Codes and Sequences Over Finite Rings

Eimear Byrne

Claude Shannon Institute and
School of Mathematical Sciences
University College Dublin
Ireland

ALCOMA10
Outline

- Background
- Rings and Weights
- Sequences and Codes
- Examples
A Binary Code

Let \((n, s) = 1\) and let \(d = 2^s + 1\). Consider the binary code:

\[
C = \{ c_{\alpha, \beta}(x) = \text{Tr}(\alpha x) + \text{Tr}(\beta x^d), \alpha, \beta \in GF(2^n) \}.
\]
Let \((n, s) = 1\) and let \(d = 2^s + 1\). Consider the binary code:

\[
C = \{c_{\alpha, \beta}(x) = \text{Tr}(\alpha x) + \text{Tr}(\beta x^d), \alpha, \beta \in GF(2^n)\}.
\]

\(C\) has generator matrix

\[
\begin{bmatrix}
  x_1 & x_2 & \cdots & x_{2^n-1} \\
  x_1^d & x_2^d & \cdots & x_{2^n-1}^d
\end{bmatrix},
\]
A Binary Code

Let \((n, s) = 1\) and let \(d = 2^s + 1\). Consider the binary code:

\[
C = \{ c_{\alpha,\beta}(x) = \text{Tr}(\alpha x) + \text{Tr}(\beta x^d), \alpha, \beta \in GF(2^n) \}.
\]

C has generator matrix

\[
\begin{bmatrix}
    x_1 & x_2 & \cdots & x_{2^{n-1}} \\
    x_1^d & x_2^d & \cdots & x_{2^{n-1}}^d
\end{bmatrix},
\]

and

\[
\omega_H(c_{\alpha,\beta}) = \left(2^n - \sum_{x \in GF(2^n)} (-1)^{\text{Tr}(\alpha x) + \text{Tr}(\beta x^d)} \right)/2.
\]
A Binary Code

Let \((n, s) = 1\) and let \(d = 2^s + 1\). Consider the binary code:

\[ C = \{ c_{\alpha,\beta}(x) = \text{Tr}(\alpha x) + \text{Tr}(\beta x^d), \alpha, \beta \in GF(2^n) \}. \]

\(C\) has generator matrix

\[
\begin{bmatrix}
  x_1 & x_2 & \cdots & x_{2^n-1} \\
  x_1^d & x_2^d & \cdots & x_{2^n-1}^d \\
\end{bmatrix},
\]

and

\[
\omega_H(c_{\alpha,\beta}) = \left( 2^n - \sum_{x \in GF(2^n)} (-1)^{\text{Tr}(\alpha x) + \text{Tr}(\beta x^d)} \right) / 2.
\]

\(C\) has length \(2^n - 1\). For odd \(n\) it has dimension \(2n\) and 3 non-zero weights:

\[ \{ 2^{n-1} - 2^{n-1}/2, 2^{n-1}, 2^{n-1} + 2^{n-1}/2 \}. \]
Finite Frobenius Rings

For a finite ring $R$, $\hat{R} := \text{Hom}_\mathbb{Z}(R, \mathbb{C}^\times)$, is an $R-R$ bimodule:

\[ r \chi(x) = \chi(rx), \quad \chi^r(x) = \chi(xr) \]

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

For a finite ring $R$, $\hat{R} := \text{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$, is an $R$-$R$ bimodule:

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

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

The following are equivalent definitions:

- $R$ is a Frobenius ring
- $soc_R R$ is left principal,
- $R(R/\text{rad } R) \simeq soc_R R$,
- $RR \simeq_R \hat{R}$
For a finite ring $R$, $\hat{R} := \text{Hom}_ℤ(R, ℂ^×)$, is an $R$-$R$ bimodule:

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

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

The following are equivalent definitions:

- $R$ is a Frobenius ring
- $soc_R R$ is left principal,
- $R(R/\text{rad } R) \cong soc_R R$,
- $RR \cong R\hat{R}$

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

The following are examples of Frobenius rings.

- integer residue rings $\mathbb{Z}_m$
- any semi-simple ring
- principal ideal rings
- direct products of Frobenius rings
- matrix rings over Frobenius rings
- group rings over Frobenius rings
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

$$\sum_{y \in Rx} w(y) = \gamma |Rx|$$

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

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>$w_{	ext{Lee}}(x)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

1 $\mathbb{R} = \mathbb{Z}_4$

2 $2\mathbb{R} = \{0, 2\}$

0 $\{0\}$
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>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_{\text{hom}}(x)$</td>
<td>0</td>
<td>$\frac{3}{4}$</td>
<td>$\frac{5}{4}$</td>
<td>$\frac{3}{4}$</td>
<td>$\frac{5}{4}$</td>
<td>2</td>
<td>$\frac{5}{4}$</td>
<td>$\frac{3}{4}$</td>
<td>$\frac{5}{4}$</td>
<td>$\frac{3}{4}$</td>
</tr>
</tbody>
</table>

$\{0,5\} = 5R$

$2R = \{0,2,4,6,8\}$
Examples of Homogeneous Weights

Example

On a local Frobenius ring \( R \) with \( q \)-element residue field the weight

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

is a homogeneous weight of average value \( \gamma = 1 \).
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.
Let $R > S$ be Frobenius rings.

**Definition**

Let $T$ be an $S$-module epimorphism $T : \mathcal{S}R \rightarrow \mathcal{S}S$ whose kernel contains no non-trivial left ideal of $R$. We say that $T$ is a trace map from $R$ onto $S$. 
Let $R > S$ be Frobenius rings.

**Definition**

Let $T$ be an $S$-module epimorphism $T : _sR \longrightarrow _sS$ whose kernel contains no non-trivial left ideal of $R$. We say that $T$ is a trace map from $R$ onto $S$.

A generating character $\Phi \in \hat{S}$ determines a generating character $\chi \in \hat{R}$ as:

$$\chi(x) = \Phi(T(x)) \forall x \in R.$$
An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on $M_n(\mathbb{Z}_m)$)

$\Phi(x) = \omega x$, where $\omega$ is a primitive $m$th root of unity in $\mathbb{C}$. $\Phi$ is the usual trace map from $M_n(\mathbb{Z}_m)$ onto $\mathbb{Z}_m$. 

Diagram:

- $M_n(\mathbb{Z}_m)$
- $\mathbb{Z}_m$
- $\mathbb{C}^\times$
- $\chi$
- $T$
- $\phi$
Example (Characters and Traces on $M_n(\mathbb{Z}_m)$)

- $\Phi(x) = \omega^x$, $\omega$ a primitive $m$th root of unity in $\mathbb{C}^\times$
Example (Characters and Traces on $M_n(\mathbb{Z}_m)$)

- $\Phi(x) = \omega^x$, $\omega$ a primitive $m$th root of unity in $\mathbb{C}^\times$
- $T$ is the usual trace map from $M_n(\mathbb{Z}_m)$ onto $\mathbb{Z}_m$. 
An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on Galois Rings)

Let $R = GR(p^n, sk), S := GR(p^n, s), B := \mathbb{Z}_{p^n}.$
Example (Characters and Traces on Galois Rings)

Let $R = GR(p^n, sk), S := GR(p^n, s), B := \mathbb{Z}_{p^n}$.

$\Phi(\chi) = \omega^x, \omega$ a primitive $p^n$th root of unity in $\mathbb{C}^\times$
An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on Galois Rings)

Let $R = GR(p^n, sk), S := GR(p^n, s), B := \mathbb{Z}_p^n$.

- $\Phi(x) = \omega^x, \omega$ a primitive $p^n$th root of unity in $\mathbb{C}^\times$
- $\sigma : R \to R : \sum_{i=0}^n p^i a_i \mapsto \sum_{i=0}^n p^i a_i^p \in Aut(R)$
Example (Characters and Traces on Galois Rings)

Let $R = GR(p^n, sk), S := GR(p^n, s), B := \mathbb{Z}_{p^n}$. 

- $\Phi(x) = \omega^x$, $\omega$ a primitive $p^n$th root of unity in $\mathbb{C}^\times$.
- $\sigma : R \longrightarrow R : \sum_{i=0}^{n} p^i a_i \longmapsto \sum_{i=0}^{n} p^i a_i^p \in Aut(R)$.
- $T_{R/S} : R \longrightarrow S : a \longmapsto a + \sigma^s(a) + \cdots + \sigma^{s(k-1)}(a)$. 
A Subring Subcode

For any map \( f : R \rightarrow R \), we define the left \( S \)-linear subring subcode

\[
C_f = \{ c_{\alpha,\beta}^f : R \rightarrow S : x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R \}.
\]
A Subring Subcode

For any map \( f : R \rightarrow R \), we define the left \( S \)-linear subring subcode

\[
C_f = \{ c_{\alpha,\beta}^f : R \rightarrow S : x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R \}.
\]

We compute the weight of each codeword as:

\[
w(c_{\alpha,\beta}^f) = \sum_{x \in R} w(c_{\alpha,\beta}^f(x))
\]
A Subring Subcode

For any map \( f : R \rightarrow R \), we define the left \( S \)-linear subring subcode

\[
C_f = \{ c^f_{\alpha, \beta} : R \rightarrow S : x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R \}.
\]

We compute the weight of each codeword as:

\[
w(c^f_{\alpha, \beta}) = \sum_{x \in R} w(c^f_{\alpha, \beta}(x)) = |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \Phi^u(T(\alpha x + \beta f(x))).
\]
A Subring Subcode

For any map \( f : R \rightarrow R \), we define the left \( S \)-linear subring subcode

\[
C_f = \{ c_{\alpha,\beta}^f : R \rightarrow S : x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R \}.
\]

We compute the weight of each codeword as:

\[
w(c_{\alpha,\beta}^f) = \sum_{x \in R} w(c_{\alpha,\beta}^f(x))
= |R| - \frac{1}{|S|^2} \sum_{u \in S^2} \sum_{x \in R} \Phi^u(T(\alpha x + \beta f(x)))
= |R| - \frac{1}{|S|^2} \sum_{u \in S^2} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)).
\]
The Spectrum of $f : R \rightarrow R$

**Definition**

Let $R > S$ be Frobenius rings with trace map $T : sR \rightarrow sS$. Let $f : R \rightarrow R$. For each $\alpha, \beta \in R$, define

$$W^f(\alpha, \beta) := \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)) = |R| - w(c^f_{\alpha, \beta}).$$

The spectrum of $f$ is the set

$$\Lambda_f := \{W^f(\alpha, \beta) : \alpha, \beta \in R\}.$$
The Spectrum of $f : R \rightarrow R$

**Definition**

Let $R > S$ be Frobenius rings with trace map $T : sR \rightarrow sS$. Let $f : R \rightarrow R$. For each $\alpha, \beta \in R$, define

$$W^f(\alpha, \beta) := \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)) = |R| - w(c^f_{\alpha, \beta}).$$

The spectrum of $f$ is the set

$$\Lambda_f := \{ W^f(\alpha, \beta) : \alpha, \beta \in R \}.$$

- If $|\Lambda_f| = k + 1$ then $C_f$ has exactly $k$ non-zero weights.
The Spectrum of $f : R \rightarrow R$

**Definition**

Let $R > S$ be Frobenius rings with trace map $T : sR \rightarrow sS$. Let $f : R \rightarrow R$. For each $\alpha, \beta \in R$, define

$$W^f(\alpha, \beta) := \frac{1}{|S \times |} \sum_{u \in S \times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)) = |R| - w(c^f_{\alpha, \beta}).$$

The spectrum of $f$ is the set

$$\Lambda_f := \{W^f(\alpha, \beta) : \alpha, \beta \in R\}.$$

- If $|\Lambda_f| = k + 1$ then $C_f$ has exactly $k$ non-zero weights.
- One of the weights of $C_f$ is $|R|$. 
Frank Sequences

Theorem

Let $R = S = GR(p^2, r), p$ prime. Write $a = a_0 + pa_1$ for each $a \in R$. Let

$$f : R \rightarrow R : a \mapsto pa_0a_1.$$  

Then

$$\Lambda_f = \{p^{2r}, p^r, 0\}.$$
Frank Sequences

Theorem

Let $R = S = GR(p^2, r)$, $p$ prime. Write $a = a_0 + pa_1$ for each $a \in R$. Let

$$f : R \rightarrow R : a \mapsto pa_0a_1.$$ 

Then

$$\Lambda_f = \{ p^{2r}, p^r, 0 \}.$$ 

- $C_f$ has length $p^{2r} - 1$, size $p^{3r}$ and weight enumerator

$$1 + p^r(p^r - 1)X^{p^r(p^r - 1)} + (p^r - 1)(p^{2r} + 1)X^{p^{2r}}.$$
**Theorem**

Let $R = S = GR(p^2, r)$, $p$ prime. Write $a = a_0 + pa_1$ for each $a \in R$. Let

$$f : R \longrightarrow R : a \mapsto pa_0a_1.$$ 

Then

$$\Lambda_f = \{p^{2r}, p^r, 0\}.$$ 

- $C_f$ has length $p^{2r} - 1$, size $p^{3r}$ and weight enumerator

$$1 + p^r(p^r - 1)X^{p^r(p^r-1)} + (p^r - 1)(p^{2r} + 1)X^{p^{2r}}.$$

- If we let $S = \mathbb{Z}_{p^n}$, $r > 1$ then

$$\Lambda_f = \{p^{2r}, p^r, -\frac{p^r}{p-1}, 0\}.$$
### Theorem

Let $R = S = \mathbb{Z}_{2p}$, $p$ prime. Let

$$f : R \rightarrow R : a \mapsto a^2.$$  

Then

$$\Lambda_f = \{2p, \frac{2p}{p-1}, 0\}.$$
Theorem

Let $R = S = \mathbb{Z}_{2p}$, $p$ prime. Let

$$f : R \rightarrow R : a \mapsto a^2.$$  

Then

$$\Lambda_f = \{2p, \frac{2p}{p - 1}, 0\}.$$  

$C_f$ has length $2p - 1$, size $2p^2$ and weight enumerator

$$1 + (1 + 4(p - 1) + (p - 1)^2)X^{2p} + (p - 1)^2 X^{2p \frac{p - 2}{p - 1}}.$$
Let $R$ be a finite commutative local ring with unique maximal ideal $M$ and residue field $K = R/M$. 
Local Commutative Rings

- Let $R$ be a finite commutative local ring with unique maximal ideal $M$ and residue field $K = R/M$.
- Then each element $a \in R$ can be expressed as
  \[ a = a_m + a_t \]
  for some unique $a_m \in M$, $a_t \in T$, where $T \setminus \{0\}$ is a cyclic subgroup of order $|K^\times|$ in $R^\times$. 
Let $R$ be a finite commutative local ring with unique maximal ideal $M$ and residue field $K = R/M$.

Then each element $a \in R$ can be expressed as

$$a = a_m + a_t$$

for some unique $a_m \in M$, $a_t \in T$, where $T \setminus \{0\}$ is a cyclic subgroup of order $|K^\times|$ in $R^\times$.

This decomposition can be useful for evaluating the spectrum of a function.
Compatibility of $\chi$ with $\text{Aut}(R)$

Suppose that

$$\chi(\sigma(x)) = \chi(x), \forall x \in R.$$
Compatibility of $\chi$ with $\text{Aut}(R)$

Suppose that

$$\chi(\sigma(x)) = \chi(x), \ \forall \ x \in R.$$  

Then, for example,

$$\chi(x\sigma(y) + \sigma(x)y) = \chi(x(\sigma(y) + \sigma^{-1}(y))).$$
Compatibility of $\chi$ with $\text{Aut}(R)$

Suppose that

$$\chi(\sigma(x)) = \chi(x), \ \forall \ x \in R.$$ 

Then, for example,

$$\chi(x\sigma(y) + \sigma(x)y) = \chi(x(\sigma(y) + \sigma^{-1}(y))).$$

Then

$$\chi(f(a)) = \chi(\sigma(a)a - \sigma(a_m)a_m)$$
$$= \chi(\sigma(a_t)a_t - \sigma(a_m)a_t - \sigma(a_t)a_m)$$
$$= \chi(\sigma(a_t)a_t)\chi((\sigma^{-1}(a_t) - \sigma(a_t))a_m).$$
Let $R$ be a finite local commutative Frobenius ring. Let $\sigma \in \text{Aut}(R)$ satisfy $\chi(\sigma(x)) = \chi(x)$ for all $x \in R$. Define
\[
f : R \longrightarrow R : a \mapsto \sigma(a)a - \sigma(a_m)a_m.\]
Then
\[
\Lambda_f = \{|R|, |M|, \frac{|R||M|}{|R \times|}, 0\}.\]
Theorem

Let $R$ be a finite local commutative Frobenius ring. Let $\sigma \in \text{Aut}(R)$ satisfy $\chi(\sigma(x)) = \chi(x)$ for all $x \in R$. Define

$$f : R \rightarrow R : a \mapsto \sigma(a)a - \sigma(a_m)a_m.$$ 

Then $C_f$ has length $|R| - 1$ and non-zero weights

$$\{ |R|, |R| - |M|, |R|(1 - \frac{|M|}{|R^\times|}) \}.$$
More

- Find more functions on local rings that give codes with small spectra.
- Determine functions that yield 2-weight codes (especially modular or projective regular codes).
- Nonlinearity.
Applications - Strongly Regular Graphs

\[ w_0 = 0 \]

\[ w_1 = 2 \]

\[ w_2 = 4 \]