Can. J. Math., Vol. XXXII, No. 1, 1980, pp. 40–58

MODULAR FORMS FROM CODES

DAVID P. MAHER

1. Introduction. In this paper we construct modular forms from combinatorial designs, and codes over finite fields. We construct codes from designs, and lattices from codes. Then we use the combinatorial properties of the designs and the weight (or shape) structures of the codes to study the theta functions of the associated lattices. These theta functions are shown to be modular forms for the modular group or for various congruence subgroups. The levels of the forms we examine are determined by the dimensions of the codes and the characteristics of the fields. Using the Lee polynomial of the codes we can write the theta functions as homogeneous polynomials in modified Jacobi theta functions. By extending the underlying combinatorial structure, a modular form of half-integral weight is associated with a modular form of integral weight.

Our codes may be nonlinear. From these we construct *nonlinear lattices*—nonlinear sets in $\mathbf{R}^n$ which are finite unions of translates of lattices. In order to show that the theta functions of these nonlinear lattices are modular forms, we extend the classical theta function transformation formula. This is done by applying the MacWilliams equations for nonlinear codes.

Our methods enable us to give explicit bases for certain spaces of modular forms, and to express the members of these bases as polynomials in Jacobi theta functions. Theta function identities can be produced as a result of this process, and by identifying what we call shape relations [**17**].

Necessary details about modular forms may be found in [**21**], [**22**], or [**19**]. The method used here of treating modular forms of half-integral weight was introduced by Shimura [**23**]. Details about relationships between designs and codes may be found in [**15**], [**7**], and [**1**].

Broué and Enguehard showed close connections between weight polynomials of linear self-dual binary and ternary codes and theta functions of unimodular lattices in [**6**]. Many of their results are generalized here. Other papers which examine theta functions associated with codes are [**5**], [**17**], and [**24**].

2. Codes, designs and lattices. Throughout this article p shall denote a positive prime integer, and $\mathbf{F}_p$, the field with p elements. A *code* of length 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

Received January 18, 1978 and in revised form December 1, 1978.

subspace of $\mathbf{F}_p^n$. The *dual* of a linear (n, k) code C over $\mathbf{F}_p^n$ is the $(n, n-k)$ code

$$C^\perp = \{x \in \mathbf{F}_p^n | x \cdot y = 0, \forall\, y \in C\}.$$

Here $x \cdot y$ denotes the usual inner product over $\mathbf{F}_p$. A linear code C is said to be *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.

We shall consider codes over the field $\mathbf{F}_4$ whose elements will be denoted by $0, 1, \zeta, \zeta^2$ where $\zeta^2 + \zeta + 1 = 0$. For $\alpha \in \mathbf{F}_4$, its conjugate $\bar{\alpha}$ is α^2. We use the Hermitian inner product to define the dual of a code over $\mathbf{F}_4$:

$$C^\perp = \{x | x \cdot \bar{y} = 0 \,\forall\, y \in C\}.$$

Self-orthogonal and self-dual codes have been intensively studied and have connections with sphere packings and designs. Most of the codes we consider here are self-orthogonal or self-dual since we can classify their theta functions as modular forms. To give ourselves a plentiful supply of such codes, we construct them from designs. We can get several infinite classes of codes from these constructions. The parameters of the design underlying a code will be shown to specify the weight and level of the associated modular form. We shall also show that codes generated by certain designs generate two modular forms; one of integral weight of low level, and one of half-integral weight of generally higher level. We shall describe the relationship between the two modular forms via the weight enumerator of the code. We begin by describing some constructions of self-orthogonal and self-dual codes from designs after we set the notation.

A t-(b, v, k, λ) *design* is a pair $(\Omega, \mathscr{B})$ where Ω, the set of *points* or *varieties* has v elements, and $\mathscr{B}$, the set of *blocks*, is a set of subsets of Ω each having k elements, and such that card $\mathscr{B} = b$. The pair must satisfy the condition that any set of t elements of Ω are contained in exactly λ blocks. If $t = 2$ and $b = v$, we call the design *projective* (such designs are also called *symmetric*), and we refer to it as a (v, k, λ) design. A *projective plane* of order N is an $(N^2 + N + 1, N + 1, 1)$ design.

The *incidence matrix* of a design is a $b \times v$ matrix indexed by the blocks and points so that the i, j^{th} entry is 1 if the i^{th} block contains the j^{th} point, and is equal to 0 otherwise. Codes are formed from designs by taking the $\mathbf{F}_p$ spans of the rows of their incidence matrices. For example, the Steiner system of type $(5, 8, 24)$ is a 5-(759, 24, 8, 1) design. The $\mathbf{F}_2$ span of its incidence matrix is a self-dual code $C_{2,24}$ known as the extended (24, 12) binary Golay code. It is extended from a (23, 12) Golay code, also known as a quadratic residue code, by adding a parity check in the 24^{th} place of each code vector. This (23, 12) code is the $\mathbf{F}_2$ span of a Steiner system of type (4, 7, 23), a 4-(253, 23, 7, 1) design. This extension process will be generalized below and will play a crucial role in the development of a relationship between modular forms of integral and half-integral weight.

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

The extended code $C_{2,24}$ is *doubly even*, that is, the number of non-zero places in each code vector (known as the vector's *weight*) is divisible by 4. We shall see that this code is associated with a function which is a modular form of weight 12 for the full modular group. It has many other interesting properties: Its minimum non-zero weight is 8 which is best possible for a doubly even self-dual (24, 12) code. A lattice constructed from this code, the Leech lattice [**11**], yields a very dense, highly symmetric packing of $\mathbf{R}^{24}$. In fact, spheres of radius 2, centered at the lattice points, have non-intersecting interiors, and each sphere touches 196, 560 others. $C_{2,24}$ has connections with sporadic simple groups, as its automorphism group is the Mathieu group M_{24}, and the Conway group is a group of symmetries of the lattice. For more information on these connections, see [**8**] and [**11**].

Let A be the incidence matrix of a (v, k, λ) design, and let p be a prime such that $-\lambda$ is a square mod p. Let A_e be the $v \times (v+1)$ $\mathbf{F}_p$ matrix whose first v columns are the columns of A, and whose last column contains $\sqrt{-\lambda} \bmod p$ in each entry. In many cases the spans of A and A_e are self-orthogonal and self-dual codes:

PROPOSITION 1. *Let C be the $\mathbf{F}_p$ span of A, and let C_e be the $\mathbf{F}_p$ span of A_e. Then if $p|k-\lambda$ but $p^2 \nmid k-\lambda$ and $p \nmid k$ then*

(i) $C^{\perp} \subset C$ *with codimension* 1;

(ii) $C_e{}^{\perp} = C_e$.

The proof, which is elementary, can be found in [**1**] or [**16**], and also in [**20**] or [**7**] for the case of projective planes.

As an example, consider a projective plane of order N. Its parameters satisfy Proposition 1 if p divides N just once, so a putative plane of order 10 yields (112,56) self-dual codes over $\mathbf{F}_2$ and $\mathbf{F}_5$. The binary code is doubly even with minimum weight 12. These facts have lent impetus to the investigation of the difficult question of existence of a plane of order 10, [**14**], [**7**]. The plane of order 2 yields the (7, 4) binary Hamming code $C_{2,7}$ and the (8, 4) doubly even self-dual extended Hamming code $C_{2,8}$.

A *lattice* in $\mathbf{R}^n$ is a discrete $\mathbf{Z}$-module of rank n contained in $\mathbf{R}^n$. To each (n, k) code C over $\mathbf{F}_p$ we define a lattice $L(C)$ in $\mathbf{R}^n$ as follows:

$$x \in L(C) \Leftrightarrow \sqrt{p}x \in \mathbf{Z}^n \quad \text{and} \quad \sqrt{p}x \text{ reduced mod } p \text{ is in } C.$$

If C is a non-linear code, we can still define $L(C)$ as above but $L(C)$ is not a lattice, it is a finite union of translates of lattices which we call a *nonlinear lattice*. The *volume* of a lattice L is the absolute value of the determinant of a basis of L. It is also the measure of a fundamental rectangle. The dual of L is

$$L^{\perp} = \{x \in \mathbf{R}^n | \quad x \cdot y \in \mathbf{Z}, \forall\, y \in L\}$$

PROPOSITION 2 [**6**]. *For C an (n, k) code over $\mathbf{F}_p$:*

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

(i) $L(C^{\perp}) = L(C)^{\perp}$;

(ii) $\mathrm{vol}(L(C)) = p^{n/2-k}$

(iii) *If* $p = 2$ *then* $x \cdot x$ *is even for every* $x \in L(C)$ *if and only if* C *is doubly even.*

The proof is straightforward and is omitted.

Example. $C_{2,8}$, the extended code we produced from the projective plane of order 2, is a doubly even self-dual code, hence by Proposition 2, $L(C_{2,8})$ is self-dual and *even*, i.e. its vectors are of even squared length. Such a lattice is also said to be unimodular and of Type II. Up to isomorphism there is only one type II unimodular lattice in $\mathbf{R}^8$, hence $L(C_{2,8})$ is the lattice of the Lie algebra of type E_8 [**21**]. $L(C_{2,24})$ is also type II unimodular, one of 24 such in $\mathbf{R}^{24}$. It is not the Leech lattice (one must use a bit more complicated construction to get that lattice), but is the lattice associated with the Lie algebra of type A_{24}. See [**18**].

Any 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. Set $A = MM^t$, t denoting transpose. $Q(x) = xAx^t$. If C is a self-orthogonal code then the quadratic form for $L(C)$ represents integers, and if C is doubly even also, then the form represents even integers.

Complex lattices constructed from codes over $\mathbf{F}_4$ are discussed at the end of the next section.

3. Enumerating polynomials and theta functions. Important in the study of codes are polynomials which count the number of vectors in each code which belong to respective classes. For example, the Hamming weight polynomial $W_C(X, Y)$ of a code C is a polynomial which enumerates the number of vectors in C in each possible weight class, where the weight of a vector x, denoted $\mathrm{wt}(x)$, is the number of non-zero elements in its coordinate places:

$$(1) \qquad W_C(X, Y) = \sum_{x \in C} X^{n-wt(x)} Y^{wt(x)}.$$

Let M_n denote the group of $n \times n$ monomial matrices with ± 1 as non-zero entries. We let M_n act naturally on $\mathbf{F}_p{}^n$ and let

$$\sigma : \mathbf{F}_p{}^n \to \mathbf{F}_p{}^n/M_n$$

be the canonical map of the induced equivalence relation. For $x \in \mathbf{F}_p{}^n$, we call $\sigma(x)$ the *shape* of x. $\sigma(x) = \sigma(y)$ 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

$$(2) \qquad P_C = \sum_{x \in C} \sigma(x) = \sum_{s \in \mathscr{S}} a_s s$$

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

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

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 less than or equal to ω. $\mathbf{F}_2 = \{0, 1\}$. We shall view P_C as a homogeneous 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

$$(3) \qquad P_C(X_0, X_1, \ldots, X_\omega) = \sum_{x \in C} X_0{}^{\sigma_0(x)} X_1{}^{\sigma_1(x)} \ldots X_\omega{}^{\sigma_\omega(x)}.$$

When $p = 2$ or 3, P_C is the Hamming weight polynomial (1). In general we call P_C the *Lee polynomial* of C.

Often a code vector $x \in \mathbf{F}_p{}^n$ will play the role of an integer vector. For example we define

$$||x||^2 = \sum_{j=1} x_j{}^2$$

where x_j is an integer such that $|x_j| \leqq \omega$. Context should eliminate any ambiguity. If s is a shape, we define $||s||^2 = ||x||^2$ where $\sigma(x) = s$. $\sigma_i(s)$ is the number of occurrences of $\pm i$ in x. For $s \in \mathscr{S}$ we will always suppose $x(s)$ to be some representative of s.

The enumerating function of a lattice L, its *theta series*, is defined

$$(4) \qquad \Theta_L = \sum_{x \in L} q^{||x||^2} = \sum_{z \in Z^n} q^{zAz^t}.$$

If the quadratic form for L represents integers only then

$$(5) \qquad \Theta_L = \sum_{k=0}^{\infty} b_k q^k \quad \text{where } b_k = \operatorname{card}\{x \in L \mid ||x||^2 = k\}.$$

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 holomorphic function on $\mathbf{H}$, and is said to be holomorphic at ∞ by virtue of the fact that (5) converges for $q = \exp(\pi i z)$, since $b_k < n^k$ for all k.

Let s be a shape and $x(s)$ a representative of s. We consider $\{x(s)\}$ as a single element, non-linear code. Denote the coefficients of the theta function of $\{x(s)\}$ by $\alpha_{s,k}$. Then

$$(6) \qquad \alpha_{s,k} = \operatorname{Card}\{y \in p\mathbf{Z}^n \mid ||x(s) + y||^2 = k\}.$$

This is the number of vectors in $L(\{x(s)\})$ at squared distance k from the origin. One may readily show that $\alpha_{s,k}$ is independent of the representative $x(s)$ of s. Consider a formal shape polynomial

$$(7) \qquad \sum r_s s \equiv \sum r_s X^{\sigma_0(s)} X_1{}^{\sigma_1(s)} \ldots X_\omega{}^{\sigma_\omega(s)}.$$

We shall say that (7) defines a *shape relation* if $\sum r_s \theta_s(z) \equiv 0$ where θ_s is the theta function of the code $\{x(s)\}$. Equivalently, (7) defines a shape relation if

$$(8) \qquad \sum r_s \alpha_{s,k} = 0 \quad \text{for all } k.$$

Shape relations are interesting because

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

(i) They define relations among theta functions.

(ii) As polynomials, they form ideals which are the kernels of the homomorphisms we shall define which map algebras of Lee polynomials into algebras of modular forms.

(iii) A shape relation holds the difference in information given by the shape enumerator of a code and that given by the theta function.

There are no shape relations for shapes over $\mathbf{F}_p$, $p = 2$ or 3, but there are for $p \geqq 5$. See [**17**].

The main result of [**17**] showed that the theta function of a code can be obtained by evaluating the Lee polynomial of the code on a set of modified Jacobi theta functions. We need to introduce a classical Jacobi theta function [**25**]:

$$\Theta_3(v|z) = \sum_{m\in\mathbf{Z}} \exp(\pi i m^2 z + 2\pi i m v) \tag{9}$$

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

$$\phi_{p,l}(z) = \exp(l^2 \pi i z/p)\,\Theta_3(lz|pz) \tag{10}$$

so that

$$\phi_{2,1}(z) = \Theta_2(0|2z) = \exp(\pi i z/2)\,\Theta_3(z|2z)$$

in the notation of [**25**].

Let $\mathscr{A}$ be a family of codes over $\mathbf{F}_p$, and let $\mathscr{P}(\mathscr{A})$ be the graded subalgebra of $\mathbf{C}[X_0, \ldots, X_\omega]$ generated by the Lee polynomials of the elements of $\mathscr{A}$. The grading is by homogeneous degree, or equivalently, according to the ambient dimensions or lengths of the associated codes. Let $\mathscr{T}(\mathscr{A})$ be the graded algebra of holomorphic functions on $\mathbf{H}$ generated by the theta functions $\Theta_{L(C)}(z)$ of elements of $\mathscr{A}$.

THEOREM 3 [**17**]. *If $\mathscr{A}$ is any family of codes over $\mathbf{F}_p$, then*

(i) $P_C(\phi_{p,0}(z), \ldots, \phi_{p,\omega}(z)) = \Theta_{L(C)}(z)$ *and hence the function* $P_C \to \Theta_{L(C)}$ *defined on the generators of* $\mathscr{P}(\mathscr{A})$ *may be extended to an algebra homomorphism* $\Phi_p : \mathscr{P}(\mathscr{A}) \to \mathscr{T}(\mathscr{A})$.

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

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

Theorem 3(i) was proven for $p = 2$ and 3 by Broué and Enguehard in [**6**]. Sloane [**24**] has proven an analog of (i) for codes over $\mathbf{F}_4$ using complex lattices:

Consider the Eisenstein integers $\mathscr{E} = \{a + b\zeta | a, b \in \mathbf{Z}\}$ where $\zeta = \exp(2\pi i/3)$. Since $\zeta^2 + \zeta + 1 = 0$ in $\mathscr{E}$ there is a natural reduction from $\mathscr{E}$ to $\mathbf{F}_4$. An $\mathscr{E}$-lattice is a rank n discrete $\mathscr{E}$-module contained in $\mathbf{C}^n$. To each (n, k) code C over $\mathbf{F}_4$ we may associate an n-dimensional $\mathscr{E}$-lattice $\Lambda(C)$ which consists of all vectors $x \in \mathbf{C}^n$ which can be obtained by adding twice an Eisenstein integer to each component of a code vector and then dividing by $\sqrt{2}$.

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

The theta function of a complex lattice is defined as in (7) except that for $x \in \mathbf{C}^n$, $||x||^2 = x \cdot \bar{x}$. Now set

$$\psi_0(z) = \Theta_2(0|2z)\Theta_2(0|6z) + \Theta_3(0|2z)\Theta_3(0|6z) \tag{11}$$

$$\psi_1(z) = \Theta_2(0|2z)\Theta_3(0|6z) + \Theta_2(0|6z)\Theta_3(0|2z) \tag{12}$$

then

$$\psi_0(z) = \Theta_{\sqrt{2}\mathcal{E}}(z) \quad \text{and} \quad \psi_1(z) = \Theta_{\frac{1}{2}+\sqrt{2}\mathcal{E}}(z).$$

THEOREM 4. (Sloane [**24**]) *If C is a code over $\mathbf{F}_4$ then*

$$\Theta_{\Lambda(C)}(z) = W_C(\psi_0(z), \psi_1(z)).$$

The Poisson summation formula [**4**] gives a relation between the sum or integral of the values of a function defined on a topological group and the sum or integral of the values of the Fourier transform of the function defined on the dual group. When this formula is applied to lattices it yields the theta function transformation formula:

$$\Theta_{L^\perp}(z) = (z/i)^{-n/2}\,\mathrm{vol}(L)\,\Theta_L(-1/z). \tag{13}$$

When the formula is applied to linear codes [**10**], [**16**], it yields the MacWilliams relations for code enumerating polynomials. For Hamming polynomials we have:

$$P_{C^\perp}(X, Y) = (\mathrm{Card}(C))^{-1}P_C(X + (p-1)Y, X - Y). \tag{14}$$

For Lee polynomials it's a bit more complicated:

For $p \geqq 3$, l, j integers set

$$\lambda(l, 0) = 1 \quad l \in \mathbf{Z} \tag{15}$$
$$\lambda(l, j) = \exp(2\pi i l j/p) + \exp(-2\pi l j/p) \quad j \neq 0$$

then

$$P_{C^\perp}(X_0, X_1, \ldots, X_\omega) = (\mathrm{Card}(C))^{-1} \times P_C\Big(\textstyle\sum_{j=0}^{\omega}\lambda(0, j)X_j, \sum_{j=0}^{\omega}\lambda(1, j)X_j, \ldots, \sum_{j=0}^{\omega}\lambda(\omega, j)X_j\Big). \tag{16}$$

These formulas may be organized as follows:

$$P_{C^\perp}(X_0, X_1, \ldots, X_\omega) = (\mathrm{Card}(C))^{-1}p^{n/2}P_C((X_0, X_1, \ldots, X_\omega)M_p) \tag{17}$$

where M_p is a matrix acting on the row vector $(X_0, X_1, \ldots, X_\omega)$ and

$$M_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad M_3 = \frac{1}{\sqrt{3}}\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix},$$

$$M_5 = \frac{1}{\sqrt{5}}\begin{pmatrix}1 & 2 & 2\\ 1 & \alpha+\alpha^4 & \alpha^2+\alpha^3\\ 1 & \alpha^2+\alpha^3 & \alpha+\alpha^4\end{pmatrix} \quad \alpha = e^{2\pi i/5},$$

$$M_7 = \frac{1}{\sqrt{7}}\begin{pmatrix}1 & 2 & 2 & 2\\ 1 & \beta+\beta^6 & \beta^2+\beta^5 & \beta^3+\beta^4\\ 1 & \beta^2+\beta^5 & \beta^3+\beta^4 & \beta+\beta^6\\ 1 & \beta^3+\beta^4 & \beta+\beta^6 & \beta^2+\beta^5\end{pmatrix} \quad \beta = e^{2\pi i/7}, \ldots.$$

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

MacWilliams, Sloane, and Goethals [**13**] proved (16) for nonlinear codes after defining the dual weight (shape) enumerator of a nonlinear code. They also define a formal dual for nonlinear binary codes that has the property that $C^{\perp\perp} = C$ if C contains the zero vector. This dual is consistent with their definition of dual weight enumerator.

We shall briefly paraphrase the development of the dual enumerator of a nonlinear code C given in [**13**] for those cases in which we are interested. We want a definition of the dual shape enumerator of a code C such that

(i) If C is linear, the dual enumerator is the enumerator of $C^{\perp}$.
(ii) The MacWilliams equations hold formally for nonlinear codes.

For C linear, the MacWilliams equation asserts that $P_{C^{\perp}}$ is equal to the average over C of the formal Fourier transform values of the shape function $x \to \sigma(x)$. This is seen to be true by applying the Poisson summation formula to the code $C^{\perp}$, using the fact that $C = C^{\perp\perp}$ is isomorphic to the character dual of $\mathbf{F}_p{}^n/C^{\perp}$. So in order to satisfy (i) and (ii) for C arbitrary, we define the dual shape enumerator $P_{C^{\perp}}$ by

$$(18) \quad P_{C^{\perp}} = \sum a_s{}^{\perp} s$$

where the coefficient $a_s{}^{\perp}$ is defined by an averaging process similar to the one mentioned above. We need to give the following definitions in order to explicitly define $a_s{}^{\perp}$ as in [**13**]:

Let G be a copy of the group $\mathbf{F}_p{}^n$ but with the addition operation of $\mathbf{F}_p{}^n$ written as multiplication in G. Now we can consider the group algebra $\mathbf{C}[G]$. The standard characters of $\mathbf{F}_p{}^n$ may be defined on G and linearly extended to $\mathbf{C}[G]$. Let C be a code with elements $x_1, \ldots, x_u$. Set $\bar{C}$ equal to $x_1 + x_2 + \ldots + x_u$ considered as an element of $\mathbf{C}[G]$. For $y \in \mathbf{F}_p{}^n$, let $\chi_{\bar{y}}$ be the character associated with its image $\bar{y}$ in $\mathbf{C}[G]$. We define $a_s{}^{\perp}$ to be the complex number

$$(19) \quad a_s{}^{\perp} = (\mathrm{Card}(C))^{-1} \sum_{\sigma(y)=s} \chi_{\bar{y}}(\bar{C})$$

where the sum is over all $y \in \mathbf{F}_p{}^n$ which have shape s. Since

$$\chi_{\bar{y}}(\bar{C}) = \sum_i \chi_{\bar{y}}(\bar{x}_i),$$

we see that in defining $a_s{}^{\perp}$ we are averaging the values of the character χ_y on the elements of C. The introduction of the group algebra permits the MacWilliams equations to be proven in a formal framework which allows averaging the values of $\chi_{\bar{y}}$ on elements of $\mathbf{C}[G]$ which correspond to codes equivalent to C. The details are in [**13**] where it is shown that (17) is satisfied with $P_{C^{\perp}}$ replaced by $P_{C^{\perp}}$, and that $P_{C^{\perp}} = P_{C^{\perp}}$ when C is linear.

Although the dual weight enumerator of a nonlinear code is not always the enumerator of another code, many pairs of nonlinear codes are known whose enumerators satisfy (17), and there are many nonlinear codes C with the property that $P_{C^{\perp}} = P_C$. These are called *formally self-dual* codes. Examples

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

may be found in [**13**]. The lattices of some of these codes are interesting in that they yield sphere packings which are denser than any of the known linear packings. So we would like a theta function transformation formula for non-linear lattices induced from codes. Such a formula will be used later to show that the theta functions of lattices formed from formally self-dual codes such as the Nordstrom-Robinson code of length 16, are modular forms. We define the *dual theta function* for a nonlinear code C in $\mathbf{F}_p^n$ to be

$$\Theta_{L(C)}^{\perp}(z) = \sum_{s\in\mathscr{S}} a_s^{\perp}\phi_{p,0}^{\sigma_0(s)}(z)\phi_{p,1}^{\sigma_1(s)}(z)\ldots\phi_{p,\omega}^{\sigma_\omega(s)}(z) \tag{20}$$

where $a_s^{\perp}$ is defined by (19).

If C is linear, then $\theta_{L(C)}^{\perp} = \theta_{L(C^{\perp})}$.

We define the *volume* of a non-linear lattice induced from a code C to be $\mathrm{Card}(C)/p^{n/2}$.

THEOREM 5. *If C is any code in $\mathbf{F}_p^n$, linear or not, then*

$$\theta_{L(C)}^{\perp}(z) = (z/i)^{-n/2}\,\mathrm{vol}(L(C))\theta_{L(C)}(-1/z).$$

We first prove

LEMMA.

$$\phi_{p,l}(-1/z) = (z/i)^{\frac{1}{2}}p^{-1/2}\Big(\sum_{j=0}^{\omega}\lambda(l,j)\phi_{p,j}(z)\Big) \quad p \neq 2; \tag{21}$$

$$\phi_{2,0}(-1/z) = (z/i)^{\frac{1}{2}}2^{-1/2}(\phi_{2,0}(z) + \phi_{2,1}(z)); \tag{22}$$

$$\phi_{2,1}(-1/z) = (z/i)^{\frac{1}{2}}2^{-1/2}(\phi_{2,0}(z) - \phi_{2,1}(z)); \tag{23}$$

where $\lambda(l,j)$ is defined by (15).

Equations (22) and (23) were proved in [**6**] and may also be deduced by appropriately modifying the following proof of (21):
Define

$$\mathscr{D}(z,x,y) = \sum_{m\in\mathbf{Z}}\exp(\pi iz(m-y)^2 + 2\pi imx - \pi ixy) \tag{24}$$

where $z \in \mathbf{H}$; $x, y \in \mathbf{C}$. The transformation formula for this function is given in [**9**]:

$$\mathscr{D}(z,x,y) = (-iz)^{-1/2}\mathscr{D}(-z^{-1}, y, -x). \tag{25}$$

By (10), (25), and (24) we have that

$$\begin{aligned}\phi_{p,l}(-1/z) &= \exp(-l^2\pi i/pz)\,\mathscr{D}(-p/z, -l/z, 0)\\ &= \exp(-l^2\pi i/pz)\cdot(-ip/z)^{-1/2}\mathscr{D}(z/p, 0, l/z)\\ &= p^{-1/2}(z/i)^{1/2}\sum_{m\in\mathbf{Z}}\exp(\pi im^2z/p - 2\pi iml/p).\end{aligned} \tag{26}$$

Now the sum in (26) may be written as

$$\begin{aligned}&\sum_{k\in p\mathbf{Z}}\sum_{j=-\omega}^{\omega}\exp(\pi i(k+j)^2z/p - 2\pi i(k+j)l/p)\\ &= \sum_{j=-\omega}^{\omega}\sum_{m\in\mathbf{Z}}\exp(\pi i(pm^2z + 2imjz + j^2z/p + 2iml - 2ijl/p))\\ &= \sum_{j=-\omega}^{\omega}\exp(2\pi ijl/p)\exp(j^2\pi iz/p)\sum_{m\in\mathbf{Z}}\exp(\pi ipm^2z + 2\pi imjz)\\ &= \sum_{j=0}^{\omega}\lambda(l,j)\phi_{p,j}(z),\end{aligned}$$

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

and the lemma is proved. Now Theorem 5 follows from the lemma, Theorem 3, and the fact that the MacWilliams relations (16) hold for nonlinear as well as linear codes.

4. Modular forms of integral weight. We begin by introducing notation and results for modular forms of integral weight and apply the theory of Sections 1 and 2 to determine the structure of the algebra of modular forms for certain congruence subgroups.

$$\textit{Set } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Set $\Gamma = SL_2(\mathbf{Z})$, the group generated by $\pm S$ and $\pm T$. Γ_θ is the subgroup generated by $\pm S$ and $\pm T^2$. For N a positive integer, we set

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | c \equiv 0 \bmod N \right\}$$

$$\Gamma_0(N, 2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) | b \equiv 2 \bmod N \right\}$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

For $\Gamma' \subseteq \Gamma$, let $\overline{\Gamma}'$ denote the image of Γ' under the canonical map $SL_2(\mathbf{Z}) \twoheadrightarrow PSL_2(\mathbf{Z})$.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, f a function on $\mathbf{H}$, $k \in \mathbf{Z}$, we set

$$(27) \quad f|[\gamma]_k = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

We define a *modular form of weight k* for a subgroup Γ' of Γ to be a function f holomorphic on $\mathbf{H}$, and at the cusps of Γ', (see [**22**], p. 29) that satisfies

$$(28) \quad f|[\gamma]_k = f \quad \text{for all } \gamma \in \Gamma'.$$

The space of all such functions will be denoted by $\mathscr{M}_k(\Gamma')$, and if χ is a non-trivial character of Γ', and if instead of (28), f satisfies

$$(29) \quad \chi(\gamma)^k f|[\gamma]_k = f$$

then we will say that f is a modular form with character χ and write $f \in \mathscr{M}_k(\Gamma', \chi)$. The algebra of modular forms for a given subgroup Γ' of Γ graded over all weights divisible by d is denoted by

$$\mathscr{M}^d(\Gamma') = \bigoplus_{\substack{k=0 \\ d|k}}^{\infty} \mathscr{M}_k(\Gamma').$$

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

PROPOSITION 6. (i) *If C is a formally self-dual code in $\mathbf{F}_p^n$, then $\Theta_{L(C)}$ is in $\mathscr{M}_{n/2}(\bar{\Gamma}_\Theta, \chi)$ where $\chi(T^2) = 1$ and $\chi(S) = i$.*

(ii) *If C is a doubly even, formally self-dual code in $\mathbf{F}_2^n$ then $\Theta_{L(C)}$ is in $\mathscr{M}_{n/2}(\bar{\Gamma})$.*

Proof. The theta function of a formally self-dual code has an expansion in $\exp(\pi i z)$, hence it is invariant under $z \to z + 2$. If the code is doubly even, it has an expansion in $\exp(2\pi i z)$, so it is invariant under $z \to z + 1$. By Theorem 5 we have that (29) is satisfied for $\gamma = S$ in cases (i) and (ii). To finish case (ii) we must have that (28) is satisfied for S, but then n would have to be divisible by 8. But all doubly even self-dual codes are of length divisible by 8. For linear codes this follows from the classification theory for type II, unimodular lattices [**21**]; it follows in general by this argument of Serre's: If $n \not\equiv 0 \bmod 8$ in case (ii), then by taking direct sums, if necessary, we can get a lattice L in dimension m such that $m \equiv 4 \bmod 8$, and then by Theorem 5,

$$\Theta_L(-1/z) = (-1)^{m/4} z^{m/2} \Theta_L(z).$$

So the differential form $\alpha = \Theta_L(z) dz^{m/4}$ is transformed into $-\alpha$ by S. Since α is invariant under T, ST transforms α into $-\alpha$, but a contradiction arises since $(ST)^3 = 1$.

Let $\mathscr{A}_p$ denote the family of formally self-dual codes over $\mathbf{F}_p$, and let $\mathscr{A}_l$ denote the family of elements of $\mathscr{A}_2$ which are doubly even.

THEOREM 7. (i) *Φ_2 maps $\mathscr{P}(\mathscr{A}_l)$ isomorphically onto $\mathscr{M}^4(\bar{\Gamma})$;*

(ii) *Φ_2 maps $\mathscr{P}(\mathscr{A}_2)$ isomorphically onto $\mathscr{M}^1(\bar{\Gamma}_\theta, \chi)$;*

(iii) *Φ_p maps $\mathscr{P}(\mathscr{A}_p)$ homomorphically into $\mathscr{M}^1(\bar{\Gamma}_\theta, \chi)$; the kernel being an ideal of shape relations on $\mathbf{F}_p^n$.*

Proof. Except for the ontoness claims, the theorem follows from Proposition 6 and Theorem 3. Now recall the doubly even self-dual binary codes $C_{2,8}$ and $C_{2,24}$ formed from the projective plane of order 2 and the 5-(759, 24, 8, 1) design. Let their theta functions be denoted by f and g. They are in $\mathscr{M}_4(\bar{\Gamma})$ and $\mathscr{M}_{12}(\bar{\Gamma})$ respectively. In fact $f(z)$ is the normalized Eisenstein series

$$E_2(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$$

and

$$(1/42)(f^3 - g) = q - 24q + 252q - \ldots = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \Delta(z)$$

where $q = e^{2\pi i z}$. It is well known [**21**], [**19**] that E_2 and Δ freely generate $\mathscr{M}^4(\bar{\Gamma})$, hence (i) follows. Now let $C_{2,2}$ be the (2, 1) self-dual code consisting of the vectors (1, 1) and (0, 0). $L(C_{2,2}) \approx \mathbf{Z}^2$. By Proposition 6, its theta function is in $\mathscr{M}_1(\bar{\Gamma}_\theta, \chi)$. It is well known [**19**], [**6**] that $\mathscr{M}^1(\bar{\Gamma}_\theta, \chi)$ is free on 2 generators of weights 1 and 4. $\Theta_{L(C_{2,2})}$ and $\Theta_{L(C_{2,8})}$ may be taken as those generators.

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

Since

$$P_{C_{2,2}} = X^2 + Y^2, \quad P_{C_{2,8}} = X^8 + 14X^4Y^4 + Y^8,$$
$$P_{C_{2,24}} = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24},$$
$$\tfrac{1}{4}(P^4_{C_{2,2}} - P_{C_{2,8}}) = X^2Y^2(X^2 - Y^2)^2$$
$$(1/42)(P^8_{C_{2,8}} - P_{C_{2,24}}) = X^4Y^4(X^4 - Y^4)^4,$$

we have as a corollary:

THEOREM 8. (Gleason [**10**]) (i) $\mathscr{P}(\mathscr{A}_2)$ *is freely generated by* $X^2 + Y^2$ *and* $X^2Y^2(X^2 - Y^2)^2$

(ii) $\mathscr{P}(\mathscr{A}_1)$ *is freely generated by* $X^8 + 14X^4Y^4 + Y^8$ *and* $X^4Y^4(X^4 - Y^4)^4$.

These are also integral generators. More direct proofs of this important theorem may be found in [**13**].

Let A be an $n \times n$ matrix for an even integral quadratic form, then A is a symmetric matrix with integral entries and even integral entries on its diagonal. Given a positive integer N we say that A has level N if NA^{-1} is also even integral. It is well known that if A has level N, the theta function $\sum_{z\in\mathbf{Z}^n} \exp(\pi i z A z^t)$ is a modular form for $\Gamma_0(N)$ with character $\left(\frac{\det A}{d}\right)$. This also follows from Shimura's transformation formula of Proposition (13) below.

THEOREM 9. (i) *If* C *is a self-orthogonal doubly even* $(4m, k)$ *code over* $\mathbf{F}_2$ *containing the all-one vector then*

(i) $\Theta_{L(C)}(z) \in \mathscr{M}_{2m}(\bar{\Gamma}_0(2))$.

(ii) Φ_2 *maps* $\mathbf{C}[X^4 + Y^4, X^4Y^4]$ *isomorphically onto* $\mathscr{M}^4(\Gamma_0(2))$.

Proof. Let $C_{2,4}$ be the binary code consisting of the two vectors (1111) and (0000). $P_{C_{2,4}} = X^4 + Y^4$, and the quadratic form for $L(C_{2,4})$ is given by

$$\begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 2 \end{bmatrix}$$

This matrix has determinant 4 but level 2, hence by the above remark

$$\Theta_{C_{2,4}} \in \mathscr{M}_2(\bar{\Gamma}_0(2)).$$

The character is trivial on $\bar{\Gamma}_0(2)$. Clearly

$$\Theta_{C_{2,8}} \in \mathscr{M}_4(\bar{\Gamma}_0(4)).$$

Now $X^4Y^4 = (1/12)(P_{C_{2,8}} - P^2_{C_{2,4}})$ hence

$$\Phi_2(\mathbf{C}[X^4 + Y^4, X^4Y^4]) \subseteq \mathscr{M}(\bar{\Gamma}_0(2)).$$

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

One calculates (see [**22**] p. 46) that

$$\dim \mathscr{M}_{n/2}(\bar{\Gamma}_0(2)) = \left[\frac{n}{8}\right] + 1,$$

hence the mapping is onto. It is injective by Theorem 3, so (ii) is proved. (i) follows since the polynomial of any linear doubly even code containing the all-one vector is in $\mathbf{C}[X^4 + Y^4, X^4Y^4]$.

COROLLARY. *A function holomorphic on* $\mathbf{H}$ *and the cusps of* $\bar{\Gamma}_0(2)$ *is a modular form for* $\bar{\Gamma}_0(2)$ *if and only if it can be written as a symmetric polynomial in the Jacobi theta functions* $\phi_{2,0}{}^4(z)$ *and* $\phi_{2,1}{}^4(z)$.

THEOREM 10.

$$\mathbf{C}[X^4, Y^4] \overset{\Phi_2}{\approx} \mathbf{C}[\phi_{2,0}^4(z), \phi_{2,1}^4(z)] = \mathscr{M}^4(\bar{\Gamma}_0(4)).$$

The proof is similar to the proof of Theorem 9. Use the code $C_{2,4}$ and the code containing only (0000). Also note that

$$\dim \mathscr{M}_{n/2}(\bar{\Gamma}_0(4)) = \left[\frac{n}{4}\right] + 1.$$

Given a series $f = \sum_{n\in\mathbf{Z}} a_n q^n$, we decompose f into even and odd parts, $f = f_e + f_0$, where $f_e = \sum_{n\in 2\mathbf{Z}} a_n q^n$ and $f_0 = f - f_e$. If $\mathscr{M}$ is a space of functions with expansions in q, we denote by $\mathscr{M}_e$ the space of even parts of $\mathscr{M}$, and by $\mathscr{M}_0$ the space of odd parts.

THEOREM 11. *For* $k \in 2\mathbf{Z}$:
(i) $\mathscr{M}_k(\bar{\Gamma}(2)) = \mathscr{M}_k(\bar{\Gamma}_\theta, \chi)_e \oplus \mathscr{M}_k(\bar{\Gamma}_\theta, \chi)_0$;
(ii) $\mathscr{M}_k(\bar{\Gamma}_0(2)) = \mathscr{M}_k(\bar{\Gamma}_\theta, \chi)_e$.

Proof. Let f be in $\mathscr{M}_k(\bar{\Gamma}_\theta, \chi)$. Then by Theorem 7, f is a sum $\sum \alpha_i \Theta_i$ of theta functions Θ_i of lattices $L(C_i)$ of self-dual binary codes. We can assume the C_i to be linear, in fact direct sums of $C_{2,2}$'s and $C_{2,8}$'s. Now the even part of each Θ_i is the theta function of the sublattice of index 2 of $L(C_i)$ consisting of all vectors of even squared length, and this sublattice is the lattice of the maximal doubly even subcode of C_i. Since $n \equiv 0 \bmod 4$, this subcode contains the all-one vector. Hence by Theorem 9, the even part of Θ_i is in $\mathscr{M}(\bar{\Gamma}_0(2))$ for all i, and so f_e is. This proves (ii), since the dimension of both $\mathscr{M}_k(\bar{\Gamma}_0(2))$ and $\mathscr{M}_k(\bar{\Gamma}_\theta, \chi)_e$ is $\left[\frac{k}{4}\right] + 1$. Both $\bar{\Gamma}_0(2)$ and $\bar{\Gamma}_\theta$ contain $\bar{\Gamma}(2)$, and χ_θ is trivial on $\bar{\Gamma}(2)$, so f, f_e and hence f_0 are in $\mathscr{M}_k(\bar{\Gamma}(2))$. The dimension of $\mathscr{M}_k(\bar{\Gamma}(2))$ is $k/2 + 1$ which is the sum of the dimensions on the right hand side of (i) ($\dim \mathscr{M}_k(\Gamma_\theta, \chi)_0 = \left[\frac{k}{4}\right]$, not $\left[\frac{k}{4}\right] + 1$, since the space is spanned by isobaric polynomials in $\Theta_{\mathbf{Z}^4}$ and the Eisenstein series E_2, but E_2 has no odd part).

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

Sloane [**24**] uses similar techniques including Theorem 4 and a transformation formula for theta functions of $\mathscr{E}$-lattices (analog of (13)), to show that $\mathscr{P}(\mathscr{C}_4)$, the algebra generated by Hamming weight polynomials of self-dual codes over $\mathbf{F}_4$, is isomorphic to the algebra of modular forms for the subgroup of substitutions of $\mathbf{H}$ generated by $z \to z + \sqrt{3}$ and $z \to (-1/z)$. He also shows that if Λ is a self-dual $\mathscr{E}$-lattice in $\mathbf{C}^n$, then $\Theta_\Lambda(2z)$ is a modular form of weight n for $\bar{\Gamma}_0(3)$. But $\mathscr{M}(\bar{\Gamma}_0(3))$ is not generated by the theta functions of these lattices. However, using Sloane's work, we can describe the structure of this algebra in terms of the Jacobi theta functions.

Sloane shows that the function

$$\Delta_6(z) = q\prod_{m=1}^{\infty}(1 - q^m)^6(1 - q^{3m})^6$$

is a linear combination of theta functions of self-dual codes over $\mathbf{F}_4$. $\Delta_6(2z)$ is a cusp form for $\bar{\Gamma}_0(3)$ of weight 6. Consider the $\mathscr{E}$-lattice Λ_3 (Example 5 of [**24**]) formed from 3 copies of the trivial code $\mathbf{F}_4{}^3$:

$$\Lambda_3 = \Lambda(\mathbf{F}_4{}^3) \cup (u + \Lambda(\mathbf{F}_4{}^3)) \cup (2u + \Lambda(\mathbf{F}_4{}^3)) \text{ where}$$

$$u = \frac{1 - \omega}{3\sqrt{2}}(1, 1, 1).$$

Now set $\alpha = \Theta_{\mathscr{E}}(2z) = \psi_0(z)$ (see (11) and (13)), and set

$$\beta = \Theta_{\Lambda_3}(4z) = \psi_0(z)^3 + \tfrac{1}{4}(\psi_0(z/3) - \psi_0(z))^3.$$

THEOREM 2. $\mathscr{M}^1(\Gamma_0(3)) = \mathbf{C}[\alpha, \beta]$.

Proof. $\alpha = \Theta_{\mathscr{E}}(2z) \in \mathscr{M}_1(\bar{\Gamma}_0(3))$ since $\mathscr{E}$ is a self-dual $\mathscr{E}$-lattice. One may directly verify that the realification of the lattice $2\Lambda_3$ is the lattice associated with the Lie algebra of type E_6 (see [**3**]). The quadratic form of this real lattice is even integral of level 3, so $\Theta_{\Lambda_3}(4z) \in \mathscr{M}_3(\bar{\Gamma}_0(3))$. Now we show that these two functions generate the entire algebra. First, let $\mathscr{N}_k$ be the space of cusp forms of weight k for $\bar{\Gamma}_0(3)$ and set

$$\mathscr{M}_k = \mathscr{M}_k(\bar{\Gamma}_0(3)).$$

Then by standard formulas derived using the Riemann-Roch theorem ([**22**], pp. 46, 47),

$$\dim \mathscr{N}_k = \left[\frac{k}{3}\right] - 1 \quad \text{and} \quad \dim \mathscr{M}_k = \left[\frac{k}{3}\right] + 1,$$

hence

$$\mathscr{N}_k = \Delta_6(2z)\mathscr{M}_{k-6}. \tag{30}$$

Now one verifies that

$$\mathscr{M}_3 = \mathbf{C}\langle\alpha^3, \beta\rangle, \quad \mathscr{M}_6 = \mathbf{C}\langle\alpha^6, \beta^2\rangle \oplus \mathbf{C}\langle\Delta_6(2z)\rangle, \quad \text{and}$$
$$\mathscr{M}_k = \mathbf{C}\langle\alpha^k, \beta^{k/3}\rangle \oplus \mathscr{N}_k \quad \text{for } k \equiv 0 \bmod 3.$$

So by induction and (30) we see that polynomials in α and β generate $\mathscr{M}_k$.

When $k \not\equiv 0 \bmod 3$, the proof follows as above by multiplying each space by α or α^2.

5. Modular forms of half-integral weight. We now turn to the class of self-orthogonal codes which have codimension one in their duals. Examples are the duals of the $\mathbf{F}_p$ spans of the incidence matrices of certain projective designs (see Proposition 1). Here the ambient dimension of a code will be odd, and so the weight of the associated theta function will be half-integral. We shall show that these functions are modular forms of level $2p$. We use Shimura's method of dealing with modular forms of half-integral weight given in [**23**]. Set

$$\Delta = \left\{ (\alpha, \pi(z)) \mid \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}),\ \pi(z) \in \mathrm{Hol}(\mathbf{H}) \right.$$

$$\left. \text{with} \quad \pi(z)^2 = t(cz + d),\ t \in \mathbf{C},\ |t| = 1 \right\}.$$

Let $\Pr : \Delta \to SL_2(\mathbf{Z})$ be the natural projection. Give Δ a group structure with composition law

$$(\alpha, \pi(z))(\beta, \rho(z)) \to (\alpha\beta, \pi(\beta(z)) \cdot \rho(z)).$$

Let Δ act on $\mathbf{H}$ by the action of its first component, and let Δ act "with weight n" on $\mathrm{Hol}(\mathbf{H})$ in the following manner:

$$(31) \quad f|[\alpha, \pi(z)]_n = f(\alpha z)\pi(z)^{-n}.$$

A calculation shows that $f|[(\alpha, \pi) \cdot (\beta, \rho)] = f|[(\alpha, \pi)]|[(\beta, \rho)]$.

Definition. A holomorphic function f on $\mathbf{H}$ is a *modular form of weight* $n/2$ *for a subgroup* Δ' *of finite index in* Δ if

(i) $f|[\zeta]_n = f$ for all $\zeta \in \Delta'$;

(ii) f is holomorphic at each cusp of Δ'.

What (ii) means is that f must have the property that the rational divisor associated with f (as in [**22**] Section 2.4), consistent with the complex Riemann surface $(\Pr \Delta'/\mathbf{H})^*$ (defined in [**22**] Section 1.5), is a positive divisor. This is characterized by a certain expansion of f at the cusp described as follows: For τ a cusp, let $\alpha \in \Delta'$, h a positive integer be such that $\alpha(\infty) = \tau$ and $\alpha\left(\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, t \right)\alpha^{-1}$ generates the free cyclic part of Δ_τ', the stability subgroup of τ. Define a real number r by $t^n = e^{2\pi i r}$, $0 \leqq r \leqq 1$. Then (ii) means that

$$(32) \quad f|[\alpha]_n(z) = \sum_{n=0}^{\infty} a_n \exp(2\pi i(n + r)z/h).$$

The theta function transformation formulas will insure that our theta functions will satisfy (32). A more general theta function will yield cusp forms for subgroups of Δ. So we will define theta functions as in [**23**].

Let A be the matrix for a quadratic form having integral entries. We define the *weak level* of A to be the least integer N such that NA^{-1} has integral entries. A complex valued spherical function P of order ν with respect to A is a polynomial in n variables which is orthogonal to all homogeneous polynomials of degree less than ν under the inner product:

$$(P, Q)_A = \int_{B(A)} P(x)\bar{Q}(x)dx$$

where $B(A) = \{x \in \mathbf{R}^n | xAx^t \leqq 1\}$. Let $h \in \mathbf{Z}^n$ be such that $Ah \in N\mathbf{Z}^n$ and let $z \in \mathbf{H}$. Then we define

$$\Theta(z, h, A, N, P) = \sum_{m=h \bmod N} P(m) \exp(2\pi i z m A m^t/N^2).$$

PROPOSITION 13. (Shimura [**23**]) *For* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ *with* $b \equiv 0 \bmod 2$, $c \equiv 0 \bmod 2N$, *we have:*

$$\Theta(\gamma z, h, A, N, P) = \exp(2\pi i a b h A h^t | N^2) \times \left(\frac{\det A}{d}\right)\left(\frac{2c}{d}\right)^n \epsilon_d^{-n}(cz + d)^{k/2}\Theta(z, ah, A, N, P) \tag{33}$$

where $k = n + 2\nu$, $\epsilon_d = 1$ *or* i *according as* $d \equiv 1$ *or* $3 \bmod 4$ *and* $(-)$ *is Shimura's quadratic residue symbol where*

$$\left(\frac{c}{d}\right) = \begin{cases} -\left(\frac{c}{|d|}\right) & \text{if } c < 0, d < 0, \\ \left(\frac{c}{|d|}\right) & \text{otherwise.} \end{cases}$$

Furthermore, if A *is even integral then the restriction* $c \equiv 0 \bmod 2N$ *may be changed to* $c \equiv 0 \bmod N$, *and if both* A *and* NA^{-1} *are even integral (i.e.* A *has level* N*) then* (33) *holds for all* $\gamma \in \Gamma_0(N)$.

For a prime p, recall that $\phi_{p,0}(z)$ is the theta function of the one dimensional lattice $\sqrt{p}\mathbf{Z}$ whose quadratic form matrix is (p). For p odd and $\gamma \in \Gamma_0(2p, 2)$, define

$$g(\gamma, z) = \frac{\phi_{p,0}\gamma(z)}{\phi_{p,0}(z)} \tag{34}$$

and for $p = 2$, $\gamma \in \Gamma_0(4)$, define $g(\gamma, z)$ in the same way.

Using proposition 13 we get that

$$g(\gamma, z) = \left(\frac{m}{d}\right)\epsilon_d^{-1}(cz + d)^{\frac{1}{2}} \tag{35}$$

where $m = c/2p$. So we see that the map $\gamma \to (\gamma, g(\gamma, z))$ defines an injection

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

of $\Gamma_0(2p, 2)$ or $\Gamma_0(4)$ into Δ. Denote the image of this injection by $\Delta_0(2p, 2)$ or $\Delta_0(4)$.

PROPOSITION 14. *If C is a self-orthogonal code in $\mathbf{F}_p^n$ such that its codimension in its orthogonal is 1, then $\Theta_{L(C)}(z)$ is a modular form for $\Delta_0(2p, 2)$. If $p = 2$ and C is also doubly even, then $\Theta_{L(C)}(z)$ is a modular form for $\Delta_0(4)$.*

Remark. A little more generally we could require the codimension of C in $C^\perp$ to be equivalent to n mod 2 as long as the associated quadratic form is of level p. Note that C satisfies the hypothesis of Proposition 14 if it is the $\mathbf{F}_p$ span of the incidence matrix of a design satisfying the hypothesis of Proposition 1.

Proof. If A is a quadratic form matrix for C, it has weak level p and determinant p so

$$\left(\frac{\det A}{d}\right)\left(\frac{c}{d}\right)^n \epsilon_d^{-n} = \left(\left(\frac{m}{d}\right)\epsilon_d^{-1}\right)^n \quad \text{where } m = c/2p.$$

Hence, using (35) and Proposition 13, we see that the proposition follows.

THEOREM 15. *Let $\mathscr{P}_1$ denote the $\mathbf{C}$-algebra generated by the weight polynomials of all doubly even codes of weak level 2, and let $\mathscr{M}(\Delta_0(4))$ denote the algebra of modular forms for $\Delta_0(4)$ graded over integral and half integral weights, then*

$$\mathscr{P}_1 = \mathbf{C}[X, Y^4] \overset{\Phi_2}{\approx} \mathbf{C}[\phi_{2,0}(z), \phi_{2,1}(z)^4] = \mathscr{M}(\Delta_0(4)).$$

The theorem follows from Theorem 3 and Proposition 14 since the trivial code (0) and $C_{2,4}$ have weak level 2 and their polynomials generate $\mathbf{C}[X, Y^4]$.

There is a class $\mathscr{B}$ of self-orthogonal codes whose quadratic forms are even integral and have determinant 2. Their theta functions thus have level 2; however we have found no nice way to define a multiplier system for $\Gamma_0(2)$ similar to the method used for $\Delta_0(2p, 2)$ and $\Delta_0(4)$. But if we define

$$\Delta_0(2) = \left\{(\gamma, g(\gamma, z)) | \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(2) \quad \text{and} \quad g(\gamma, z) = \left(\frac{c}{d}\right)\epsilon_d^{-1}(cz + d)^{\frac{1}{2}}\right\},$$

and we let $\mathscr{M}_n$ be the linear space generated by the weight polynomials of self-orthogonal doubly even binary $(n, (n-1)/2)$ codes, then

$$\Phi_2(\mathscr{B}_n) \subseteq \mathscr{M}_{n/2}(\Delta_0(2)).$$

We can see that the forms of half-integral weight we have constructed for $\Delta_0(2p, 2)$, $\Delta_0(4)$ and $\Delta_0(2)$ are associated with forms of integral weight for Γ_θ or Γ by virtue of the fact that the combinatorial structures underlying the associated lattices may be simply extended to yield lattices for forms for $\bar{\Gamma}_\theta$

or $\bar{\Gamma}$. This is true for forms associated with codes derived from designs satisfying the hypothesis of Proposition 1. This association between the forms may be reflected algebraically via the polynomial representation. For example, if $\Theta \in \Phi_2(\mathscr{B})_n$ then

$$\Theta = P(\phi_{2,0}(z), \phi_{2,1}(z))$$

for some polynomial P, and

$$\phi_{2,0}P(\phi_{2,0}, \phi_{2,1}) + \phi_{2,1}P(\phi_{2,1}, \phi_{2,0}) \in \mathscr{M}_{(n+1)/2}(\bar{\Gamma}).$$

6. Remarks. 1) Viewed from the perspective of [**12**], Theorem 3 produces mappings from algebras of invariants for certain finite matrix groups to algebras of modular forms. Polynomials of self-dual codes turn out to be invariants for matrix groups by virtue of the MacWilliams equations (17), and various types of regularity in the shapes represented by the vectors in such codes. These mappings are discussed in [**17**]. Relationships involving the modular group and invariance groups for polynomials of self-dual binary and ternary codes may be found in [**6**].

2) The methods given in this paper may be used to produce theta function identities in two ways:

i) By equating different polynomial representations of the same function: One example: For $p = 2$ or $p \equiv 1 \bmod 4$, let $B_{p,2}$ be the $(2, 1)$ linear code over $\mathbf{F}_p$ generated by $(1, \sqrt{-1})$. Then

$$P_{B_{2,2}} = X^2 + Y^2, P_{B_{2,5}} = X^2 + 4YZ, \text{ etc.}$$

Now

$$\Phi_p(P_{B_{p,2}}) = \Theta_{\mathbf{Z}^2}$$

and so

$$1 + 4q + 4q^4 + 8q^5 + \ldots = \phi_{2,0}(z)^2 + \phi_{2,1}{}^2(z)$$
$$= \phi_{5,0}(z)^2 + 4\phi_{5,1}(z)\phi_{5,2}(z) = \ldots$$

Other examples may be found in [**6**] and [**24**]. The technique is useful in finding product expansions for some functions.

ii) The Φ_p images of shape relations give theta function identities. So these relations can be found by calculating the kernels of the Φ_p's. For example, it was shown in [**17**] that the kernel of Φ_5 restricted to $\mathscr{P}(\mathscr{A}_5)$ is a principal ideal generated by $X^4YZ - X^2Y^2Z^2 + 2Y^3Z^3 - XZ^5 - XY^5$.

References

1. E. F. Assmus, Jr. and D. P. Maher, *Nonexistence proofs for projective designs*, to appear, American Mathematical Monthly.
2. E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, *Gleason's theorem on self-dual codes*, IEEE Trans. Info. Theory *18* (1972), 409–414.

https://doi.org/10.4153/CJM-1980-005-6 Published online by Cambridge University Press

3. N. Bourbaki, *Groups et algebres de Lie*, Ch. 4, 5, and 6 (Hermann, Paris, 1968).
4. ——— *Theories spectrales* (Hermann, Paris, 1967).
5. M. Broué, *Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux elements et formes quadratiques entières définies positives à discriminant* +1, pp. 71–108 of Comptes Rendus des Journées Mathématiques de la Société Math. de France, Univ. Sci. Tech. Languedoc, Montpellier 1974. Reprinted in Discrete Math. *17* (1977), 247–269.
6. M. Broué and M. Enguehard, *Polynômes des poids de certains codes et functions thêta de certains réseaux*, Ann. Scient. Ec. Norm. Sup. *5* (1972), 157–181.
7. P. J. Cameron and J. H. van Lint, *Graph theory, coding theory, and block designs*, London Math. Soc. Lecture Note Series *19* (Cambridge Univ. Press, 1975).
8. J. H. Conway, *A group of order* 8,315,553,613,086,720,000, Bull. London Math. Soc. *1* (1969), 79–88.
9. M. Eichler, *Introduction to the theory of algebraic numbers and functions* (Academic Press, N.Y., 1966).
10. A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities* in: Actes Congrés Internl. de Mathematique *3*, 1970 (Gauthier-Villars, Paris, 1971), 211–215.
11. J. Leech. *Notes on sphere packings*, Can. J. Math. *19* (1967), 251–267.
12. 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.
13. F. J. MacWilliams, N. J. A. Sloane and J. M. Goethals, *The MacWilliams identities for nonlinear codes*, Bell Syst. Tech. J. *51* (1972), 803–819.
14. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *On the existence of a projective plane of Order* 10, J. Combinatorial Theory *14A* (1973), 66–78.
15. F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes* (North-Holland, Amsterdam, 1977).
16. D. P. Maher, *Self-orthogonal codes and modular-forms*, Ph.D. Thesis, Lehigh University, 1976.
17. ——— *Lee polynomials of codes and theta functions of lattices*, Can. J. Math. *30* (1978), 738–747.
18. H. V. Niemeier, *Definite Quadratische Formen der Dimension* 24 *und Diskcriminante* 1, J. Number Theory *5* (1973), 1942–178.
19. A. Ogg, *Modular forms and Dirichlet series* (W. A. Benjamin, Inc., N. Y., 1969).
20. H. Sachar, *Error-correcting codes associated with finite projective planes*, Ph.D. dissertation, Lehigh University, 1973.
21. J. P. Serre, *Cours d'arithmétique* (Presses Univ. de France, 1970). English translation published by Springer Verlag, 1973.
22. G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Princeton University Press, Princeton, N.J., 1971).
23. ——— *On modular forms of half-integral weight*, Annals of Mathematics, 2nd Ser. *97* No. 3 (1973).
24. N. J. A. Sloane, *Codes over GF*(4) *and complex lattices*, J. Algebra *52* (1978), 168–181.
25. J. Tannery and J. Molk, *Eléments de la théorie des fonctions elliptiques*, 4 vols., 2nd edition, reprinted Chelsea, N.Y. (1972).

Worcester Polytechnic Institute,
Worcester, Massachusetts