Locally recoverable codes over finite chain rings

Giulia Cavicchioni

University of Trento, Department of Mathematics

Joint work with Eleonora Guerrini (LIRMM) and Alessio Meneghetti (UniTn)

WCC 2024, June 20th

Locally recoverable codes

$$c = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} \\ \hline \end{array}$$

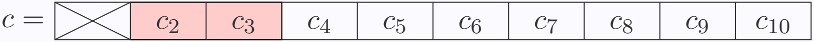
IDEA: It is possible to recover an erased coordinate by only looking at a subset of the coordinates

Locally recoverable codes

$$c = \boxed{\times} \; c_2 \; c_3 \; c_4 \; c_5 \; c_6 \; c_7 \; c_8 \; c_9 \; c_{10}$$

IDEA: It is possible to recover an erased coordinate by only looking at a subset of the coordinates

Locally recoverable codes



IDEA: It is possible to recover an erased coordinate by only looking at a subset of the coordinates

Linear codes over finite chain rings

Basic definitions

Let R be a finite ring. Let

- R^* be the group of units 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 rings.

Definition: Ring-linear code

Let R be a finite chain 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 linear codes	Ring-linear codes
Alphabet	Finite field $\mathbb{F}_q$	Finite chain ring R
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

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

Rank

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

$$\phi \colon C \to R^K \quad \text{as } R\text{-modules} \; .$$

Introduction to locally recoverable codes

LRC: definition

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

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

- 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.

LRC bound

The research mainly aimed at:

1. Establishing bounds on the minimum distance[1]

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 LRC*.

[1] Parikshit 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]

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

[3] Xudong 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.

[4] Itzhak 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 LRC over finite chain rings.[5]

[5] Giulia Cavicchioni, Eleonora Guerrini, and Alessio Meneghetti (2023). "A class of locally recoverable codes over finite chain rings". preprint: https://arxiv.org/abs/2401.05286.

Polynomials over rings

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

Well-conditioned sets

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

1. either $\{a_1, \ldots, a_n\}$ is subtractive in R^*;
2. or $\{a_1, \ldots a_{i-1}, a_{i+1}, \ldots, a_n\}$ 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 $\{a_1, \ldots, a_n\}$ be a well-conditioned subset of R and let $\{y_1, \ldots, y_n\}$ 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 a free (n, K, r)-code which is optimal LRC.

Open problems

Removing constraints on the code length

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

Removing constraints on the 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 construction is the constraint on the code length.

Removing constraints on the code length

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

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

Removing constraints on the code length

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

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

Here an overview on three generalizations with $R = GR(p^s, m)$:

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

Bound on the maximum length of an LRC code over R

For a finite chain ring R let $\mathbb{K} = R/M$ where M is the maximal ideal of R. Let C be an R-linear code and let $\bar{C}$ be its projection over $\mathbb{K}$.

Parameters of $\bar{C}$

	C	$\bar{C}$
Alphabet	free over R	Linear over $\mathbb{K}$
Length	n	n
Rank / Dimension	K	K
Locality	r	$\bar{r} \leq r$ s.t. $\lceil \frac{K}{\bar{r}} \rceil = \lceil \frac{K}{r} \rceil$
Minimum distance	$d = n - K - \lceil \frac{K}{r} \rceil + 2$	$d = n - K - \lceil \frac{K}{r} \rceil + 2$

Bound on the maximum length of an LRC code over R

The problem of determining the maximum possible length of an optimal LRC over a ring is closely related to the same problem over fields[6].

Maximum lenght of an optimal LRC

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

- if $d = 2, 3, 4$ optimal LRCs with unbounded exist;
- If $d \geq 5$, one cannot have unbounded length optimal LRCs;
- In particular, if $d = 5$ then $n \leq \mathcal{O}(q^2)$.

[6] Venkatesan Guruswami, Chaoping Xing, and Chen Yuan (2019). "How Long Can Optimal Locally Repairable Codes Be?" In: *IEEE Transactions on Information Theory* 65.6, pp. 3662–3670. DOI: 10.1109/TIT.2019.2891765.

Existence of good polynomials

Over finite fields, various techniques for designing good polynomials are known.[7]

Good polynomials over well-conditioned sets of a ring exist.

A class of good polynomials

A class of good polynomial over R can be constructed from class of good polynomials over $\mathbb{K}$ using Hensel lifting.

? Are there other interesting classes of good polynomials?

[7] Giacomo 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!