

# Refined Upper Bounds for Ring-Linear Codes

Eimear Byrne<sup>1</sup>, Marcus Greferath<sup>1</sup>, Axel Kohnert<sup>2</sup>,  
Vitaly Skachek<sup>1</sup>

<sup>1</sup>Claude Shannon Institute and  
School of Mathematical Sciences  
University College Dublin  
Ireland

<sup>2</sup>Dept Mathematics  
University of Bayreuth  
Germany

June 18 2009

# Outline

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

- Codes over finite fields
- Code optimality
- Bounds for codes for the Hamming weight
- Ring-linear coding
- The homogeneous weight
- Bounds on the size of a code for the homogeneous weight

# Notation

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

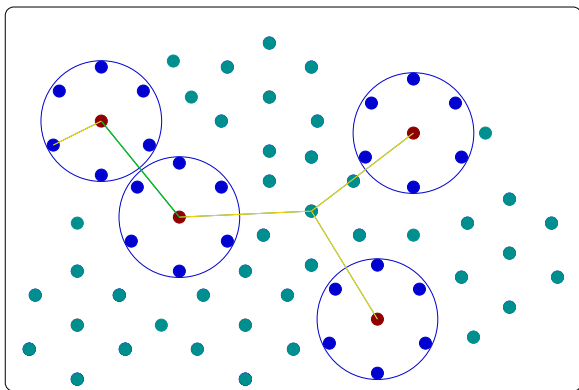
- $F = GF(q)$ ,  $q = p^m$  some prime  $p$
- $R$  is a finite ring with identity
- $\hat{R} := \text{Hom}_{\mathbf{Z}}(R, \mathbb{C}^{\times})$  the characters on  $(R, +)$
- $\chi \in \hat{R}$  is a character on  $(R, +)$
- $C$  is a code of length  $n$  and minimum distance  $d$

# Sphere Packing

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

A good code is one with a large number of codewords for a given minimum distance and length.

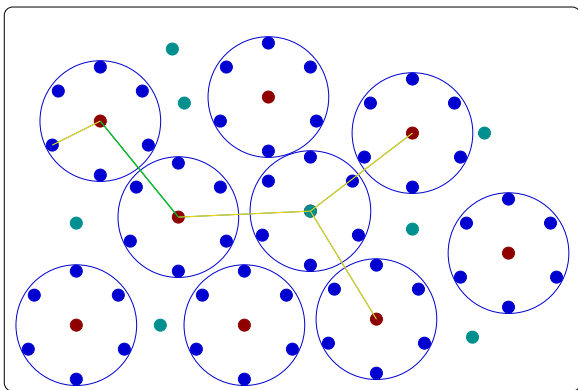


# Sphere Packing

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

A good code is one with a large number of codewords for a given minimum distance and length.



# Code Optimality

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## The Main Coding Problem:

- 1 For fixed length  $n$  and minimum distance  $d$ , what is the maximum size of any code over  $R$ ?  
i.e., what is  $A_R(n, d)$ ?
- 2 For a fixed length  $n$  and minimum distance  $d$ , what is the maximum size of any linear code over  $R$ ?  
i.e., what is  $B_R(n, d)$ ?

# Some Distance Functions

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition (Hamming Metric)

Let  $\mathbf{u}, \mathbf{v} \in R^n$ . The Hamming distance between  $\mathbf{u}$  and  $\mathbf{v}$  is the number of components where  $\mathbf{u}$  and  $\mathbf{v}$  differ, i.e.

$$d_{\text{Ham}}(\mathbf{u}, \mathbf{v}) = |\{i : u_i \neq v_i\}|$$

$$\mathbf{u} = [0, 0, 1, 1, 3, 3], \mathbf{v} = [1, 2, 2, 1, 1, 3] \in \mathbf{Z}_4$$

$$d_{\text{Ham}}(\mathbf{u}, \mathbf{v}) = 4.$$

# Some Distance Functions

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition (Lee Metric)

Let  $u, v \in \mathbf{Z}_m$ . The Lee distance between  $u$  and  $v$  is the absolute value modulo  $m$  of  $u - v$ , i.e.

$$d_{\text{Lee}}(u, v) = |u - v|_m = \begin{cases} u - v & \text{if } u - v \in \{0, \dots, \lfloor m/2 \rfloor\} \\ v - u & \text{otherwise} \end{cases}$$

If  $\mathbf{u}, \mathbf{v} \in \mathbf{Z}_m^n$  then  $d_{\text{Lee}}(\mathbf{u}, \mathbf{v}) = \sum_{i=1..n} |u_i - v_i|_m$ .

$$\mathbf{u} = [0, 0, 1, 1, 3, 3], \mathbf{v} = [1, 2, 2, 1, 1, 3] \in \mathbf{Z}_4$$

$$d_{\text{Lee}}(\mathbf{u}, \mathbf{v}) = 1 + 2 + 1 + 2 = 6$$



# Some Bounds for Codes over Finite Fields

Refined Upper  
Bounds for  
Ring-Linear  
Codes

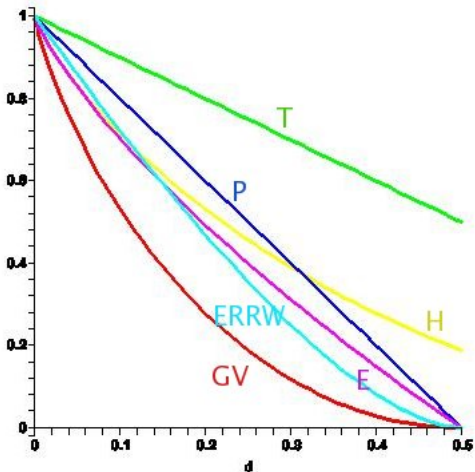
Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

- Singleton:  $|C| \leq A_q(n, d) \leq q^{n-d+1}$
- Hamming:  $|C| \leq A_q(n, d) \leq \frac{q^n}{V_q(n, \lfloor \frac{d-1}{2} \rfloor)}$ ,
- Plotkin:  $|C| \leq A_q(n, d) \leq \frac{d}{d-\gamma n}$ ,  $\gamma = \frac{q-1}{q}$ , if  $n < \frac{d}{\gamma}$
- Gilbert-Varshamov:  $A_q(n, d) \geq \frac{q^n}{V_q(n, d-1)}$
- Elias-Bassalygo bound
- Mc-Eliece-Rodemich-Rumsey-Welch bound
- Linear Programming bound

# Asymptotic Representations

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek



# Codes over Finite Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

An code of length  $n$  over  $R$  is a nonempty subset of  $R^n$ . A (left) linear code of length  $n$  over  $R$  is a left  $R$ -submodule of  $R^n$ .

# Codes over Finite Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

An code of length  $n$  over  $R$  is a nonempty subset of  $R^n$ . A (left) linear code of length  $n$  over  $R$  is a left  $R$ -submodule of  $R^n$ .

We will usually assume that  $R$  is a finite Frobenius ring.

# Codes over Finite Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

An code of length  $n$  over  $R$  is a nonempty subset of  $R^n$ . A (left) linear code of length  $n$  over  $R$  is a left  $R$ -submodule of  $R^n$ .

We will usually assume that  $R$  is a finite Frobenius ring.

Many of the foundational results of classical coding theory (e.g. the MacWilliams' theorems) can be extended to the finite ring case when  $R$  is Frobenius.

[Wood, Honold, Nechaev, Greferath, Schmidt..]

# Finite Frobenius Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

For a finite ring  $R$ ,  $\hat{R}$  is an  $R - R$  bimodule via

$$\chi^r(x) = \chi(rx), \quad {}^r\chi(x) = \chi(xr)$$

for all  $x, r \in R, \chi \in \hat{R}$ .

# Finite Frobenius Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

For a finite ring  $R$ ,  $\hat{R}$  is an  $R - R$  bimodule via

$$\chi^r(x) = \chi(rx), \quad {}^r\chi(x) = \chi(xr)$$

for all  $x, r \in R, \chi \in \hat{R}$ .

$R$  is a finite Frobenius ring iff

$$\begin{aligned} \text{soc } {}_R R \text{ is left principal, iff} \\ {}_R(R/\text{rad } R) \simeq \text{soc } {}_R R, \text{ iff} \\ {}_R R \simeq {}_R \hat{R} \end{aligned}$$

# Finite Frobenius Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

For a finite ring  $R$ ,  $\hat{R}$  is an  $R - R$  bimodule via

$$\chi^r(x) = \chi(rx), \quad {}^r\chi(x) = \chi(xr)$$

for all  $x, r \in R, \chi \in \hat{R}$ .

$R$  is a finite Frobenius ring iff

$$\begin{aligned} \text{soc } {}_R R \text{ is left principal, iff} \\ {}_R(R/\text{rad } R) \simeq \text{soc } {}_R R, \text{ iff} \\ {}_R R \simeq {}_R \hat{R} \end{aligned}$$

Then  ${}_R \hat{R} = {}_R \langle \chi \rangle$  for some (left) generating character  $\chi$ .



# Finite Frobenius Rings

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

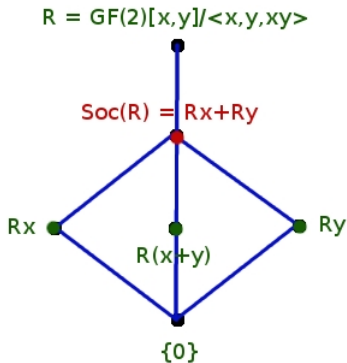
Let  $R$  and  $S$  be finite Frobenius rings, let  $G$  be a finite group.  
The following are examples of Frobenius rings.

- integer residue rings  $\mathbf{Z}_m$
- Galois rings
- principal ideal rings
- $R \times S$
- the matrix ring  $M_n(R)$
- the group ring  $R[G]$

# Not a Frobenius Ring

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek



$R = \mathbb{F}_2[x,y]/\langle x,y,xy \rangle$  is not Frobenius since  $R/\text{Rad } R = R$ ,  
but  $\text{Soc } R = Rx + Ry$ .

# Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

A weight  $w : R \rightarrow \mathbf{Q}$  is *(left) homogeneous*, if  $w(0) = 0$  and

- 1 If  $Rx = Ry$  then  $w(x) = w(y)$  for all  $x, y \in R$ .
- 2 There exists a real number  $\gamma$  such that

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

# Examples of Homogeneous Weights

## Example

On every finite field  $\mathbb{F}_q$  the Hamming weight is a homogeneous weight of average value  $\gamma = \frac{q-1}{q}$ .

# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

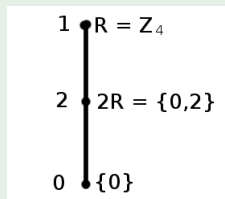
## Example

On every finite field  $\mathbb{F}_q$  the Hamming weight is a homogeneous weight of average value  $\gamma = \frac{q-1}{q}$ .

## Example

On  $\mathbf{Z}_4$  the Lee weight is homogeneous with  $\gamma = 1$ .

$x$	0	1	2	3
$w_{\text{Lee}}(x)$	0	1	2	1



# Examples of Homogeneous Weights

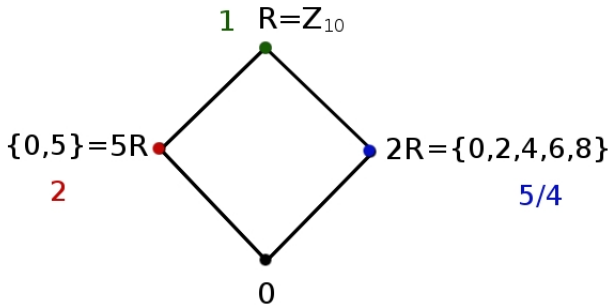
Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On  $\mathbf{Z}_{10}$  the following weight is homogeneous with  $\gamma = 1$ :

$x$	0	1	2	3	4	5	6	7	8	9
$w_{\text{hom}}(x)$	0	1	$\frac{5}{4}$	1	$\frac{5}{4}$	2	$\frac{5}{4}$	1	$\frac{5}{4}$	1



# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On the ring  $R$  of  $2 \times 2$  matrices over  $\text{GF}(2)$  the weight

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

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

# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On the ring  $R$  of  $2 \times 2$  matrices over  $\text{GF}(2)$  the weight

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

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

$R$  has 3 principal ideals - each of size - 4 and six units. We have

$$0 + \underbrace{9 \frac{4}{3} \gamma}_{\text{sing.}} + \underbrace{6 \frac{2}{3} \gamma}_{\text{units}} = 16\gamma.$$



# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On a local Frobenius ring  $R$  with  $q$ -element residue field the weight

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

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

# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On a local Frobenius ring  $R$  with  $q$ -element residue field the weight

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

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

Which finite rings admit a homogeneous weight?

# Examples of Homogeneous Weights

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

On a local Frobenius ring  $R$  with  $q$ -element residue field the weight

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

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

Which finite rings admit a homogeneous weight?

Up to the choice of  $\gamma$ , every finite ring admits a unique homogeneous weight .

# Homogeneous Weights of FFRs

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Theorem (Honold)

*Let  $R$  be a finite Frobenius ring with generating character  $\chi$ .  
Then the homogeneous weights on  $R$  are precisely the functions*

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

*where  $\gamma$  is a real number.*

# Bounds on $A_R(n, d)$ for the Homogeneous Weight

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

The following bounds have been found for codes over FFRs for the homogeneous weight.

- Sphere-packing (Hamming)
- Sphere-covering (Gilbert-Varshamov)
- Plotkin-like bounds
- Elias-like bounds
- Singleton-like bound
- Linear programming bound

# A Key Lemma

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

Let  $x \in R^n$ ,  $C \leq_R R^n$ . We define  $\pi_C(x) := (x_i)_{i \notin \text{supp} C}$ .

## Lemma

Let  $C \leq_R R^n$  be a linear code, and let  $x \in R^n$ . Then

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

# A Key Lemma

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

**Proof:** WLOG, let  $\gamma = 1$ . We compute  $\sum_{c \in C} w(x + c)$

$$= \sum_{c \in C} \sum_{i \in \text{supp} C} w(x_i + c_i) + \sum_{c \in C} \sum_{i \notin \text{supp} C} w(x_i)$$

$$= \sum_{i \in \text{supp} C} \sum_{c \in C} w(x_i + c_i) + |C|w(\pi_C(x))$$

$$= \sum_{i \in \text{supp} C} \sum_{c \in C} \left[ 1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(u(x_i + c_i)) \right] + |C|w(\pi_C(x))$$

$$= |\text{supp} C| \left[ |C| - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(ux_i) \sum_{c \in C} \chi(uc_i) \right] + |C|w(\pi_C(x))$$

$$= |C| [|\text{supp} C| + w(\pi_C(x))].$$

# Residual Codes

## Definition

Let  $C \leq_R R^n$ ,  $c \in R^n$ .  $\text{Res}(C, c) := \{(x_i) : x \in C, c_i = 0\}$ .



# Residual Codes

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Definition

Let  $C \leq_R R^n$ ,  $c \in R^n$ .  $\text{Res}(C, c) := \{(x_i) : x \in C, c_i = 0\}$ .

## Example

Let  $C$  be the  $\mathbb{Z}_4$ -linear code generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{bmatrix}.$$

Let  $c = [0, 0, 0, 2, 0, 2, 2, 2]$ . Then  $\text{Res}(C, c)$  is generated by

$$\begin{bmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

# Residual Codes - the Main Theorem

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Theorem (BGKS)

Let  $C \leq_R R^n$  have minimum homogeneous weight  $d$ , and let  $c \in C$  satisfy  $\ell(c) := w_{\text{Ham}}(c) < \frac{d}{\gamma}$ . Then  $\text{Res}(C, c)$  has

- length  $n - \ell(c)$ ,
- minimum homogeneous weight  $d' \geq d - \gamma \ell(c)$ ,
- $\text{Res}(C, c) \cong C/Rc$  : in particular  $|\text{Res}(C, c)| = \frac{|C|}{|Rc|}$ ,
- $|C| \leq |Rc| \frac{d - \gamma \ell(c)}{d - \gamma n}$ .

# Bounds on $B_R(n, d)$ for the Homogeneous Weight

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Corollary (BGKS)

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

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

# Bounds on $B_R(n, d)$ for the Homogeneous Weight

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Corollary (BGKS)

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

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

# A Plotkin Optimal Code

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R = \mathbb{F}_2^{2 \times 2}$ . Let  $C$  be the length  $16^m - 1$  Simplex Code over  $R$ . Then  $|C| = |R|^m = 16^m$ ,

$$d = |R|^m \gamma = 16^m \gamma,$$

$$\ell := d_{\text{Ham}}(C) = 16^m - \frac{16^m}{4} = \frac{3}{4}16^m.$$

# A Plotkin Optimal Code

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R = \mathbb{F}_2^{2 \times 2}$ . Let  $C$  be the length  $16^m - 1$  Simplex Code over  $R$ . Then  $|C| = |R|^m = 16^m$ ,

$$d = |R|^m \gamma = 16^m \gamma,$$

$$\ell := d_{\text{Ham}}(C) = 16^m - \frac{16^m}{4} = \frac{3}{4}16^m.$$

$R$  has 3 minimal ideals, each of size  $Q = 4$  and so

$$\begin{aligned} |C| &\leq Q \frac{d - \gamma \ell}{d - \gamma n} \\ &= 4 \frac{16^m \gamma - \frac{3}{4}16^m \gamma}{16^m \gamma - (16^m - 1)\gamma} = 4 \frac{16^m}{4} = 16^m. \end{aligned}$$

# Bounds on $B_R(n, d)$ for the Homogeneous Weight

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

Singleton-like bounds:

## Theorem (BGKS)

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

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

# Bounds on $B_R(n, d)$ for the Homogeneous Weight

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

Singleton-like bounds:

## Theorem (BGKS)

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

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

## Theorem (BGKS)

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

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



# Singleton-Like Bounds

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

These bounds arise by repeated applications of the main theorem, to obtain a sequence of  $[n_i, d_i]$  codes

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

with minimum Hamming distance  $\ell_i$ .

# Singleton-Like Bounds

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

These bounds arise by repeated applications of the main theorem, to obtain a sequence of  $[n_i, d_i]$  codes

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

with minimum Hamming distance  $\ell_i$ . Then

$$\begin{aligned} |C| &= |Rc^0| |Rc^1| \cdots |Rc^{r-1}| |C_r| \\ &\leq P^{r-1} |C_r| \leq P^{r-1} |R| \end{aligned}$$

where  $P = \max\{|Ra| : a \in R^n, Ra \leq C, \ell(a) < n\}$ ,

# Singleton-Like Bounds

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

These bounds arise by repeated applications of the main theorem, to obtain a sequence of  $[n_i, d_i]$  codes

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

with minimum Hamming distance  $\ell_i$ . Then

$$\begin{aligned} |C| &= |Rc^0| |Rc^1| \cdots |Rc^{r-1}| |C_r| \\ &\leq P^{r-1} |C_r| \leq P^{r-1} |R| \end{aligned}$$

where  $P = \max\{|Ra| : a \in R^n, Ra \leq C, \ell(a) < n\}$ , so

$$n \geq \frac{|Rc| - 1}{|Rc|} \frac{d}{\gamma} + r \geq \frac{P - 1}{P} \frac{d}{\gamma} + \log_P(|C| - |R|).$$

# A Class of MDS Codes

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R$  be a chain ring of length 2. Then  $R^\times = R \setminus \text{rad } R$  and  $|R| = q^2$ . Let  $U := R^2 \setminus \text{rad } R^2$ , let  $\mathcal{P} := \{xR : x \in U\}$ . Then  $|\mathcal{P}| = q^2 + q$ .

Let  $C <_R R^n$  be the length  $n := q^2 + q$  code with  $2 \times n$  generator matrix whose columns are the distinct elements of  $\mathcal{P}$ .

# A Class of MDS Codes

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R$  be a chain ring of length 2. Then  $R^\times = R \setminus \text{rad } R$  and  $|R| = q^2$ . Let  $U := R^2 \setminus \text{rad } R^2$ , let  $\mathcal{P} := \{xR : x \in U\}$ . Then  $|\mathcal{P}| = q^2 + q$ .

Let  $C <_R R^n$  be the length  $n := q^2 + q$  code with  $2 \times n$  generator matrix whose columns are the distinct elements of  $\mathcal{P}$ . Clearly  $\ell(c) < n$  for each  $c \in C$ .

# A Class of MDS Codes

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R$  be a chain ring of length 2. Then  $R^\times = R \setminus \text{rad } R$  and  $|R| = q^2$ . Let  $U := R^2 \setminus \text{rad } R^2$ , let  $\mathcal{P} := \{xR : x \in U\}$ . Then  $|\mathcal{P}| = q^2 + q$ .

Let  $C <_R R^n$  be the length  $n := q^2 + q$  code with  $2 \times n$  generator matrix whose columns are the distinct elements of  $\mathcal{P}$ . Clearly  $\ell(c) < n$  for each  $c \in C$ .  $C$  is free of rank 2 and the maximal cyclic submodules of  $C$  have size  $P := |R| = q^2$ .

# A Class of MDS Codes

Refined Upper  
Bounds for  
Ring-Linear  
Codes

Eimear Byrne,  
Marcus  
Greferath,  
Axel Kohnert,  
Vitaly  
Skachek

## Example

Let  $R$  be a chain ring of length 2. Then  $R^\times = R \setminus \text{rad } R$  and  $|R| = q^2$ . Let  $U := R^2 \setminus \text{rad } R^2$ , let  $\mathcal{P} := \{xR : x \in U\}$ . Then  $|\mathcal{P}| = q^2 + q$ .

Let  $C <_R R^n$  be the length  $n := q^2 + q$  code with  $2 \times n$  generator matrix whose columns are the distinct elements of  $\mathcal{P}$ . 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  $r = \lceil \log_P |C| - 1 \rceil = \log_{q^2} q^4 - 1 = 1$ .

## Example (cont.)

Setting  $\gamma = 1$ , each nonzero word  $xG$  of  $C$  has weight

$$w(xG) = \begin{cases} q^2 + q & \text{if } x \in U \\ \frac{q^3}{q-1} & \text{if } x \in \text{rad}R^2 \setminus 0 \end{cases} ,$$



## Example (cont.)

Setting  $\gamma = 1$ , each nonzero word  $xG$  of  $C$  has weight

$$w(xG) = \begin{cases} q^2 + q & \text{if } x \in U \\ \frac{q^3}{q-1} & \text{if } x \in \text{rad}R^2 \setminus 0 \end{cases},$$

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

# 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 and W. Heise, *A metric for codes over residue class rings of integers*, Problemy Peredachi Informatsii **33** (1997), no. 3, 22–28.
- M. Greferath and M. E. O'Sullivan, *On Bounds for Codes over Frobenius Rings under Homogeneous Weights*, Discrete Mathematics **289** (2004), 11–24.
- T. Honold, *A characterization of finite Frobenius rings*, Arch. Math. (Basel), **76** (2001), 406–415.
- J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), 555–575.