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:

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

A Binary Code

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

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

C has generator matrix

$$\left[\begin{array}{c|c|c|c} x_1 & x_2 & \cdots & x_{2^n-1} \\ x_1^d & x_2^d & \cdots & x_{2^n-1}^d \end{array} \right],$$

A Binary Code

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

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

C has generator matrix

$$\left[\begin{array}{c|c|c|c} x_1 & x_2 & \cdots & x_{2^n-1} \\ x_1^d & x_2^d & \cdots & x_{2^n-1}^d \end{array} \right],$$

and

$$w_H(c_{\alpha,\beta}) = \left(2^n - \sum_{x \in GF(2^n)} (-1)^{\mathrm{Tr}(\alpha x) + \mathrm{Tr}(\beta x^d)} \right) /2.$$

A Binary Code

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

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

C has generator matrix

$$\left[\begin{array}{c|c|c|c} x_1 & x_2 & \cdots & x_{2^n-1} \\ x_1^d & x_2^d & \cdots & x_{2^n-1}^d \end{array} \right],$$

and

$$w_H(c_{\alpha,\beta}) = \left(2^n - \sum_{x \in GF(2^n)} (-1)^{\mathrm{Tr}(\alpha x)+\mathrm{Tr}(\beta x^d)} \right) /2.$$

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

$$\{2^{n-1} - 2^{\frac{n-1}{2}}, 2^{n-1}, 2^{n-1} + 2^{\frac{n-1}{2}}\}.$$

Finite Frobenius Rings

For a finite ring R, $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$, 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,
- $_R(R/rad\ R) \simeq soc_R R$,
- $_R R \simeq {}_R\hat{R}$

Finite Frobenius Rings

For a finite ring R, $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$, 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,
- $_R(R/rad\ R) \simeq soc_R R$,
- $_R R \simeq {}_R\hat{R}$

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

Finite Frobenius Rings

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 $w : R \longrightarrow \mathbb{Q}$ 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 γ such that

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

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

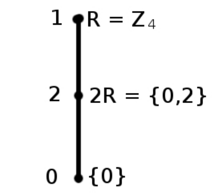
Example

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 $\gamma = 1$.

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

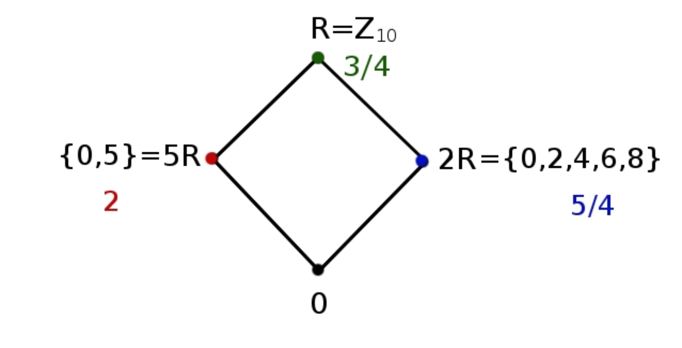


Examples of Homogeneous Weights

Example

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

x	0	1	2	3	4	5	6	7	8	9
$\mathrm{w}_{\mathrm{hom}}(x)$	0	$\frac{3}{4}$	$\frac{5}{4}$	$\frac{3}{4}$	$\frac{5}{4}$	2	$\frac{5}{4}$	$\frac{3}{4}$	$\frac{5}{4}$	$\frac{3}{4}$



Examples of Homogeneous Weights

Example

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

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

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

Homogeneous Weights of FFRs

Theorem (Honold)

Let R be a finite Frobenius ring with generating character χ. 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 γ is a real number.

Characters and Trace Maps

Let $R > S$ be Frobenius rings.

Definition

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

Characters and Trace Maps

Let $R > S$ be Frobenius rings.

Definition

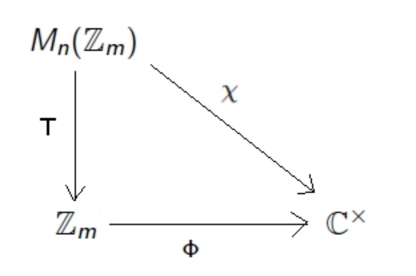
Let T be an S-module epimorphism $T : {}_SR \longrightarrow {}_SS$ whose kernel contains no non-trivial left ideal of R.
We say that T is a trace map from R onto S.

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

$$\chi(x) = \Phi(T(x)) \; \forall \, x \in R.$$

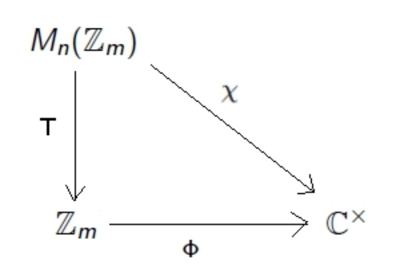
An Example - $M_n(\mathbb{Z}_m)$

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



An Example - $M_n(\mathbb{Z}_m)$

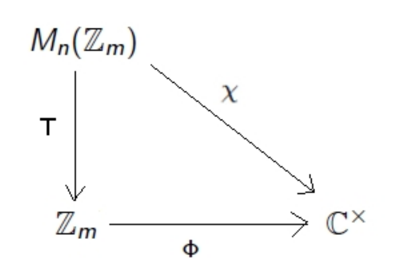
Example (Characters and Traces on $M_n(\mathbb{Z}_m)$)



- $\Phi(x) = \omega^x, \omega$ a primitive mth root of unity in $\mathbb{C}^\times$

An Example - $M_n(\mathbb{Z}_m)$

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

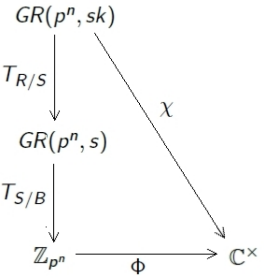


- $\Phi(x) = \omega^x, \omega$ a primitive mth root of unity in $\mathbb{C}^\times$
- T is the usual trace map from $M_n(\mathbb{Z}_m)$ onto $\mathbb{Z}_m$.

An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on Galois Rings)

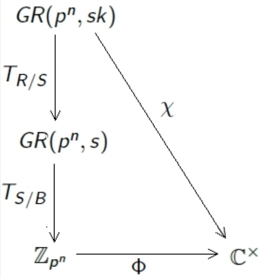
Let $R = GR(p^n, sk), S := GR(p^n, s), B := \mathbb{Z}_{p^n}$.



An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on Galois Rings)

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

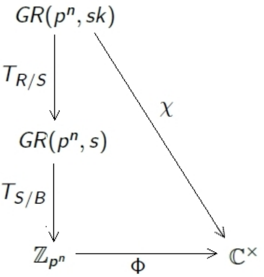


- $\Phi(x) = \omega^x, \omega$ a primitive p^nth root of unity in $\mathbb{C}^\times$

An Example - $M_n(\mathbb{Z}_m)$

Example (Characters and Traces on Galois Rings)

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

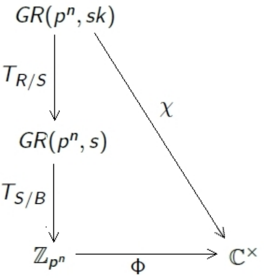


- $\Phi(x) = \omega^x, \omega$ a primitive p^nth root of unity in $\mathbb{C}^\times$
- $\sigma : R \longrightarrow R : \sum_{i=0}^{n} p^i a_i \mapsto \sum_{i=0}^{n} p^i a_i^p \in Aut(R)$

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^nth root of unity in $\mathbb{C}^\times$
- $\sigma : R \longrightarrow R : \sum_{i=0}^n p^i a_i \mapsto \sum_{i=0}^n p^i a_i^p \in Aut(R)$
- $T_{R/S} : R \longrightarrow S : a \mapsto a + \sigma^s(a) + \cdots + \sigma^{s(k-1)}(a)$

A Subring Subcode

For any map $f : R \longrightarrow R$, we define the left S-linear subring subcode

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

A Subring Subcode

For any map $f : R \longrightarrow R$, we define the left S-linear subring subcode

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

We compute the weight of each codeword as:

$$w(c^f_{\alpha,\beta}) = \sum_{x \in R} w(c^f_{\alpha,\beta}(x))$$

A Subring Subcode

For any map $f : R \longrightarrow R$, we define the left S-linear subring subcode

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

We compute the weight of each codeword as:

$$\begin{aligned} w(c^f_{\alpha,\beta}) &= \sum_{x \in R} w(c^f_{\alpha,\beta}(x)) \\ &= |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \Phi^u(T(\alpha x + \beta f(x))) \end{aligned}$$

A Subring Subcode

For any map $f : R \longrightarrow R$, we define the left S-linear subring subcode

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

We compute the weight of each codeword as:

$$\begin{aligned} w(c^f_{\alpha,\beta}) &= \sum_{x \in R} w(c^f_{\alpha,\beta}(x)) \\ &= |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \Phi^u(T(\alpha x + \beta f(x))) \\ &= |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)). \end{aligned}$$

The Spectrum of $f : R \longrightarrow R$

Definition

Let $R > S$ be Frobenius rings with trace map $T : {}_SR \longrightarrow {}_SS$. Let $f : R \longrightarrow R$. 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 $f : R \longrightarrow R$

Definition

Let $R > S$ be Frobenius rings with trace map $T : {}_SR \longrightarrow {}_SS$. Let $f : R \longrightarrow R$. 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 $f : R \longrightarrow R$

Definition

Let $R > S$ be Frobenius rings with trace map $T : {}_SR \longrightarrow {}_SS$. Let $f : R \longrightarrow R$. 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*

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

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

$$f : R \longrightarrow R : a \mapsto pa_0 a_1.$$

Then

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

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

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

Frank Sequences

Theorem

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

$$f : R \longrightarrow R : a \mapsto pa_0 a_1.$$

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

Chu Sequences

Theorem

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

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

Then

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

Chu Sequences

Theorem

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

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

Then

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

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

$$1 + (1 + 4(p-1) + (p-1)^2)X^{2p} + (p-1)^2 X^{2p\frac{p-2}{p-1}}.$$

Local Commutative Rings

- 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 $T\backslash\{0\}$ is a cyclic subgroup of order $|K^\times|$ in $R^\times$.

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 $T \backslash \{0\}$ 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 χ with $Aut(R)$

Suppose that

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

Compatibility of χ with $Aut(R)$

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 χ with $Aut(R)$

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

$$\begin{aligned}
\chi(f(a)) &= \chi(\sigma(a)a - \sigma(a_m)a_m) \\
&= \chi(\sigma(a_t)a_t - \sigma(a_m)a_t - \sigma(a_t)a_m) \\
&= \chi(\sigma(a_t)a_t)\chi((\sigma^{-1}(a_t) - \sigma(a_t))a_m).
\end{aligned}$$

Local Commutative Rings

Theorem

Let R be a finite local commutative Frobenius ring. Let $\sigma \in Aut(R)$ 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

$$\Lambda_f = \{|R|, |M|, \frac{|R||M|}{|R^\times|}, 0\}.$$

Local Commutative Rings

Theorem

Let R be a finite local commutative Frobenius ring. Let $\sigma \in Aut(R)$ 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 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

$$\{000\} \quad w_0 = 0$$

$$\left.\begin{array}{c}130\\013\\103\\310\\031\\301\end{array}\right\} \quad w_1 = 2$$

$$\left.\begin{array}{c}121\\112\\323\\211\\332\\202\\233\\220\\022\end{array}\right\} \quad w_2 = 4$$