

# Linear Codes over Finite Chain Rings—Algebraic Theory

Thomas Honold

Institute of Information and Communication Engineering  
Zhejiang University

CIMPA Summer School  
August 2008

## 1 Linear Code Constructions

## 2 Linearly Representable Codes

# Today's Lecture: #5

To compute the weight enumerator

$$A_C(X_0, \dots, X_m) = \sum_{\mathbf{i}=(i_0, \dots, i_m) \in I} A_{\mathbf{i}} X_0^{i_0} \cdots X_m^{i_m}$$

of  $C$  (where  $I$  consists of all  $m + 1$ -tuples  $\mathbf{i} \in \mathbb{N}_0^{m+1}$  satisfying  $i_0 + \cdots + i_m = n$ ), we establish a correspondence between codewords of  $C$  and hyperplanes of  $\text{PG}(R_R^k)$ .

All hyperplanes of  $\text{PG}(R_R^k)$  (or  $\text{PHG}(R_R^k)$ ) have the form  $H = (R\mathbf{x})^\perp$  for some  $\mathbf{x} \in (R^k)^\times$ .

## Definition

The  $\mathfrak{R}$ -type of  $H$  is the sequence  $(a_0, \dots, a_m)$  where

$$a_i := \sum_{\substack{P \in \mathcal{P} \\ P \subseteq H + \theta^i R^k \\ P \not\subseteq H + \theta^{i+1} R^k}} \mathfrak{R}(P) \quad \text{for } 0 \leq i \leq m.$$

## Remark

If  $\mathfrak{R}$  is a multiset in  $\text{PHG}(R_R^k)$  (i.e.  $\text{supp } \mathfrak{R}$  contains only free points), then  $a_i$  counts the number of points of  $\mathfrak{R}$  which are  $i$ -neighbours but not  $i + 1$ -neighbours to  $H$ .

## Proposition

Let  $\mathfrak{K}$  be a multiset in  $\text{PG}(R_R^k)$  associated with  $C \leq_R R^n$ , and suppose the correspondence  $C \mapsto \mathfrak{K}$  is given by  $\mathbf{G} \in R^{k \times n}$ . For each hyperplane  $H = (R\mathbf{x})^\perp$  of  $\mathfrak{K}$ -type

$$(0, \dots, 0, a_j, \dots, a_m) \quad \text{with } a_j \neq 0$$

the cyclic subcode  $R\mathbf{x}\mathbf{G} \leq_R C$  has weight enumerator

$$X_m^n + \sum_{s=j}^{m-1} (q^{m-s} - q^{m-s-1}) X_s^{a_j} X_{s+1}^{a_{j+1}} \dots X_{m-1}^{a_{j+m-1-s}} X_m^{a_{j+m-s} + \dots + a_m}$$

## Proof.

Let  $\mathbf{G} = (\mathbf{g}_1 | \dots | \mathbf{g}_n)$  and  $\mathbf{c} = \mathbf{x}\mathbf{G} = (\mathbf{x} \cdot \mathbf{g}_1, \dots, \mathbf{x} \cdot \mathbf{g}_n)$ .

## Observation (easy to verify)

$\mathbf{g}_j \in H + \theta^i R^k \setminus (H + \theta^{i+1} R^k)$  is equivalent to  $\mathbf{x} \cdot \mathbf{g}_j \in N^i \setminus N^{i+1}$ .

Hence  $(a_0, \dots, a_m)$  is the weight composition of  $\mathbf{c}$ .

The rest follows from  $R\mathbf{c} \cong N^j$  (as left  $R$ -modules) and the fact that multiplication by  $\theta$  shifts the weight composition as follows:

$$(b_0, \dots, b_{m-1}, b_m) \mapsto (0, b_0, \dots, b_{m-2}, b_{m-1} + b_m).$$

## Remarks

- The weight enumerator of  $C$  can be computed from the weight enumerators of the cyclic subcodes of  ${}_R C$  using the principle of inclusion and exclusion. In the classical case this is trivial, since  $C = \{\mathbf{0}\} \uplus \biguplus_{\mathbf{c} \in S} (\mathbb{F}_q \mathbf{c} \setminus \{\mathbf{0}\})$ .
- Sometimes (especially in the case  $m = 2$ ) it is easier to compute the weight enumerators of  $C^\times$  and  $C \setminus C^\times$  separately.  
If  $a_0 \neq 0$ ,  $H$  gives rise to  $q^m - q^{m-1}$  codewords in  $C^\times$  (the words in  $R^\times \mathbf{xG}$ ). All these have weight composition equal to the  $\mathfrak{R}$ -type of  $H$ .

## Example

We compute the weight enumerator of the linear code  $K$  over  $\mathbb{Z}_4$  generated by

$$\mathbf{K} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}.$$

The code  $K$  is associated with a hyperoval of the projective Hjelmslev plane  $\text{PHG}(\mathbb{Z}_4^3) = \text{PHG}(2, \mathbb{Z}_4)$ .

Since  $2C$  is a simplex code over  $\{0, 2\}$ ,

$$A_{2C}(X_0, X_1, X_2) = X_2^7 + 7X_1^4 X_2^3.$$

type	#lines	
$(4, 1, 2)$	21	<i>secants</i>
$(4, 3, 0)$	7	<i>passants</i>

This gives

$$A_{C \times}(X_0, X_1, X_2) = 42X_0^4 X_1 X_2^2 + 14X_0^4 X_1^3,$$

$$A_C(X_0, X_1, X_2) = X_2^7 + 42X_0^4 X_1 X_2^2 + 7X_1^4 X_2^3 + 14X_0^4 X_1^3.$$

## Example (Weight enumerator of the Octacode)

The Octacode  $O$  is generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

The associated multiset  $\mathfrak{D}$  is an *arc* in  $\text{PHG}(3, \mathbb{Z}_4)$  (i.e. no 4 points of  $\mathfrak{D}$  are on the same hyperplane).

Since  $2O$  is the extended  $[8, 4, 4]$  Hamming code over  $\{0, 2\}$ ,

$$A_{2O}(X_0, X_1, X_2) = X_2^8 + 14X_1^4X_2^4 + X_1^8.$$

Let  $n_i$  be the number of planes of  $\text{PHG}(3, \mathbb{Z}_4)$  meeting  $\mathfrak{D}$  in  $i$  points ( $0 \leq i \leq 3$ ).

$$\begin{aligned} n_0 + n_1 + n_2 + n_3 &= 120 \\ n_1 + 2n_2 + 3n_3 &= 8 \cdot 28 \\ n_2 + 3n_3 &= \binom{8}{2} \cdot 6 \\ n_3 &= \binom{8}{3} \end{aligned}$$

## Example (cont'd)

Solving the system gives  $n_0 = 8$ ,  $n_1 = n_3 = 56$ ,  $n_2 = 0$ .

Since  $O/2O$  is the extended Hamming code, there is 1 neighbourhood class of planes of  $\mathfrak{D}$ -type  $(8, 0, 0)$  (the class containing  $\mathbb{Z}_4(1111)^\perp$ ) and 14 classes of  $\mathfrak{D}$ -type  $(4, *, *)$ .

$\mathfrak{D}$ -type	#planes	
$(8, 0, 0)$	8	$H \cap \mathfrak{D} = \emptyset$
$(4, 1, 3)$	56	$ H \cap \mathfrak{D}  = 3$
$(4, 3, 1)$	56	$ H \cap \mathfrak{D}  = 1$

This gives

$$\begin{aligned}
 A_{O^\times}(X_0, X_1, X_2) &= 16X_0^8 + 112X_0^4X_1X_2^3 + 112X_0^4X_1^3X_2, \\
 A_O(X_0, X_1, X_2) &= X_2^8 + 112X_0^4X_1X_2^3 + 14X_1^4X_2^4 + 16X_0^8 \\
 &\quad + 112X_0^4X_1^3X_2 + X_1^8
 \end{aligned}$$

## MacWilliams Identity

### Theorem

The weight enumerators of  $C \leq_R R^n$  and its dual code  $C^\perp \leq R_R^n$  are related by

$$A_{C^\perp}(X_0, X_1, \dots, X_m) = \frac{1}{|C|} \cdot A_C(A_m - X_{m-1}, A_{m-1} - qX_{m-2}, \dots, A_1 - q^{m-1}X_0, A_0),$$

where  $A_i = X_m + (q-1)X_{m-1} + \dots + (q^{m-i} - q^{m-i-1})X_i$  is the weight enumerator of  $N^i$ .

### Sketch of proof.

(1) Define  $\alpha \in \text{Aut } \mathbb{Q}[X_0, \dots, X_m]$  by

$$(\alpha f)(X_0, X_1, \dots, X_m) = f(A_m - X_{m-1}, A_{m-1} - qX_{m-2}, \dots, A_1 - q^{m-1}X_0, A_0)$$

Verify the identity  $\alpha(A_C) = |C| A_{C^\perp}$  for the  $m+1$  codes  $N^i$  ( $0 \leq i \leq m$ ) of length 1, whose weight enumerators  $A_i$  form a basis of  $\langle X_0, \dots, X_m \rangle_{\mathbb{Q}}$ .

## Proof cont'd.

(2) If  $C = C_1 \times C_2$  is a decomposable code and  $\alpha(A_{C_i}) = |C_i| A_{C_i^\perp}$  holds for  $i = 1, 2$ , then  $C^\perp = C_1^\perp \times C_2^\perp$ ,  $A_C = A_{C_1} A_{C_2}$ ,  $A_{C^\perp} = A_{C_1^\perp} A_{C_2^\perp}$  and hence

$$\alpha(A_C) = \alpha(A_{C_1} A_{C_2}) = \alpha(A_{C_1}) \alpha(A_{C_2}) = |C_1| |C_2| A_{C_1^\perp} A_{C_2^\perp} = |C| A_{C^\perp}.$$

It follows that  $\alpha(A_C) = |C| A_{C^\perp}$  also holds for the  $\binom{n+m}{m}$  completely decomposable codes

$$C = \underbrace{R \times \cdots \times R}_{n_0} \times \underbrace{N \times \cdots \times N}_{n_1} \times \cdots \times \underbrace{\{0\} \times \cdots \times \{0\}}_{n_m},$$

whose weight enumerators form a basis of  $\mathbb{Q}[X_0, \dots, X_m]_n$ .

(3) Show the existence of a  $\mathbb{Q}$ -linear endomorphism of  $\mathbb{Q}[X_0, \dots, X_m]$  which sends  $A_C$  to  $|C| A_{C^\perp}$ .

If  $\chi$  is a generating character of  $R$ , then the Fourier transform

$$(\mathcal{F}f)(\mathbf{y}) = \sum_{\mathbf{x} \in R^n} f(\mathbf{x}) \chi(\mathbf{x} \cdot \mathbf{y}) \quad \text{for } f \in \mathbb{Q}R^n \quad (n \geq 0).$$

has this property.



## Simplex Codes

### Definition

The linear code  $C$  associated with the multiset  $\mathfrak{K}$  in  $\text{PG}(R_R^k)$ , defined by  $\mathfrak{K}(P) = 1$  if  $P \in \mathcal{P}$  is a free point and  $\mathfrak{K}(P) = 0$  otherwise, is called the  $k$ -dimensional simplex code over  $R$  and is denoted by  $\text{Sim}(k, R)$ .

The code  $\text{Sim}(k, R)$  has length  $q^{(k-1)(m-1)} \binom{k}{1}_q$ , shape  $\underbrace{(m, \dots, m)}_k$ ,

and cardinality  $|\text{Sim}(k, R)| = q^{km}$ .

All hyperplanes  $H$  of  $\text{PG}(R_R^k)$  have the same  $\mathfrak{K}$ -type  $(a_0, a_1, \dots, a_m)$  given by

$$a_0 = q^{(k-1)(m-1)} \left( \binom{k}{1}_q - \binom{k-1}{1}_q \right) = q^{(k-1)m},$$

$$a_j = q^{(k-2)(m-1)} \binom{k-1}{1}_q (q^{m-j} - q^{m-j-1}), \quad j = 1, \dots, m-1,$$

$$a_m = q^{(k-2)(m-1)} \binom{k-1}{1}_q.$$

To prove this, observe that  $\sum_{s \geq j} a_s$  is the number of free rank 1 submodules contained in  $H + \theta^j R^k$ , a module of shape  $(\underbrace{m, \dots, m}_{k-1}, m - j)$ .

Hence

$$\sum_{s \geq j} a_s = \begin{cases} q^{(k-1)(m-1)} \binom{k}{1}_q & \text{if } j = 0, \\ q^{(k-1)(m-1)} \binom{k-1}{1}_q \cdot q^{1-j} & \text{if } 1 \leq j \leq m. \end{cases}$$

Solving for  $a_j$  gives the stated formulas.

# Hamming Codes

## Definition

The dual code  $\text{Sim}(k, R)^\perp$  is called the *k-th order Hamming code* over  $R$  and is denoted by  $\text{Ham}(k, R)$ .

$\text{Ham}(k, R)$  is free of rank  $q^{(k-1)(m-1)} \binom{k}{1}_q - k$ .

In particular  $|\text{Ham}(k, R)| = q^{mq^{(k-1)(m-1)} \binom{k}{1}_q - mk}$ .

The weight distribution of  $\text{Ham}(k, R)$  can be computed using the MacWilliams identity.

## Example

$C := \text{Sim}(2, \mathbb{Z}_4)$  and  $C^\perp = \text{Ham}(2, \mathbb{Z}_4)$  are generated by

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 3 & 3 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & 1 & 0 & 0 \\ 2 & 3 & 0 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and have weight distributions

$$\begin{aligned} A_C(X_0, X_1, X_2) &= X_2^6 + 3X_1^4 X_2^2 + 12X_0^4 X_1 X_2, \\ A_{C^\perp}(X_0, X_1, X_2) &= \frac{1}{16} A_C(X_2 - X_1, X_1 + X_2 - 2X_0, X_1 + X_2 + 2X_0) \\ &= \dots \end{aligned}$$

$R$  chain ring with  $|R| = q^m$  and  $R/N \cong \mathbb{F}_q$ .

Let

$$C_1 \subset C_2 \subset C_3 \subset \dots \subset C_m \subseteq \mathbb{F}_q^l$$

be a chain of linear  $[l, i, d_i]$  codes of length  $l \geq m$  over  $\mathbb{F}_q$ .  
Suppose that  $C_i$  has generator matrix

$$\mathbf{G}^{(i)} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_i \end{bmatrix}, \quad \mathbf{g}_i \in \mathbb{F}_q^l.$$

Let  $\Gamma$  be a Teichmüller set of  $R$ . Then every  $r \in R$  is uniquely representable as

$$r = r_0 + r_1\theta + \dots + r_{m-1}\theta^{m-1}, \quad \text{where } r_i \in \Gamma.$$

Writing  $\bar{r} = r + N$  for  $r \in R$  define the mapping

$$\psi: \begin{cases} R & \rightarrow \mathbb{F}_q^l \\ r & \rightarrow (c_1, \dots, c_l) \end{cases}$$

by  $\psi(r) = (\bar{r}_{m-1}, \bar{r}_{m-2}, \dots, \bar{r}_0) \mathbf{G}^{(m)} = (c_1, c_2, \dots, c_l)$ .

## Theorem

Let  $C$  be a linear code of length  $n$  over the chain ring  $R$ . Then the code

$$\psi(C) = \left\{ (\psi(c_1), \dots, \psi(c_n)) \mid (c_1, \dots, c_n) \in C \right\}$$

is a code of length  $nl$  over  $\mathbb{F}_q$  having minimum distance

$$d(\psi(C)) \geq \min_{\mathbf{0} \neq \mathbf{c} \in C} \left\{ \sum_{i=0}^{m-1} d_{m-i} \cdot a_i(\mathbf{c}) \right\}.$$

## Corollary

If the codes  $C_i$  in the definition of  $\psi$  are  $[l, i]$  MDS-codes,  $i = 1, \dots, m$ , then the minimum distance of  $\psi(C)$  satisfies

$$d(\psi(C)) \geq \min_{\mathbf{0} \neq \mathbf{c} \in C} \left\{ \sum_{i=0}^{m-1} (l - m + i + 1) a_i(\mathbf{c}) \right\}.$$

Moreover, if  $|R| = q^2$  and  $l = q$  we have

$$d(\psi(C)) = \min_{\mathbf{0} \neq \mathbf{c} \in C} \{ (q-1)a_0(\mathbf{c}) + qa_1(\mathbf{c}) \}.$$

## Reed-Solomon map

In the case  $|R| = q^2$ ,  $l = q$  the map  $\psi$  can be defined by

$$\mathbf{G} = \mathbf{G}^{(2)} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{q-1} \end{pmatrix},$$

where  $\mathbb{F}_q = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$ .

## The case $\text{char } R = p$

$R \cong \mathbb{F}_q[X; \sigma]/(X^m)$  for some  $\sigma \in \text{Aut } \mathbb{F}_q$

$\Gamma$  is a subfield of  $R$

$R$  is a (two-sided) vector space over  $\Gamma$ .

## Theorem

*If the characteristic of  $R$  is  $p$  then the mapping  $\psi: {}_{\Gamma}R \rightarrow \mathbb{F}_q^n$  is semilinear, and consequently  $\psi(C)$  is a linear code over  $\mathbb{F}_q$  for every code  $C$  which is linear over  $R$ .*

## Definition

A code  $C$  over a  $q$ -ary alphabet is said to be *linearly representable* over the chain ring  $R$  if there exists a linear code  $D$  over  $R$  and a mapping  $\psi$  such that  $\psi(D)$  is isomorphic to  $C$ .

## Theorem

Every binary Reed-Muller code  $\mathcal{R}(r, n)$  is linearly representable over  $\mathbb{F}_2[X]/(X^2)$ .

The Reed-Muller codes are in general (for  $3 \leq r \leq n - 2$ ) not linearly representable over  $\mathbb{Z}_4$ .

## Proof.

This follows from the following

## Lemma

A binary code  $C$  containing the zero word is linearly representable over  $R = \mathbb{F}_2[X]/(X^2)$  if and only if  $C$  is linear and the automorphism group of  $C$  contains a regular coordinate permutation of order 2.

Multiplication by  $(1 + X) \in R$  corresponds to a coordinate swap in the Gray image  $\psi(R) = \mathbb{F}_2^2$ . □

# On the MacDonald Codes

## Definition

Let  $K, U$  be positive integers with  $U \leq K$ . A linear code over  $\mathbb{F}_q$  associated with the complement of an  $U - 1$ -dimensional subspace of the projective space  $\text{PG}(K - 1, q)$  is called a *MacDonald code* with parameters  $K, U$ .

A  $q$ -ary MacDonald code with parameters  $K, U$  has length  $N = (q^K - q^U)/(q - 1)$ , dimension  $K$  and only two nonzero weights  $W_1 = q^{K-1} - q^{U-1}$ ,  $W_2 = q^{K-1}$ .

## Theorem

*Every  $q$ -ary MacDonald code whose parameters  $K, U$  satisfy the condition  $U \geq K/2$  is linearly representable over any of the rings  $\mathbb{F}_q[X; \sigma]/(X^2)$ .*

## Proof.

Suppose  $R$  is a chain ring with invariants  $q$  and 2. Choose a free rank  $u$  submodule  $\Sigma$  in  $\text{PHG}(R_R^k)$ ,  $u < k$ . Let  $\mathfrak{K}$  be the set of points in  $\text{PHG}(R_R^k)$  which are neighbours to  $\Sigma$ .

It turns out that the  $q$ -ary Reed-Solomon image  $\psi(C)$  of a linear code  $C$  over  $R$  associated with  $\Sigma$  is a two-weight code with parameters

$$N = \frac{q^{k+u} - q^k}{q - 1}, \quad |\psi(C)| = q^{k+u},$$

$$D = W_1 = q^{k+u-1} - q^{k-1}, \quad W_2 = q^{k+u-1}.$$

Setting  $K = k + u$ ,  $U = k$  we get codes with the same parameters and weight distribution as the  $(K, U)$  MacDonal codes satisfying the condition  $U \geq K/2$ .

If  $R$  has characteristic  $p$ , the resulting codes are linear and hence isomorphic to the corresponding MacDonal codes. □



T. Honold and I. Landjev.

All Reed-Muller codes are linearly representable over the ring of dual numbers over  $\mathbb{Z}_2$ .

*IEEE Transactions on Information Theory*,  
45(2):700–701, Mar. 1999.



T. Honold and I. Landjev.

Linearly representable codes over chain rings.

*Abhandlungen aus dem mathematischen Seminar der  
Universität Hamburg*, 69:187–203, 1999.



T. Honold and I. Landjev.

Linear codes over finite chain rings.

*Electronic Journal of Combinatorics*, 7:Research Paper  
11, 22 pp. (electronic), 2000.



T. Honold and A. A. Nechaev.

Weighted modules and representations of codes.

*Problems of Information Transmission*, 35(3):205–223,  
1999.



G. J. Janusz.

Separable algebras over commutative rings.

*Transactions of the American Mathematical Society*,  
122:461–479, 1966.



G. H. Norton and A. Sălăgean.

On the Hamming distance of linear codes over a finite  
chain ring.

*IEEE Transactions on Information Theory*,  
46(3):1060–1067, May 2000.



G. H. Norton and A. Sălăgean.

On the structure of linear and cyclic codes over a finite  
chain ring.

*AAECC*, 10:489–506, 2000.



R. Raghavendran.

Finite associative rings.

*Compositio Mathematica*, 21:195–229, 1969.



J. A. Wood.

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

*American Journal of Mathematics*, 121(3):555–575, 1999.