

Locally recoverable codes over Galois rings

Giulia Cavicchioni

joint work with Alessio Meneghetti (UniTn) and Eleonora Guerrini (LIRMM, UM)

University of Trento, Department of Mathematics

YRAC2023, 26th July 2023

- 1 Linear codes over finite chain rings
- 2 Introduction to locally recoverable codes
- 3 Locally recoverable codes over finite chain rings
- 4 Open problems

Linear codes over finite chain rings

Basic definitions

Let R be a finite ring. Let

- R^* be the group of unity of R ;
- $S \subseteq R^*$. We say S is *subtractive* if for all $a, b \in S$ we have $a - b \in R^*$.

We are interested in codes over finite rings.

Definition: Ring-linear code

Let R be a finite commutative ring.

- A *linear code* \mathcal{C} of length n in the alphabet R is a submodule of R^n ;
- A *free code* \mathcal{C} is a free submodule of R^n .

Ring-Linear codes: Parameters 1

	Classical codes	Ring-linear codes
Alphabet	Finite field \mathbb{F}_q	Finite chain ring R
Ambient space	Finite dim.vector space \mathbb{F}_q^n	Free module R^n
Linear code \mathcal{C}	k -dim. subspace of \mathbb{F}_q^n	submodule of R^n
Code length	n	n
Code minimum distance	d	d
Code dimension	k	??

Ring-Linear codes: Parameters 2

Let C be an R -linear code.

The rank is one of the analogues of the dimension for classical codes:

Rank

The *rank* of C is the minimum K such that there exists a monomorphism

$$\phi: C \rightarrow R^K \text{ as } R\text{-modules .}$$

Introduction to locally recoverable codes

LRC: definition and motivation

The goal of local recovery is to retrieve data using a fraction of the codeword's information. Let $C \subseteq R^n$ be a code and $c = (c_1, \dots, c_n) \in C$.

Locally Recoverable Codes (LRC)

- The i th coordinate has *locality* r if there exists $S_i \subseteq \{1, \dots, n\} \setminus i$, $|S_i| \leq r$, and a map $\Phi_i: R^{S_i} \rightarrow R$ such that for any $c \in C$

$$c_i = \Phi_i(c|_{S_i}).$$

- S_i is a *recovering set* for i .
- C is a *locally recoverable code with locality* r if each coordinate has locality r .

If c is error-free except for an erasure at i , we can retrieve c by only examining the coordinates in S_i .

Locally recoverable codes over finite fields

The research mainly aimed at:


- 1 Establishing bounds on the minimum distance¹

Bound on the minimum distance for an LRC code

Let C be an (n, k) -code with locality r over \mathbb{F}_q . Then

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

A code that achieves the bound is called *optimal*.


¹Parikshit Gopalan et al. (2012). “On the locality of codeword symbols”. In: *IEEE Transactions on Information theory* 58.11, pp. 6925–6934. 

Locally recoverable codes over finite fields

- ② Developing techniques for constructing optimal LRC codes:
 - ▶ Using Vandermonde matrices;²
 - ▶ Using elliptic curves;³
 - ▶ Using particular types of polynomials over \mathbb{F}_q .⁴

²Chaoping Xing and Chen Yuan (2018). “Construction of optimal locally recoverable codes and connection with hypergraph”. In: *arXiv preprint arXiv:1811.09142*.

³Xudong Li, Liming Ma, and Chaoping Xing (2018). “Optimal locally repairable codes via elliptic curves”. In: *IEEE Transactions on Information Theory* 65.1, pp. 108–117.

⁴Itzhak Tamo and Alexander Barg (2014). “A family of optimal locally recoverable codes”. In: *IEEE Transactions on Information Theory* 60.8, pp. 4661–4676. 

Locally recoverable codes over finite chain rings

LRC bound for Ring-linear codes

Let R be a finite chain ring.

Bound on the minimum distance for an R -linear LRC code

Let C be an R -linear code of length n , rank K and locality r . Then

$$d \leq n - K - \left\lceil \frac{K}{r} \right\rceil + 2.$$

A Tamo-Barg-like construction method allows to gain optimal linear codes over finite chain rings.

Polynomial over rings

Polynomial reconstruction is not well-defined for rings...

Well-conditioned sets

A set $\{a_1, \dots, a_n\} \subseteq R$ is *well-conditioned* in R if:

- 1 either $\{a_1, \dots, a_n\}$ is subtractive in R^* ;
- 2 or $\{a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n\}$ is subtractive in R^* and a_i is a zero-divisor or $a_i = 0$.

...But it is well-defined over well-conditioned sets:

Polynomial interpolation over rings

Let $\{a_1, \dots, a_n\}$ be a well-conditioned subset of R and let $\{y_1, \dots, y_n\}$ be a subset of R . There exists a unique $f \in R[x]$ of degree at most $n - 1$ such that $f(a_i) = y_i$ for all $1 \leq i \leq n$.

Tamo-Barg-Like construction

Good polynomials play a fundamental role in the construction.

Good polynomials

Let $g \in R[x]$ and $l \in \mathbb{N}^+$. We say that g is (r, l) -good if:

- Its degree is $r + 1$;
- Its leading coefficient is a unit;
- There exist A_1, \dots, A_l distinct subsets of R such that
 - 1 g is constant on A_i ;
 - 2 $|A_i| = r + 1$;
 - 3 $A_i \cap A_j = \emptyset$ for any $i \neq j$.

Tamo-Barg-Like codes

- Let $A = \bigcup_{i=1}^l A_i$ be a well-conditioned set in R , $|A_i| = r + 1$ for all i ;
- $g(x) \in R[x]$ be an (r, l) -good polynomial on the blocks of the partition of A ;
- For $t \leq l$, $n = (r + 1)l$ and $K = rt$;
- Let $a = (a_{i,j}, 0 \leq i \leq r - 1, 0 \leq j \leq t - 1) \in R^K$ be a message vector;
- The *encoding polynomial* of a is $f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{i,j} g(x)^j x^i$;
- We define the code as

$$C = \left\{ (f_a(\alpha), \alpha \in A) \mid a \in R^K \right\}.$$

Code parameters

C is free (n, K, r) -code which is optimal.

Good polynomials over Galois ring

Good polynomials over rings which are not fields exist.

Let $R = GR(p^s, m)$ be a Galois Ring.

Costruction of a maximal well-conditioned set

Let G be the cyclic subgroup of R^* whose elements are the roots of the polynomial $x^{p^m-1} - 1 \in R[x]$. Then

- G has order $p^m - 1$;
- G is the unique maximal cyclic subgroup of R^* of order coprime with p ;
- G is subtractive subset of maximum size in R^* .

Good polynomials over Galois Ring

Let H be a subgroup of the cyclic group G . The cosets of H induce a partition of G .

Good polynomial over a well-conditioned set

The annihilator polynomial of the subgroup

$$g(x) = \prod_{h \in H} (x - h) = x^{|H|} - 1,$$

is constant on the cosets of H .

g is a good polynomial for the set G .

Open problems

Removing constraints on the code length

The main problem affecting the previous constructions is the constraint on the code length.

Removing the constraints on code length

- Let $A = \bigcup_{i=1}^l A_i$ be a **well-conditioned** set in R , $|A_i| = r + 1$ for all i ;
- $g(x) \in R[x]$ be an (r, l) -good polynomial on the blocks of the partition of A ;
- For $t \leq l$, $n = (r + 1)l$ and $K = rt$;
- Let $a = (a_{i,j}, 0 \leq i \leq r - 1, 0 \leq j \leq t - 1) \in R^K$ be a message vector;
- The *encoding polynomial* of a is $f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{i,j} g(x)^j x^i$;
- We define the code as

$$C = \left\{ (f_a(\alpha), \alpha \in A) \mid a \in R^K \right\}.$$

Code parameters

C is free (n, K, r) -code which is optimal.

Removing constraints on the code length

The main problem affecting the previous constructions is the constraint on the code length.

Removing constraints on the code length

The main problem affecting the previous constructions is the constraint on the code length.

- 1 The set $A = \bigcup_{i=1}^r A_i$ must be well conditioned;
- 2 $r + 1$ has to divide n .

Removing constraints on the code length

The main problem affecting the previous constructions is the constraint on the code length.


- 1 The set $A = \bigcup_{i=1}^r A_i$ must be well conditioned;
- 2 $r + 1$ has to divide n .

Here an overview on three generalizations:

	Gen. 1	Gen. 2	Gen. 3
Constraint removed	$(r + 1) n$	$(r + 1) n$	A subtractive
Maximum length	$p^m - 1$	$p^m - 1$	$ R^* = p^{s-1}(p^m - 1)$
Block length	$ A_i = s < r + 1$	$r + \rho - 1, \rho \geq 3$	$r + 1$
Code minimum distance	$d \geq n - K - \frac{K}{r} + 1$	$d = n - K + 1 - (\frac{K}{r} - 1)(\rho - 1)$	$d = n - p^{s-1}(K + \frac{K}{r} - 2)$
Optimality	Almost optimal	Optimal	?

Future works

- 1 The main difficulty is to overcome the restrictions on the code parameters.
 - ▶ Find optimal codes with $n \geq p^m - 1$;
 - ▶ Find optimal codes with $n \geq |R|$.
- 2 Construct good polynomials: analogously to the classical case⁵, try to find a wider class of good polynomials using Galois theory.

⁵Giacomo Micheli (2019). “Constructions of locally recoverable codes which are optimal”. In: *IEEE transactions on information theory* 66.1, pp. 167–175. 

Thank you for your attention!