International Mathematics Research Notices 1933, No. 5

ON CODES AND SIEGEL MODULAR FORMS

W. DUKE

1. Introduction. In this paper I will connect the theory of Siegel modular forms to the study of multiple weight enumerators of certain binary linear codes. As an application, it will be shown that the algebras spanned by the biweight enumerators of doubly-even codes containing the all-ones vector and of doubly-even self-dual codes are finitely generated over $\mathbf{C}$, and explicit generators for them will be given. This will be based on results of Igusa and Ozeki on the structure of algebras of Siegel modular forms of degree two.

Let $\mathscr{C}_2$ be the set of all doubly-even codes containing the all-ones vector and $\mathscr{C}_1$ the set of all doubly-even self-dual codes, so that $\mathscr{C}_1 \subset \mathscr{C}_2$ (see §2 for definitions). Codes in $\mathscr{C}_1$ are of special interest, and those of length $\leqslant 32$ have been classified (see [4]). On the other hand, the number of equivalence classes $H_1(n)$ of such codes of length n satisfies $\log H_1(n) \gg n^2$ as $n \to \infty$ with $8|n$ (see [19, Chapter 19]). This fact makes it desirable to have class invariants which can distinguish between different classes of a given length but which span a finitely generated algebra.

Natural candidates for such invariants are the following multiple weight enumerators. For any binary linear code C of length n and $r \in \mathbf{Z}^+$, we define the r-fold weight enumerator of C to be

$$W_r(x; C) = \sum_{(c_1,\ldots,c_r)\in C^r} \prod_{\alpha \in \mathbf{F}_2^r} x_\alpha^{\omega_\alpha(c_1,\ldots,c_r)}, \tag{1.1}$$

where $x = (x_\alpha)$ is a 2^r-tuple of variables with $\alpha \in \mathbf{F}_2^r$ and $\omega_\alpha(c_1, \ldots, c_r)$ is the number of occurrences of α as a row in the matrix of column vectors $(c_1, \ldots, c_r)$. The polynomial $W_r \in \mathbf{Z}[x]$ is homogeneous of degree n and can be written using multi-indices $m = (m_\alpha)$ as

$$W_r(x; C) = \sum_m A_m x^m,$$

where $\sum_\alpha m_\alpha = n$ and A_m is the number of r-tuples $(c_1, \ldots, c_r)$ from C which have m_α occurrences of α in their rows for each α. Thus $W_1(x; C) = W_1(x_0, x_1; C)$ is the ordinary weight enumerator of C, while $W_2(x; C) = W_2(x_{00}, x_{01}, x_{10}, x_{11}; C)$ is the biweight enumerator of C introduced in [18] (see also [19]). The variables $x_{00}, x_{01}, x_{10}, x_{11}$, will also be denoted by x_0, x_1, x_2, x_3, corresponding to the binary expansion of their subscripts.

Received 1 March 1993.
Communicated by Peter Sarnak.
Author's research supported by NSF Grant DMS-9202022.

Now $W_r(x; C)$ is a class invariant, and it holds that

$$W_r(x; C_1 \oplus C_2) = W_r(x; C_1)W_r(x; C_2).$$

As $\mathscr{C}_N$ is closed under $\oplus$ for $N = 1$ or 2, the set $\mathscr{W}_r(N)$ of all finite $\mathbf{C}$-linear combinations of 1 and $W_r(x; C)$ for $C \in \mathscr{C}_N$ forms a (graded) subalgebra of $\mathbf{C}[x]$. In fact,

$$\mathscr{W}_r(N) = \bigoplus_{d \equiv 0 \pmod{8/N}} \mathscr{W}_r^d(N),$$

where $\mathscr{W}_r^d(N)$ is the vector space of polynomials in $\mathscr{W}_r(N)$ which are homogeneous of degree d. Let

$$P(t) = P_{r,N}(t) = \sum_{d \equiv 0 \pmod{8/N}} \dim \mathscr{W}_r^d(N)t^d$$

be the associated "Poincaré series". Two basic problems are (i) to show that $\mathscr{W}_r(N)$ is finitely generated and (ii) to compute $P(t)$.

When $r = N = 1$, these problems were solved by Gleason in 1970 [9], from which it follows that $W_1(1)$ is actually freely generated by

$$x_0^8 + 14x_0^4x_1^4 + x_1^8 \quad \text{and} \quad x_0^{24} + 759x_0^{16}x_1^8 + 2576x_0^{12}x_1^{12} + 759x_0^8x_1^{16} + x_1^{24}.$$

These polynomials are the weight enumerators of the [8, 4] Hamming code and the [24, 12] Golay code, both of which are in $\mathscr{C}_1$. Thus, one also has

$$P_{1,1}(t) = \frac{1}{(1 - t^8)(1 - t^{24})}.$$

Gleason obtained this result by identifying $\mathscr{W}_1(1)$ with the algebra of invariant polynomials for a finite unitary reflection group of order 192. Later proofs were given based on a connection with classical modular forms (see [2], [3], and [5]). This approach also leads to a solution of these problems for $r = 1$ and $N = 2$. It follows from [20, Theorem 9] that $W_1(2)$ is freely generated by

$$x_0^4 + x_1^4 \quad \text{and} \quad x_0^8 + x_1^8,$$

which are the weight enumerators of the [4, 1] and [8, 1] repetition codes and are in $\mathscr{C}_2$, and so

$$P_{1,2}(t) = \frac{1}{(1 - t^4)(1 - t^8)}.$$

It is apparently not known whether $\mathscr{W}_r(N)$ is in general finitely generated for $r > 1$. This result will be proved here for $r = 2$ by developing a connection with Siegel

modular forms. Associated to a doubly-even code C of length n is an even integral lattice $L(C)$ of rank n defined by

$$L(C) = \{\ell \in \mathbf{R}^n : \sqrt{2}\ell \in \mathbf{Z}^n \text{ and } \sqrt{2}\ell \equiv c \pmod 2, \text{ for some } c \in C\}. \tag{1.2}$$

If $C \in \mathscr{C}_2$, then $L = L(C)$ has level 1 or 2 according as $C \in \mathscr{C}_1$ or not. The associated Siegel analytic class invariant of degree r is given by

$$\vartheta_r(\tau; L) = \sum_{\ell_1, \ldots, \ell_r \in L} e\left(\frac{1}{2}\operatorname{tr} \tau w(\ell_1, \ldots, \ell_r)\right), \tag{1.3}$$

where $w(\ell_1, \ldots, \ell_r)$ is the nonnegative $r \times r$ matrix with entries $\langle \ell_i, \ell_j \rangle$ and $\tau \in \mathbf{H}^r$, the Siegel upper half-space of degree r. Let $\mathscr{M}_r(N)^{(d)}$ be the graded algebra generated by all Siegel modular forms of degree r for $\Gamma_0^r(N)$ with weights divisible by d:

$$\mathscr{M}_r(N)^{(d)} = \bigoplus_{d|k} \mathscr{M}_r^k(N),$$

where $\mathscr{M}_r^k(N)$ is the vector space of degree r Siegel modular forms of weight k for $\Gamma_0^r(N)$. Finally, let $\theta(\tau) = \left(\theta\begin{bmatrix}\alpha\\0\end{bmatrix}(2\tau|0)\right)_{\alpha \in \mathbf{F}_2^r}$ be the 2^r-vector of second-order theta constants, where, for $\alpha, \beta \in \mathbf{F}_2^r$, $\tau \in \mathbf{H}^r$, and $z \in \mathbf{C}^r$,

$$\theta\begin{bmatrix}\alpha\\\beta\end{bmatrix}(\tau|z) = \sum_{b \in \mathbf{Z}^r} e\left(\frac{1}{2}(b + \alpha/2)\tau^t(b + \alpha/2) + (b + \alpha/2)^t(z + \beta/2)\right) \tag{1.4}$$

defines the theta function with characteristic $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$.

Our main result is the following.

THEOREM 1. *For $r \geqslant 1$ and $N = 1$ or 2, the map $W \mapsto W(\theta(\tau))$ defines an algebra homomorphism from $\mathscr{W}_r(N)$ to $\mathscr{M}_r(N)^{(4/N)}$ with $W_r(\theta(\tau); C) = \vartheta_r(\tau; L(C))$ for $C \in \mathscr{C}_N$. If $r \leqslant 2$, this map is an isomorphism.*

This was shown in [3] when $r = 1$, $N = 1$, and in [20] when $r = 1$, $N = 2$. Since it is known that $\mathscr{M}_r(N)$ is finitely generated (see [7]), it follows that $\mathscr{W}_2(N)$ is as well. In fact, more precise information is available in this case. Let r_n, d_n, d_n^+, g_{24} be the codes of length n defined in (2.2)–(2.5) of §2, with r_n, $d_n \in \mathscr{C}_2$ for $n \equiv 0 \pmod 4$ and d_n^+, $g_{24} \in \mathscr{C}_1$ for $n \equiv 0 \pmod 8$.

THEOREM 2. (i) *$\mathscr{W}_2(2)$ is freely generated by the biweight enumerators of r_4, r_8, r_{12}, and d_8 so that*

$$P_{2,2}(t) = \frac{1}{(1 - t^4)(1 - t^8)^2(1 - t^{12})}.$$

(ii) $\mathcal{W}_2(1) = \mathcal{W} \oplus W_2(x; d_{32}^+)\mathcal{W}$, *where* $\mathcal{W}$ *is freely generated by the biweight enumerators of* d_8^+, d_{24}^+, d_{40}^+, *and* g_{24}, *so that*

$$P_{2,1}(t) = \frac{1 + t^{32}}{(1 - t^8)(1 - t^{24})^2(1 - t^{40})}.$$

In order to express symmetric weight enumerators succinctly, it is convenient to introduce a symmetrizing operator on polynomials. This is defined on monomials x^m by

$$\text{Sym } x^m = \frac{1}{|\{\pi \in S_k : \pi m = m\}|} \sum_{\pi \in S_k} x^{\pi m},$$

where $\pi m = (m_{\pi(0)}, \ldots, m_{\pi(k-1)})$, and is extended linearly.

It is readily verified that

$$W_2(x; r_n) = \text{Sym } x^{(0,0,0,n)}$$

and

$$W_2(x; d_8) = \text{Sym}(x^{(0,0,0,8)} + 6x^{(0,0,4,4)} + 24x^{(2,2,2,2)}).$$

It follows that $\mathcal{W}_2(2)$ (hence also $\mathcal{W}_2(1)$) consists of polynomials which are symmetric in x_0, x_1, x_2, and x_3. A calculation [6] gives

$$\begin{aligned} W_2(x; g_{24}) = \text{Sym}(&x^{(0,0,0,24)} + 759x^{(0,0,8,16)} + 2576x^{(0,0,12,12)} + 22770x^{(0,8,8,8)} \\ &+ 340032x^{(2,6,6,10)} + 212520x^{(4,4,4,12)} + 1275120x^{(4,4,8,8)} \\ &+ 4080384x^{(6,6,6,6)}), \end{aligned}$$

while for general d_n, d_n^+, we have the identities

$$W_2(x; d_n) = \frac{1}{4} \sum_{\beta \in \mathbb{F}_2^2} \left(\sum_{\alpha \in \mathbb{F}_2^2} (-1)^{\langle \alpha, \beta \rangle} x_\alpha^2 \right)^{n/2}, \qquad \text{for } n \equiv 0 \pmod 4$$

and

$$W_2(x; d_n^+) = \frac{1}{4} \sum_{\beta, \gamma \in \mathbb{F}_2^2} \left(\sum_{\alpha \in \mathbb{F}_2^2} (-1)^{\langle \alpha, \beta \rangle} x_{\alpha+\gamma} x_\alpha \right)^{n/2}, \qquad \text{for } n \equiv 0 \pmod 8.$$

One can use these explicit generators to compute the biweight enumerator of an extremal code in $\mathcal{C}_1$ of length 48, as well as the biweight enumerator that extremal

codes of length 72 and 96, if they exist, would have; see [6]. The computation shows that these enumerators are in fact unique. For example, if e_{48} is an extremal code of length 48 (one is known to exist; see [19]), then

$$\begin{aligned} W_2(x; e_{48}) = \operatorname{Sym}(&x^{(0,0,0,48)} + 17296x^{(0,0,12,36)} + 535095x^{(0,0,16,32)} \\ &+ 3995376x^{(0,0,20,28)} + 7681680x^{(0,0,24,24)} + 10896480x^{(0,12,12,24)} \\ &+ 59930640x^{(0,12,16,20)} + 153037170x^{(0,16,16,16)} \\ &+ 143833536x^{(2,10,10,26)} + 2054764800x^{(2,10,14,22)} \\ &+ 4954266240x^{(2,10,18,18)} + 14383353600x^{(2,14,14,18)} \\ &+ 128422800x^{(4,8,8,28)} + 5094104400x^{(4,8,12,24)} \\ &+ 29845458720x^{(4,8,16,20)} + 104279313600x^{(4,12,12,20)} \\ &+ 279876088800x^{(4,12,16,16)} + 15981504x^{(6,6,6,30)} \\ &+ 1917780480x^{(6,6,10,26)} + 29006429760x^{(6,6,14,22)} \\ &+ 69040097280x^{(6,6,18,18)} + 131367962880x^{(6,10,10,22)} \\ &+ 963684691200x^{(6,10,14,18)} + 2970162518400x^{(6,14,14,14)} \\ &+ 34224676200x^{(8,8,8,24)} + 743439589200x^{(8,8,12,20)} \\ &+ 1970391020400x^{(8,8,16,16)} + 7304226541920x^{(8,12,12,16)} \\ &+ 4631359951680x^{(10,10,10,18)} + 14095686528000x^{(10,10,14,14)} \\ &+ 26737956967680x^{(12,12,12,12)}). \end{aligned}$$

The direct computation of this biweight enumerator from the code is thereby avoided.

It is also possible to use invariant theory to study biweight enumerators, as was done for certain classes of codes in [18]. It was shown in [10] that $\mathscr{W}_2(1) \subset \mathscr{A}^{(8)}$, where $\mathscr{A}$ is the algebra of polynomial invariants for a finite unitary reflection group of order 46080 (group number 31 in [25]). The invariant theory of this group was studied as early as 1887 by Maschke [21]. It follows from Theorem 2 that actually $\mathscr{W}_2(1) = \mathscr{A}^{(8)}$ since the generators of $\mathscr{A}$ have degrees 8, 12, 24, 20. It is actually possible to express the generators of $\mathscr{A}^{(8)}$ in terms of $W_2(x; C)$, for $C = d_8^+, d_{24}^+, d_{32}^+, d_{40}^+, g_{24}$ and thus give another proof of Theorem 2(ii).

Nothing seems to be known about our basic problems when $r \geqslant 3$. The homomorphism $W \mapsto W(\theta)$ of Theorem 1 is certainly not injective when $r = 3$. In fact, a computation [6] shows that

$$W(x) \stackrel{\text{def}}{=} W_3(x; d_8^+ \oplus d_8^+) - W_3(x; d_{16}^+) \neq 0$$

while a result of Igusa [15] on the genus 4 Schottky relation together with Lemma 5 shows that $W(\theta) = 0$.

Acknowledgements. I would like to thank H. Bass, Z. Rudnick, and N. J. A. Sloane for their comments, and I. Vardi for several contributions.

2. Codes and associated lattices. By a code of length n, we mean a binary linear code of length n, which is a subspace of $\mathbf{F}_2^n$, where $\mathbf{F}_2$ is the field with two elements. We can identify $\mathbf{F}_2^n$ with $\{0, 1\}^n \subset \mathbf{R}^n$ and, letting $\langle \cdot, \cdot \rangle$ denote the usual inner product in $\mathbf{R}^n$, define the weight of a codeword $c \in C$ to be $\omega_1(c) = \langle c, c \rangle$. An $[n, k]$ code is a code of length n with dimension k. Two codes are equivalent if there is a permutation of coordinates taking one to the other. The dual code is

$$C^\perp = \{c \in \mathbf{F}_2^n : \langle c, b \rangle \equiv 0 \pmod 2 \text{ for all } b \in C\}$$

and is a code with $C^{\perp\perp} = C$. If $C = C^\perp$, then C is called self-dual. If $\langle c, c \rangle \equiv 0 \pmod 4$ for all $c \in C$, then C is called doubly-even.

LEMMA 1. *A code C is doubly-even if and only if $C \subset C^\perp$ and C has a basis $(c_1, \ldots, c_k)$ with $\langle c_i, c_i \rangle \equiv 0 \pmod 4$ for $i = 1, \ldots, k$.*

Proof. This follows from the identity (in $\mathbf{R}^n$)

$$\langle a + b, a + b \rangle = \langle a, a \rangle + 2\langle a, b \rangle + \langle b, b \rangle, \tag{2.1}$$

together with the observation that $\langle a + b, a + b \rangle$ is the same mod 4 if $a + b$ is computed mod 2 or mod 4. □

Define the level N of a doubly-even code C to be the smallest $N \in \mathbf{Z}^+$ such that $N\langle c, c \rangle \equiv 0 \pmod 4$ for all $c \in C^\perp$. Clearly $N = 1, 2$, or 4.

LEMMA 2. *Let C be a doubly-even code.*
(i) *C has level 1 or 2 if and only if $\mathbf{1} = (1, \ldots, 1) \in C$.*
(ii) *C has level 1 if and only if C is self-dual.*

Proof. (i) C has level 1 or 2 if and only if, for all $c \in C^\perp$,

$$\langle c, \mathbf{1} \rangle = \langle c, c \rangle \equiv 0 \pmod 2,$$

which happens if and only if $\mathbf{1} \in C^{\perp\perp} = C$.

(ii) If C has level 1, then $C^\perp$ is doubly-even, and so by Lemma 1, $C^\perp \subset C^{\perp\perp} = C$ and $C \subset C^\perp$; so $C = C^\perp$. Conversely, if $C = C^\perp$, then $\langle c, c\rangle \equiv 0 \pmod 4$ for all $c \in C^\perp$, and so C has level 1. □

Let $\mathscr{C}_2$ be the set of all doubly-even codes containing $\mathbf{1}$ and $\mathscr{C}_1$ the set of all doubly-even self-dual codes. By Lemma 2 we have that $\mathscr{C}_1 \subset \mathscr{C}_2$ and by [9] that the length n of any $C \in \mathscr{C}_N$ satisfies $n \equiv 0 \pmod{8/N}$ for $N = 1$ or 2.

Important examples of codes for us are denoted by r_n, d_n, d_n^+, g_{24}, and are defined as follows:

(2.2) The code r_n is the $[n, 1]$ repetition code spanned by $\mathbf{1}$ with $r_n \in \mathscr{C}_2 - \mathscr{C}_1$ if $n \equiv 0 \pmod 4$.

(2.3) The code d_n is the $[n, n/2 - 1]$ code for $n \equiv 0 \pmod 4$ with generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & & & \cdots & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \cdots & 0 \\ & & & & & & & \ddots & & \\ 0 & \cdots & & & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

meaning that its rows form a basis for d_n. Now $d_n \in \mathscr{C}_2 - \mathscr{C}_1$ by Lemma 1 and 2.

(2.4) The code $d_n^+ = d_n \cup (a + d_n)$, where $a = (1, 0, 1, 0, \ldots, 1, 0)$, and $n \equiv 0 \pmod 8$. This is denoted by E_n in [23, p. 320], and $d_n^+ \in \mathscr{C}_1$.

(2.5) The code g_{24} is the [24, 12] Golay code defined, for example, in [19], with $g_{24} \in \mathscr{C}_1$.

Recall that a full lattice $L \subset \mathbf{R}^n$ is a discrete subgroup with $\det(L) = \mathrm{vol}^2(\mathbf{R}^n/L)$ finite. Two lattices are equivalent if there is an orthogonal transformation taking one to the other. The dual lattice is

$$L^\perp = \{\ell \in \mathbf{R}^n : \langle \ell, m\rangle \in \mathbf{Z} \text{ for all } m \in L\},$$

and is a full lattice with $L^{\perp\perp} = L$. If $L = L^\perp$, L is called self-dual. If $\langle \ell, \ell\rangle \equiv 0 \pmod 2$ for all $\ell \in L$, then L is called even. By (2.1) a lattice L is even if and only if $L \subset L^\perp$ and L has a $\mathbf{Z}$-basis $\ell_1, \ldots, \ell_n$ with $\langle \ell_i, \ell_i\rangle \equiv 0 \pmod 2$ for $i = 1, \ldots, n$. The level of an even lattice L is the smallest $N \in \mathbf{Z}^+$ such that $N\langle \ell, \ell\rangle \equiv 0 \pmod 2$ for all $\ell \in L^\perp$. An even lattice is self-dual if and only if it has level 1.

Associated to any $[n, k]$ code C is the full lattice $L(C) \subset \mathbf{R}^n$ defined in (1.2) and called construction A in [5, p. 182], which is a basic reference for this section. From [5], if (I_k, B) is a generator matrix for C, where $B \in \mathrm{Mat}_{k,n-k}(\mathbf{F}_2)$, and I_k is the $k \times k$

identity matrix, then $L(C)$ has a $\mathbf{Z}$-basis given by the rows of

$$\frac{1}{\sqrt{2}}\begin{pmatrix} I_k & B \\ 0 & 2I_{n-k} \end{pmatrix}. \tag{2.6}$$

Using this and the above lemmas, it is straightforward to establish the following result.

LEMMA 3. *For any codes* C, C_1, C_2,
(i) $L(C^{\perp}) = L(C)^{\perp}$,
(ii) $L(C_1 \oplus C_2) = L(C_1) \oplus L(C_2)$,
(iii) $C_1 \subset C_2$ *if and only if* $L(C_1) \subset L(C_2)$, *in which case* $|C_2/C_1| = |L(C_2)/L(C_1)|$,
(iv) $L(C)$ *is even if and only if* C *is doubly-even, in which case their levels coincide.*

In particular, Lemma 2, (2.6), and Lemma 3(iv) lead to the following result.

LEMMA 4. *If* $C \in \mathscr{C}_2$, *then* $L(C)$ *is an even lattice of level 1 or 2 depending on whether* $C \in \mathscr{C}_1$ *or not. Furthermore,* $\det(L(C))$ *is a square integer.*

Although we do not need this fact here, it can be shown that for $N = 1$ or 2 an even lattice of level N can be expressed as $L(C)$ for some $C \in \mathscr{C}_N$ of length n exactly when $\sqrt{2}\mathbf{Z}^n \subset L$, and two such lattices are equivalent if and only if the associated codes are equivalent (see [17, Theorem 2]).

3. Weight enumerators and analytic class invariants. In this section the first statement in Theorem 1 will be proved. Recall definitions (1.1)–(1.4).

LEMMA 5. *For any code* C *and* $r \geqslant 1$, *one has*

$$W_r(\theta(\tau); C) = \vartheta_r(\tau; L(C)),$$

for any $\tau \in \mathbf{H}^r$.

Proof. From (1.3)

$$\vartheta_r(\tau; L(C)) = \sum_{\ell_1, \ldots, \ell_r \in L(C)} e\left(\frac{1}{2}\operatorname{tr}(\ell_1, \ldots, \ell_r)\tau^t(\ell_1, \ldots, \ell_r)\right),$$

where each ℓ_i is written as a column vector in $\mathbf{R}^n$ and this is

$$= \sum_{c \in C^r} \prod_{\alpha \in \mathbf{F}_2^r} \left(\sum_{b \in \mathbf{Z}^r} e((b + \alpha/2)\tau^t(b + \alpha/2)) \right)^{\omega_\alpha(c)}$$

upon using the definition of $L(C)$ in (1.2) and collecting together those columns of ${}^t(\ell_1, \ldots, \ell_r)$ which receive the same contribution α from $c = (c_1, \ldots, c_r) \in C^r$. Thus $\vartheta_r(\tau; L(C)) = W_r(\theta(\tau); C)$. □

Recall that $\mathcal{M}_r^k(N)$ is the **C**-vector space of all Siegel modular forms of weight k and degree r for $\Gamma_0^r(N)$ (see [1] for definitions). The following standard result can be found in [1, p. 64].

LEMMA 6. *If $L \subset \mathbf{R}^n$ for $4|n$ is an even lattice of level N with* $\det(L)$ *a square, then for each $r \geqslant 1$*

$$\vartheta_r(\tau; L) \in \mathcal{M}_r^{n/2}(N).$$

Recall that $\mathcal{W}_r(N)$ for $N = 1$ or 2 is the **C**-algebra of finite **C**-linear combinations of 1 and $W_r(x; C)$ for $C \in \mathcal{C}_N$. For $W \in \mathcal{W}_r(N)$, we have to consider the map

$$W \mapsto W(\theta(\tau)).$$

In view of Lemmas 4, 5, and 6, this gives a map from $\mathcal{W}_r(N)$ to $\mathcal{M}_r(N)^{(4/N)}$ since $4/N$ divides $n/2$ for codes of length n in $\mathcal{C}_N$ (recall below Lemma 2). It is clearly an algebra homomorphism. This proves the first statement in Theorem 1.

4. Algebraic independence of theta constants. Turning to the proof of the second statement in Theorem 1, we may assume that $r = 2$ since the case $r = 1$ is known from [3] and [20]. To show that our homomorphism is injective, consider the theta constants from (1.4) when $r = 2$:

$$\theta(\tau) = (\theta_0(\tau), \theta_1(\tau), \theta_2(\tau), \theta_3(\tau))$$

$$= \left(\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}(2\tau|0), \theta\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}(2\tau|0), \theta\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}(2\tau|0), \theta\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}(2\tau|0)\right).$$

Injectivity follows immediately from the next lemma.

LEMMA 7. *The functions $\theta_0(\tau)$, $\theta_1(\tau)$, $\theta_2(\tau)$, and $\theta_3(\tau)$ on $\mathbf{H}^2$ are algebraically independent over* **C**.

Proof. Consider the determinant

$$D(\tau) = \begin{vmatrix} \theta_0(\tau) & \theta_1(\tau) & \theta_2(\tau) & \theta_3(\tau) \\ \partial_1\theta_0(\tau) & \partial_1\theta_1(\tau) & \partial_1\theta_2(\tau) & \partial_1\theta_3(\tau) \\ \partial_2\theta_0(\tau) & \partial_2\theta_1(\tau) & \partial_2\theta_2(\tau) & \partial_2\theta_3(\tau) \\ \partial_3\theta_0(\tau) & \partial_3\theta_1(\tau) & \partial_3\theta_2(\tau) & \partial_3\theta_3(\tau) \end{vmatrix},$$

where $\partial_i = \partial/\partial\tau_i$ with $\tau = \begin{pmatrix}\tau_1 & \tau_2\\ \tau_2 & \tau_3\end{pmatrix}$. A sufficient condition for algebraic independence is the nonvanishing of $D(\tau)$ at a point and hence in a nonempty open set

$\mathscr{U} \subset \mathbf{H}^2$. This follows in a standard way by differentiating a purported homogeneous algebraic relation together with Euler's relation and using the chain rule to derive a nonzero homogeneous linear solution, hence a contradiction.

Recall that τ is reducible if it is equivalent under $Sp(4, \mathbf{Z})$ to a matrix of the form $\begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}$.

LEMMA 8.

$$D(\tau) = \pm 4\pi^3 i \prod_{\langle \alpha, \beta \rangle \equiv 0 \pmod 2} \theta \begin{bmatrix} \alpha \\ \beta \end{bmatrix} (\tau|0)$$

and $D(\tau)$ vanishes exactly when τ is reducible.

Proof. Using the heat equation, see [14, p. 187], it follows that

$$D(\tau) = \frac{i}{2\pi^3} \begin{vmatrix} \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (2\tau|0) & \cdots & \theta \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} (2\tau|0) \\ \frac{\partial^2}{\partial z_1 \partial z_1} \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (2\tau|0) & \cdots & \frac{\partial^2}{\partial z_1 \partial z_1} \theta \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} (2\tau|0) \\ \vdots & & \vdots \\ \frac{\partial^2}{\partial z_2 \partial z_2} \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (2\tau|0) & \cdots & \frac{\partial^2}{\partial z_2 \partial z_2} \theta \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} (2\tau|0) \end{vmatrix}.$$

In [24, p. 119] this determinant is evaluated using Rosenhain's derivative formula from [8, p. 248] to yield the formula of the lemma. The fact that $D(\tau) = 0$ if and only if τ is reducible follows from [24] or [16, p. 115]. □

Choosing τ irreducible in Lemma 8 now yields the proof of Lemma 7. □

5. The basis problem for degree-two modular forms. Finally, I will apply known results about the structure of algebras of degree-two Siegel modular forms to finish the proof of Theorem 1 and to prove Theorem 2. In the last section the map $W \mapsto W(\theta)$ was shown to be injective, and it will now be shown that this map is also surjective for $N = 1, 2$. This fact is based ultimately on the fundamental results of Igusa (see [12], [13], and [14]).

In case $N = 1$, it follows from [22] that $\mathscr{M}_2(1)^{(4)}$ is generated by $\vartheta_2(\tau; L(d_n^+))$ for $n = 8, 24, 32, 40$, and by $\vartheta_2(\tau; L(g_{24}))$. This proves surjectivity. Part (ii) of Theorem 2 now follows since a computer calculation of their Jacobian determinant shows that the biweight enumerators of $d_8^+, d_{24}^+, d_{40}^+$, and g_{24} are algebraically independent over $\mathbb{C}$ and since $W_2(x, d_{32}^+)^2$ can be expressed as a polynomial in the biweight enumerators of $d_8^+, d_{24}^+, d_{32}^+, d_{40}^+$, and g_{24}, in which only the first power of $W_2(x; d_{32}^+)$ occurs.

In case $N = 2$, it follows from [11, p. 33] that $\mathcal{M}_2(2)^{(2)}$ is freely generated by forms of weights 2, 4, 4, and 6. On the other hand, a computer calculation shows that $W_2(x; r_4)$, $W_2(x; r_8)$, $W_2(x; r_{12})$, and $W_2(x; d_8)$ are algebraically independent. Hence the surjectivity follows, as does Theorem 2(i).

Added in proof: After this paper was written, I learned that some of its results were also obtained by N. Herrmann in his (unpublished) Diplomthesis.

References

[1] A. N. Andrianov, *Quadratic Forms and Hecke Operators*, Grundlehren Math. Wiss. **286**, Springer-Verlag, Berlin, 1987.

[2] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, *Gleason's theorem on self-dual codes*, IEEE Trans. Inform. Theory **18** (1972), 409–414.

[3] M. Broué and M. Enguehard, *Polynômes de poids de certains codes et fonction thêta de certain réseaux*, Ann. Sci. École Norm. Sup. **6** (1973), 17–52.

[4] J. H. Conway, V. Pless, and N. J. A. Sloane, *The binary self-dual codes of length up to 32, a revised enumeration*, J. Combin. Theory Ser. A **60** (1992), 183–195.

[5] J. H. Conway and N. J. Sloane, *Sphere Packings, Lattices, and Groups*, Grundlehren Math. Wiss. **290**, Springer-Verlag, New York, 1988.

[6] W. Duke and I. Vardi, *Multiple weight enumerators of codes*, preprint, 1993.

[7] E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren Math. Wiss. **254**, Springer-Verlag, Berlin, 1983.

[8] F. G. Frobenius, "Über die constanten Factoren der Thetareihen" in *Gesammelte Abhandlungen, Band 2*, Springer-Verlag, Berlin, 1968, 241–260.

[9] A. M. Gleason, "Weight polynomials of self-dual codes and the MacWilliams identities" in *Actes Congrès International des Mathématiciens, Nice, 1970, Tôme 3*, Gauthier-Villars, Paris, 1971, 211–215.

[10] W. C. Huffman, *The biweight enumerator of self-dual orthogonal binary codes*, Discrete Math. **26** (1979), 129–143.

[11] T. Ibukiyama, *On Siegel modular varieties of level 3*, Internat. J. Math. **2** (1991), 17–35.

[12] J. Igusa, *On Siegel modular forms of genus two, I*, American J. Math. **84** (1962), 175–200; *II*, **86** (1964), 392–412.

[13] ———, *On the graded ring of theta-constants*, American J. Math. **86** (1964), 219–246.

[14] ———, *Theta Functions*, Grundlehren Math. Wiss. **194**, Springer-Verlag, Berlin, 1972.

[15] ———, "Schottky's invariant and quadratic forms" in *E. B. Christoffel, Aachen/Monschau, 1979*, Birkäuser, Basel, 1981, 352–362.

[16] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge Stud. Adv. Math. **20**, Cambridge Univ. Press, Cambridge, 1990.

[17] H. V. Koch, "Unimodular lattices and self-dual codes" in *Proceedings of the International Congress of Mathematicians, Berkeley, 1986*, Amer. Math. Soc., Providence, 1987, 457–465.

[18] 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. Inform. Theory **18** (1972), 794–805.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Math. Library **16**, North-Holland, Amsterdam, 1978.

[20] D. P. Maher, *Modular forms from codes*, Canad. J. Math. **32** (1980), 40–58.

[21] H. Maschke, *Ueber die quaternäre, endliche, lineare Substitutionsgruppe der Borchardt'schen Moduln*, Math. Ann. **80** (1887), 496–515.

[22] M. Ozeki, *On basis problem for Siegel modular forms of degree 2*, Acta Arith. **31** (1976), 17–30.

[23] V. PLESS AND N. J. A. SLOANE, *On the classification and enumeration of self-dual codes*, J. Combin. Theory Ser. **A18** (1975), 313–335.

[24] R. SASAKI, *Modular forms vanishing at the reducible points of the Siegel upper-half space*, J. Reine Angew. Math. **345** (1983), 111–121.

[25] G. C. SHEPARD AND J. A. TODD, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903, USA