1998

Lee weights of Z/4Z-codes from elliptic curves

José Felipe Voloch
University of Canterbury, felipe.voloch@canterbury.ac.nz

Judy L. Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

Published in Codes, Curves, and Signals: Common Threads in Communications (A. Vardy, ed.),
Boston: Kluwer Academic Publishers. (1998) pp. 53-62.

LEE WEIGHTS OF $\mathbb{Z}/4\mathbb{Z}$-CODES FROM ELLIPTIC CURVES

JOSÉ FELIPE VOLOCH AND JUDY L. WALKER

Abstract. In [15], the second author defined algebraic geometric codes over rings. This definition was motivated by two recent trends in coding theory: the study of algebraic geometric codes over finite fields, and the study of codes over rings. In that paper, many of the basic parameters of these new codes were computed. However, the Lee weight, which is very important for codes over the ring $\mathbb{Z}/4\mathbb{Z}$, was not considered. In [14], this weight measure, as well as the more general Euclidean weight for codes over $\mathbb{Z}/p^l\mathbb{Z}$, is considered for algebraic geometric codes arising from elliptic curves.

In this paper, we will focus on the specific case of codes over $\mathbb{Z}/4\mathbb{Z}$ and we will show how everything works in an explicit example.

1. Introduction

The study of linear codes over finite rings has received much attention lately. This is due in large part to the paper of Hammons, et al. ([2]), in which it is shown that certain nonlinear binary codes are actually the images of linear codes over the ring $\mathbb{Z}/4\mathbb{Z}$ under the Gray map. This idea has prompted many authors (see [1] or [11], for example) to consider the question of how to construct linear codes over $\mathbb{Z}/4\mathbb{Z}$, with the hope that these codes might have good binary images under the Gray map.

In [15], a new method of constructing linear codes over $\mathbb{Z}/4\mathbb{Z}$ is proposed. The idea there is to generalize the construction of algebraic geometric codes over finite fields ([12], [13]) to allow the use of a local Artin ring to play the role of the finite field. In that paper, the length, dimension (rank), and minimum Hamming distance of these new codes are computed. However, the crucial Lee weight, which is the same as the Hamming weight of their binary images under the Gray map, is not treated there.

It turns out that computing the minimum Lee weight of an algebraic geometric code is very difficult. In [16], it is shown how the notion of Lee weight for codes over $\mathbb{Z}/4\mathbb{Z}$ generalizes to a weight measure called Euclidean weight for codes over $\mathbb{Z}/p^l\mathbb{Z}$, where p is any prime and $l \geq 1$ is an integer. Also in that paper, the minimum Euclidean weight of an algebraic geometric code over $\mathbb{Z}/p^l\mathbb{Z}$ is expressed in terms of an exponential sum.

In [14], a bound on this sum is found in the special case that the curve over which the code is defined is a certain type of elliptic curve. In this paper, we will

Date: December 21, 1997.

1991 *Mathematics Subject Classification.* Primary 94B27; Secondary 11T71, 11G07.

Key words and phrases. Codes, Artin rings, Exponential sums, Elliptic curves.

The first author was supported in part by NSA Grant #MDA904-97-1-0037 and TARP Grant #ARP-006.

The second author was supported in part by NSF Grant #DMS-9709388.

To Dick Blahut, in honor of his sixtieth birthday.

examine in detail the case of [14] where $p = l = 2$, so that the code in question is a code over $\mathbb{Z}/4\mathbb{Z}$. To illustrate our results, we work a specific example in detail.

2. Galois and Witt rings, and Algebraic geometric codes over them

A common method of constructing long codes over small fields is to construct a code over an extension field and then consider the trace code. A similar approach can be taken to construct codes over the ring $\mathbb{Z}/4\mathbb{Z}$ by first constructing codes over a *Galois ring* $GR(4, m)$, and then considering the trace code. Recall ([2]) that the Galois ring $GR(4, m)$ is simply $(\mathbb{Z}/4\mathbb{Z})[x]/(f)$, where $f \in (\mathbb{Z}/4\mathbb{Z})[x]$ is monic, irreducible, and a divisor of the polynomial $x^{2^m-1} - 1$. More generally, the Galois ring $GR(p^l, m)$ is $(\mathbb{Z}/p^l\mathbb{Z})[x]/(f)$, where $f \in (\mathbb{Z}/p^l\mathbb{Z})[x]$ is monic and irreducible and divides the polynomial $x^{p^m-1} - 1$. Notice that $GR(p^l, 1) \simeq \mathbb{Z}/p^l\mathbb{Z}$. Recall that the *Teichmüller set* of $GR(p^l, m)$ is the multiplicative lifting of the field $\mathbb{F}_{p^m}$ living inside $GR(p^l, m)$.

It is often more convenient to think of the ring $GR(4, m)$ as the ring $W_2(\mathbb{F}_{2^m})$ of 2-dimensional *Witt vectors* over the field $\mathbb{F}_{2^m}$. As a set, this ring looks like vectors of length 2 with coordinates in $\mathbb{F}_{2^m}$, and the operations are given as follows:

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1 + a_0 b_0)$$
$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0, a_0^2 b_1 + b_0^2 a_1)$$

This ring may be thought of as the quotient modulo 4 of $W(\mathbb{F}_{2^m})$, the ring of infinite length Witt vectors over $\mathbb{F}_{2^m}$ (see [5]). Also, one can consider Witt rings over fields of characteristic other than 2, or of finite lengths other than 2.

Notice that the map

$$W_2(\mathbb{F}_2) \to \mathbb{Z}/4\mathbb{Z} \tag{2.1}$$

given by

$$\begin{aligned}(0,0) &\mapsto 0\\ (1,0) &\mapsto 1\\ (0,1) &\mapsto 2\\ (1,1) &\mapsto 3\end{aligned}$$

is an isomorphism of rings. More generally, $W_l(\mathbb{F}_p) \simeq \mathbb{Z}/p^l\mathbb{Z}$ for any prime p and any positive integer l. Similarly, $W_2(\mathbb{F}_{2^m}) \simeq GR(4, m)$ for all m and more generally $W_l(\mathbb{F}_{p^m}) \simeq GR(p^l, m)$. The Teichmüller set of $GR(p^l, m)$ corresponds to the vectors in $W_l(\mathbb{F}_{p^m})$ which are zero beyond the first coordinate.

The map $F : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_{p^m})$ given by $(a_0, a_1, \dots, a_{l-1}) \mapsto (a_0^p, a_1^p, \dots, a_{l-1}^p)$ is an additive endomorphism of order m. The trace map $T : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_p) \simeq \mathbb{Z}/p^l\mathbb{Z}$ is given by $T(a) = F(a) + F^2(a) + \cdots + F^{m-1}(a)$.

The generalization of algebraic geometric codes which we will describe below will make sense for any *local Artin* ring A. Recall that a local ring is one with only one maximal ideal. $GR(p^l, m)$ is local with its unique maximal ideal being the one generated by p. In $W_l(\mathbb{F}_{p^m})$, this ideal consists of the elements having zeros in the first coordinate. An Artin ring is one in which every descending chain of ideals is eventually stable; since any finite ring obviously satisfies this property, $GR(p^l, m) \simeq W_l(\mathbb{F}_{p^m})$ is an Artin ring.

Next, we describe how to generalize the construction of algebraic geometric codes over finite fields ([13], [12]) to give codes over local Artin rings such as $W_l(\mathbb{F}_{p^m}) \simeq GR(p^l, m)$. The set-up for the generalized construction is as follows:

Let A be a local Artin ring, and let $\mathbf{X}$ be a curve defined over A (i.e., a connected irreducible scheme over Spec A which is smooth and of relative dimension one). One may think of $\mathbf{X}$ as being defined by polynomial equations with coefficients in A. In this case, A-points on $\mathbf{X}$ are solutions in A to the equations defining $\mathbf{X}$. Letting $\mathfrak{m}$ be the maximal ideal of A, we get a curve X over the field $A/\mathfrak{m}$ by reducing the equations defining $\mathbf{X}$ modulo $\mathfrak{m}$. By reducing the coordinates of an A-point of $\mathbf{X}$ modulo $\mathfrak{m}$, we get a $A/\mathfrak{m}$-rational point of X. We say two A-points of $\mathbf{X}$ are *disjoint* if their reductions modulo $\mathfrak{m}$ give two distinct $A/\mathfrak{m}$-rational points of X. Let $\mathcal{Z}$ be a set of disjoint A-points on $\mathbf{X}$. Associated to a line bundle $\mathcal{L}$ on $\mathbf{X}$ is an A-module $\Gamma(\mathbf{X}, \mathcal{L})$ of rational functions on $\mathbf{X}$, and $\mathcal{L}$ may easily be chosen so that it makes sense to evaluate the functions in $\Gamma(\mathbf{X}, \mathcal{L})$ at the points of $\mathcal{Z}$.

With A, $\mathbf{X}$, $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$, and $\mathcal{L}$ as above, the algebraic geometric code $C_A(\mathbf{X}, \mathcal{Z}, \mathcal{L})$ is defined to be the image of the evaluation map

$$\begin{aligned} \Gamma(\mathbf{X}, \mathcal{L}) &\to A^n \\ f &\mapsto (f(Z_1), \ldots, f(Z_n)) \end{aligned}$$

Some of the properties of these codes are summarized in the following theorem; see [15] for proofs.

Theorem 2.1. *Let $\mathbf{X}$, X, $\mathcal{L}$, and $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ be as above. Let g denote the genus of X, and suppose $2g - 2 < \deg \mathcal{L} < n$. Set $C = C(\mathbf{X}, \mathcal{Z}, \mathcal{L})$. Then C is a linear code of length n over A, and is free as an A-module. The dimension (rank) of C is $k = \deg \mathcal{L} + 1 - g$, and the minimum Hamming distance of C is at least $n - \deg \mathcal{L}$. Further, under the additional assumption that A is Gorenstein, the class of algebraic geometric codes is closed under taking duals. In particular, there exists a line bundle $\mathcal{E}$ such that $C^\perp = C(\mathbf{X}, \mathcal{Z}, \mathcal{E})$.*

Remark 2.2. The rings $W_l(\mathbb{F}_p) \simeq \mathbb{Z}/p^l\mathbb{Z}$ and $W_l(\mathbb{F}_{p^m}) \simeq GR(p^l, m)$ are Gorenstein, so everything in the above theorem applies to these rings in particular.

In practice, one is usually most interested in codes over the ring $\mathbb{Z}/4\mathbb{Z}$. Such a code can be obtained in two ways using the construction above. First, one can simply set $A = \mathbb{Z}/4\mathbb{Z}$ and construct an algebraic geometric code over $\mathbb{Z}/4\mathbb{Z}$ directly. The drawback of this is that the codes obtained in this manner will be short. A second method is to set $A = W_2(\mathbb{F}_{2^m}) = GR(4, m)$, construct an algebraic geometric code over A, and then apply the trace map $T : A \to \mathbb{Z}/4\mathbb{Z}$ coordinatewise to the code to get a code over $\mathbb{Z}/4\mathbb{Z}$. Since $T : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ is the identity map, we need only consider the second of these two constructions.

3. Lee weight

Theorem 2.1 gives the length, dimension, and minimum Hamming distance of an algebraic geometric code over a ring. However, for codes over $\mathbb{Z}/4\mathbb{Z}$, the relevant weight measure is the Lee weight. The reason for this is that the Gray map is an isometry

$$((\mathbb{Z}/4\mathbb{Z})^n, \text{Lee weight}) \to ((\mathbb{F}_2)^{2n}, \text{Hamming weight})$$

so that the minimum Hamming weight of the binary image of a $\mathbb{Z}/4\mathbb{Z}$-code is the Lee weight of the code over $\mathbb{Z}/4\mathbb{Z}$. Our goal is to find the minimum Lee weight of (trace codes of) algebraic geometric codes over $\mathbb{Z}/4\mathbb{Z}$.

Recall that the Lee weight is defined on $\mathbb{Z}/4\mathbb{Z}$ by $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, and $w_L(2) = 2$. The Lee weight of a vector in $(\mathbb{Z}/4\mathbb{Z})^n$ is the sum of the Lee weights of the coordinates of the vector. Our first task is to find an "algebraic" expression for Lee weight, so that it will be easier to study.

Notice that for each $x \in \mathbb{Z}/4\mathbb{Z}$, $w_L(x)$ is exactly half the square of the distance in the complex plane between $1 = i^0$ and i^x, where $i = \sqrt{-1}$. Using a little trigonometry, we see that $w_L(x) = 1 - \cos(\frac{\pi}{2}x) = 1 - \mathrm{Re}(e^{\pi i x/2})$.

Therefore, for a vector $\mathbf{x} = (x_1, \ldots, x_n)$ in $(\mathbb{Z}/4\mathbb{Z})^n$, we have

$$\begin{aligned} w_L(\mathbf{x}) &= \sum_{j=1}^{n} (1 - \mathrm{Re}(e^{\pi i x_j/2})) \\ &\geq n - \left| \sum_{j=1}^{n} e^{\pi i x_j/2} \right|. \end{aligned}$$

If the vector $\mathbf{x}$ is actually a codeword in a trace code of an algebraic geometric code, then we have

$$\mathbf{x} = (T(f(Z_1)), \ldots, T(f(Z_n)))$$

where $Z_1, \ldots, Z_n$ are disjoint A-points on some curve $\mathbf{X}$ over $A = W_2(\mathbb{F}_{2^m}) \simeq GR(4, m)$ and f is a global section of a line bundle on $\mathbf{X}$. In this case, we have

$$w_L(\mathbf{x}) \geq n - \left| \sum_{j=1}^{n} e^{\pi i T(f(Z_j))/2} \right|$$

so we see that finding a lower bound on the minimum Lee weight of the trace code of an algebraic geometric code amounts to finding an upper bound on the modulus of an exponential sum of the form

$$\sum_{j=1}^{n} e^{\pi i T(f(Z_j))/2}. \tag{3.1}$$

In the case of the projective line, sums similar to this have received much attention recently; see [4] and [6]. In both cases, the A-points on $\mathbb{P}^1$ over which the sum is taken are not arbitrary but instead are the Teichmüller points of A. An analogous concept exists for certain elliptic curves over rings, and it is here where we will focus our attention for the remainder of this paper.

4. Ordinary Elliptic Curves and Canonical Lifts

An elliptic curve over a field of characteristic 2 is called *ordinary* if its group of 2-torsion points has order 2. (Otherwise, its group of 2-torsion points is trivial, and the curve is called *supersingular.*) Every elliptic curve has an isogeny called the *Frobenius*; on points, the Frobenius takes (x, y) to (x^2, y^2). A special case of Serre-Tate theory (see [7] or [3]) implies that every ordinary elliptic curve E over a finite field k of characteristic 2 has a *canonical lift* to an elliptic curve over the ring of infinite length Witt vectors $W(k)$. By reducing modulo 4, we get that E has a canonical lift to an elliptic curve $\mathbf{E}$ over $W_2(k)$. The existence of a canonical lift is in fact equivalent to the existence of an injective homomorphism $\tau : E(k) \to$

$\mathbf{E}(W_2(k))$, called the *elliptic Teichmüller lift.* $W_2(k)$-points Z on $\mathbf{E}$ which are of the form $Z = \tau(P)$ for some k-rational point P on E are the analogies of the Teichmüller points on $\mathbb{P}^1$.

Our first question, then, is: How can we tell if an elliptic curve $\mathbf{E}$ over $W_2(k)$ is actually the canonical lift of an ordinary elliptic curve over k? The answer to this question is found in the next proposition, which is true for any characteristic $p > 0$ and is proven in [14]. Before we can state it, however, we need one more definition. Let $\mathbf{X}$ be a scheme over $W_l(k)$, where k is a field and $l \geq 0$. The *Greenberg transform* $G(\mathbf{X})$ is the variety over k formed by writing out the equations for $\mathbf{X}$ in terms of their Witt components. For example, if $\mathbf{X}$ is the elliptic curve over $W_2(\mathbb{F}_2)$ defined by the equation $\mathbf{y}^2 + \mathbf{x}\mathbf{y} = \mathbf{x}^3 + 1$, then $G(\mathbf{X})$ is the variety over $\mathbb{F}_2$ defined by the equations $y_0^2 + x_0y_0 = x_0^3 + 1$ and $x_0y_0^3 + x_0^2y_1 + x_1y_0^2 = x_0^3 + x_0^4x_1$. Notice that the k-rational points of $G(\mathbf{X})$ are in one-to-one correspondence with the $W_l(k)$-points of $\mathbf{X}$.

Proposition 4.1. *Let k be a perfect field of characteristic $p > 0$ and E/k an ordinary elliptic curve. If $\mathbf{E}$ is the canonical lift of E to $W_2(k)$, then* $\deg x_1 < 3p, \deg y_1 < 4p$. *Conversely, let $\mathbf{E}$ be any elliptic curve defined over $W_2(k)$ with reduction E. Assume that the projection given by reduction from $G(\mathbf{E})$ to E admits a section τ in the category of k-schemes over $E \setminus \{O\}$ (where O is the origin for the group law on E) given by $(x_0, y_0) \mapsto (\mathbf{x}, \mathbf{y}) = ((x_0, x_1), (y_0, y_1))$ where x_1, y_1 are regular away from O and satisfy* $\deg x_1 < 3p, \deg y_1 < 4p$. *Then τ is regular at O, $\mathbf{E}$ is the the canonical lift of E and τ is the elliptic Teichmüller lift.*

5. A simplification in the case of characteristic 2

Let k be a finite field of characteristic 2 and let E be the elliptic curve over k defined by the Weierstrass equation $y^2 + xy = x^3 + a$, for some $a \in k$. E is the reduction modulo 2 of the curve $\mathbf{E}$ over $W_2(k)$ with equation $\mathbf{y}^2 + \mathbf{x}\mathbf{y} = \mathbf{x}^3 + (a, a^2)$, and it is easy to check that the map $\tau : E(k) \to \mathbf{E}(W_2(k))$ given by $(x_0, y_0) \mapsto ((x_0, a), (y_0, (x_0^2 + x_0)y_0 + x_0^3 + ax_0^2 + a))$ satisfies the hypotheses of Proposition 4.1. Therefore, we know that $\mathbf{E}$ is the canonical lift of E and τ is the elliptic Teichmüller lift on points.

For an integer $r \geq 1$, we may consider the line bundle $\mathcal{L} = \mathcal{O}_{\mathbf{E}}(r\mathbf{O})$ on $\mathbf{E}$. Global sections of this line bundle must have their only pole at $\mathbf{O}$ and that pole must have order at most r. Since $\mathbf{x}$ has a pole of order 2 at $\mathbf{O}$ and $\mathbf{y}$ has a pole of order 3 at $\mathbf{O}$, this means that elements of $\Gamma(\mathbf{E}, \mathcal{L})$ are of the form $A + B\mathbf{y}$, where A and B are polynomials in $\mathbf{x}$ of degrees at most $\lfloor \frac{r}{2} \rfloor$ and $\lfloor \frac{r-3}{2} \rfloor$ respectively. Using the map τ above, we see that for $P \in E(k)$ and $f \in \Gamma(\mathbf{E}, \mathcal{L})$, we have

$$f(\tau(P)) = (f_0(P), f_1(P))$$

as a Witt vector, where f_0 and f_1 are rational functions on E which have poles only at O and those poles are of orders at most r and $2r + 1$ respectively. In other words, $f_0 \in \Gamma(E, \mathcal{O}_E(rO))$ and $f_1 \in \Gamma(E, \mathcal{O}_E((2r + 1)O))$.

Thus, for this particular curve $\mathbf{E}$ and a line bundle of the form $\mathcal{L} = \mathcal{O}_{\mathbf{E}}(r\mathbf{O})$, the sum 3.1 is the same as the sum

$$\sum_{j=1}^{n} e^{\pi i T(f_0(P), f_1(P))/2} \tag{5.1}$$

Notice that this sum no longer involves $\mathbf{E}$, but instead is expressed solely in terms of data on the curve E, which is defined over the field k.

Further, we can actually say something much stronger. It is true that *every* ordinary elliptic curve over a field k of characteristic 2 is is isomorphic over $\bar{k}$ to a curve with Weierstrass equation $y^2 + xy = x^3 + a$; see [10], Propositions A.1.1 and A.1.2. Since the degree of a line bundle is invariant under base change, this means that for every ordinary elliptic curve in characteristic 2, finding a bound on a sum of the form 3.1 is equivalent to finding a bound on a sum of the form 5.1.

6. The bound

We need one more result in order to bound the modulus of our sums 3.1 and 5.1. This result can be proven much more generally (see [14]), but we will state it in only the specific case we need here. First, we set up some notation.

Let E be an elliptic curve over the field $\mathbb{F}_{2^m}$, and let K denote the field of rational functions on E. Let $f_0, f_1 \in K$, and assume $f_i \in \Gamma(E, \mathcal{O}_E(r_i O))$ where O is the origin of E and $r_i \geq 1$ is an integer for $i = 0, 1$. Set $\mathbf{f} = (f_0, f_1) \in W_2(K)$. Let $\mathcal{P} = E(k) \backslash \{O\}$, and for $P \in \mathcal{P}$, define $\mathbf{f}(P) = (f_0(P), f_1(P)) \in W_2(\mathbb{F}_{2^m})$. Let F be the additive endomorphism defined in Section 2, and let $T : W_2(\mathbb{F}_{2^m}) \to W_2(\mathbb{F}_2) \simeq \mathbb{Z}/4\mathbb{Z}$ be the trace map which was also defined in that section.

Theorem 6.1. *With notation as above, assume that* $\mathbf{f}$ *is not of the form* $\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + \mathbf{c}$ *for any* $\mathbf{g} \in W_2(K)$ *and* $\mathbf{c} \in W_2(\mathbb{F}_{2^m})$*. Then*

$$\left| \sum_{P \in \mathcal{P}} e^{\pi i T(\mathbf{f}(P))/2} \right| \leq (1 + \max\{2r_0, r_1\}) 2^{\frac{m}{2}}.$$

A proof of a more general version of this theorem can be found in [14], and most of the steps can actually be found in either [8] or [9]. The basic idea is to consider the degree of the Artin L-function of the Artin-Schreier-Witt cover of $\mathbf{E}$ defined by $F(\mathbf{t}) - \mathbf{t} = \mathbf{f}$. Notice that if $\mathbf{f}$ is of the excluded form, then $T(\mathbf{f}(P))$ would be a constant vector.

By combining this result with the argument in Section 5 above, we get the following result.

Theorem 6.2. *Let* $\mathbf{E}$ *be an elliptic curve over* $W_2(\mathbb{F}_{2^m})$ *which is the canonical lift of an elliptic curve* E *over* $\mathbb{F}_{2^m}$*. Let* $\mathcal{Z} = \{\tau(P) \,|\, P \in E(\mathbb{F}_{2^m}) \setminus \{O\}$*, where* $\tau : E(\mathbb{F}_{2^m}) \to \mathbf{E}(W_2(\mathbb{F}_{2^m}))$ *is the elliptic Teichmüller lift. Let* $f \in \Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(r\mathbf{O}))$ *for some integer* $r \geq 1$*. Then*

$$\left| \sum_{Z \in \mathcal{Z}} e^{\pi i T(f(Z))/2} \right| \leq (2r + 2) 2^{\frac{m}{2}},$$

unless $f \circ \tau \in W_2(\mathbb{F}_{2^m})$ *is of the form* $F(\mathbf{g}) - \mathbf{g} + \mathbf{c}$ *for some Witt vector* $\mathbf{g}$ *of rational functions on* E *and some* $\mathbf{c} \in W_2(\mathbb{F}_{2^m})$*.*

We can now translate this back into a statement about codes.

Theorem 6.3. *Let* $\mathbf{E}$ *and* $\mathcal{Z}$ *be as above, and let* $\mathcal{L} = \mathcal{O}_{\mathbf{E}}(r\mathbf{O})$ *for some integer* $r \geq 1$*. Set* $C = C_{\mathbb{Z}/4\mathbb{Z}}(\mathbf{E}, \mathcal{Z}, \mathcal{L})$*. Then the minimum Lee weight of the code* $T(C)$ *satisfies*

$$w_L(T(C)) \geq n - (2r + 2) 2^{\frac{m-3}{2}},$$

where $n = \#\mathcal{Z}$ *is the length of* C*.*

Proof. Let f be a global section of $\mathcal{L}$. If $f \circ \tau$ is not of the form excluded by Theorem 6.2, then the Lee weight of the trace of the codeword corresponding to f satisfies the desired inequality by that theorem. Otherwise, the trace of the codeword corresponding to f is constant, so its Lee weight is either 0, n, or $2n$. $\square$

7. An Example

Let $\mathbf{E}$ be the curve over $W_2(\bar{\mathbb{F}}_2)$ defined by the equation $\mathbf{y}^2+\mathbf{xy} = \mathbf{x}^3-\mathbf{x}^2-2\mathbf{x}-1$, so that its reduction modulo 2 is the curve E over $\bar{\mathbb{F}}_2$ defined by the equation $y^2 + xy = x^3 + x^2 + 1$. (Although E is isomorphic over $\bar{\mathbb{F}}_2$ to the curve with equation $y^2 + xy = x^3 + 1$, we work with E rather than this latter curve because E has more $\mathbb{F}_8$-rational points.) It is easy to check that if (x_0, y_0) is a point on E, then $((x_0, 1), (y_0, x_0^2(1 + y_0)))$ is a point on $\mathbf{E}$. Further, the map $\tau : E(\bar{\mathbb{F}}_2) \to \mathbf{E}(W_2(\bar{\mathbb{F}}_2))$ given by $(x_0, y_0) \mapsto ((x_0, 1), (y_0, x_0^2(1 + y_0)))$ satisfies the hypotheses of Proposition 4.1 above, so we can conclude that $\mathbf{E}$ is the canonical lift of E. We will construct a code over $W_2(\mathbb{F}_8)$ using $\mathbf{E}$. Applying the trace map will give us a code over $\mathbb{Z}/4\mathbb{Z}$, and applying the Gray map will give us a binary code.

Write $\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1)$. In addition to the origin O, there are 13 finite $\mathbb{F}_8$-rational points on E. They are the elements of the set:

$$\begin{aligned}\mathcal{P} = \{&(0,1), (t^2, 1+t), (t^2, 1+t+t^2), (t, 1+t^2), (t, 1+t+t^2),\\ &(t+t^2, 1+t^2), (t+t^2, 1+t), (1+t^2, 0), (1+t^2, 1+t^2),\\ &(1+t, 0), (1+t, 1+t), (1+t+t^2, 0), (1+t+t^2, 1+t+t^2)\}\end{aligned}$$

Applying the map τ described above, one gets the origin $\mathbf{O}$ of $\mathbf{E}$ and the following thirteen points of $\mathbf{E}$ defined over $W_2(\mathbb{F}_8)$:

$$\begin{aligned}\mathcal{Z} = \{&((0,1),(1,0)), ((t^2,1),(1+t,1+t+t^2)), ((t^2,1),(1+t+t^2,t)),\\ &((t,1),(1+t^2,t+t^2)), ((t,1),(1+t+t^2,1+t^2)),\\ &((t+t^2,1),(1+t^2,1+t)), ((t+t^2,1),(1+t,t^2)),\\ &((1+t^2,1),(0,1+t+t^2)), ((1+t^2,1),(1+t^2,1)),\\ &((1+t,1),(0,1+t^2)), ((1+t,1),(1+t,1)),\\ &((1+t+t^2,1),(0,1+t)), ((1+t+t^2,1),(1+t+t^2,1))\}\end{aligned}$$

We wish to consider the code $C = C_{W_2(\mathbb{F}_8)}(\mathbf{E}, \mathcal{Z}, \mathcal{L})$, where $\mathcal{L} = \mathcal{O}_{\mathbf{E}}(3\mathbf{O})$. The degree of $\mathcal{L}$ is 3, so by the Riemann-Roch theorem [15], the rank of the $W_2(\mathbb{F}_8)$-module $\Gamma(\mathbf{E}, \mathcal{L})$ is 3. It is easy to check that $\{1, \mathbf{x}, \mathbf{y}\}$ is a basis for this module, so a (3×13) generator matrix for C is constructed simply by evaluating these three functions at each of the thirteen points in $\mathcal{Z}$.

In fact, we are interested in the trace code $T(C)$ of C, which will be a code over $W_2(\mathbb{F}_2) = \mathbb{Z}/4\mathbb{Z}$. By a ring-version of Theorem VIII.1.6 of [12], we know that the rank of $T(C)$ (as a $\mathbb{Z}/4\mathbb{Z}$-module) is at most 7; we will show that it is exactly 7.

Since $\{1, t, t^2\}$ is a basis for $W_2(\mathbb{F}_8)$ as a $W_2(\mathbb{F}_2)$-module, we know that

$$\{1, t, t^2, \mathbf{x}, t\mathbf{x}, t^2\mathbf{x}, \mathbf{y}, t\mathbf{y}, t^2\mathbf{y}\}$$

is a basis for $\Gamma(\mathbf{E}, \mathcal{L})$ as a $W_2(\mathbb{F}_2)$-module. Some subset of this basis, when evaluated at the points in $\mathcal{Z}$, will give us a set of codewords whose traces form a basis for the trace code $T(C)$. Since $T(1)$, $T(t)$, and $T(t^2)$ are all proportional, we can throw away t and t^2, and look at the 7×13 matrix whose rows are

$(T(f(Z_1)), \ldots, T(f(Z_{13})))$, where $Z_1, \ldots, Z_{13}$ are the points in $\mathcal{Z}$ and f runs over the set $\{1, \mathbf{x}, t\mathbf{x}, t^2\mathbf{x}, \mathbf{y}, t\mathbf{y}, t^2\mathbf{y}\}$. If this matrix has full rank (7), then it is the generator matrix for $T(C)$.

The matrix described above works out to be (after replacing elements of $W_2(\mathbb{F}_2)$ with their usual representatives in the ring $\mathbb{Z}/4\mathbb{Z}$, as given in 2.1):

$$\begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 1 & 1 & 2 & 2 & 1 & 1 & 3 & 3 & 2 & 2 & 1 & 1 \\ 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 3 & 3 \\ 3 & 3 & 1 & 1 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 2 & 3 \\ 2 & 0 & 3 & 1 & 1 & 1 & 2 & 2 & 3 & 0 & 2 & 2 & 1 \\ 2 & 1 & 1 & 2 & 1 & 0 & 3 & 0 & 2 & 2 & 1 & 2 & 3 \end{pmatrix}$$

Since the submatrix consisting of the last 7 columns of this matrix has determinant $3 \pmod 4$, this is indeed a generator matrix for the trace code.

By Theorem 6.3, the minimum Lee weight of the code with the above generator matrix is at least 5. One can check that in fact it is exactly 5. By appending a check digit which is the sum of the first three coordinates, we get a code over $\mathbb{Z}/4\mathbb{Z}$ of length 14, rank 7, and minimum Lee weight 6. The generator matrix is:

$$\begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 2 \\ 0 & 1 & 1 & 2 & 2 & 1 & 1 & 3 & 3 & 2 & 2 & 1 & 1 & 2 \\ 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 3 & 3 & 0 \\ 3 & 3 & 1 & 1 & 3 & 3 & 1 & 2 & 3 & 2 & 3 & 2 & 3 & 3 \\ 2 & 0 & 3 & 1 & 1 & 1 & 2 & 2 & 3 & 0 & 2 & 2 & 1 & 1 \\ 2 & 1 & 1 & 2 & 1 & 0 & 3 & 0 & 2 & 2 & 1 & 2 & 3 & 0 \end{pmatrix}$$

Applying the Gray map gives a binary code of length 28 with $2^{14} = 16384$ codewords and minimum Hamming distance 6. The best code with this length and number of codewords has minimum Hamming distance 7.

It is interesting to note that the first four rows and the odd-numbered columns of the generator matrix above define the $[7, 4]$ Hamming code over $\mathbb{Z}/4\mathbb{Z}$ (see [2]). Since only the functions 1 and $\mathbf{x}$ are used here, this gives a construction of this code as a trace code of an algebraic geometric code over $\mathbb{P}^1$. For a more direct construction of the $[7, 4]$ Hamming code over $\mathbb{Z}/4\mathbb{Z}$ as an algebraic geometric code, see [17].

References

1. A. R. Calderbank and G. M. McGuire, *Construction of a* $(64, 2^{37}, 12)$ *code via Galois rings*, Designs, Codes, and Cryptography **10** (1997), 157–165.
2. A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory **40** (1994), 301–319.
3. N. M. Katz, *Serre-tate local moduli*, Algebraic surfaces (Orsay, 1976-78), Lecture Notes in Math., vol. 868, Springer, Berlin-New York, 1981, pp. 138–202.
4. P. V. Kumar, T. Helleseth, and A. R. Calderbank, *An upper bound for some exponential sums over Galois rings and applications*, IEEE Transactions on Information Theory **41** (1995), 456–468.
5. S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1974.
6. W-C. W. Li, *Character sums over p-adic fields*, preprint, 1997.

7. J. Lubin, J-P. Serre, and J. Tate, *Elliptic curves and formal groups*, Proc. of the Woods Hole summer institute in algebraic geometry, 1964.
8. H. L. Schmid, *Zur arithmetik der zyklischen p-Körper*, Crelles J. **176** (1936), 161–167.
9. ______, *Kongruenzzetafunktionen in zyklischen Körpern*, Abh. Preuss. Akad. Wiss. Math.-Nat. Kl. **1941** (1942), 30pp.
10. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
11. P. Solé, *A quaternary cyclic code and a family of quadriphase sequences with low correlation*, Coding Theory and Applications (Toulon, 1988) (New York), Lecture Notes in Computer Science, vol. 388, Springer, 1989, pp. 193–201.
12. H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.
13. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Kluwer, Dordrecht, 1991.
14. J.-F. Voloch and J. L. Walker, *Euclidean weights of codes from elliptic curves over rings*, submitted for publication.
15. J. L. Walker, *Algebraic geometric codes over rings*, submitted for publication.
16. ______, *Algebraic geometric codes over rings*, Ph.D. thesis, University of Illinois, 1996.
17. ______, *The Nordstrom Robinson code is algebraic geometric*, IEEE Transactions on Information Theory **43** (1997), 1588–1593.

Department of Mathematics, University of Texas, Austin, TX 78712
E-mail address: voloch@math.utexas.edu

Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323
E-mail address: jwalker@math.unl.edu