HOMOGENEOUS WEIGHTS AND EXPONENTIAL SUMS

JOSÉ FELIPE VOLOCH AND JUDY L. WALKER

Abstract. In this paper, we give a formula as an exponential sum for a homogeneous weight defined by Constantinescu and Heise [3] in the case of Galois rings (or equivalently, rings of Witt vectors) and use this formula to estimate the weight of codes obtained from algebraic geometric codes over rings.

1. Introduction

The Gray map is the isometry $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{F}_2^2$ defined by $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, and $\phi(3) = (1,0)$, where $\mathbb{Z}/4\mathbb{Z}$ is given the Lee metric and $\mathbb{F}_2^2$ the Hamming metric. It is extended to a map, again denoted by $\phi : (\mathbb{Z}/4\mathbb{Z})^n \to \mathbb{F}_2^{2n}$, by applying the previous ϕ to each coordinate. The Gray map allows us to construct (non-linear) binary codes from linear codes over $\mathbb{Z}/4\mathbb{Z}$ and this has been the subject of many recent papers (see, for example, [9] and [4]).

Carlet [2] generalized the Gray map to a bijection between $\mathbb{Z}/2^k\mathbb{Z}$ and a subset of $\mathbb{F}_2^{2^{k-1}}$, which is in fact the first-order Reed-Muller code $R(1, k-1)$. Naturally one can extend the map coordinatewise to $(\mathbb{Z}/2^k\mathbb{Z})^n$ and thus construct (non-linear) binary codes from $\mathbb{Z}/2^k\mathbb{Z}$-linear codes. Carlet also gave a formula for the weight of an element in $\mathbb{Z}/2^k\mathbb{Z}$ (obtained by pulling back the Hamming weight in $\mathbb{F}_2^{2^{k-1}}$) as an exponential sum.

Greferath and Schmidt [6] further generalized the Gray map to an arbitrary finite chain ring with a certain homogeneous weight, recalled below. They used their map to construct interesting non-linear binary codes, but did not produce a formula like Carlet's for their weight.

Date: January 17, 2003.

The first author was supported in part by NSA Grant #MDA904-00-1-0053.

The second author was supported in part by NSF Grants #DMS-001008 and #DMS-001011.

The notion of homogeneous weight was first introduced by Constantinescu and Heise ([3]) for $\mathbb{Z}/m\mathbb{Z}$ and studied further by Honold and Nechaev ([7] and [8]) and by Greferath and Schmidt [6]. The results of [7] can be used to give a formula as an exponential sum for the homogeneous weight in the case of Galois rings (or equivalently, rings of Witt vectors). The main purpose of this paper is to use this formula to estimate the weight of codes obtained from algebraic geometric codes over rings.

2. Homogeneous weights

Let $\mathbb{F}_q$ denote the finite field of q elements and let p be the characteristic of $\mathbb{F}_q$, so that $q = p^\mu$ for some μ. Let $W_\ell(\mathbb{F}_q)$ be the ring of Witt vectors of length ℓ over $\mathbb{F}_q$. The ring $W_\ell(\mathbb{F}_q)$ is a finite local ring with q^ℓ elements and maximal ideal generated by p, such that $p^\ell = 0$. It is isomorphic to the Galois ring denoted by $GR(p^\ell, \mu)$, which is the degree μ extension of $\mathbb{Z}/p^\ell\mathbb{Z} \cong W_\ell(\mathbb{F}_p)$.

One can define the Frobenius and trace maps for a ring of Witt vectors $W_\ell(\mathbb{F}_{p^\mu})$. Let $x = (x_0, x_1, \ldots, x_{\ell-1}) \in W_\ell(\mathbb{F}_{p^\mu})$. The Frobenius $F : W_\ell(\mathbb{F}_{p^\mu}) \to W_\ell(\mathbb{F}_{p^\mu})$ is given by $F(x) = F((x_0, x_1, \ldots, x_{\ell-1})) = (x_0^p, x_1^p, \ldots, x_{\ell-1}^p)$. The trace map $\mathrm{Tr} : W_\ell(\mathbb{F}_{p^\mu}) \to W_\ell(\mathbb{F}_p) \cong \mathbb{Z}/p^\ell\mathbb{Z}$ is given by $\mathrm{Tr}(x) = x + F(x) + \cdots + F^{\mu-1}(x)$.

Following Constantinescu and Heise ([3]) we define the *(homogeneous) weight* of $x \in W_\ell(\mathbb{F}_q)$ as follows:

$$\mathrm{wt}(x) := \begin{cases} 0 & \text{if } x = 0, \\ q^{\ell-1} & \text{if } x \text{ is a nonzero element of the ideal generated by } p^{\ell-1}, \\ (q-1)q^{\ell-2} & \text{otherwise.} \end{cases}$$

Note that when $\ell = 1$ this does not give the Hamming weight but $(q-1)/q$ times the Hamming weight. However, for the most part, our results are not interesting for $\ell = 1$.

It is well-known that the space of complex valued functions on any finite abelian group G has a basis consisting of characters, that is, homomorphisms $G \to \mathbb{C}^\times$. Applying this to the additive group of $W_\ell(\mathbb{F}_q)$, we see that any weight, in particular w, will be given as a

linear combination of characters. The characters of the additive group of $W_\ell(\mathbb{F}_q)$ are all of the form $x \mapsto \zeta^{\mathrm{Tr}(ax)}$, where ζ is a primitive p^ℓ-th root of unity, Tr is the trace map defined above and a runs through $W_\ell(\mathbb{F}_q)$. This is well-known, see e.g. [15] Example 4.4 (vi).

We proceed to give explicitly the (Fourier) coefficients of the expansion of the weight defined by Greferath and Schmidt as a linear combination of characters. This result follows from the results of [7], which are more general, but we will give a simple, direct proof.

Theorem 2.1. *For any x in $W_\ell(\mathbb{F}_q)$ we have*

$$w(x) = (q-1)q^{\ell-2} - \frac{1}{q}\sum_{a\in U}\zeta^{\mathrm{Tr}(ax)},$$

where U is the group of units of $W_\ell(\mathbb{F}_q)$.

Proof. Since $|U| = q^\ell - q^{\ell-1}$, the formula holds for $x = 0$. If $x = p^{\ell-1}y$ is in the ideal generated by $p^{\ell-1}$, so is ax and $\mathrm{Tr}(ax) = p^{\ell-1}\,\mathrm{Tr}(ay)$. Now, $\xi = \zeta^{p^{\ell-1}}$ is a primitive p-th root of unity and y can be taken to be in $\mathbb{F}_q^\times$ by identifying $y \in \mathbb{F}_q$ with its Teichmüller representative. Further, $p^{\ell-1}\,\mathrm{Tr}(ay)$ only depends on a modulo p and given a residue class modulo p, there are $q^{\ell-1}$ possible values of a. We now count the number of solutions $a \in \mathbb{F}_q^\times$ to the equation $\mathrm{Tr}(ay) = c \in \mathbb{F}_p$. We see that c has q/p pre-images under Tr in $\mathbb{F}_q$, which are all non-zero if c is non-zero, thus there are q/p solutions to our equation if c is non-zero. When $c = 0$, we have again q/p pre-images under Tr but one of them is the zero element of $\mathbb{F}_q$, which we exclude, and we obtain $q/p - 1$ solutions to our equation. The right-hand-side of the formula in the theorem becomes:

$$(q-1)q^{\ell-2} - \frac{1}{q}q^{\ell-1}\big(\frac{q}{p} - 1 + \frac{q}{p}\sum_{c\in\mathbb{F}_p^\times}\xi^c\big)$$

and recalling that $\sum_{c\in\mathbb{F}_p^\times}\xi^c = -1$, the last expression becomes

$$(q-1)q^{\ell-2} - q^{\ell-2}(q/p - 1 - q/p) = q^{\ell-1},$$

as desired.

If x is not in the ideal generated by $p^{\ell-1}$, then $x = p^r y$, for some unit y of $W_{\ell-r}(\mathbb{F}_q)$ and some $r < \ell - 1$. As above, we can replace ζ with ζ^{p^r} and replace x by y. Since y is a unit, we can re-index the sum so that we are left needing to show that $\sum_{a\in U} \zeta^{\mathrm{Tr}(a)} = 0$ for any $\ell > 1$. Given $c \in \mathbb{Z}/p^\ell\mathbb{Z}$, there are $(q/p)^\ell$ solutions in $W_\ell(\mathbb{F}_q)$ to $\mathrm{Tr}(a) = c$. If c is a unit, all these solutions are units, whereas if c is not a unit, only $(q/p)^\ell - (q/p)^{\ell-1}$ of these solutions are units. Thus

$$\begin{aligned}\sum_{a\in U} \zeta^{\mathrm{Tr}(a)} &= \sum_{c\in\mathbb{Z}/p^\ell\mathbb{Z}\setminus(\mathbb{Z}/p^\ell\mathbb{Z})^\times} ((q/p)^\ell - (q/p)^{\ell-1})\zeta^c + \sum_{c\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} (q/p)^\ell \zeta^c \\ &= \sum_{c\in\mathbb{Z}/p^\ell\mathbb{Z}} ((q/p)^\ell - (q/p)^{\ell-1})\zeta^c + \sum_{c\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} (q/p)^{\ell-1} \zeta^c.\end{aligned}$$

On the other hand, clearly $\sum_{c\in\mathbb{Z}/p^\ell\mathbb{Z}} \zeta^c = 0$ and we also have $\sum_{c\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} \zeta^c = 0$ since this is the $\mathbb{Q}(\zeta)/\mathbb{Q}$-trace of ζ, which is, up to sign, the coefficient of $x^{p^\ell(p-1)-1}$ in the polynomial $(x^{p^\ell} - 1)/(x^{p^{\ell-1}} - 1)$ and this coefficient is zero for $\ell > 1$. This completes the proof. □

3. Algebraic geometric codes

Generalizing the work of Goppa for codes over finite fields, the second author has constructed codes from curves over finite rings and shown, for instance, that the Nordstrom-Robinson code can be obtained from her construction followed by the Gray mapping (see [13], [14]). The authors have further studied this construction in [11], [12] and there has been further work along these lines in [1] and [5].

To construct these codes, one begins with a local Artinian ring A with finite residue field $\mathbb{F}_q$ and a curve (a connected irreducible scheme over $\operatorname{Spec} A$ which is smooth of relative dimension one) $\mathbf{X}$ defined over A. Assume that the closed fiber $X := \mathbf{X} \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q$ of $\mathbf{X}$ is absolutely irreducible, and 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 $\mathbf{G}$ be a (Cartier) divisor on $\mathbf{X}$ such that no P_i is in the support of $\mathbf{G}$, and let $\mathcal{O}_{\mathbf{X}}(\mathbf{G})$ be the corresponding line bundle. If $f \in L(\mathbf{G}) := \Gamma(\mathbf{X}, \mathcal{O}_{\mathbf{X}}(\mathbf{G}))$, we may think of f as a rational function on $\mathbf{X}$, and since each Z_i is an A-point whose specialization is not in $\mathrm{supp}(\mathbf{G})$, we have that $f(Z_i) \in A$ for $i = 1, \ldots, n$.

Definition 3.1. ([13]) Let A, $\mathbf{X}$, $\mathcal{Z}$ and $\mathbf{G}$ be as above. Then

$$C(\mathbf{X}, \mathcal{Z}, \mathbf{G}) := \{(f(Z_1), \ldots, f(Z_n)) \mid f \in L(\mathbf{G})\}$$

is the *algebraic geometric code* over A associated to $\mathbf{X}$, $\mathcal{Z}$ and $\mathbf{G}$.

The following theorem summarizes some of the main results of [13].

Theorem 3.2. ([13]) *Let $\mathbf{X}$, $\mathbf{G}$, and $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ be as above. Let g denote the genus of $\mathbf{X}$, and suppose $2g - 2 < \deg \mathbf{G} < n$. Set $C = C(\mathbf{X}, \mathcal{Z}, \mathbf{G})$. Then C is a linear code of length n over A, and is free as an A-module. The dimension (rank) of C is $k = \deg \mathbf{G} + 1 - g$, and the minimum Hamming distance of C is at least $n - \deg \mathbf{G}$.*

Remark 3.3. The minimum Hamming distance is obtained by comparing zeros and poles and the dimension computation is a consequence of the Riemann-Roch Theorem. See [13] for details.

Now restrict to the case $A = W_\ell(\mathbb{F}_q)$, as in Section 2. We see from above that if $(x_1, \ldots, x_n)$ is a codeword in $C(\mathbf{X}, \mathcal{Z}, \mathbf{G})$ for some $\mathbf{X}$, $\mathbf{G}$, and $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$ as above, then there is a function $f \in L(\mathbf{G})$ such that $x_j = f(Z_j)$ for $j = 1, \ldots, n$. The homogeneous weight of this codeword is then

$$w(x_1, \ldots, x_n) = n(q-1)q^{\ell-2} - \frac{1}{q} \sum_{j=1}^{n} \sum_{a \in U} \zeta^{\mathrm{Tr}(af(Z_j))}, \tag{1}$$

where, as before, U is the group of units of A. To find a lower bound on the minimum homogeneous weight of the code $C(\mathbf{X}, \mathcal{Z}, \mathbf{G})$, then, we need to find an upper bound on the double sum

$$\sum_{j=1}^{n} \sum_{a \in U} \zeta^{\mathrm{Tr}(af(Z_j))}, \tag{2}$$

for $f \in L(\mathbf{G})$.

For simplicity, we restrict to the case where the divisor $\mathbf{G}$ on $\mathbf{X}$ is of the form rZ for some A-point Z on $\mathbf{X}$ and some integer $r > 2g - 2$, where g is the genus of $\mathbf{X}$. We further assume that the disjoint A-points $Z_1, \ldots, Z_n$ are chosen so that $X(\mathbb{F}_q)$ is precisely $\{P_1, \ldots, P_n\} \cup \{Q\}$,

where Q is the unique closed point contained in Z and P_i is the unique closed point contained in Z_i for $i = 1, \ldots, n$.

Using the results of Section 4 below in addition to [11], [12], and [5], we can bound the sum (2) in several situations. The first step in each situation is to translate the sum from being a sum over A-points on the curve $\mathbf{X}$ defined over A, to being a sum over $\mathbb{F}_q$-points on the curve $X = \mathbf{X} \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q$, which is defined over $\mathbb{F}_q$. Doing so also changes the rational function $f \in L(\mathbf{G}) = L(rZ)$ on $\mathbf{X}$ to a Witt vector of rational functions $\mathbf{f} = (f_0, \ldots, f_{\ell-1})$, where each f_i is a rational function on X having all of its poles at Q. Then we apply the following theorem, which is a special case of a theorem in [11].

Theorem 3.4. ([11]) *Let X be a curve of genus g defined over the finite field $\mathbb{F}_q$ with function field $K := \mathbb{F}_q(X)$. Let $f_1, \ldots, f_{\ell-1} \in K$ have poles only at Q and consider the Witt vector of rational functions $\mathbf{f} := (f_0, \ldots, f_{\ell-1}) \in W_\ell(K)$. Set $X_0 = X \setminus \{Q\}$ and assume that $\mathbf{f}$ is not of the form $F(\mathbf{g}) - \mathbf{g} + c$ for any $\mathbf{g} \in W_\ell(K)$ and any $c \in W_\ell(\mathbb{F}_q)$. For $i = 1, \ldots, n$, let $\deg f_i = -v_Q(f_i)$ be the order of the pole of f_i at Q. Then*

$$\left| \sum_{P \in X_0(\mathbb{F}_q)} \zeta^{\operatorname{Tr}(\mathbf{f}(P))} \right| \leq (2g - 1 + \max\{p^{\ell-1-i} \deg f_i \mid 0 \leq i \leq \ell - 1\}\sqrt{q}.$$

4. Basic estimates

From the discussion above, it is clear that we need to understand, for each $\mathbf{f} \in W_\ell(K)$, the set

$$B(\mathbf{f}) := \{a \in U \mid a\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + c \text{ for some } \mathbf{g} \in W_\ell(K) \text{ and some } c \in W_\ell(\mathbb{F}_q)\}.$$

Notice that if $F(\mathbf{g}_1) - \mathbf{g}_1 + c_1 = F(\mathbf{g}_2) - \mathbf{g}_2 + c_2$, then $\operatorname{Tr}(c_1) = \operatorname{Tr}(c_2)$. Thus we have a well-defined function $t : B(\mathbf{f}) \to \mathbb{Z}/p^\ell\mathbb{Z}$ given by $t(a) = \operatorname{Tr}(c)$ for any c such that $a\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + c$ for some $\mathbf{g} \in W_\ell(K)$. We partition the set $B(\mathbf{f})$ into three subsets: $B(\mathbf{f}) = B_1(\mathbf{f}) \cup B_2(\mathbf{f}) \cup$

$B_3(\mathbf{f})$, where

$$B_1(\mathbf{f}) := \{a \in B(\mathbf{f}) \,|\, t(a) \notin p^{\ell-1}\mathbb{Z}/p^\ell\mathbb{Z}\},$$
$$B_2(\mathbf{f}) := \{a \in B(\mathbf{f}) \,|\, t(a) \in p^{\ell-1}\mathbb{Z}/p^\ell\mathbb{Z} \setminus \{0\}\},$$
$$B_3(\mathbf{f}) := \{a \in B(\mathbf{f}) \,|\, t(a) = 0\}.$$

The sum (2) now splits as

$$\begin{aligned} \sum_{a\in B_1(\mathbf{f})} \sum_{P\in X_0(\mathbb{F}_q)} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))} &+ \sum_{a\in B_2(\mathbf{f})} \sum_{P\in X_0(\mathbb{F}_q)} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))} \\ &+ \sum_{a\in B_3(\mathbf{f})} \sum_{P\in X_0(\mathbb{F}_q)} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))} + \sum_{a\in U\setminus B(\mathbf{f})} \sum_{P\in X_0(\mathbb{F}_q)} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))}, \end{aligned} \tag{3}$$

where $\mathbf{f}$ is the Witt vector of rational functions on X_0 corresponding to the rational function f on $\mathbf{X}$.

We will treat each of the four terms in the sum above separately, with the fourth being covered by Theorem 3.4. Note that if $a\mathbf{f} = F(\mathbf{g}) - \mathbf{g} + c$ then $ra\mathbf{f} = F(r\mathbf{g}) - r\mathbf{g} + rc$ and so for $i = 1, 2, 3$, if $a \in B_i(\mathbf{f})$ then so is ra for each $r \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$. Thus each $B_i(\mathbf{f})$ splits into $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$-orbits.

Lemma 4.1. *Let $\mathbf{f} \in W_\ell(K)$, $P \in X_0(\mathbb{F}_q)$, and $a \in B(\mathbf{f})$. Then*

$$\sum_{r\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} \zeta^{\mathrm{Tr}(ra\mathbf{f}(P))} = \begin{cases} 0 & \text{if } a \in B_1(\mathbf{f}), \\ -p^{\ell-1} & \text{if } a \in B_2(\mathbf{f}), \\ p^\ell - p^{\ell-1} & \text{if } a \in B_3(\mathbf{f}). \end{cases}$$

Proof. First note that for $a \in B(\mathbf{f})$ and $r \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$, we have $t(ra) = rt(a)$. Thus we have

$$\sum_{r\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} \zeta^{\mathrm{Tr}(ra\mathbf{f}(P))} = \sum_{r\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} \left(\zeta^{t(a)}\right)^r.$$

Suppose $a \in B_1(\mathbf{f})$. Then $pt(a) \neq 0$ and so the map $s \mapsto (\zeta^{pt(a)})^s$ is a nontrivial additive character on $p^{\ell-1}\mathbb{Z}/p^\ell\mathbb{Z}$. Thus in this case we have

$$\sum_{r\in(\mathbb{Z}/p^\ell\mathbb{Z})^\times} \left(\zeta^{t(a)}\right)^r = -\sum_{s\in\mathbb{Z}/p^{\ell-1}\mathbb{Z}} \left(\zeta^{pt(a)}\right)^s = 0.$$

If $a \in B_2(\mathbf{f})$, then $\zeta^{t(a)}$ is a primitive pth root of unity. Noting that $\sum_{r\in\mathbb{F}_p^\times} \omega^r = -1$ for any primitive pth root of unity ω gives the result in this case.

Finally, if $a \in B_3(\mathbf{f})$, then $\zeta^{t(a)} = 1$, completing the proof. □

Using the Lemma, we have that the sum (3) is at most

$$|B_3(\mathbf{f})|\,|X_0(\mathbb{F}_q)| + \left(q^\ell - q^{\ell-1} - |B_3(\mathbf{f})|\right) \max_{a\in U\setminus B(\mathbf{f})} \left| \sum_{P\in X_0(\mathbb{F}_q)} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))} \right|, \tag{4}$$

and we see we need to find $|B_3(\mathbf{f})|$.

We treat the case $\ell = 1$ first. Let X be a curve over $\mathbb{F}_q$, fix $P \in X(\mathbb{F}_q)$, and set $L(\infty P) = \cup_{r\geq 0} L(rP)$. Let $R = \{r \geq 0 \,|\, L(rP) \neq L((r-1)P)\}$, so that $L(\infty P)$ is in fact $\cup_{r\in R} L(rP)$. The set $L(\infty P)$ is an infinite-dimensional vector space over $\mathbb{F}_q$, and we wish to choose a basis for it. This basis can be indexed by R, so that the basis element f_r lives in $L(rP)$ but not in $L(sP)$ for any $s < r$ in R. In particular $\deg f_r = r$, where "deg" is understood to mean the negative of the valuation at P. Set $f_0 = 1$, and assume f_t has been chosen for all $t \in R$ with $t < r$. If r is divisible by p and $s := r/p$ is in R, set $f_r = f_s^p$. Otherwise, choose f_r arbitrarily in $L(rP) \setminus L((r-1)P)$.

Define $\phi : L(\infty P) \to L(\infty P)$ by $\phi(g) = g^p - g$. (Note that ϕ could be defined on all of $\mathbb{F}_q(X)$, but since $\phi(g) \in L(\infty P)$ if and only if $g \in L(\infty P)$, we can restrict our definition of ϕ to this set.) We are interested in the following question: Given $g \in L(\infty P)$, for how many values of $a \in \mathbb{F}_q^\times$ is $a\phi(g)$ in the image of ϕ? To this purpose define an equivalence relation on R by $r \sim r'$ if r/r' is a power of p. Call an element of $L(\infty P)$ *pure* if, in its expansion as linear combination of the f_r, non-zero coefficients occur only for r in a single equivalence class with respect to $\sim$. It is clear that every element of $L(\infty P)$ can be written as a sum of

pure functions in a unique way. From our construction of the f_r it is clear that ϕ maps pure functions to pure functions.

Proposition 4.2. *Let $g \in L(\infty P), g \notin \mathbb{F}_q$. If $\deg g = p^m e$ where either e is not divisible by p or $e/p \notin R$, then there are at most $p^{m+1} - 1$ values of $a \in \mathbb{F}_q^\times$ such that $a\phi(g)$ is in the image of ϕ.*

Proof. If we have an equation $a\phi(g) = \phi(h)$ and we decompose g and h as a sum of pure functions, we will get an equation for each of the corresponding summands. Moreover, there is a term in the decomposition of g of degree $p^m e$. It follows that we may assume that g and h are pure. Let $R_e = \{r \in R \,|\, r = p^j e, 0 \leq j \leq m\}$ and write $g = \sum_{r \in R_e} \gamma_r f_r$ and $h = \sum_{r \in R_e} \eta_r f_r$. It follows that $\eta_{p^m e}^p = a\gamma_{p^m e}^p$ and that for $1 \leq j \leq m-1$, $\eta_{p^j e}^p - a(\gamma_{p^j e}^p - \gamma_{p^{j+1} e}) = \eta_{p^{j+1} e}$ and $\eta_e = a\gamma_e$. We can successively eliminate the η's from this system of equations to obtain a polynomial equation of degree p^{m+1} in a in terms of the γ's. This polynomial equation has no constant term, and so $a = 0$ is one solution. That leaves at most $p^{m+1} - 1$ solutions in $\overline{\mathbb{F}}_p^\times$. $\square$

Now we treat the case of general ℓ. For $g = (g_0, \ldots, g_{\ell-1}) \in W_\ell(K)$, define $\phi(g) = F(g) - g$. The notation is consistent with our previous use of ϕ in the case $\ell = 1$. The following technical lemma will be useful.

Lemma 4.3. *If we write $(z_0, \ldots, z_n) = (1, 0, \ldots, 0, x_n)(y_0, y_1, \ldots, y_n)$, then $z_n \equiv y_n + x_n y_0^{p^n} \pmod{p}$.*

Proof. In general, if $(z_0, \ldots, z_n) = (x_0, \ldots, x_n)(y_0, \ldots, y_n)$, then

$$z_0^{p^n} + pz_1^{p^{n-1}} + \cdots + p^n z_n = (x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n)(y_0^{p^n} + py_1^{p^{n-1}} + \cdots + p^n y_n)$$

by definition. Plugging in $x_0 = 1$ and $x_i = 0$ for $0 < i < n$, we get

$$y_0^{p^n} + py_1^{p^{n-1}} + \cdots + p^{n-1} y_{n-1}^p + p^n z_n = (1 + p^n x_n)(y_0^{p^n} + py_1^{p^{n-1}} + \cdots + p^n y_n)$$

because $(1,0,...,0)(y_0,...,y_i) = (y_0,...,y_i)$ since $(1,0,...,0)$ is the identity for multiplication in W_n. So,

$$p^n z_n = p^n y_n + p^n x_n (y_0^{p^n} + p y_1^{p^{n-1}} + \cdots + p^n y_n).$$

Dividing by p^n we get

$$z_n \equiv y_n + x_n y_0^{p^n} \pmod{p},$$

as we wanted. □

Theorem 4.4. *Let* $\mathbf{g} = (g_0, \ldots, g_{\ell-1}) \in W_\ell(L(\infty P))$*, where* $L(\infty P)$ *is as above. Assume* $g_0 \notin \mathbb{F}_q$*. If* $\deg g_0 = p^m e$ *where either* e *is not divisible by* p *or* $e/p \notin R$*, then there are at most* $p^{(\ell-1)(m+1)}(p^{m+1}-1)$ *values of* $a \in W_\ell(\mathbb{F}_q)^\times$ *such that* $a\phi(\mathbf{g})$ *is in the image of* ϕ*.*

Proof. We proceed by induction on ℓ, with the base case given by Proposition 4.2. Suppose $a \equiv a' \pmod{p^{\ell-1}}$ and there are functions $\mathbf{h}$ and $\mathbf{h}'$ such that $a(F(\mathbf{g}) - \mathbf{g}) = F(\mathbf{h}) - \mathbf{h}$ and $a'(F(\mathbf{g}) - \mathbf{g}) = F(\mathbf{h}') - \mathbf{h}'$. Then $a'a^{-1}(F(\mathbf{h}) - \mathbf{h}) = F(\mathbf{h}') - \mathbf{h}'$, with $a'a^{-1} \equiv 1 \pmod{p^{\ell-1}}$ and $\deg h_0 = \deg g_0$. We will show that the number of $a \in W_\ell(\mathbb{F}_q)^\times$ such that $a\phi(\mathbf{g})$ is in the image of ϕ, with $a \equiv 1 \pmod{p^{\ell-1}}$, i.e., a of the form $a = (1, 0, \ldots, 0, a_{\ell-1})$ for some $a_{\ell-1} \in \mathbb{F}_q$, is at most p^{m+1}. The induction hypothesis entails that there are at most $p^{(\ell-2)(m+1)}(p^{m+1}-1)$ values of $a \in W_{\ell-1}(\mathbb{F}_q)^\times$ such that $a\phi(g_0, \ldots, g_{\ell-2})$ is in the image of ϕ and the theorem will follow.

So assume $a = (1, 0, \ldots, 0, a_{\ell-1})$ and $a\phi(\mathbf{g}) = \phi(\mathbf{h})$ for some h. Then we have $\phi(\mathbf{g}) \equiv \phi(\mathbf{h}) \pmod{p^{\ell-1}}$ and so we may assume $h_i = g_i$ for $0 \le i \le \ell - 2$. The last coordinate of $\phi(\mathbf{g})$ is of the form $g_{\ell-1}^p - g_{\ell-1} + S(g_0, \ldots, g_{\ell-2})$ for some polynomial S, and so by Lemma 4.3 and the previous sentence, we get the equation $a_{\ell-1}(g_0^p - g_0)^{p^{\ell-1}} = (h_{\ell-1} - g_{\ell-1})^p - (h_{\ell-1} - g_{\ell-1})$, and we just need to count the number of $a_{\ell-1} \in \mathbb{F}_q$ such that this is possible. Picking $b \in \mathbb{F}_q$ and $k \in K$ such that $b^{p^{\ell-1}} = a_{\ell-1}$ and $k^{p^{\ell-1}} = h_{\ell-1} - g_{\ell-1}$ (such a b and k necessarily exist and are unique), we see that this equation is satisfied if and only if $b(g_0^p - g_0) = k^p - k$. Proposition 4.2 shows that there are at most $p^{m+1} - 1$ non-zero b satisfying this equation, thus at most p^{m+1} total values of b, as desired. □

Now we can state and prove our basic estimate.

Theorem 4.5. *Let $\mathbf{X}$ be a curve of genus g defined over $A := W_\ell(\mathbb{F}_q)$ and let $X = \mathbf{X} \times_{\operatorname{Spec} A} \operatorname{Spec} \mathbb{F}_q$. Let Z be an A-point on $\mathbf{X}$ containing the point $Q \in X(\mathbb{F}_q)$ and pick an integer $r > 2g-2$. Let $X_0 = X \setminus \{Q\}$. Assume there is some lift of points $\lambda : X_0(\mathbb{F}_q) \to \mathbf{X}(A)$ so that for $f \in L(rZ)$ and $P \in X_0(\mathbb{F}_q)$, we have $f(\lambda(P)) = (f_0(P), \ldots, f_{\ell-1}(P))$ as a Witt vector, where $f_i \in L(\infty Q)$ for each i. For $f \in L(rZ)$, let $\epsilon(f)$ be the corresponding codeword in $C(\mathbf{X}, \mathcal{Z}, rZ)$. Assume that $pr \le q$ and that $n \ge \left(2g - 1 + \max_{0\le i\le \ell-1}\{p^{\ell-1-i}\deg f_i\}\right)\sqrt{q}$, then*

$$\operatorname{wt}(\epsilon(f)) \ge \left((q-1)q^{\ell-2} - \frac{1}{q}(pr)^{\ell-1}(pr-1)\right)\left(n - \left(2g-1+\max_{0\le i\le\ell-1}\{p^{\ell-1-i}\deg f_i\}\right)\sqrt{q}\right).$$

Proof. If $f_0 \notin \mathbb{F}_q$ choose m with $p^m < r \le p^{m+1}$ and apply Theorem 4.4 to get $|B_3(\mathbf{f})| \le p^{(\ell-1)(m+1)}(p^{m+1}-1) \le (pr)^{\ell-1}(pr-1)$ (note for further reference that the last quantity is at most $q^{\ell-1}(q-1)$ by hypothesis). Now using Theorem 3.4 and equations (1), (2), (3), and (4) it follows that

$$\begin{aligned}
w(\epsilon(f)) &= n(q-1)q^{\ell-2} - \frac{1}{q}\sum_{j=1}^{n}\sum_{a\in U}\zeta^{\operatorname{Tr}(af(Z_j))} \\
&\ge n(q-1)q^{\ell-2} - \frac{1}{q}\Bigg(|B_3(\mathbf{f})|\,n + \left(q^\ell - q^{\ell-1} - |B_3(\mathbf{f})|\right)\cdot \\
&\qquad\qquad \max_{a\in U\setminus B(\mathbf{f})}\left|\sum_{P\in X_0(\mathbb{F}_q)}\zeta^{\operatorname{Tr}(af(P))}\right|\Bigg) \\
&= \left((q-1)q^{\ell-2} - \frac{1}{q}|B_3(\mathbf{f})|\right)\left(n - \max_{a\in U\setminus B(\mathbf{f})}\left|\sum_{P\in X_0(\mathbb{F}_q)}\zeta^{\operatorname{Tr}(af(P))}\right|\right) \\
&\ge \left((q-1)q^{\ell-2} - \frac{1}{q}(pr)^{\ell-1}(pr-1)\right)\left(n - \left(2g-1+\max_{0\le i\le\ell-1}\{p^{\ell-1-i}\deg f_i\}\right)\sqrt{q}\right).
\end{aligned}$$

Now suppose f_0 is a nonzero constant. Then $f(\lambda(P))$ is a unit for each $P \in X_0(\mathbb{F}_q)$, and so $\operatorname{wt}(\epsilon(f)) = n(q-1)q^{\ell-1}$.

Finally, suppose $f_0 = 0$. Let j be chosen so that $f_i = 0$ for $i < j$ and $f_j \ne 0$. If $j = \ell - 1$, then $f(\lambda(P)) \in p^{\ell-1}A$ for each $P \in X_0(\mathbb{F}_q)$ and so $\operatorname{wt}(\epsilon(f)) = nq^{\ell-1}$. If $j < \ell - 1$, then

since $L(rZ)$ is a free A-module, there is a rational function $h \in L(rZ)$ such that $f = p^j h$. Write $\mathbf{h} := h \circ \lambda = (h_0, \ldots, h_{\ell-1})$ so that $f = (0, \ldots, 0, h_0^{p^j}, \ldots, h_{\ell-j-1}^{p^j})$. We know $h_0 \neq 0$. If $h_0 \in \mathbb{F}_q$, then $\mathrm{wt}(\epsilon(f)) = n(q-1)q^{\ell-2}$. Otherwise, we have

$$\begin{aligned}\mathrm{wt}(\epsilon(f)) &= n(q-1)q^{\ell-2} - \frac{1}{q} \sum_{P \in X_0(\mathbb{F}_q)} \sum_{a \in U} \zeta^{\mathrm{Tr}(a\mathbf{f}(P))} \\ &= n(q-1)q^{\ell-2} - \frac{1}{q} \sum_{P \in X_0(\mathbb{F}_q)} \sum_{a \in U} \xi^{\mathrm{Tr}(a\mathbf{h}(P))},\end{aligned}$$

where $\xi = \zeta^{p^j}$ is a primitive $p^{\ell-j}$th root of unity. Applying induction on ℓ gives the result. □

5. Applications

5.1. **Projective line.** There is a natural well-known lift of points from $\mathbb{P}^1(\mathbb{F}_q)$ to $\mathbb{P}^1(W_\ell(\mathbb{F}_q))$, namely the Teichmüller lift. The point at infinity over $\mathbb{F}_q$ lifts to the point Z_∞ at infinity over $W_\ell(\mathbb{F}_q)$ and the affine point with coordinate x lifts to $\tau(x) = (x, 0, \ldots, 0)$. If f is a polynomial with coefficients in $W_\ell(\mathbb{F}_q)$ and degree r then $f \circ \tau$ is given by a Witt vector $\mathbf{f} = (f_0, f_1, \ldots, f_{\ell-1})$ where the f_i's are polynomials with coefficients in $\mathbb{F}_q$ satisfying $\deg f_i \leq p^i r$. Consider $C = C(\mathbb{P}^1, \mathcal{Z}, \mathbf{G})$, where $\mathcal{Z}$ consists of the Teichmüller lifts of the affine points of $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbf{G} = rZ_\infty$ for some $r \geq 0$. Thus $n = q$ and applying Theorem 4.5 if $pr \leq q$ and $\sqrt{q} \geq p^{\ell-1}r - 1$, we see that the minimum homogeneous weight of this code is at least

$$\left((q-1)q^{\ell-2} - \frac{1}{q}(pr)^{\ell-1}(pr-1)\right)\left(q - \left(p^{\ell-1}r - 1\right)\sqrt{q}\right).$$

5.2. **Elliptic curves.** Let E be an ordinary elliptic curve defined over the field $\mathbb{F}_q$, let $\mathbf{E}$ be the curve over $W_\ell(\mathbb{F}_q)$ obtained by reducing the Serre-Tate canonical lift (see [10]) of E modulo p^ℓ, and let $\tau : E(\mathbb{F}_q) \to \mathbf{E}(W_\ell(\mathbb{F}_q))$ be the associated elliptic Teichmüller lift of points. The next theorem is from [11].

Theorem 5.1. ([11]) *Let E and $\mathbf{E}$ be as above, and let $\mathbf{G} = r\tau(Q)$ for some $Q \in E(\mathbb{F}_q)$ and $r \geq 0$. Then for $f \in L(\mathbf{G})$ and $P \in E \setminus \{Q\}$, we have $f(\tau(P)) = (f_0(P), f_1(P), \ldots, f_{\ell-1}(P))$ as a Witt vector, where $f_i \in L((2p)^i rP)$ for $i = 0, 1, \ldots, \ell-1$.*

Combining Theorem 5.1 with Theorem 4.5, we get:

Corollary 5.2. *Let E, $\mathbf{E}$, and $\mathbf{G}$ be as above, set $\mathcal{Z} := \{\tau(P) \,|\, P \in E(\mathbb{F}_q) \setminus \{Q\}\}$, and let $n = \#\mathcal{Z}$. Then, provided that $pr \leq q$ and $n \geq \left(1 + (2p)^{\ell-1} r\right)\sqrt{q}$, the minimum homogeneous weight of $C(\mathbf{E}, \mathcal{Z}, \mathbf{G})$ is at least*

$$\left((q-1)q^{\ell-2} - \frac{1}{q}(pr)^{\ell-1}(pr-1)\right)\left(n - \left(1 + (2p)^{\ell-1} r\right)\sqrt{q}\right).$$

In the specific cases where $\ell = 2$ or $\ell = 3$, Finotti [5] was able to improve upon the degrees of the functions f_i in Theorem 5.1 which leads to a corresponding improvement in the above theorems.

5.3. **Plane curves with a unique point at infinity; $\ell = 2$.** In [12], the results of [11] were extended to the case of a plane curve with a unique point at infinity defined over a ring of Witt vectors of length 2. More precisely, let $\mathbf{X}$ be a proper plane curve over $W_2(\mathbb{F}_q)$ with affine open subset given by $\mathbf{H}(\mathbf{x}, \mathbf{y}) = 0$. Setting $X := \mathbf{X} \times_{\operatorname{Spec} W_2(\mathbb{F}_q)} \operatorname{Spec} \mathbb{F}_q$, we have that X has an affine open subset given by $H(x_0, y_0) = 0$, where H is the reduction of $\mathbf{H}$ modulo p. We will assume that $\mathbf{H}$ is of the form $\sum_{di+ej \leq de} a_{ij}\mathbf{x}^i\mathbf{y}^j$, where d and e are coprime integers with $a_{e0} \not\equiv 0 \pmod{p}$ and $a_{0d} \not\equiv 0 \pmod{p}$, and that the affine curve $H(x_0, y_0) = 0$ is smooth. Notice that the complement of the affine subset of X consists of a single point P_∞, and that the genus of X can be computed to be $(d-1)(e-1)/2$.

Theorem 5.3. ([12]) *Let $\mathbf{X}$, X, and P_∞ be as above. Then there is a "lift of points" $\lambda : X(\mathbb{F}_q) \setminus \{P_\infty\} \to \mathbf{X}(W_2(\mathbb{F}_q))$ such that for any $f \in L(rZ_\infty)$, we have $f \circ \lambda = (f_0, f_1) \in W_2(\mathbb{F}_q(X))$. Further, $f_0 \in L(rP_\infty)$ and $f_1 \in L(\gamma(r)P_\infty)$, where $\gamma(r)$ is a linear polynomial in r, independent of f and satisfying $\gamma(r) \leq p(r-1) + 2g(p+1)$.*

Again, we apply Theorem 4.5 to get:

Theorem 5.4. *Let $\mathbf{X}$, X, P_∞, Z_∞, and r be as above, and set $\mathcal{Z} := \{\lambda(P) \,|\, P \in X(\mathbb{F}_q) \setminus \{P_\infty\}\}$. Then, provided that $pr \leq q$ and $n \geq ((2p+4)\,g + p\,(r-1) - 1)\sqrt{q}$, the minimum*

homogeneous weight of $C(\mathbf{X}, \mathcal{Z}, rZ_\infty)$ *is at least*

$$\left(q - 1 - \frac{1}{q}(pr)(pr-1)\right)(n - ((2p+4)\,g + p\,(r-1) - 1)\,\sqrt{q})$$

The above results include hyperelliptic curves as special cases. However, in this case Finotti [5] also used his methods to provide results about the degrees of certain lifts of hyperelliptic curves, which are better than the above. Finally, Blache [1] has obtained general bounds on degrees of lifts for arbitrary curves. They are weaker than the above results but apply to more general curves.

References

[1] Blache, R. Bounds for exponential sums over Galois rings. Preprint, 2001.

[2] Carlet, C. $\mathbb{Z}_{2^k}$-Linear Codes. *IEEE Transactions on Information Theory*, 44:1543–1547, 1998.

[3] Constantinescu, I. and T. Heise. A metric for codes over residue class rings of integers. *Problems in Information Transmission* 33:208–213 (1998).

[4] Calderbank, A. R. and Gary M. McGuire. Construction of a $(64, 2^{37}, 12)$ code via Galois rings. *Designs, Codes, and Cryptography* 10:157–165, 1997.

[5] Finotti, L. R. A. Degrees of the Elliptic Teichmüller Lift. *Journal of Number Theory*, to appear.

[6] Greferath, M. and S. E. Schmidt. Gray Isometries for Finite Chain Rings and a Nonlinear Ternary $(36, 3^{12}, 15)$ Code *IEEE Transactions on Information Theory*, 45:2522–2524, 1999.

[7] Honold, T. Characterization of finite Frobenius rings. *Arch. Math. (Basel)* 76:406–415, 2001.

[8] Honold, T. and A. A. Nechaev. Fully weighted modules and representations of codes. *Problems in Information Transmission* 35:205–223, 1999.

[9] Hammons, A. R., Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40:301–319, 1994.

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

[11] Voloch, J. F. and J. L. Walker. Euclidean weights of codes from elliptic curves over rings. *Transactions of the American Mathematical Society*, 352:5063–5076, 2000.

[12] Voloch, J. F. and J. L. Walker. Codes over rings from curves of higher genus. *IEEE Transactions on Information Theory*, 45:1768–1776, 1999.

[13] Walker, J. L. Algebraic geometric codes over rings. *Journal of Pure and Applied Algebra*, 144:91–110, 1999.

[14] Walker, J. L. The Nordstrom Robinson code is algebraic geometric. *IEEE Transactions on Information Theory*, 43:1588–1593, 1997.

[15] Wood, J. A. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121:555–575, 1999.

Department of Mathematics, University of Texas, Austin, TX 78712

E-mail address: voloch@math.utexas.edu

Department of Mathematics and Statistics, University of Nebraska, Lincoln, NE 68588-0323

E-mail address: jwalker@math.unl.edu