Euclidean weights of codes from elliptic curves over rings

José Felipe Voloch and Judy L. Walker

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 certain exponential sums and some results on canonical lifts of elliptic curves. These results may be of independent interest.

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. Such codes are used in applications where one transmits information through noisy channels. By building redundancy into the code, transmitted messages can be recovered at the receiving end. A code has parameters that measure its efficiency and error-correcting capability. 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. ([HKCSS]) 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 [G]; see [St] or [TV] for instance. In [TVZ], 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 local Artinian rings and shown, for instance, that the Nordstrom-Robinson code can be obtained from her construction followed the Gray mapping; see [W1] and [W2]. 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 this paper we consider the second author's construction in the special case of elliptic curves which are defined over finite local rings and which are the canonical lifts of their reductions. (See section 4 for more about canonical lifts.) For these codes, the missing parameter can be estimated and we do so.

Another application of our construction is to obtain low-correlation sequences suitable for use in code-division multiple access (CDMA) schemes, which are used when multiple users need to share a common communication channel, such as in the case of cellular telephones. We will use our results to obtain such sequences. In a way, our results are the analogues for elliptic curves of the results of Kumar et al. ([KHC]), which can be viewed as being for the multiplicative group. Since we can work with any ordinary elliptic curve over a finite field, our results are more flexible.

This paper is organized as follows. In section 2 we recall the main results of [W1] on the construction of codes from curves over rings and review the definitions pertaining to error-correcting codes. We also set the stage in this section for the results we need. In section 3 we prove a general estimate for certain exponential sums along curves. This result extends a number of recent results but, paradoxically, is based on an old paper of H. L. Schmid. In section 4 we prove a number of results about canonical lifts of elliptic curves. Finally, in section 5, we put everything together, obtaining our main results and their applications.

2. Algebraic geometric codes over rings

In [W1], the idea of algebraic geometric codes over rings other than fields is introduced, and foundational results about these codes are proven. In [W2], the methods of [W1] are used to explicitly construct the $\mathbb{Z}/4$-version of the Nordstrom-Robinson code as an algebraic geometric code. In order to construct other codes over $\mathbb{Z}/4$ 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 [W1] 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 $A/\mathfrak{m} = \mathbb{F}_q$. 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. Let G be a (Cartier) divisor on $\mathbf{X}$ such that no P_i is in the support of G, and let $\mathcal{L} = \mathcal{O}_{\mathbf{X}}(G)$ be the corresponding line bundle. For each i, $\Gamma(Z_i, \mathcal{L}|_{Z_i}) \simeq A$, and thinking of elements of $\Gamma(\mathbf{X}, \mathcal{L})$ as rational functions on $\mathbf{X}$, we may think of the composition $\Gamma(\mathbf{X}, \mathcal{L}) \to \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A$ as evaluation of these functions at Z_i. Summing over all i, we have a map $\gamma : \Gamma(\mathbf{X}, \mathcal{L}) \to \bigoplus \Gamma(Z_i, \mathcal{L}|_{Z_i}) \to A^n$, given by $f \mapsto (f(Z_1), \ldots, f(Z_n))$.

Definition 2.1. 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 [W1].

Theorem 2.2. *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 $n - \deg \mathcal{L}$. Further, under the additional assumption that A is Gorenstein, the class of algebraic geometric codes is closed under taking duals. In particular, there exists a line bundle $\mathcal{E}$ such that $C^{\perp} = C(\mathbf{X}, \mathcal{Z}, \mathcal{E})$.*

Remark 2.3. The dimension and minimum Hamming distance computations are consequences of the Riemann-Roch Theorem, and it is here that the assumption $2g - 2 < \deg \mathcal{L} < n$ is used. The duality result follows from a generalized version of the Residue Theorem which holds for Gorenstein rings. See [W1] for details.

The following result will be useful in section 5.

Lemma 2.4. *Let A, $\mathbf{X}$, and $\mathcal{L}$ be as in Theorem 2.2. Let $\mathbf{K}$ be the total quotient ring of rational functions on $\mathbf{X}$, and let $\mathbf{L} = \Gamma(\mathbf{X}, \mathcal{L})$. Define $p^{-1}\mathbf{L} = \{\mathbf{g} \in$*

$\mathbf{K} \mid p\mathbf{g} \in \mathbf{L}\}$. *Then* $p^{-1}\mathbf{L} = \mathbf{L} + \ker(\beta)$, *where* β *is the map* $\mathbf{K} \to \mathbf{K}$ *given by multiplication by* p.

Proof. Consider the map of the short exact sequence $0 \to \mathbf{L} \to \mathbf{K} \to \mathbf{K}/\mathbf{L} \to 0$ to itself given by multiplication by p. By the Snake Lemma, the kernels and cokernels fit into an exact sequence. But it is shown in [W1] that $\mathbf{L} \otimes_A A/m = \Gamma(X, \mathcal{L}')$, where $\mathcal{L}'$ is the pullback of $\mathcal{L}$ to X. This means that the cokernels form a short exact sequence by themselves, so the kernels must also. To set up notation, let $\gamma : \mathbf{K}/\mathbf{L} \to \mathbf{K}/\mathbf{L}$ be multiplication by p, let π_0 be the surjection $\ker(\beta) \to \ker(\gamma)$, and let π be the surjection $\mathbf{K} \to \mathbf{K}/\mathbf{L}$. With this notation, $p^{-1}\mathbf{L} = \ker(\pi\beta) = \ker(\gamma\pi)$.

Let $\mathbf{g} \in p^{-1}\mathbf{L}$. Then $\pi(\mathbf{g}) \in \ker(\gamma)$. Since π_0 is surjective, there is some $\mathbf{g}' \in \ker(\beta)$ with $\pi_0(\mathbf{g}') = \pi(\mathbf{g})$. But then $\pi(\mathbf{g} - \mathbf{g}') = 0$, so $\mathbf{g} - \mathbf{g}' \in \mathbf{L}$. In other words, there is some $\mathbf{f}' \in \mathbf{L}$ with $\mathbf{g} = \mathbf{f}' + \mathbf{g}'$, which is precisely what we needed to show.

For applications, one is usually concerned with constructing codes over $\mathbb{Z}/4$, or more generally, over rings of the form $\mathbb{Z}/p^l$, 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 $A = \mathbb{Z}/p^l$ in the definition of algebraic geometric codes above. Alternatively, we can construct an algebraic geometric code over $GR(p^l, m)$ and look at the associated trace code over $\mathbb{Z}/p^l$. Here, $GR(p^l, m)$ denotes the degree $m \geq 1$ Galois extension of $\mathbb{Z}/p^l$ (see, for example, [KHC] for details). It is easily seen that such a ring is isomorphic to the ring of length l Witt vectors over the field $\mathbb{F}_{p^m}$, and this representation is used in sections 3 and 4 below. In particular, there is a trace map $T : GR(p^l, m) \to \mathbb{Z}/p^l$, and by the trace code of a code, we mean the code obtained by applying this trace map coordinatewise to the codewords.

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

For linear codes over rings of the form $\mathbb{Z}/p^l$, 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 $\mathbb{Z}/p^l$ 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 2.5. 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 $\mathbb{Z}/p^l$, 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 $(\mathbb{Z}/p^l)^n$ 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 $(\mathbb{Z}/p^l)^n$ has squared Euclidean weight at least this.

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

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

Hence, to find a lower bound on the minimum Euclidean weight of a linear code over $\mathbb{Z}/p^l$, 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 $x \in \mathbb{Z}/4$. From this we see that the Euclidean weight of a codeword over $\mathbb{Z}/4$ 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 $(\mathbb{Z}/4)^n$ is either 0, n, or $2n$.

Finally, let C be an algebraic geometric code over $GR(p^l, m)$, and let $T : GR(p^l, m) \to \mathbb{Z}/p^l$ 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 $\mathbb{Z}/p^l$. Codewords in $T(C)$ are of the form $(T(f(Z_1)), \ldots, T(f(Z_n)))$, where f is a rational function on some curve $\mathbf{X}$ defined over $GR(p^l, m)$ and $Z_1, \ldots, Z_n$ are $GR(p^l, m)$-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

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

We investigate this sum in sections 3 and 4 below.

3. Exponential sums

In this section we will give estimates for some kinds of exponential sums along curves. The approach follows the classical method of relating the exponential sum to the sum of the reciprocals of the zeros of an L-function and applying the Riemann hypothesis. Of course the abstract set-up is well-known in even greater generality

(see, for example, [D]), but it is the calculation of the degree of the L-function that requires working out. We will be dealing with characters of order p^l, where p is the characteristic. In this case, the degree of the L-function was computed by Schmid [S1], [S2].

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 as in section 2, 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 3.1. *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*

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

Proof. As mentioned above, the essential steps are done in [S1], [S2], but we will repeat them here for the reader's convenience. Consider the Artin-Schreier-Witt extension $Y : F(\mathbf{y}) - \mathbf{y} = \mathbf{f}$ of X, which is a cover of X with Galois group contained in $\mathbb{Z}/p^l\mathbb{Z}$. Assume first it is a geometric cover, i.e., that there is no constant field extension, and that it has positive degree. If χ is a character of the Galois group then we can form the (Artin) L-function $L(X, \chi, t)$. As long as $\chi \neq 1$, $L(X, \chi, t)$ is a polynomial in t of a certain degree B_χ satisfying

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

with equality holding if χ is injective (see [S1], [S2], and especially [S2], Satz 8). When $\chi = 1$, $L(X, \chi, t)$ is the zeta function of X. Taking the product over all

characters χ of the Galois group of Y/X, $\prod L(X,\chi,t)$ is the zeta function of Y. From this our bound will follow since, by the general theory (e.g. [S2](2.7)), $S_{\mathbf{f},\mathbb{F}_q} = \sum_{P\in X_0(\mathbb{F}_q)} \chi(P)$ for a character χ, where $\chi(P)$ means χ evaluated at the Frobenius substitution of P. Also, $\sum_{P\in X_0(\mathbb{F}_q)} \chi(P)$ equals the negative of the sum of the reciprocals of the roots of $L(X,\chi,t)$ and these roots have absolute value $q^{-1/2}$ by the Riemann hypothesis.

We now treat the case where Y is not necessarily a geometric cover of X. Let $L = K(\mathbf{y})$ so L/K is cyclic. Now if $\mathbb{F}_q$ is not algebraically closed in L, then L contains $k = \mathbb{F}_{q^p}$. Set $M = Kk \subset L$, so that $[M : K] = [k : \mathbb{F}_q] = p$. Since L is cyclic, the intermediate field extension of degree p over K is unique, so we have $M = K(y_0)$. Thus $K(y_0)/K$ is a constant field extension, which implies that $f_0 = g^p - g + a$ for some $g \in K$ and $a \in \mathbb{F}_q$. Letting $\mathbf{g} = (g, 0, \dots, 0) \in W_l(K)$ and $\mathbf{a} = (a, 0, \dots, 0) \in W_l(\mathbb{F}_q)$, we can find $\mathbf{h} \in W_{l-1}(K)$ such that $\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + \mathbf{a} + p\mathbf{h}$. Then

$$S_{\mathbf{f},\mathbb{F}_q} = e^{2\pi i T(\mathbf{a})} \sum_{P\in X_0(\mathbb{F}_q)} e^{2\pi i T(\mathbf{h}(P))/p^{l-1}}.$$

Notice that if $\mathbf{h} = F(\mathbf{k}) - \mathbf{k} + \mathbf{d}$ with $\mathbf{k} \in W_{l-1}(K)$ and $\mathbf{d} \in W_{l-1}(\mathbb{F}_q)$, then $\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + \mathbf{a} + p(F(\mathbf{k}) - \mathbf{k} + \mathbf{d}) = F(\mathbf{g} + p\mathbf{k}) - (\mathbf{g} + p\mathbf{k}) + (\mathbf{a} + \mathbf{d})$, which contradicts the hypothesis of the theorem. Therefore, we can assume by induction on l that $|S_{\mathbf{f},\mathbb{F}_q}| \le Cq^{1/2}$, with

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

where $m_{ij} = -v_j(h_i)$. Further, a computation gives $m_i \le \max\{p^{i-j} n_j \mid 0 \le j \le i+1\}$, so in fact

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

and from this the theorem follows.

Remark 3.2. There has been some recent interest on exponential sums of the kind considered in the above theorem, in the case of $\mathbb{P}^1$, see Kumar et al. ([KHC]) and Li ([L]). These authors use elements of $W_l(\mathbb{F}_q)[x]$ instead of $W_l(\mathbb{F}_q[x])$, to form

their exponential sums. The latter is a bigger ring but, for exponential sums, it doesn't matter. W. Li has informed us that their results can be deduced from the above theorem. In any rate, we can recover directly the applications in [KHC] to low-correlation sequences by following the same procedure of section 5, replacing the elliptic curve by the multiplicative group.

4. Canonical liftings

Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$. Then E has a canonical lifting to an elliptic curve over $W(\mathbb{F}_q)$ for which the Frobenius of E also lifts. This is a special case of the Serre-Tate theory (see [LST] or [K]). If $\mathbf{E}$ denotes the lift of E to $W(\mathbb{F}_q)$, there is also an injective homomorphism $\tau : E(\bar{\mathbb{F}}_q) \to \mathbf{E}(W(\bar{\mathbb{F}}_q))$ (analogous to the Teichmüller lift for $\mathbb{G}_m$), compatible with the action of Frobenius, which we will call the elliptic Teichmüller lift (see [Bu2]). In fact, a characterization of the canonical lift is the existence of such a homomorphism. We will recall its construction below.

On the other hand $\mathbf{E}$ has a Greenberg transform $G(\mathbf{E})$ which is an infinite-dimensional scheme over $\mathbb{F}_q$, together with a map $\gamma : \mathbf{E}(W(\bar{\mathbb{F}}_q)) \to G(\mathbf{E})(\bar{\mathbb{F}}_q)$. Our purpose is to compute the degrees of the Witt coordinate functions of $\gamma \circ \tau$. By [Bu2] we know that $\gamma \circ \tau$ actually corresponds to a section of the canonical morphism of $\mathbb{F}_q$-schemes $G(\mathbf{E}) \to E$. By abuse of language, we will often identify $\mathbf{E}$ and $G(\mathbf{E})$ in what follows.

Theorem 4.1. *Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and $\mathbf{E}$ the canonical lift of E to $W(\mathbb{F}_q)$. Let $\mathbf{G}$ be an effective Cartier divisor on $\mathbf{E}$ and G its restriction to E. Let $\mathbf{f}$ be a global section of $\mathcal{O}_{\mathbf{E}}(\mathbf{G})$. Then for $P \in E, P \notin \operatorname{supp} \mathbf{G}$, $\mathbf{f}(\tau(P)) = (f_0(P), f_1(P), \dots)$ as a Witt vector, where f_i is a global section of $\mathcal{O}_E((2p)^i G)$ for $i = 0, 1, \dots$.*

Proof. A procedure for computing the f_i's is given in [Bu1], Lemmas 2.6 and 2.7. First one computes the p-jet coordinates, g_i say, which are reduction modulo p of $\delta^i \mathbf{f}$, where $\delta u = (u \circ \phi - u^p)/p$ is a p-derivation on the structure sheaf of $\mathbf{E}/W(\mathbb{F}_q)$ and ϕ is the lift of Frobenius on $\mathbf{E}/W(\mathbb{F}_q)$, as follows from Lemma

2.7 of [Bu1] together with [Bu2]. As ϕ is an isogeny of degree p, it follows that $\deg \delta u$ is at most $2p \deg u$ and therefore, by induction $\deg g_i \leq (2p)^i \deg G$. Now, from Lemma 2.6 of [Bu1], $f_i + P_i(f_0, \ldots, f_{i-1}) = g_i$, for universal polynomials P_i computed in the proof there. On the other hand, it is clear that the f_i are regular away from $\operatorname{supp} G$ and thus so are the g_i. Using the proof of Lemma 2.6 of [Bu1], one can show that $P_n(zf_0, z^p f_1, \ldots, z^{p^{n-1}} f_{n-1}) = z^{p^n} P_n(f_0, f_1, \ldots, f_{n-1})$ for $z \in K$, so that monomials of $P_n(f_0, f_1, \ldots, f_{n-1})$ are of the form $f_0^{i_0} f_1^{i_1} \ldots f_{n-1}^{i_{n-1}}$, with $i_0 + pi_1 + \ldots p^{n-1} i_{n-1} = p^n$. This implies that $\deg(P_n(f_0, f_1, \ldots, f_{n-1})) \leq \max\{p^{n-i} \deg f_i | 0 \leq i \leq n-1\}$. A straightforward induction argument now gives $\deg f_i \leq (2p)^i \deg G$ and the theorem then follows.

Suppose that $\mathbf{x}, \mathbf{y}$ are coordinates of a Weierstrass equation for $\mathbf{E}$. The above proof then produces functions $x_0, x_1, \ldots, y_0, y_1, \ldots$ on E such that x_0, y_0 are the coordinates of the reduced Weierstrass equation for E and

$$\tau((x_0, y_0)) = ((x_0, x_1, \ldots), (y_0, y_1, \ldots)).$$

By reducing modulo p^l, we can consider the canonical lift of E to $W_l(\mathbb{F}_q)$. The following proposition gives us tools to help explicitly calculate this in the important case $l = 2$.

Proposition 4.2. *Let k be a perfect field of characteristic $p > 0$ and E/k an ordinary elliptic curve. If $\mathbf{E}$ is the canonical lift of E to $W_2(k)$, then $\deg x_1 < 3p, \deg y_1 < 4p$. Conversely, let $\mathbf{E}$ be any elliptic curve defined over $W_2(k)$ with reduction E. Assume that the projection given by reduction from $G(\mathbf{E})$ to E admits a section τ in the category of k-schemes over $E \setminus \{O\}$ (where O is the origin for the group law on E) given by $(x_0, y_0) \mapsto (\mathbf{x}, \mathbf{y}) = ((x_0, x_1), (y_0, y_1))$ where x_1, y_1 are regular away from O and satisfy $\deg x_1 < 3p, \deg y_1 < 4p$. Then τ is regular at O, $\mathbf{E}$ is the the canonical lift of E and τ is the elliptic Teichmüller lift.*

Proof. Theorem 4.1 gives that $\deg x_1 \leq 4p$ but since both $\mathbf{x} \circ \phi$ and $\mathbf{x}^p$ have a pole at the origin of $\mathbf{E}$, we actually get $\deg x_1 < 4p$. Here again, ϕ denotes the lift of Frobenius on $\mathbf{E}$. Consider the differential $\phi^*(d\mathbf{x}/\mathbf{y})/p$. As shown by Mazur [M], this is a well-defined, holomorphic differential on $\mathbf{E}$ and its reduction modulo

p, ω say, depends only on dx/y. Moreover $C(\omega) = dx/y$, where C is the Cartier operator. Hence $\omega = A^{-1}dx/y$, where A is the Hasse invariant of E. On the other hand, from the proof of Theorem 4.1,

$$\frac{1}{p}\phi^*(\frac{d\mathbf{x}}{\mathbf{y}}) = \frac{1}{p}\frac{d(\mathbf{x}^p + px_1)}{\mathbf{y}^p + py_1} = \frac{x_0^{p-1}dx_0 + dx_1}{y_0^p}.$$

This gives $dx_1/dx_0 = A^{-1}y_0^{p-1} - x_0^{p-1}$, which is a polynomial in x_0 of degree $3(p-1)/2$. Since $\deg x_1 < 4p$, this determines x_1 up to a linear combination of 1 and x_0^p and thus x_1 is a polynomial in x_0 of degree $(3p-1)/2$, hence $\deg x_1 < 3p$. Examining the Weierstrass equation for $\mathbf{E}$ gives the bound for y_1.

To show the converse, first we need to show that τ is regular at O and $\tau(O) = \mathbf{O}$, where $\mathbf{O}$ is the origin for the group law on $\mathbf{E}$. It is enough to show that $\mathbf{x}/\mathbf{y}$ is regular at $\mathbf{O}$ and that $\mathbf{x}/\mathbf{y}(\mathbf{O}) = 0$. A computation gives $\mathbf{x}/\mathbf{y} = (x_0/y_0, x_1/y_0^p - y_1x_0^p/y_0^{2p})$ and both x_1/y_0^p and $y_1x_0^p/y_0^{2p}$ vanish at O, since $\deg x_1 < 3p, \deg y_1 < 4p$.

Fix $P_0 \in E, P_0 \neq O$ and consider $f(P) = \tau(P + P_0) - \tau(P) - \tau(P_0)$. So f is a morphism from E to $\ker(G(\mathbf{E}) \to E)$. However E is projective and $\ker(G(\mathbf{E}) \to E)$ is affine, so f is constant. But $f(O) = \mathbf{O}$ so $f = \mathbf{O}$ and τ is a homomorphism. From the definition of the canonical lift, this forces $\mathbf{E}$ to be the canonical lift of E. Finally if τ' is the elliptic Teichmüller lift then $\tau - \tau'$ is a morphism from E to $\ker(G(\mathbf{E}) \to E)$. And $(\tau - \tau')(O) = \mathbf{O}$, so by the same argument as above, $\tau = \tau'$.

Remark 4.3. Applying Proposition 4.2 we can check the following examples of canonical lifts. If $\mathbf{E}$ is given by $\mathbf{y}^2 + \mathbf{xy} = \mathbf{x}^3 - \mathbf{x}^2 - 2\mathbf{x} - 1$ over $W(\bar{\mathbb{F}}_2)$, then it is the canonical lift of its reduction modulo two. A computation gives $x_1 = 1, y_1 = x_0^2(1 + y_0)$. More generally, if k is a field of characteristic 2 and $a \in k, a \neq 0$, consider the elliptic curve E/k given by $y_0^2 + x_0y_0 = x_0^3 + a$. Its canonical lift to $W_2(k)$ is $\mathbf{y}^2 + \mathbf{xy} = \mathbf{x}^3 + (a, a^2)$ and the elliptic Teichmüller lift is given by $\mathbf{x} = (x_0, a), \mathbf{y} = (y_0, (x_0^2 + x_0)y_0 + x_0^3 + ax_0^2 + a)$. The canonical lift to $W_2(k)$ of $y_0^2 = x_0^3 + x_0^2 + a$ over a field k of characteristic three is $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 + (a, 0)$ and the elliptic Teichmüller lift is $\mathbf{x} = (x_0, x_0^4 + (1-a)x_0^3 + ax_0 - a^2), \mathbf{y} = (y_0, x_0^2y_0)$. For another example, $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}$ is the canonical lift of its special fiber in characteristic five and the elliptic Teichmüller lift to W_2 is given by $(x_0, y_0) \mapsto (\mathbf{x}, \mathbf{y}) = ((x_0, x_1), (y_0, y_1))$ where $x_1 = 4x_0^7 + x_0^3, y_1 = y_0(x_0^8 + 2x_0^6 + 2x_0^4 + x_0^2 + 3)$. These

examples show that the bounds in Proposition 4.2 on $\deg x_1$ and $\deg y_1$ cannot be any smaller.

Corollary 4.4. *Notation as in the theorem. If* $\mathbf{f} \circ \tau \neq F(\mathbf{g}) - \mathbf{g} + \mathbf{c}$, *for any* $\mathbf{g} \in W_l(K), \mathbf{c} \in W_l(\mathbb{F}_q)$, *then*

$$|\sum_{P \in E_0(\mathbb{F}_q)} e^{2\pi i T(\mathbf{f}(\tau(P)))/p^l}| \leq ((2p)^{l-1} \deg G + 1) q^{1/2}.$$

Proof. Combine Theorem 3.1 with Theorem 4.1.

Remark 4.5. If $\mathbf{E}/W_2(k)$ is the lift of an elliptic curve E/k given by a Weierstrass equation with coordinates $\mathbf{x}, \mathbf{y}$, the global sections of $\mathcal{O}_{\mathbf{E}}(r\mathbf{O})$ are of the form $A + B\mathbf{y}$, where A, B are polynomials in $\mathbf{x}$ of degrees at most $[r/2], [(r-3)/2]$ respectively. It follows from the examples in remark 4.3 that, in the situation of Theorem 4.1 in characteristic two, we have $\deg f_1 \leq 2r+1$, which improves slightly on the bound $4r$ coming from Theorem 4.1. Correspondingly, we can improve the bound in the above corollary to $(2r+2)q^{1/2}$.

Remark 4.6. It follows from [Bu1], Propositions 1.7 and 1.8, that, if there is a section of the reduction map from a projective curve $\mathbf{X}/W(\mathbb{F}_q)$ to its special fibre $X/\mathbb{F}_q$ then X is of genus zero or one. If the genus is zero then the section exists. If the genus is one and X is ordinary the section exists if and only if $\mathbf{X}$ is the canonical lift of X, hence the restrictions in the above result. It is possible to obtain sections of reductions of affine curves over Witt vectors of finite length, but the degree of the sections grow much faster than that given by the above theorem, so the bounds are correspondingly worse.

5. Applications

We now return to the study of Euclidean weights of algebraic geometric codes defined using elliptic curves over Galois rings. In order to apply the results of sections 3 and 4 above, we make a few extra assumptions. Let $\mathbf{E}$ be an elliptic curve defined over the Galois ring $A = GR(p^l, m) = W_l(\mathbb{F}_q)$, where $q = p^m$. Let E be the fiber of $\mathbf{E}$ over the closed point of $\operatorname{Spec} A$, i.e., the reduction modulo p of $\mathbf{E}$.

Then E is an elliptic curve over $\mathbb{F}_q$. We now make the additional assumptions that E is ordinary and that $\mathbf{E}$ is the canonical lift of E to A (by which we mean the reduction modulo p^l of the canonical lift of E to $W(\mathbb{F}_q)$, as discussed in section 4.)

Let Z_0 be an A-point on $\mathbf{E}$ and let P_0 be the corresponding $\mathbb{F}_q$-rational point of E. Set $E_0 = E \setminus \{P_0\}$. Let $\{P_1, \ldots, P_n\} = E_0(\mathbb{F}_q)$, and let $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$, where $Z_i = \tau(P_i)$ for $i = 1, \ldots, n$ and τ is the canonical lifting of points from section 4. Let $r \geq 1$ and set $\mathcal{L} = \mathcal{O}_{\mathbf{E}}(rZ_0)$.

Theorem 5.1. *Let A, $\mathbf{E}$, $\mathcal{Z}$, $\mathcal{L}$ be as above. Let $C = C_A(\mathbf{E}, \mathcal{Z}, \mathcal{L})$, and let $T : A \to W_l(\mathbb{F}_p) = \mathbb{Z}/p^l$ denote the absolute trace map. Then the minimum squared Euclidean weight of $T(C)$ satisfies*

$$w_E^2(T(C)) \geq min\{2n - ((2p)^{l-1}r + 1)p^{\frac{m}{2}}, 4n\frac{\pi^2}{p^{2l}}(1 + \frac{\pi^2}{3p^{2l}})\}.$$

Proof. Simply choose the group law for $\mathbf{E}$ so that Z_0 is the origin and hence P_0 is the origin for E. Then this theorem is a direct consequence of Corollary 4.4. Indeed, we need only to bound the Euclidean weight of the images of those $\mathbf{f}$ of the form $F(\mathbf{g}) - \mathbf{g} + \mathbf{c}$, where $\mathbf{g} \in W_l(K), \mathbf{c} \in W_l(\mathbb{F}_q)$. In this case, $(T(\mathbf{f}(P_1)), \ldots, T(\mathbf{f}(P_n)))$ is a constant vector so the bound follows from the discussion in section 2.

Corollary 5.2. *Use the same notation as above, but now assume that $p = l = 2$, so that $T(C)$ is a code over $\mathbb{Z}/4$. Then the minimum Lee weight of $T(C)$, and hence the minimum Hamming weight of $\varphi(T(C))$, where φ is the Gray map described in the introduction, satisfies*

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

Proof. Immediate from Remark 4.5, since $w_H(\varphi(T(C))) = w_L(T(C)) = \frac{1}{2}w_E^2(T(C))$, as explained in section 2.

Our methods can also be used to construct low-correlation sequences for use in CDMA (Code Division Multiple Access) communications systems, which are used in applications such as cellular telephones. For details on this, the reader is referred to [KHC] and the references therein. We include here only a very brief overview

of the basic idea. We consider infinite sequences of period n with symbols in $\mathbb{Z}/p^l$. The idea is to form a large family of such sequences which are pairwise cyclically distinct (i.e. no sequence is a shift of any other) and which have small correlation. Here the correlation $c_{st}(\Delta)$ between sequences $s = \{s(j)\}$ and $t = \{t(j)\}$ of period n for shift Δ is

$$c_{st}(\Delta) = \left| \sum_{j=0}^{n-1} e^{\frac{2\pi i(s(j+\Delta)-t(j))}{p^l}} \right|$$

One measures whether or not a family of sequences is good by considering the maximum correlation parameter

$$C_{\max} = \max\{c_{st}(\Delta) \,|\, s, t \in \mathcal{F} \text{ and either } s \neq t \text{ or } \Delta \neq 0\}.$$

In applications, the large family size allows for a large number of users and a small correlation parameter translates to little interference from one user to another.

A family of sequences can be constructed as follows. Take $\mathbf{E}$ as above and assume that $E(\mathbb{F}_q)$ is cyclic of order n, and let P be its generator. Let $\mathbf{G}$ be a Cartier divisor on $\mathbf{E}/W_l(\mathbb{F}_q)$ consisting of the Galois orbit of the lift of a point of E having degree r. In particular, $\mathbf{G}$ is a sum of distinct points and so is its reduction G. We will assume that $(r, n) = 1$ and the following lemma will be useful in the proof of Theorem 5.4 below.

Lemma 5.3. *Let $E/\mathbb{F}_q$ be an elliptic curve with n rational points and let r be an integer, $(r, n) = 1$. For any point of E of degree r over $\mathbb{F}_q$ and for any σ in the Galois group of $\mathbb{F}_q(P)/\mathbb{F}_q$, we have that $P^\sigma - P \notin E(\mathbb{F}_q) \setminus \{O\}$.*

Proof. Let σ be of order $d|r$. If $P^\sigma - P = P_0 \in E(\mathbb{F}_q)$, then

$$O = P^{\sigma^d} - P = \sum_{i=1}^{d} P^{\sigma^i} - P^{\sigma^{i-1}} = \sum_{i=1}^{d} (P^\sigma - P)^{\sigma^{i-1}} = dP_0.$$

However, since d is coprime to n, this implies $P_0 = O$, proving the lemma.

For each class in $\Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(\mathbf{G}))/W_l(\mathbb{F}_q)$, choose a representative $\mathbf{f}$ in $\Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(\mathbf{G}))$ and define the sequence $s_{\mathbf{f}}(j) = T(\mathbf{f}(\tau(jP_1)))$.

Theorem 5.4. *Let $\mathcal{F}$ be the family of sequences defined above. Then the maximum correlation parameter $C_{\max}$ of $(\mathcal{F})$ satisfies*

$$C_{\max} \leq 1 + ((2p)^{l-1} 2 \deg \mathbf{G} + 1) p^{\frac{m}{2}}.$$

Furthermore, if $\deg \mathbf{G}$ *and the above bound for* $C_{\max}$ *are both less than* n*, then* $|\mathcal{F}| = q^{l(\deg \mathbf{G}-1)}$.

Proof. The correlation of $s_{\mathbf{f}}$ and $s_{\mathbf{g}}$ for shift Δ is

$$|\sum_{j=1}^{n} e^{2\pi i T(\mathbf{f}(\tau(jP_1))-\mathbf{g}(\tau((j+\Delta)P_1)))/p^l}|.$$

Consider the automorphism α of $\mathbf{E}$ given by translation by $\tau(\Delta P_1)$. Let $\mathbf{h} = \mathbf{f}-\mathbf{g}\circ\alpha$. The above sum is then the kind of sum considered in Corollary 4.4, say, but with $\mathbf{G}$ replaced by $\mathbf{G}+\alpha^*\mathbf{G}$. If $\mathbf{h}\circ\tau$ is not of the form $F(\mathbf{k})-\mathbf{k}+\mathbf{c}$, where $\mathbf{k} \in W_l(K)$ and $\mathbf{c} \in W_l(\mathbb{F}_q)$, then the result follows from Corollary 4.4 since the degree of the divisor $\mathbf{G}+\alpha^*\mathbf{G}$ is at most $2\deg \mathbf{G}$.

We now assume that $\mathbf{h}$ is of the type excluded by Corollary 4.4, so that $\mathbf{h} = F(\mathbf{k}) - \mathbf{k} + \mathbf{c}$ for some $\mathbf{k} \in W_l(K)$ and $\mathbf{c} \in W_l(\mathbb{F}_q)$. The first Witt coordinate of the equation $(\mathbf{f} - \mathbf{g}\circ\alpha)\circ\tau = F(\mathbf{k}) - \mathbf{k} + \mathbf{c}$ is an equation of the form $f_0 - g_0\circ\alpha = k_0^p - k_0 + c_0$. Now from our hypothesis f_0 and g_0 have simple poles so $f_0 - g_0\circ\alpha$ also has simple poles. But $k_0^p - k_0 + c_0$ won't have simple poles unless it is constant, so $f_0 - g_0\circ\alpha$ is constant.

If $\Delta \neq 0$, Lemma 5.3 ensures that G and α^*G have disjoint support and therefore f_0 and $g_0\circ\alpha$ have disjoint polar divisors unless f_0 and g_0 are both constants. Therefore, $f_0 - g_0\circ\alpha$ constant implies that f_0 and g_0 are both constants. We take the (usual) Teichmüller lifts of these constants and subtract them from $\mathbf{f}$, $\mathbf{g}$, so that we may assume that f_0, g_0 are both zero. This implies that $\mathbf{f} = p\mathbf{f}'$ and $\mathbf{g} = p\mathbf{g}'$ for some $\mathbf{f}', \mathbf{g}' \in \mathbf{K}$, where $\mathbf{K}$ is the total quotient ring of rational functions on $\mathbf{E}$. Using Lemma 2.4, we can write $\mathbf{f} = p\mathbf{f}'$, $\mathbf{g} = p\mathbf{g}'$, where $\mathbf{f}'$ and $\mathbf{g}'$ are in the space of global sections of the line bundle associated to $\mathbf{G}$. As in the proof of Theorem 3.1, we may consider $\mathbf{f}'$ and $\mathbf{g}'$ to be defined over $W_{l-1}(K)$, so we use induction. Either we have a bound for the exponential sum formed with $\mathbf{f}' - \mathbf{g}'\circ\alpha$ which is better than the bound in the statement of the theorem, or we can repeat the process and finally get that $\mathbf{f}$ and $\mathbf{g}$ are constant, and this possibility is excluded by the construction of our family.

If $\Delta = 0$, α is the identity, so $f_0 - g_0 = c_0$, a constant. In order to compute correlations, the choice of the representative $\mathbf{f}$ is immaterial, so we may subtract

from $\mathbf{f}$ the (usual) Teichmüller lift of c_0 and assume that $c_0 = 0$. As above $\mathbf{f} - \mathbf{g} = p\mathbf{h}$, for some $\mathbf{h}$ in $\Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(\mathbf{G}))$ and we can proceed by induction on l as before.

To estimate $|\mathcal{F}|$, we note that $s_{\mathbf{f}} = s_{\mathbf{g}}$ implies that the correlation of the two sequences is n, so by the above argument $\mathbf{f} - \mathbf{g}$ is a constant, hence $|\mathcal{F}| = |\Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(\mathbf{G}))|/|W_l(\mathbb{F}_q)|$. Finally, $\Gamma(\mathbf{E}, \mathcal{O}_{\mathbf{E}}(\mathbf{G}))$ is a free $W_l(\mathbb{F}_q)$-module of rank $\deg \mathbf{G}$, by Theorem 2.2.

Acknowledgments: The authors acknowledge the use of the software packages Mathematica and Pari in some calculations. The first author would also like to thank A. Buium and J. Tate for useful comments and the NSA (grant MDA904-97-1-0037) for financial support. The second author thanks Winnie Li and Patrick Solé for their useful comments and the NSF (grant DMS-9709388) for financial support.

References.

[Bu1] A. Buium, *Geometry of p-jets*, Duke Math. Journal **82** (1996), 349–367.

[Bu2] A. Buium, *An approximation property for Teichmüller points*, Math. Research Letters, **3** (1996) 453–457.

[D] P. Deligne: *Applications de la formule des traces aux sommes trigonométriques* in *Cohomologie étale (SGA* $4\frac{1}{2}$*)*, Lecture Notes in Math. 569, Springer-Verlag, Berlin, Heidelberg, New York (1977).

[G] V. D. Goppa, *Codes associated with divisors*, Probl. Peredachi Inf. **13** (1977), 33-39. (English translation in *Probl. Inf. Transm.,* 13:22-27, (1977).)

[HKCSS] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-Linearity of Kerdock, Preparata, Goethals, and Related Codes*, IEEE Transactions on Information Theory **40** (1994), 301-319.

[K] N. M. Katz, *Serre-Tate local moduli*, Springer LNM 868 (1981) 138-202.

[KHC] P. V. Kumar, T. Helleseth, and A. R. Calderbank,*An upper bound for some exponential sums over Galois rings and applications*, IEEE Transactions on Information Theory **41** (1995), 456-468.

[Li] W-C. W. Li, *Character sums over p-adic fields*, preprint (1997).

[LST] J. Lubin, J-P. Serre and J. Tate, *Elliptic curves and formal groups*, Proc. of the Woods Hole summer institute in algebraic geometry 1964. Unpublished. Available at http://www.ma.utexas.edu/users/voloch/lst.html.

[M] B. Mazur, *Frobenius and the Hodge filtration, estimates*, Ann. Math. **98** (1973) 58-95.

[S1] H. L. Schmid, *Zur Arithmetik der zyklischen p-Körper*, Crelles J., **176** (1936), 161-167.

[S2] H. L. Schmid, *Kongruenzzetafunktionen in zyklischen Körpern*, Abh. Preuss. Akad. Wiss. Math.-Nat. Kl. 1941, (1942). no. 14, 30 pp.

[St] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.

[TV] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[TVZ] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Modular curves, Shimura curves, and Goppa Codes, better than the Varshamov-Gilbert bound*, Math. Nachrichten, **109** (1982), 21-28.

[W1] J. L. Walker, *Algebraic geometric codes over rings*, submitted for publication.

[W2] J. L. Walker, *The Nordstrom Robinson code is algebraic geometric*, IEEE Transactions on Information Theory **43** (1997), 1588-1593.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu

Dept. of Mathematics and Statistics, Univ.of Nebraska, Lincoln, NE 68588-0323, USA

e-mail: jwalker@math.unl.edu