Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Codes over finite rings

Marcus Greferath

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

May 2023

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

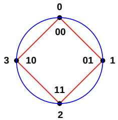
The Gray isometry

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

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

- It turns out that $(\mathbb{Z}_4, w_{\text{Lee}})$ 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 ${}_RM$ will be unital, i.e. $1m = m$ for all $m \in M$.

Further Useful Facts:

- Projective modules ${}_RP$ are those where every epimorphism onto ${}_RP$ 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 ${}_RR$ 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 Frobenius ring, 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) $\frac{1}{|Rx|} \sum_{y \in Rx} w(y) = \gamma$, 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.