Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Finishing coding over finite rings

Marcus Greferath

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

May 2023

Code Optimality

- Let R be a finite ring and let δ be a metric on R, additively extended to a metric on R^n.
- **Definition:** For non-negative numbers d and n define

$$A_{R,\delta}(n,d) := \max\{M \mid \exists\ (n,M,d)\text{-Code over } R\}.$$

- **Goal:** Determine $A_{R,\delta}(n,d)$ for given n and d.
- **Note:** Here d is (obviously) referring to the minimum distance with respect to the metric δ.
- In all what follows either $R = \mathbb{F}_2$ and $\delta = \delta_H$ the Hamming metric, or $R = \mathbb{Z}_4$ and $\delta = \delta_{\text{Lee}}$ the Lee metric.

An optimal binary $(10, 40, 4)$ code

- It was known for long that

$$A_{\mathbb{F}_2,\delta_H}(10,4) \;\le\; 40.$$

- Best [1978] came up with the construction of a binary code meeting this bound. It consists of the words

$$0100000011, 0011111101, 1100101100, 0001010111$$

together with all cyclic shifts of these.

- The distance enumerator of Best's code is given by

$$D_H(x,y) \;=\; x^{10} + 22x^6y^4 + 12x^4y^6 + 5x^2y^8.$$

An optimal binary $(10, 40, 4)$ code

- Best also determined the automorphism group of the code in question: it is a semidirect product of the dihedral group D_5 and $\mathbb{Z}_2^5$ and hence has 320 elements.

- Litsyn and Vardy [1993] showed that Best's code is unique, i.e. any binary $(10, 40, 4)$ code must be isometric to Best's code.

- Applying what is called **Construction A** to Best's $(10, 40, 4)$ code yields the densest sphere packing presently known in 10 dimensions.

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

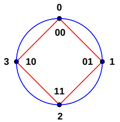
The Gray isometry

- Recall the Lee metric on $\mathbb{Z}_4$ defined as

$$\begin{array}{rcl} \delta_{\mathrm{Lee}} : \mathbb{Z}_4 \times \mathbb{Z}_4 & \longrightarrow & \mathbb{N}, \\ (x, y) & \mapsto & \min\{|(x-y)_4|, |4-(x-y)_4|\}. \end{array}$$

- It turns out that $(\mathbb{Z}_4, \delta_{\mathrm{Lee}})$ is isometric to $(\mathbb{Z}_2^2, \delta_H)$ 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 an isometry between $(\mathbb{Z}_4^n, \delta_{\mathrm{Lee}})$ and $(\mathbb{Z}_2^{2n}, \delta_H)$.

The pentacode

An observation by Conway and Sloane 1994

- The Code $P \subseteq \mathbb{Z}_4^5$ consisting of all words

$$(c-d, b, c, d, b+c) \quad \text{where} \quad b, c, d \in \{1, 3\}$$

  and all cyclic shifts of these has parameters $(5, 40, 4)$.

- The Gray image of P is (up to equivalence) the $(10, 40, 4)$ code discovered by Best.

- P is invariant under the automorphisms

$$\begin{aligned}
(a, b, c, d, e) &\mapsto (-a, -b, -c, -d, -e), \\
(a, b, c, d, e) &\mapsto (-a, 2-b, c, 2-d, -e), \\
(a, b, c, d, e) &\mapsto (b, c, d, e, a), \\
(a, b, c, d, e) &\mapsto (2+e, 2+d, 2+c, 2+b, 2+a).
\end{aligned}$$

Cyclic codes and group rings

- For a finite ring R consider the group ring

$$R[\mathbb{Z}_n] \;:=\; \text{set of all } R\text{-valued functions on } \mathbb{Z}_n$$

equipped with natural addition $+$ and multiplication $\star$ that is given by cyclic convolution

$$g \star f\,(i) \;:=\; \sum_{j \in \mathbb{Z}_n} g(i-j)f(j).$$

- A cyclic code of length n over R can then be under- stood as a subset in $R[\mathbb{Z}_n]$ that is closed under multi- plication by δ_1, where

$$\delta_1(i) = \begin{cases} 1 & : \quad i = 1, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

Discrete Fourier transform

Definition: Let $S:R$ be a ring extension that contains a primitive n-th root of unity ω, and assume $n \in R^\times$.

- For $f \in S[\mathbb{Z}_n]$ define the <u>Fourier transform</u> $\hat{f} \in S[\mathbb{Z}_n]$ by

$$\hat{f}(i) \ := \ \sum_{j \in \mathbb{Z}_n} f(j)\, \omega^{-ji}.$$

- In fact, the inverse transform is given by

$$\tilde{f}(i) \ := \ \frac{1}{n} \sum_{j \in \mathbb{Z}_n} f(j)\, \omega^{ij},$$

and this means we have $\tilde{\hat{f}} = f = \hat{\tilde{f}}$ for all $f \in S[\mathbb{Z}_n]$.

The Fourier transform of the pentacode

- We chose to analyse the pentacode, because Best's original binary code does not satisfy $n \in \mathbb{F}_2^\times$.
- For this we find that the Galois ring $\mathrm{GR}(4,4)$ as an extension of $\mathbb{Z}_4$ contains the required primitive 5-th root of unity ω.
- The minimal polynomial of ω over $\mathbb{Z}_4$ is given by

$$\varphi_\omega = x^4 + x^3 + x^2 + x + 1.$$

- We computed the Fourier transform of all words of the pentacode and arrived at the following list.

The Fourier transform of the pentacode

$$(1, 3\,\omega^3 + \omega^2, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 3, \omega^3 + \omega^2 + 2\,\omega + 1, \omega^3 + 3\,\omega^2)$$
$$(1, \omega^3 + 3\,\omega^2 + 3\,\omega, \omega^3 + 2\,\omega + 1, 2\,\omega^3 + 3\,\omega^2 + 2\,\omega + 3, 2\,\omega^2 + \omega + 1)$$
$$(1, 2\,\omega^3 + \omega^2 + 3\,\omega + 1, 3\,\omega^3 + 2\,\omega^2 + \omega, \omega^3 + 2\,\omega^2 + 3\,\omega + 3, 2\,\omega^3 + 3\,\omega^2 + \omega + 2)$$
$$(1, 3\,\omega^3 + 3\,\omega^2 + 3\,\omega + 2, \omega^3 + 3, \omega^2 + 3, \omega + 3)$$
$$(1, 3\,\omega^3 + \omega^2 + 3\,\omega + 2, 3\,\omega^3 + 2\,\omega^2 + 2\,\omega + 1, \omega^2 + 2\,\omega + 3, 2\,\omega^3 + \omega + 3)$$
$$(1, 2\,\omega^3 + \omega^2 + 3\,\omega + 2, 3\,\omega^3 + 2\,\omega^2 + \omega + 1, \omega^3 + 2\,\omega^2 + 3\,\omega, 2\,\omega^3 + 3\,\omega^2 + \omega + 3)$$
$$(1, 3\,\omega + 1, 3\,\omega^2 + 1, 3\,\omega^3 + 1, \omega^3 + \omega^2 + \omega + 2)$$
$$(1, \omega^3 + \omega^2 + 2\,\omega, 3\,\omega^3 + \omega^2 + 3, \omega^3 + 3\,\omega^2 + 3, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 2)$$
$$(1, \omega^3 + \omega^2 + 2\,\omega + 2, 3\,\omega^3 + \omega^2 + 1, \omega^3 + 3\,\omega^2 + 1, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega)$$
$$(1, 2\,\omega^2 + 3\,\omega + 3, 2\,\omega^3 + \omega^2 + 2\,\omega + 1, 3\,\omega^3 + 2\,\omega + 3, 3\,\omega^3 + \omega^2 + \omega)$$
$$(1, \omega^3 + \omega^2 + 3\,\omega, 3\,\omega^3 + 2\,\omega^2 + 3, 2\,\omega^3 + 3\,\omega^2 + 3, 2\,\omega^3 + 2\,\omega^2 + \omega + 1)$$
$$(1, 3\,\omega^2 + \omega, \omega^3 + 2\,\omega^2 + \omega + 1, \omega^3 + 3\,\omega, 2\,\omega^3 + 3\,\omega^2 + 3\,\omega + 3)$$
$$(1, 2\,\omega^3 + 3\,\omega + 1, 3\,\omega^2 + 2\,\omega + 1, \omega^3 + 2\,\omega^2 + 2\,\omega + 3, \omega^3 + 3\,\omega^2 + \omega + 2)$$
$$(1, 2\,\omega^3 + \omega^2 + \omega + 1, 3\,\omega^3 + \omega, 3\,\omega^3 + 2\,\omega^2 + 3\,\omega + 3, \omega^2 + 3\,\omega)$$
$$(1, 2\,\omega^3 + 2\,\omega^2 + 3\,\omega + 3, 2\,\omega^3 + \omega^2 + 1, \omega^3 + 2\,\omega^2 + 1, 3\,\omega^3 + 3\,\omega^2 + \omega)$$
$$(1, 3\,\omega^3 + \omega^2 + 2, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 1, \omega^3 + \omega^2 + 2\,\omega + 3, \omega^3 + 3\,\omega^2 + 2)$$
$$(1, 2\,\omega^3 + 3\,\omega^2 + 3\,\omega, \omega^3 + 3\,\omega + 1, \omega^3 + 2\,\omega^2 + \omega + 2, 3\,\omega^2 + \omega + 1)$$
$$(1, \omega^2 + \omega + 3, 3\,\omega^3 + 3\,\omega + 2, \omega^3 + \omega + 3, 3\,\omega^2 + 3\,\omega + 2)$$
$$(1, \omega^2 + 3\,\omega + 3, 3\,\omega^3 + 2\,\omega^2 + 3\,\omega + 2, 3\,\omega^3 + \omega + 3, 2\,\omega^3 + \omega^2 + \omega)$$
$$(1, \omega^2 + \omega + 2, 3\,\omega^3 + 3\,\omega + 1, \omega^3 + \omega + 2, 3\,\omega^2 + 3\,\omega + 1)$$

The Fourier transform of the pentacode

$(3, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 2, \omega^3 + 3\,\omega^2 + 3, 3\,\omega^3 + \omega^2 + 3, \omega^3 + \omega^2 + 2\,\omega)$
$(3, 2\,\omega^3 + 3\,\omega^2 + 3\,\omega + 3, \omega^3 + 3\,\omega, \omega^3 + 2\,\omega^2 + \omega + 1, 3\,\omega^2 + \omega)$
$(3, 2\,\omega^3 + \omega^2 + \omega, 3\,\omega^3 + \omega + 3, 3\,\omega^3 + 2\,\omega^2 + 3\,\omega + 2, \omega^2 + 3\,\omega + 3)$
$(3, 2\,\omega^3 + \omega + 3, \omega^2 + 2\,\omega + 3, 3\,\omega^3 + 2\,\omega^2 + 2\,\omega + 1, 3\,\omega^3 + \omega^2 + 3\,\omega + 2)$
$(3, 2\,\omega^3 + 2\,\omega^2 + \omega + 1, 2\,\omega^3 + 3\,\omega^2 + 3, 3\,\omega^3 + 2\,\omega^2 + 3, \omega^3 + \omega^2 + 3\,\omega)$
$(3, 3\,\omega^2 + 3\,\omega + 1, \omega^3 + \omega + 2, 3\,\omega^3 + 3\,\omega + 1, \omega^2 + \omega + 2)$
$(3, \omega^3 + 3\,\omega^2, \omega^3 + \omega^2 + 2\,\omega + 1, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 3, 3\,\omega^3 + \omega^2)$
$(3, 2\,\omega^3 + 3\,\omega^2 + \omega + 2, \omega^3 + 2\,\omega^2 + 3\,\omega + 3, 3\,\omega^3 + 2\,\omega^2 + \omega, 2\,\omega^3 + \omega^2 + 3\,\omega + 1)$
$(3, \omega^2 + 3\,\omega, 3\,\omega^3 + 2\,\omega^2 + 3\,\omega + 3, 3\,\omega^3 + \omega, 2\,\omega^3 + \omega^2 + \omega + 1)$
$(3, 3\,\omega^3 + 3\,\omega^2 + \omega, \omega^3 + 2\,\omega^2 + 1, 2\,\omega^3 + \omega^2 + 1, 2\,\omega^3 + 2\,\omega^2 + 3\,\omega + 3)$
$(3, \omega^3 + \omega^2 + \omega + 2, 3\,\omega^3 + 1, 3\,\omega^2 + 1, 3\,\omega + 1)$
$(3, 2\,\omega^3 + 3\,\omega^2 + \omega + 3, \omega^3 + 2\,\omega^2 + 3\,\omega, 3\,\omega^3 + 2\,\omega^2 + \omega + 1, 2\,\omega^3 + \omega^2 + 3\,\omega + 2)$
$(3, \omega + 3, \omega^2 + 3, \omega^3 + 3, 3\,\omega^3 + 3\,\omega^2 + 3\,\omega + 2)$
$(3, 3\,\omega^2 + \omega + 1, \omega^3 + 2\,\omega^2 + \omega + 2, \omega^3 + 3\,\omega + 1, 2\,\omega^3 + 3\,\omega^2 + 3\,\omega)$
$(3, \omega^3 + 3\,\omega^2 + 2, \omega^3 + \omega^2 + 2\,\omega + 3, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega + 1, 3\,\omega^3 + \omega^2 + 2)$
$(3, 3\,\omega^3 + 3\,\omega^2 + 2\,\omega\omega^3 + 3\,\omega^2 + 1, 3\,\omega^3 + \omega^2 + 1, \omega^3 + \omega^2 + 2\,\omega + 2)$
$(3, 3\,\omega^3 + \omega^2 + \omega, 3\,\omega^3 + 2\,\omega + 3, 2\,\omega^3 + \omega^2 + 2\,\omega + 1, 2\,\omega^2 + 3\,\omega + 3)$
$(3, \omega^3 + 3\,\omega^2 + \omega + 2, \omega^3 + 2\,\omega^2 + 2\,\omega + 3, 3\,\omega^2 + 2\,\omega + 1, 2\,\omega^3 + 3\,\omega + 1)$
$(3, 2\,\omega^2 + \omega + 1, 2\,\omega^3 + 3\,\omega^2 + 2\,\omega + 3, \omega^3 + 2\,\omega + 1, \omega^3 + 3\,\omega^2 + 3\,\omega)$
$(3, 3\,\omega^2 + 3\,\omega + 2, \omega^3 + \omega + 3, 3\,\omega^3 + 3\,\omega + 2, \omega^2 + \omega + 3)$

The Fourier transform of the pentacode

Results

- It is apparent that the spectrum of each word of P is not only non-zero, but solely consists of invertible elements in $\mathrm{GR}(4,4)$.
- An afternoon's work revealed the following fact. Let

$$\begin{aligned}
\hat{f} &:= (1, 3\omega+1, 3\omega^2+1, 3\omega^3+1, 3\omega^4+1) \\
\hat{g} &:= (1, 3\omega+2, 3\omega^2+2, 3\omega^3+2, 3\omega^4+2) \\
\hat{h} &:= (1, 2\omega+3, 2\omega^2+3, 2\omega^3+3, 2\omega^4+3) \\
\hat{u} &:= (1, \omega, \omega^2, \omega^3, \omega^4)
\end{aligned}$$

Then for each word $c \in P$ there holds

$$\hat{c} = (-1)^i \hat{f} \cdot \hat{g}^j \cdot \hat{h}^k \cdot \hat{u}^n, \quad i, j, k \in \mathbb{Z}_2,\ n \in \mathbb{Z}_5.$$

The algebraic structure of the pentacode

Results

- Transforming back we can reformulate, namely:

$$\begin{aligned} f &= (2,0,1,1,1) \\ g &= (2,3,0,0,0) \\ h &= (3,2,0,0,0) \\ u &= (0,1,0,0,0) \end{aligned}$$

  Then for each word $c \in P$ there holds

$$c = (-1)^i f \star g^j \star h^k \star u^n, \quad i,j,k \in \mathbb{Z}_2,\ n \in \mathbb{Z}_5.$$

- **Remark:** As $\gcd(10,2) \neq 1$, we would not have been able to apply spectral arguments directly to Best's code.
- We observe however that $\gcd(5,4) = 1$, and this enabled the current work!

The algebraic structure of the pentacode

Results, continued

- Transferring this result into the ring $\mathbb{Z}_4[x]/(x^5-1)$ we find after rescaling:

$$\begin{aligned} f &= x^4+x^3+x^2+2 \\ g &= x+2 \\ h &= 2x+1 \\ u &= x \end{aligned}$$

  Here, $h^2=1$, g is of order 10 and $u=g^6$.

- **Conclusion:** Each word $c \in P$ is of the form

$$c \;=\; (-1)^i\, f\, h^j\, g^k, \quad i,j \in \mathbb{Z}_2,\; k \in \mathbb{Z}_{10}.$$

The algebraic structure of the pentacode

Results, continued

- Consequently, the pentacode is a coset

$$P = fU$$

  where U is a 40 element subgroup of the group of invertible elements of $\mathbb{Z}_4[x]/(x^5 - 1)$.

- There are 155 subgroups of order 40 in the 480-element unit group of $\mathbb{Z}_4[x]/(x^5 - 1)$.
- Only 2 of these subgroups yield (up to equivalence) the pentacode.
- Moreover, the pentacode occurs twice among the 12 cosets of each of these two subgroups.

What can further be done?

Perspectives

- **Definition:** Let R be a finite ring and let n be a positive integer, such that $n \in R^{\times}$. A strong character is a map $\mathbb{Z}_n \xrightarrow{\chi} R^{\times} \cap Z(R)$ such that:

$$\sum_{j \in \mathbb{Z}} \chi(ji) = \begin{cases} n & : \text{ if } i = 0, \\ 0 & : \text{ otherwise.} \end{cases}$$

- If this is the case we will say, R is target of a strong character on $\mathbb{Z}_n$.

- We then obtain the Fourier transform of a word $c \in R^n$ as $\hat{c} \in R^n$ defined by :

$$\hat{c}_i := \sum_{j \in \mathbb{Z}_n} c_j \chi(ji) \text{ for } i \in \mathbb{Z}_n.$$

The discrete Fourier transform (cnt'd)

- In fact, the inverse transform is given by

$$\tilde{c}_i \;:=\; \frac{1}{n} \sum_{j \in \mathbb{Z}_n} c_j \, \chi(-ij) \;\text{ for }\; i \in \mathbb{Z}_n \,,$$

  meaning that we have $\tilde{\hat{c}} = c = \hat{\tilde{c}}$.

- **Remark:** The Fourier transform satisfies the famous convolution theorem, which says

$$\widehat{f \star g} \;=\; \hat{f} \cdot \hat{g}, \quad \text{for all } \; f, g \in R^n \,.$$

- Here $\star$ denotes the additive convolution which means

$$(f \star g)_i \;=\; \sum_{a+b=i} f_a g_b.$$

The discrete Fourier transform (cnt'd)

- So far, the convolution theorem relies on the character χ taking values only in the center $Z(S)$.
- Fourier transform and convolution theorem are both important ingredients in the proof of the BCH bound.
- **Original question:** Which finite rings are target of a strong character on $\mathbb{Z}_n$?
- **Relaxed version:** Which finite rings R have a unital extension S that is target of a strong character on $\mathbb{Z}_n$?

Previous results: strong characters do exist

- **Theorem (2011):** Let n be a positive integer. Every finite ring R with $n \in R^{\times}$ has a unital extension S that is target of a strong character on $\mathbb{Z}_n$.

- **Proof:** We define $S \ := \ R[\mathbb{Z}_n]/I$, where:

$$I \ := \ {}_{R[\mathbb{Z}_n]}\Big\langle \sum_{j \in \mathbb{Z}_n i} j \mid i \in \mathbb{Z}_n,\ i \neq 0 \Big\rangle.$$

Then for $\chi : \mathbb{Z}_n \longrightarrow S,\ i \mapsto i$, most parts of the claim are easily checked. The (crucial) fact that $S \geq R$ and particularly $S \neq \{0\}$ follows from the fact that $n \in R^{\times}$ and I has trivial intersection with $R\chi(0)$. $\square$

Technical preparation

- For all what follows, let R be a ring that is target of the regular character χ on $\mathbb{Z}_n$ where $n \in R^\times$.

- For $k \in \mathbb{Z}_n$ consider the word $q^{(k)} \in R^n$ defined by

$$(q^{(k)})_i \ := \ \frac{1}{n}\,[1 - \chi(i-k)]\,.$$

- The only zero of this word is at $i = k$. For the Fourier transform of $q^{(k)}$ we have

$$(\widehat{q^{(k)}})_i \ = \begin{cases} 1 & : \quad i = 0, \\ -\chi(-k) & : \quad i = 1, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

Technical preparation (cnt'd)

- **Lemma:** For a subset T of $\mathbb{Z}_n$ with $|T| \leq \delta$, the word

$$p := \prod_{k \in T} q^{(k)}$$

has the following properties:

(i) $p_i = 0$ for all $i \in T$.
(ii) $\widehat{p}_0 = 1$.
(iii) $\widehat{p}_i = 0$ for all $i > \delta$.

- **Proof:** Property **(i)** directly follows from the construction of p. In polynomial language, the word $\widehat{q^{(k)}}$ is given by $1 - \chi(-k)x$, and the convolution becomes ordinary polynomial multiplication. This immediately yields **(ii)** and **(iii)**. □

Result: BCH bound for ring codes

- **Theorem (2011):** Let $c \in R^n$ be a word with $w_H(c) \leq \delta$. If $\widehat{c}$ has δ consecutive zeros, then $c = 0$.

- **Proof** (cf. Wicker's textbook): We apply the foregoing lemma to $T = \mathrm{supp}(c)$ and obtain from **(i)** the equality $p \cdot c = 0$, which implies $\widehat{p} \star \widehat{c} = 0$ by the convolution theorem. This means that $\sum_{j=0}^{n-1} \widehat{p}_j \widehat{c}_{i-j} = 0$ for all $i \in \mathbb{Z}_n$. Using **(ii)** and **(iii)** of the same lemma, we rewrite this as a recursion formula:

$$\widehat{c}_i = -\sum_{j=1}^{\delta} \widehat{p}_j \widehat{c}_{i-j} \quad \text{for all } i \in \mathbb{Z}_n.$$

 If $\widehat{c}$ has δ consecutive zeros, then this results in $\widehat{c} = 0$ and consequently in $c = 0$. □

Possible goals for future endeavor

- Instead of $\mathbb{Z}_n$ assume a possibly non-abelian group G to be underlying.
- Design a Fourier transform $\hat{c}$ for words $c \in R^G$ where R is some finite ring.
- Develop a relationship between the properties of a word in $c \in R^G$ and the properties of its Fourier transform $\hat{c} \in S^?$ where S is a suitable ring extension of R.
- Prove BCH-bound like theorems for codes over finite fields or rings, when G is underlying.
- This is ongoing work, but our success so far encourages continuation.