9-1999

# Codes Over Rings from Curves of Higher Genus

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

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

Published in IEEE Transactions on Information Theory, vol 45, iss 6 (Sept 1999), pp 1768-1776
DOI: 10.1109/18.782098

# 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.**

***Index Terms*— Algebraic geometry, codes, codes over rings, plane curves.**

## I. Introduction

The purpose of this paper is to construct certain error-correcting codes over finit 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 affin curves from field 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 finit set (called the alphabet). Usually $A$ is just the fiel 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 nonlinear 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 finit fields The construction of such codes was firs 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 finit fiel 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 finit 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 proceed differently. We fin that on an open set there are lifts which are sufficientl good so we use those. For these codes, the missing parameter can be estimated and we do so. We also obtain fine 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 define an analog 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.

Manuscript received November 12, 1998; revised March 30, 1999. The work of J. F. Voloch was supported in part by NSA under Grant MDA904-97-1-0037 and TARP under Grant ARP-006. The work of J. L. Walker was supported in part by NSF under Grant DMS-9709388.

J. F. Voloch is with the Department of Mathematics, University of Texas, Austin, TX 78712 USA.

J. L. Walker is with the Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323 USA.

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifie S 0018-9448(99)06066-6.

## II. Codes Over Witt Rings

In this section we recall the definitio of the ring of Witt vectors over a finit fiel 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 finit fiel case. We believe that Theorem II.3 is known, but we include it for lack of a good reference. In contrast, Theorem II.2 is new, having only appeared previously in the second author's thesis [16].

Recall the definition of the Frobenius and trace maps for finit fields Let $p$ be prime and consider the fiel extension $\mathbb{F}_{p^m}/\mathbb{F}_p$. Then the Frobenius automorphism $\sigma\colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is the element of $\mathrm{Gal}\,(\mathbb{F}_{p^m}/\mathbb{F}_p)$ given by $\sigma(x) = x^p$, and the trace map $\mathrm{tr}\colon \mathbb{F}_{p^m} \to \mathbb{F}_p$ is given by

$$\begin{aligned}\mathrm{tr}\,(x) &= x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{m-1}(x)\\ &= x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}.\end{aligned}$$

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 define by

$$\begin{aligned}&(x_0, x_1, \cdots, x_{l-1}) + (y_0, y_1, \cdots, y_{l-1})\\ &\qquad\qquad = (S_0, S_1, \cdots, S_{l-1})\\ &(x_0, x_1, \cdots, x_{l-1})(y_0, y_1, \cdots, y_{l-1})\\ &\qquad\qquad = (P_0, P_1, \cdots, P_{l-1})\end{aligned}$$

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

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

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 fiel $\mathbb{F}_{p^m}$. It is easy to check that the Galois ring $\mathrm{GR}(p^l, m)$ 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 fiel with $p^m$ elements. In particular, $W_l(\mathbb{F}_p) \cong \mathbb{Z}/p^l\mathbb{Z}$.

One can now defin the Frobenius and trace maps for a Witt ring $W_l(\mathbb{F}_{p^m})$. Let $\boldsymbol{x} = (x_0, x_1, \cdots, x_{l-1}) \in W_l(\mathbb{F}_{p^m})$. The Frobenius $F$: $W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_{p^m})$ is given by

$$F(\boldsymbol{x}) = F((x_0, x_1, \cdots, x_{l-1})) = (x_0^p, x_1^p, \cdots, x_{l-1}^p).$$

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

$$T(\boldsymbol{x}) = \boldsymbol{x} + F(\boldsymbol{x}) + \cdots + F^{m-1}(\boldsymbol{x}).$$

It is a standard fact that for any

$$\boldsymbol{x} = (x_0, x_1, \cdots, x_{l-1}) \in W_l(\mathbb{F}_{p^m})$$

we have

$$p\boldsymbol{x} = (0, x_0^p, x_1^p, \cdots, x_{l-2}^p)$$

and

$$\boldsymbol{x} \cdot (y_0, 0, \cdots, 0) = (x_0 y_0, x_1 y_0^p, \cdots, x_{l-1} y_0^{p^{l-1}})$$

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 $\mathrm{tr}\,(C)$ the linear code over $\mathbb{F}_q$ obtained by applying the trace map $\mathrm{tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ coordinate wise 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

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

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

*Lemma II.1:* Let $\pi : W_l(\mathbb{F}_{p^m}) \to \mathbb{F}_{p^m}$ be the natural projection, and let $\sigma$, $\mathrm{tr}$, $F$, and $T$ be as above. Then

1) $\pi \circ F = \sigma \circ \pi$ and $\pi \circ T = \mathrm{tr} \circ \pi$.
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 $x_0 \in \mathbb{F}_{p^m}$ with $T((x_0, 0, \cdots, 0)) \not\equiv 0 \pmod{p}$.
4) Let $\boldsymbol{x}$ be a nonzero element of $W_l(\mathbb{F}_{p^m})$. Then there is some $\boldsymbol{y} \in W_l(\mathbb{F}_{p^m})$ with $T(\boldsymbol{xy}) \neq 0$.

*Proof:* Part 1) is a straightforward calculation. Consider an arbitrary element

$$\boldsymbol{x} = (x_0, x_1, \cdots, x_{l-1}) \in W_l(\mathbb{F}_{p^m}).$$

We have

$$\pi \circ F(\boldsymbol{x}) = \pi((x_0^p, x_1^p, \cdots, x_{l-1}^p)) = x_0^p = \sigma \circ \pi(\boldsymbol{x})$$

and

$$\pi \circ T(\boldsymbol{x}) = \pi(\boldsymbol{x} + F(\boldsymbol{x}) + \cdots + F^{m-1}(\boldsymbol{x})) = x_0 + x_0^p + \cdots + x_0^{p^{m-1}} = \mathrm{tr}\,(x_0) = \mathrm{tr} \circ \pi(\boldsymbol{x}).$$

For 2), firs note that it is well known that $\mathrm{tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is onto (see, for example, [10]). Since $\pi$ is onto, we see that $\pi \circ T = \mathrm{tr} \circ \pi$ 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 $\boldsymbol{x}$ be any element of $W_l(\mathbb{F}_{p^m})$. We can write $\boldsymbol{x} = (x_0, 0, \cdots, 0) + p\boldsymbol{y}$ for some $\boldsymbol{y} \in W_l(\mathbb{F}_{p^m})$. Then

$$T(\boldsymbol{x}) = T((x_0, 0, \cdots, 0)) + pT(y) \in p\mathbb{Z}/p^l\mathbb{Z}.$$

Since $\boldsymbol{x}$ was arbitrary, this contradicts 2) above.

Finally, to see why 4) is true, write $\boldsymbol{x} = (x_0, x_1, \cdots, x_{l-1})$ and let $i$ be minimal with $x_i \neq 0$. Then

$$\boldsymbol{x} = p^i((\sigma^{-i}(x_i), 0, \cdots, 0) + p\boldsymbol{x}')$$

for some $\boldsymbol{x}' \in W_l(\mathbb{F}_{p^m})$. By 3), there is some $y_0 \in F_{p^m}$ such that $\pi(T((\sigma^{-i}(x_i)y_0, 0, \cdots, 0))) \neq 0$. But then

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

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 II.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

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

*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 $\boldsymbol{c} \cdot T(\boldsymbol{a}) = 0$ for every $\boldsymbol{c} = (c_1, \cdots, c_n) \in C|_{\mathbb{Z}/p^l\mathbb{Z}}$ and $\boldsymbol{a} = (a_1, \cdots, a_n) \in C^{\perp}$. But

$$\begin{aligned} \boldsymbol{c} \cdot T(\boldsymbol{a}) &= \sum_{i=1}^{n} c_i T(a_i) = T\left(\sum c_i a_i\right) \\ &= T(\boldsymbol{c} \cdot \boldsymbol{a}) = T(0) = 0. \end{aligned}$$

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 this is not the case. Then for some $\boldsymbol{u} \in (T(C^{\perp}))^{\perp}$, $\boldsymbol{u} \notin C$. Hence there is some $\boldsymbol{v} \in C^{\perp}$

with $\boldsymbol{u}\cdot\boldsymbol{v} \neq \boldsymbol{0}$. By Lemma II.1 4), there is some $\boldsymbol{x} \in W_l(\mathbb{F}_{p^m})$ with $T(\boldsymbol{xu}\cdot\boldsymbol{v}) \neq \boldsymbol{0}$. So we have

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

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

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 II.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 $(a_0, \cdots, a_{l-1}) \mapsto (a_0^p, \cdots, a_{l-1}^p)$ and let $T$: $W_l(\mathbb{F}_{p^m}) \to W_l(\mathbb{F}_p)$ be the trace mapping, so that $T(\boldsymbol{a}) = \boldsymbol{a} + F(\boldsymbol{a}) + \cdots + F^{m-1}(\boldsymbol{a})$. Then for any $\boldsymbol{a} \in W_l(\mathbb{F}_{p^m})$, we have $T(\boldsymbol{a}) = 0$ if and only if $\boldsymbol{a} = \boldsymbol{b} - F(\boldsymbol{b})$ for some $\boldsymbol{b} \in W_l(\mathbb{F}_{p^m})$.

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

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

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

## III. Algebraic–Geometric Codes Over Rings

In [17], the idea of algebraic–geometric codes over rings other than field 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 firs investigate the Lee and Euclidean weights of these codes. In this section, we recall the definition 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 fiel $A/\mathfrak{m}$ 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 $\boldsymbol{X}$ be a curve over $A$, that is, a connected irreducible scheme over $\operatorname{Spec} A$ which is smooth of relative dimension one. Let $\boldsymbol{X} \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q = X \subset \boldsymbol{X}$ be the fibe of $\boldsymbol{X}$ 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 $\mathcal{Z} = \{Z_1, \cdots, Z_n\}$ be a set of $A$-points on $\boldsymbol{X}$ with distinct specializations $P_1, \cdots, P_n$ in $X$.

Recall that in the case of a curve $C$ over a fiel $k$, 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 $\mathcal{O}_C(D)$.

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

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

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

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

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

$$\gamma : L(\boldsymbol{G}) \to \bigoplus \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A^n$$

given by $f \mapsto (f(Z_1), \cdots, f(Z_n))$.

*Definition III.1:* Let $A$, $\boldsymbol{X}$, $\mathcal{Z}$, $\mathcal{L}$, and $\gamma$ be as above. Defin $C_A(\boldsymbol{X}, \mathcal{Z}, \mathcal{L})$ to be the image of $\gamma$. $C_A(\boldsymbol{X}, \mathcal{Z}, \mathcal{L})$ is called the algebraic–geometric code over $A$ associated to $\boldsymbol{X}$, $\mathcal{Z}$, and $\mathcal{L}$.

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

*Theorem III.2:* Let $\boldsymbol{X}$, $\mathcal{L}$, and $\mathcal{Z} = \{Z_1, \cdots, Z_n\}$ be as above. Let $g$ denote the genus of $\boldsymbol{X}$, and suppose $2g - 2 < \deg \mathcal{L} < n$. Set $C = C(\boldsymbol{X}, \mathcal{Z}, \mathcal{L})$. 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 III.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 definitio 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 (nonlinear) binary codes from codes over $\mathbb{Z}/4\mathbb{Z}$ and is define as follows. Consider the map $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2^2$ define by $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$, $\phi(3) = (1, 0)$. Now we defin a map, again denoted by $\phi : (\mathbb{Z}/4\mathbb{Z})^n \to \mathbb{F}_2^{2n}$, by applying the previous $\phi$ 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 definin Euclidean weights. We identify an element $x$ of the cyclic group $\mathbb{Z}/p^l\mathbb{Z}$ with the corresponding

$p^l$th root of unity via the map

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

*Definition III.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

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

In fact, it is usually the square of the Euclidean weight in which one is interested. This is given by

$$w_E^2(x) = 2 - 2\cos(2\pi x/p^l).$$

For vectors $\boldsymbol{x} = (x_1, \cdots, x_n)$ and $\boldsymbol{y} = (y_1, \cdots, y_n)$ over $\mathbb{Z}/p^l\mathbb{Z}$, we defin

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

and

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

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

$$4n(\pi^2/p^{2l})(1 + (\pi^2/3p^{2l})).$$

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 $\cos(2\pi x/p^l) = \mathrm{Re}(e_{p^l}(x))$, we have

$$\begin{aligned} w_E^2(\boldsymbol{x}) &= \sum_{j=1}^{n}(2 - 2\,\mathrm{Re}(e_{p^l}(x_j))) \\ &= 2n - 2\,\mathrm{Re}\sum_{j=1}^{n} e_{p^l}(x_j) \\ &\geq 2n - 2\left|\sum_{j=1}^{n} e_{p^l}(x_j)\right|. \end{aligned}$$

Hence, to fin  a lower bound on the minimum Euclidean weight of a linear code over $\mathbb{Z}/p^l\mathbb{Z}$, it is enough to fin  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 define 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 $(T(f(Z_1)), \cdots, T(f(Z_n)))$, where $f$ is a rational function on some curve $\boldsymbol{X}$ define  over $W_l(\mathbb{F}_{p^m})$ and $Z_1, \cdots, Z_n$ are $W_l(\mathbb{F}_{p^m})$-points on $\boldsymbol{X}$. From the argument above, to fin  a lower bound for the minimum Euclidean weight of $T(C)$ it suffice  to fin  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 III.5 below, which we proved in [14], is very useful. Let $X$ be a curve over the finit  fiel  $\mathbb{F}_q$, where $q = p^m$ with $p$ prime. Denote by $K = \mathbb{F}_q(X)$ the function fiel  of $X$. Let $f_0, \cdots, f_{l-1} \in K$ and consider the Witt vector $\boldsymbol{f} = (f_0, \cdots, f_{l-1}) \in W_l(K)$. Let $X_0$ be the maximal affin  open subvariety of $X$ where $f_0, \cdots, f_{l-1}$ do not have poles and let $P \in X_0(\mathbb{F}_q)$. We can then consider the Witt vector $\boldsymbol{f}(P) = (f_0(P), \cdots, f_{l-1}(P)) \in W_l(\mathbb{F}_q)$. 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

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

*Theorem III.5:* With notation as above, assume $X \setminus X_0$ consists of the points above the valuations $v_1, \cdots, v_s$ of $K$. Let $g$ be the genus of $X$, $n_{ij} = -v_j(f_i)$, $i = 0, \cdots, l-1$, $j = 1, \cdots, s$, and assume that $\boldsymbol{f}$ is not of the form $\boldsymbol{f} = F(\boldsymbol{g}) - \boldsymbol{g} + \boldsymbol{c}$ for any $\boldsymbol{g} \in W_l(K)$ and $\boldsymbol{c} \in W_l(\mathbb{F}_q)$, where $F$ denotes the additive endomorphism on $W_l(K)$ given by

$$F(g_0, g_1, \cdots, g_{l-1}) = (g_0^p, g_1^p, \cdots, g_{l-1}^p).$$

Then $|S_{\boldsymbol{f}, \mathbb{F}_q}| \leq B q^{1/2}$, where

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

## IV. Liftings

In what follows, we consider an affin  curve $\boldsymbol{U}$ over $W_2(k)$ define  by a polynomial equation $\boldsymbol{H}(\boldsymbol{x}, \boldsymbol{y}) = 0$. Assume that $\boldsymbol{H}(\boldsymbol{x}, \boldsymbol{y})$ has the form $\sum_{di+ej \leq de} a_{ij} \boldsymbol{x}^i \boldsymbol{y}^j$ 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 affin  curve $U$ define  over $k$ by $H(x_0, y_0) = 0$, where $H$ is the reduction of $\boldsymbol{H}$ modulo $p$, is smooth. Letting $\boldsymbol{X}$ be the projective closure of $\boldsymbol{U}$, we have that $X = \boldsymbol{X} \times_{\mathrm{Spec}\, W_2(k)} \mathrm{Spec}\, k$ 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 infinit  of $f$.

*Lemma IV.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 $P_\infty$ be the point at infinit 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 firs 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 $s - g + 1$, $(m+s+n+s) - 2g + 2$, and $(n+m+s) - g + 1$, 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 $n + m + s \ge r$ and $s \ge 2g$. $\square$

The next theorem uses explicit computations with Witt vectors to show that there is a "lift of points" from $U$ to $\boldsymbol{U}$. 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 IV.2:* Assume that the equation $\boldsymbol{H}(\boldsymbol{x}, \boldsymbol{y}) = 0$ satisfie the conditions above. Let $P_\infty$ be the unique point of $X$ at infinity Then there is a "lift of points" $\lambda : X(k) \setminus \{P_\infty\} \to \boldsymbol{X}(W_2(k))$ 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 the following condition.

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

$$\gamma(r) \le p(r-1) + (d-1)(e-1)(p+1) = p(r-1) + 2g(p+1).$$

*Proof:* Notice firs that $x_0$ has a pole at $P_\infty$ of order $d$ and $y_0$ has a pole at $P_\infty$ 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 $\boldsymbol{H}((x_0, x_1), (y_0, y_1)) = 0$ 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 $P_\infty$.

We can apply Lemma IV.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 $r \le pde$. 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 IV.1 then gives us that $x_1$ and $y_1$ exist with

$$\deg x_1 \le pe(d-1) + (d-1)(e-1) = (pe+e-1)(d-1)$$

and

$$\deg y_1 \le pd(e-1) + (d-1)(e-1) = (pd+d-1)(e-1).$$

To see why at least one of the two lower bounds mentioned in the theorem must hold, let $\lambda : X(k) \setminus \{P_\infty\} \to \boldsymbol{X}(W_2(k))$ be any lift of points. Recall that the Greenberg transform $G(\boldsymbol{X})$ of $\boldsymbol{X}$ can be thought of as the variety over $k$ obtained by looking at the coordinate components of the Witt vector equations which defin $\boldsymbol{X}$. In particular, the coordinate ring of the affin part of $G(\boldsymbol{X})$ 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 $G(\boldsymbol{X}) \to X$. Then $\lambda$ is in fact a map from the affin open subset $U = X \setminus \{P_\infty\}$ of $X$ to the Greenberg transform $G(\boldsymbol{X})$ which is a partial splitting of the map $G(\boldsymbol{X}) \to X$. Since the genus of $X$ is at least 2, a result of Raynaud [8] implies that $G(\boldsymbol{X})$ is affine so that the image of the extension $\overline{\lambda} : X \to \overline{G(\boldsymbol{X})}$ (where $\overline{G(\boldsymbol{X})}$ is the projective closure of $G(\boldsymbol{X})$) cannot lie entirely within $G(\boldsymbol{X})$. In particular, we must have $\overline{\lambda}(P_\infty) \in \overline{G(\boldsymbol{X})} \setminus G(\boldsymbol{X})$. Examining the implications of this condition at a local parameter for $P_\infty$, we get our desired lower bound as follows.

Since $\gcd(d, e) = 1$ by assumption, we can fin integers $u, v$ with $du + ev = 1$. This means that $t = x_0^{-u} y_0^{-v}$ is a local parameter at $P_\infty$. 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 $P_\infty$. But the valuation of $t_1$ at $P_\infty$ 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, firs notice that $L(rZ_\infty)$ has a basis consisting of all those monomials $\boldsymbol{x}^i \boldsymbol{y}^j$ 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

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

The firs 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. $\square$

*Corollary IV.3:* Let $\boldsymbol{X}$, $X$, and $\lambda : X(k) \to \boldsymbol{X}(W_2(\mathbb{F}_q))$ be as above. Let $P_\infty$ be the unique point at infinit on $X$, and let $Z_\infty$ be any $W_2(\mathbb{F}_q)$-point of $\boldsymbol{X}$ containing $P_\infty$. For a positive integer $r$ and a rational function $\boldsymbol{f} \in L(rZ_\infty)$, let

$S_{\boldsymbol{f},\mathbb{F}_q}$ denote the exponential sum

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

Then

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

*Proof:* Write

$$\boldsymbol{f}(\lambda(P))=(f_0(P),\, f_1(P)).$$

By 3) of Theorem IV.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 III.5 above, we get the desired bound. $\square$

## V. A Lower Bound on the Size of the Trace Code

Let $q=p^m$ and, as before, let $\boldsymbol{U}$ denote an affin curve over $W_2(\mathbb{F}_q)$ define by a polynomial equation $\boldsymbol{H}(\boldsymbol{x},\boldsymbol{y})$ satisfying the conditions of the previous section. Let $\boldsymbol{X}$ be the projective closure of $\boldsymbol{U}$, and $U$ and $X$ the reductions modulo $p$ of $\boldsymbol{U}$ and $\boldsymbol{X}$, 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 $ev: L(rZ_\infty)\to (W_l(\mathbb{F}_q))^n$ the map which define the code.

Corollary IV.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 fin 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 finit fields In particular, the following result extends to rings a result of van der Vlugt [13] over fields

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

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

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

*Remark V.2:* In specifi examples, this proposition can be made to involve a general condition on the divisor $rZ_\infty$ rather than a condition on the function $\boldsymbol{f}$.

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

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

But also, by Theorem III.5, we have

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

Putting this together we have

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

which contradicts the assumption of the proposition. $\square$

*Theorem V.3:* Let $\boldsymbol{f}\in L(rZ_\infty)$ and assume that condition (V.1) holds. Then $T(ev(\boldsymbol{f}))=0$ if and only if $\boldsymbol{f}\circ\lambda=F(\boldsymbol{g})-\boldsymbol{g}$ for some $\boldsymbol{g}\in W_l(K)$.

*Proof:* If $\boldsymbol{f}\circ\lambda=F(\boldsymbol{g})-\boldsymbol{g}$, then a coordinate of $T(ev(\boldsymbol{f}))$ is

$$\begin{aligned}T(\boldsymbol{f}\circ\lambda(P)) &= T((F(\boldsymbol{g}))(P)-\boldsymbol{g}(P))\\ &= T(F(\boldsymbol{g}(P)))-T(\boldsymbol{g}(P))=0.\end{aligned}$$

Conversely, suppose that $T(ev(\boldsymbol{f}))=0$. Then we know that $\boldsymbol{f}\circ\lambda$ is of the form $F(\boldsymbol{h})-\boldsymbol{h}+\boldsymbol{c}$ for some $\boldsymbol{h}\in W_l(K)$ and some $\boldsymbol{c}\in W_l(\mathbb{F}_q)$ by Proposition V.1 above. But then we have

$$0=T(\boldsymbol{f}\circ\lambda(P))=T(F(\boldsymbol{h}(P))-\boldsymbol{h}(P))+T(\boldsymbol{c})=T(\boldsymbol{c})$$

so that $T(\boldsymbol{c})=0$. By Theorem II.3, $\boldsymbol{c}$ must be of the form $\boldsymbol{b}-F(\boldsymbol{b})$ for some $\boldsymbol{b}\in W_l(\mathbb{F}_q)$. But then we have

$$\boldsymbol{f}\circ\lambda=F(\boldsymbol{h})-\boldsymbol{h}+\boldsymbol{b}-F(\boldsymbol{b})=F(\boldsymbol{h}-\boldsymbol{b})-(\boldsymbol{h}-\boldsymbol{b})$$

and we are done. $\square$

We see from Theorem V.3 that findin the size of $\ker T$ is equivalent to findin the size of the set

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

In order to study this set, we restrict to the case $l=2$. For $\boldsymbol{f}\in L(rZ_\infty)$, we have that $\boldsymbol{f}\circ\lambda=(f_0,f_1)$ with $f_j\in L(r_jP_\infty)$, where $r_0=r$ and $r_1=\gamma(r)$, for some linear polynomial $\gamma$ which we compute explicitly from the equation for the curve and the map $\lambda$. Condition (V.1) of Theorem V.1 can be rewritten as

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

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

$$\begin{aligned}(f_0,\,f_1)&=F(g_0,\,g_1)-(g_0,\,g_1)\\ &=\left(g_0^p-g_0,\, g_1^p-g_1-\frac{1}{p}\left((g_0^p-g_0)^p-\left(g_0^{p^2}-g_0^p\right)\right)\right).\end{aligned}$$

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 V.4:* In the case where $l = 2$, if $T(ev(\boldsymbol{f})) = 0$ and condition (V.2) is satisfied then $\boldsymbol{f} \circ \lambda = F(\boldsymbol{g}) - \boldsymbol{g}$, where $\boldsymbol{g} = (g_0, g_1) \in W_l(K)$ with $g_j \in L(s_j P_\infty)$ where

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

and

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

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

$$F((g_0, g_1)) - (g_0, g_1) = \boldsymbol{f} \circ \lambda$$

for some $\boldsymbol{f} \in L(rZ_\infty)$ satisfying (V.2) and such that $T(ev(\boldsymbol{f})) = 0$.

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

*Lemma V.5:* If $\boldsymbol{f} \circ \lambda = (f_0, f_1)$ then

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

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

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

Also,

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

Combining these two equations gives

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

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

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

as desired. □

*Theorem V.6:* Under the above conditions

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

*Proof:* Let

$$A(x) = (1/p)((x^p - x)^p - (x^{p^2} - x^p)) \bmod p.$$

Then $A'(x) = -(x^p - x)^{p-1} - x^{p-1}$. Suppose that $\boldsymbol{f} \circ \lambda = F(\boldsymbol{g}) - \boldsymbol{g}$, where $\boldsymbol{g} = (g_0, g_1)$. 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

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

Thus if $\deg \boldsymbol{f} = r$, 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 fixe 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 firs 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 V.7:* In the situation above, the cardinality of the trace code satisfie

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

*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 V.6. □

## VI. An Upper Bound on the Size of the Trace Code

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

*Definition VI.1:* For $B \subseteq (W_l(\mathbb{F}_{p^m}))^n$, defin

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

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 rank $(B)$ its rank.

*Proposition VI.2 (c.f. [10, Proposition VIII.1.4, p. 223]):* 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:* Defin $\wp : B \to C$ 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 $\lambda$, we know that the Frobenius lifts to a map $\Phi : R \to R$, where $R = \Gamma(\boldsymbol{U}, \mathcal{O}_{\boldsymbol{X}}(\boldsymbol{U}))$ is the ring of regular functions on $\boldsymbol{U}$. Further, for $\boldsymbol{f} \in R$ we have $F(\boldsymbol{f} \circ \lambda) = (\Phi(\boldsymbol{f})) \circ \lambda$.

*Lemma VI.3:* In the situation of Theorem IV.2, assume $d < e$ and set $t = \lfloor \frac{r}{e(p+1)} \rfloor$. Then $\Phi(\boldsymbol{g}) \in L(rZ_\infty)$ for every $\boldsymbol{g} \in L(tZ_\infty)$.

*Proof:* Since $\boldsymbol{g} \in R$, we have $\Phi(\boldsymbol{g}) \in R$ so we just need to fin the order of the pole at infinit of $\Phi(\boldsymbol{g})$. Recall that $L(tZ_\infty)$ is generated by monomials of the form $\boldsymbol{x}^i\boldsymbol{y}^j$ where $i \geq 0$, $0 \leq j \leq d-1$, and $id + je \leq t$. Writing $\boldsymbol{g} = \boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y})$, we have

$$\Phi(\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y})) = \boldsymbol{g}(\Phi(\boldsymbol{x}), \Phi(\boldsymbol{y})) = \boldsymbol{g}(\boldsymbol{x}^p + px_1, \boldsymbol{y}^p + py_1)$$

so

$$\deg \Phi(\boldsymbol{g}) = \deg \boldsymbol{g}(\boldsymbol{x}^p + px_1, \boldsymbol{y}^p + py_1).$$

For any monomial $\boldsymbol{x}^i\boldsymbol{y}^j$ appearing in $\boldsymbol{g}$, we have

$$\deg \Phi(\boldsymbol{x}^i\boldsymbol{y}^j) = \deg\left((\boldsymbol{x} + px_1)^i(\boldsymbol{y} + py_1)^j\right) \leq (p+1)et \leq r$$

and adding constant multiples of such monomials together will not increase the degree. □

*Theorem VI.4:* In the situation of Theorem IV.2 with $d < e$, set $t = \lfloor r/e(p+1) \rfloor$. For a positive integer $s$, defin $\dim_{\boldsymbol{X}}(s) = \operatorname{rank}(L(sZ_\infty))$. Let $C$ be the algebraic–geometric code define on $\boldsymbol{X}$ using the divisor $rZ_\infty$. Then

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

*Proof:* Set $B := C_{W_l(\mathbb{F}_{p^m})}(\boldsymbol{X}, \mathcal{Z}, tZ_\infty)$. Then since $F((\boldsymbol{g} \circ \lambda)(P)) = (\Phi(\boldsymbol{g}) \circ \lambda)(P)$ and $\Phi(\boldsymbol{g}) \in L(rZ_\infty)$ for each $\boldsymbol{g} \in L(tZ_\infty)$, 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 fin $\#B|_{W_l(\mathbb{F}_p)}$.

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

## VII. 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 $W_2(\mathbb{F}_{p^m})[\boldsymbol{x}]$. Given a polynomial $\boldsymbol{f}(\boldsymbol{x}) \in W_2(\mathbb{F}_{p^m})[\boldsymbol{x}]$, a simple calculation shows that $\boldsymbol{f} \circ \lambda = (f_0, f_1)$, where $f_1 \equiv (\boldsymbol{f}(\boldsymbol{x})^p - \boldsymbol{f}(\boldsymbol{x}^p))/p \pmod{p}$. It follows that $\deg f_1 \leq p \deg \boldsymbol{f}$, so we can take $\gamma(r) = pr$.

The case of genus one was studied extensively in our previous work [14]. An ordinary elliptic curve define over a finit fiel $\mathbb{F}_q$ has a canonical lifting to an elliptic curve $\boldsymbol{E}$ over $W_2(\mathbb{F}_q)$ for which the Frobenius of $E$ also lifts to an isogeny $\phi : \boldsymbol{E} \to \boldsymbol{E}^{(p)}$ of degree $p$. In addition, there is an injective homomorphism $\tau : E(\overline{\mathbb{F}}_q) \to \boldsymbol{E}(W(\overline{\mathbb{F}}_q))$ (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 $\boldsymbol{f}$ on $\boldsymbol{E}$ we have $\boldsymbol{f} \circ \tau = (f_0, f_1)$, where $f_1 \equiv (\boldsymbol{f} \circ \phi - \boldsymbol{f}^p)/p \pmod{p}$. In [4, Proposition 4.2] we prove that, if $\boldsymbol{E}$ is given by a Weierstrass equation in coordinates $\boldsymbol{x}$, $\boldsymbol{y}$, then $\deg x_1 \leq 3p - 1$, $\deg y_1 \leq 4p - 1$. In the affin coordinate ring generated by $\boldsymbol{x}$, $\boldsymbol{y}$, every function is a polynomial in $\boldsymbol{x}$, $\boldsymbol{y}$ of degree at most 1 in $\boldsymbol{y}$ and it follows from this that $\deg f_1 \leq p(\deg \boldsymbol{f} + 1) - 1$ for any $\boldsymbol{f}$ 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 fiel $\mathbb{F}_{16} := \mathbb{F}_2[t]/(t^4 + t + 1)$. This curve is supersingular so we cannot consider its canonical lift. It is easy to see that the curve $\boldsymbol{E}$ over $W_2(\mathbb{F}_{16})$ given by the equation $\boldsymbol{y}^2 + \boldsymbol{y} = \boldsymbol{x}^3 + (t^3, 0)$ certainly has $E$ as its reduction. Further, it is easy to check that whenever $(x_0, y_0)$ is an affin point on $E$

$$\lambda((x_0, y_0)) := ((x_0, 0), (y_0, y_0^3 + x_0^3 t^3))$$

satisfie the equation definin $\boldsymbol{E}$ so we get a lift of points on the affin curve.

The curve $E$ has 24 affin $\mathbb{F}_{16}$-rational points. Let $P_\infty$ be the point at infinit on $\boldsymbol{E}$. If we use the basis $\{1, \boldsymbol{x}, \boldsymbol{y}\}$ for the global sections of $\mathcal{O}_{\boldsymbol{E}}(3P_\infty)$ on $\boldsymbol{E}$, 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 $\{1, \boldsymbol{x}\}$) at the lifts of only half the points, we get a pretty good code. In particular, it is easy to see that the affin $F_{16}$-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 $\boldsymbol{x}$ 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 $\boldsymbol{X}$ be the Hermitian curve define by

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

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 $X$ define by the equation

$$y_0^qz_0+y_0z_0^q=x_0^{q+1}.$$

The equation $F(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{y}^q+\boldsymbol{y}-\boldsymbol{x}^{q+1}=0$ define an open affin subset $\boldsymbol{U}$ of $\boldsymbol{X}$, and the equation $F_0(x_0,y_0)=y_0^q+y_0-x_0^{q+1}$ define an open affin subset $U$ of $X$. Notice also that $X=U\cup\{P_\infty\}$, where $P_\infty$ is the unique point at infinit on $X$. Fix a $W_2(\mathbb{F}_{p^m})$-point $Z_\infty$ of $\boldsymbol{X}$ containing $P_\infty$.

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 $\boldsymbol{X}$ and the divisor $rZ_\infty$ to construct a free code $C$ over $W_2(\mathbb{F}_{p^m})$ having length $n$, rank $r+1-(q(q-1)/2)$, 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 IV.2, we know that there is a "lift of points" $\lambda: X(\mathbb{F}_{p^m})\setminus\{P_\infty\}\to\boldsymbol{X}(W_2(\mathbb{F}_{p^m}))$ 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 $g:=q(q-1)/2\geq 2$, 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 $\lambda$ given by

$$\lambda((x_0,y_0))=((x_0,x_1),(y_0,y_1))$$

where $x_1$ is any constant $c$ and

$$y_1=cx_0^{pq}+(1/p)((y_0^q+y_0)^p-y_0^{pq}-y_0^p)$$

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 $\lambda$ is "good," in the sense that it satisfie the conditions of the conclusion of Theorem IV.2.

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

$$\boldsymbol{x}^i\boldsymbol{y}^j=\left(x_0^iy_0^j,\, jx_0^{pi}y_0^{p(j-1)}y_1+ix_0^{p(i-1)}y_0^{pj}x_1\right).$$

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 III.5 and using the fact that $\gamma(r)\geq pr$ for all $p$, we see that if $\boldsymbol{f}\in L(rZ_\infty)$, then

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

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 V.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, $p^m+1+p(p-1)p^{m/2}$ if $m\equiv 2 \pmod 4$, and $p^m+1-p(p-1)p^{m/2}$ if $4|m$, so we shall fi $m\equiv 2\pmod 4$. Choosing $r$ with $p(p-1)<r<n:=p^m+p(p-1)p^{m/2}$, we construct a free $W_2(\mathbb{F}_{p^m})$-code $C$ of length $n$, rank $r+1-(p(p-1)/2)$, 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

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

elements and minimum squared Euclidean weight at least

$$\begin{aligned}&2n-2(p^3+pr-2p+1)p^{m/2}\\&\quad=2\left(p^m+1-(p^3-p^2-p+pr+1)p^{m/2}\right).\end{aligned}$$


## ACKNOWLEDGMENT

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. J.*, vol. 82, pp. 349–367, 1996.

[2] V. D. Goppa, "Codes associated with divisors," *Probl. Pered. Inform.*, vol. 13, pp. 33–39, 1977; English translation in *Probl. Inform. Transm.*, vol. 13, pp. 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, Mar. 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 field and a conjecture of Serge Lang," in *Algebraic Geometry* (Lecture Notes in Mathematics, vol. 1016). Berlin, Germany: Springer-Verlag, 1983, pp. 1–19.

[9] J.-P. Serre, *Local Fields* (Graduate Texts in Mathematics, vol. 67) New York: Springer-Verlag, 1979.

[10] H. Stichtenoth, *Algebraic Function Fields and Codes.* Berlin, Germany: Springer, 1993.

[11] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes.* Dordrecht, The Netherlands: Kluwer, 1991.

[12] M. A. Tsfasman, S. G. Vlăduţ, 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] ——, "Lee weights of $\mathbb{Z}/4\mathbb{Z}$-codes from elliptic curves," *Codes, Curves, and Signals: Common Threads in Commun.*, to be published.

[16] J. L. Walker, "Algebraic geometric codes over rings," Ph.D. dissertation, Univ. Illinois, 1996.

[17] ——, "Algebraic geometric codes over rings," *J. Pure Appl. Alg.*, to be published.

[18] ——, "The Nordstrom–Robinson code is algebraic geometric," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1588–1593, Sept. 1997.