MINIMUM HOMOGENEOUS WEIGHTS OF A CLASS OF CYCLIC CODES OVER PRIMARY INTEGER RESIDUE RINGS*

MARCUS GREFERATH†

Key words. ring-linear codes, Galois rings, homogeneous weight, minimum distance.

AMS subject classifications. 94B15, 94B65, 16Lxx

EXTENDED ABSTRACT. Most of the results in traditional finite-field linear coding theory regarding the minimum distance of linear codes refer to the Hamming metric. Important early exceptions are given by Berlekamp's nega-cyclic codes (cf. [1]) and Mazur's [9] low-rate codes, both having interesting properties in terms of the Lee-metric.

At the beginning of the nineties of the previous century an important observation revealed the role of finite rings (cf. [11, 5]) and moreover the necessity to discuss more general weight functions (cf. [3, 4]). In fact, it appears that the most important ring class for contemporary coding theory is given by the class of (finite) Frobenius rings, and a most prominent weight for these rings is the homogeneous weight, which was first introduced by Heise and Constantinescu [3] for general integer residue rings.

Galois rings, a subclass of all finite Frobenius rings, can be considered as Galois extensions of (primary) integer residue rings. More precisely, if $f \in \mathbb{Z}_{p^m}[x]$ is a basic monic polynomial of degree r, then the quotient ring $\mathbb{Z}_{p^m}[x]/(f)$ is a commutative chain ring of characteristic p^m, and its residue field is given by the finite field $\mathrm{GF}(p^r)$. Up to isomorphism, this ring depends only on the choice of p^m and r and not on the choice of f. It is denoted by $\mathrm{GR}(p^m, r)$ and was first described by Krull [7].

Homogeneous weights are defined by two properties that they share with the Hamming weight in finite field coding theory: given a finite ring R, the homogeneous weight of average value $\gamma \in \mathbb{Q}$ is a function $w : R \longrightarrow \mathbb{Q}$ satisfying $w(0) = 0$ and $w(x) = w(y)$ for all $x, y \in R$ with $Rx = Ry$ under the additional requirement

$$\frac{1}{|Rx|} \sum_{y \in Rx} w(y) \;=\; \gamma \quad \text{for all } \; 0 \neq x \in R.$$

For a Galois ring R with q-element residue field, homogeneous weights take the comparably simple form

$$w : R \longrightarrow \mathbb{Q}, \quad x \mapsto \gamma \begin{cases} 1 & : \; x \notin \mathrm{soc}(R), \\ \frac{q}{q-1} & : \; x \in \mathrm{soc}(R),\, x \neq 0, \\ 0 & : \; \text{otherwise.} \end{cases}$$

Note that the Hamming weight on the finite field $\mathrm{GF}(q)$ is a homogeneous weight, and its average value is given by $\gamma = \frac{q-1}{q}$.

During the recent decade, notable work has been done regarding the minimum homogeneous weight of certain linear codes over Galois rings. For details, the reader is referred to papers by Walker and Voloch [13]. In this paper we attempt to generalize a method from [9] and derive results in the spirit of those in [13]. One of our main

*This work was supported by Science Foundation Ireland, Grants 06/MI/006 and 08/IN.1/I1950.

†School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Republic of Ireland (marcus.greferath@ucd.ie).

ingredients are a Fourier analysis of the homogeneous weight and a generalized version of the famous Carlitz-Uchiyama bound which has been presented in [8].

Main results. Galois rings form a subclass of the class of all finite Frobenius rings. This latter class of rings is distinguished by the fact that its members possess what are called generating characters. More precisely, let R be a finite Frobenius ring and let $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$ denote its character group. It is known that R being a bimodule over itself imposes a bimodule structure on $\hat{R}$. And it can be shown that a finite ring is Frobenius if and only if ${}_R R \cong {}_R\hat{R}$ or $R_R \cong \hat{R}_R$ (for details see [14]).

A character χ is therefore called generating if $\hat{R} = R\chi$ (and hence $\hat{R} = \chi R$). For our analysis of homogeneous weights the following lemma is crucial. It was first observed by Honold [6] and has since then be vastly used in the literature on linear codes over rings with homogeneous weights.

LEMMA 1.1. *Let R be a finite Frobenius ring and χ be a generating character of $\hat{R}$. Then a weight function $w : R \longrightarrow \mathbb{Q}$ is homogeneous of average γ if and only if*

$$w(x) = \gamma \Big[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu)\Big].$$

The discrete Fourier transform is defined as

$$\mathrm{FT} : \mathbb{C}^R \longrightarrow \mathbb{C}^R, \quad f \mapsto \hat{f}, \qquad \text{where } \hat{f}(x) := \sum_{r \in R} f(r)\chi(-rx).$$

It allows to derive the following lemma:

LEMMA 1.2. *If R is a finite Frobenius ring with generating character χ, and if w is a homogeneous weight of average γ then*

$$\hat{w} \;=\; \gamma\,|R| \Big[\mathbf{1}_{\{0\}} - \frac{1}{|R^\times|}\mathbf{1}_{R^\times}\Big] \qquad \textit{where} \quad \mathbf{1}_X : R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 1 & : \; x \in X, \\ 0 & : \; \textit{else} \end{cases}$$

is the indicator function of a subset X of R.

Proof. Using the homogeneous weight in its form in 1.1 we compute

$$\begin{aligned} \hat{w}(y) = \sum_{r \in R} w(r)\chi(-ry) \;&=\; \sum_{r \in R} \gamma\Big[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(ru)\Big]\chi(-ry) \\ &= \gamma \sum_{r \in R} \chi(ry) - \gamma \sum_{u \in R^\times} \sum_{r \in R} \chi(r[u-y]) \;=\; \gamma|R| \begin{cases} 1 & : \; y = 0, \\ -\frac{1}{|R^\times|} & : \; y \in R^\times, \\ 0 & : \; \text{else}, \end{cases} \end{aligned}$$

which proves the claim. □

In the course of this paper the sum of the absolute values of the nonzero frequencies in the spectrum of a homogeneous weight will be of importance. In light of this, the foregoing analysis has particularly shown that if R is a finite Frobenius ring with generating character χ, and w is a homogeneous weight on R then $\hat{w}$ vanishes on the (proper) zero divisors of R.

Weil-Carlitz-Uchiyama Bound for Galois Rings. This section only briefly puts together the essentials of the generalization of the Weil-Carlitz-Uchiyama (W-CU) bound that has been presented in [8].

Let $R := \mathrm{GR}(p^m, r)$ be the Galois ring of charactistic p^m and degree r. As indicated earlier, its residual field F has p^r elements, and the polynomial $x^{p^r-1} -$

$1 \in F[x]$ splits into pairwise distinct linear factors over $F[x]$. Using Hensel's lemma (cf. [10,]) this factorization can in a unique way be lifted to a factorization of the polynomial $x^{p^r-1} - 1 \in R[x]$. The zeros of the occuring linear factors form a cyclic subgroup of the group $R^\times$ of invertible elements of R, and we define the *Teichmüller set* of R as the set

$$T_r \ := \ \{y \in R \mid y^{p^r-1} - 1 = 0\} \cup \{0\}.$$

It can now be shown that every element $z \in R$ allows for a representation $z = z_0 + z_1 p + z_2 p^2 + \ldots + z_{m-1} p^{m-1}$, where $z_i \in T_r$ for all $i \in \{0, \ldots, m-1\}$. Such a representation is called a p-adic representation, and it is clear that it can be extended to any free R-module, and in particular to the polynomial ring $R[x]$, i.e. every polynomial $f \in R[x]$ allows for a representation

$$f \ = \ f_0 + f_1 p + f_2 p^2 + \ldots + f_{m-1} p^{m-1},$$

where $f_i \in T_r[x]$ for all $i \in \{0, \ldots, m-1\}$.

Let n_i be the degree of f_i in this p-adic representation of the polynomial $f \in R[x]$ for all $i = 0, \ldots, m-1$. We define the weighted degree of f to be the number

$$N(f) \ := \ \max\{n_0 p^{m-1}, n_1 p^{m-2}, \ldots, n_{m-1}\}.$$

Let $f_i = \sum_{j=0}^{n_i} f_i^j x^j$ for all $i = 0, \ldots, m-1$. We will say that f is non-degenerate, if $f_i^j = 0$ whenever $j \equiv 0 \pmod p$ for all $0 \le i \le m-1$ and $0 \le j \le n_i$.

Now a main theorem [8, Theorem 1] states the following:

THEOREM 1.3. *For non-degenerate $f \in R[x]$ of weighted degree $N(f)$ there holds*

$$\Big| \sum_{x \in T_r} \chi(f(x)) \Big| \ \le \ (N(f) - 1)\sqrt{q}.$$

Homogeneous Distance of Trace Codes. Let $R := \mathrm{GR}(p^m, r)$ be the Galois ring as above; its automorphism group fixes $\mathbb{Z}_{p^m}$ and is cyclic of order r generated by an element τ the action of which is conveniently described using the coefficients $z_i \in T_r$ of the p-adic representation, namely

$$\tau : R \longrightarrow R, \quad \sum_{i=0}^{m-1} z_i \, p^i = z \ \mapsto \ \tau(z) := \sum_{i=0}^{m-1} z_i^p \, p^i.$$

From this we obtain the trace function

$$\mathrm{tr} : R \longrightarrow \mathbb{Z}_{p^m}, \quad z \ \mapsto \ \sum_{j=0}^{r-1} \tau^j(z).$$

For arbitrary $t \in \mathbb{N}$ we define a $\mathbb{Z}_{p^m}$-linear code C of length $q := p^r$ by

$$C \ := \ \{(\mathrm{tr} f(x))_{x \in T_r} \mid f \in R[x], \deg(f) \le t\}.$$

We will also be interested in the shortened code

$$C_0 \ := \ \{(\mathrm{tr} f(x))_{x \in T_r \setminus \{0\}} \mid f \in R[x], \deg(f) \le t \ \text{ and } f(0) = 0\}.$$

We now prepare our main result regarding the minimum weight of the code C.

THEOREM 1.4. *For $f \in R[x]$ let $c_f := (\mathrm{tr} f(x))_{x\in T_r} \in C$ and set $q := p^r$. If w is an arbitrary weight function w on $\mathbb{Z}_{p^m}$ of average value γ then there holds:*

$$w(c_f) - \gamma\, q \;=\; \frac{1}{|\mathbb{Z}_{p^m}|} \sum_{y\in\mathbb{Z}_{p^m}\setminus\{0\}} \hat{w}(y)\, E_f(y),$$

where $E_f(y) = \sum_{x\in T_r} \chi(y\,\mathrm{tr} f(x))$.

COROLLARY 1.5. *Let w be the homogeneous weight of average value γ on $\mathbb{Z}_{p^m}$, and assume $f \in R[x]$ with $f(0) = 0$ and $c_f \neq 0$, then*

$$w(c_f) - \gamma\, q \;=\; -\gamma\, \frac{1}{|\mathbb{Z}_{p^m}^{\times}|} \sum_{y\in\mathbb{Z}_{p^m}^{\times}} E_f(y)$$

Combining the result in the preceding corollary with the above-mentioned generalization of the W-CU bound, we obtain the following:

COROLLARY 1.6. *Assumptions as in the preceding statement. Then*

$$|w(c_f) - \gamma\, q| \;\leq\; \gamma\,(\tilde{N}(f) - 1)\,\sqrt{q}\,,$$

where $\tilde{N}(f) = \frac{1}{|\mathbb{Z}_{p^m}^{\times}|} \sum_{y\in\mathbb{Z}_{p^m}^{\times}} N(yf)$.

REFERENCES

[1] E. R. Berlekamp, "Negacyclic codes for the Lee metric", 1969 Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967) pp. 298–316 Univ. North Carolina Press, Chapel Hill, N.C.

[2] L. Carlitz, S. Uchiyama, "Bounds for exponential sums", Duke Math. J. 24 (1957), 37–41.

[3] I. Constantinescu, W. Heise: "A metric for codes over residue class rings of integers", *Problemy Peredachi Informatsii*, Vol. 33, no. 3, pp. 22–28, 1997.

[4] M. Greferath, S. E. Schmidt, "Finite-ring combinatorics and MacWilliams' equivalence theorem", J. Combin. Theory Ser. A 92 (2000), no. 1, 17–28.

[5] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé: "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes", *IEEE Trans. Inform. Theory*, Vol. 40, pp. 301–319, 1994.

[6] T. Honold, "Characterization of finite Frobenius rings", Arch. Math. (Basel) 76 (2001), no. 6, 406–415.

[7] W. Krull, "Über den Galoisring", (German) Math. Ann. 185 1970 25–37.

[8] P. V. Kumar, T. Helleseth, A. R. Calderbank: "An upper bound for Weil exponential sums over Galois rings and applications", IEEE Trans. Inform. Theory 41 (1995), no. 2, 456–468.

[9] L. E. Mazur, "Codes correcting errors of large weight in the Lee metric", (Russian) Problemy Peredaŭ10di Informacii 9 (1973), no. 4, 11–16.

[10] B. R. McDonald, "Finite rings with identity", Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974. ix+429p.

[11] A. A. Nechaev, A. S. Kuzmin: "Kerdock Codes in a Cyclic Form", *Discrete Math. Appl*, vol. 1, 1991, pp. 365-384.

[12] J. V. Uspensky, "Theory of Equations", McGraw-Hill, NY 1948.

[13] J. F. Voloch, J. L. Walker, "Homogeneous weights and exponential sums" Finite Fields Appl. 9 (2003), no. 3, 310–321.

[14] J. A. Wood,"Duality for modules over finite rings and applications to coding theory", Amer. J. Math. 121 (1999), no. 3, 555–575.