21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

A Grey-Rankin Bound for Codes over Frobenius Rings

Marcus Greferath [1] and Jens Zumbrägel [2]

***Abstract*— We provide a generalized version of the Grey-Rankin bound for self-complementary codes over finite Frobenius rings and present some examples where the bound can be applied and where the bound is sharp.**

I. Introduction

Codes over ring alphabets have become prominent when it was discovered at the end of the previous century that large families of non-linear binary codes of high quality could be derived from $\mathbb{Z}_4$-linear codes.

Since then a number of authors have dedicated their work to codes over rings and published foundational results as well as constructions of codes that outperform traditional finite-field linear codes.

Particular interest of algebraic coding theory over rings is in code optimality, and hence in bounds on the sizes and minimum distances of codes over rings. In that respect several papers have been published, among them the author's previous work on Plotkin and Elias bound (cf. [3]) as well as the paper [2] dealing with possible generalizations of the Griesmer bound.

This paper aims at a generalization of the Grey-Rankin bound for self-complementary codes over finite Frobenius rings that are equipped with the homogeneous weight. We will derive such a bound and present examples where the bound can be applied and where the bound is sharp. We thereby generalize the classical Grey-Rankin bound for binary self-complementary codes (cf. [6]) as well as the q-ary version of the Grey-Rankin bound given by Bassalygo, Dodunekov, Helleseth, and Zinoviev [1].

II. Proof of the Grey-Rankin bound

Let R be a finite Frobenius ring and let χ be a generating character of R. Let $w : R \longrightarrow \mathbb{Q}$ be the homogeneous weight on R with average value $\gamma \geq 0$, which can be written as

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

As common in coding theory, we extend w additively to the ambient space R^n, where n is a positive integer. Furthermore, for any vectors $x, y \in R^n$ we let their distance be $d(x,y) = w(x-y) = \sum_{i=1}^n w(x_i - y_i)$.

*This work was supported by Science Foundation Ireland under grant 08/IN.1/I1950 and Irish Research Council cofunded by Marie Curie Actions under grant ELEVATEPD/2013/82

[1] Marcus Greferath is with the School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland marcus.greferath@ucd.ie

[2] Jens Zumbrägel is with the Institute of Algebra, Dresden University of Technology, 01062 Dresden, Germany jens.zumbragel@ucd.ie

By a *code* C of length n we mean any nonempty subset of R^n; we will *not* assume linearity of the code unless stated otherwise. We assume $C \times C$ being equipped with the uniform probability distribution and consider the distance function

$$d_C : C \times C \longrightarrow \mathbb{Q}\,, \quad (x,y) \mapsto w(x-y)$$

as a random variable. In order to derive a Grey-Rankin bound we will bound the variance of d_C from below and above. Whereas the lower bound will hold for any code with expected value $\mathrm{E}(d_C) = \gamma n$, the upper bound will require some self-complementariness property.

A. Lower Bound on the Variance

Proposition 1: Assume the code $C \subseteq R^n$ is of average distance $\mathrm{E}(d_C) = \gamma n$. Then its distance variance is bounded from below as

$$\mathrm{Var}(d_C) \;\geq\; \frac{\gamma^2 n}{|R^\times|}\,.$$

Proof: We compute

$$\begin{aligned}
\mathrm{Var}(d_C) &= \frac{1}{|C|^2}\sum_{x,y\in C}\big(\gamma n - d_C(x,y)\big)^2 \\
&= \frac{1}{|C|^2}\sum_{x,y\in C}\big(\sum_{i=1}^n(\gamma - w(x_i-y_i))\big)^2 \\
&= \frac{1}{|C|^2}\sum_{x,y\in C}\sum_{i,j=1}^n(\gamma - w(x_i-y_i))(\gamma - w(x_j-y_j)) \\
&= \frac{\gamma^2}{|C|^2|R^\times|^2}\sum_{x,y\in C}\sum_{i,j=1}^n\sum_{u,v\in R^\times}\chi((x_i-y_i)u)\,\chi((x_j-y_j)v) \\
&= \frac{\gamma^2}{|C|^2|R^\times|^2}\sum_{i,j=1}^n\sum_{u,v\in R^\times}\sum_{x,y\in C}\chi(x_iu+x_jv)\,\overline{\chi(y_iu+y_jv)} \\
&= \frac{\gamma^2}{|C|^2|R^\times|^2}\sum_{i,j=1}^n\sum_{u,v\in R^\times}\big|\sum_{x\in C}\chi(x_iu+x_jv)\big|^2 \\
&\geq \frac{\gamma^2}{|C|^2|R^\times|^2}\sum_{i=1}^n\sum_{u\in R^\times}\big|\sum_{x\in C}\chi(x_iu-x_iu)\big|^2 = \frac{\gamma^2 n}{|R^\times|}\,,
\end{aligned}$$

so that $\mathrm{Var}(d_C) \geq \frac{\gamma^2 n}{|R^\times|}$, as desired. ∎

The following property of the homogeneous weight will be useful, particularly when securing the premise of the foregoing proposition.

Lemma 2: Let $c \in R\setminus\{0\}$, $a \in R$, and consider $S := Rc + a \subseteq R$. Then

$$\frac{1}{|S|}\sum_{x\in S} w(x) = \gamma\,.$$

ISBN: 978-90-367-6321-9

Proof: We find that

$$\gamma - \frac{1}{|S|}\sum_{s\in S} w(s) \;=\; \frac{1}{|S|\,|R^\times|}\sum_{s\in S}\sum_{u\in R^\times}\chi(su)$$
$$= \frac{1}{|S|\,|R^\times|}\sum_{u\in R^\times}\sum_{x\in Rc}\chi((x+a)u)$$
$$= \frac{1}{|S|\,|R^\times|}\sum_{u\in R^\times}\chi(au)\sum_{x\in Rc}\chi(xu) \;=\; 0\,,$$

since Rcu is a nonzero left ideal for all $u\in R^\times$. ∎

Remark 3: Let C be a code of length n. Consider the coordinate projections $\pi_i : C \longrightarrow R$, $x \mapsto x_i$, for $i\in\{1,\ldots,n\}$. Suppose these maps have image $\pi_i(C) = Rc_i + a_i$ for some $c_i \in R\setminus\{0\}$ and $a_i \in R$, and are uniformly distributed onto this image. Then for all $y\in R^n$ we have

$$\frac{1}{|C|}\sum_{x\in C} w(x_i - y_i) \;=\; \gamma$$

by applying Lemma 2 with $S = Rc_i + a_i - y_i$. Therefore,

$$\mathrm{E}(d_C) \;=\; \frac{1}{|C|^2}\sum_{x,y\in C} w(x-y)$$
$$= \frac{1}{|C|}\sum_{y\in C}\sum_{i=1}^{n}\frac{1}{|C|}\sum_{x\in C} w(x_i-y_i) \;=\; \gamma n\,.$$

Remark 4: Let now C be a *linear code* of length n, i.e., C is a left submodule of R^n. We again assume the uniform probability distribution on C and consider the weight $w_C : C\longrightarrow\mathbb{Q}$, $x\mapsto w(x)$ as a random variable; it will have the same distribution as the distance random variable d_C. If all (linear) coordinate projections π_i are nonzero then Remark 3 applies, so we have $\mathrm{E}(w_C) = \gamma n$, and therefore

$$\mathrm{Var}(w_C) \;\geq\; \frac{\gamma^2 n}{|R^\times|}\,.$$

Moreover, we observe that in the proof of Proposition 1 we have $\sum_{x\in C}\chi(x_iu + x_jv) = 0$ except if $x_iu = -x_jv$ for all $x\in C$. It then follows that as soon as the coordinate maps π_i are linearly independent then equality holds, i.e., $\mathrm{Var}(w_C) = \frac{\gamma^2 n}{|R^\times|}$.

B. Upper Bound on the Variance

As is common in coding theory, a subset $C\subseteq R^n$ is called an (n,M,d) *code* if $|C| = M$ and its minimum distance

$$\min_{\substack{x,y\in C\\ x\neq y}} d(x,y) = \min_{\substack{x,y\in C\\ x\neq y}} w(x-y) \;=\; d.$$

Our generalization of the notion of self-complementary codes appears in the statement of the next result.

Proposition 5: Assume the (n,M,d) code C is partitioned into subcodes $C_1,\ldots C_{\frac{M}{L}}$ of size L such that

$$\frac{1}{L}\sum_{y\in C_k} d(x,y) \;=\; \gamma n$$

for all $k = 1,\ldots,\frac{M}{L}$ and $x\in C$. Then

$$\mathrm{Var}(d_C) \;\leq\; \frac{M-L}{M}(L-1)(\gamma n - d)^2 + \frac{L^2}{M^2}\sum_k \mathrm{Var}(d_{C_k})\,,$$

where $\mathrm{Var}(d_{C_k}) = \frac{1}{L^2}\sum_{x,y\in C_k}(d(x,y)-\gamma n)^2$.

Proof: We have $\mathrm{E}(d_C) = \gamma n$, since $\frac{1}{M}\sum_{y\in C} d(x,y) = \gamma n$ for all $x\in C$. Therefore,

$$\mathrm{Var}(d_C) = \frac{1}{M^2}\sum_{x,y\in C}(d(x,y)-\gamma n)^2$$
$$= \frac{1}{M^2}\sum_{j,k=1}^{\frac{M}{L}}\sum_{x\in C_j}\sum_{y\in C_k}(d(x,y)-\gamma n)^2\,.$$

We show that $\sum_{y\in C_k}(d(x,y)-\gamma n)^2 \leq L(L-1)(\gamma n-d)^2$ whenever $x\notin C_k$, i.e., $j\neq k$, from which the proposition follows easily.

Let $x\notin C_k$ be fixed and write $t_1,\ldots,t_L$ for the distances $d(x,y)$, $y\in C_k$, so that $\sum_{y\in C_k}(d(x,y)-\gamma n)^2 = \sum_\ell (t_\ell - \gamma n)^2$, where $t_\ell \geq d$ for all ℓ and $\sum_\ell t_\ell = L\gamma n$ by assumption. Then the maximum value of $\sum_\ell(t_\ell-\gamma n)^2$ is attained for $t_\ell = d$ for $\ell < L$ and $t_L = L\gamma n - (L-1)d$. Accordingly, it follows that

$$\sum_\ell (t_\ell-\gamma n)^2 \;\leq\; (L-1)\,(\gamma n - d)^2 + \big((L-1)\,(\gamma n-d)\big)^2$$
$$= L\,(L-1)\,(\gamma n-d)^2\,,$$

as desired. ∎

Lemma 6: Let $C = Rc + a$, where $c\in(R^\times)^n$ and $a\in R^n$. Then

$$\mathrm{Var}(d_C) \;=\; \frac{\gamma^2 n^2}{|R^\times|}\,.$$

Proof: By Lemma 2 we have $\mathrm{E}(d_C) = \gamma n$, and from by the proof of Proposition 1 it follows that

$$\mathrm{Var}(d_C) \;=\; \frac{\gamma^2}{|C|^2|R^\times|^2}\sum_{i,j=1}^{n}\sum_{u,v\in R^\times}\Big|\sum_{x\in C}\chi(x_iu + x_jv)\Big|\,.$$

Now the map $C\longrightarrow R$, $x\mapsto x_iu + x_jv$ is affine linear; it is constant if and only if $c_iu + c_jv = 0$, and otherwise it holds $\sum_{x\in C}\chi(x_iu+x_jv) = 0$. Since all $c_i\in R^\times$, the number of quadruples (i,j,u,v) such that $c_iu + c_jv = 0$ equals $n^2|R^\times|$, hence we conclude that

$$\mathrm{Var}(d_C) = \frac{\gamma^2}{|R^\times|^2}\,n^2\,|R^\times| = \frac{\gamma^2 n^2}{|R^\times|}\,,$$

as stated. ∎

Remark 7: Consider the finite field case $R = \mathbb{F}_q$, so that $w = w_H$, the Hamming weight, with $\gamma = \frac{q-1}{q}$. Let C be any (q,n,q) code, then

$$\mathrm{Var}(d_C) \;=\; \frac{(q-1)\,n^2}{q^2}\,,$$

so that $\mathrm{Var}(d_C) = \frac{\gamma^2 n^2}{|R^\times|}$ as in Lemma 6 as well.

Indeed, $\mathrm{E}(d_C) = \gamma n$ by Remark 3 and thus $\mathrm{Var}(d_C) = \frac{1}{q^2}\sum_{x,y\in C}\big(d(x,y)-\gamma n\big)^2 = \frac{1}{q^2}\big(q(q-1)(n-\gamma n)^2 + q(\gamma n)^2\big) = \frac{1}{q^3}\big((q-1)+(q-1)^2\big) = \frac{1}{q^2}(q-1)n^2$.

Now combining the lower bound and the upper bound on the distance variance we get our main result.

Theorem 8: Let C be an (n, M, d) code that is partitioned into subcodes $C_k = Rc_k + a_k$ for some $c_k \in (R^\times)^n$ and $a_k \in R^n$ for all k. Then

$$M \le |R| \frac{\gamma^2 n^2 - |R^\times|(|R|-1)(\gamma n - d)^2}{\gamma^2 n - |R^\times|(|R|-1)(\gamma n - d)^2},$$

provided the denominator is positive.

Proof: From Proposition 1 and Proposition 5 with Lemma 6 we get

$$\frac{\gamma^2 n}{|R^\times|} \le \mathrm{Var}(d_C) \le \frac{M-|R|}{M}(|R|-1)(\gamma n - d)^2 + \frac{|R|}{M}\frac{\gamma^2 n^2}{|R^\times|},$$

from which the stated bound follows easily. ∎

III. Special Cases and Applications

In the following it is understood that the upper bounds only apply if the denominator is positive. When R is a finite field $\mathbb{F}_q$ we re-establish the q-analog of the Grey-Rankin bound proved in [1, Thm. 2]. Note however that [1] proves a slightly more general version of the bound, where the alphabet size q may be any integer.

Theorem 9: Let C be an (n, M, d) code over a finite field $\mathbb{F}_q$ that is partitioned into a set of (n, q, n) subcodes. Then

$$M \le q \frac{n^2 - ((q-1)n - qd)^2}{n - ((q-1)n - qd)^2}.$$

Proof: This result can be established exactly the same way as Theorem 8, only this time using Proposition 1 and Proposition 5 with Remark 7. ∎

In particular, for $q = 2$ we deduce the classical Grey-Rankin bound for self-complementary binary (n, M, d) codes (see [6]), namely

$$M \le \frac{8\,d\,(n-d)}{n - (n-2d)^2}.$$

As codes over the ring $R = \mathbb{Z}_4$ equipped with the Lee weight are of particular importance, we also state the bound for this case explicitly.

Theorem 10: Let C be an (n, M, d) code over $R = \mathbb{Z}_4$ equipped with the Lee weight and let C be partitioned into subcodes $C_k = Rc_k + a_k$ for some $c_k \in (R^\times)^n$ and $a_k \in R^n$ for all k. Then

$$M \le 4 \cdot \frac{n^2 - 6\,(n-d)^2}{n - 6\,(n-d)^2}.$$

Proof: Apply Theorem 8 and note that for $R = \mathbb{Z}_4$ the Lee weight is the homogeneous weight with $\gamma = 1$. ∎

A. Codes Meeting the Grey-Rankin Bound

It is clear that codes with parameters $(n, |R|n, \gamma n)$ meet the bound of Theorem 8. In the Hamming weight scenario such codes are called *difference matrix codes* in [1], and it is shown [1, Th. 3] that these codes automatically satisfy the self-complementariness property of Theorem 9.

In [1], also a construction of such codes, over finite fields, is given. We present a family of these codes over local Frobenius rings.

Proposition 11: Let R be a finite local Frobenius ring. For any positive integer m and $n = |R|^m$ there exists a linear $(n, |R|n, \gamma n)$ code C partitioned into a family of subcodes $C_k = Rc_k + a_k$ for some $c_k \in (R^\times)^n$ and $a_k \in R^n$ for all k, i.e., for which the bound of Theorem 8 is sharp.

Proof: Consider the codewords as maps $R^m \to R$ and let C be the code consisting of all affine linear maps $f : R^m \to R$, where $f(x_1, \ldots, x_m) = \sum_i x_i c_i + a$, for some $c_1, \ldots, c_m \in R$ and $a \in R$.

If such an affine map f is non-constant, then $w(f) = \gamma n$ by Lemma 2. Otherwise, if $f \equiv a$ is a non-zero constant map then $w(f) = w(a)\,n \ge \gamma n$, since R is a local Frobenius ring. Hence, C is an $(n, |R|n, \gamma n)$ code.

Clearly, C can be partitioned into subcodes $C_k = Rh + f_k$, where $h \equiv 1$ is the constant map. ∎

B. Application to Recently Found Quaternary Codes

Kiermaier and Zwanzger recently report [4], [5] on the existence of some $\mathbb{Z}_4$-linear codes with very good parameters, so that their binary images under the grey map are better than any binary linear codes known. The natural question arises whether self-complementary codes with the same parameters, either over $\mathbb{Z}_4$ or over $\mathbb{F}_2$, exist.

In particular, a code over $\mathbb{Z}_4$ with parameters $(29, 128, 28)$ was derived from a hyperoval [4]; its grey image is a $(58, 128, 28)$ binary code. Now the bound from Theorem 10 gives $M \le 145$ and the binary Grey-Rankin bound gives $M \le 124$. Therefore, codes with these parameters cannot be self-complementary over $\mathbb{F}_2$, but might be self-complementary over $\mathbb{Z}_4$.

Furthermore, codes over $\mathbb{Z}_4$ with parameters $(57, 256, 56)$ and $(994, 4096, 992)$ were found [5]; their grey image are $(114, 256, 56)$ and $(1988, 4096, 992)$ codes. Here the bound from Theorem 10 gives $M \le 254$ and $M \le 4074$, respectively, and the binary bound states that $M \le 236$ and $M \le 4008$, respectively. Consequently, codes with these parameters cannot be self-complementary, neither over $\mathbb{Z}_4$, nor over $\mathbb{F}_2$.

References

[1] L. Bassalygo, S. Dodunekov, T. Helleseth, V. Zinoviev, On a New q-ary Combinatorial Analog of the Binary Grey-Rankin Bound and Codes Meeting This Bound, Proc. IEEE Information Theory Workshop (ITW 2006), Punta del Este, Uruguay, 5 p., March 2006.

[2] E. Byrne, M. Greferath, A. Kohnert, V. Skachek, New Bounds for Codes over Finite Frobenius Rings, Des. Codes Cryptogr. 57 (2010), pp. 169–179.

[3] M. Greferath, M. E. O'Sullivan, On Bounds for Codes over Frobenius Rings under Homogeneous Weights, Discr. Math. 289 (2004), pp. 11–24.

[4] M. Kiermaier, J. Zwanzger, A $\mathbb{Z}_4$-Linear Code of High Minimum Lee Distance Derived from a Hyperoval, Adv. Math. Comm. 5 (2011), pp. 275–286.

[5] M. Kiermaier, J. Zwanzger, A New Series of $\mathbb{Z}_4$-Linear Codes of High Minimum Lee Distance Derived from the Kerdock Codes, Proc. Mathematical Theory of Networks and Systems (MTNS 2010), Budapest, Hungary, 4 p., July 2010.

[6] G. McGuire, Quasi-Symmetric Designs and Codes Meeting the Grey-Rankin Bound, J. Combin. Th., Ser. A 78 (1997), pp. 280–291.