 that we can find an s and a corresponding periodic packing K of spheres $K+\underline{a}_i+\underline{b}_j$ $(\underline{b}_j \in (s\mathbb{Z})^n,\ 1 \leq i \leq N)$ such that $\rho_+(K) > \sigma_n$, i.e. $N\mu(K)/\mu(C_s) > \sigma_n$. The system of points $\underline{a}_i + \underline{b}_j$ $(1 \leq i \leq N, j \in \mathbb{N})$ has covering radius $R \leq s\sqrt{n}$. Consider the corresponding Voronoi-polyhedra and their canonical dissection into simplices. This is a periodic dissection of $\mathbb{R}^n$. Let $T_1, T_2, \ldots, T_M$ be representatives of the different classes of simplices mod $(s\mathbb{Z})^n$. One easily sees that

$$\mu(C_s) = \sum_{k=1}^{M} \mu(T_k),$$

$$N\mu(K) = \sum_{k=1}^{M} \sum_{i=1}^{N} \sum_{j=1}^{\infty} \mu([K+\underline{a}_i+\underline{b}_j] \cap T_k).$$

However, each simplex of a Voronoi-polyhedron meets only the sphere centered at its own "$\underline{c}_0$-vertex". So somewhere we must have one of these simplices,

say V, and a sphere B such that $\mu(B\cap V)/\mu(V) > \sigma_n$. As before let $\underline{0} = \underline{c}_0,\underline{c}_1,\ldots,\underline{c}_n$ be the vertices of V. Consider the linear transformation L which maps $\lambda_1\underline{c}_1+\ldots+\lambda_n\underline{c}_n$ into $\underline{g}_0 + \sum_{i=1}^n \lambda_i(\underline{g}_i-\underline{g}_0)$, where the $\underline{g}_i$ are the points introduced above. Then L(V) = G and L(B) is an ellipsoid E. If $\underline{x}$ is in B then $\underline{x} = \sum_{i=1}^n \lambda_i \underline{c}_i$ and $\langle\underline{x},\underline{x}\rangle \le 1$. For $\underline{y} = L(\underline{x})$ we find, using (a) and Lemma 1.8

$$\langle\underline{y}-\underline{g}_0,\underline{y}-\underline{g}_0\rangle = \sum_{i=1}^n\sum_{j=1}^n \lambda_i\lambda_j \langle\underline{g}_i-\underline{g}_0,\underline{g}_j-\underline{g}_0\rangle$$

$$\le \sum_{i=1}^n\sum_{j=1}^n \lambda_i\lambda_j \langle\underline{c}_i,\underline{c}_j\rangle = \langle\underline{x},\underline{x}\rangle \le 1.$$

Therefore E is inside the sphere B_1 with center $\underline{g}_0$ and radius 1. Hence

$$\sigma_n < \frac{\mu(B\cap V)}{\mu(V)} = \frac{\mu(E\cap G)}{\mu(G)} \le \frac{\mu(G\cap B_1)}{\mu(G)} = \sigma_n,$$

a contradiction. Our assumption $\Delta(K) > \sigma_n$ was false. □

COROLLARY. $\Delta_2 = \pi/(2\sqrt{3}) = 0.9069\ldots$.

PROOF. $\mathbb{R}^2$ can be dissected into congruent equilateral triangles. □

This is the only case where Δ_n is known. Usually one studies the *center density* $\delta_n := \Delta_n/V_n$ where V_n is the volume of a sphere of radius 1 in $\mathbb{R}^n$, i.e. $V_n = \pi^{n/2}/\Gamma(\frac{1}{2}n+1)$. If only lattice packings are considered then the densest packings are known for $n \le 8$. Connected with the sphere-packing problem there is also the problem of touching spheres. The *contact number* τ_n is the greatest number of non-overlapping spheres of radius 1 in $\mathbb{R}^n$ that can touch another sphere of radius 1. Clearly $\tau_2 = 6$. The number τ_n is known for $n \le 9$. In the following we study lattice packings only.

2. MODULAR FUNCTIONS AND MODULAR FORMS

In the next section we shall introduce the theta-function of a lattice. As a preparation we treat part of the classical theory of modular forms in this section.

Let the complex numbers ω_1,ω_2 be a basis for the lattice Ω in $\mathbb{C}$. Other bases are obtained by transformations $\begin{pmatrix}\omega_2'\\ \omega_1'\end{pmatrix} = \begin{pmatrix}a&b\\ c&d\end{pmatrix}\begin{pmatrix}\omega_2\\ \omega_1\end{pmatrix}$, where a,b,c,d are integers with ad-bc = ±1. A meromorphic function f which is doubly periodic,

i.e. $\forall_{z\in\mathbb{C}}\forall_{\omega\in\Omega}[f(z+\omega) = f(z)]$, is called an *elliptic* function. If such a function has no pole in a period parallelogram (the parallelogram spanned by a basis pair ω_1,ω_2) then f is bounded and therefore constant. By considering 1/f we see that a non-constant elliptic function has zeros. We assume that there are no zeros or poles on the boundary of the period parallelogram (otherwise we translate it slightly) and we refer to such a region C as a *cell*. By the double periodicity we have $\oint_{\partial C} f(z)dz = 0$, i.e. if f is not constant then f has a pole of order ≥ 2 or at least two poles in C. In the same way contour integration of f'/f shows that the number of zeros (counting multiplicities) in a cell equals the number of poles. This number is called the *order* of f.

It is easily established that $\sum_{\omega\in\Omega\setminus\{0\}}\omega^{-\alpha}$ is absolutely convergent iff $\alpha > 2$.

DEFINITION 2.1. Given Ω we define the *Eisenstein series* of order n by

$$G_n := \sum_{\omega\in\Omega\setminus\{0\}} \omega^{-n} \qquad (n \geq 3).$$

Let $\alpha > 2$ and $R > 0$. If $|z| > R$ and $|\omega| \geq 2R$ then $|z-\omega|^{-\alpha} \leq 2^{\alpha}|\omega|^{-\alpha}$ and therefore $\sum_{\omega\in\Omega,\,|\omega|\geq 2R}(z-\omega)^{-\alpha}$ is absolutely and uniformly convergent on $\{z \in \mathbb{C} \mid |z| < R\}$.

LEMMA 2.2. $\sum_{\omega\in\Omega}(z-\omega)^{-3}$ *is an elliptic function of order* 3.

PROOF. We have already seen that the sum of the series is meromorphic with a pole of order 3 in 0. The double periodicity follows from the absolute convergence of the series and from the invariance of Ω under translation by elements of Ω. □

DEFINITION 2.3. The *Weierstrasz* $\wp$*-function* is defined by

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega\in\Omega\setminus\{0\}} \left\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right\}.$$

Clearly $\wp$ is an even function with a pole of order 2 at each point of Ω. Since $\wp'(z) = -2\sum_{\omega\in\Omega}(z-\omega)^{-3}$ we see from Lemma 2.2 that for $\omega \in \Omega$ the function $\wp(z+\omega)-\wp(z)$ is constant. Taking $z = -\frac{1}{2}\omega$ we find that the constant is 0, i.e. $\wp$ is an elliptic function of order 2.

THEOREM 2.4. *For* $0 < |z| < \min\{|\omega| \mid \omega \in \Omega\setminus\{0\}\}$ *we have*

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} (2n+1)G_{2n+2}z^{2n}.$$

PROOF. In (2.3) expand $(z-\omega)^{-2}$ in a Taylor series and change the order of summation. □

THEOREM 2.5. $[\wp'(z)]^2 = 4[\wp(z)]^3 - 60G_4\wp(z) - 140G_6$.

PROOF. By applying Theorem 2.4 we find the Laurent expansion of $[\wp'(z)]^2 + - 4[\wp(z)]^3 + 60G_4\wp(z)$. It turns out that this elliptic function has no poles, i.e. it is constant. □

The expressions $g_2 := 60G_4$ and $g_3 := 140G_6$ are called the *invariants* of $\wp$. We also define

$$e_1 := \wp\left(\frac{\omega_1}{2}\right), \quad e_2 := \wp\left(\frac{\omega_2}{2}\right), \quad e_3 := \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

THEOREM 2.6. $4[\wp(z)]^3 - g_2\wp(z) - g_3 = (\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$; *The three zeros* e_1, e_2, e_3 *are different and hence the discriminant* $g_2^3-27g_3^2$ *is not zero.*

PROOF. $\wp'$ is odd and $\wp'$ does not have a pole at $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$ or $\frac{1}{2}(\omega_1+\omega_2)$. The periodicity implies that $\wp'(-\frac{1}{2}\omega_1) = \wp'(\frac{1}{2}\omega_1)$, etc. Therefore $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, and $\frac{1}{2}(\omega_1+\omega_2)$ are simple zeros of $\wp'$. Now apply Theorem 2.5. If $e_1 = e_2$ then $\wp(z)-e_1$ would have a double zero at $\frac{1}{2}\omega_1$ and at $\frac{1}{2}\omega_2$ which contradicts the fact that $\wp$ has order 2. □

DEFINITION 2.7. $\Delta(\omega_1,\omega_2) := g_2^3 - 27g_3^2$.

From the definitions we see that g_2, g_3 and Δ are homogeneous of degree -4, -6, and -12, respectively. Therefore it is sufficient to study them for pairs $(\omega_1,\omega_2) = (1,\tau)$ where τ is in the upper half-plane of $\mathbb{C}$, which we denote by $\mathbb{H}$. In the following we shall write

$$g_2(\tau) := 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-4},$$

$$g_3(\tau) := 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} (m+n\tau)^{-6},$$

$$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau).$$

By Theorem 2.6 $\Delta(\tau) \neq 0$ for $\tau \in \mathbb{H}$. Observe that we no longer have a fixed lattice Ω but we now consider ω_2/ω_1 as variable.

We also introduce the function

$$J(\tau) := g_2^3(\tau)/\Delta(\tau),$$

known as *Klein's modular function*. By comparing $|m+n\tau|^2$ with $|m+ni|^2$ one shows (with some effort) that the functions g_2, g_3, Δ, and J are analytic in $\mathbb{H}$. As we observed above $g_2^3(\omega_1,\omega_2)$ and $\Delta(\omega_1,\omega_2)$ are homogeneous of degree -12. So their quotient is homogeneous of degree 0, i.e. $J(\omega_2/\omega_1)$ is homogeneous of degree 0. If a,b,c,d are integers such that ad-bc = 1, then $\begin{pmatrix}\omega_2'\\ \omega_1'\end{pmatrix} = \begin{pmatrix}a&b\\ c&d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ is a basis for the lattice Ω, yielding the same $\wp$, g_2, g_3, Δ, etc. Therefore J is invariant under this transformation. We have therefore proved:

THEOREM 2.8. $J(\frac{a\tau+b}{c\tau+d}) = J(\tau)$ *if* a,b,c,d *are integers with* ad-bc = 1.

We introduce the notation $z := e^{2\pi i\tau}$. This maps $\mathbb{H}$ onto the punctured unit disc. It follows from Theorem 2.8 that $f(z) := J(\tau)$ is well defined and that f is analytic. Therefore f has a Laurent series, i.e. $J(\tau)$ can be expanded in a Fourier series $\sum_{n=-\infty}^{\infty} a_n e^{2\pi in\tau}$. Such Fourier series are what we are interested in. By completely straightforward methods one finds the following expansions.

THEOREM 2.9. *Let* $\sigma_\alpha(k) := \sum_{d|k} d^\alpha$. *Then for* $\tau \in \mathbb{H}$ *we have*

$$g_2(\tau) = \frac{4\pi^4}{3}\{1 + 240\sum_{k=1}^{\infty}\sigma_3(k)\, e^{2\pi ik\tau}\},$$

$$g_3(\tau) = \frac{8\pi^6}{27}\{1 - 504\sum_{k=1}^{\infty}\sigma_5(k)\, e^{2\pi ik\tau}\},$$

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\, e^{2\pi in\tau},\ \tau(n)\ \textit{an integer},\ \tau(1) = 1,$$

$$J(\tau) = (\frac{1}{12})^3\{e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n)\, e^{2\pi in\tau}\},\ c(n)\ \textit{an integer}.$$

The set of all Möbius transformations

$$\tau \to \frac{a\tau+b}{c\tau+d}\ ;\ a,b,c,d \text{ integers, } ad-bc = 1$$

is called the *modular group* $\hat{\Gamma}(1)$. We write $\Gamma(1) = SL_2(\mathbb{Z})$ and observe that $\hat{\Gamma}(1) = SL_2(\mathbb{Z})/\{\pm I\}$. The transformations of $\hat{\Gamma}(1)$ can be represented by matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

THEOREM 2.10. *$\hat{\Gamma}(1)$ is generated by the transformations*

$$T\tau := \tau + 1, \qquad S\tau := -1/\tau.$$

PROOF. Consider $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. It is sufficient to consider $c \geq 0$. If $c = 0$ we are finished. If $c = 1$ then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = T^a S T^d$. If $c > 1$ let $d = cq+r$ with $0 < r < c$. Then

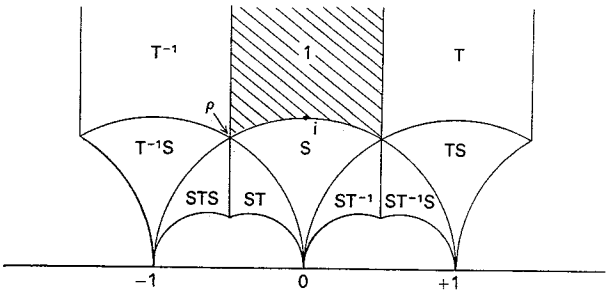
$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) T^{-q} S = \left(\begin{smallmatrix} -aq+b & -a \\ r & -c \end{smallmatrix}\right)$$

and the proof follows by induction. □

Observe that $S^2 = (ST)^3 = I$.

DEFINITION 2.11. An open subset R of $\mathbb{H}$ is called a *fundamental region* for the subgroup G of $\hat{\Gamma}(1)$ if no two distinct points of R belong to the same orbit and every orbit has at least one point in $\bar{R}$.

It is not difficult to show that $\{\tau \in \mathbb{H} \mid |\tau| > 1, -\frac{1}{2} < \operatorname{Re} \tau < \frac{1}{2}\}$ is a fundamental region for $\hat{\Gamma}(1)$. By repeated applications of S and T we find other fundamental regions as in the figure below.



DEFINITION 2.12. A function f is called a *modular function* if

(i) f is meromorphic on $\mathbb{H}$,

(ii) $\forall_{A \in \hat{\Gamma}(1)} \; \forall_{\tau \in \mathbb{H}} \; f(A\tau) = f(\tau)$],

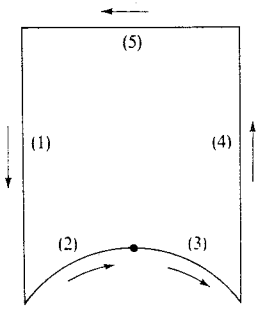
(iii) f has a Fourier expansion of the form

$$f(\tau) = \sum_{n=-m}^{\infty} a(n)\, e^{2\pi i n\tau} \qquad (\tau \in \mathbb{H}).$$

By Theorems 2.8 and 2.9 J is a modular function. When counting zeros and poles in the fundamental region we make the following conventions. The order of a zero or pole at ρ is divided by 3, the order of a zero or pole at i is divided by 2, the order at $i\infty$ is the order of the zero or pole at $z = 0$ where $z = e^{2\pi i\tau}$. Only one point from every orbit is counted (e.g. only the left half of the boundary is counted).

THEOREM 2.13. *If f is a modular function, not identically* 0, *then in a fundamental region (with part of the boundary) the number of zeros equals the number of poles.*

PROOF. We integrafe f'/f over the contour in the figure below. First assume there are no zeros or poles on the boundary.



Since f is a modular function the contributions of (1) and (4) cancel as do those of (2) and (3). If we take (5) sufficiently high and substitute $z = e^{2\pi i\tau}$ we find a contribution by the zero or pole at $i\infty$ in accordance with our convention. The modifications by obvious detours for zeros and poles on the boundary are straightforward. The angle of 60° at ρ and $\rho + 1$ accounts for the division by 3, etc. □

We shall now generalize (2.12). We use the following notation. If $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ we write $f|_k A$ for the function with value $(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$ in τ.

DEFINITION 2.14. An *entire modular form of weight* k is a function f which satisfies:

(i) f is analytic in $\mathbb{H}$,

(ii) $f|_k A = f$ for all $A \in \Gamma(1)$,

(iii) f has an expansion $f(\tau) = \sum_{n=0}^{\infty} c(n)e^{2\pi i n\tau}$.

Extensions of the definition are possible in several ways. One can drop the word "entire" by replacing "analytic" in (i) by "meromorphic" and making (iii) less restrictive. One can restrict A to a subgroup of $\Gamma(1)$. Finally one can replace (ii) by $f|_k A = v(A)f$ where $v(A)$ depends on A only. We shall need all these generalizations later on but in this brief exposition we restrict ourselves to (2.14). If in (iii) we have $c(0) = 0$ then the form is called a *cusp form.*

Exactly the same argument that proved Theorem 2.8 shows that $\Delta(\tau)$ is a modular form of weight 12 and by Theorem 2.9 it is a cusp form. In the same way we see that the *Eisenstein* series introduced in (2.1), i.e.

$$G_{2k}(\tau) := \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-2k} \qquad (k \geq 2)$$

is a modular form of weight $2k$.

THEOREM 2.15. *If we count the number of zeros of a non-constant entire modular form in the fundamental region using the conventions of Theorem 2.13 we find* $\frac{k}{12}$ *zeros, or in an obvious notation*

$$k = 12N + 6N(i) + 4N(\rho) + 12N(i\infty).$$

PROOF. The proof is the same as for Theorem 2.13. However, now (2) and (3) do not cancel but yield $\frac{k}{12}$ (which is easily checked). □

COROLLARY. *Every nonconstant entire modular form has even weight* $k \geq 4$. *If it is a cusp form then* $k \geq 12$.

THEOREM 2.16. *Let* M_k *be the space of all entire modular forms of weight* k. *Then* M_k *is a linear space of dimension*

$$\left\lfloor \frac{k}{12} \right\rfloor \qquad \text{if } k \equiv 2 \pmod{12},$$

$$\left\lfloor \frac{k}{12} \right\rfloor + 1 \text{ if } k \not\equiv 2 \pmod{12},$$

and $f \in M_k$ *can be uniquely expressed as*

$$f = \sum_{\substack{r=0 \\ k-12r\neq 2}}^{\lfloor k/12 \rfloor} a_r G_{k-12r} \Delta^r$$

(*where* $G_0 = 1$).

PROOF.

(i) For $k < 12$ this follows from Theorem 2.15. E.g. if f has weight 4 then f/G_4 is entire and it has weight 0, i.e. it is a constant.

(ii) Let f be an entire modular form of weight $k \geq 12$. Since $G_k(i\infty) \neq 0$ we can define $c := f(i\infty)/G_k(i\infty)$. Then $f - cG_k$ is a cusp form in M_k and it can therefore be written as $\Delta \cdot h$ where h is an entire modular form of weight k-12. The proof follows by induction. Uniqueness is obvious because the functions $G_{k-12r}\Delta^r$ are clearly linearly independent. □

COROLLARY. *If* $k \equiv 0 \pmod 4$ *then an entire modular form of weight* k *is a polynomial in* G_4 *and* Δ.

PROOF. The proof is the same as above using powers of G_4 of the right weight and the fact that $G_4(i\infty) \neq 0$. □

We now briefly look at one subgroup of $\bar{\Gamma}(1)$ which is important for our purposes. This is the group Γ_θ generated by T^2 and S. It consists of transformations described by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $cd \equiv ab \equiv 0 \pmod 2$. This group has index 3 in the modular group. The regions 1,T, and TS in the figure following Definition 2.11 form a fundamental region for Γ_θ. The behaviour of a function near $\tau = 1$ is described by transforming this point to $i\infty$ with an element of $\bar{\Gamma}(1)$. Theorem 2.15 has an analogue in this case which is

$$k = 4N + 4N(i\infty) + 4N(1) + 2N(i).$$

In this case one can also define Eisenstein series, etc. For details we refer to the literature.

DEFINITION 2.17. $\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{\pi i \tau n^2}$.

Clearly $\theta(\tau+2) = \theta(\tau)$. In Theorem 3.4 we shall show that $\theta(-1/\tau) = (-i\tau)^{\frac{1}{2}}\theta(\tau)$. Therefore θ^8 is an entire modular form of weight 4 for Γ_θ (with a zero at $\tau = 1$).

It is this function which is responsible for the name *theta-functions*. We introduce a number of similar functions which will be used again later.

DEFINITION 2.18. For $\tau \in \mathbb{H}$ and $q := e^{\pi i \tau}$ we define

$$\theta_2(\tau) := 2 \sum_{m=0}^{\infty} q^{(m+\frac{1}{2})^2},$$

$$\theta_3(\tau) := \theta(\tau) = 1 + 2 \sum_{m=1}^{\infty} q^{m^2},$$

$$\theta_4(\tau) := 1 + 2 \sum_{m=1}^{\infty} (-q)^{m^2}.$$

There exist many relations between these functions. We mention two which are obvious.

LEMMA 2.19.
(i) $\theta_3(4\tau) + \theta_2(4\tau) = \theta_3(\tau)$,
(ii) $\theta_3(4\tau) - \theta_2(4\tau) = \theta_4(\tau)$.

3. CODES, LATTICES, AND THETA-FUNCTIONS

Let Λ be a lattice in $\mathbb{R}^n$ with basis $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$ and let M be the matrix with columns $\underline{e}_i$, i.e. $\Lambda = \{M\underline{x} \mid \underline{x} \in \mathbb{Z}^n\}$. The *minimum squared distance* of Λ is given by

$$d(\Lambda) = \min\{\langle \underline{x}-\underline{y}, \underline{x}-\underline{y} \rangle \mid \underline{x} \in \Lambda, \underline{y} \in \Lambda, \underline{x} \neq \underline{y}\}.$$

If we take the points of Λ as centers of spheres of radius $\rho = \frac{1}{2}\sqrt{d(\Lambda)}$ we obtain a sphere-packing K_Λ with center density $\delta(K_\Lambda) = \rho^n/\det \Lambda$. The *dual lattice* $\Lambda^\perp$ is defined by

$$\Lambda^\perp := \{\underline{x} \in \mathbb{R}^n \mid \forall_{\underline{y} \in \Lambda}[\langle \underline{x}, \underline{y} \rangle \in \mathbb{Z}]\}.$$

It is easily seen that $(M^{-1})^t$ is a generator matrix for $\Lambda^\perp$, i.e. $\Lambda^\perp := \{(M^{-1})^t \underline{u} \mid \underline{u} \in \mathbb{Z}^n\}$. A lattice with $\Lambda = \Lambda^\perp$ is called *self-dual*.

Our first theorem on lattices is a special case of the *Poisson summation formula*:

LEMMA 3.1. *Let* $f : \mathbb{R}^n \to \mathbb{C}$ *be a function such that*

$$\sum_{k_1, k_2, \ldots, k_n = -\infty}^{\infty} f(k_1+x_1, k_2+x_2, \ldots, k_n+x_n)$$

is absolutely uniformly convergent on compact subsets of $\mathbb{R}^n$. *Then we have*

$$\sum_{\underline{k}\in\mathbb{Z}^n}^{\infty} f(\underline{k}+\underline{a}) = \sum_{\underline{\nu}\in\mathbb{Z}^n} e^{2\pi i<\nu,a>} \int_{\mathbb{R}^n} e^{-2\pi i<\underline{\nu},\underline{y}>} f(\underline{y})\,dy_1\ldots dy_n$$

for $\underline{a} \in \mathbb{R}^n$.

PROOF. We refer to standard text books on analysis. □

THEOREM 3.2. *Let* f *satisfy the conditions of Lemma 3.1. Define*

$$\hat{f}(\underline{v}) := \int_{\mathbb{R}^n} e^{-2\pi i<\underline{u},\underline{v}>} f(\underline{u})\,du_1du_2\ldots du_n.$$

If Λ *is a lattice in* $\mathbb{R}^n$ *then we have*

$$\sum_{\underline{x}\in\Lambda} f(\underline{x}) = (\det \Lambda)^{-1} \sum_{\underline{v}\in\Lambda^{\perp}} \hat{f}(\underline{v}).$$

PROOF. In Lemma 3.1 we replace $f(\underline{k})$ by $f(M\underline{k})$ and we take $\underline{a} = \underline{0}$. Then we find

$$\sum_{\underline{x}\in\Lambda} f(\underline{x}) = \sum_{\underline{k}\in\mathbb{Z}^n} f(M\underline{k}) = \sum_{\underline{\nu}\in\mathbb{Z}^n} \int_{\mathbb{R}^n} e^{-2\pi i<\underline{\nu},\underline{y}>} f(M\underline{y})\,dy_1\ldots dy_n.$$

In the integral we substitute $\underline{y} = M^{-1}\underline{u}$ and we observe that

$$<\underline{\nu},\underline{y}> = \underline{y}^t\underline{\nu} = \underline{u}^t(M^{-1})^t\underline{\nu} = <(M^{-1})^t\underline{\nu},\underline{u}>. \quad \square$$

The squared length of a vector $\underline{x} = M\underline{k}$ in Λ is given by

$$<\underline{x},\underline{x}> = \underline{k}^tM^tM\underline{k} = \underline{k}^tA\underline{k}$$

where $A = M^tM$ is a positive definite symmetric matrix.

DEFINITION 3.3. The *theta-function* of Λ is given by

$$\Theta_\Lambda(\tau) := \sum_{\underline{x}\in\Lambda} e^{\pi i\tau<\underline{x},\underline{x}>} = \sum_{\underline{k}\in\mathbb{Z}^n} e^{\pi i\tau\underline{k}^tA\underline{k}}.$$

Since $\underline{k}^tA\underline{k} > c\,<\underline{k},\underline{k}>$ for some $c > 0$, the series defines a function which is analytic in $\mathbb{H}$.

THEOREM 3.4. $\Theta_{\Lambda^{\perp}}(\tau) = \det\Lambda\,(-i\tau)^{-n/2}\Theta_{\Lambda}(-1/\tau)$.

PROOF. The function $f(\underline{x}) := e^{\pi i\tau<\underline{x},\underline{x}>}$ satisfies the conditions of Lemma 3.1. Therefore we have by Theorem 3.2

$$\theta_\Lambda(\tau) = (\det \Lambda)^{-1} \sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}<\underline{v},\underline{v}>} \int_{\mathbb{R}^n} e^{\pi i\tau<\underline{u}-\frac{\underline{v}}{\tau},\underline{u}-\frac{\underline{v}}{\tau}>} du_1\ldots du_n.$$

The value of the integral is not changed by the translation $\underline{u} \to \underline{u} + \frac{\underline{v}}{\tau}$. If we then take $\tau = it$ the integral becomes

$$\int_{\mathbb{R}^n} e^{-\pi t(u_1^2+\ldots+u_n^2)} du_1\ldots du_n = t^{-n/2}.$$

So by analytic continuation we have

$$\theta_\Lambda(\tau) = (\det \Lambda)^{-1}(-i\tau)^{-n/2} \sum_{\underline{v}\in\Lambda^\perp} e^{-\frac{\pi i}{\tau}<\underline{v},\underline{v}>}.$$

The required result follows by replacing Λ by $\Lambda^\perp$. □

The special case $n = 1$, $\Lambda = \mathbb{Z}$ yields the functional equation for $\theta(\tau)$ announced in Section 2.

The properties of lattices and their theta-functions described in the first part of this section have quite a lot of analogy with properties of linear codes. We assume that the reader is familiar with the terminology of coding theory. In the homogeneous weight enumerator $W_C(x,y)$ of a code for length n over $\mathbb{F}_q$,

$$W_C(x,y) = \sum_{\underline{u}\in C} x^{n-w(\underline{u})}y^{w(\underline{u})} = \sum_{i=0}^{n} A_i x^{n-i}y^i,$$

where $w(\underline{u})$:= weight of $\underline{u}$, the coefficient A_i counts the number of code words of weight i. In Definition 3.3 we have

$$\theta_\Lambda(\tau) = \sum_{\underline{x}\in\Lambda} e^{\pi i\tau<\underline{x},\underline{x}>} = \sum_{\ell} A_\ell e^{\pi i\tau\ell},$$

where A_ℓ is the number of lattice points $\underline{x}$ with $|\underline{x}|^2 = \ell$. The well-known theorem of MacWilliams for $W_C(x,y)$ and the weight enumerator of the dual code, i.e.

$$W_{C^\perp}(x,y) = q^{-k}W_C(x+(q-1)y,x-y),$$

if C is an (n,k)-code over $\mathbb{F}_q$, has as its analogue the functional equation (3.4). The relation between W_C and $W_{C^\perp}$ is extremely useful if C is self-dual, i.e. $C = C^\perp$. In the same way we see that if a lattice is self-dual then (3.4) makes it possible to apply the powerful theory of modular forms treated in Section 2. For this we have only to observe that $\Theta_\Lambda(\tau+2) = \Theta_\Lambda(\tau)$ and hence (3.4) shows that for $n \equiv 0 \pmod 8$ the function $\Theta_\Lambda(\tau)$ for a self-dual lattice is a modular form of weight $\frac{n}{2}$ for Γ_θ. We shall return to this later.

We now describe two constructions which produce sphere-packings starting from binary codes. Following Sloane we call them construction A and B. Construction A starts with an arbitrary binary code C of length n and minimum distance d. We assume $\underline{0} \in C$. The set $\Lambda(C)$ in $\mathbb{R}^n$ consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{-\frac{1}{2}}\underline{x} \pmod 2 \in C$. The points of $\Lambda(C)$ are the centers of a sphere-packing with spheres of radius

$$\rho_C = \begin{cases} 2^{-3/2}\, d^{1/2} & \text{if } d \le 4, \\ 2^{-1/2} & \text{if } d \ge 4. \end{cases}$$

By definition this sphere-packing is periodic. We only have to consider a cube of side $2^{\frac{1}{2}}$ to find the center density:

$$\delta_C = |C| \cdot \rho_C^n \cdot 2^{-n/2}.$$

THEOREM 3.5. *The set* $\Lambda(C)$ *described in construction* A *is a lattice iff* C *is a linear code. If* C *is an* (n,k)*-code then* $\det \Lambda(C) = 2^{\frac{1}{2}n-k}$ *and furthermore*

$$\Lambda(C^\perp) = \Lambda(C)^\perp.$$

PROOF.

(i) The first assertion follows from the fact that the mapping $\phi: \mathbb{Z}^n \to \mathbb{F}_2^n$ defined by $\phi(\underline{k}) := \underline{k} \pmod 2$ is a homomorphism.

(ii) If C has generator matrix (IB) then the matrix $2^{-\frac{1}{2}}\begin{pmatrix} I & B \\ 0 & 2I \end{pmatrix}^t$ is a generator matrix for the lattice $\Lambda(C)$. Here B is of size k by n-k. This makes the second assertion obvious. The final assertion follows directly from the definition. □

The following theorem shows that the theta-function of $\Lambda(C)$ is closely related to the weight enumerator of C.

THEOREM 3.6. *If* C *is linear with weight enumerator* $W_C(x,y)$ *then the theta-function of the lattice* $\Lambda(C)$ *is given by*

$$\theta_{\Lambda(C)}(\tau) = W_C(\theta_3(2\tau),\theta_2(2\tau)).$$

PROOF. By (3.3) we have

$$\theta_{\Lambda(C)}(\tau) = \sum_{\underline{c}\in C} \sum_{\underline{k}\in\mathbb{Z}^n} e^{\frac{\pi i\tau}{2}\langle \underline{c}+2\underline{k},\underline{c}+2\underline{k}\rangle}.$$

In the inner sum we assume that $\underline{c}$ has w coordinates 1. Then this sum equals

$$\left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k)^2}\right)^{n-w}\left(\sum_{k=-\infty}^{\infty} e^{\frac{\pi i\tau}{2}(2k+1)^2}\right)^{w}.$$

The result immediately follows from (2.18) and the definition of $W_C(x,y)$. □

EXAMPLE 3.7. Let C be the code of length n consisting of all words of even weight. For this code the minimum distance d is 2. So construction A yields a sphere-packing with spheres of radius $\frac{1}{2}$. The center density is $2^{-\frac{1}{2}n-1}$. Since $W_C(x,y) = \frac{1}{2}\{(x+y)^n + (x-y)^n\}$ we find

$$\theta_{\Lambda(C)}(\tau) = \tfrac{1}{2}\{(\theta_3(2\tau)+\theta_2(2\tau))^n + (\theta_3(2\tau)-\theta_2(2\tau))^n\}.$$

By Lemma 2.19 this equals $\frac{1}{2}\{\theta_3(\frac{1}{2}\tau)^n + \theta_4(\frac{1}{2}\tau)^n\}$. We remark that it is known that for n = 3,4 or 5 this is the densest possible lattice packing in $\mathbb{R}^n$.

EXAMPLE 3.8. Consider construction A for the extended Hamming code H_8 of length 8. This yields a lattice $\Lambda(H_8)$. By Theorem 3.4 and Theorem 3.5 the corresponding theta-function is an entire modular form of weight 4 for Γ_θ. However, every $\underline{x}$ in $\Lambda(H_8)$ satisfies $\langle \underline{x},\underline{x}\rangle \equiv 0 \pmod 2$, so $\theta_{\Lambda(H_8)}$ is in fact an entire modular form of weight 4 for $\hat{\Gamma}(1)$. By Theorem 2.16 and Theorem 2.9 we therefore have

$$\theta_{\Lambda(H_8)} = 1 + 240\sum_{k=1}^{\infty}\sigma_3(k)e^{2\pi ik\tau}.$$

As an exercise we recommend that the reader show by hand that $\Lambda(H_8)$ has

240 $\sigma_3(5) = 240*126$ vectors $\underline{x}$ with $\langle \underline{x},\underline{x} \rangle = 10$. This will make it clear that the theory of modular functions is a powerful tool in studying the distribution of vectors in lattices. We remark that it is known that $\Lambda(H_8)$ yields the densest lattice packing in $\mathbb{R}^8$.

We now turn to construction B. In this case we start with an (n,k)-code C with minimum distance 8 for which all weights are $\equiv 0 \pmod 4$. The lattice L(C) consists of all $\underline{x} \in \mathbb{R}^n$ such that $2^{-\frac{1}{2}}\underline{x} = \underline{c} + 2\underline{k}$ where $\underline{c} \in C$ and $\underline{k} \in \mathbb{Z}^n$ such that $\Sigma k_i \equiv 0 \pmod 2$. The corresponding sphere-packing has spheres of radius 1.

EXAMPLE 3.9. Start with the extended Golay code of length 24 and apply construction B. This yields a lattice. If we shift this lattice over the vector $2^{-3/2}(1,1,\ldots,1,-3)$ then the union of the two sets is again a lattice. This is the famous Leech lattice Λ_{24}.

We return to the analogy between certain parts of coding theory and the theory of lattices. For this purpose we consider so-called type II codes, i.e. self-dual codes C for which all weights are $\equiv 0 \pmod 4$, and type II lattices, i.e. self-dual lattices Λ for which $\langle \underline{x},\underline{x} \rangle$ is even for every $\underline{x} \in \Lambda$. A famous theorem of A.M. GLEASON (cf. [2]) states that the weight enumerator $W_C(x,y)$ of a type II code is a polynomial in ξ and η, where ξ is the weight enumerator of the extended Hamming code H_8 and η is the weight enumerator of the extended Golay code G_{24}. We can now understand this theorem in the following way. Let C be a type II code. By construction A we find a lattice $\Lambda(C)$ which by Theorem 3.5 is self-dual. By the construction we see that $\Lambda(C)$ is of type II. Therefore the corresponding theta-function $\Theta_{\Lambda(C)}$ satisfies

$$\Theta_{\Lambda(C)}\Big|_{n/2} T = \Theta_{\Lambda(C)},$$

$$\Theta_{\Lambda(C)}\Big|_{n/2} S = (-i)^{n/2}\Theta_{\Lambda(C)},$$

where we have used Theorem 3.4.

By the same method as we used in Theorem 2.15 one shows that such a modular form is 0 unless n is a multiple of 8. In the latter case $\Theta_{\Lambda(C)}$ is an entire modular form of weight $\frac{n}{2}$ for $\tilde{\Gamma}(1)$. By the corollary to Theorem 2.16 it follows that $\Theta_{\Lambda(C)}$ is a polynomial in G_4 and Δ. In Example 3.8 we

already saw that in this way H_8 and construction A produced G_4. In the same way the Golay code G_{24} leads to a polynomial in G_4 and Δ. The theorem for $W_C(x,y)$ is now proved by returning to weight enumerators via Theorem 3.6. The original proof of Gleason's theorem did not use the method described above.

There are many other analogies between codes and lattices. Not everything is completely understood. As was stated in the introduction this short survey will hopefully interest the reader into looking at the extensive literature on this subject and also at some of the still open problems.

REFERENCES

[1] T.M. APOSTOL, *Modular functions and Dirichlet series,* Springer, Berlin, 1976.

[2] A.M. GLEASON, *Weight polynomials of self-dual codes and the MacWilliams identities,* in: Actes Congrès Intern. des Math. 1970, Gauthier Villars, Paris, 1971, Vol. 3, pp. 211-215.

[3] C.A. ROGERS, *The packing of equal spheres,* Proc. London Math. Soc. (3) 8 (1958) 609-620.

[4] C.A. ROGERS, *Packing and covering,* Cambridge Univ. Press, Cambridge, 1964.

[5] J.P. SERRE, *A course in arithmetic,* Springer, Berlin, 1973.

[6] N.J.A. SLOANE, *Binary codes, lattices, and sphere-packings,* in: "Combinatorial Surveys" (Proc. Sixth British Comb. Conf., Egham, 1977; P.J. Cameron, ed.), Academic Press, London, 1977, pp. 117-164.