Can. J. Math., Vol. XXX, No. 4, 1978, pp. 738–747

LEE POLYNOMIALS OF CODES AND THETA FUNCTIONS OF LATTICES

DAVID P. MAHER

0. Introduction. Several authors [**2**; **3**; **10**; **12**] have noticed the similarities between the theory of codes and the theory of Euclidean lattices. It is interesting to compare the two theories since they share a common problem, viz. the sphere packing problem. In the theory of codes one would like to find a code over $\mathbf{F}_p$, i.e. a subspace of $\mathbf{F}_p^n$, such that non-intersecting spheres with respect to a given metric, centered at the code vectors, pack $\mathbf{F}_p^n$ densely. We would like to maximize both the number of spheres and the common radius. There is the same problem concerning lattices in Euclidean space. Leech [**9**] and Leech and Sloane [**10**] have produced good Euclidean sphere packings from good codes. The repercussions have reached into the theory of sporadic simple groups [**4**; **5**].

Of concern here are the similarities between the theory of theta functions of lattices and the theory of Lee weight enumerators of codes. Broué and Enguehard [**3**] have exhibited isomorphisms between algebras of Hamming polynomials of self-dual binary codes and algebras of theta functions of unimodular lattices. Mallows, Odlyzko, and Sloane [**12**] have found upper bounds for minimum Euclidean distances of even, unimodular lattices and minimum Hamming distances of binary, doubly even, self-dual codes. The proofs of the bounds in the two cases are formally the same, and involve theta functions and weight enumerators respectively. Maher [**14**] has derived a theta function transformation formula for non-linear lattices from the MacWilliams equations for Lee weight enumerators of non-linear codes.

In this paper we shall be considering non-binary as well as binary codes and shall examine the relationships between Lee weight polynomials of codes and theta series of lattices. The theory may be extended to include codes over non-prime fields if we use complex lattices. Sloane [**19**] has considered the case of codes over $\mathbf{F}_4$ where the associated lattices are modules over the Eisenstein integers. In a forthcoming paper we shall apply the results we obtain here to the theory of modular forms. In particular we shall show that one can construct modular forms of weight $n/2$ for certain congruence subgroups of level p from polynomials of degree n of modified Jacobi theta functions. These polynomials are Lee weight polynomials of self-orthogonal codes of dimension $(n-1)/2$ in $\mathbf{F}_p^n$.

Received March 28, 1977 and in revised form, November 11, 1977 and January 12, 1978.

1. Definitions. Throughout this article, p shall denote a prime number, and $\mathbf{F}_p$, the field with p elements. A *code* of ambient dimension n over $\mathbf{F}_p$ is a subset of $\mathbf{F}_p{}^n$, and a *linear* (n, k) *code* over $\mathbf{F}_p$ is a k-dimensional subspace of $\mathbf{F}_p{}^n$. The *dual* $C^\perp$ of a linear code C over $\mathbf{F}_p{}^n$ is the set of all elements y of $\mathbf{F}_p{}^n$ orthogonal to each vector of C under the usual inner product. A code is said to be *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$. Let M_n denote the group of $n \times n$ monomial matrices with ± 1 as non-zero entries. We let M_n act on $\mathbf{F}_p{}^n$ in the obvious way and let σ: $\mathbf{F}_p{}^n \to \mathbf{F}_p{}^n/M_n$ be the canonical map of the induced equivalence relation. For $x \in \mathbf{F}_p{}^n$ we call $\sigma(x)$ the *shape* of x. This is consistent with J. H. Conway's terminology for lattice vectors. $\sigma(x) = \sigma(y)$ if and only if x can be gotten from y by changing signs and permuting coordinates. For fixed p and n we abbreviate $\mathbf{F}_p{}^n/M_n$ by $\mathscr{S}$, the group of shapes in $\mathbf{F}_p{}^n$.

For C a code over $\mathbf{F}_p$, the *shape enumerator* of C is the formal sum

$$P_C = \sum_{x \in C} \sigma(x) = \sum_{s \in \mathscr{S}} a_s s$$

where $a_s = \text{card } \{x \in C | \sigma(x) = s\}$.

For an odd prime p, set $\omega = (p - 1)/2$; for $p = 2$ set $\omega = 1$. Throughout the article an element of $\mathbf{F}_p$, p odd, will be represented by an integer of absolute value $\leqq \omega$. $\mathbf{F}_2 = \{0, 1\}$. We shall view P_C as a polynomial in $\omega + 1$ variables as follows: for $x \in \mathbf{F}_p{}^n$ we can represent $\sigma(x)$ by an $(\omega + 1)$-tuple $(\sigma_0(x), \sigma_1(x), \ldots, \sigma_\omega(x))$ where $\sigma_i(x)$ is the number of occurrences of $\pm i$ in the coordinate places of x. Now for a code C we can write P_C as

$$P_C(X_0, X_1, \ldots, X_\omega) = \sum_{x \in C} X_0{}^{\sigma_0(x)} X_1{}^{\sigma_1(x)} \ldots X_\omega{}^{\sigma_\omega(x)}.$$

This homogeneous polynomial representing the shape enumerator is known as the *Lee weight polynomial of the code* C. This is somewhat inappropriate, for the *Lee weight* of a code vector $x = (x_1, \ldots, x_n)$ is the integer $\sum_{j=1}^n |x_j|$ where $|x_j|$ is the absolute value of the appropriate integer according to our convention above. Note that for $p \geqq 5$ the polynomial enumerates shapes, not weights. When $p = 2$ or 3 the polynomial is known as the *Hamming weight polynomial.*

Often a code vector $x \in \mathbf{F}_p{}^n$ will play the role of an integer vector; for example, we define $||x||^2 = \sum_{j=1}^n x_j{}^2$ where x_j is an integer such that $|x_j| \leqq \omega$. Context should eliminate any ambiguity. If s is a shape then we define $||s||^2 = ||x||^2$ where $\sigma(x) = s$.

Let $s \in \mathscr{S}$, and let x_s be a representative of s. Let $k \in \mathbf{Z}$, and define the integer

$$\alpha_{s,k} = \text{card } \{y \in p\mathbf{Z}^n | \, ||x_s + y||^2 = k\}.$$

One may easily verify that $\alpha_{s,k}$ is independent of choice of the representative x_s.

Now consider a function r: $\mathscr{S} \to \mathbf{C}$. We say that r defines a *shape relation* on $\mathscr{S}$ if $r(s) \not\equiv 0$ and

$$\sum_{s \in \mathscr{S}} r(s)\alpha_{s,k} = 0 \quad \text{for all } k = 0, 1, 2, 3, \ldots .$$

Shape relations are interesting for two reasons: as we shall see, a shape relation describes the information lost in passing from the shape enumerator to the theta series of a code, and it also defines a relation on a set of modified Jacobi theta series. It shall be convenient to represent r by a polynomial R in $\omega + 1$ variables defined by:

$$R(X_0, \ldots, X_\omega) = \sum_{s \in \mathscr{S}} r(s)X_s$$

where X_s is the monomial in $X_0, \ldots, X_\omega$ defined by the shape s as above.

A *lattice* in $\mathbf{R}^n$ is a free $\mathbf{Z}$-module of rank n in $\mathbf{R}^n$. To each (n, k) code C in $\mathbf{F}_p{}^n$ we may define a lattice in $\mathbf{R}^n$ in any number of ways. From different points of view some lattice constructions are more interesting than others. Here we define lattices $L_0(C)$ and $L(C)$ associated with C by $x \in L_0(C) \Leftrightarrow x \in \mathbf{Z}^n$ and $x \bmod p \in C$, and $L(C) = (1/\sqrt{p})L_0(C)$. If C is non-linear, then $L(C)$ is not a lattice, but it is a union of translates of lattices which we shall call a *non-linear lattice*.

Any (linear) lattice L defines a quadratic form Q: $\mathbf{Z}^n \to \mathbf{R}$ whose matrix A may be defined as follows: let M be a matrix whose rows are a basis of L, then $A = MM^t$, t denoting transpose, and $Q(x) = xMM^tx^t$. If Q_0 is the form associated with the lattice $L_0(C)$, then the image of Q_0 is contained in $\mathbf{Z}$. If C is self-orthogonal (i.e. the $\mathbf{F}_p$ inner product of every vector in C with every vector in C is 0), then the image of Q_0 is contained in $p\mathbf{Z}$; hence the image of the quadratic form associated with $L(C)$, viz. $(1/p)Q_0$, is contained in $\mathbf{Z}$.

The *theta series* of a lattice L is defined by:

$$\theta_L = \sum_{x \in L} q^{||x||^2} = \sum_{z \in \mathbf{Z}^n} q^{zAz^t}.$$

If the quadratic form for L represents integers only, then

$$\theta_L = \sum_{k=0}^{\infty} b_k q^k \quad \text{where } b_k = \text{card}\,\{x \in L \mid ||x||^2 = k\}.$$

The theta series for lattices $L(C)$ of self-dual binary and ternary codes have been studied in [3]. If we replace the formal variable q by $\exp(\pi i z)$ where z is in $\mathbf{H}$, the upper half complex plane, then $\theta_L(z)$ is a function on $\mathbf{H}$. It is holomorphic there since the series converges absolutely in z, as a volume argument shows that the Fourier coefficients b_k are of order n^k or less.

2. Algebras of Lee polynomials and algebras of theta series. Let $\mathscr{C}$ be a family of codes over $\mathbf{F}_p$, and let $\mathscr{P}(\mathscr{C})$ be the graded subalgebra of $\mathbf{C}[X_0, \ldots, X_\omega]$ generated by the Lee polynomials of the elements of $\mathscr{C}$. The grading is by homogeneous degree or equivalently, according to the ambient

https://doi.org/10.4153/CJM-1978-063-3 Published online by Cambridge University Press

dimension of the associated codes. Let $\mathscr{T}(\mathscr{C})$ be the graded algebra of holomorphic functions on $\mathbf{H}$ generated by the theta functions $\theta_{L(C)}(z)$ of elements of $\mathscr{C}$. Again the grading is by ambient dimension of the associated codes.

THEOREM 1. *If $\mathscr{C}$ is any family of codes over $\mathbf{F}_p$, then*

(i) *the function $P_C \to \theta_{L(C)}$ defined on the set of Lee polynomials of elements of $\mathscr{C}$ may be extended to an algebra homomorphism Φ_p: $\mathscr{P}(\mathscr{C}) \to \mathscr{T}(\mathscr{C})$.*

(ii) *The kernel of Φ_p is an ideal of shape relations.*

(iii) *Φ_p is injective if $p = 2$ or 3.*

Proof. (i) We introduce a classical Jacobi theta function which in the notation of [**20**] is:

$$\theta_3(v|z) = \sum_{m=-\infty}^{\infty} \exp(\pi i m^2 z + 2\pi i m v)$$

where $v \in \mathbf{C}$, $z \in \mathbf{H}$. We define for given p and $l \in \{0, 1, \ldots, \omega\}$

$$\varphi_{p,l}(z) = \exp(l^2 \pi i z/p)\theta_3(lz|pz).$$

For $s \in \mathscr{S}$, let $x \in s$; then s is identified with $X_0^{\sigma_0(x)} X_1^{\sigma_1(x)} \ldots X_\omega^{\sigma_\omega(x)}$. We assign to s a function $t_s(z)$ holomorphic on $\mathbf{H}$ by:

$$t_s(z) = \varphi_{p,0}^{\sigma_0(x)} \varphi_{p,1}^{\sigma_1(x)} \ldots \varphi_{p,\omega}^{\sigma_\omega(x)}$$

Now let C be a code over $\mathbf{F}_p$ and consider the map

$$\sum_{s \in \mathscr{S}} a_s s \to \sum_{s \in \mathscr{S}} a_s t_s(z)$$

which is equivalently

$$P_C(X_0, X_1, \ldots, X_\omega) \to P_C(\varphi_{p,0}, \varphi_{p,1}, \ldots, \varphi_{p,\omega}).$$

We wish to show that this map is given by Φ_p, i.e. that

$$(1) \quad P_C(\varphi_{p,0}(z), \ldots, \varphi_{p,\omega}(z)) = \theta_{L(C)}(z).$$

Recall $x \in L(C) \Leftrightarrow x = (1/\sqrt{p})(w + y)$, where $w \in C$, $y \in p\mathbf{Z}^n$, so

$$(2) \quad \theta_{L(C)}(z) = \sum_{x \in L(C)} \exp(\pi i z ||x||^2) = \sum_{w \in C} \sum_{y \in p\mathbf{Z}^n} \exp\left(\frac{\pi i z}{p} ||w + y||^2\right)$$

We notice that the inner sum of (2) is dependent only on the shape of the vector w. Hence if $w(s)$ represents a vector of shape s, and $w_i(s)$ the ith coordinate:

$$\begin{aligned}
\theta_{L(C)}(z) &= \sum_{s \in \mathscr{S}} a_s \sum_{y \in p\mathbf{Z}^n} \exp\left(\frac{\pi i z}{p} ||w(s) + y||^2\right) \\
&= \sum_{s \in \mathscr{S}} a_s \sum_{y \in p\mathbf{Z}^n} \prod_{i=1}^{n} \exp\left(\frac{\pi i z}{p} (w_i(s) + y_i)^2\right) \\
&= \sum_{s \in \mathscr{S}} a_s \prod_{i=1}^{n} \sum_{y \in p\mathbf{Z}^n} \exp\left(\frac{\pi i z}{p} (w_i(s) + y_i)^2\right) \\
&= \sum_{s \in \mathscr{S}} a_s \varphi_{p,0}^{\sigma_0(w(s))}(z) \varphi_{p,1}^{\sigma_1(w(s))}(z) \ldots \varphi_{p,\omega}^{\sigma_\omega(w(s))}(z).
\end{aligned}$$

https://doi.org/10.4153/CJM-1978-063-3 Published online by Cambridge University Press

The last step follows because:

$$\begin{aligned}\varphi_{p,l}(z) &= \exp\left(\frac{l^2\pi iz}{p}\right)\theta_3(lz|pz)\\ &= \exp\left(\frac{l^2\pi iz}{p}\right)\sum_{m\in p\mathbf{Z}}\exp\left(\frac{\pi ipm^2}{p^2}z + 2\pi ilmz/p\right)\\ &= \sum_{m\in p\mathbf{Z}}\exp\left(\frac{\pi iz}{p}(m+l)^2\right).\end{aligned}$$

Hence the identity (1) follows, and it is clear that the map $P_C \to \theta_{L(C)}$ is linear and multiplicative.

A more direct proof of (i) is possible using the fact that $\theta_{L_1\oplus L_2} = \theta_{L_1}\theta_{L_2}$ and $P_{C_1\oplus C_2} = P_{C_1}P_{C_2}$. However the identity (1) is of independent interest.

(ii) We wish to show that anything in the kernel of Φ_p defines a shape relation. Let $P \in \mathscr{P}(\mathscr{C})$ be homogeneous. We can identify P with a sum $\sum_{s\in\mathscr{S}} b_s s$, $b_s \in \mathbf{C}$. If $\Phi_p(P) = 0$, then $\sum_{s\in\mathscr{S}} b_s t_s(z) = 0$. So

$$\sum_{s\in\mathscr{S}} b_s \sum_{y\in p\mathbf{Z}^n}\exp\left(\frac{\pi iz}{p}||y + w(s)||\right) = 0$$

where $w(s) \in \mathbf{F}_p{}^n$ and $\sigma(w(s)) = s$. Hence if

$$\alpha_{s,k} = \text{card}\,\{y \in p\mathbf{Z}^n |\, ||w(s) + y|| = k\}$$

we have that:

$$\begin{aligned}&\sum_s b_s \sum_{k=0}^{\infty}\alpha_{s,k}\exp\left(\frac{\pi izk}{p}\right) = 0\\ &\Rightarrow \sum_{k=0}^{\infty}\sum_s b_s\alpha_{s,k}\exp\left(\frac{\pi izk}{p}\right) = 0\\ &\Rightarrow \sum_s b_s\alpha_{s,k} = 0 \quad \text{for all } k\end{aligned}$$

by uniqueness of representation of an absolutely convergent Fourier series. So by definition the function $r(s) = b_s$ defines a shape relation represented by the polynomial P. We shall give examples of shape relations later on. In fact, we will show that if $\mathscr{C}_5$ is the family of self-dual codes over $\mathbf{F}_5$, then Ker Φ_5 restricted to $\mathscr{C}_5$ is a principal ideal generated by a polynomial of degree 6.

(iii) This part follows from the fact that there are no non-trivial shape relations over $\mathbf{F}_2$ or $\mathbf{F}_3$, which we now prove. First note that for $p = 2$ or 3, a shape s is uniquely determined by $||s||^2$. Let r be a nontrivial shape relation on $\mathscr{S}$. Then $\sum_{s\in\mathscr{S}} r(s)\alpha_{s,k} = 0$ for all $k \in \mathbf{N}$. Let s_0 be the unique shape in $\mathscr{S}$ such that $r(s_0) \neq 0$ and $0 < ||s_0|| < ||s||$ for every $s \neq s_0$ such that $r(s) \neq 0$. Then

$$\sum_s r(s)\alpha_{s,||s_0||^2} = 0 \Rightarrow r(s_0)\alpha_{s_0,||s_0||^2} = 0.$$

This is true since if $||s|| > ||s_0||^2$, $\alpha_{s,||s_0||^2} = 0$ because $\alpha_{s,||s_0||^2} =$

https://doi.org/10.4153/CJM-1978-063-3 Published online by Cambridge University Press

card $\{y \in \mathbf{Z}^n | \ ||x + py|| = ||s_0||^2\}$ for any $x \in \mathbf{F}_p{}^n$ such that $\sigma(x) = s$, but if $||py + x||^2 = ||s_0||^2$ then $\sum_{i=1}^n ((py_i)^2 + 2py_ix_i) < 0$. But $|x_i| \leqq 1$, so each term in the sum is $\geqq 0$. However, since $\alpha_{s_0, ||s_0||^2} \neq 0$ we must have $r(s_0) = 0$ contradicting our choice of s_0.

3. Applications and examples. Theorem 1 may be used to construct modular forms, including modular forms of half-integral weight. It may also be applied to characterize the algebra of holomorphic modular forms for certain subgroups of the modular group. This application is demonstrated in [**14**] and will be more thoroughly discussed elsewhere.

We now consider the question of how much information about a code is contained in its Lee polynomial and theta series. We know there exist non-isomorphic codes with identical Hamming polynomials. For example, there are two non-isomorphic binary (16, 8) self-dual codes C_1 and C_2 with all weights divisible by 4 [**16**]. By Gleason's theorem [**6**], $P_{C_1} = P_{C_2}$. However, there is an algebraic similarity between the codes themselves. Let M_1 and M_2 be the matrices of the quadratic forms for the lattices $L(C_1)$ and $L(C_2)$. Then there is a rational matrix T such that $M_1 = TM_2T^t$. That is, the two quadratic forms are rationally congruent. We shall see that this is a consequence of the fact that $P_{C_1} = P_{C_2}$. The two lattices $L(C_1)$ and $L(C_2)$ represent the two isomorphism classes of even unimodular lattices in $\mathbf{R}^{16}$. Their theta series are identical, i.e. the sets of integers represented by their quadratic forms are identical. The result stated above concerning the congruence of the quadratic forms generated by C_1 and C_2 follows from

THEOREM (Kitaoka [**8**]). *Two even integral quadratic forms with identical theta series are rationally congruent.*

Theorem 1 and Kitaoka's theorem together imply:

THEOREM 2. *If the Lee polynomials of two linear codes over $\mathbf{F}_p$ are identical or differ by a shape relation, then their associated quadratic forms are rationally congruent.*

Kitoaka's result requires the quadratic forms involved to represent even integers, but we note that for any linear code C, the quadratic form associated with $2\sqrt{pL}(C) = 2L_0(C)$ represents even integers. Furthermore, two quadratic forms Q_1 and Q_2 represent the same numbers if and only if $2pQ_1$ and $2pQ_2$ represent the same integers and Q_1 and Q_2 are rationally congruent if and only if $2pQ_1$ and $2pQ_2$ are.

We wish to give an example involving shape relations, so we shall consider codes over $\mathbf{F}_5$, but first we make some observations:

a) If C is a self-dual code over $\mathbf{F}_p$, then $L(C)$ is a unimodular integral lattice, i.e. the quadratic form associated with $L(C)$ represents integers and the determinant of a basis of $L(C)$ is 1. We see that if C is self-orthogonal then $L(C)$ is

integral, and if C is a linear (n, k) code, then one may verify that $\det L(C) = p^{k-n/2}$. So if C is self-dual, $k = n/2$ and $\det L(C) = 1$. Furthermore, if C is doubly even, i.e. all weights are divisible by 4, then $L(C)$ is even (often referred to as Type II in the unimodular case), i.e. the quadratic form represents only even integers.

b) The graded **C**-algebra generated by theta series of all unimodular lattices of even dimension is free on 2 generators of degrees 2 and 8. The graded **C**-algebra generated by theta series of all even integral unimodular lattices is free on 2 generators of degrees 8 and 24. This is well known [**7**; **15**; **17**]. The first case follows from the fact that such a theta series is a modular form with character for the subgroup of $\Gamma = SL_2(Z)$ generated by $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ which we call Γ_θ. The second case follows because those theta series are modular forms for the full modular group. Unimodular Type II lattices must have dimension a multiple of 8.

Now let $\mathscr{C}_p$ be the family of self-dual linear codes over $\mathbf{F}_p$, and $\mathscr{C}_{2,l}$ be the family of self-dual doubly even binary codes. Gleason [**6**], and MacWilliams, Mallows, and Sloane [**11**] have studied the algebra $\mathscr{P}(\mathscr{C}_p)$ as a subalgebra of the algebra of invariants of a certain matrix group. For example,

$\mathscr{P}(\mathscr{C}_2)$ is the full algebra of invariants of a 2-dimensional representation of the dihedral group of order 16.

$\mathscr{P}(\mathscr{C}_{2,l})$ is the algebra of invariants of a unitary group generated by reflections of order 192.

$\mathscr{P}(\mathscr{C}_3)$ is the algebra of invariants of a unitary group of order 48.

$\mathscr{P}(\mathscr{C}_5)$ is the algebra of invariants of a 3-dimensional representation of the icosahedral group of order 120.

$\mathscr{P}(\mathscr{C}_7)$ is a subalgebra of invariants of the 4-dimensional complex representation of $SL(2, 7)$ which has order 336. See [**13a**] for more details of this interesting case.

Two elements of $\mathscr{P}(\mathscr{C}_2)$ are the polynomials for the code generated by (11) and the (8, 4) extended Hamming code. One may use these polynomials $x^2 + y^2$ and $x^8 + 14x^4y^4 + y^8$, and Theorem 1 to prove:

$$(2) \quad \mathscr{P}(\mathscr{C}_2) \approx \mathscr{T}(\mathscr{C}_2) = \mathscr{M}(\Gamma_\theta)$$

where this last algebra is the algebra of modular forms for Γ_θ. This proves part of Gleason's theorem, viz. that $\mathscr{P}(\mathscr{C}_2)$ is freely generated by polynomials of degree 2 and 8, in particular those given above. The fact that $\mathscr{P}(\mathscr{C}_{2,l})$ is freely generated by polynomials of degrees 8 and 24 may be proven using the extended (8, 4) Hamming code, the extended (24, 12) Golay code, Theorem 1 and the second case of observation b) above.

We also have by Theorem 1 and observation b), the following result.

THEOREM 3. *Φ_p maps $\mathscr{P}(\mathscr{C}_p)$ homomorphically into $\mathscr{M}(\Gamma_\theta)$.*

Φ_p is injective for $p = 2$ or 3, but has a kernel for $p \geqq 5$. We study the map Φ_5 restricted to $\mathscr{P}(\mathscr{C}_5)$:

THEOREM 4. *The image $\mathscr{T}(\mathscr{C}_5)$ of the algebra $\mathscr{P}(\mathscr{C}_5)$ under the map Φ_5 is free on 2 generators of degree 2 and 10. The kernel of Φ_5 restricted to $\mathscr{P}(\mathscr{C}_5)$ is a principal ideal of shape relations generated by a polynomial of degree 6, viz.* $x^4yz - x^2y^2z^2 + 2y^3z^3 - xz^5 - xy^5$.

Proof. MacWilliams, Mallows, and Sloane [**19**] have proven that $\mathscr{P}(\mathscr{C}_5)$ is freely generated by the polynomials of 3 codes:

$$F_2 = \mathbf{F}_5 \text{ span of } [1 \quad 2]$$

$$F_6 = \mathbf{F}_5 \text{ span of } \begin{bmatrix} 1 & 0 & 0 & 1 & -2 & -2 \\ 0 & 1 & 0 & -2 & 1 & -2 \\ 0 & 0 & 1 & -2 & -2 & 1 \end{bmatrix}$$

$$F_{10} = \mathbf{F}_5 \text{ span of } \begin{bmatrix} 1 & 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & -2 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 2 & -1 & 2 & 0 & -1 & -2 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Now $\Phi_5\mathscr{P}(\mathscr{C}_5) \subseteq \mathscr{M}(\Gamma_\theta)$, and the dimension of the homogeneous space of degree n of $\mathscr{M}(\Gamma_\theta)$ is $[n/8] + 1$. Hence the polynomials P_{F_6} and $P_{F_2}{}^3$ have the same image under Φ_5, and in fact this image is $\theta(\mathbf{Z}^6)$. $P_{F_2} = x^2 + 4yz$ and $P_{F_6} = x^6 + 60x^2y^2z^2 + 40y^3z^3 + 12(xy^5 + xz^5)$ hence $(1/12)(P_{F_2}{}^3 - P_{F_6}) = x^4yz - x^2y^2z^2 + 2y^3z^3 - xz^5 - xy^5$ is in the kernel of Φ_5 and represents a shape relation. Now $\theta(L(F_2))^5 = 1 + 20q + \ldots$ and $\theta(L(F_{10})) = 1 + 4q + \ldots$ are linearly independent and generate the homogenous space of degree 10 of $\mathscr{M}(\Gamma_\theta)$ which is also generated by $\theta(\mathbf{Z}^2)^5$ and $\theta(\mathbf{Z}^2)E_2$ where E_2 is the normalized Eisenstein series of weight 4 (weight k = degree $2k$). See [**17**]. $\theta(L(F_2))$ and $\theta(L(F_{10}))$ are algebraically independent for a relation between them would imply a relation between $\theta(\mathbf{Z}^2)$ and $\theta(\mathbf{Z}^2)E_2$ which would contradict the fact that $\mathscr{M}(\Gamma_\theta)$ is freely generated by $\theta(\mathbf{Z}^2)$ and E_2. Hence $P_{F_2}{}^3 - P_{F_6}$ generates the kernel of Φ_5 restricted to $\mathscr{P}(\mathscr{C}_5)$ and Theorem 4 is proved.

Theorem 2 implies that the lattices $L(F_2 \oplus F_2 \oplus F_2)$ and $L(F_6)$ have quadratic forms which are rationally congruent, but they are in fact integrally congruent although the 2 codes are not isomorphic.

4. Bounds on minimum distance. We consider a distance function on $\mathbf{F}_p{}^n$. Let $x \in \mathbf{F}_p{}^n$, and let $(x_1, \ldots, x_n)$ be the representation of x where the x_i are integers via the convention above. Then we define a function from $\mathbf{F}_p{}^n$ to the non-negative integers by

$$d(x) = \sum_{j=1}^{n} x_i{}^2 = ||x||^2.$$

$d(x - y)$ will be called the *squared Euclidean distance between x and y*. If $\mathscr{C}$ is a linear code over $\mathbf{F}_p$, then d restricted to $\mathscr{C}$ is translation invariant. For such a linear code C we shall be interested in its minimum squared Euclidean distance

$$d_m = \min_{x \in C - \{0\}} d(x).$$

If C is to be used to correct errors in information transmitted over certain channels under phase modulation, then d_m gives some idea of its performance [**1**].

For any self-orthogonal linear code C, d_m is equal to p times the subscript of the first nonzero coefficient of

$$\theta(L(C)) - \theta(pZ^n) = \sum_{k=d_m/p} b_k q^k$$

and if $p \geqq 3$, the number of vectors having squared length d_m is $b_{d_m/p}$. For $p = 2$ this number is $2^{-d_m} b_{d_m/p}$ because $+1 = -1$ in $\mathbf{F}_2$.

Now from the structure of the algebra $\mathscr{M}(\Gamma_\theta)$ which contains the image of $\mathscr{P}(\mathscr{C}_p)$ under Φ_p we know that for C an $(n, n/2)$ self-dual code over $\mathbf{F}_p$, $\theta(L(C))$ is the sum of at most $[n/8] + 1$ basis functions. It is well-known in the theory of modular forms [**17**] that the theta function of a unimodular integral lattice may be uniquely expressed as the sum of a cusp form and two Eisenstein series. One may use the theory of Hecke operators to show that the first $[n/8] - 1$ Fourier coefficients of such a cusp form determine the rest [**18**, p. 81]. Hence the first $[n/8] + 1$ coefficients of $\theta(L(C)) - \theta(p\mathbf{Z}^n)$ determine the rest, and it is quite unlikely that all of these coefficients will be 0. In fact, a formula for the $[n/8] + 1$ *st* coefficient has been found [**14**], although it is very unpleasant looking in the general case. The formula reinforces the conjecture that $d_m \leqq p([n/8] + 1)$ for all self dual codes over $\mathbf{F}_p$. This has been verified [**13b**] for $p = 2$ and is also true whenever $p > [n/8]$.

If we know more about the subalgebra of $\mathscr{M}(\Gamma_\theta)$ which is the image of $\mathscr{P}(\mathscr{C}_p)$ under Φ_p we might get a better upper bound for d_m. For example, Theorem 4 suggests an upper bound of $5[n/10] + 5$ for d_m for self-dual codes over $\mathbf{F}_5$. For $p = 3$ we know the dimension of the nth homogeneous space of $\mathscr{P}(\mathscr{C}_3)$ is $[n/12] + 1$ and the bound $d_m \leqq 3[n/12] + 3$ has been verified [**13b**]. And since $\mathscr{P}(\mathscr{C}_{2,1}) \approx \mathscr{M}(\Gamma)$ whose nth homogeneous space has dimension $[n/24] + 1$ we would expect $d_m \leqq 4[n/24] + 4$. This also has been verified in [**13b**]. Although these bounds are attained for small n, they may not be reached asymptotically. It has been shown that the last bound is not even achieved within a constant asymptotically [**12**].

References

1. E. R. Berlekamp, *Algebraic coding theory* (McGraw-Hill, N.Y., 1968).

2. M. Broué, *Codes correcteurs d'erreurs auto-orthogonaux sur le corps á deux elements et formes quadratiques entieres definies positives á discriminant* $+1$, Comptes Rendus des Journees

Mathematiques de la Societé Math. de France, Univ. Sci. Tech. Languedoc (Montpellier, 1974), 71–108.

3. M. Broué and M. Enguehard, *Polynomes des poids de certains codes et fonctions thêta de certains réseaux*, Ann. Scient. Ec. Norm. Sup. *5* (1972), 157–181.

4. J. H. Conway, *A group of order* 8,315,553,613,086,720,000, Bull. London Math. Soc. *1* (1969), 79–88.

5. ——— Invent. Math. *7* (1969), 137–142.

6. A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes Congres Internl. de Mathematique *3*, 1970 (Gauthier-Villars, Paris 1971), 211–215.

7. R. C. Gunning, *Lectures on modular forms* (Princeton Univ. Press, 1962).

8. Y. Kitaoka, *On the relation between the positive definite quadratic forms with the same representation numbers*, Proc. Japan Acad. *47* (1971).

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 *18* (1972), 794–805.

12. C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, *Upperbounds for modular forms, lattices, and codes*, J. Algebra *36* (1975), 68–76.

13a. C. L. Mallows and N. J. A. Sloane, *On the invariants of a linear group of order* 336, Proc. Camb. Phil. Soc. *74* (1973), 435–440.

13b. ——— *An upper bound for self-dual codes*, Information and Control *22* (1973), 188–200.

14. D. P. Maher, *Self-orthogonal codes and modular forms*, Ph.D. Thesis, Lehigh University, Bethlehem, Pa., 1976.

15. A. Ogg, *Modular forms and dirichlet series* (W. A. Benjamin, Inc., N.Y., 1969).

16. V. Pless, *A classification of self-orthogonal codes over* $GF(2)$, Discrete Math. *3* (1972), 209–246.

17. J. P. Serre, *A course in arithmetic* (Springer-Verlag, New York, 1970).

18. G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Princeton University Press, Princeton, N.J., 1971).

19. N. J. A. Sloane, *Codes over* $GF(4)$ *and complex lattices*, J. Algebra, to appear.

20. J. Tannery and J. Molk, *Elements de la theorie des fonctions elliptiques*, t.2 (Gauthier-Villars, Paris 1898).

Worcester Polytechnic Institute,
Worcester, Massachusetts