Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 55-61*

Refined bounds for ring-linear codes

Eimear Byrne[1], Marcus Greferath[2] ebyrne, marcus.greferath@ucd.ie
School of Mathematical Sciences and Claude Shannon Institute,
University College Dublin, Belfield, Dublin 4, IRELAND

Axel Kohnert axel.kohnert@uni-bayreuth.de
Mathematics Department, University of Bayreuth,
D-95440 Bayreuth, GERMANY

Vitaly Skachek[3] vitaly.skachek@ucd.ie
School of Mathematical Sciences and Claude Shannon Institute,
University College Dublin, Belfield, Dublin 4, IRELAND

Abstract. We give further results on the question of code optimality for linear codes over finite Frobenius rings for the homogeneous weight. This article improves on the existing Plotkin bound derived in an earlier paper [4], and suggests a version of a Singleton bound. We also present some families of codes meeting these new bounds.

1 Introduction

The homogeneous weight, discovered by Heise and Constantinescu [2], has emerged as important in the context of finite rings. Examples of homogeneous weights include the Hamming weight on finite fields and the Lee weight on $\mathbb{Z}_4$. The homogeneous weight may be viewed as a natural generalisation of the Hamming weight for codes over finite rings.

Many of the classical bounds for codes over finite fields have found an equivalent expression for finite ring codes for the homogeneous weight. The Plotkin and Elias bounds have been given in [4]. In [1], a linear programming bound is derived. In this note we present further bounds for codes over finite Frobenius rings for the homogeneous weight. We give a refinement of the Plotkin bound given in [4] for linear codes. We also suggest a Singleton-like bound.

2 Technical Preliminaries

In all that follows, let R be a finite ring with identity. The character group of the additive group of R is denoted by $\widehat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$. This group has the

[1]Research supported Science Foundation Ireland Grant 08/RFP/MTH1181
[2]Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006
[3]Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006

structure of an R-R-bimodule by defining $\chi^r(x) := \chi(rx)$ and ${}^r\chi(x) := \chi(xr)$ for all $r, x \in R$, and for all $\chi \in \widehat{R}$. Summarizing elements from [6] we come to the following definition:

Definition 2.1 *A finite ring R is called a* Frobenius ring *if ${}_R\widehat{R} \cong {}_RR$, in which case ${}_R\hat{R} := \{{}^r\chi \mid r \in R\}$ for some left-generating character χ.*

The results presented here involve two weight functions on elements R^n. The first is the Hamming weight, which counts the number of the nonzero components of a word $c \in R^n$ or equivalently its support size; we denote it by $\ell(c)$. The second is the homogeneous weight, defined as follows.

Definition 2.2 *A weight w on the finite ring R is called* (left) homogeneous*, if $w(0) = 0$ and the following is true:*

(H1) *If $Rx = Ry$ then $w(x) = w(y)$ for all $x, y \in R$.*

(H2) *There exists a real number γ such that*

$$\sum_{y \in Rx} w(y) \;=\; \gamma\,|Rx| \qquad \text{for all } x \in R \setminus \{0\}\,.$$

Up to the choice of γ, every finite ring admits a unique (left) homogeneous weight [3, Theorem 1.3].

Example 2.3 *If R is a local Frobenius ring R with residue field $GF(q)$ then the function*

$$w\colon R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & : \; x = 0, \\ \frac{q}{q-1} & : \; x \in \operatorname{soc}(R),\ x \neq 0, \\ 1 & : \; \textit{otherwise}, \end{cases}$$

is a homogeneous weight of average value $\gamma = 1$.

Example 2.4 *On the ring R of 2×2 matrices over $GF(2)$ the weight*

$$w\colon R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & : \; x = 0, \\ 2 & : \; x \textit{ singular},\ x \neq 0, \\ 1 & : \; \textit{otherwise}, \end{cases}$$

is a homogeneous weight of average value $\gamma = \frac{3}{2}$.

The weight function w on R is additively extended to a weight on the R-module ${}_RR^n$, i.e.

$$w(c) \;:=\; \sum_{i=1}^{n} w(c_i), \quad \text{for } c \in R^n$$

We use the notation $[n, d]$ to denote a linear code in ${}_R R^n$ with minimum homogeneous weight d. If R is a finite field then the notion of dimension of a linear code is well defined and we write $[n, k, d]$ to denote a linear code of length n, dimension k and minimum weight d. We write (n, M, d) to denote a nonlinear code over a finite field of length n and minimum distance d with M words.

3 Shortened and Residual Codes

We construct new codes from a given code by 'shortening' and puncturing. The results of this section will be applied in later sections to derive further bounds. Given a linear code $C \leq {}_R R^n$ and word $c \in R^n$, we define the code

$$\mathrm{Sho}(C, c) := \{z \in C \mid \mathrm{supp}(z) \subset \mathrm{supp}(c)\}, \mathrm{Res}(C, c) := \{(z_i)_{i \notin \mathrm{supp}(c)} \mid z \in C\}.$$

Denoting by π_c the projection of R^n onto the coordinates not contained in $\mathrm{supp}(c)$, it is clear that $\mathrm{Sho}(C, c) = \ker(\pi_c) \cap C$ and $\mathrm{Res}(C, c) = \pi_c(C)$. Moreover, these codes are related by $C/\mathrm{Sho}(C, c) \cong \mathrm{Res}(C, c)$.

Lemma 3.1 *Let $C \leq {}_R R^n$ be a linear code, and let $x \in R^n$. Then*

$$\frac{1}{|C|} \sum_{c \in C} w(x + c) = \gamma |\mathrm{supp}(C)| + w(\pi_c(x)).$$

In general there is no relationship between $\mathrm{Sho}(C, x)$ and Rx, but for $x \in C$ we observe that $\mathrm{Sho}(C, x) \geq Rx$. The following lemma gives conditions for which we have equality.

Lemma 3.2 *Let $C \leq {}_R R^n$ be a linear code of homogeneous minimum weight d, and let c be a word in C that satisfies $\ell(c) < \frac{d}{\gamma}$. Then $\mathrm{Sho}(C, c) = Rc$.*

Corollary 3.3 *Let $C \leq {}_R R^n$ be a linear $[n, d]$ code, and let $c \in C$ satisfy $\ell(c) < \frac{d}{\gamma}$. Then $\mathrm{Res}(C, c)$ is an $[n - \ell(c), \geq d - \gamma\ell(c)]$ code satisfying $|\mathrm{Res}(C, c)| = |C|/|Rc|$.*

Example 3.4 *Let C be the linear $\mathbb{Z}_4$-octacode, which has 256 words and minimum Lee distance 6 (cf. [5]). It contains the word $c = [0, 0, 0, 2, 0, 2, 2, 2]$ which satisfies $\gamma\ell(c) = 4 < 6 = d$ (recall $\gamma = 1$ when the homogeneous weight coincides with the Lee weight on $\mathbb{Z}_4$). Clearly, $|Rc| = 2$ and we puncture C on the coordinates $4, 6, 7, 8$ to obtain $C_1 = \mathrm{Res}(C, c)$, which by Corollary 3.3 is a linear $[4, d_1 \geq 2]$ code of size 128. (In fact $d_1 = 2$ here). Considering the Gray image of C_1 we arrive at an $(8, 128, 2)$ code that obviously meets the (finite-field coding theory) Singleton bound. For this reason we deduce that C_1 is an optimal linear $[4, 2]$ code.*

4 A Refinement of the Plotkin Bound

If a linear code $C \leq {}_R R^n$ has maximal support, meaning $|\mathrm{supp}(C)| = n$, then by observations in [4] or by applying Lemma 3.1 we find

$$\frac{|C|-1}{|C|}\, d \;\leq\; \frac{1}{|C|}\sum_{c\in C} w(c) \;=\; \gamma n. \tag{1}$$

We combine this observation with the following theorem to obtain a Plotkin-like bound for linear codes.

Theorem 4.1 *Let $C \leq {}_R R^n$ be a linear $[n,d]$ code satisfying $n < \frac{d}{\gamma}$. Then*

$$|C| \leq |Rc|\,\frac{d-\gamma\ell}{d-\gamma n}$$

for any $c \in C$ such that $\ell := \ell(c) < \frac{d}{\gamma}$.

Example 4.2 *Let $m \in \mathbb{N}$ and let $n = m \times (|R|^m - 1)$. Let $C \leq {}_R R^n$ be the Simplex code, which is generated by the $m \times n$ matrix G whose columns comprise the distinct nonzero elements of R^m. It is not hard to see that C is a constant weight code of homogeneous weight $\gamma|R|^m$. Moreover, $n = |R|^m - 1 < |R|^m = \frac{d}{\gamma}$ and $\ell(c) \leq n < \frac{d}{\gamma}$ for each word $c \in C$. For any word $c = xG \in C$ we have*

$$\ell(c) = |R|^m - |x^\perp| = |R|^m - \frac{|R|^m}{|Rc|},$$

thus the upper bound on $|C|$ determined by Theorem 4.1 met sharply by $|C|$.

Corollary 4.3 *Let $C \leq {}_R R^n$ be a linear code of minimum homogeneous weight d and minimum Hamming weight ℓ where $\ell \leq n \leq \frac{d}{\gamma}$. Then*

$$|C| \leq |R|\,\frac{d-\gamma\ell}{d-\gamma n}.$$

It is straightforward to verify that for linear codes, this gives a refinement of the Plotkin bound given in [4] for $\ell < \dfrac{d}{\gamma} < \ell\dfrac{|R|}{|R|-1}$.

In fact we can do even better, taking into account some properties of R.

Corollary 4.4 *Let $C \leq {}_R R^n$ be a linear code of minimum homogeneous weight d and minimum Hamming weight ℓ where $\ell < n \leq \frac{d}{\gamma}$. Let Q be the maximum size of any minimal ideal of R. Then*

$$|C| \leq Q\,\frac{d-\gamma\ell}{d-\gamma n}.$$

Example 4.5 *We again study the Simplex Code, this time over the ring R of all 2×2-matrices over $\mathbb{F}_2$. This code is of length $n = 16^m - 1$ for suitable m, and its minimum Hamming weight of is $16^m - \frac{16^m}{4} = \frac{3}{4}16^m$. The ring R has 3 minimal ideals, each of size 4, and and so from Corollary 4.4 we have*

$$16^m \;=\; |C| \;\leq\; 4\,\frac{16^m\gamma - \frac{3}{4}16^m\gamma}{16^m\gamma - (16^m-1)\gamma} \;=\; 4\frac{16^m}{4} \;=\; 16^m.$$

4.1 A Singleton bound

Let C be an $[n,d]$ code over R satisfying $n \leq \dfrac{d}{\gamma}$. If there exists some codeword $c \in C$ satisfying $\ell = \ell(c) < n \leq \dfrac{d}{\gamma}$ then from Corollary 3.3, $C_1 := \mathrm{Res}(C,c)$ is an $[n_1,d_1]$ code over R, isomorphic to C/Rc with $d_1 \geq d - \gamma\ell$ and

$$n_1 = n - \ell \leq \frac{d}{\gamma} - \ell \leq \frac{d_1}{\gamma}.$$

Let $C_0 := C$. We now construct a sequence of $[n_i,d_i]$ codes C_i as follows. For each i, as long as there exists some $c^i \in C_i$ with Hamming weight $\ell_i := \ell(c^i) < n_i$, define $C_{i+1} := \mathrm{Res}(C_i,c^i)$. By assumption, $n \leq \frac{d}{\gamma}$, which implies that $\ell_i < n_i = n_{i-1} - \ell_i < \frac{d_i}{\gamma}$ for each $i \geq 1$. Therefore, from Lemma 3.2 we have a finite sequence of codes

$$C = C_0,\; C_1 \cong C/Rc,\; C_2 \cong C_1/Rc^1,\; ..., C_r \cong C_{r-1}/Rc^{r-1}$$

of length $r+1$ for some nonnegative integer r. Moreover, for each $i \in \{1,...,r\}$ we have

$$|C_i| = \frac{|C_{i-1}|}{|Rc^{i-1}|} = \frac{|C|}{|Rc^0|\cdots|Rc^{i-1}|} \text{ and } d_i \geq d_{i-1} - \gamma\ell_{i-1} > 0. \tag{2}$$

Observe that the final code C_r has the property that each of its non-zero words has constant Hamming weight n_r, so taking any further quotients by $c^r \in C_r$ results in a code of length zero. We may write $C_r = \mathrm{Sho}(C_r,c^r)$ for any $c^r \in C_r$. Since it may occur that $\ell(c^r) := \ell_r = n_r = \frac{d_r}{\gamma}$ we cannot apply Lemma 3.2 to determine that $C_r = \mathrm{Sho}(C_r,c^r) = Rc^r$. However, by a simple counting argument it can be shown that $|C_r| \leq |R|$: if there are more than $|R|$ words in C then at least one pair of words of C have the same symbol in a given position, in which case their difference is a word of Hamming weight less than n.

From (2) we have

$$|C| = |Rc^0||Rc^1|\cdots|Rc^{r-1}||C_r|. \tag{3}$$

The existence of such a sequence of $r+1$ codes leads to the following inequality.

$$n = \sum_{i=0}^{r} \ell_i \quad \geq \quad \frac{|Rc|-1}{|Rc|}\frac{d}{\gamma} + \sum_{i=1}^{r} \ell_i \geq \frac{|Rc|-1}{|Rc|}\frac{d}{\gamma} + r, \tag{4}$$

This gives a type of Singleton bound for the homogeneous weight:

Theorem 4.6 *Let C be an $[n,d]$ code over R satisfying $n \leq \frac{d}{\gamma}$ and $\ell(C) < n$. Let $P := \max\{|Ra| : a \in R^n, Ra \leq C, \ell(a) < n\}$. Then*

$$n - \left\lceil \frac{P-1}{P}\frac{d}{\gamma} \right\rceil \geq \lceil \log_P |C| - \log_P |R| \rceil .$$

Corollary 4.7 *Let C be an $[n,d]$ code over R satisfying $n < \frac{d}{\gamma}$, and let $Q := \max\{|Ra| : a \in R^n, Ra \leq C\}$. Then*

$$n - \left\lceil \frac{Q-1}{Q}\frac{d}{\gamma} \right\rceil \geq \left\lceil \log_Q |C| - 1 \right\rceil .$$

We may deduce the following weaker result directly from (3).

Proposition 4.8 *Let $C \leq {}_RR^n$ be an $[n,d]$ linear code and suppose that $n \leq \frac{d}{\gamma}$. Then*

$$n - \left\lceil \frac{|R|-1}{|R|}\frac{d}{\gamma} \right\rceil \geq \left\lceil \log_{|R|} |C| - 1 \right\rceil .$$

We give an example of an MDS code over a finite chain ring R, using points from the projective Hjelmslev geometry.

Example 4.9 *Let R be a chain ring of length 2 with $\mathrm{soc}R \simeq R/\mathrm{rad}R \simeq GF(q)$. Then $R^\times = R\backslash \mathrm{rad}R$ and $|R| = q^2$. Let $F := R^2 \backslash \mathrm{rad}R^2$. We denote by $PHG(R^2)$ the projective Hjelmslev line, with points $\mathcal{P} = \{xR : x \in F\}$. $PHG(R^2)$ has q^2+q distinct points.*

Let $C < {}_RR^n$ be the length $n := q^2+q$ code with $2 \times n$ generator matrix $G = [g_1, ..., g_n]$ whose columns comprise elements of R^2 corresponding to distinct points in $PHG(R^2)$. Clearly $\ell(c) < n$ for each $c \in C$. C is free of rank 2 and the maximal cyclic submodules of C have size $P := |R| = q^2$. Let $r = \lceil \log_P |C| - 1 \rceil = \log_{q^2} q^4 - 1 = 1$. Setting $\gamma = 1$, each word xG of C has weight

$$w(xG) = |J_1| + \frac{q}{q-1}|J_2| = \begin{cases} q^2 + \frac{q}{q-1}(q-1) = q^2+q & \text{if } x \in F \\ q^2\frac{q}{q-1} = \frac{q^3}{q-1} & \text{if } x \in \mathrm{rad}R^2 \end{cases},$$

where $J_1 = \{j \mid x \cdot g_j \in R^\times\}$ *and* $J_2 = \{j \mid x \cdot y_j \in \mathrm{rad}R\backslash\{0\}\}$. *Then* $d = n = q^2 + q$ *and*

$$\begin{aligned} n - \left\lceil \frac{q^2-1}{q^2} d \right\rceil &= n - \left\lceil \frac{q^2-1}{q^2}(q^2+q) \right\rceil = n - \left\lceil q^2 + q - 1 - \frac{1}{q} \right\rceil \\ &= q^2 + q - q^2 - q + 1 = 1 = r, \end{aligned}$$

which meets the bound given in Theorem 4.6.

References

[1] E. Byrne, M. Greferath, M. E. O'Sullivan, *The linear programming bound for codes over finite Frobenius rings,* Designs, Codes and Cryptography, Vol. 42 , **3** (2007), pp. 289 - 301.

[2] I. Constantinescu, W. Heise, A metric for codes over residue class rings of integers, *Probl. Pered. Inform.* 33, 1997, no. 3, 22-28.

[3] M. Greferath, S. E. Schmidt, Finite-ring combinatorics and MacWilliams equivalence theorem, *J. Combin. Theory* A-92, 2000, 17-28.

[4] M. Greferath, M. E. O'Sullivan, On bounds for codes over Frobenius rings under homogeneous weights, *Discr. Math.* 289, 2004, 11-24.

[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* 1994, 301–319.

[6] J. A. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* 121, 1999, 555-575.