JOURNAL OF COMBINATORIAL THEORY, Series A 57, 163–186 (1991)

Hecke Operators and the Weight Distributions of Certain Codes

RENÉ SCHOOF*

Mathematisch Instituut, Rijksuniversiteit Utrecht, Budapestlaan 6, 3508 TA Utrecht, The Netherlands

AND

MARCEL VAN DER VLUGT

Subfaculteit Wiskunde en Informatica, Universiteit van Leiden, Niels Bohrweg 1, 2300 RA Leiden, The Netherlands

Communicated by Andrew Odlyzko

Received April 6, 1989

We obtain the weight distributions of the Melas and Zetterberg codes and the double error correcting quadratic Goppa codes in terms of the traces of certain Hecke operators acting on spaces of cusp forms for the congruence subgroup $\Gamma_1(4) \subset SL_2(\mathbf{Z})$. The result is obtained from a description of the weight distributions of the dual codes in terms of class numbers of binary quadratic forms and a combination of the Eichler Selberg Trace Formula with the MacWilliams identities. © 1991 Academic Press, Inc.

1. INTRODUCTION

For an integer $m \geqslant 3$ and $q = 2^m$, the Melas codes $M(q)$ are defined to be certain binary cyclic codes of length $q-1$ and dimension $q-1-2m$. The minimum distance of these codes is 3 or 5, depending on whether q is a square or not. The Zetterberg codes $N(q)$ are similar; these are binary cyclic codes of length $q+1$ and dimension $q+1-2m$. The minimum distance is 5 or 3 depending on whether q is a square or not [12, Chap. 7, Problems 28 and 29]. The even weight subcodes of these codes are isomorphic to the extended double error correcting quadratic Goppa codes [17].

In this paper we will determine the weight distributions of the Melas and Zetterberg codes as follows: we first study the duals of the codes $M(q)$ and

* Supported by the Netherlands Organization for Scientific Research.

0097-3165/91 $3.00

$N(q)$. These codes appear to be related to a certain family of elliptic curves over the finite field $\mathbf{F}_q$ which all possess an $\mathbf{F}_q$-rational point of order 4. The weights are essentially the cardinalities of the groups of $\mathbf{F}_q$-rational points of the curves occurring in this family. The frequency of a given weight is given by the number of curves in the family with a fixed number of rational points and it can be expressed in terms of a Kronecker class number. The weights have been obtained earlier by Lachaud and Wolfmann [7, 8].

The MacWilliams identities relate the weight distributions of the dual codes to the weight distributions of the Melas and Zetterberg codes themselves. The resulting expressions for the weights appear to be similar to the Eichler Selberg Trace Formulas for the traces of the Hecke operators acting on certain spaces of cusp forms of weight $k \geqslant 2$ for the group $\Gamma_1(4)$.

Our main result, Theorems (4.2) and (5.2), is a description of the weight distributions of the Melas and Zetterberg codes in terms of the traces of these Hecke operators. As an easy consequence we obtain the weight distributions of the double error correcting quadratic Goppa codes as well.

The route we follow is like the one followed in [12, Sect. 15.3] to obtain the weight distributions of the double error correcting BCH codes. In that case, however, the family of elliptic curves that arises is a family of supersingular curves. Since these curves are quite rare, only very few weights occur in the dual code. Therefore the MacWilliams identities become particularly simple and the weight distributions of the double error correcting BCH codes are easily obtained. In our case matters are more complicated; our family contains, in a sense, all possible elliptic curves that are not supersingular and the number of occurring weights in the dual codes of $M(q)$ and $N(q)$ is approximately $\sqrt{q}$.

The proof of the main result is not very satisfactory: the group $\Gamma_1(4)$ is closely related to families of elliptic curves with a point of order 4 and it seems that one should be able to obtain our formulas in a way more direct than via the Eichler Selberg Trace Formula. Our formulas are very suitable for actual computation. In the final section this is illustrated by some examples. As a byproduct we confirm and extend certain numerical data obtained by Dür [5] and by MacWilliams and Seery [11].

The paper is organized as follows: In Section 2 we briefly discuss Kronecker class numbers and traces of Hecke operators. In Section 3 an auxiliary code C is discussed; its weight distribution is given in terms of Kronecker class numbers. In Section 4 the weight distributions of the Melas codes and their duals are derived. The same is done for the Zetterberg codes in Section 5. Finally, in Section 6, we explicitly compute the frequencies of some small weights in the Melas, Zetterberg, and Goppa codes.

2. Class Numbers and Traces of Hecke Operators

In this section certain class numbers are introduced; these occur in the Eichler Selberg Trace Formula which is stated for Hecke operators acting on the spaces of cusp forms of weight k, for the group $\Gamma_0(N)$ and with character χ.

Nothing in this section is new. The section is included for the convenience of the reader. It is supposed to contain enough information to be able to perform calculations similar to those in Section 6.

For a negative integer Δ congruent to 0 or 1 (mod 4) we let $B(\Delta)$ denote the set of positive definite binary quadratic forms,

$$B(\Delta) = \{aX^2 + bXY + cY^2 : a, b, c \in \mathbf{Z},\ a > 0 \text{ and } b^2 - 4ac = \Delta\}.$$

By $b(\Delta)$ we denote the primitive such forms,

$$b(\Delta) = \{aX^2 + bXY + cY^2 \in B(\Delta) \colon \gcd(a, b, c) = 1\}.$$

The group $SL_2(\mathbf{Z})$ acts on $B(\Delta)$ by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot f(X, Y) = f(\alpha X + \beta Y, \gamma X + \delta Y) \qquad \text{for} \quad f(X, Y) \in B(\Delta);$$

this action respects the primitive forms. It is well known that there are only finitely many orbits. The number of orbits in $b(\Delta)$ is called the class number of Δ and is denoted by $h(\Delta)$. The Kronecker class number of Δ is denoted by $H(\Delta)$; it is defined to be the number of orbits in $B(\Delta)$, but one should count the forms $aX^2 + aY^2$ and $aX^2 + aXY + aY^2$, if at all present in $B(\Delta)$, with multiplicity $\frac{1}{2}$ and $\frac{1}{3}$, respectively.

The relation between the Kronecker class numbers and the ordinary class numbers is given as follows:

Proposition 2.1. *Let Δ in $\mathbf{Z}_{<0}$ be congruent to* 0 *or* 1 (mod 4). *Then*

$$H(\Delta) = \sum_f h_w\left(\frac{\Delta}{f^2}\right),$$

where f runs over all positive divisors of Δ for which $\Delta/f^2 \in \mathbb{Z}$ is congruent to 0 *or* 1 (mod 4) *and where h_w is defined as follows*

$$h_w(-3) = \tfrac{1}{3},$$

$$h_w(-4) = \tfrac{1}{2},$$

$$h_w(\Delta) = h(\Delta) \qquad \text{for} \quad \Delta < -4.$$

Proof. For any quadratic form $aX^2+bXY+cY^2 \in B(\Delta)$ the $\gcd(a, b, c)$ is not affected by the action of $SL_2(\mathbf{Z})$. Therefore it makes sense to sort the orbits according to the gcd's of the coefficients of their elements. The orbits with a fixed $\gcd = d$ of their coefficients are in one-to-one correspondence with the orbits of the primitive forms of discriminant Δ/d^2; this is easily seen by dividing the coefficients of the forms by d. It follows that the number of orbits in $B(\Delta)$ is precisely $\sum_f h(\Delta/f^2)$, where f runs over the positive divisors of Δ for which $\Delta/f^2 \in \mathbf{Z}$ is congruent to 0 or 1 (mod 4). It is classical that $h(-3)=h(-4)=1$: all forms in $b(-3)$ are equivalent to X^2+XY+Y^2 and all forms in $b(-4)$ are equivalent to X^2+Y^2. From this and the definitions of the $h_w(\Delta)$ and the Kronecker class numbers $H(\Delta)$ the result follows at once.

The numbers $h(\Delta)$ and $H(\Delta)$ can be calculated efficiently using the theory of reduced forms: a quadratic form $aX^2+bXY+cY^2$ is called reduced when $|b| \leqslant a \leqslant c$ and $b>0$ whenever $|b|=a$ or $a=c$. Every $SL_2(\mathbf{Z})$-orbit contains precisely one reduced form. For a reduced form $aX^2+bXY+cY^2$ it holds that $|\Delta| = -b^2+4ac \geqslant -a^2+4a^2$ and therefore that $|b| \leqslant a \leqslant \sqrt{|\Delta|/3}$ which shows that it is easy to count all reduced forms (primitive or not) having a fixed discriminant Δ.

For $\Delta < -4$, the ordinary class number $h(\Delta)$ is equal to $(1/\pi)\sqrt{|\Delta|}\, L_\Delta(1)$, where $L_\Delta(1)$ denotes the value at 1 of the Dirichlet L-series associated to the quadratic residue symbol $(\frac{\Delta}{x})$. These values are rather erratic as functions of Δ. Probably it holds that $|\log L_\Delta(1)| = O(\log\log\log|\Delta|)$. A very rough approximation of $h(\Delta)$ is therefore $(1/\pi)\sqrt{|\Delta|}$. The same approximation is valid for $H(\Delta)$.

See [2] for more information on binary quadratic forms. In [2, 14] small tables of class numbers are given.

Next we discuss cusp forms. For a systematic introduction see the books by S. Lang [9] and J.-P. Serre [15].

Let $GL_2(\mathbf{R})^+$ denote the group of matrices $\{\sigma \in GL_2(\mathbf{R})\colon \det(\sigma)>0\}$. The group $GL_2(\mathbf{R})^+$ acts on the upper halfplane $\mathbf{H} = \{z \in C\colon \operatorname{Im} z > 0\}$ via fractional linear transformations: for $z \in \mathbf{H}$ and $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbf{R})^+$ we let $\sigma(z) = (az+b)/(cz+d)$. For every integer $k \geqslant 2$ we define an action of $GL_2(\mathbf{R})^+$ on the holomorphic functions on $\mathbf{H}$ as follows

$$f|_k\sigma = (\det\sigma)^{k/2}\,(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \tag{1}$$

where $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbf{R})^+$.

For any $N \in \mathbf{Z}_{\geqslant 1}$, let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \colon c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \colon a \equiv d \equiv 1 \pmod{N} \right\}.$$

The group $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$.

The space $S_k(\Gamma_1(N))$ of cusp forms of weight k for the group $\Gamma_1(N)$ is defined by

$$S_k(\Gamma_1(N)) = \{ f \colon \mathbf{H} \to \mathbf{C} \text{ holomorphic} \colon f|_k \sigma = f \text{ for all } \sigma \in \Gamma_1(N), \lim_{\operatorname{im} z \to \infty} f(\sigma z) = 0 \text{ for all } \sigma \in SL_2(\mathbf{Z}) \}.$$

An application of (1) to the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ shows that any cusp form $f(z)$ for $\Gamma_1(N)$ satisfies $f(z) = f(z+1)$. We can therefore write $f(z)$ as a Fourier series: $f = \sum_{m=1}^{\infty} a_m e^{2\pi i m z}$. Note that the constant term vanishes since f is a cusp form.

The space $S_k(\Gamma_1(N))$ can be decomposed according to the characters χ of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbf{Z}/N\mathbf{Z})^*$. We have

$$S_k(\Gamma_1(N)) = \bigoplus_{\chi} S_k(\Gamma_0(N), \chi),$$

where $S_k(\Gamma_0(N), \chi)$ consists of the cusp forms $f \in S_k(\Gamma_1(N))$ for which

$$f|_k \sigma = \chi(d) \cdot f(z)$$

for all $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

The spaces $S_k(\Gamma_1(N))$ are finite dimensional complex vector spaces; a formula for their dimensions is given in Corollary (2.3). On the $S_k(\Gamma_1(N))$ the Hecke operators T_n, $(n \in \mathbf{Z}_{\geqslant 1})$ act. These linear operators respect the above decomposition of $S_k(\Gamma_1(N))$. They are, for $f(z) = \sum_{m=1}^{\infty} a_m e^{2\pi i m z} \in S_k(\Gamma_0(N), \chi)$, defined as follows:

$$T_n \cdot f(z) = \sum_{m=1}^{\infty} \left(\sum_{d | m, n} \chi(d)\, d^{k-1} a_{mn/d^2} \right) e^{2\pi i m z}. \tag{2}$$

An application of (1) to the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ gives us that $f(z)(-1)^k = \chi(-1) f(z)$ and hence that

$$S_k(\Gamma_0(N), \chi) = 0 \qquad \text{whenever} \quad \chi(-1) \neq (-1)^k.$$

The Eichler Selberg Trace Formula gives an expression for the traces of Hecke operators in terms of class numbers of binary quadratic forms:

THEOREM 2.2. *Let $N \in \mathbf{Z}_{\geqslant 1}$ and let $\chi: (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ be a character of conductor N_χ. Furthermore, let $k \geqslant 2$ be an integer for which $\chi(-1) = (-1)^k$.*

For every integer $n \geqslant 1$ the trace Tr *of the Hecke operator T_n acting on the space of cusp forms $S_k(\Gamma_0(N), \chi)$ is given by*

$$\mathrm{Tr}(T_n) = A_1 + A_2 + A_3 + A_4,$$

where

$$A_1 = n^{k/2-1}\chi(\sqrt{n})\frac{k-1}{12}\psi(N).$$

(Here $\chi(\sqrt{n}) = 0$ whenever $\sqrt{n} \notin \mathbf{Z}$ and $\psi(N)$ denotes $N\prod_{p \mid N}(1 + 1/p)$, where the product runs over the prime divisors p of N).

$$A_2 = -\frac{1}{2}\sum_{t \in \mathbf{Z}, t^2 < 4n} \frac{\rho^{k-1} - \bar{\rho}^{k-1}}{\rho - \bar{\rho}} \sum_f h_w\left(\frac{t^2 - 4n}{f^2}\right)\mu(t, f, n).$$

(Here ρ and $\bar{\rho}$ denote the zeroes of the polynomial $X^2 - tX + n$ and the sum runs over the positive divisors f of $t^2 - 4n$ for which $(t^2 - 4n)/f^2 \in \mathbf{Z}$ is congruent to 0 *or* 1 (mod 4). *The numbers $\mu(t, f, n)$ are given by*

$$\mu(t, f, n) = \frac{\psi(N)}{\psi(N/N_f)} \sum_{\substack{x \pmod N \\ x^2 - tx + n \equiv 0 \pmod{N_f N}}} \chi(x),$$

where N_f denotes $\gcd(N, f)$. It is left to the reader to verify that the x's occurring in the sum are well defined.)

$$A_3 = -\sum_{\substack{d \mid n \\ 0 < d \leqslant \sqrt{n}}}{}' d^{k-1} \sum_{\substack{c \mid N \\ \gcd(c, N/c) \mid \gcd(N/N_\chi, n/d - d)}} \phi\left(\gcd\left(c, \frac{N}{c}\right)\right)\chi(y).$$

(Here ϕ denotes Euler's ϕ-function; the prime in the first summation indicates that the contribution of the term $d = \sqrt{n}$, if it occurs, should be multiplied by $\frac{1}{2}$. The number y is defined modulo $N/\gcd(c, N/c)$ by $y \equiv d \pmod c$, $y \equiv (n/d) \pmod{N/c}$.)

$$A_4 = \sum_{\substack{0 < t \mid n, \\ \gcd(N, n/t) = 1}} t \qquad \text{if } k = 2 \text{ and } \chi = 1,$$

$$= 0 \qquad \text{otherwise.}$$

(The unit character is denoted by 1. *We recall that every character χ is extended to $\mathbf{Z}/N\mathbf{Z}$ by $\chi(m) = 0$ whenever $\gcd(m, N) > 1$).*

Proof. These formulas are taken from H. Cohen's paper [3]. Cohen's unpublished proof is along the lines of the proof D. Zagier gave for the case $N=1$ and $\chi=1$, see [9, 18]. The reader is referred to J. Oesterlé's thesis [13] for a complete proof.

COROLLARY 2.3. *Let $N \in \mathbf{Z}_{\geqslant 1}$ and let $\chi: (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ be a character of conductor N_χ. Let $k \geqslant 2$ be an integer satisfying $\chi(-1) = (-1)^k$. Then*

$$\begin{aligned}
&\dim S_k(\Gamma_0(N), \chi) \\
&= \frac{k-1}{12}\psi(N) - \left(\frac{k-1}{3} - \left[\frac{k}{3}\right]\right) \sum_{\substack{x \pmod N \\ x^2+x+1 \equiv 0 \pmod N}} \chi(x) \\
&\quad - \left(\frac{k-1}{4} - \left[\frac{k}{4}\right]\right) \sum_{\substack{x \pmod N \\ x^2+1 \equiv 0 \pmod N}} \chi(x) \\
&\quad - \frac{1}{2} \sum_{\substack{c \mid N \\ \gcd(c, N/c) \mid (N/N_\chi)}} \phi\left(\gcd\left(c, \frac{N}{c}\right)\right) + \begin{cases} 1 & \text{if } k=2 \text{ and } \chi=1, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

Proof. Since the Hecke operator T_1 is just the identity map, we have that $\dim S_k(\Gamma_0(N), \chi) = \mathrm{Tr}(T_1)$. Therefore Theorem (2.2) gives us a formula for the dimensions of the spaces $S_k(\Gamma_0(N), \chi)$.

Remark 2.4. The numbers $(\rho^{k-1} - \bar{\rho}^{k-1})/(\rho - \bar{\rho})$, being symmetric expressions in ρ and $\bar{\rho}$ can be written as polynomials $Q_{k-2}(t, n)$ in $t = \rho + \bar{\rho}$ and $n = \rho\bar{\rho}$.

For future purposes, we introduce some notation concerning these polynomials. We have

$$\begin{aligned}
Q_0(t, n) &= 1, \\
Q_1(t, n) &= t, \\
Q_{k+1}(t, n) &= tQ_k(t, n) - nQ_{k-1}(t, n) \qquad (k \geqslant 1).
\end{aligned}$$

When we assign the variable t a weight equal to 1 and n a weight equal to 2, then the polynomial $Q_k(t, n)$ is seen to be homogeneous of weight k. Viewed as a polynomial in t it is monic and we can therefore write

$$t^i = \sum_{j=0,\, j \text{ even}}^{i} \lambda_{i,j} Q_{i-j}(t, n)\, n^{j/2}; \tag{3}$$

the $\lambda_{i,j} \in \mathbf{Z}$ are easily seen to satisfy

$$\begin{aligned} &\lambda_{i,j} = 0 \qquad \text{whenever } j \notin \{0, 1, ..., i\} \text{ or } j \text{ odd}, \\ &\lambda_{0,0} = \lambda_{1,0} = 1, \\ &\lambda_{i+1,j} = \lambda_{i,j-2} + \lambda_{i,j}. \end{aligned} \tag{4}$$

One has in fact that $\lambda_{i,2j} = \binom{i-1}{j} - \binom{i-1}{j-2}$.

Finally we apply the Trace Formula in Theorem (2.2) to the case of $\Gamma_1(4)$:

THEOREM 2.5. *Let $m \geqslant 1$ and $q = 2^m$. The trace of the Hecke operator T_q acting on the space of cusp forms $S_k(\Gamma_1(4))$ is given by*

$$\begin{aligned} \operatorname{Tr}(T_q) &= -1 + q - \sum_t H(t^2 - 4q) = 0 && \text{for } k = 2, \\ &= -1 - (-1)^{qk/2} \sum_t Q_{k-2}(t, q) H(t^2 - 4q) && \text{for } k \geqslant 3. \end{aligned}$$

The summation variables t run over $\{t \in \mathbf{Z}: t^2 < 4q$, and $t \equiv 1 \pmod 4\}$.

Proof. The space $S_k(\Gamma_1(4))$ is equal to $S_k(\Gamma_0(4), 1)$ when k is even and to $S_k(\Gamma_0(4), \omega)$, where ω denotes the non-trivial character of $(\mathbf{Z}/4\mathbf{Z})^*$ when k is odd. One checks that $A_3 = -1$ and that for fixed t, all the $\mu(t, f, q)$ occurring in the trace formula are equal. In fact, one finds that $\mu(t, f, q) = (-1)^{q/2} \chi(t)$, where χ denotes 1 or ω according as k is even or odd. Therefore, by Proposition (2.1), the sums of the class numbers h_w may be replaced by Kronecker class numbers. The result now follows directly from the Trace Formula in Theorem (2.2). For $k = 2$ the trace is 0 because $\dim S_2(\Gamma_1(4)) = 0$.

3. Codes and Elliptic Curves

In this section we will determine the weight distributions of certain auxiliary codes. These codes were introduced by G. Lachaud and J. Wolfmann [7]. They independently obtained the results of this section [8]. For the sake of completeness, we present our approach.

Let $m \geqslant 3$ and let $q = 2^m$ denote a fixed power of 2. Let $\operatorname{Tr}: \mathbf{F}_q \to \mathbf{F}_2$ denote the trace map; this is an $\mathbf{F}_2$-linear map whose kernel consists precisely of the elements of the form $y^2 + y$ with $y \in \mathbf{F}_q$.

Let V be an $\mathbf{F}_2$-vector space with coordinates indexed by $\mathbf{F}_q^*$. The binary code $C(q) \subset V$ of length $q - 1$ is defined by

$$C(q) = \{c(a, b) = (\operatorname{Tr}(ax + b/x))_{x \in \mathbf{F}_q^*}: a \in \mathbf{F}_q, b \in \mathbf{F}_2\}.$$

We will determine the weight distribution of the code $C(q)$. This will involve elliptic curves over $\mathbf{F}_q$. For the basic properties of elliptic curves see J. Silverman's book [16].

PROPOSITION 3.1. *The weights of the words $c(a, b)$ in $C(q)$ are as follows:*

(1) $c(0, 0)$ *has weight* 0,

(2) $c(0, 1)$ *has weight* $\frac{1}{2}q$,

(3) $c(a, 0)$ *has weight* $\frac{1}{2}q$ *for* $a \neq 0$,

(4) $c(a, 1)$ *has weight* $q - \frac{1}{2}\#E_a(\mathbf{F}_q)$ *for* $a \neq 0$.

Here $E_a(\mathbf{F}_q)$ denotes the group of points defined over $\mathbf{F}_q$ on the elliptic curve E_a an affine Weierstrass equation of which is given by

$$Y^2 + XY = X^3 + aX.$$

Proof. The weights of the words $c(a, b)$ are easily determined whenever $ab = 0$. Let therefore $a \neq 0$ and $b = 1$. For a given $x \in \mathbf{F}_q^*$ the equation $Y^2 + Y = ax + 1/x$ has two or no solutions in $\mathbf{F}_q$ depending on whether $\mathrm{Tr}(ax + 1/x)$ equals 0 or 1. We conclude that

$$\mathrm{Tr}(ax + 1/x) = 1 - \tfrac{1}{2}\#\{y \in \mathbf{F}_q : y^2 + y = ax + 1/x\}$$

and hence that the weight of the word $c(a, b)$ is equal to

$$q - 1 - \tfrac{1}{2}\#C_a(\mathbf{F}_q).$$

Here $C_a(\mathbf{F}_q)$ denotes the number of finite points on the curve C_a which is given by

$$Y^2 + Y = aX + 1/X.$$

Using the transformation $Y \leftarrow aXY$, $X \leftarrow aX$ we see that the projective curve given by C_a is isomorphic to the curve

$$E_a : Y^2 + XY = X^3 + aX.$$

Since the curve E_a has only one point at infinity while the curve C_a has the two points with $X = 0$ viz. $(0 : 0 : 1)$ and $(0 : 1 : 0)$ at infinity, we see that $\#C_a(\mathbf{F}_q) = \#E_a(\mathbf{F}_q) - 2$ and the result follows easily.

COROLLARY 3.2. *The code $C(q)$ has dimension $m + 1$ over $\mathbf{F}_2$.*

Proof. Consider the homomorphism $\mathbf{F}_q \times \mathbf{F}_2 \to C(q)$ given by $(a, b) \mapsto (\mathrm{Tr}(ax + b/x))_{x \in \mathbf{F}_q^*}$. Suppose (a, b) is in the kernel of this map. Then the weight of $c(a, b)$ is 0 and either $a = b = 0$ or the elliptic curve E_a has $2q$

points over $\mathbf{F}_q$. Since $|q+1-\#E_a(\mathbf{F}_q)| \leqslant 2\sqrt{q}$ (see [16]) we conclude that $q-1 \leqslant 2\sqrt{q}$ which is impossible since $m \geqslant 3$. Therefore the map is injective and the corollary follows.

THEOREM 3.3. *The non-zero weights in the code* $C(q)$ *are* $w_t = (q-1+t)/2$, *where* $t \in \mathbf{Z}$, $t^2 < 4q$ *and* $t \equiv 1 \pmod 4$.

For $t \neq 1$ *the weight* w_t *has frequency* $H(t^2-4q)$ *while* w_1 *has frequency* $H(1-4q)+q$.

Proof. Consider the family of curves

$$E_a: Y^2 + XY = X^3 + aX \qquad (a \in \mathbf{F}_q^*).$$

These are elliptic curves with j-invariants equal to a^{-2}. Every element in $\mathbf{F}_q^*$ occurs exactly once as a j-invariant in this family. Over $\mathbf{F}_q$ there are for every non-zero j-invariant precisely two elliptic curves having this j-invariant [14, Thm. 4.6]. If one of these has $q+1-t$ points over $\mathbf{F}_q$, then the other has $q+1+t$ points. Since every curve in the family has $(a^{q/2}, 0)$ as an $\mathbf{F}_q$-rational point of order 4, we conclude that actually every elliptic curve E over $\mathbf{F}_q$ with 4 dividing $\#E(\mathbf{F}_q)$ occurs exactly once in our family. The number of elliptic curves over $\mathbf{F}_q$ with precisely $q+1-t$ points over $\mathbf{F}_q$ is known; see for instance [14, Prop. 5.7]: when $t^2 > 4q$ there are no such curves and when $t^2 < 4q$ and t is odd, the number of such curves is equal to the Kronecker class number $H(t^2-4q)$. For even t satisfying $t^2 \leqslant 4q$, we refer to [14], since we do not need those numbers here.

By Proposition (3.1) and the discussion above we have that the non-zero weights of $C(q)$ are the numbers $q - \frac{1}{2}(q+1-t) = (q-1+t)/2$, where $t^2 < 4q$ and $t \equiv 1 \pmod 4$. When $t \neq 1$ only words of type $c(a, 1)$ can have weight $(q-1+t)/2$ and there are precisely $H(t^2-4q)$ such words. When $t=1$ the words $c(0,1)$ and $c(a,0)$ with $a \in \mathbf{F}_q^*$ have weight $(q-1+t)/2 = \frac{1}{2}q$; we conclude that $H(1-4q)+q$ words have weight $\frac{1}{2}q$.

This proves the theorem.

4. THE MELAS CODES

Let $m \geqslant 3$ and let $q = 2^m$. Let α be a generator of the multiplicative group $\mathbf{F}_q^*$. Consider the cyclic code M' of length $q-1$ over $\mathbf{F}_q$ with generator polynomial $(X-\alpha)(X-\alpha^{-1})$. The dual of this code is cyclic with zeroes 1, α^2, α^3, ..., α^{q-3}; these are precisely the zeroes of the polynomials

$$\sum_{i=0}^{q-2} (a\alpha^i + b\alpha^{-i})\, X^i \in \mathbf{F}_q[X]/(X^{q-1}-1) \qquad (a, b \in \mathbf{F}_q)$$

and one concludes that the dual code is just

$$\left\{\left(ax+\frac{b}{x}\right)_{x\in\mathbf{F}_q^*} : a, b\in\mathbf{F}_q\right\}.$$

The Melas code $M(q)$ of length $q-1$ is defined to be the restriction to $\mathbf{F}_2$ of M'. Since the dual of a restriction is the trace of the dual code [12, Chap. 7. Thm. 11.], we see that the dual $M(q)^\perp$ is the $2m$-dimensional code

$$\left\{\left(\operatorname{Trace}_{\mathbf{F}_q/\mathbf{F}_2}\left(ax+\frac{b}{x}\right)\right)_{x\in\mathbf{F}_q^*} : a, b\in\mathbf{F}_q\right\}.$$

The codes $M(q)^\perp$ and therefore $M(q)$ do not depend on the choice of the generator α. We have the following description of the weight distribution of $M(q)^\perp$:

THEOREM 4.1. *The non-zero weights of the dual Melas code $M(q)^\perp$ are $w_t=(q-1+t)/2$, where $t\in\mathbf{Z}$, $t^2<4q$ and $t\equiv 1 \pmod 4$.*

For $t\neq 1$ the frequency of w_t is $(q-1)H(t^2-4q)$; the weight $w_1=q/2$ has frequency $(q-1)(H(1-4q)+2)$.

Proof. The group $\mathbf{F}_q^*$ acts on the code $M(q)^\perp$ by $\zeta\colon (a, b)\mapsto(\zeta a, \zeta^{-1}b)$ for $\zeta\in\mathbf{F}_q^*$; it is easily seen that words in the same orbit have the same weight. For $b=0$ we find the zero-word and $q-1$ words of weight $\frac{1}{2}q$ in $M(q)^\perp$. The set of words with $b\neq 0$ is stable under the action of $\mathbf{F}_q^*$; every orbit has length $q-1$ and contains exactly one word $c(a, 1)$ of the code $C(q)$ in Section 3.

Apart from the weight $\frac{1}{2}q$, the theorem now follows from Theorem (3.3). The $q-1$ words with $b=0$ and the $q-1$ words in the orbit of $c(0, 1)$ all have weight $\frac{1}{2}q$. Together with the $H(1-4q)$ orbits of words $c(a, 1)$ with $a\neq 0$ that have weight $\frac{1}{2}q$ in $C(q)$ we find $(q-1)(H(1-4q)+2)$ words of weight $w_1=\frac{1}{2}q$, as required.

The rough approximations of the Kronecker class numbers mentioned in Section 2 imply rough estimates for the weight distributions of the dual Melas codes: for t as in Theorem (4.1), the number of words of weight $w_t=(q-1+t)/2$ is approximately equal to $((q-1)/\pi)\sqrt{4q-t^2}$.

We combine Theorem (4.1) with the MacWilliams identities to obtain an expression for the weight distribution of the Melas codes $M(q)$ themselves.

THEOREM 4.2. *The number A_i of code words of weight i in the Melas code $M(q)$ is given by*

$$q^2 A_i = \binom{q-1}{i} + 2(-1)^{[(i+1)/2]}(q-1)\binom{q/2-1}{[i/2]}$$
$$-(q-1)\sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} W_{i,j}(q)(1+\tau_{j+2}(q));$$

here the polynomials $W_{i,j}(q)$ *are for* $0 \leqslant j \leqslant i$ *and* $i \equiv j \pmod 2$ *defined by*

$$W_{0,0} = 1, \qquad W_{1,1} = -1,$$
$$(i+1)\, W_{i+1,j+1} = -qW_{i,j+2} - W_{i,j} - (q-i)\, W_{i-1,j+1}$$

(*otherwise the* $W_{i,j}$ *are* 0).

By $\tau_k(q)$ *we denote for* $k \geqslant 3$ *the trace of the Hecke operator* T_q *on* $S_k(\Gamma_1(4))$. *For convenience we let* $\tau_2(q) = -q$.

Proof. For $0 \leqslant l \leqslant q-1$ let $P_l(X)$ denote the lth Krawtchouk polynomial [12, Sect. 5.2]. We define

$$f_l(X) = P_l\left(\frac{q-1+X}{2}\right).$$

The recurrence relation satisfied by the Krawtchouk polynomials becomes

$$f_0(X) = 1; \qquad f_1(X) = -X;$$
$$(l+1)\, f_{l+1}(X) = -Xf_l(X) - (q-l)\, f_{l-1}(X);$$

it follows that f_l has degree l and that the parity of f_l is equal to the parity of l. We can therefore write

$$f_l(X) = \sum_{\substack{k=0 \\ k \equiv l \pmod 2}}^{l} \pi_l(k)\, X^k. \tag{5}$$

We have that $\pi_0(0) = 1$ and $\pi_1(1) = -1$ and by the recurrence relation that

$$(l+1)\, \pi_{l+1}(k+1) = -\pi_l(k) - (q-l)\, \pi_{l-1}(k+1). \tag{6}$$

We apply the MacWilliams identities [12, Chap. 5, formula (13)] to the weight distributions of the code $M(q)$ and its dual

$$q^2 A_i = \sum_t \text{frequency}(w_t)\, P_i\left(\frac{q-1+t}{2}\right) + P_i(0),$$

where t runs over $\{t \in \mathbf{Z}: t^2 < 4q \text{ and } t \equiv 1 \pmod 4\}$. Using Theorem (4.1) and the polynomial f_i introduced above we find

$$\frac{q^2}{q-1} A_i = \sum_t f_i(t)\, H(t^2 - 4q) + \frac{P_i(0)}{q-1} + 2f_i(1). \tag{7}$$

It is not difficult to see that

$$P_i(0) = \binom{q-1}{i} \tag{8}$$

and that

$$f_i(1) = (-1)^{[(i+1)/2]} \binom{q/2 - 1}{[i/2]}. \tag{9}$$

From (5) we obtain that

$$\sum_t f_i(t)\, H(t^2 - 4q) = \sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} \pi_i(j) \sum_t t^j H(t^2 - 4q).$$

By formula (3) this becomes

$$\sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} \pi_i(j) \sum_{\substack{k=0 \\ k \text{ even}}}^{j} \lambda_{j,k} q^{k/2} \sum_t Q_{j-k}(t, q)\, H(t^2 - 4q).$$

Since 4 divides q, this becomes by Theorem (2.5)

$$\sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} \pi_i(j) \sum_{\substack{k=0 \\ k \text{ even}}}^{j} \lambda_{j,k} q^{k/2} (-1 - \tau_{j-k+2}(q))$$

which after changing the summation variables somewhat is seen to be equal to

$$\sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} W_{i,j}(q)(-1 - \tau_{j+2}(q)), \tag{10}$$

where

$$W_{i,j}(q) = \sum_{\substack{k=0 \\ k \text{ even}}}^{i-j} \pi_i(k+j)\, \lambda_{k+j,k} q^{k/2}.$$

Clearly formula's (7), (8), (9), and (10) imply the theorem. It only remains to check the recurrence relation for the $W_{i,j}(q)$.

One verifies at once that $W_{0,0}=1$ and that $W_{1,1}=-1$. Combining the recurrence relation (6) for the $\pi_i(j)$ and the relations (4) for the $\lambda_{i,j}$ one easily finds that

$$(i+1)\,W_{i+1,j+1}=-qW_{i,j+2}-W_{i,j}-(q-i)\,W_{i-1,j+1}$$

as required.

As an application of Theorem (4.2) we derive formula's for the asymptotic behavior of the frequencies A_i for a fixed weight i as q tends to infinity.

THEOREM 4.3. *Let i be a fixed positive integer and let A_i denote the number of words in $M(q)$ of weight i. Then*

$$A_i=\frac{1}{q^2}\binom{q-1}{i}+\frac{(-1)^i a_i}{i!}q^{i/2}+O(q^{(i-1)/2}),\qquad q\to\infty.$$

Here $a_i=a_{i,0}$ where the $a_{i,j}$ are defined as follows: they are zero whenever $j\notin\{0,\ldots,i\}$ or $i\not\equiv j \pmod 2$. We have $a_{0,0}=1$, $a_{1,1}=-1$ and the recursion is given by $a_{i+1,j+1}=a_{i,j+2}+a_{i,j}-ia_{i-1,j+1}$.

Proof. One shows by induction that $\deg W_{i,j}(q)$ does not exceed $(i-j)/2$. For odd k it is well known that the absolute values of the eigenvalues of T_2 acting on $S_k(\Gamma_1(4))=S_k(\Gamma_0(4),\omega)$ are equal to $2^{(k-1)/2}$ see, e.g., [10, Thm. 3].

For even k one uses the Trace Formula to verify that the trace of T_2 is equal to the trace of T_2 acting on $S_k(\Gamma_0(2),1)$. The eigenvalues of T_2 acting on the latter space come in two types: the ones coming from $S_k(\Gamma_0(2),1)^{\text{new}}$ have absolute values equal to $2^{k/2-1}$ as is easy to show [10, Thm. 3]; the ones coming from the old part are the zeroes of the polynomials $X^2-\lambda X+2^{k-1}$, where λ is an eigevalue of T_2 acting on $S_k(SL_2(\mathbf{Z}))$. It follows from Deligne's Theorem on the Ramanujan–Petersson conjecture [4, Thm. 8.2] that the absolute values of these zeroes are $2^{(k-1)/2}$. See [1, 9] and Section 6 for the decomposition of the spaces in old and new parts.

To obtain the estimates for the eigenvalues $\tau_k(q)$ of T_q we observe that on $S_k(\Gamma_0(4),\omega)$ and $S_k(\Gamma_0(2),1)$ we have that $T_q=T_2^m$ and therefore that, for $k\geqslant 3$, the eigenvalues of T_q on these spaces are $O(q^{(k-1)/2})$. We have, of course, by convention that $\tau_2(q)=-q$.

We conclude that $W_{i,j}(q)(1+\tau_{j+2}(q))$ is $O(q^{(i+1)/2})$ for every $j\geqslant 1$ and $i\geqslant 0$. Since $a_i=0$ for odd i, the result follows for odd i at once from Theorem (4.2).

For even i we must take the contribution of $\tau_2(q)$ into account. Since deg $W_{i,0}$ does not exceed $i/2$, we see that the contribution is equal to (ith coefficient of $W_{i,0}(q)$) $q^{i/2-2}(1-q)^2$. It is easy to see that this ith coefficient is just $(-1)^i a_i/i!$ and that modulo $O(q^{(i-1)/2})$ the contribution is $(a_i/i!)\, q^{i/2}$. This proves the theorem.

Remark 4.4. Observe that we only used Deligne's Theorem to obtain the asymptotics of the even weights. One does not need Deligne's Theorem to obtain the somewhat weaker statement

$$A_i = \frac{1}{q^2}\binom{q-1}{i} + O(q^{i/2}), \qquad q \to \infty$$

which is much easier to prove.

Remark 4.5. The even weight subcode of $M(q)$ is isomorphic to the extended double error correcting quadratic Goppa code with reducible quadratic polynomial over $\mathbf{F}_q$. Since this code admits a transitive automorphism group, the weight distribution of the quadratic Goppa code $G_{\text{red}}(q)$ itself follows at once from Theorem (4.2), see [12, Chap. 8, Thm. 14]: The number of words in $G_{\text{red}}(q)$ of weight i is given by

$$C_i = \frac{i+1}{q-1} A_{i+1} \qquad \text{for odd } i,$$

$$= \frac{q-1-i}{q-1} A_i \qquad \text{for even } i.$$

Note that only the A_i for even i are involved. Therefore the formulas for C_i that result from Theorem (4.2) will only involve the traces of the Hecke operators T_q for the full modular group $SL_2(\mathbf{Z})$. In Section 6 a small table of the A_i is given.

5. The Zetterberg Codes

Let $m \geqslant 3$ and $q = 2^m$. Let β be a generator of the group $\mu_{q+1} \subset \mathbf{F}_{q^2}^*$ of $q+1$st roots of unity. Consider the cyclic code N' of length $q+1$ over $\mathbf{F}_q^*$ with generator polynomial $X-\beta$. The Zetterberg code $N(q)$ of length $q+1$ is defined to be the restriction of N' to $\mathbf{F}_2$. It is a code of codimension $2m$. Similar to the discussion of the Melas codes in the previous section we have that

$$N(q)^\perp = \{(\operatorname{Trace}_{\mathbf{F}_{q^2}/\mathbf{F}_2}(ax))_{x \in \mu_{q+1}} : a \in \mathbf{F}_{q^2}\}.$$

Note that $N(q)$ and $N(q)^\perp$ do not depend on the choice of β.

The weight distribution of $N(q)^\perp$ is as follows:

THEOREM 5.1. *The non-zero weights of the dual Zetterberg code $N(q)^{\perp}$ are $w_t = (q+1-t)/2$, where $t \in \mathbf{Z}$, $t^2 < 4q$ and $t \equiv 1 \pmod 4$.*
The weight w_t has frequency $(q+1)H(t^2-4q)$.

Proof. Since $\mathbf{F}_{q^2}^*$ is the direct product of μ_{q+1} and $\mathbf{F}_q^*$, we can write any $a \in \mathbf{F}_{q^2}^*$ as $a = A \cdot \zeta$, where $A \in \mathbf{F}_q^*$ and $\zeta \in \mu_{q+1}$. The weight of $(\mathrm{Tr}(ax))_{x \in \mu_{q+1}}$ is equal to the weight of $(\mathrm{Tr}(Ax))_{x \in \mu_{q+1}}$. We have

$$(\mathrm{Tr}(Ax))_{x \in \mu_{q+1}} = (\operatorname{Trace}_{\mathbf{F}_q/\mathbf{F}_2}(Ax + (Ax)^q))_{x \in \mu_{q+1}},$$

$$= (\operatorname{Trace}_{\mathbf{F}_q/\mathbf{F}_2}(A(x + 1/x)))_{x \in \mu_{q+1}}.$$

It is easily seen that the sets $\{A(x+1/x)\colon x \in \mu_{q+1}\}$ and $\{A(x+1/x)\colon x \in \mathbf{F}_q^*\}$ have intersection $\{0\}$ and union $\mathbf{F}_q$. We conclude that

$$\mathrm{weight}(\mathrm{Tr}(ax)_{x \in \mu_{q+1}}) = q - \mathrm{weight}((A(x+1/x))_{x \in \mathbf{F}_q^*}).$$

When A runs over $\mathbf{F}_q^*$, the words $\mathrm{Tr}(A(x+1/x))$ run, as in the proof of Theorem (4.1), over a set of representatives of the orbits of the words $c(a, b)$ of the dual Melas code $M(q)^{\perp}$. Since every $A \in \mathbf{F}_q^*$ occurs for $q+1$ values of $a \in \mathbf{F}_{q^2}^*$ the result follows from Theorem (4.1).

Theorem (5.1) confirms certain numerical results obtained by Dür [5] and MacWilliams and Seery [11].

The weight distribution of the Zetterberg codes themselves are obtained by applying the MacWilliams identities.

THEOREM 5.2 *The number B_i of code words of weight i in the Zetterberg code $N(q)$ is given by*

$$q^2 B_i = \binom{q+1}{i} - (q+1) \sum_{\substack{j=0 \\ j \equiv i \pmod 2}}^{i} V_{i,j}(q)(1 + \tau_{j+2}(q));$$

here the polynomials $V_{i,j}(q)$ are for $0 \leqslant j \leqslant i$ and $i \equiv j \pmod 2$ defined by

$$V_{0,0} = 1, \qquad V_{1,1} = 1,$$

$$(i+1)\, V_{i+1,j+1} = q V_{i,j+2} + V_{i,j} - (q+2-i)\, V_{i-1,j+1}$$

(otherwise the $V_{i,j}$ are 0).

By $\tau_k(q)$ we denote for $k \geqslant 3$ the trace of the Hecke operator T_q on $S_k(\Gamma_1(4))$. For convenience we let $\tau_2(q) = -q$.

Proof. The proof is very similar to the proof of Theorem 4.2 and is left to the reader.

Remark 5.3. Instead of proving Theorem (5.2) directly, one can also derive the theorem from Theorem (4.2) as follows. We know the weight enumerators

$$A_{M^\perp}(z) = \sum_t (q-1) H(t^2-4q)\, z^{(q-1+t)/2} + 2(q-1)\, z^{q/2} + 1$$

of the dual Melas code $M(q)^\perp$ and

$$A_{N^\perp}(z) = \sum_t (q+1) H(t^2-4q)\, z^{(q+1-t)/2} + 1$$

of the dual Zetterberg code $N(q)^\perp$. Exploiting their similarity and the formulas that relate the weight enumerators of linear codes to the weight enumerators of their duals, we can relate the weight enumerators of the Zetterberg codes $A_{N(q)}$ to the weight enumerators $A_{M(q)}$ of the Melas codes as given in Theorem (4.2). After some straightforward calculations one finds

$$\begin{aligned} q^2 A_{N(q)}(z) = {} & q^2 \left(\frac{q+1}{q-1}\right)(1-z^2)\, A_{M(q)}(-z) \\ & - 2(q+1)(1+z)(1-z^2)^{q/2} \\ & - \left(\frac{q+1}{q-1}\right)(1+z)(1-z)^q + (1+z)^{q+1}. \end{aligned}$$

This leads to the following formula for the number B_i of code words of weight i in the Zetterberg code $N(q)$ in terms of the frequencies A_i of Theorem (4.2):

$$\begin{aligned} \frac{q^2}{q+1} B_i = {} & \frac{1}{q+1}\binom{q+1}{i} + (-1)^i \frac{q^2}{q-1}(A_i - A_{i-2}) \\ & - 2(-1)^{[i/2]} \binom{q/2}{[i/2]} - \frac{(-1)^i}{q-1}\left(\binom{q}{i} - \binom{q}{i-1}\right). \end{aligned}$$

One can check that Theorem (5.2) follows from this. One also obtains expressions for the $V_{i,j}$ in terms of the $W_{i,j}$.

We have the following formulas for the behavior of the B_i's as q tends to infinity:

THEOREM 5.4. *Let i be a fixed positive integer and let B_i denote the number of words in $N(q)$ of weight i. Then*

$$B_i = \frac{1}{q^2}\binom{q+1}{i} + \frac{a_i}{i!}q^{i/2} + O(q^{(i-1)/2}), \qquad q \to \infty.$$

Here the a_i are defined as in Theorem (4.3).

Proof. The proof is similar to the proof of Theorem (4.3) and is left to the reader. Without Deligne's Theorem it is easy to show that

$$B_i = \frac{1}{q^2}\binom{q+1}{i} + O(q^{i/2}), \qquad q \to \infty.$$

Remark 5.5. The even weight subcode of $N(q)$ is isomorphic to the extended double error correcting quadratic Goppa code with irreducible quadratic polynomial over $\mathbf{F}_q$. As in Remark (4.5), the number of words in the quadratic Goppa code $G_{\text{irr}}(q)$ of weight i is given by

$$D_i = \frac{i+1}{q+1}B_{i+1} \qquad \text{for odd } i,$$

$$= \frac{q+1-i}{q+1}B_i \qquad \text{for even } i.$$

Only the B_i for even i are involved. Therefore the formulas for D_i that result from Theorem (5.2) will only involve the traces of the Hecke operators T_q for the full modular group $SL_2(\mathbf{Z})$. In Section 6 a small table of the B_i is given.

6. CALCULATIONS AND EXAMPLES

In this section we will illustrate Theorems (4.2) and (5.2). We will compute the frequencies of some small weights of the Melas, Zetterberg, and quadratic Goppa codes.

Since the binomial coefficients and the polynomials $W_{i,j}$ and $V_{i,j}$ that appear in Theorems (4.2) and (5.2) are very easily computed using their recurrence relations, the main problem in applying the theorems is the calculation of the $\tau_k(q)$ for $k \geqslant 2$. By convention we have that $\tau_2(q) = -q$ while for $k \geqslant 3$, $\tau_k(q)$ is the trace of the Hecke operator T_q acting on the space $S_k(\Gamma_1(4))$. We will explain the well known way in which these traces can be computed. For an extensive discussion of modular forms for the group $\Gamma_1(4)$ see [6]. As always we let $m \geqslant 3$ and $q = 2^m$.

For odd k we deduce from Corollary (2.3) that the dimension of $S_k(\Gamma_1(4)) = S_k(\Gamma_0(4), \omega) = (k-3)/2$. As an example we prove the following.

PROPOSITION 6.1. *The trace $\tau_k(q)$ of T_q acting on $S_k(\Gamma_0(4), \omega)$ is for $k = 3, 5, 7, 9, 11,$ and 13 given as*

$$\tau_3(q) = 0,$$
$$\tau_5(q) = \pm q^2,$$
$$\tau_7(q) = \mathrm{Trace}(\alpha_7^m)\, q^3,$$
$$\tau_9(q) = (1 + \mathrm{Trace}(\alpha_9^m))\, q^4,$$
$$\tau_{11}(q) = \mathrm{Trace}(\alpha_{11}^m)\, q^5,$$
$$\tau_{13}(q) = (\pm 1 + \mathrm{Trace}(\alpha_{13}^m))\, q^6,$$

where the α_i are algebraic numbers of absolute value 1 given by $\alpha_7 = (1 + \sqrt{-15})/4$, $\alpha_9 = (-5 + \sqrt{-39})/8$, $\alpha_{11} = (3 + \sqrt{-510 + 6\sqrt{505}})/32$ and $\alpha_{13} = (-27 + \sqrt{1129} + \sqrt{-2238 + 54\sqrt{1129}})/32$. Here $\pm$ denotes $(-1)^m$ and the Trace of an algebraic number is the sum of all its conjugates.

Proof. Since $\dim S_3(\Gamma_0(4), \omega) = 0$, we have that $\tau_3(q) = 0$. We will for $k = 5, 7, 9, 11,$ and 13 compute the eigenvalues of T_2 acting on $S_k(\Gamma_1(4)) = S_k(\Gamma_0(4), \omega)$.

The Trace formula in Theorem (2.5) gives us that for weight k

$$\mathrm{Tr}(T_2) = -1 + Q_{k-2}(1, 2) H(-7),$$
$$\mathrm{Tr}(T_4) = -1 - Q_{k-2}(1, 4) H(-15) - Q_{k-2}(-3, 4) H(-7)$$

and that

$$\mathrm{Tr}(T_8) = -1 - Q_{k-2}(1, 8)\, H(-31) - Q_{k-2}(-3, 8) \times H(-23) - Q_{k-2}(5, 8)\, H(-7).$$

Using the recurrence relation for the polynomials $Q_{k-2}(t, q)$ and the fact that $H(-7) = 1$, that $H(-15) = 2$ and that $H(-23) = H(-31) = 3$ one finds the entries of the three columns in the table below.

The roots ζ of the characteristic polynomial of T_2 have absolute value $2^{(k-1)/2}$. This implies that the polynomial $F_k(X)$ with roots $\zeta/2^{(k-1)/2}$ is self-reciprocal. Therefore the first $[(k-3)/4] + 1$ coefficients, which are easily obtained from the values of $\mathrm{Tr}(T_{2^i})$ for $1 \leqslant i \leqslant [(k-3)/4] + 1$, determine $F_k(X)$.

k	$\mathrm{Tr}(T_2)$	$\mathrm{Tr}(T_4)$	$\mathrm{Tr}(T_8)$	$F_k(X)$
5	-4	-16	-64	$X+1$
7	4	-112	-704	$X^2-\frac{1}{2}X+1$
9	-4	144	11456	$(X-1)(X^2+\frac{5}{4}X+1)$
11	-12	16	-36288	$X^4+\frac{3}{8}X^3+\frac{1}{16}X^2+\frac{3}{8}X+1$
13	44	2576	188864	$(X+1)(X^4-\frac{27}{16}X^3+\frac{103}{64}X^2-\frac{27}{16}X+1)$

The zeroes of the polynomials $F_k(X)$ are ± 1 and the α_k. This proves the proposition.

Since $T_q = T_2^m$, the traces $\tau_k(q)$ are easily computed recursively from the coefficients of the characteristic polynomial of T_2. It is easy to extend this Proposition a bit further by computing the traces of T_{2^m} for a few $m \geqslant 4$.

For even k we proceed in a different way, which will take us much further. We now have that $S_k(\Gamma_1(4)) = S_k(\Gamma_0(4), 1)$. The Trace formula for T_2 acting on $S_k(\Gamma_0(2), 1)$ is identical to the one given in Theorem (2.2). We will study the space $S_k(\Gamma_0(2), 1)$ since it has smaller dimension. It will be denoted by $S_k(\Gamma_0(2))$.

The theory of newforms of Atkin and Lehner [1, 9] provides us with a decomposition

$$S_k(\Gamma_0(2)) = S_k(\Gamma_0(2))^{\mathrm{new}} \oplus S_k(\Gamma_0(2))^{\mathrm{old}}$$

which is respected by the Hecke operators. The old part is spanned by the forms $f(z)$ and $f(2z)$ where f is a cusp form for the group $\Gamma_0(1) = SL_2(\mathbf{Z})$.

PROPOSITION 6.2. *Let $k \geqslant 4$ be an even integer. We have*

$$\tau_k(q) = \mathrm{Tr}(T_q \text{ on } S_k(SL_2(\mathbf{Z}))) - 2^{k-1}\,\mathrm{Tr}(T_{q/4} \text{ on } S_k(SL_2(\mathbf{Z})))$$
$$+ \begin{cases} \dim S_k(\Gamma_0(2))^{\mathrm{new}}\, q^{k/2-1} & \text{for } m \text{ even,} \\ -q^{k/2-1} & \text{for } m \text{ odd, } k \equiv 0 \pmod 8, \\ q^{k/2-1} & \text{for } m \text{ odd, } k \equiv 2 \pmod 8, \\ 0 & \text{for } m \text{ odd, otherwise,} \end{cases}$$

and

$$\dim S_k(\Gamma_0(2))^{\mathrm{new}} = \left[\frac{k}{12}\right] + \begin{cases} -1 & \text{for } k \equiv 0 \pmod{12}, \\ 0 & \text{for } k \equiv 4 \text{ or } 6 \pmod{12}, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The trace $\tau_k(q)$ is equal to the sum of the traces of T_q acting on the old and new parts. We will discuss these parts separately.

Let λ denote an eigenvalue of T_2 acting on $S_k(SL_2(\mathbf{Z}))$ and let α and β denote the zeroes of the polynomial $X^2-\lambda X+2^{k-1}$. The corresponding eigenspace is also an eigenspace for the Hecke operator T_q with eigenvalue $\alpha^m+\alpha^{m-1}\beta+\cdots+\beta^m$. One checks that the eigenvalues of T_2 acting on $S_k(\Gamma_0(2))^{\text{old}}$ are precisely the α and β for all possible λ. Therefore the trace of T_q acting on $S_k(\Gamma_0(2))^{\text{old}}$ is equal to the sum of the $\alpha^m+\beta^m$ which is easily seen to be equal to $\operatorname{Tr}(T_q \text{ on } S_k(SL_2(\mathbf{Z})))-2^{k-1}\operatorname{Tr}(T_{q/4} \text{ on } S_k(SL_2(\mathbf{Z})))$.

It is easy to see [1, Thm. 3] that the eigenvalues of T_2 acting on $S_k(\Gamma_0(2))^{\text{new}}$ are $\pm 2^{k/2-1}$. One can find the multiplicities of the eigenvalues by subtracting the traces of T_2 for the groups $\Gamma_0(2)$ and $SL_2(\mathbf{Z})$, respectively. The result is

$$\begin{aligned}
\operatorname{Tr}(T_2 \text{ on } S_k(\Gamma_0(2))^{\text{new}}) &= -2^{k/2-1} && \text{for } k\equiv 0 \pmod 8,\\
&= 2^{k/2-1} && \text{for } k\equiv 2 \pmod 8,\\
&= 0 && \text{otherwise.}
\end{aligned}$$

Since T_q acts as $(T_2)^m$ on $S_k(\Gamma_0(2))^{\text{new}}$, we obtain the required result.

The dimension of $S_k(\Gamma_0(2))^{\text{new}}$ is equal to $\dim S_k(\Gamma_0(2))-2\dim S_k(SL_2(\mathbf{Z}))$ and can be computed explicitly using Corollary (2.3). For $k\geqslant 4$, one finds the required result. This proves the Proposition.

So, the only complicated quantity to compute appears to be the trace of T_q acting on $S_k(SL_2(\mathbf{Z}))$. This is very classical. We refer to Koblitz's book [6] and Serre's course [15] for the details.

PROPOSITION 6.3. *Let q be a power of 2; The trace of the Hecke operator T_q acting on the space $S_k(\Gamma_0(4))$ is for even k satisfying $4\leqslant k\leqslant 26$ given as follows*

k	$\operatorname{Trace}(T_q)$	k	$\operatorname{Trace}(T_q)$
4	0	16	$\tau'_{16}(q)\pm q^7$
6	0	18	$\tau'_{18}(q)+q^8$
8	$\pm q^3$	20	$\tau'_{20}(q)+(1\pm 1)\,q^9$
10	q^4	22	$\tau'_{22}(q)+(1\pm 1)\,q^{10}$
12	$\tau'_{12}(q)$	24	$\tau'_{24}(q)+(1\pm 2)\,q^{11}$
14	$(1\pm 1)\,q^6$	26	$\tau'_{26}(q)+(3\pm 2)\,q^{12}$

where for $k=12, 16, 18, 20, 22, 26$ the $\tau'_k(2^m)$ are given by

$$\tau'_k(1) = 2,$$

$$\tau'_k(2) = -24, 216, -528, 456, -288, -48$$

for $k = 12, 16, 18, 20, 22, 26$, *respectively*,

$$\tau'_k(2^{m+1}) = \tau'_k(2^m)\,\tau'_k(2) - 2^{k-1}\tau'_k(2^{m-1})$$

$(m \geqslant 1)$.

For $k = 24$ *we refer the reader to* [6, *Exercise* III.5.6]. *By* $\pm$ *we denote* $(-1)^m$.

Proof. This follows from some standard calculations with modular forms for the group $SL_2(\mathbf{Z})$: For $k = 4, 6, 8, 10, 14$ the spaces $S_k(SL_2(\mathbf{Z}))$ are zero. For $k = 12, 16, 18, 20, 22, 26$ the spaces are one-dimensional. In these cases let λ denote the unique eigenvalue of T_2 and let α and β denote the zeroes of $X^2 - \lambda X + 2^{k-1}$. It is clear that the numbers $\mathrm{Tr}(T_q) - 2^{k-1}\,\mathrm{Tr}(T_{q/4}) = \alpha^m + \beta^m$ satisfy recurrence relations like the ones above. By Proposition (6.2) it remains to show that $\tau'_k(2) = \alpha + \beta =$ Trace T_2 on $S_k(SL_2(\mathbf{Z}))$.

A generator of $S_{12}(SL_2(\mathbf{Z}))$ is the well-known Δ-function

$$\Delta(z) = e^{2\pi iz} \prod_{m=1}^{\infty} (1 - e^{2\pi imz})^{24}$$

$$= \sum_{m=1}^{\infty} \tau(m)\, e^{2\pi imz},$$

where $\tau(m)$ denotes the famous Ramanujan τ-function. We see that $\tau'_{12}(2) = \tau(2) = -24$. Generators for the other one-dimensional spaces can be obtained by multiplying $\Delta(z)$ by suitable Eisenstein series see [6, p. 111] or [15]. It is then trivial to compute the $\tau'_k(2)$ for the other values of k.

The space $S_{24}(SL_2(\mathbf{Z}))$ is two-dimensional. We refer the reader to [6, Exercise III.5.6] for this case. This proves the proposition.

Next we combine Theorems (4.2) and (5.2) with Propositions (6.1) and (6.2) to obtain explicit formulas for the numbers of words A_i in the Melas codes $M(q)$ of a given weight i. We do the same for the numbers of words B_i in the Zetterberg codes $N(q)$. It is a trivial matter to obtain the frequencies of the weights of the quadratic Goppa codes from those of the Melas and Zetterberg codes. We include two small tables (see Tables 6.1 and 6.2). The symbolic manipulation language MACSYMA was of great help in obtaining these formula's. In all tables $\pm$ denotes $(-1)^m$. Ramanujan's τ-function is denoted by τ. The number t_k denotes Trace(α_k^m) as in Proposition (6.1).

TABLE 6.1. Frequencies A_i of Small Weights i in the Melas Codes $M(q)$

$$A_1 = A_2 = A_4 = 0$$
$$A_3 = ((1 \pm 1)/3!)(q-1)$$
$$A_5 = ((q-1)/5!)(q^2 - 14q + 41 \pm (-6q + 30) + qt_7)$$
$$A_6 = ((q-1)/6!)(q^3 - 15q^2 + 65q - 80 \mp q)$$
$$A_7 = ((q-1)/7!)(q^4 - 27q^3 + 296q^2 - 1441q + 2549 \pm (35q^2 - 476q + 1519) + (-15q^2 + 91q)\, t_7 + q^2 t_9)$$
$$A_8 = ((q-1)/8!)(q^5 - 35q^4 + 490q^3 - 3235q^2 + 9604q - 9856 \pm (21q^2 - 140q))$$
$$A_9 = ((q-1)/9!)(q^6 - 44q^5 + 826q^4 - 8652q^3 + 52816q^2 - 174224q + 238545 \pm (-204q^3 + 5628q^2 - 47292q + 122156) + (189q^3 - 2808q^2 + 10038)\, t_7 + (-28q^3 + 204q^2)\, t_9 + q^3 t_{11})$$
$$A_{10} = ((q-1)/10!)(q^7 - 54q^6 + 1266q^5 - 16842q^4 + 135108q^3 - 630291q^2 + 1513539q - 1377792 \pm (-350q^3 + 5565q^2 - 21378q) - (\tau(q) - 2048\tau(q/4))/q^2)$$
$$A_{11} = ((q-1)/11!)(q^8 - 65q^7 + 1860q^6 - 30810q^5 + 327207q^4 - 2298988q^3 + 10400303q^2 - 27394553q + 31839237 \pm (991q^4 - 55440q^3 + 947562q^2 - 6351840q + 14466221) + (-2365q^4 + 62865q^3 - 537042q^2 + 1467290q)\, t_7 + (594q^4 - 10120q^3 + 41778q^2)\, t_9 + (-45q^4 + 385q)\, t_{11} + q^4 t_{13})$$
$$A_{12} = ((q-1)/12!)(q^9 - 77q^8 + 2640q^7 - 53130q^6 + 697158q^5 - 6210820q^4 + 37216619q^3 - 140826290q^2 + 293391846q - 244721664 \pm (5620q^4 - 156310q^3 + 1403787q^2 - 4054028q) + (55q - 506)((\tau(q) - 2048\tau(q/4))/q^2))$$

TABLE 6.2. Frequencies B_i of Small Weights i in the Zetterberg Codes $N(q)$

$$B_1 = B_2 = B_4 = 0$$
$$B_3 = ((1 \mp 1)/3!)(q+1)$$
$$B_5 = ((q+1)/5!)(q^2 - 6q + 11 \pm (6q - 10) - qt_7)$$
$$B_6 = (q(q+1)/6!)(q^2 - 5q + 5 \mp 1)$$
$$B_7 = ((q+1)/7!)(q^4 - 15q^3 + 84q^2 - 239q + 309 \pm (-35q^2 + 224q - 259) + (15q^2 - 49q)\, t_7 - q^2 t_9)$$
$$B_8 = (q(q-4)(q+1)/8!)(q^3 - 17q^2 + 86q - 91 \pm 21)$$
$$B_9 = ((q+1)/9!)(q^6 - 28q^5 + 322q^4 - 1932q^3 + 6784q^2 - 14776q + 16407 \pm (204q^3 - 3108q^2 + 13020q - 12788) + (-189q^3 + 1728q^2 - 3486q)\, t_7 + (28q^3 - 132q^2)\, t_9 - q^3 t_{11})$$
$$B_{10} = (q(q+1)/10!)(q^6 - 36q^5 + 546q^4 - 4494q^3 + 20448q^2 - 45309q + 34299 \pm (-350q^2 + 3675q - 8778) - (\tau(q) - 2048\tau(q/4))/q^3)$$
$$B_{11} = ((q+1)/11!)(q^8 - 45q^7 + 870q^6 - 9450q^5 + 62679q^4 - 263572q^3 + 734537q^2 - 1384967q + 1411785 \pm (-991q^4 + 33000q^3 - 328482q^2 + 1149720q - 1029061) + (2365q^4 - 42075q^3 + 228162q^2 - 363110q)\, t_7 + (-594q^4 + 7040q^3 - 19338q^2)\, t_9 + (45q^4 - 275q^3)\, t_{11} - q^4 t_{13})$$
$$B_{12} = (q(q+1)/12!)(q^8 - 55q^7 + 1320q^6 - 18150q^5 + 158598q^4 - 908908q^3 + 3260411q^2 - 6269670q + 4444506 \pm (5620q^3 - 110110q^2 + 669207q - 1232132) + (55q - 374)((\tau(q) - 2048\tau(q/4))/q^3)$$

Using the formulas in Remarks (4.5) and (5.5) one can easily deduce the frequencies of the small weights of the quadratic Goppa codes from Tables 6.1 and 6.2. Note once more that one only needs the *even* weights and that in the resulting expressions for the weight distributions of the quadratic Goppa codes only the traces of Hecke operators acting on modular forms for the *full* modular group $SL_2(\mathbf{Z})$ occur.

REFERENCES

1. A. O. L. ATKIN AND J. LEHNER, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.
2. Z. BOREVIC AND I. ŠAFAREVIČ, "Number Theory," Academic Press, London/New York, 1966.
3. H. COHEN, Trace des opérateurs de Hecke sur $\Gamma_0(N)$, *in* "Séminaire de Théorie des Nombres," exp. no. 4, Bordeaux, 1976–1977.
4. P. DELIGNE, La conjecture de Weil, I, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.
5. A. DÜR, The weight distribution of double-error-correcting Goppa codes, *in* "Lecture Notes Computer in Science," Vol. 307, pp. 29–42, Springer-Verlag, New York, 1987.
6. N. KOBLITZ, Introduction to elliptic curves and modular forms, *in* "Graduate Texts in Math.," Vol. 97, Springer-Verlag, New York, 1984.
7. G. LACHAUD AND J. WOLFMANN, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2, *C. R. Acad. Sci. Paris* **305** (1987), 881–883.
8. G. LACHAUD AND J. WOLFMANN, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Trans. Inform. Theory*, to appear.
9. S. LANG, Introduction to Modular Forms, *in* "Grundlehren Math. Wiss." Vol. 222, Springer-Verlag, New York, 1976.
10. W. W. LI, Newforms and functional equations, *Math. Ann.* **212** (1975), 285–315.
11. J. MACWILLIAMS AND J. SEERY, The weight distributions of some minimal cyclic codes, *IEEE Trans. Inform. Theory* **27** (1981), 796–806.
12. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1983.
13. J. OESTERLÉ, "Sur la trace des opérateurs de Hecke," Thèse de 3° cycle, Orsay, 1977.
14. R. SCHOOF, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), 183–211.
15. J.-P. SERRE, "Cours d'arithmétique," Presses Univ. de France, Paris, 1970.
16. J. SILVERMAN, The Arithmetic of elliptic curves, *in* "Graduate Texts in Math.," Vol. 106, Springer-Verlag, New York, 1986.
17. K. K. TZENG AND K. ZIMMERMAN, On extending Goppa codes to cyclic codes, *IEEE Trans. Inform. Theory* **21** (1975), 712–716.
18. D. B. ZAGIER, Correction to "The Eichler-Selberg trace formula on $SL_2(\mathbf{Z})$," *in* Lecture Notes in Math., Vol. 627, pp. 171–173, Springer-Verlag, New York, 1977.