Upper Bounds for Ring-Linear Codes

Eimear Byrne\(^1\), Marcus Greferath\(^1\), Axel Kohnert\(^2\), Vitaly Skachek\(^1\)

\(^1\)Claude Shannon Institute and School of Mathematical Sciences
University College Dublin
Ireland

\(^2\)Dept Mathematics
University of Bayreuth
Germany

May 19 2009
Outline

- 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

- $F = GF(q)$, $q = p^m$ some prime $p$
- $R$ is a finite ring with identity
- $\hat{R} := \text{Hom}_\mathbb{Z}(R, \mathbb{C}^\times)$ the characters on $(R, +)$
- $\chi \in \hat{R}$ is a character on $(R, +)$
- $C$ is a code of length $n$ and minimum distance $d$
One parameter that indicates the error-correcting capability of a code is its minimum distance.
Using Codes for Error Correction

One parameter that indicates the error-correcting capability of a code is its minimum distance. The higher the minimum distance, the more errors that can be detected and corrected by the receiver.
Using Codes for Error Correction

One parameter that indicates the error-correcting capability of a code is its minimum distance. The higher the minimum distance, the more errors that can be detected and corrected by the receiver.
One parameter that indicates the error-correcting capability of a code is its minimum distance. The higher the minimum distance, the more errors that can be detected and corrected by the receiver.
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

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.

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

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

\[
d_{\text{Ham}}(\mathbf{u}, \mathbf{v}) = 4.
\]
Some Distance Functions

**Definition (Lee Metric)**

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

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

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

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

$$d_{\text{Lee}}(u, v) = 1 + 2 + 1 + 2 = 6$$
Some Bounds for Codes over Finite Fields

- 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: $|C| \leq A_q(n, d) \leq \frac{d}{d-\gamma n}, \gamma = \frac{q-1}{q}, \text{ if } n < \frac{d}{\gamma}$
- 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
Codes over Finite Rings

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

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

$$RR \cong R\hat{R}$$

Then $R\hat{R} = R\langle \chi \rangle$ for some (left) generating character $\chi$.
Let $R$ and $S$ be finite Frobenius rings, let $G$ be a finite group. The following are examples of Frobenius rings.

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

Definition

A weight \( w : R \rightarrow \mathbb{Q} \) 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 $\gamma = \frac{q-1}{q}$.

Example

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

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_{\text{Lee}}(x)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

1. $R = \mathbb{Z}_4$
2. $2R = \{0, 2\}$
3. $0 \in \{0\}$
Examples of Homogeneous Weights

Example

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

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>$\frac{5}{4}$</th>
<th>1</th>
<th>$\frac{5}{4}$</th>
<th>2</th>
<th>$\frac{5}{4}$</th>
<th>1</th>
<th>$\frac{5}{4}$</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_{\text{hom}}(x)$</td>
<td>0</td>
<td>1</td>
<td>$\frac{5}{4}$</td>
<td>1</td>
<td>$\frac{5}{4}$</td>
<td>2</td>
<td>$\frac{5}{4}$</td>
<td>1</td>
<td>$\frac{5}{4}$</td>
<td>1</td>
</tr>
</tbody>
</table>
Examples of Homogeneous Weights

Example

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

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

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

Example

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

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

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

**Theorem (Honold)**

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

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

where $\gamma$ is a real number.
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
Lemma

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

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

**Definition**

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

**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

Theorem

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

- length $n - \ell(c)$,
- minimum homogeneous weight $d' \geq d - \gamma \ell(c)$,
- $|\text{Res}(C, c)| = \frac{|C|}{|Rc|}$ and
- $|C| \leq |Rc| \frac{d - \gamma \ell(c)}{d - \gamma n}$. 
**Corollary (BGKS)**

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

$$|C| \leq |R| \frac{d - \gamma \ell}{d - \gamma n}.$$
Corollary (BGKS)

Let $C \leq \mathbb{R}^R$ be a linear code of minimum homogeneous weight $d$ and minimum Hamming weight $\ell$ 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

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

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

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

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

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

$$= 4 \frac{16^m \gamma - \frac{3}{4} 16^m \gamma}{16^m \gamma - (16^m - 1) \gamma} = 4 \frac{16^m}{4} = 16^m.$$
Bounds on $B_R(n, d)$ for the Homogeneous Weight

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

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

**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

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

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

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

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

$$= q^2 + q - q^2 - q + 1 = 1 = r.$$
References


