CODES OVER RINGS FROM CURVES OF HIGHER GENUS

JOSÉ FELIPE VOLOCH AND JUDY L. WALKER

Abstract. We construct certain error-correcting codes over finite rings and estimate their parameters. These codes are constructed using plane curves and the estimates for their parameters rely on constructing "lifts" of these curves and then estimating the size of certain exponential sums.

1. Introduction

The purpose of this paper is to construct certain error-correcting codes over finite rings and estimate their parameters. For this purpose, we need to develop some tools; notably an estimate for the dimension of trace codes over rings (generalizing work of van der Vlugt over fields) and some results on lifts of affine curves from fields of characteristic p to Witt vectors of length two. This work partly generalizes our previous work on elliptic curves, although there are some differences which we will point out below.

A code is a subset of A^n, where A is a finite set (called the alphabet). Usually A is just the field of two elements and, in this case, one speaks of binary codes. For various reasons one often restricts attention to linear codes, which are linear subspaces of A^n when A is a field. However, there are non-linear binary codes (such as the Nordstrom-Robinson, Kerdock, and Preparata codes) that outperform linear codes for certain parameters. These codes have remained somewhat mysterious until recently when Hammons, et al. ([3]) discovered that one can obtain these codes from linear codes over rings (i.e. submodules of A^n, A a ring) via the Gray mapping, which we recall below.

In a different vein, over the last decade there has been a lot of interest in linear codes coming from algebraic curves over finite fields. The construction of such codes was first proposed by Goppa in [2]; see [10] or [11] for instance. In [12], it is proven that for $q \geq 49$ a square, there exist sequences of codes over the finite field with q elements which give asymptotically the best known linear codes over these fields. The second author has extended Goppa's construction to curves over finite rings and shown, for instance, that the Nordstrom-Robinson code can be obtained from her construction followed by the Gray mapping; see [17] and [18]. While most of the parameters for these new codes were estimated in the above papers, the crucial parameter needed to describe the error-correcting capability of the images of these codes under the Gray mapping was still lacking.

In our previous work ([14], [15]) we used elliptic curves which were canonical lifts of their reductions and we were able to estimate the minimum distance in that case. Curves of higher genus unfortunately do not have canonical lifts so we need to

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.

proceed differently. We find that on an open set there are lifts which are sufficiently good so we use those. For these codes, the missing parameter can be estimated and we do so. We also obtain finer estimates on the dimension of the trace codes.

The work of Mochizuki [7], indicates that there might be a general framework for working with lifts for curves of higher genus, with the proviso that the lift of points is only on *certain* open subsets of the curve. Mochizuki defines an analogue of ordinary curves and of canonical liftings for such. It remains to be seen if the corresponding lift of points is of small degree, which is essential for applications.

2. Codes over Witt rings

In this section we recall the definition of the ring of Witt vectors over a finite field and prove some general results about such rings and codes over them. The two theorems in this section are both generalizations of results which are known in the finite field case. We believe that Theorem 2.3 is known, but we include it for lack of a good reference. In contrast, Theorem 2.2 is new, having only appeared previously in the second author's thesis ([16]).

Recall the definitions of the Frobenius and trace maps for finite fields: Let p be prime and consider the field extension $\mathbb{F}_{p^m}/\mathbb{F}_p$. Then the Frobenius automorphism $\sigma : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is the element of $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ given by $\sigma(x) = x^p$, and the trace map $tr : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is given by $tr(x) = x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{m-1}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}$.

We will be working mostly with rings of Witt vectors or Witt rings, for short. See, e.g., [9] for an introduction to Witt rings. Let us just point that the Witt ring $W_l(\mathbb{F}_{p^m})$ is, as a set, $\mathbb{F}_{p^m}^l$, and the operations are defined by

$$(x_0, x_1, \ldots, x_{l-1}) + (y_0, y_1, \ldots, y_{l-1}) = (S_0, S_1, \ldots, S_{l-1}),$$
$$(x_0, x_1, \ldots, x_{l-1})(y_0, y_1, \ldots, y_{l-1}) = (P_0, P_1, \ldots, P_{l-1}),$$

where the S_i's and P_i's are certain polynomials with integer coefficients in x_0, $x_1, \ldots, x_{l-1}$, y_0, $y_1, \ldots, y_{l-1}$. In particular, we have

$$(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1 + \frac{1}{p}((x_0 + y_0)^p - x_0^p - y_0^p))$$
$$(x_0, x_1)(y_0, y_1) = (x_0 y_0, x_0^p y_1 + y_0^p x_1)$$

The ring $W_l(\mathbb{F}_{p^m})$ is a local ring with maximal ideal generated by p, satisfying $p^l = 0$ and having residue field $\mathbb{F}_{p^m}$. It is easy to check that the Galois Ring $GR(p^l, m)$ of degree m over $\mathbb{Z}/p^l\mathbb{Z}$ is isomorphic to the ring $W_l(\mathbb{F}_{p^m})$ of length l Witt vectors over the field with p^m elements. In particular, $W_l(\mathbb{F}_p) \cong \mathbb{Z}/p^l\mathbb{Z}$.

One can now define the Frobenius and trace maps for a Witt ring $W_l(\mathbb{F}_{p^m})$. Let $\mathbf{x} = (x_0, x_1, \ldots, x_{l-1}) \in W_l(\mathbb{F}_{p^m})$. The Frobenius $F : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_{p^m})$ is given by $F(\mathbf{x}) = F((x_0, x_1, \ldots, x_{l-1})) = (x_0^p, x_1^p, \ldots, x_{l-1}^p)$. The trace map $T : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_p) \cong \mathbb{Z}/p^l\mathbb{Z}$ is given by $T(\mathbf{x}) = \mathbf{x} + F(\mathbf{x}) + \cdots + F^{m-1}(\mathbf{x})$.

It is a standard fact that for any $\mathbf{x} = (x_0, x_1, \ldots, x_{l-1}) \in W_l(\mathbb{F}_{p^m})$, we have $p\mathbf{x} = (0, x_0^p, x_1^p, \ldots, x_{l-2}^p)$ and $\mathbf{x} \cdot (y_0, 0, \ldots, 0) = (x_0 y_0, x_1 y_0^p, \ldots, x_{l-1} y_0^{p^{l-1}})$ for every $y_0 \in \mathbb{F}_{p^m}$.

We would like to prove a version of Delsarte's Theorem for Witt rings. The usual statement of this theorem goes as follows: Let C be a linear code over $\mathbb{F}_{q^m}$. Denote by $tr(C)$ the linear code over $\mathbb{F}_q$ obtained by applying the trace map $tr : \mathbb{F}_{q^m} \to \mathbb{F}_q$

coordinatewise to the codewords of C. Denote by $C|_{\mathbb{F}_q}$ the subcode of C consisting of all codewords whose coordinates all lie in $\mathbb{F}_q$. Then

$$(C|_{\mathbb{F}_q})^\perp = tr(C^\perp).$$

In order prove our version of this theorem, we must check that several of the standard properties of σ and tr still hold for F and T. This checking is done in the following technical lemma.

Lemma 2.1. *Let $\pi : W_l(\mathbb{F}_{p^m}) \to \mathbb{F}_{p^m}$ be the natural projection, and let σ, tr, F, and T be as above. Then*

1. *$\pi \circ F = \sigma \circ \pi$ and $\pi \circ T = tr \circ \pi$.*
2. *The map $T : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_p) = \mathbb{Z}/p^l\mathbb{Z}$ is onto.*
3. *There is some $x_0 \in F_{p^m}$ with $T((x_0, 0, \ldots, 0)) \not\equiv 0 \pmod p$.*
4. *Let $\mathbf{x}$ be a nonzero element of $W_l(\mathbb{F}_{p^m})$. Then there is some $\mathbf{y} \in W_l(\mathbb{F}_{p^m})$ with $T(\mathbf{xy}) \neq 0$.*

Proof. Part (1) is straight forward calculation. Consider an arbitrary element $\mathbf{x} = (x_0, x_1, \ldots, x_{l-1}) \in W_l(\mathbb{F}_{p^m})$. We have $\pi \circ F(\mathbf{x}) = \pi((x_0^p, x_1^p, \ldots, x_{l-1}^p)) = x_0^p = \sigma \circ \pi(\mathbf{x})$ and $\pi \circ T(\mathbf{x}) = \pi(\mathbf{x} + F(\mathbf{x}) + \cdots + F^{m-1}(\mathbf{x})) = x_0 + x_0^p + \cdots + x_0^{p^{m-1}} = tr(x_0) = tr \circ \pi(\mathbf{x})$.

For (2), first note that it is well known that $tr : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is onto (see, for example, [10]). Since π is onto, we see that $\pi \circ T = tr \circ \pi$ is onto. If T is not onto, then its image is contained in a $\mathbb{Z}/p^l\mathbb{Z}$-submodule of $\mathbb{Z}/p^l\mathbb{Z}$, i.e., an ideal. Since $\mathbb{Z}/p^l\mathbb{Z}$ is local with maximal ideal (p), we have $T(W_l(\mathbb{F}_{p^m})) \subset p\mathbb{Z}/p^l\mathbb{Z}$, which implies $\pi \circ T = 0$, contradicting (1).

Now suppose that (3) fails, and let $\mathbf{x}$ be any element of $W_l(\mathbb{F}_{p^m})$. We can write $\mathbf{x} = (x_0, 0, \ldots, 0) + p\mathbf{y}$ for some $\mathbf{y} \in W_l(\mathbb{F}_{p^m})$. Then $T(\mathbf{x}) = T((x_0, 0, \ldots, 0)) + pT(y) \in p\mathbb{Z}/p^l\mathbb{Z}$. Since $\mathbf{x}$ was arbitrary, this contradicts (2) above.

Finally, to see why (4) is true, write $\mathbf{x} = (x_0, x_1, \ldots, x_{l-1})$ and let i be minimal with $x_i \neq 0$. Then $\mathbf{x} = p^i((\sigma^{-i}(x_i), 0, \ldots, 0) + p\mathbf{x}')$ for some $\mathbf{x}' \in W_l(\mathbb{F}_{p^m})$. By (3), there is some $y_0 \in F_{p^m}$ such that $\pi(T((\sigma^{-i}(x_i)y_0, 0, \ldots, 0))) \neq 0$. But then

$$\begin{aligned} T(\mathbf{x} \cdot (y_0, 0, \ldots, 0)) &= T(p^i((\sigma^{-i}(x_i)y_i, 0, \ldots, 0) + p\mathbf{x}' \cdot (y_0, \ldots, 0))) \\ &= p^i T(\sigma^{-i}(x_i)y_0, 0, \ldots, 0) + p^{i+1}T(\mathbf{x}' \cdot (y_0, 0, \ldots, 0)). \end{aligned}$$

Since this is nonzero modulo p^{i+1}, it is nonzero. □

We are now equipped to prove a version of Delsarte's theorem for codes over Witt rings.

Theorem 2.2. *Let C be any linear code over $W_l(\mathbb{F}_{p^m})$ and let $C^\perp$ be the dual code of C. Write $C|_{\mathbb{Z}/p^l\mathbb{Z}}$ for the subcode $C \cap (\mathbb{Z}/p^l\mathbb{Z})^n$ of C. Then*

$$(C|_{\mathbb{Z}/p^l\mathbb{Z}})^\perp = T(C^\perp).$$

Proof. (following [10]) First we show $T(C^\perp) \subset (C|_{\mathbb{Z}/p^l\mathbb{Z}})^\perp$. For this, it is enough to show that $\mathbf{c} \cdot T(\mathbf{a}) = 0$ for every $\mathbf{c} = (c_1, \ldots, c_n) \in C|_{\mathbb{Z}/p^l\mathbb{Z}}$ and $\mathbf{a} = (a_1, \ldots, a_n) \in C^\perp$. But

$$\mathbf{c} \cdot T(\mathbf{a}) = \sum_{i=1}^{n} c_i T(a_i) = T(\sum c_i a_i) = T(\mathbf{c} \cdot \mathbf{a}) = T(0) = 0.$$

To see that $(C|_{\mathbb{Z}/p^l\mathbb{Z}})^\perp \subset T(C^\perp)$, it is enough to show that $(T(C^\perp))^\perp \subset C|_{\mathbb{Z}/p^l\mathbb{Z}}$. Suppose not. Then for some $\mathbf{u} \in (T(C^\perp))^\perp$, $\mathbf{u} \notin C$. Hence there is some $\mathbf{v} \in C^\perp$ with $\mathbf{u} \cdot \mathbf{v} \neq 0$. By Lemma 2.1(4), there is some $\mathbf{x} \in W_l(\mathbb{F}_{p^m})$ with $T(\mathbf{xu} \cdot \mathbf{v}) \neq 0$. So we have

$$0 \neq T(\mathbf{xu} \cdot \mathbf{v}) = T(\mathbf{u} \cdot \mathbf{xv}) = \mathbf{u} \cdot T(\mathbf{xv}).$$

However, $\mathbf{xv} \in C^\perp$ and so $T(\mathbf{xv}) \in T(C^\perp)$, which means that $\mathbf{u} \cdot T(\mathbf{xv}) = 0$, a contradiction. □

Finally, we would like to point out that the proof of the additive form of Hilbert's Theorem 90 as given in [5] goes through for Witt vectors. It is given here for reference.

Theorem 2.3. *(Hilbert's Theorem 90 for Witt vectors) Let $F : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_{p^m})$ be the map $(a_0, \ldots, a_{l-1}) \mapsto (a_0^p, \ldots, a_{l-1}^p)$ and let $T : W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_p)$ be the trace mapping, so that $T(\mathbf{a}) = \mathbf{a} + F(\mathbf{a}) + \cdots + F^{m-1}(\mathbf{a})$. Then for any $\mathbf{a} \in W_l(\mathbb{F}_{p^m})$, we have $T(\mathbf{a}) = 0$ if and only if $\mathbf{a} = \mathbf{b} - F(\mathbf{b})$ for some $\mathbf{b} \in W_l(\mathbb{F}_{p^m})$.*

Proof. Clearly $T(\mathbf{b} - F(\mathbf{b})) = 0$, so assume $\mathbf{a} \in W_l(\mathbb{F}_{p^m})$ is arbitary with $T(\mathbf{a}) = 0$. Since the map T is onto by Lemma 2.1(2) above, there is some $\mathbf{c} \in W_l(\mathbb{F}_{p^m})$ with $T(\mathbf{c}) = 1_{W_l(\mathbb{F}_p)}$. Setting

$$\mathbf{b} = \sum_{r=0}^{m-2} \sum_{i=0}^{r} F^i(\mathbf{a}) F^r(\mathbf{c}),$$

it is straightforward to check that $\mathbf{a} = \mathbf{b} - F(\mathbf{b})$. □

3. Algebraic geometric codes over rings

In [17], the idea of algebraic geometric codes over rings other than fields is introduced, and foundational results about these codes are proven. In [18], the methods of [17] are used to explicitly construct the $\mathbb{Z}/4\mathbb{Z}$-version of the Nordstrom-Robinson code as an algebraic geometric code. In order to construct other codes over $\mathbb{Z}/4\mathbb{Z}$ with good nonlinear binary shadows, we must first investigate the Lee and Euclidean weights of these codes. In this section, we recall the definitions and some results from [17] and explain how the Lee and Euclidean weights of algebraic geometric codes over rings are related to exponential sums.

Let A be a local Artinian ring with maximal ideal $\mathfrak{m}$. We assume that the field $A/\mathfrak{m}$ is finite; say $A/\mathfrak{m} = \mathbb{F}_q$. For example, we could take $A = W_l(\mathbb{F}_{p^m})$, and then $\mathfrak{m} = (p)$ and $A/\mathfrak{m} = \mathbb{F}_{p^m}$. Let $\mathbf{X}$ be a curve over A, that is, a connected irreducible scheme over $\operatorname{Spec} A$ which is smooth of relative dimension one. Let $\mathbf{X} \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q = X \subset \mathbf{X}$ be the fiber of $\mathbf{X}$ over the closed point of $\operatorname{Spec} A$. We assume X is absolutely irreducible, so that it is the type of curve on which algebraic geometric codes over $\mathbb{F}_q$ are defined. Let $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ be a set of A-points on $\mathbf{X}$ with distinct specializations $P_1, \ldots, P_n$ in X.

Recall that in the case of a curve C over a field k, given a (Weil) divisor D on a curve C, there is a corresponding line bundle $\mathcal{O}_C(D)$, and we have the k-vector space of global sections of $\mathcal{O}_C(D)$.

$$L(D) = \Gamma(C, \mathcal{O}_C(D)) = \{f \in k(C) \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

A similar thing holds in the case of the curve $\mathbf{X}$ over A and a Cartier divisor. Thus, for a Cartier divisor $\mathbf{D}$ on $\mathbf{X}$, we define

$$L(\mathbf{D}) = \Gamma(\mathbf{X}, \mathcal{O}_{\mathbf{X}}(\mathbf{D}))$$

to be the A-module of global sections of $\mathcal{O}_{\mathbf{X}}(\mathbf{D})$ on $\mathbf{X}$.

In particular, let $\mathbf{G}$ be a (Cartier) divisor on $\mathbf{X}$ such that no P_i is in the support of $\mathbf{G}$, and let $\mathcal{L} = \mathcal{O}_{\mathbf{X}}(\mathbf{G})$ be the corresponding line bundle. For each i, $\Gamma(Z_i, \mathcal{L}|_{Z_i}) \simeq A$, and thinking of elements of $L(\mathbf{G})$ as rational functions on $\mathbf{X}$, we may think of the composition $L(\mathbf{G}) \to \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A$ as evaluation of these functions at Z_i. Summing over all i, we have a map $\gamma : L(\mathbf{G}) \to \bigoplus \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A^n$, given by $f \mapsto (f(Z_1), \ldots, f(Z_n))$.

Definition 3.1. Let A, $\mathbf{X}$, $\mathcal{Z}$, $\mathcal{L}$, and γ be as above. Define $C_A(\mathbf{X}, \mathcal{Z}, \mathcal{L})$ to be the image of γ. $C_A(\mathbf{X}, \mathcal{Z}, \mathcal{L})$ is called the algebraic geometric code over A associated to $\mathbf{X}$, $\mathcal{Z}$, and $\mathcal{L}$.

The following theorem summarizes some of the main results of [17].

Theorem 3.2. *Let $\mathbf{X}$, $\mathcal{L}$, and $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ be as above. Let g denote the genus of $\mathbf{X}$, 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 $n - \deg \mathcal{L}$.*

Remark 3.3. The minimum Hamming distance is obtained by comparing zeros and poles and the dimension computation is a consequence of the Riemann-Roch Theorem. These estimates require the assumption $2g-2 < \deg \mathcal{L} < n$. The duality result follows from a generalized version of the Residue Theorem which holds for Gorenstein rings. See [17] for details.

For applications, one is usually concerned with constructing codes over $\mathbb{Z}/4\mathbb{Z}$, or more generally, over rings of the form $\mathbb{Z}/p^l\mathbb{Z}$, where p is prime and $l \geq 1$. We can use algebraic geometry to construct such codes in two different ways. First, we can simply set $A = \mathbb{Z}/p^l\mathbb{Z}$ in the definition of algebraic geometric codes above. Alternatively, we can construct an algebraic geometric code over $W_l(\mathbb{F}_{p^m})$ and look at the associated trace code over $W_l(F_p) = \mathbb{Z}/p^l\mathbb{Z}$.

The Gray map allows us to construct (non-linear) binary codes from codes over $\mathbb{Z}/4\mathbb{Z}$ and is defined as follows. Consider the map $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2^2$ defined by $\phi(0) = (0,0), \phi(1) = (0,1), \phi(2) = (1,1), \phi(3) = (1,0)$. Now we define a map, again denoted by $\phi : (\mathbb{Z}/4\mathbb{Z})^n \to \mathbb{F}_2^{2n}$, by applying the previous ϕ to each coordinate.

For linear codes over rings of the form $\mathbb{Z}/p^l\mathbb{Z}$, it is often either the Euclidean or Lee weight rather than the Hamming weight which is of interest. In particular, when $p^l = 4$, the Euclidean and Lee weights are closely related, and the Lee weight gives the Hamming weight of the associated nonlinear binary code.

We begin by defining Euclidean weights. We identify an element x of the cyclic group $\mathbb{Z}/p^l\mathbb{Z}$ with the corresponding p^lth root of unity via the map

$$x \to e_{p^l}(x) := e^{2\pi i x/p^l}.$$

Definition 3.4. The Euclidean distance between x and y is the distance $d_E(x, y)$ in the complex plane between the points $e_{p^l}(x)$ and $e_{p^l}(y)$, and the Euclidean weight of x is the distance $w_E(x)$ between $e_{p^l}(x)$ and $e_{p^l}(0) = 1$.

We have

$$w_E(x) = \sqrt{\sin^2\left(\frac{2\pi x}{p^l}\right) + (1-\cos\left(\frac{2\pi x}{p^l}\right))^2}$$
$$= \sqrt{2-2\cos\left(\frac{2\pi x}{p^l}\right)}.$$

In fact, it is usually the square of the Euclidean weight in which one is interested. This is given by $w_E^2(x) = 2 - 2\cos(\frac{2\pi x}{p^l})$. For vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ over $\mathbb{Z}/p^l\mathbb{Z}$, we define

$$d_E^2(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} d_E^2(x_j, y_j)$$

and

$$w_E^2(\mathbf{x}) = \sum_{j=1}^{n} w_E^2(x_j)$$

For example, the squared Euclidean weight of the all-one vector in $(\mathbb{Z}/p^l\mathbb{Z})^n$ is $2n(1-\cos(2\pi/p^l))$. Using the Taylor expansion of cosine, we get that this is at least $4n\frac{\pi^2}{p^{2l}}(1+\frac{\pi^2}{3p^{2l}})$. Further, any other nonzero constant vector in $(\mathbb{Z}/p^l\mathbb{Z})^n$ has squared Euclidean weight at least this.

For general vectors, since $\cos(\frac{2\pi x}{p^l}) = \operatorname{Re}\left(e_{p^l}(x)\right)$, we have

$$w_E^2(\mathbf{x}) = \sum_{j=1}^{n} \left(2 - 2\operatorname{Re}\left(e_{p^l}(x_j)\right)\right)$$
$$= 2n - 2\operatorname{Re}\sum_{j=1}^{n} e_{p^l}(x_j)$$
$$\geq 2n - 2\left|\sum_{j=1}^{n} e_{p^l}(x_j)\right|.$$

Hence, to find a lower bound on the minimum Euclidean weight of a linear code over $\mathbb{Z}/p^l\mathbb{Z}$, it is enough to find an upper bound on the modulus of the exponential sum

$$\sum_{j=1}^{n} e_{p^l}(x_j).$$

Now consider the case $p^l = 4$. Then $e_4(0) = 1$, $e_4(1) = i$, $e_4(2) = -1$, and $e_4(3) = -i$. Hence $w_E^2(0) = 0$, $w_E^2(1) = w_E^2(3) = 2$, and $w_E^2(2) = 4$. Since the Lee weight is defined by $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, and $w_L(2) = 2$, we have

$$w_L(x) = \frac{1}{2}w_E^2(x)$$

for any $x \in \mathbb{Z}/4\mathbb{Z}$. From this we see that the Euclidean weight of a codeword over $\mathbb{Z}/4\mathbb{Z}$ is twice the Hamming weight of the binary codeword obtained by applying the Gray map. Notice that the Lee weight of a constant vector in $(\mathbb{Z}/4\mathbb{Z})^n$ is either 0, n, or $2n$.

Finally, let C be an algebraic geometric code over $W_l(\mathbb{F}_{p^m})$, and let $T : W_l(\mathbb{F}_{p^m}) \to \mathbb{Z}/p^l\mathbb{Z}$ denote the trace map as before. We are interested in the minimum Euclidean weight of $T(C)$, the trace code of C, which is a linear code over $\mathbb{Z}/p^l\mathbb{Z}$. Codewords in $T(C)$ are of the form $(T(f(Z_1)), \dots, T(f(Z_n)))$, where f is a rational function on some curve $\mathbf{X}$ defined over $W_l(\mathbb{F}_{p^m})$ and $Z_1, \dots, Z_n$ are $W_l(\mathbb{F}_{p^m})$-points on $\mathbf{X}$. From the argument above, to find a lower bound for the minimum Euclidean weight of $T(C)$ it suffices to find an upper bound on the modulus of

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

To estimate these kinds of sums, Theorem 3.5 below, which we proved in [14], is very useful. Let X be a curve over the finite field $\mathbb{F}_q$, where $q = p^m$ with p prime. Denote by $K = \mathbb{F}_q(X)$ the function field of X. Let $f_0, \dots, f_{l-1} \in K$ and consider the Witt vector $\mathbf{f} = (f_0, \dots, f_{l-1}) \in W_l(K)$. Let X_0 be the maximal affine open subvariety of X where $f_0, \dots, f_{l-1}$ do not have poles and let $P \in X_0(\mathbb{F}_q)$. We can then consider the Witt vector $\mathbf{f}(P) = (f_0(P), \dots, f_{l-1}(P)) \in W_l(\mathbb{F}_q)$. Letting $T : W_l(\mathbb{F}_q) \to W_l(\mathbb{F}_p) \cong \mathbb{Z}/p^l\mathbb{Z}$ denote the trace map, we can consider the exponential sum

$$S_{\mathbf{f},\mathbb{F}_q} = \sum_{P \in X_0(\mathbb{F}_q)} e^{2\pi i T(\mathbf{f}(P))/p^l}.$$

Theorem 3.5. *With notation as above, assume $X \setminus X_0$ consists of the points above the valuations $v_1, \dots, v_s$ of K. Let g be the genus of X, $n_{ij} = -v_j(f_i)$, $i = 0, \dots, l-1$, $j = 1, \dots, s$, and assume that $\mathbf{f}$ is not of the form $\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + \mathbf{c}$ for any $\mathbf{g} \in W_l(K)$ and $\mathbf{c} \in W_l(\mathbb{F}_q)$, where F denotes the additive endomorphism on $W_l(K)$ given by $F(g_0, g_1, \dots, g_{l-1}) = (g_0^p, g_1^p, \dots, g_{l-1}^p)$. Then $|S_{\mathbf{f},\mathbb{F}_q}| \le Bq^{1/2}$, where*

$$B \le 2g - 1 + \sum_{j=1}^{s} \max\{p^{l-1-i} n_{ij} \mid 0 \le i \le l-1\} \deg v_j.$$

4. Liftings

In what follows, we consider an affine curve $\mathbf{U}$ over $W_2(k)$ defined by a polynomial equation $\mathbf{H}(\mathbf{x}, \mathbf{y}) = 0$. Assume that $\mathbf{H}(\mathbf{x}, \mathbf{y})$ has the form $\sum_{di+ej \le de} a_{ij} \mathbf{x}^i \mathbf{y}^j$ where d and e are relatively prime integers, $a_{e0} \not\equiv 0 \pmod p$, and $a_{0d} \not\equiv 0 \pmod p$. Assume further that the affine curve U defined over k by $H(x_0, y_0) = 0$, where H is the reduction of $\mathbf{H}$ modulo p, is smooth. Letting $\mathbf{X}$ be the projective closure of $\mathbf{U}$, we have that $X = \mathbf{X} \times_{\operatorname{Spec} W_2(k)} \operatorname{Spec} k$ is the projective closure of U, and we see that $X \setminus U$ consists of a single point, which we call the point at infinity. Moreover, the genus g of X can be computed to be $(d-1)(e-1)/2$ by the Plücker formula. Let $R = k[x_0, y_0]/H(x_0, y_0)$ be the coordinate ring of U. For $f \in R$, let $\deg f$ denote the order of the pole at infinity of f.

Lemma 4.1. *Let $a, b, c \in R$ with $(a, b) = 1$, $\deg(a) = n$, $\deg(b) = m$, and $\deg(c) = r$. Then there exist $u, v \in R$ satisfying $au + bv = c$ with $\deg(u) \le m + s$ and $\deg(v) \le n + s$, where $s = \max\{2g, r - n - m\}$.*

Proof. Let P_∞ be the point at infinity of X. Then $a \in L(nP_\infty)$, $b \in L(mP_\infty)$, and $c \in L(rP_\infty)$. For any positive integer s, consider the map $L((m+s)P_\infty) \oplus L((n+s)P_\infty) \to L((n+m+s)P_\infty)$ given by $(u, v) \mapsto au + bv$. We wish first to

describe the kernel of this map. If $au + bv = 0$, then since $(a, b) = 1$, we have $u = bz$ and $v = -az$ for some $z \in R$, which is then in $L(sP_\infty)$. Thus the kernel is isomorphic to $L(sP_\infty)$. Now we examine the image. If $s > 2g$, Riemann-Roch gives the dimensions of $L(sP_\infty)$, $L((m+s)P_\infty) \oplus L((n+s)P_\infty)$, and $L((n+m+s)P_\infty)$ as $s - g + 1$, $(m + s + n + s) - 2g + 2$, $(n + m + s) - g + 1$, respectively. Thus, since the dimension of our domain is equal to sum of the dimension of our range with the dimension of our kernel, our map must be surjective. Since we want c in the image we take $n + m + s \geq r$ and $s \geq 2g$. □

The next theorem uses explicit computations with Witt vectors to show that there is a "lift of points" from U to $\mathbf{U}$. Notice that part (2) of the theorem, giving the lower bound on what the degrees of the coordinates of the "lift" must be, is primarily of theoretical interest and is not used in the remainder of the paper.

Theorem 4.2. *Assume that the equation* $\mathbf{H}(\mathbf{x}, \mathbf{y}) = 0$ *satisfies the conditions above. Let* P_∞ *be the unique point of* X *at infinity. Then there is a "lift of points"* $\lambda : X(k) \setminus \{P_\infty\} \to \mathbf{X}(W_2(k))$ *given by* $\lambda((x_0, y_0)) = ((x_0, x_1), (y_0, y_1))$*, where* x_1 *and* y_1 *are polynomials in* x_0 *and* y_0 *satisfying*

1. x_1 *and* y_1 *have poles of order at most* $(d-1)(pe+e-1)$ *and* $(e-1)(pd+d-1)$ *respectively at* P_∞*, and*
2. *If the genus of* X *is at least two, then either* x_1 *has a pole at* P_∞ *of order at least* $p(e-1)$*, or* y_1 *has a pole at* P_∞ *of order at least* $p(d-1)$*.*
3. *For any* $\mathbf{f} \in L(rZ_\infty)$*, we have* $\mathbf{f} \circ \lambda = (f_0, f_1)$*, a Witt vector of rational functions on* X*. Further,* $\deg f_0 \leq r$ *and* $\deg f_1 \leq \gamma(r)$*, where* $\gamma(r)$ *is a linear polynomial in* r*, independent of* $\mathbf{f}$ *and satisfying* $\gamma(r) \leq p(r-1) + (d-1)(e-1)(p+1) = p(r-1) + 2g(p+1)$*.*

Proof. Notice first that x_0 has a pole at P_∞ of order d and y_0 has a pole at P_∞ of order e.

By calculations in the Witt ring, we see that if x_1 and y_1 are polynomials in x_0 and y_0 such that $\mathbf{H}((x_0, x_1), (y_0, y_1)) = 0$ whenever $H(x_0, y_0) = 0$, then x_1 and y_1 must satisfy

$$(\partial H/\partial x_0)^p \, x_1 + (\partial H/\partial y_0)^p \, y_1 + J(x_0, y_0) = 0$$

where $J(x_0, y_0)$ is a polynomial in x_0 and y_0, having a pole of order at most pde at P_∞.

We can apply Lemma 4.1 with $a = (\partial H/\partial x_0)^p$, $b = (\partial H/\partial y_0)^p$, and $c = J(x_0, y_0)$. Then $n = \deg a = pd(e-1)$, $m = \deg b = pe(d-1)$, and $r \leq pde$. Since $g = (d-1)(e-1)/2$, we have $s = \max\{(d-1)(e-1), pde - pd(e-1) - pe(d-1)\} = (d-1)(e-1)$. Lemma 4.1 then gives us that x_1 and y_1 exist with $\deg x_1 \leq pe(d-1) + (d-1)(e-1) = (pe+e-1)(d-1)$ and $\deg y_1 \leq pd(e-1) + (d-1)(e-1) = (pd+d-1)(e-1)$.

To see why at least one of the two lower bounds mentioned in the theorem must hold, let $\lambda : X(k) \setminus \{P_\infty\} \to \mathbf{X}(W_2(k))$ be any lift of points. Recall that the Greenberg transform $G(\mathbf{X})$ of $\mathbf{X}$ can be thought of as the variety over k obtained by looking at the coordinate components of the Witt vector equations which define $\mathbf{X}$. In particular, the coordinate ring of the affine part of $G(\mathbf{X})$ is $k[x_0, y_0, x_1, y_1]/(H(x_0, y_0), H_1(x_0, y_0, x_1, y_1))$, so there is a canonical map $G(\mathbf{X}) \to X$. Then λ is in fact a map from the affine open subset $U = X \setminus \{P_\infty\}$ of X to the Greenberg transform $G(\mathbf{X})$ which is a partial splitting of the map $G(\mathbf{X}) \to X$. Since the genus of X is at least 2, a result of Raynaud ([8]) implies that $G(\mathbf{X})$

is affine, so that the image of the extension $\overline{\lambda} : X \to \overline{G(\mathbf{X})}$ (where $\overline{G(\mathbf{X})}$ is the projective closure of $G(\mathbf{X})$) cannot lie entirely within $G(\mathbf{X})$. In particular, we must have $\overline{\lambda}(P_\infty) \in \overline{G(\mathbf{X})} \setminus G(\mathbf{X})$. Examining the implications of this condition at a local parameter for P_∞, we get our desired lower bound as follows.

Since $\gcd(d, e) = 1$ by assumption, we can find integers u, v with $du + ev = 1$. This means that $t = x_0^{-u} y_0^{-v}$ is a local parameter at P_∞. Then we have that $t \circ \lambda = (t_0, t_1)$, where $t_0 = x_0^{-u} y_0^{-v}$ and $t_1 = -vt_0^p y_0^{-p} y_1 - ut_0^p x_0^{-p} x_1$. The condition on $\overline{\lambda}(P_\infty)$ above amounts to a requirement that t_1 have a pole at P_∞. But the valuation of t_1 at P_∞ is at least $\min\{p - ep + v_{P_\infty}(y_1), p - dp + v_{P_\infty}(x_1)\}$. Requiring this minimum to be negative proves (2) of the theorem.

Finally, to see why (3) is true, first notice that $L(rZ_\infty)$ has a basis consisting of all those monomials $\mathbf{x}^i \mathbf{y}^j$ which satisfy the three conditions $0 \le j \le d - 1$, $0 \le i$, and $di + ej \le r$. If $(x_0, y_0) \in X(k) \setminus \{P_\infty\}$, then we have

$$\mathbf{x}^i \mathbf{y}^j (\lambda((x_0, y_0))) = (x_0^i y_0^j, i(x_0^i y_0^j)^p x_0^{-p} x_1 + j(x_0^i y_0^j)^p y_0^{-p} y_1).$$

The first coordinate of the above expression has degree $di + ej \le r$, and the second has degree at most

$$\max\{p(di + ej) - pd + \deg x_1, p(di + je) - pe + \deg y_1\}$$

which is at most $p(r - 1) + (p + 1)(d - 1)(e - 1) = p(r - 1) + 2(p + 1)g$. Adding constant multiples of these monomials together will not increase the degrees of the coordinate functions. □

Corollary 4.3. *Let $\mathbf{X}$, X, and $\lambda : X(k) \to \mathbf{X}(W_2(\mathbb{F}_q))$ be as above. Let P_∞ be the unique point at infinity on X, and let Z_∞ be any $W_2(\mathbb{F}_q)$-point of $\mathbf{X}$ containing P_∞. For a positive integer r and a rational function $\mathbf{f} \in L(rZ_\infty)$, let $S_{\mathbf{f},\mathbb{F}_q}$ denote the exponential sum*

$$S_{\mathbf{f},\mathbb{F}_q} = \sum_{P \in X(\mathbb{F}_q) \setminus \{P_\infty\}} e^{2\pi i T(\mathbf{f}(\lambda(P)))/p^2}.$$

Then $|S_{\mathbf{f},\mathbb{F}_q}| \le ((2p + 4)g + p(r - 1) - 1)\sqrt{q}$.

Proof. Write $\mathbf{f}(\lambda(P)) = (f_0(P), f_1(P))$. By (3) of Theorem 4.2, we know that $f_0 \in L(rP_\infty)$ and $f_1 \in L(p(r - 1) + 2(p + 1)gP_\infty)$. Applying Theorem 3.5 above, we get the desired bound. □

5. A lower bound on the size of the trace code

Let $q = p^m$ and, as before, let $\mathbf{U}$ denote an affine curve over $W_2(\mathbb{F}_q)$ defined by a polynomial equation $\mathbf{H}(\mathbf{x}, \mathbf{y})$ satisfying the conditions of the previous section. Let $\mathbf{X}$ be the projective closure of $\mathbf{U}$, and U and X the reductions modulo p of $\mathbf{U}$ and $\mathbf{X}$ respectively. Let T denote both the trace map $W_l(\mathbb{F}_q) \to W_l(\mathbb{F}_p)$ and the coordinate-wise trace map $(W_l(\mathbb{F}_q))^n \to (W_l(\mathbb{F}_p))^n$.

Let r be a positive integer and denote by $\mathrm{ev} : L(rZ_\infty) \to (W_l(\mathbb{F}_q))^n$ the map which defines the code.

Corollary 4.3 above can be used to estimate the squared Euclidean weight of the trace code $T(C)$ of an algebraic geometric code C. In this section and the next, our aim is to estimate the size of $T(C)$. While it is true that $T(C)$ will be a linear code over $\mathbb{Z}/p^l\mathbb{Z}$ (a $\mathbb{Z}/p^l\mathbb{Z}$-module), it need not be true that $T(C)$ is a free code (module). Thus, we are forced to discuss the cardinality, rather than the rank, of $T(C)$. We will do this by considering the size of the kernel of the trace map T.

In this section, we find an upper bound on the size of this kernel, hence a lower bound on the size of the trace code. The general structure of our approach follows the approach taken by van der Vlugt in [13] as he studied trace codes of algebraic geometric codes over finite fields. In particular, the following result extends to rings a result of van der Vlugt [13] over fields.

Proposition 5.1. *Let* $\mathbf{f} \in L(rZ_\infty)$ *and suppose that* $\mathbf{f} \circ \lambda$ *is not of the form* $F(\mathbf{h}) - \mathbf{h} + \mathbf{c}$ *for any* $\mathbf{h} \in W_l(K)$ *and* $\mathbf{c} \in W_l(k)$*. Write* $\mathbf{f} \circ \lambda = (f_0, \dots, f_{l-1})$ *with each* $f_j \in K$*, and suppose that*

$$\max\{p^{l-1-j} \deg f_j \,|\, 0 \le j \le l-1\} < \frac{\#X(k) - 1}{\sqrt{q}} + 1 - 2g. \tag{1}$$

Then $T(\mathrm{ev}(\mathbf{f})) \neq 0$.

Remark 5.2. In specific examples, this proposition can be made to involve a general condition on the divisor rZ_∞ rather than a condition on the function $\mathbf{f}$.

Proof. Assume that $T(\mathrm{ev}(\mathbf{f})) = 0$. Then $T(\mathbf{f} \circ \lambda(P)) = 0$ for all $P \in X(\mathbb{F}_q) \setminus \{P_\infty\}$. Further, $\mathbf{f} \circ \lambda$ is not constant by assumption, so

$$\left| \sum_{P \in X(\mathbb{F}_q) \setminus \{P_\infty\}} e^{2\pi i T(\mathbf{f} \circ \lambda(P))/p^l} \right| = \#X(\mathbb{F}_q) - 1.$$

But also, by Theorem 3.5 we have

$$\left| \sum_{P \in X(\mathbb{F}_q) \setminus \{P_\infty\}} e^{2\pi i T(\mathbf{f} \circ \lambda(P))/p^l} \right| \le (2g - 1 + \max\{p^{l-1-j} \deg f_j \,|\, 0 \le j \le l-1\})\sqrt{q}.$$

Putting this together we have

$$\#X(\mathbb{F}_q) - 1 \le (2g - 1 + \max\{p^{l-1-j} \deg f_j \,|\, 0 \le j \le l-1\})\sqrt{q},$$

which contradicts the assumption of the proposition. □

Theorem 5.3. *Let* $\mathbf{f} \in L(rZ_\infty)$ *and assume that condition (1) holds. Then* $T(\mathrm{ev}(\mathbf{f})) = 0$ *if and only if* $\mathbf{f} \circ \lambda = F(\mathbf{g}) - \mathbf{g}$ *for some* $\mathbf{g} \in W_l(K)$.

Proof. If $\mathbf{f} \circ \lambda = F(\mathbf{g}) - \mathbf{g}$, then a coordinate of $T(\mathrm{ev}(\mathbf{f}))$ is $T(\mathbf{f} \circ \lambda(P)) = T((F(\mathbf{g}))(P) - \mathbf{g}(P)) = T(F(\mathbf{g}(P))) - T(\mathbf{g}(P)) = 0$. Conversely, suppose that $T(\mathrm{ev}(\mathbf{f})) = 0$. Then we know that $\mathbf{f} \circ \lambda$ is of the form $F(\mathbf{h}) - \mathbf{h} + \mathbf{c}$ for some $\mathbf{h} \in W_l(K)$ and some $\mathbf{c} \in W_l(\mathbb{F}_q)$ by Proposition 5.1 above. But then we have $0 = T(\mathbf{f} \circ \lambda(P)) = T(F(\mathbf{h}(P)) - \mathbf{h}(P)) + T(\mathbf{c}) = T(\mathbf{c})$ so that $T(\mathbf{c}) = 0$. By Theorem 2.3, $\mathbf{c}$ must be of the form $\mathbf{b} - F(\mathbf{b})$ for some $\mathbf{b} \in W_l(\mathbb{F}_q)$. But then we have $\mathbf{f} \circ \lambda = F(\mathbf{h}) - \mathbf{h} + \mathbf{b} - F(\mathbf{b}) = F(\mathbf{h} - \mathbf{b}) - (\mathbf{h} - \mathbf{b})$ and we are done. □

We see from Theorem 5.3 that finding the size of $\ker T$ is equivalent to finding the size of the set

$$\{\mathbf{g} \in W_l(K) \,|\, F(\mathbf{g}) - \mathbf{g} = \mathbf{f} \circ \lambda \text{ for some } \mathbf{f} \in L(rZ_\infty)\}.$$

In order to study this set, we restrict to the case $l = 2$. For $\mathbf{f} \in L(rZ_\infty)$, we have that $\mathbf{f} \circ \lambda = (f_0, f_1)$ with $f_j \in L(r_j P_\infty)$, where $r_0 = r$ and $r_1 = \gamma(r)$, for some

linear polynomial γ which we compute explicitly from the equation for the curve and the map λ. Condition (1) of Theorem 5.1 can be rewritten as

$$\max\{pr, \gamma(r)\} < \frac{\#X(k) - 1}{\sqrt{q}} + 1 - 2g. \tag{2}$$

In particular, notice that (2) does not depend at all on a specific choice of rational function $\mathbf{f} \in L(rZ_\infty)$. Assuming (2), we know that if $T(\mathrm{ev}(\mathbf{f})) = 0$, then $\mathbf{f} \circ \lambda = F(\mathbf{g}) - \mathbf{g}$. If we write $\mathbf{g} = (g_0, g_1)$ we see that

$$(f_0, f_1) = F(g_0, g_1) - (g_0, g_1) = (g_0^p - g_0, g_1^p - g_1 - \frac{1}{p}((g_0^p - g_0)^p - (g_0^{p^2} - g_0^p))).$$

Combining this with our knowledge about f_0 and f_1, we see that

$$p \deg g_0 \leq r$$

and

$$\max\{p \deg g_1, (p^2 - p + 1) \deg g_0\} \leq \gamma(r).$$

This gives three conditions which must be satisfied:

(1) $\deg g_0 \leq \lfloor \frac{r}{p} \rfloor$
(2) $\deg g_0 \leq \lfloor \frac{\gamma(r)}{p^2 - p + 1} \rfloor$
(3) $\deg g_1 \leq \lfloor \frac{\gamma(r)}{p} \rfloor$

Putting (1) and (2) together, we have proven the following:

Theorem 5.4. *In the case where $l = 2$, if $T(\mathrm{ev}(\mathbf{f})) = 0$ and condition (2) is satisfied, then $\mathbf{f} \circ \lambda = F(\mathbf{g}) - \mathbf{g}$, where $\mathbf{g} = (g_0, g_1) \in W_l(K)$ with $g_j \in L(s_j P_\infty)$ where*

$$s_0 = \min\{\lfloor \frac{r}{p} \rfloor, \lfloor \frac{\gamma(r)}{p^2 - p + 1} \rfloor\}$$

and

$$s_1 = \lfloor \frac{\gamma(r)}{p} \rfloor.$$

We now set out to bound the size of $\ker T$. We will do this by bounding the number of pairs $(g_0, g_1) \in W_l(K)$ such that, in the notation of the previous theorem, $g_j \in L(s_j P_\infty)$ and $F((g_0, g_1)) - (g_0, g_1) = \mathbf{f} \circ \lambda$ for some $\mathbf{f} \in L(rZ_\infty)$ satisfying (2) and such that $T(\mathrm{ev}(\mathbf{f})) = 0$.

Because of the existence of λ, there exists also $\phi : \mathbf{U} \to \mathbf{U}^\sigma$ lifting Frobenius by [1]. Let us choose some function $\mathbf{x}$ regular on $\mathbf{U}$. Then $\phi^*(d\mathbf{x})/p \equiv \omega \pmod{p}$, where ω is a differential regular on U, as shown by Mazur in [6].

Lemma 5.5. *If $\mathbf{f} \circ \lambda = (f_0, f_1)$ then $df_1/dx = (df_0/dx)^p \omega/dx - f_0^{p-1} df_0/dx$.*

Proof. Let $\phi : \mathbf{U} \to \mathbf{U}^\sigma$ be the lift of Frobenius. Then we have $f_1 \equiv (\mathbf{f} \circ \phi - \mathbf{f}^p)/p \pmod{p}$. Differentiating this last equation gives

$$df_1 \equiv (\phi^*(d\mathbf{f}) - p\mathbf{f}^{p-1} d\mathbf{f})/p \pmod{p}.$$

Also,

$$\phi^*(d\mathbf{f}) \equiv \phi^*(d\mathbf{x})(d\mathbf{f}/d\mathbf{x}) \circ \phi).$$

Combining these two equations gives

$$df_1 \equiv \omega(d\mathbf{f}/d\mathbf{x}) \circ \phi) - \mathbf{f}^{p-1} d\mathbf{f} \pmod{p},$$

which simplifies to (using that $\mathbf{g} \circ \phi \equiv \mathbf{g}^p \pmod p$ for any $\mathbf{g}$)

$$df_1/dx = (df_0/dx)^p \omega/dx - f_0^{p-1} df_0/dx$$

as desired. □

Theorem 5.6. *Under the above conditions,*

$$\begin{aligned} \#\ker(T) &\leq \#L(\lfloor \frac{r}{p} \rfloor P_\infty) \cdot \#L(\lfloor \frac{\gamma(r)}{p^2} \rfloor P_\infty) \\ &\leq q^{\lfloor \frac{\gamma(r)}{p^2} \rfloor + \frac{r}{p} + 2}. \end{aligned}$$

Proof. Let $A(x) = \frac{1}{p}((x^p - x)^p - (x^{p^2} - x^p)) \mod p$. Then $A'(x) = -(x^p - x)^{p-1} - x^{p-1}$. Suppose that $\mathbf{f} \circ \lambda = F(\mathbf{g}) - \mathbf{g}$, where $\mathbf{g} = (g_0, g_1)$. By computation with Witt vectors, this translates to the pair of equations $f_0 = g_0^p - g_0$ and $f_1 = g_1^p - g_1 - A(g_0)$. Differentiating these equations gives $df_0/dx = -dg_0/dx$ and

$$\begin{aligned} -dg_1/dx &= df_1/dx + A'(g_0) g_0' \\ &= (df_0/dx)^p \omega/dx - f_0^{p-1} df_0/dx + A'(g_0) g_0' \\ &= -(dg_0/dx)^p \omega/dx + (g_0^p - g_0)^{p-1} dg_0/dx + A'(g_0) g_0' \\ &= -(dg_0/dx)^p \omega/dx - g_0^{p-1} dg_0/dx. \end{aligned}$$

Thus, if $\deg \mathbf{f} = r$, then $\deg f_0 \leq r, \deg f_1 \leq \gamma(r)$. It then follows that $\deg g_0 \leq r/p$ and $\deg g_1 \leq \gamma(r)/p$. Moreover, $g_1 = \Psi(g_0) + u^p$, where $\Psi(g_0)$ is a fixed solution to $d\Psi(g_0)/dx = -(dg_0/dx)^p \omega/dx - g_0^{p-1} dg_0/dx$, with $\deg \Psi(g_0) \leq s/p$, provided such solution exists (otherwise we cannot have such a pair (g_0, g_1)). Then $\deg u \leq \gamma(r)/p^2$. Given r, the number of possible $(g_0, g_1) \in W_l(\mathbb{F}_q)$ is at most the number of possible g_0 times the number of possible u. This gives the first estimate in the theorem. The second follows from using the trivial estimate that $\dim L(D) \leq \deg D + 1$ for any effective divisor D on a curve X over a field. □

Theorem 5.7. *In the situation above, the cardinality of the trace code satisfies*

$$\#T(C) \geq q^{2r - 2g - \lfloor \frac{r}{p} \rfloor - \lfloor \frac{\gamma(r)}{p^2} \rfloor}.$$

Proof. Just use the fact that $\#C = q^{2(r+1-g)}$ and the estimate on the size of the kernel of the trace map in Theorem 5.6. □

6. An upper bound on the size of the trace code

After finding a lower bound on the size of the trace code in the previous section, the aim of this section is to find an upper bound on how large a trace code can be.

Definition 6.1. For $B \subseteq (W_l(\mathbb{F}_{p^m}))^n$, define

$$F(B) := \{(F(b_1), \ldots, F(b_n)) \,|\, (b_1, \ldots, b_n) \in B\}$$

and

$$B|_{W_l(\mathbb{F}_p)} := B \cap (W_l(\mathbb{F}_p))^n.$$

If B is a free $W_l(\mathbb{F}_{p^m})$-module, we denote by $\operatorname{rank}(B)$ its rank.

Proposition 6.2. *(compare* [10] *Proposition VIII.1.4, p223) Let C be a free code over the ring $W_l(\mathbb{F}_{p^m})$ and let $B \subseteq C$ be a free subcode such that $F(B) \subseteq C$. Then*

$$\#T(C) \leq p^{lm(\operatorname{rank}(C)-\operatorname{rank}(B))} \cdot \#B|_{W_l(\mathbb{F}_p)}.$$

Proof. Define $\wp : B \to C$ by $\wp(b) = F(b) - b$. Then $b \in \ker \wp \iff F(b) = b \iff b \in B|_{W_l(\mathbb{F}_p)}$. But $T(a) = T(F(a))$ for any a, so $\operatorname{im} \wp \subseteq \ker T$. Thus

$$\#\ker T \geq \#\operatorname{im} \wp = \#B/\#\ker \wp = \#B/\#B|_{W_l(F_p)}$$

and the result follows by simply noting that $\#T(C) = \#C/\#\ker T$. □

Because of the existence of λ, we know that the Frobenius lifts to a map $\Phi : R \to R$, where $R = \Gamma(\mathbf{U}, \mathcal{O}_{\mathbf{X}}(\mathbf{U}))$ is the ring of regular functions on $\mathbf{U}$. Further, for $\mathbf{f} \in R$ we have $F(\mathbf{f} \circ \lambda) = (\Phi(\mathbf{f})) \circ \lambda$.

Lemma 6.3. *In the situation of Theorem 4.2, assume $d < e$ and set $t = \lfloor \frac{r}{e(p+1)} \rfloor$. Then $\Phi(\mathbf{g}) \in L(rZ_\infty)$ for every $\mathbf{g} \in L(tZ_\infty)$.*

Proof. Since $\mathbf{g} \in R$, we have $\Phi(\mathbf{g}) \in R$ so we just need to find the order of the pole at infinity of $\Phi(\mathbf{g})$. Recall that $L(tZ_\infty)$ is generated by monomials of the form $\mathbf{x}^i\mathbf{y}^j$ where $i \geq 0$, $0 \leq j \leq d-1$, and $id + je \leq t$. Writing $\mathbf{g} = \mathbf{g}(\mathbf{x}, \mathbf{y})$, we have $\Phi(\mathbf{g}(\mathbf{x}, \mathbf{y})) = \mathbf{g}(\Phi(\mathbf{x}), \Phi(\mathbf{y})) = \mathbf{g}(\mathbf{x}^p + px_1, \mathbf{y}^p + py_1)$, so $\deg \Phi(\mathbf{g}) = \deg \mathbf{g}(\mathbf{x}^p + px_1, \mathbf{y}^p + py_1)$. For any monomial $\mathbf{x}^i\mathbf{y}^j$ appearing in $\mathbf{g}$, we have $\deg \Phi(\mathbf{x}^i\mathbf{y}^j) = \deg((\mathbf{x} + px_1)^i(\mathbf{y} + py_1)^j) \leq (p+1)et \leq r$, and adding constant multiples of such monomials together will not increase the degree. □

Theorem 6.4. *In the situation of of Theorem 4.2 with $d < e$, set $t = \lfloor \frac{r}{e(p+1)} \rfloor$. For a positive integer s, define $\dim_{\mathbf{X}}(s) = \operatorname{rank}(L(sZ_\infty))$. Let C be the algebraic geometric code defined on $\mathbf{X}$ using the divisor rZ_∞. Then*

$$\#T(C) \leq p^{lm(\dim_{\mathbf{X}}(r)-\dim_{\mathbf{X}}(s))+l}.$$

Proof. Set $B := C_{W_l(\mathbb{F}_{p^m})}(\mathbf{X}, \mathcal{Z}, tZ_\infty)$. Then since $F((\mathbf{g} \circ \lambda)(P)) = (\Phi(\mathbf{g}) \circ \lambda)(P)$ and $\Phi(\mathbf{g}) \in L(rZ_\infty)$ for each $\mathbf{g} \in L(tZ_\infty)$, we have $F(B) \subseteq C$. Therefore, by the above proposition, we have

$$\#T(C) \leq p^{lm(\dim_X(r)-\dim_X(t))} \cdot \#B|_{W_l(\mathbb{F}_p)}$$

and we only need to find $\#B|_{W_l(\mathbb{F}_p)}$.

Suppose $\mathbf{h} \in L(tZ_\infty)$ is such that $\mathbf{h} \circ \lambda(P) \in W_l(\mathbb{F}_p)$ for each P. Since $\Phi(\mathbf{h}) \in L(rZ_\infty)$ and $\mathbf{h} \in L(tZ_\infty) \subseteq L(rZ_\infty)$, we have $\mathbf{f} := \Phi(\mathbf{h}) - \mathbf{h} \in L(rZ_\infty)$. But since $\mathbf{h} \circ \lambda(P) \in W_l(\mathbb{F}_p)$, we have $\mathbf{f} \circ \lambda(P) = 0$ for each P, so that $\mathbf{f}$ is in the kernel of the evaluation map which defines the code. Our assumption that $r < n$ forces this map to be injective, so we have $\mathbf{f} = 0$. Thus $\Phi(\mathbf{h}) = \mathbf{h}$, but this means that $\mathbf{h} \in W_l(\mathbb{F}_p)$. □

7. Examples

We start by considering curves of genus zero, noting that certain aspects of this case were previously considered in [4] without using the language of algebraic geometry. In our language, we see that the curve $\mathbb{A}^1$ has a natural lifting of points given by the Teichmüller lift, $\lambda(x) = (x, 0)$. The coordinate ring of $\mathbb{A}^1/W_2(\mathbb{F}_{p^m})$ is $W_2(\mathbb{F}_{p^m})[\mathbf{x}]$. Given a polynomial $\mathbf{f}(\mathbf{x}) \in W_2(\mathbb{F}_{p^m})[\mathbf{x}]$, a simple calculation shows that $\mathbf{f} \circ \lambda = (f_0, f_1)$, where $f_1 \equiv (\mathbf{f}(\mathbf{x})^p - \mathbf{f}(\mathbf{x}^p))/p \pmod p$. It follows that $\deg f_1 \leq p \deg \mathbf{f}$, so we can take $\gamma(r) = pr$.

The case of genus one was studied extensively in our previous work, [14]. An ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ has a canonical lifting to an elliptic curve $\mathbf{E}$ over $W_2(\mathbb{F}_q)$ for which the Frobenius of E also lifts to an isogeny $\phi : \mathbf{E} \to \mathbf{E}^{(p)}$ of degree p. In addition, there is an injective homomorphism $\tau : E(\bar{\mathbb{F}}_q) \to \mathbf{E}(W(\bar{\mathbb{F}}_q))$ (analogous to the Teichmüller lift), compatible with the action of Frobenius, which we will call the elliptic Teichmüller lift. Analogously to the case of $\mathbb{A}^1$, given a function $\mathbf{f}$ on $\mathbf{E}$ we have $\mathbf{f} \circ \tau = (f_0, f_1)$, where $f_1 \equiv (\mathbf{f} \circ \phi - \mathbf{f}^p)/p \pmod p$. In Proposition 4.2 of [14] we prove that, if $\mathbf{E}$ is given by a Weierstrass equation in coordinates $\mathbf{x}, \mathbf{y}$, then $\deg x_1 \leq 3p-1, \deg y_1 \leq 4p-1$. In the affine coordinate ring generated by $\mathbf{x}, \mathbf{y}$, every function is a polynomial in $\mathbf{x}, \mathbf{y}$ of degree at most 1 in $\mathbf{y}$ and it follows from this that $\deg f_1 \leq p(\deg \mathbf{f} + 1) - 1$ for any $\mathbf{f}$ in this ring. In other words, we can take $\gamma(r) = p(r+1) - 1$.

For a numerical example, consider the curve E given by the equation $y^2 + y = x^3 + t^3$ over the field $\mathbb{F}_{16} := \mathbb{F}_2[t]/(t^4+t+1)$. This curve is supersingular so we cannot consider its canonical lift. It is easy to see that the curve $\mathbf{E}$ over $W_2(\mathbb{F}_{16})$ given by the equation $\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + (t^3, 0)$ certainly has E as its reduction. Further, it is easy to check that whenever (x_0, y_0) is an affine point on E, $\lambda((x_0, y_0)) := ((x_0, 0), (y_0, y_0^3 + x_0^3 t^3))$ satisfies the equation defining $\mathbf{E}$ so we get a lift of points on the affine curve.

The curve E has 24 affine $\mathbb{F}_{16}$-rational points. Let P_∞ be the point at infinity on $\mathbf{E}$. If we use the basis $\{1, \mathbf{x}, \mathbf{y}\}$ for the global sections of $\mathcal{O}_{\mathbf{E}}(3P_\infty)$ on $\mathbf{E}$, we get a binary code of length 48 with 2^{18} codewords and minimum distance 8. As the best linear code of this length with this many codewords has minimum distance somewhere between 12 and 14, this is not a good code.

However, if we evaluate the rational functions in $L(2P_\infty)$ (using the basis $\{1, \mathbf{x}\}$) at the lifts of only half the points, we get a pretty good code. In particular, it is easy to see that the affine F_{16}-rational points on E occur in pairs sharing the same x-coordinate. Taking one point from each of these pairs, lifting them and evaluating the functions 1 and $\mathbf{x}$ at these lifts yields a code whose trace code has generator matrix

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

The image under the Gray mapping of this code is a binary code of length 24 with 2^{10} codewords and minimum Hamming distance 8. This matches the best possible binary linear code with this length and number of codewords.

For another class of examples, let $\mathbf{X}$ be the Hermitian curve defined by

$$\mathbf{y}^q \mathbf{z} + \mathbf{y} \mathbf{z}^q = \mathbf{x}^{q+1}$$

over the ring $W_2(\mathbb{F}_{p^m})$, $m \geq 1$, where q is a power of the prime p. Its reduction modulo p is the curve X defined by the equation

$$y_0^q z_0 + y_0 z_0^q = x_0^{q+1}$$

The equation $F(\mathbf{x}, \mathbf{y}) = \mathbf{y}^q + \mathbf{y} - \mathbf{x}^{q+1} = 0$ defines an open affine subset $\mathbf{U}$ of $\mathbf{X}$, and the equation $F_0(x_0, y_0) = y_0^q + y_0 - x_0^{q+1}$ defines an open affine subset U of X.

Notice also that $X = U \cup \{P_\infty\}$, where P_∞ is the unique point at infinity on X. Fix a $W_2(\mathbb{F}_{p^m})$-point Z_∞ of $\mathbf{X}$ containing P_∞.

Letting $n := \#X(\mathbb{F}_{p^m}) - 1$, and choosing r with $q^2 - q - 2 < r < n$, we see by [17] that we can use $\mathbf{X}$ and the divisor rZ_∞ to construct a free code C over $W_2(\mathbb{F}_{p^m})$ having length n, rank $r + 1 - \frac{q(q-1)}{2}$ and minimum Hamming weight at least $n - r$. We are interested in the parameters of the trace code $T(C)$ over $W_2(\mathbb{F}_p) = \mathbb{Z}/p^2\mathbb{Z}$.

By Theorem 4.2, we know that there is a "lift of points" $\lambda : X(\mathbb{F}_{p^m}) \setminus \{P_\infty\} \to \mathbf{X}(W_2(\mathbb{F}_{p^m}))$ given by $\lambda((x_0, y_0)) = ((x_0, x_1), (y_0, y_1))$ with $\deg x_1 \leq (q-1)(pq + p + q)$, $\deg y_1 \leq q(pq + q - 1)$, and, if $g := \frac{q(q-1)}{2} \geq 2$, either $\deg x_1 \geq pq$ or $\deg y_1 \geq p(q-1)$. In fact, one can check by brute force that the map λ given by $\lambda((x_0, y_0)) = ((x_0, x_1), (y_0, y_1))$, where x_1 is any constant c and $y_1 = cx_0^{pq} + \frac{1}{p}((y_0^q + y_0)^p - y_0^{pq} - y_0^p)$ is a lift of points satisfying $\deg x_1 = 0$ and $\deg y_1 = \max\{pq^2, (pq - q + 1)(q + 1)\} = pq^2 + \epsilon$, where $\epsilon = 0$ if $p \neq q$ and $\epsilon = 1$ if $p = q$. Notice that λ is "good", in the sense that it satisfies the conditions of the conclusion of Theorem 4.2.

A basis for the global sections of $L(rZ_\infty)$ is $\{\mathbf{x}^i\mathbf{y}^j \mid i \geq 0, 0 \leq j \leq q-1, qi + (q+1)j \leq r\}$. Setting $\mathbf{x} = (x_0, x_1)$ and $\mathbf{y} = (y_0, y_1)$ and doing computations in the Witt ring, we get

$$\mathbf{x}^i\mathbf{y}^j = (x_0^i y_0^j, j x_0^{pi} y_0^{p(j-1)} y_1 + i x_0^{p(i-1)} y_0^{pj} x_1).$$

Writing the above expression as (f_0, f_1), we see (using the facts that $\deg x_0 = q+1$ and $\deg y_0 = q$) that $\deg f_0 \leq r$ and $\gamma(r) := \deg f_1 \leq pr + pq^2 - pq - p + \epsilon$, where $\epsilon = 0$ if $p \neq q$ and $\epsilon = 1$ if $p = q$.

Applying Theorem 3.5 and using the fact that $\gamma(r) \geq pr$ for all p, we see that if $\mathbf{f} \in L(rZ_\infty)$, then

$$\left| \sum_{P \in X(\mathbb{F}_{p^m}) \setminus \{P_\infty\}} e^{2\pi i T(\mathbf{f} \circ \lambda(P))/p^2} \right| \leq (q^2 - q + pr + pq^2 - pq - p + \epsilon)\sqrt{p^m}.$$

This means that the minimum squared Euclidean weight of $T(C)$ is at least $2n - 2(q^2 - q + pr + pq^2 - pq - p + \epsilon)\sqrt{p^m}$. Notice that this is an improvement upon the general result of Theorem 5.7, which would only yield that the squared Euclidean weight is at least $2n - ((2p+4)(q-1)q - 2p(r-1) + 2)\sqrt{p^m}$.

Finally, we know that the number of elements in the kernel of the trace map $T : C \to W_2(\mathbb{F}_p)$ is at most $p^{m(\gamma(r)/p^2 + r/p + 2)}$.

Let's now restrict to the case where $p = q$. The number of $\mathbb{F}_{p^m}$-rational points on X is $p^m + 1$ if m is odd, $p^m + 1 + p(p-1)p^{\frac{m}{2}}$ if $m \equiv 2 \pmod 4$, and $p^m + 1 - p(p-1)p^{\frac{m}{2}}$ if $4|m$, so we'll fix $m \equiv 2 \pmod 4$. Choosing r with $p(p-1) < r < n := p^m + p(p-1)p^{\frac{m}{2}}$, we construct a free $W_2(\mathbb{F}_{p^m})$-code C of length n, rank $r + 1 - \frac{p(p-1)}{2}$, and minimum Hamming distance at least $n - r$. The trace code $T(C)$ is a (not necessarily free) $W_2(\mathbb{F}_p) = \mathbb{Z}/p^2\mathbb{Z}$-module of length n with at least

$$p^{m(2r - \frac{r}{p} - \frac{\gamma(r)}{p^2} - p(p-1))}$$

elements and minimum squared Euclidean weight at least

$$2n - 2(p^3 + pr - 2p + 1)p^{\frac{m}{2}} = 2(p^m + 1 - (p^3 - p^2 - p + pr + 1)p^{\frac{m}{2}})$$

8. Acknowledgments

The authors acknowledge the use of the software packages Mathematica and Pari in some calculations.

References

[1] A. Buium, "Geometry of p-jets," *Duke Math. Journal*, vol. 82, pp. 349-367, 1996.
[2] V. D. Goppa, "Codes associated with divisors," *Probl. Peredachi Inf.*, vol. 13, pp. 33-39, 1977. (English translation in *Probl. Inf. Transm.,* 13:22-27, 1977.)
[3] 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 Trans. Inform. Theory*, vol. 40, pp. 301-319, 1994.
[4] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for some exponential sums over Galois rings and applications," *IEEE Trans. Inform. Theory*, vol. 41, pp. 456-468, 1995.
[5] S. Lang, *Algebra*. Reading, MA: Addison-Wesley, 1974.
[6] B. Mazur, "Frobenius and the Hodge filtration, estimates," *Ann. Math.*, vol. 98, pp. 58-95, 1973.
[7] S. Mochizuki, "A theory of ordinary p-adic curves," *Publ. Res. Inst. Math. Sci.*, vol. 32, pp. 957-1152, 1996.
[8] M. Raynaud, "Around the Mordell conjecture for function fields and a conjecture of Serge Lang," in *Algebraic Geometry*. Lecture Notes in Math. **1016**, pp. 1-19, Berlin: Springer-Verlag, 1983.
[9] Serre, *Local Fields*. Graduate Texts in Math. **67**, New York: Springer-Verlag, 1979.
[10] H. Stichtenoth, *Algebraic function fields and codes*. Berlin: Springer, 1993.
[11] M. A. Tsfasman and S. G. Vlădut, *Algebraic-Geometric Codes*. Dordrecht: Kluwer, 1991.
[12] M. A. Tsfasman, S. G. Vlădut, and Th. Zink, "Modular curves, Shimura curves, and Goppa Codes, better than the Varshamov-Gilbert bound," *Math. Nachrichten*, vol. 109, pp. 21-28, 1982.
[13] M. van der Vlugt, "A new upper bound for the dimension of trace codes," *Bull. London Math. Soc.*, vol. 23, pp. 395-400, 1991.
[14] J. F. Voloch and J. L. Walker, "Euclidean weights of codes from elliptic curves over rings," submitted for publication.
[15] J. F. Voloch and J. L. Walker, "Lee weights of Z/4Z-codes from elliptic curves", to appear in *Codes, Curves, and Signals: Common Threads in Communications*.
[16] J. L. Walker, *Algebraic geometric codes over rings*. Ph.D. dissertation, University of Illinois, 1996.
[17] J. L. Walker, "Algebraic geometric codes over rings", *J. Pure Appl. Algebra*, to appear.
[18] J. L. Walker, "The Nordstrom Robinson code is algebraic geometric," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1588-1593, 1997.

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