Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Transition from classical to ring-linear case

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University School of Sciences
marcus.greferath@aalto.fi

May 2023

- **Definition:** Let ω be a primitive element of $\mathbb{F}_q$, and let $0 \leq b \leq q-2$ and δ be a positive integer. The polynomial

$$g := \prod_{i=b}^{b+\delta-2} (x - \omega^i) \in \mathbb{F}_q[x]$$

generates a cyclic code of length $q-1$ that we call a Reed-Solomon Code.

- **Remark:** Using Vandermonde determinants one can show that the Reed-Solomon code is a $[q-1, q-\delta, \delta]$ code.

- Reed Solomon codes satisfy the Singleton bound with equality, and hence they are MDS codes.

- **Definition:** Let n be a positive integer, and let ω be a primitive n-th root of unity in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. Let $0 \leq b \leq n-1$ and δ be a positive integer. Let $g \in \mathbb{F}_q[x]$ be the non-zero (monic) polynomial of smallest degree satisfying

$$g(\omega^i) = 0 \ \text{ for } i = b, b+1, \ldots, b+\delta-2.$$

  The cyclic code of length n generated by g is called a BCH code of designed distance δ.

- **Remark:** BCH codes have minimum distance at least δ. They were discovered by Bose, Chaudhuri and Hocquenghem around 1960.

- They are not MDS in general, as the polynomial g will not vanish on full cyclotomic cosets of the ω^i involved.

- **Example:** Let $n = \frac{q^r-1}{q-1}$ with $\gcd(q,r)=1$ and let C_1 be the cyclotomic coset containing 1. For

$$g = \prod_{i \in C_1} (x - \omega^i),$$

the cyclic code generated by g is (equivalent to) the q-ary Hamming code of rank r.

- So, at least for the case $\gcd(q,r)=1$, we see that there are cyclic versions of the Hamming codes.
- The literature is full of further generalizations which run under the names Alternant Codes, Goppa Codes, and many more.
- All these codes can be decoded without big effort using the Euclidean Algorithm to find gcds of polynomials.

- The most famous algorithm for BCH decoding however is the Berlekamp-Massey algorithm.
- More recent developments by M. Sudan and V. Guruswami in the nineties allow to correct error patterns even beyond half of the minimum distance of these codes.
- Further codes would deserve discussion, among them the powerful Algebraic Geometry codes. We will not be able to do this here in light of the temporal restrictions.
- Sudan's list decoding algorithm was particularly spectacular, as it allowed to decode even the Algebraic Geometry codes, for which there had not been an efficient decoder so far.

- Let n be an odd prime and p an arbitrary prime such that p is a quadratic residue modulo n.
- Let ω be a primitive n-th root (in some extension field of $\mathbb{F}_p$, and define

$$g_0 := \prod_{i \in Q} (x - \omega^i) \text{ and } g_1 := \prod_{i \in N} (x - \omega^i)$$

  where Q and N describe the quadratic residues (except 0) and non-residues modulo n.
- **Definition:** We have the factorization $x^n - 1 = (x - 1)g_0 g_1$ in $\mathbb{F}_p[x]$, and the cyclic code C generated by g_0 (or g_1) are called a Quadratic Residue Code.

- Their extended versions are self-dual if $n \equiv -1 \pmod 4$, otherwise, they are not self-dual, but iso-dual.
- Important examples are the binary $[7, 4, 3]$ Hamming code of length and the two Golay codes.
- For their minimum distance $d_H(C)$ there is a rather weak bound that says $w_H(C) \geq \sqrt{n}$.
- The literature contains a number of (successful) attempts to improve over this bound in given cases.
- The famous Gleason-Prange theory provides strong tools to prove structural results and derive weight enumerators.

Two miraculous non-linear families

Kerdock and Preparata codes

- **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 (or better distance) enumerators.

A brief sketch: From Assmus & Mattson to Nechaev

- **1963:** Assmus and Mattson mention rings as possible alphabets in their article Error-Correcting Codes: an Axiomatic Approach.
- **1972:** Blake presents linear codes first over semi-simple, later for primary integer residue rings.
- ...
- **1987:** Klemm considers linear codes over integer residue rings and proves MacWilliams' weight enumerator theorem.
- **1989:** Nechaev discovers that all Kerdock codes become cyclic when considered as codes over $\mathbb{Z}_4$.

$\mathbb{Z}_4$-linear representation of binary codes

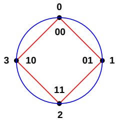
The Gray isometry

- 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:

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



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

Three important results

- **1994** Hammons et al: All Kerdock, Preparata, Goethals and Goethals-Delsarte Codes are binary images of $\mathbb{Z}_4$-linear codes.

- **1995** Bonnecaze and Solé: How to obtain the Leech lattice by construction A from a $\mathbb{Z}_4$-version of the binary Golay code.

- **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 $[32, 16, 14]$.

Finite rings and modules

Note: Rings R are associative and possess an identity 1.

Useful Facts:

- The Jacobson radical $J(R)$ of R is the intersection of all maximal (left) ideals of R. It is a two-sided ideal.
- If R is finite, then $J(R)$ is a nilpotent ideal.
- If R is finite then $R/J(R)$ is a direct product of full matrix rings over finite fields.
- The left socle $\mathrm{soc}({}_R R)$ is the sum of all minimal left ideals of R. It is two-sided, but might not coincide with the right socle.
- The polynomial ring $R[x]$ is anything but a unique factori- zation domain. Is it a mess? Well. . .

Finite rings and modules

Note: Modules ${}_R M$ will be unital, i.e. $1m = m$ for all $m \in M$.

Further Useful Facts:

- Projective modules ${}_R P$ are those where every epimorphism onto ${}_R P$ has a kernel that is a direct summand.
- Projective modules are characterized as direct summands of free modules.
- Injective modules occur as direct summands wherever they are embedded.
- (Left) Self-injective rings R are those where the module ${}_R R$ is injective.
- If R is finite, then self-injectivity is left-right symmetric; these rings are then called quasi-Frobenius rings.

Finite Frobenius rings

Recall: For a finite Ring R we have

- $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$, the character module of R.
- $\hat{R}$ becomes an R-R-bimodule, by the definition:
  - ${}^r\chi(x) := \chi(xr)$, and
  - $\chi^r(x) := \chi(rx)$,

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

Definition: R is called a <u>Frobenius ring</u>, if any of the following equivalent (left-right symmetric) conditions hold:

- ${}_R R \cong {}_R \hat{R}$,
- $\mathrm{soc}({}_R R)$ is left principal.

Examples of finite Frobenius rings

How the Frobenius property inherits

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 $\mathbb{Z}_2[x, y]/(x^2, y^2, xy)$.

The discrete Fourier transform

Definition: Let R be a finite Frobenius ring, and let χ be a generating character, i.e. $\hat{R}$ is generated by χ.

- For a complex valued function f on R define its Fourier transform $\hat{f} : R \longrightarrow \mathbb{C}$ by

$$\hat{f}(s) := \sum_{r \in R} f(r)\chi(-rs), \quad \text{for } s \in R.$$

- The inverse transform is given by

$$\tilde{f}(s) := \frac{1}{|R|} \sum_{r \in R} f(r)\chi(sr), \quad \text{for } s \in R,$$

meaning, we have $\tilde{\hat{f}} = f = \hat{\tilde{f}}$.

Homogeneous weights

History: Homogeneous weights were introduced by Heise et al. [1995] for $\mathbb{Z}_m$ to generalise the Hamming weight.

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

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

(ii) $\displaystyle\frac{1}{|Rx|} \sum_{y \in Rx} w(y) = \gamma$, provided $x \neq 0$.

Remark: Indeed, property (ii) is a length 1 version of a well-known fact in finite-field coding theory:

$$\frac{1}{|C|} \sum_{c \in C} w_H(c) = \frac{q-1}{q} |\mathrm{supp}(C)|.$$

Homogeneous weights on Frobenius rings

- Homogeneous weights do exist on any finite ring and module.
- They enjoy a description involving the Möbius function on the poset of principal left ideals of the underlying ring.
- **Theorem:** Homogeneous weights on a finite Frobenius ring R are of the form

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

where again, χ is a generating character of R.

Examples of homogeneous weights

- w_H on $\mathbb{F}_q$ is homogeneous with $\gamma = \frac{q-1}{q}$; the Lee weight w_{Lee} on $\mathbb{Z}_4$ is homogeneous with $\gamma = 1$.

- 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

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

Cyclic codes

- **Definition:** An R-linear code is called cyclic, if it is invariant under cyclic coordinate shifts.
- Cyclic codes of length n can be identified with ideals in the residue ring $R[x]/(x^n - 1)$.
- **Known Fact:** If $C \leq \mathbb{F}_q^n$ is a cyclic code then there exists a unique monic divisor g of $x^n - 1$ in $\mathbb{F}_q[x]$ such that

$$C = \mathbb{F}_q[x]g/(x^n - 1).$$

- The proof of this fact is quite elementary, however vastly relies on the euclidean property of $\mathbb{F}_q[x]$.
- **Question:** What remains true in the ring-linear case?

Cyclic codes

- **Definition:** Let R be a finite ring. We call an R-linear code $C \leq {}_R R^n$ a splitting code, if it is a direct summand of ${}_R R^n$.
- **G. 1997:** For a linear code $C \leq {}_R R^n$ the following are equivalent:
  - C is a cyclic splitting code.
  - There exists a polynomial g dividing $x^n - 1$, such that

$$C \;=\; R[x]g/(x^n - 1).$$

- The proof of this fact is less elementary; it relies on all the facts that we mentioned in the preliminaries on finite rings and modules.

Equivalence of linear codes

Two definitions

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

Recall: A monomial transformation φ on ${}_R R^n$ 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.

Equivalence of linear codes

A general justification

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 $R = \mathbb{Z}_m$ 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, Wood, and Zumbrägel 2015: Characterisation of all weight functions on a finite Frobenius ring that allow for MacWilliams' equivalence theorem.

Code duality

Basic definitions

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

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

- 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

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

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

Code duality

Generalisations

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

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

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 compatible pairs of partitions on the base ring R.

Existence bounds

A Plotkin bound

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

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

Remark: The first result is the Plotkin bound, the second is the Elias bound. Both results can also be combined to derive an asymptotic version of the Elias bound.

Existence bounds

Further bounds

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**.

A final remark

Is the Frobenius property necessary?

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.