



Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

# On Existence Bounds for Codes over Rings

Marcus Greferath

Claude Shannon Institute for Discrete Mathematics, Coding  
and Cryptography Ireland — University College Dublin

CIMPA Summer School  
Ankara, Turkey 2008



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# A suitable class of rings

## Finite Frobenius rings

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Definition:** For a finite Ring  $R$  we define

- $\hat{R} := \text{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$ , the character module of  $R$ , and
- $\text{soc}({}_R R) := \sum \{I \leq {}_R R \mid I \text{ minimal}\}$ , the (left) socle of  $R$ .

$R$  is called a Frobenius ring, if any of the following equivalent condition holds:

- ${}_R R \cong {}_R \hat{R}$
- $R_R \cong \hat{R}_R$
- $\text{soc}({}_R R)$  is left principal
- $\text{soc}(R_R)$  is right principal



# Examples of finite Frobenius rings

How the Frobenius property inherits

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

## Examples:

- Every finite field is Frobenius.
- Every Galois ring is Frobenius.
- If  $R$  and  $S$  are Frobenius, then so will be  $R \times S$ .
- If  $R$  is Frobenius, then so will be  $M_n(R)$ .
- If  $R$  is Frobenius and  $G$  is a finite group, then  $R[G]$  is Frobenius.

**Note:** The class of finite Frobenius rings is large. As a non-Frobenius example consider  $\mathbb{Z}_2[x, y]/(x^2, y^2, xy)$ .



# An important weight function

The homogeneous weight

**Definition:** Let  $R$  be a finite ring. A mapping  $w : R \rightarrow \mathbb{Q}$  is called (left) homogeneous weight if  $w(0) = 0$  and there is  $\gamma \in \mathbb{Q}$  such that for all  $x, y \in R$  there holds:

- (i)  $Rx = Ry$  implies  $w(x) = w(y)$ ,
- (ii)  $\sum_{y \in Rx} w(y) = \gamma |Rx|$  whenever  $x \neq 0$ .

**Examples:** The Hamming weight on  $\mathbb{F}_q$  is homogeneous with  $\gamma = \frac{q-1}{q}$ . The Lee weight on  $\mathbb{Z}_4$  is homogeneous with  $\gamma = 1$ .

**Question:** Do homogeneous weights exist on every finite ring?

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References



# Homogeneous weights on Frobenius rings

## Existence and uniqueness

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation  
Krawtchouk  
Polynomials  
Bound with  
Examples

References

**Theorem:** Let  $R$  be a finite Frobenius ring. Then homogeneous weights exist on  $R$  and are of the form

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

Here  $\chi$  is a generating character of  $R$ , which means

$$\hat{R} = R\chi = \chi R.$$

**Note:** There is also a characterisation of homogeneous weights on finite rings that makes use of the Möbius function on the poset of principal left ideals.



# Homogeneous weights on Frobenius rings

## Examples

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- If  $R$  is a chain ring with  $q$ -element residue field then homogeneous weights have the form

$$R \longrightarrow \mathbb{Q}, \quad r \mapsto \gamma \begin{cases} q-1 & : r \notin \text{soc}(R), \\ q & : 0 \neq r \in \text{soc}(R), \\ 0 & : r = 0. \end{cases}$$

- Homogeneous weights on  $M_2(\mathbb{Z}_2)$  are given by

$$M_2(\mathbb{Z}_2) \longrightarrow \mathbb{Q}, \quad A \mapsto \gamma \begin{cases} 1 & : \text{rk}(A) = 2, \\ 2 & : \text{rk}(A) = 1, \\ 0 & : A = 0. \end{cases}$$



# Bounds on the cardinality of codes

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Definition:** Let  $R$  be a finite Frobenius ring that is equipped with a homogeneous weight of average value  $\gamma$ . For given  $d$  and  $n$  we define

$$A(n, d) := \max\{M \mid \text{there exists an } (n, M, d) \text{-code over } R\}$$

**Remark:**

- A natural goal of coding is to maximise  $A(n, d)$  given  $n$  and  $d$ .
- There are a number of upper bounds on  $A_q(n, d)$ .
- A well-known lower bound is the Gilbert-Varshamov bound.



# Existence bounds

## Sphere-Packing and Gilbert-Varshamov Bound

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Theorem:** (Sphere-Packing Bound) Assume the  $\Delta$ -inequality is valid for  $w$ . For every  $n, d$  and  $t < d/2$  there holds

$$A(n, d) \leq \frac{|R|^n}{V(n, t)}.$$

**Theorem:** (Gilbert-Varshamov Bound) For every  $n, d$  and  $t < d$  there holds

$$A(n, d) \geq \frac{|R|^n}{V(n, t)}.$$

In both cases,  $V(n, t)$  denotes the volume of the disk of radius  $t$  around 0 in  $R^n$ .



# Existence bounds

A Plotkin bound and and Elias bound

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Theorem:** (G. and O'Sullivan 2004) For every  $n, d$  with  $\gamma n < d$  there holds

$$A(n, d) \leq \frac{d}{d - \gamma n}.$$

**Theorem:** (G. and O'Sullivan 2004) For every  $n, d, t$  with  $0 \leq t \leq \gamma n$  and  $t^2 - 2t\gamma n + d\gamma n > 0$  there holds

$$A(n, d) \leq \frac{\gamma n d}{t^2 - 2t\gamma n + d\gamma n} \cdot \frac{|R|^n}{V(n, t)}.$$

**Note:** Both theorems can also be combined to derive an asymptotic version of the Elias bound.



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound**
  - **Duality and Symmetrisation**
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# Code duality

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Definition:** Let  $R$  be a finite Frobenius ring, and let  $C \leq_R R^n$  be a linear code. The dual of  $C$  is defined as

$$C^\perp := \left\{ x \in R^n \mid \sum_{i=1}^n c_i x_i = 0 \text{ for all } c \in C \right\} \leq R_R^n.$$

**Wood 1995:** If  $C$  is an  $R$ -linear code of length  $n$ , then for the Hamming weight enumerators of  $C$  and  $C^\perp$  there holds:

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (|R| - 1)y, x - y).$$

**Remark:** This result is obtained from a result regarding complete weight enumerators by symmetrisation.



# Symmetrisation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

## Note:

- For a while we thought that symmetrised versions of this theorem depend on the symmetrising partition being compatible with the Fourier transform.
- One example of such a partition is namely the one induced by the Hamming weight, i.e. the partition  $\{\{0\}, R \setminus \{0\}\}$ .
- Another example is induced by any central subgroup  $U$  of  $R^\times$  giving rise to the partition  $\{rU \mid r \in R\}$ .
- Results of this type and related work can be found in papers by Wood, Honold and Landjev, and Zinoviev et al.



# Symmetrised MacWilliams Transform

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- Let  $E(R)$  denote the set of all partitions on the finite Frobenius ring  $R$ .
- Given such a partition  $\theta \in E(R)$ , we write  $r\theta$  for the equivalence class containing the element  $r \in R$ .

- We consider  $\Phi : E(R) \longrightarrow E(R)$ ,  $\theta \mapsto \Phi(\theta)$ , where

$$s\Phi(\theta)s' \text{ iff } \sum_{t \in \theta} \chi(ts) = \sum_{t \in \theta} \chi(ts') \text{ for all } r \in R.$$

- Some partitions, but certainly not all, satisfy  $\Phi(\theta) = \theta$ .



# Symmetrised MacWilliams Transform

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- **Example:** On  $\mathbb{Z}_8$  the weight  $w_{\text{hom}}$  induces the partition  $\theta_{\text{hom}} = \{\{0\}, \{4\}, \{1, 2, 3, 5, 6, 7\}\}$ . Then  $\Phi(\theta_{\text{hom}})$  is given by  $\{\{0\}, \{2, 4, 6\}, \{1, 3, 5, 7\}\}$ .
- In this example we have  $\Phi^2(\theta_{\text{hom}}) = \theta_{\text{hom}}$ , however  $\Phi^2 \neq \text{id}$  in general.
- **Theorem:** If  $R$  is a local Frobenius ring, and  $\theta = \{\{0\}, \text{rad}(R) \setminus \{0\}, R^\times\}$  then  $\Phi(\theta) = \theta_{\text{hom}}$ .



# Symmetrised MacWilliams Transform

Bounds for Codes over Rings

Marcus Greferath

Rings and Weights

Some Basic Bounds

LP Bound

Duality and Symmetrisation

Krawtchouk Polynomials

Bound with Examples

References

**Theorem:** Consider the partitions  $\theta$  and  $\tau = \Phi(\theta)$  on  $R$ . There exists a map  $N$  making the following diagram commutative.

$$\begin{array}{ccc} \mathbb{C}[x_r \mid r \in R] & \xrightarrow{\alpha} & \mathbb{C}[z_i \mid i \in \theta] \\ M \downarrow & & \downarrow N \\ \mathbb{C}[x_r \mid r \in R] & \xrightarrow{\beta} & \mathbb{C}[y_j \mid j \in \tau] \end{array}$$

Here  $M$  is the MacWilliams transform for the complete weight enumerator, and  $\alpha, \beta$  are the natural epimorphisms induced by the partitions  $\theta, \tau$ .



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound**
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials**
  - The LP Bound for Codes over Frobenius Rings
- 4 References and Further Reading



# An implicit definition

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- We will write  $z^\alpha$  for  $\prod_{i \in \theta} z_i^{\alpha_i}$  and  $|\alpha| = n$  to indicate that  $\sum_{i \in \theta} \alpha_i = n$ . Likewise we proceed with  $y^\beta$  etc.

- **Definition:** Given  $N : \mathbb{C}[z_i \mid i \in \theta] \longrightarrow \mathbb{C}[y_j \mid j \in \tau]$  which is homogeneous of degree 1. For  $\alpha$  with  $|\alpha| = n$  set

$$Nz^\alpha =: \sum_{|\beta|=n} P_\beta(\alpha) y^\beta,$$

where  $P_\beta(\alpha)$  will be called generalised Krawtchouk polynomials.



# Structure of the Presentation

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- 1 Finite Rings and Weight Functions
- 2 Sphere-Packing, Gilbert-Varshamov, Plotkin, and Elias Bounds
- 3 The Linear Programming Bound**
  - Duality and Symmetrisation
  - Generalised Krawtchouk polynomials
  - The LP Bound for Codes over Frobenius Rings**
- 4 References and Further Reading



# The Linear Programming Bound

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- **Definition:** Let  $R$  be a finite Frobenius ring, and let  $w$  be a weight function on  $R$ .
- For (non-negative) numbers  $d$  and  $n$  we define
$$A(n, d) := \max\{M \mid \text{there is an } (n, M, d) \text{-code over } R\}.$$
- **Goal:** We are interested to maximise  $A(n, d)$  given  $n$  and  $d$ .
- **Note:** Here  $d$  is the minimum weight with respect to  $w$  which is not necessarily a homogeneous weight.



# The Linear Programming Bound

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

**Theorem:** There holds

$$A(n, d) \leq \max_{|\alpha|=n} \left\{ \sum c_\alpha \right\}$$

where the maximum is taken over all  $c_\alpha$  satisfying

$$c_\alpha \geq 0,$$

$$c_\alpha = \begin{cases} 1 & : \alpha = n\delta_0 \\ 0 & : \sum_{i \in \theta_w} \alpha_i w(i) < d \end{cases}$$

$$\text{and } \sum_{|\alpha|=n} c_\alpha P_\beta(\alpha) \geq 0 \text{ for all } |\beta| = n.$$



# Several Examples I

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- The extended  $\mathbb{Z}_8$ -linear Hensel lift of the binary Hamming code is generated by the matrix

$$\begin{bmatrix} 1 & 6 & 5 & 7 & 0 & 0 & 0 & 5 \\ 0 & 1 & 6 & 5 & 7 & 0 & 0 & 5 \\ 0 & 0 & 1 & 6 & 5 & 7 & 0 & 5 \\ 0 & 0 & 0 & 1 & 6 & 5 & 7 & 5 \end{bmatrix}.$$

- This code is of homogeneous minimum distance 5, and we were wondering if an  $[8, 4, 6]$  code might exist.
- We enter the linear programming bound with partitions

$$\theta = \{\{0\}, \{4\}, \{1, 2, 3, 5, 6, 7\}\} \text{ and}$$

$$\tau = \{\{0\}, \{2, 4, 6\}, \{1, 3, 5, 7\}\}.$$



# Several Examples II

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- The underlying Krawchouk polynomials result from the  $\mathbb{C}$ -algebra homomorphism  $N$  which is represented by the  $3 \times 3$ -matrix

$$N = \begin{bmatrix} 1 & 4 & 3 \\ 1 & 0 & -1 \\ 1 & -4 & 3 \end{bmatrix}$$

- An evaluation of the linear programming bound numerically yields the bound

$$A_{\mathbb{Z}_8}(8, 6) \leq 2239 < 4096 = 8^4.$$

- **Remark:** A symmetrisation with respect to  $\mathbb{Z}_8^\times$  is computationally less efficient, but yields the same result.



# Several Examples III

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References

- What is  $A_{\mathbb{Z}_8}(8, 16)$  when the Lee weight is involved?  
Our implementation yields

$$A_{\mathbb{Z}_8}(8, 16) \leq 32.$$

- Indeed, an optimal code reaching this bound is generated by the matrix

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}.$$

- **Remark:** Working with coarser partitions is computationally more efficient.  $(\mathbb{Z}_8, w_{\text{Lee}})$  is of higher complexity than  $(\mathbb{Z}_8, w_{\text{hom}})$ .



# References I

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References



A. R. Hammons, P. V. Kumar, P. Vijay, A. R. Calderbank,  
N. J. A. Sloane, and P. Solé.

The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and  
related codes.

*IEEE Trans. Inform. Theory* **40** (1994): 301–319.



I. Constantinescu and W. Heise.

A metric for codes over residue class rings of integers.

*Problemy Peredachi Informatsii* **33** (1997): 22–28.



J. A. Wood.

Duality for modules over finite rings and applications to  
coding theory.

*Amer. J. Math.* **121** (1999): 555–575.



# References II

Bounds for  
Codes over  
Rings

Marcus  
Greferath

Rings and  
Weights

Some Basic  
Bounds

LP Bound

Duality and  
Symmetrisation

Krawtchouk  
Polynomials

Bound with  
Examples

References



M. Greferath and M. E. O'Sullivan.

On bounds for codes over Frobenius rings under homogeneous weights.

*J Discrete Math.* **289** (2004): 11–24.



M. Greferath, A. Nechaev, and R. Wisbauer.

Finite quasi-Frobenius modules and linear codes.

*J. Algebra Appl.* **3** (2004): 247–272.



E. Byrne, M. Greferath, and M. O'Sullivan.

The Linear Programming Bound for Codes over Finite Frobenius Rings.

*Designs, Codes, Cryptography* (to appear).