New Bounds for Codes over Finite Frobenius Rings

Eimear Byrne · Marcus Greferath · Axel Kohnert · Vitaly Skachek

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 [6], and suggests a version of a Singleton bound. We also present some families of codes meeting these new bounds.

Key Words: codes over rings, finite Frobenius rings, homogeneous weights, Plotkin and Singleton bounds.

Introduction

In the early 1990s interest in algebraic codes over finite rings was vastly increased due to the discovery that certain non-linear binary codes have \mathbb{Z}_4 -linear representations (cf. [7,11]). Many papers on the topic have been published since then. A new weight function called the *homogeneous weight* was

M. Greferath

School of Mathematical Sciences University College Dublin, Belfield, Dublin 4, Ireland E-mail: marcus.greferath@ucd.ie

A. Kohnert

Mathematics Department, University of Bayreuth, D-95440 Bayreuth, Germany E-mail: axel.kohnert@uni-bayreuth.de

Vitaly Skachek

School of Mathematical Sciences University College Dublin, Belfield, Dublin 4, Ireland E-mail: vitaly.skackek@ucd.ie

Research supported Science Foundation Ireland Grant 08/RFP/MTH1181, Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006

E. Byrne,

School of Mathematical Sciences University College Dublin, Belfield, Dublin 4, Ireland E-mail: ebyrne@ucd.ie

discovered by Heise and Constantinescu [2,3] and has since proven to be useful in the context of codes over 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.

As in traditional algebraic coding theory, a natural question when dealing with codes over ring alphabets concerns the criteria that best measure the quality and determine optimality of a code. For this reason, the theory requires the establishment of fundamental bounds relating the standard parameters of code length, size, minumum distance. Many of the classical bounds for codes over finite fields have found an equivalent expression for finite ring codes for the homogeneous weight. For example, Plotkin and Elias bounds were given in [6] and constructions of Plotkin-optimal codes can be read in [5]. In [1], a linear programming bound was derived.

In this note we present further bounds for linear codes over finite Frobenius rings for the homogeneous weight. We give a refinement of the Plotkin bound given in [6]. We also suggest a Singleton-like bound.

1 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 $\widehat{R} := \operatorname{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$. This group has the 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 [12] we come to the following definition:

Definition 1 A finite ring R is called a *Frobenius ring* if $_R \hat{R} \cong _R R$.

It can be seen (cf. [12]) that if R is a finite Frobenius ring, then R and \hat{R} are isomorphic also as right R-modules. Hence, there exist characters χ and ψ such that

$$\widehat{R} = \{ {}^{r}\chi \mid r \in R \} = \{ \psi^{r} \mid r \in R \}.$$

Such characters are called *left generating* or *right generating*, respectively. Moreover, every left generating character is at the same time right generating, and a character is (left and/or right) generating if and only if its kernel does not contain any non-zero left or right ideal of R.

The class of finite Frobenius rings is quite large, as the following proposition shows. For a proof see [12] and also [4].

Proposition 1 (a) Any finite principal ideal ring is Frobenius.

- (b) If R and S are Frobenius ring, then so is $R \times S$.
- (c) If R is a Frobenius ring, then so is $M_n(R)$, the ring of all $n \times n$ -matrices over R.

(d) If R is a Frobenius ring, and G a finite group, then the group ring R[G] is again a Frobenius ring.

Weight Functions

The Hamming weight of a word $c \in \mathbb{R}^n$ counts the number of the nonzero components of c, and hence gives the size of $\operatorname{supp}(c)$. In a way, it could be considered as the actual length of c, and hence, we will denote it by $\ell(c)$. For a code $C \leq {}_{\mathbb{R}}\mathbb{R}^n$, we write $\ell(C) := |\operatorname{supp}(C)|$.

We are aware that this notation deviates from the literature, however we ask the reader to accept it, as it will help to avoid confusion with the homogeneous weight and minimum distance that we are going to present now.

Definition 2 A weight function $w : R \longrightarrow \mathbb{R}$ 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

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

Homogeneous weights were first introduced by Heise and Constantinescu in [3] for integer residue rings, and later generalised to Frobenius rings in [8], and to arbitrary finite rings in [4].

The number γ may be thought of as the *average value* of w, and condition **(H2)** simply states that this average is the same on all nonzero principal left ideals.

It was shown in [4, Theorem 1.3] that, up to the choice of γ , every finite ring admits a unique (left) homogeneous weight. Moreover, Honold observed in [9] that, provided R is Frobenius, the homogeneous weight will allow for an expression in terms of a generating character. We let R^{\times} denote the group of units of R.

Proposition 2 Let R be a finite Frobenius ring with generating character χ . Then the (left) homogeneous weights on R are precisely the functions

$$w: R \longrightarrow \mathbb{R}, \quad x \mapsto \gamma \Big[1 - \frac{1}{|R^{\times}|} \sum_{u \in R^{\times}} \chi(xu) \Big]$$

where γ is a real number.

As an immediate consequence, if R is a finite Frobenius ring, then every left homogeneous weight is also right homogeneous with the same average value $\gamma\,,$ since

$$\sum_{u \in R^{\times}} \chi(xu) = \sum_{u \in R^{\times}} \chi(ux).$$

As we will restrict to Frobenius rings in the sequel we will not distinguish between left and right homogeneous weights any more, and simply refer to homogeneous weights instead. Before we continue, we will give examples of homogeneous weights on various instances of finite Frobenius rings.

- *Example 1* (a) On every finite field \mathbb{F}_q the Hamming weight is a homogeneous weight of average value $\gamma = \frac{q-1}{q}$.
- (b) On \mathbb{Z}_4 the Lee weight is homogeneous with $\gamma = 1$.
- (c) On a local Frobenius ring R with q-element residue field the weight

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

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

(d) On the ring R of 2×2 matrices over GF (2) the weight

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

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

As is common in coding theory, a weight w on a finite ring R is additively extended to a weight on the R-module $_{R}R^{n}$, i.e.

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

The minimum weight of a linear code is the minimum non-zero weight of any codeword. A linear code of length n and minimum homogeneous weight d will frequently be referred to as an [n, d]-code. 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 not necessarily linear code over a finite field of length n and minimum distance d with M words.

2 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.

Lemma 1 Let $C \leq {}_{R}R^{n}$ be a linear code, and let $x \in R^{n}$. Then

$$\frac{1}{|C|} \sum_{c \in C} w(x+c) = \gamma \ell(C) + \sum_{i \notin \text{supp}(C)} w(x_i).$$

Proof: We compute

$$\frac{1}{|C|} \sum_{c \in C} w(x+c) = \frac{1}{|C|} \sum_{c \in C} \sum_{i=1}^{n} w(x_i+c_i)$$
$$= \frac{1}{|C|} \sum_{i=1}^{n} \sum_{c \in C} \gamma \Big[1 - \frac{1}{|R^{\times}|} \sum_{u \in R^{\times}} \chi((x_i+c_i)u) \Big]$$
$$= \gamma n - \gamma \frac{1}{|R^{\times}|} \sum_{i=1}^{n} \sum_{u \in R^{\times}} \chi(x_iu) \frac{1}{|C|} \sum_{c \in C} \chi(c_iu).$$

Clearly the projection of $\,C\,$ onto some $\,i\,{\rm th}$ coordinate is an ideal of $\,R\,,$ and since $\,\chi\,$ is a generating character we have

$$\frac{1}{|C|} \sum_{c \in C} \chi(c_i u) = \begin{cases} 0 : i \in \operatorname{supp}(C), \\ 1 : \operatorname{otherwise}, \end{cases}$$

and hence

$$\frac{1}{|C|} \sum_{c \in C} w(x+c) = \gamma n - \gamma \frac{1}{|R^{\times}|} \sum_{i=1}^{n} \sum_{u \in R^{\times}} \chi(x_{i}u)$$
$$= \gamma \ell(C) + \sum_{i \notin \text{supp}(C)} \gamma \left[1 - \frac{1}{|R^{\times}|} \sum_{u \in R^{\times}} \chi(x_{i}u) \right]$$
$$= \gamma \ell(C) + \sum_{i \notin \text{supp}(C)} w(x_{i}),$$

which was the claim.

Given a linear code $\,C\,\leq\,_R R^n\,$ and a subset $\,S\,\subseteq\,\{1,\ldots,n\}\,,$ we define the code

$$Sho(C, S) := \{c \in C \mid supp(c) \subset S\}$$

which is essentially (namely up to omitting vanishing coordinates) a shortened code. Moreover, we define the residual code

$$\operatorname{Res}(C,S) := \{ (c_i)_{i \notin S} \mid c \in C \}.$$

Denoting by π_S the projection of \mathbb{R}^n onto the coordinates *not* contained in S, it is clear that $\operatorname{Sho}(C, S) = \ker(\pi_S) \cap C$ and $\operatorname{Res}(C, S) = \pi_S(C)$. Obviously, these codes are related by $C/\operatorname{Sho}(C, S) \cong \operatorname{Res}(C, S)$.

Finally, for arbitrary $x \in \mathbb{R}^n$, for the sake of simplicity of notation we write $\operatorname{Sho}(C, x)$ to mean $\operatorname{Sho}(C, \operatorname{supp}(x))$ and $\operatorname{Res}(C, x)$ in place of $\operatorname{Res}(C, \operatorname{supp}(x))$. Likewise we will write π_x where $\pi_{\operatorname{supp}(x)}$ is meant.

In general there is no relationship between $\operatorname{Sho}(C, x)$ and Rx, except that for $x \in C$ there holds $\operatorname{Sho}(C, x) \geq Rx$. The following lemma gives a condition for equality in this containment.

Lemma 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 $\gamma \ell(c) < d$. Then $\operatorname{Sho}(C, c) = Rc$.

Proof: Assuming that there exists $x \in \text{Sho}(C, c)$ that is not contained in Rc we first observe that $0 \notin x + Rc$, which implies

$$d \leq \frac{1}{|Rc|} \sum_{y \in Rc} w(x+y)$$

We have $\operatorname{supp}(x) \subseteq \operatorname{supp}(c)$ and thus may use Lemma 1 to observe

$$\frac{1}{|Rc|} \sum_{y \in Rc} w(x+y) = \gamma \ell(c) + \sum_{i \not\in \text{supp}(c)} w(x_i) = \gamma \ell(c) < d,$$

which is a contradiction showing the claim.

Corollary 1 Let $C \leq {}_{R}R^{n}$ be of homogeneous minimum weight d, and let $c \in C$ satisfy $\gamma \ell(c) < d$. Then $\operatorname{Res}(C, c)$ is of length $n - \ell(c)$, homogeneous minimum weight at least $d - \gamma \ell(c)$, and satisfies $|\operatorname{Res}(C, c)| = |C|/|Rc|$.

Proof: Let $\operatorname{Res}(C, c)$ have minimum homogeneous weight d', and let $x \in C$ such that $w(\pi_c(x))$ assumes d'. Then, invoking Lemma 1, we have

$$d \leq \gamma \ell(c) + \sum_{i \notin \text{supp}(c)} w(x_i) = \gamma \ell(c) + w(\pi_c(x)) = \gamma \ell(c) + d',$$

which yields $d' \ge d - \gamma \ell(c)$. Our claim regarding the size of $\operatorname{Res}(C, c)$ follows from the fact that $\operatorname{Sho}(C, c) = Rc$.

Example 2 Let C be the \mathbb{Z}_4 -linear Octacode generated by

[1	0	0	0	3	1	2	1
0	1	0	0	1	2	3	1
0	0	1	0	3	3	3	2
0	0	0	1	2	3	1	1

The code C has 256 words and minimum Lee distance 6 (cf. [7]). It contains the word c = [0, 0, 0, 2, 0, 2, 2, 2] which satisfies $\gamma \ell(c) = 4 < 6 = d$ where we recall that the Lee weight is homogeneous with $\gamma = 1$. Clearly, |Rc| = 2and we puncture C on the coordinates 4, 6, 7, 8 to obtain $\operatorname{Res}(C, c)$, which by Corollary 1 is a linear $[4, d' \geq 2]$ code of size 128. Considering the Gray image (cf. [7]) of $\operatorname{Res}(C, c)$ we arrive at an $(8, 128, \geq 2)$ code that obviously meets the (traditional) Singleton bound. This shows that d' = 2 and hence, $\operatorname{Res}(C, c)$ is an optimal code.

3 A Refinement of the Plotkin Bound

If a linear code $C \leq {}_{R}R^{n}$ has maximal support, meaning $\ell(C) = n$, then by observations in [6] or by applying Lemma 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 Plotkinlike bound for linear codes.

Theorem 1 Let $C \leq {}_{R}R^{n}$ be a linear [n, d] code satisfying $\gamma n < d$, and let $c \in C$ be such that $\gamma \ell(c) < d$. Then there holds

$$|C| \leq |Rc| \frac{d - \gamma \ell(c)}{d - \gamma n}.$$

Proof: Suppose that $C_1 := \operatorname{Res}(C, c)$ has length n_1 and minimum homogeneous weight d_1 . From (1) and Corollary 1 we have

$$n = \ell(c) + n_1 \ge \ell(c) + \frac{|C_1| - 1}{|C_1|} \frac{d_1}{\gamma} \ge \ell(c) + \frac{|C_1| - 1}{|C_1|} \left(\frac{d}{\gamma} - \ell(c)\right)$$

From Corollary 1 we know that $|C_1| = |C|/|Rc|$, which gives

$$n \ge \ell(c) + \left(1 - \frac{|Rc|}{|C|}\right) \left(\frac{d}{\gamma} - \ell(c)\right).$$

Rearranging this inequality yields the result.

C

is

Example 3 Let
$$m \in \mathbb{N}$$
 and let $n = m \times (|R|^m - 1)$. We consider the code $C \leq {}_{R}R^n$ which is generated by the $m \times n$ matrix G whose columns comprise the distinct nonzero elements of R^m . It is not difficult to see that C is a constant weight code of homogeneous weight $\gamma |R|^m$. If namely $x \in R^m$ then

$$\begin{split} w(xG) &= \sum_{g \in R^m} w(x \cdot g) = \sum_{g \in R^m} \gamma \Big[1 - \frac{1}{|R^{\times}|} \sum_{u \in R^{\times}} \chi(ux \cdot g) \Big] \\ &= \gamma \Big[|R|^m - \frac{1}{|R^{\times}|} \sum_{u \in R^{\times}} \sum_{g \in R^m} \chi(ux \cdot g) \Big] \\ &= \begin{cases} 0 &: x = 0 \\ \gamma |R|^m : \text{otherwise.} \end{cases} \end{split}$$

Moreover, $n=|R|^m-1<|R|^m=\frac{d}{\gamma}$. It can also be shown that $\ell(c)\leq n<\frac{d}{\gamma}$ for each word $c\in C$. The Hamming weight of an arbitrary word c=xG of

C corresponds to the size of the annhibitor submodule $\,x^\perp=\{y\in R^m\mid x\cdot y=0\}\leq R^m_R\,$ by the equation

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

Therefore, the upper bound on |C| determined by Theorem 1 is

$$|C| \leq |Rc| \frac{d - \gamma \ell(c)}{d - \gamma n} = |Rc| \Big[|R|^m - |R|^m + \frac{|R|^m}{|Rc|} \Big] = |R|^m$$

which is met sharply by C.

We will refer to the code in the preceding example as a *Simplex code*.

Corollary 2 Let $C \leq {}_{R}R^{n}$ be 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 [6] for $\ell < \frac{d}{\gamma} < \ell \frac{|R|}{|R|-1}$.

In fact we can do even better, taking into account some properties of R. For this, we first make an elementary but useful observation.

Lemma 3 Let $C \leq {}_{R}R^{n}$ and let $c \in C$ have minimum Hamming weight in C. Then there exists $\alpha \in R$ and a family $(u_{i})_{i \in \text{supp}(c)}$ of invertible elements of R such that $c_{i} = \alpha u_{i}$ for all $i \in \text{supp}(c)$. In particular, $Rc \cong R\alpha$.

Proof: Since c is of minimal Hamming weight, we have $\ell(\lambda c) = \ell(c)$ for each $\lambda \in R$, unless $\lambda c = 0$. For this reason, the left annihilators $c_i^{\perp} := \{\lambda \in R \mid \lambda c_i = 0\}$ must all be the same for $i \in \operatorname{supp}(c)$, which holds if and only if the $c_i R$ coincide for all such $i \in \operatorname{supp}(c)$. Then the claim follows from [12, Thm 5.1].

Lemma 4 Let $C \leq {}_{R}R^{n}$ be a linear code of minimum homogeneous weight d and minimum Hamming weight ℓ where $\gamma \ell < d$. If $c \in C$ is a word of minimum Hamming weight then Rc is a simple submodule of C.

Proof: Suppose that $Rc' \leq Rc$ for some nonzero $c' \in C$. Then $\ell(c) = \ell(c')$ and in particular supp(c') = supp(c). By Lemma 2, we find that Rc' = Sho(C, c') = Sho(C, c) = Rc. Thus Rc is a simple submodule of C. □

Corollary 3 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

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

Proof: Let $c \in C$ be of Hamming weight ℓ . By the preceding lemma we know that Rc is a simple submodule of C. Combining this with Corollary 2 the claim follows immediately. □

Example 4 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 so, from Corollary 3, we have

$$16^m = |C| \le 4 \frac{16^m \gamma - \frac{3}{4} 16^m \gamma}{16^m \gamma - (16^m - 1)\gamma} = 4 \frac{16^m}{4} = 16^m$$

showing that the bound in the previous corollary is met sharply.

3.1 A Singleton bound

Let C be an [n,d] code over R satisfying $n \leq \frac{d}{\gamma}$. If $c \in C$ is a codeword satisfying $\ell := \ell(c) < n \leq \frac{d}{\gamma}$ then by Corollary 1 we see that $C_1 := \operatorname{Res}(C,c)$ is an $[n_1,d_1]$ code over R, isomorphic to C/Rc with $d_1 \geq d - \gamma \ell$ and

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

Setting $C_0 := C$, we construct a sequence of $[n_i, d_i]$ codes C_i as follows: for each i, as long as there exists $c^i \in C_i$ with Hamming weight $\ell_i := \ell(c^i) < n_i$, define $C_{i+1} := \operatorname{Res}(C_i, c^i)$. We observe that $n \leq \frac{d}{\gamma}$ implies $\ell_i < n_i = n_{i-1} - \ell_i < \frac{d_i}{\gamma}$ for each $i \geq 1$. Therefore, from Lemma 2 we have a finite sequence of codes

$$C_0 = C, \ C_1 \cong C_0/Rc^0, \ C_2 \cong C_1/Rc^1, ..., \ C_r \cong C_{r-1}/Rc^{r-1}$$

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

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

Note 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 $c^r \in C_r$ will result in a code of length zero. Employing a simple counting argument (e.g. traditional Singleton bound for the Hamming distance) it can be shown that $|C_r| \leq |R|$.

From Equation (2) we have

$$C| = |Rc^{0}| |Rc^{1}| \cdots |Rc^{r-1}| |C_{r}|.$$
(3)

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

$$n = \sum_{i=0}^{r} \ell_i \ge \frac{|Rc| - 1}{|Rc|} \frac{d}{\gamma} + \sum_{i=1}^{r} \ell_i$$
(4)

$$\geq \frac{|Rc| - 1}{|Rc|} \frac{d}{\gamma} + r,\tag{5}$$

This will yield a type of Singleton bound for the homogeneous weight. First we need one further observation.

Lemma 5 Let C be an [n,d] code over R satisfying $\gamma n \leq d$. Let $Q := \max\{|Rc| \mid c \in C\}$ and let $P := \max\{|Rc| \mid c \in C, \ell(c) < n\}$. If $c \in C$ satisfies $\ell(c) < n$ then $|Rc'| \leq Q$ for each $c' \in \operatorname{Res}(C,c)$. Moreover, if $\ell(c') < n - \ell(c)$ then $|Rc'| \leq P$.

Proof: Let $c' \in \operatorname{Res}(C, c)$. From Lemma 2, we have $\operatorname{Res}(C, c) \cong C/Rc$ and hence, there is some $x \in C$ such that $Rc' \cong (Rx + Rc)/Rc$. Consequently,

$$|Rc'| = \frac{|Rx + Rc|}{|Rc|} = \frac{|Rx|}{|Rx \cap Rc|} \le |Rx| \le Q$$

If |Rc'| > P then |Rx| > P and hence $\ell(x) = n$, which implies $\ell(c') = n - \ell(c)$.

Theorem 2 Let C be an [n,d] code over R satisfying $\gamma n \leq d$ and with minimum Hamming weight less than n. Let $P := \max\{|Rc| \mid c \in C, \ell(c) < n\}$. Then

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

Proof: Let $c \in C$ such that |Rc| = P. With the same notation as before, from Lemma 2 and Corollary 1, there exists a sequence of words $c = c^0, c^1, ..., c^{r-1}$ and linear codes $C = C_0, C_1, ..., C_r$ such that, for i = 1, ..., r, $C_i := \operatorname{Res}(C_{i-1}, c^{i-1})$ is an $[n_i, d_i]$ code, and for i = 0, ..., r-1, $c^i \in C_i$, $\ell(c^i) < n_i \leq \frac{d_i}{\gamma}$ and $C_i \cong C_{i-1}/Rc^{i-1}$. As observed in Lemma 5, we have $|Rc^i| \leq P$ for i = 1, ..., r-1. The code $C_r = \operatorname{Sho}(C_r, c^r)$ has constant Hamming weight n_r and hence $|C_r| \leq |R|$. Then

$$|C| = |Rc| |Rc^{1}| \cdots |Rc^{r-1}| |C_{r}| \le P^{r} |R|,$$

so clearly $r \ge \lceil \log_P |C| - \log_P |R| \rceil$. The inequality in (5) gives

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

Corollary 4 Let C be an [n,d] code over R satisfying $n < \frac{d}{\gamma}$, and let $Q := \max\{|Rc| \mid c \in C\}$. Then

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

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

Proposition 3 Let $C \leq {}_{R}R^{n}$ be an [n,d] linear code and suppose that $\gamma n \leq d$. Then

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

We give an example of what could be called an MDS code over a finite chain ring R, using points from a *projective Hjelmslev geometry*.

Example 5 Let R be a chain ring of length 2 with q-element residual field. Then $R^{\times} = R \setminus \operatorname{rad}(R)$ and $|R| = q^2$. Let $F := R^2 \setminus \operatorname{rad}(R^2)$. We denote by $\operatorname{PHG}(R^2)$ the projective Hjelmslev line with point set $\mathcal{P} := \{xR \mid x \in F\}$. Note that \mathcal{P} contains $q^2 + q$ distinct points (cf. [10, p. 83]).

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

$$w(xG) = |J_1| + \frac{q}{q-1}|J_2| = \begin{cases} q^2 + \frac{q}{q-1}(q-1) = q^2 + q : x \in F \\ q^2 \frac{q}{q-1} = \frac{q^3}{q-1} & : x \in \operatorname{rad}(R^2), \ x \neq 0 \end{cases}$$

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

$$n - \left\lceil \frac{q^2 - 1}{q^2} d \right\rceil = n - \left\lceil \frac{q^2 - 1}{q^2} (q^2 + q) \right\rceil = n - \left\lceil q^2 + q - 1 - \frac{1}{q} \right\rceil$$

= $q^2 + q - q^2 - q + 1 = 1 = r,$

which meets the bound given in Theorem 2.

References

- E. Byrne, M. Greferath and 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.
- I. Constantinescu, Lineare Codes über Restklassenringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik, Ph.D. thesis, Technische Universität München, 1995.
- 3. I. Constantinescu and W. Heise, A metric for codes over residue class rings of integers, Problemy Peredachi Informatsii **33** (1997), no. 3, 22–28.
- 4. M. Greferath and S. E. Schmidt, *Finite-Ring Combinatorics and MacWilliams Equivalence Theorem*, J. of Combinatorial Theory (A) **92** (2000), 17–28.
- M. Greferath, G. McGuire, M. E. O'Sullivan, On Plotkin Optimal Codes over Finite Frobenius Rings, Journal of Algebra and Its Applications 5 (2006), no. 6, 799-815.
- M. Greferath and M. E. O'Sullivan, On Bounds for Codes over Frobenius Rings under Homogeneous Weights, Discrete Mathematics 289 (2004), 11–24.
- A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* Z₄-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40 (1994), 301–319.
- 8. W. Heise, T. Honold, A. A. Nechaev, Weighted modules and representations of codes, Proceedings of the ACCT 6 (Pskov, Russia, 1998), 123-129.
- T. Honold, A characterization of finite Frobenius rings, Arch. Math. (Basel), 76 (2001), 406–415.
- R. Kaya, P. Plaumann, K. Strambach, *Rings and Geometry*, NATO ASI Series, Reidel, (1984).
- 11. A. A. Nechaev, Kerdock codes in a cyclic form, Discrete Math. Appl. 1 (1991), 365–384.
- J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121 (1999), 555–575.