Ring-Linear Coding

Unde Venis – Quo Vadis?

Marcus Greferath

School of Mathematical Sciences
University College Dublin
and
Claude-Shannon-Institute for
Discrete Mathematics, Coding, and Cryptography
Ireland

ALCOMA '10 – Thurnau, April 2010

Structure of the Presentation

Structure of the Presentation

- **1963:** In their article on *Error-Correcting Codes: an Axiomatic Approach*, Assmus and Mattson first mention rings as possible alphabets for linear codes.
- **1972/75:** Blake presents linear codes first over semi-simple, later for primary integer residue rings. Analogs of Hamming, Reed-Solomon and BCH Codes are introduced.
- **1977/78:** Spiegel pursues a group-algebraic approach to linear codes over $\mathbb{Z}_m$. Like Blake, he uses the Chinese Remainder Theorem to investigate BCH Codes over these rings.

Ring-linear coding between 1960 and 1990

Shankar, Satyanarayana, $\cdots$

- **1979:** Shankar presents a polynomial approach to cyclic codes over integer residue rings. This enables notions of generator polynomials for cyclic codes.

- **1979:** Satyanarayana investigates linear codes over integer residue rings equipped with the Lee weight. Constant weight codes and Reed-Muller type codes are presented as well.

Note: Most of the early papers only consider the Hamming weight. Although the Lee metric is used by Satyanarayana, a serious consideration of non-Hamming metrics occurs only much later.

Ring-linear coding between 1960 and 1990

Klemm, Nechaev, ···

- **1987/89:** Klemm considers linear codes over integer residue rings and proves MacWilliams' weight enumerator theorem. He uses a suitable weight function to obtain his result.
- **1989:** Nechaev discovers that all Kerdock codes can be understood as $\mathbb{Z}_4$-linear codes.

Note: Nechaev's result, although predating the later breakthrough by Hammons et al, does not involve a statement regarding metrics.

Structure of the Presentation

- **1967:** Nordstrom and Robinson find an optimal binary code with parameters $(16, 2^8, 6)$; the best linear example of same length and distance has 2^7 words.
- **1968:** For even $m \in \mathbb{N}$ Preparata constructs a family of optimal binary codes with parameters $(2^m, 2^{2^m - 2m}, 6)$.
- **1972:** Again, for even $m \in \mathbb{N}$ Kerdock discovers a family of low rate codes with parameters $(2^m, 2^{2m}, 2^{m-1} - 2^{\frac{m-2}{2}})$.

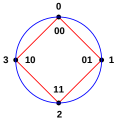
Note: The discovered families appear to be dual in terms of their weight enumerators.

- The Lee weight on $\mathbb{Z}_4$ is defined as

$$w_{\mathrm{Lee}} : \mathbb{Z}_4 \longrightarrow \mathbb{N}, \quad x \mapsto \min\{|x|, |4-x|\}.$$

- It turns out that $(\mathbb{Z}_4, w_{\mathrm{Lee}})$ is isometric to $(\mathbb{Z}_2^2, w_H)$ via the so-called Gray isometry:

$$\begin{array}{rcl} \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2^2, \\ a + 2\,b & \mapsto & a\,(0,1) + b\,(1,1). \end{array}$$



- Componentwise extension of this mapping to $\mathbb{Z}_4^n$ yields a $\mathbb{Z}_4$-linear representation of the Kerdock, Preparata and other Codes.

The most important results

Kerdock, Preparata, Goethals, Delsarte, Calderbank, McGuire, Leech, $\cdots$

- **1994** Hammons et al: All Kerdock, Preparata, Goethals and Goethals-Delsarte Codes are binary images of $\mathbb{Z}_4$-linear codes.
- **1995** Solé: discovery of the relation between the $\mathbb{Z}_4$-linear lift of the binary Golay code and the Leech lattice.
- **1997** Calderbank and McGuire: Discovery of binary codes with parameters $(64, 2^{37}, 12)$ and $(64, 2^{32}, 14)$. These are binary images of $\mathbb{Z}_4$-linear codes with parameters $[32, 16 + \frac{5}{2}, 12]$ and $[32, 16, 14]$.

Structure of the Presentation

Definition: For a finite Ring R we define

- $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$, the character module of R, and
- $\mathrm{soc}({}_RR) := \sum\{I \leq {}_RR \mid I \text{ minimal}\}$, the (left) socle of R.

R is called a Frobenius ring, if any of the following equivalent condition holds:

- ${}_RR \cong {}_R\hat{R}$
- $R_R \cong \hat{R}_R$
- $\mathrm{soc}({}_RR)$ is left principal
- $\mathrm{soc}(R_R)$ is right principal

Examples:

- Every finite field is Frobenius.
- Every Galois ring is Frobenius.
- If R and S are Frobenius, then so will be $R \times S$.
- If R is Frobenius, then so will be $M_n(R)$.
- If R is Frobenius and G is a finite group, then $R[G]$ is Frobenius.

Note: The class of finite Frobenius rings is large. As a non-Frobenius example consider $\mathbb{Z}_2[x, y]/(x^2, y^2, xy)$.

Definition: Let R be a finite ring. A mapping $w : R \longrightarrow \mathbb{Q}$ is called (left) homogeneous weight if $w(0) = 0$ and there is $\gamma \in \mathbb{Q}$ such that for all $x, y \in R$ there holds:

(i) $Rx = Ry$ implies $w(x) = w(y)$,

(ii) $\sum_{y \in Rx} w(y) = \gamma\, |Rx|$ whenever $x \neq 0$.

Examples: The Hamming weight on $\mathbb{F}_q$ is homogeneous with $\gamma = \frac{q-1}{q}$. The Lee weight on $\mathbb{Z}_4$ is homogeneous with $\gamma = 1$.

Question: Do homogeneous weights exist on every finite ring?

Theorem: Let R be a finite Frobenius ring. Then homogeneous weights exist on R and are of the form

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

Here χ is a generating character of R, which means

$$\hat{R} = R\chi = \chi R.$$

Note: There is also a characterisation of homogeneous weights on finite rings that makes use of the Möbius function on the poset of principal left ideals.

- If R is a chain ring with q-element residue field then homogeneous weights have the form

$$R \longrightarrow \mathbb{Q}, \quad r \mapsto \gamma \begin{cases} q-1 & : \quad r \notin \mathrm{soc}({}_R R), \\ q & : \quad 0 \neq r \in \mathrm{soc}({}_R R), \\ 0 & : \quad r = 0. \end{cases}$$

- Homogeneous weights on $M_2(\mathbb{Z}_2)$ are given by

$$M_2(\mathbb{Z}_2) \longrightarrow \mathbb{Q}, \quad A \mapsto \gamma \begin{cases} 1 & : \quad \mathrm{rk}(A) = 2, \\ 2 & : \quad \mathrm{rk}(A) = 1, \\ 0 & : \quad A = 0. \end{cases}$$

Structure of the Presentation

Ring-Linear Coding

Marcus Greferath

History
The First Attempts
Kerdock and Preparata Codes: An Enigma and a Break-Through
Current Problems and Perspectives
Finite Rings and Weight Functions
The Equivalence Theorem
Duality and Weight Enumerators
Existence Bounds
Low-Density Parity-Check Codes
Network Coding over Rings
References and Further Reading

Definition 1: Two codes $C, D \leq {}_RR^n$ are called equivalent, if there is a monomial transformation $\varphi : {}_RR^n \longrightarrow {}_RR^n$ such that $\varphi(C) = D$.

Recall: A monomial transformation φ on ${}_RR^n$ can be written as $\varphi = PD$ where $P \in M_n(R)$ is a permutation matrix, and $D \in M_n(R)$ is an invertible diagonal matrix.

Definition 2: Call two R-linear codes C and D isometric, if there is an isomorphism $\varphi : C \longrightarrow D$ that preserves the distance of codewords.

MacWilliams' 1962: Every isometry between two linear codes over $\mathbb{F}_q$ can be extended to a monomial transformation of the ambient space.

Honold et al 1995: If R is an integer residue ring then every homogeneous isometry (and every Hamming isometry) between R-linear codes can be monomially extended.

Wood 1997: If R is a finite Frobenius ring then every Hamming isometry between two R-linear codes can be monomially extended.

Further Results and Projects

G. and Schmidt 2000: Honold et al's results are true for all finite Frobenius rings. Moreover, a linear mapping between two R-linear codes is a homogeneous isometry if and only if it is a Hamming isometry.

Wood 2000: Characterisation of weight functions on a commutative chain ring that allow for MacWilliams' extension theorem.

G., Honold, McFadden, and Zumbrägel 2010: Characterisation of all weight functions on a commutative principal ideal ring that allow for MacWilliams' equivalence theorem.

Structure of the Presentation

Definition: Let R be a finite Frobenius ring, and let $C \leq {}_R R^n$ be a linear code.

- The dual of C is defined as

$$C^{\perp} \; := \; \Big\{ x \in R^n \mid \sum_{i=1}^{n} c_i x_i = 0 \;\text{ for all }\; c \in C \Big\}.$$

- The (Hamming) weight enumerator of C is the polynomial

$$W_C(x, y) \; = \; \sum_{c \in C} x^{w_H(c)} y^{n - w_H(c)}.$$

Code duality

A classical result

Question: Relation between weight enumerators of mutually dual codes?

Theorem: (MacWilliams' 1962) If $C \leq \mathbb{F}_q^n$ is a linear code then

$$W_{C^\perp}(x,y) \;=\; \frac{1}{|C|} W_C\Big(y-x, y+(q-1)x\Big).$$

Question: What can be said about this theorem in the framework of ring-linear coding?

Wood 1997: If R is a finite Frobenius ring and C an R-linear code of length n, then

$$W_{C^\perp}(x,y) \;=\; \frac{1}{|C|}\,W_C\Big(y-x,\,y+(|R|-1)x\Big).$$

Wood 1997: An according result holds for the complete weight enumerators, and certain symmetrised weight enumerators.

Byrne, G., and O'Sullivan 2007: A general MacWilliams' relation for pairs of so-called compatible partitions on the base ring R.

Question: The Frobenius property is sufficient. Is it necessary?

Results:

- Wood 1997: For commutative rings this can be shown easily.
- Wood 2008: This also holds in the non-commutative case.
- G., Nechaev, and Wisbauer 2004: Exchanging the alphabet R by the R-module $\hat{R}$ all foundational statements hold for **any** finite ring R.

Structure of the Presentation

Premises:

- Let R be a finite Frobenius ring, and let w be the homogeneous weight of average value γ on R.
- Agree on $A_w(n, d)$ denoting the maximal possible code cardinality under length n and distance d.

G. and O'Sullivan 2004: For every n, d with $\gamma\, n < d$ there holds

$$A_w(n, d) \;\leq\; \frac{d}{d - \gamma\, n}.$$

Existence bounds

An Elias bound

Premise: Additionally, denote by $V_w(n,t)$ the volume of the homogeneous disk of radius t in n-space.

G. and O'Sullivan 2004: For every n, d, t with $t \leq \gamma\, n$ and $t^2 - 2\, t\gamma\, n + d\gamma\, n > 0$ there holds

$$A_w(n,d) \;\leq\; \frac{\gamma\, n\, d}{t^2 - 2\, t\gamma\, n + d\gamma\, n} \cdot \frac{|R|^n}{V_w(n,t)}.$$

Note: Both theorems can also be combined to derive an asymptotic version of the Elias bound.

Byrne, G., and O'Sullivan: Several versions of the LP-bound allowing for symmetrisation with respect to

- homogeneous weights,
- subgroups of the group $R^{\times}$ of invertible elements,
- further important weights, like the Lee-weight.

Remark:

- It is comparably trivial to formulate a sphere-packing and a Gilbert-Varshamov bound (regardless of the underlying weight).
- For a Singleton bound and further refinements see **Byrne, G., Kohnert, and Skachek 2010.**

Structure of the Presentation

- Hensel-lifting the generator polynomials of cyclic codes sometimes induces ring-linear codes of good homogeneous minimum weight.
- The quality of these codes is often measured in terms of parameters of images under so-called generalised Gray isometries.
- **Duursma, G., Litsyn, and Schmidt 2001:** A binary $(96, 2^{37}, 24)$-code can be derived from a $\mathbb{Z}_8$-linear lift of the binary Golay code. The best previously known distance was 20.

- **Kou, Lin, and Fossorier 2001:** Finite-Geometry codes are examples of very good LDPC codes.
- These codes are of moderate girth 6, but seem to have reasonable minimum distances to make them useful for communications.
- As (a class of) projective geometry codes can be taken into cyclic form, it is obviously interesting to wonder, how Hensel lifts of these codes might perform.
- **Thesis project McFadden:** The lifted codes are strictly spoken of girth 4, but each cycle of length 4 in their Tanner graph contains an edge of weight 2.

We lift the generator of the binary $[7,4,3]$ Hamming code to $\mathbb{Z}_4$, and write down a matrix consisting of all 7 cyclic shifts of this generator.

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

This matrix checks the $\mathbb{Z}_4$-linear $[7,3,6]$ Kerdock code.

- Ring-linear LDPC codes have been studied in **Mo and Armand 2008**, where the constructions was based on latin squares.
- Random constructions of LDPC codes over $\mathbb{Z}_4$ and $\mathbb{Z}_8$ were considered by **Fuja et al 2005**.
- A most important item to solve is to amend the iterative decoding algorithm in the appropriate way.
- Discussions with electrical engineering experts have revealed their high interest in this topic in the context of what is called higher order modulation.

Structure of the Presentation

- We restrict our focus to Random Network Coding as introduced by **Koetter and Kschischang 2008.**
- The dimension formula on subspace lattices of vector spaces explains the properties of the induced distance function.
- It is easy to observe that the rank function on a (modular) lattice induces a metric in the same fashion.
- **Byrne et al 2009:** At least for submodule lattices of free modules over chain rings there is no gain, if the rank metric is used.

- Traditional algebraic coding theory experienced a breakthrough when it was discovered that a non-Hamming metric has to be used.

- **Question:** Is there a metric on submodule lattices, that generalises the rank metric of vector space lattices in the same way, as the homogeneous weight generalises the Hamming weight?

- In any case, a ring-analog of q-ary design theory as it is pursued in the Bayreuth group **(Kohnert/Wassermann)** should give rise to new network code constructions over rings.

References I

J. van Lint.
An Introduction to Coding Theory.
Springer Verlag, 1998.

A. R. Hammons, P. V. Kumar, P. Vijay, A. R. Calderbank, N. J. A. Sloane, and P. Solé.
The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes.
IEEE Trans. Inform. Theory 40 (1994): 301–319.

J. A. Wood.
Duality for modules over finite rings and applications to coding theory.
Amer. J. Math. 121 (1999): 555–575.

References II

- M. Greferath and M. E. O'Sullivan.
  On bounds for codes over Frobenius rings under homogeneous weights.
  J Discrete Math. 289 (2004): 11–24.
- M. Greferath, A. Nechaev, and R. Wisbauer.
  Finite quasi-Frobenius modules and linear codes.
  J. Algebra Appl. 3 (2004): 247–272.
- E. Byrne, M. Greferath, and M. O'Sullivan.
  The linear programming bound for codes over finite Frobenius rings.
  Designs, Codes, Cryptography. 42 (2007): 289–301.