Sequential Locally Recoverable Codes for Multiple Erasures from Finite Geometry

Marc Newman

Institute of Computer Science, University of St. Gallen

July 14th, 2022

Joint work with Akram Baghban[1,2], Anna-Lena Horlemann[2], and Mehdi Ghiyasvand [1]

[1]Bu-Ali Sina University
[2]University of St. Gallen

Overview

1. Background
    - Locally Repairable Codes (LRCs)
    - Parallel Locally Repairable Codes (PLRCs)
    - Sequential Locally Repairable Codes (SLRCs)
2. Constructions
    - Product Construction
    - Products of SLRCs
    - General Bounds on Recovery
    - Results
3. Resolvable Configuration
    - Definition
    - Examples
4. Iteration Counting
    - Overview
    - Example
    - Results and Conjectures
5. Conclusion
6. References

Background

Locally Repairable Codes (LRCs)

Definition

For $\mathcal{C}$ a $[n,k]$-linear code over $\mathbb{F}_q$ and $i \in [n]$, a subset $R_i \subseteq [n] \setminus \{i\}$ is called an **$(r, \mathcal{C})$-recovery set** of i if:

- $|R_i| \leq r$,
- for all $j \in R_i$ there exist $a_j \in \mathbb{F}_q$ such that for all $(x_1, \ldots, x_n) \in \mathcal{C}$,

$$x_i = \sum_{j \in R_i} a_j \cdot x_j.$$

We say a code $\mathcal{C}$ has **locality** r if every symbol of $\mathcal{C}$ has an $(r, \mathcal{C})$-recovery set.

A code with some locality r (preferably with $r < k$) is called a **locally repairable code (LRC)**.

Background

Parallel Locally Repairable Codes (PLRCs)

Definition

For $i \in [n]$, the number of $(r, \mathcal{C})$-recovery sets of i, denoted $a(i)$, is called the **repair alternativity**.

The **repair alternativity** of $\mathcal{C}$ is defined to be $a = \min \{a(i)\}_{i \in [n]}$.

Definition

An $[n, k]$ linear code $\mathcal{C}$ is said to be an **$(\boldsymbol{n}, \boldsymbol{k}, \boldsymbol{r}, \boldsymbol{t})$-parallel locally repairable code (PLRC)** if for each $E \subseteq [n]$ of size $|E| \leq t$, each $i \in E$ has a $(r, \mathcal{C})$-recovery set $R_i \in [n] \setminus E$.

Background

Sequential Locally Repairable Codes (SLRCs)

Definition

For an ordered set $E = \{i_1, \ldots, i_t\} \subseteq [n]$, $\mathcal{C}$ is said to be **(E, r)-recoverable** if each $i_j \in E$ has an $(r, \mathcal{C})$-recovery set $R_{i_j} \subseteq [n] \setminus \{i_j, i_{j+1}, \ldots, i_t\}$.

Definition

An $[n, k]$ linear code $\mathcal{C}$ is said to be an **(n, k, r, t)-sequential locally repairable code (SLRC)** if for each $E \subseteq [n]$ of size $|E| \leq t$, $\mathcal{C}$ is an (E, r)-recoverable code.

Proposition ([5])

$\mathcal{C}$ is an (n, k, r, t)-SLRC if and only if for any nonempty $E \subseteq [n]$ of size $|E| \leq t$, there exists an $i \in E$ such that i has a recovery set $R_i \subseteq [n] \setminus E$.

Constructions

Product Construction

Definition

Let $\mathcal{A}$ and $\mathcal{B}$ (respectively) be $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ linear codes with generator matrices G_A and G_B. Then the product code $\mathcal{A} \times \mathcal{B}$ is the $[n_1 \cdot n_2, k_1 \cdot k_2, d_1 \cdot d_2]$ linear code with generator matrix $G_A \otimes G_B$.

Constructions

Products of SLRCs

Theorem

For all $i \in [\ell]$, let $\mathcal{C}_i$ be an $[n_i, k_i, d_i]$ code with locality r_i and let

$$n = \prod_{i=1}^{\ell} n_i, \qquad k = \prod_{i=1}^{\ell} k_i, \qquad d = \prod_{i=1}^{\ell} d_i, \qquad r = \max\{r_i\}_{1 \leq i \leq \ell}$$

Then $\mathcal{C}_1 \times \cdots \times \mathcal{C}_\ell$ is an $[n, k, d]$-SLRC with locality r.

Corollary

The product of ℓ codes, each with erasure correcting capacity t_i, will have erasure correcting capacity

$$t = \left(\prod_{i=1}^{\ell} t_i + 1 \right) - 1.$$

Constructions

General Bounds on Recovery

For ℓ products of an $[n, k]$-MDS code, we get the following bounds on the number of recoverable erasures x:

- If $x \leq \ell(n-k)$, we can perform full parallel recovery.
- If $\ell(n-k) < x < (n-k+1)^{\ell}$, we can fully sequentially recover.
- If $(n-k+1)^{\ell} \leq x \leq n^{\ell} - k^{\ell}$, we can possibly recover depending on the erasure pattern.
- If $n^{\ell} - k^{\ell} < x$, we definitely can't fully recover.

In the following, let $\mathcal{P}_q$ be the $[q+1, 2, q]_q$ MDS code, $\mathcal{D}_{q,n}$ be the $[n, n-1, 2]_q$ MDS code, and $\mathcal{R}_{q,n,k}$ be the $[n, k, n-k+1]_q$ Reed-Solomon code (which is MDS).

Constructions

Results for $q = 3, k \leq 10$

q	k	r	ℓ	Code	t	Construction
3	4	2	2	$[16, 4, 9]$	8	$\mathcal{P}_3 \times \mathcal{P}_3$
				$[12, 4, 6]$	5	$\mathcal{P}_3 \times \mathcal{D}_{3,3}$
				$[9, 4, 4]$	3	$\mathcal{D}_{3,3} \times \mathcal{D}_{3,3}$
3	6	3	2	$[16, 6, 6]$	5	$\mathcal{P}_3 \times \mathcal{D}_{3,4}$
				$[12, 6, 4]$	3	$\mathcal{D}_{3,4} \times \mathcal{D}_{3,4}$
3	8	2	3	$[64, 8, 27]$	26	$\mathcal{P}_3 \times \mathcal{P}_3 \times \mathcal{P}_3$
				$[48, 8, 18]$	17	$\mathcal{P}_3 \times \mathcal{P}_3 \times \mathcal{D}_{3,3}$
				$[36, 8, 12]$	11	$\mathcal{P}_3 \times \mathcal{D}_{3,3} \times \mathcal{D}_{3,3}$
				$[27, 8, 8]$	7	$\mathcal{D}_{3,3} \times \mathcal{D}_{3,3} \times \mathcal{D}_{3,3}$
3	8	4	2	$[20, 8, 6]$	5	$\mathcal{P}_3 \times \mathcal{D}_{3,5}$
				$[15, 8, 4]$	3	$\mathcal{D}_{3,3} \times \mathcal{D}_{3,5}$
3	9	3	2	$[16, 9, 4]$	3	$\mathcal{D}_{3,4} \times \mathcal{D}_{3,4}$
3	10	5	2	$[24, 10, 6]$	5	$\mathcal{P}_3 \times \mathcal{D}_{3,6}$
				$[18, 10, 4]$	3	$\mathcal{D}_{3,3} \times \mathcal{D}_{3,6}$

Additionally, constructions for $k = 8, r = 3, \ell = 2$ exist using BCH codes.

Constructions

Results for $q = 5, k \in \{4, 6\}$

q	k	r	ℓ	Code	t	Construction
5	4	2	2	$[36, 4, 25]$	24	$\mathcal{P}_5 \times \mathcal{P}_5$
				$[30, 4, 20]$	19	$\mathcal{P}_5 \times \mathcal{R}_{5,5,2}$
				$[25, 4, 16]$	15	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,5,2}$
				$[24, 4, 15]$	14	$\mathcal{P}_5 \times \mathcal{R}_{5,4,2}$
				$[20, 4, 12]$	11	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,4,2}$
				$[18, 4, 10]$	9	$\mathcal{P}_5 \times \mathcal{D}_{5,3}$
				$[16, 4, 9]$	8	$\mathcal{R}_{5,4,2} \times \mathcal{R}_{5,4,2}$
				$[15, 4, 8]$	7	$\mathcal{R}_{5,5,2} \times \mathcal{D}_{5,3}$
				$[12, 4, 6]$	5	$\mathcal{R}_{5,4,2} \times \mathcal{D}_{5,3}$
				$[9, 4, 4]$	3	$\mathcal{D}_{5,3} \times \mathcal{D}_{5,3}$
5	6	3	2	$[30, 6, 15]$	14	$\mathcal{P}_5 \times \mathcal{R}_{5,5,3}$
				$[25, 6, 12]$	11	$\mathcal{R}_{5,5,3} \times \mathcal{R}_{5,5,2}$
				$[24, 6, 10]$	9	$\mathcal{P}_5 \times \mathcal{D}_{5,4}$
				$[20, 6, 9]$	8	$\mathcal{R}_{5,5,3} \times \mathcal{R}_{5,4,2}$
				$[15, 6, 6]$	5	$\mathcal{R}_{5,5,3} \times \mathcal{D}_{5,3}$
				$[12, 6, 4]$	3	$\mathcal{D}_{5,4} \times \mathcal{D}_{5,3}$

Constructions

Results for $q = 5, k = 8$

q	k	r	ℓ	Code	t	Construction
5	8	4	2	$[30, 8, 10]$	9	$\mathcal{P}_5 \times \mathcal{D}_{5,5}$
				$[25, 8, 8]$	7	$\mathcal{R}_{5,5,2} \times \mathcal{D}_{5,5}$
				$[20, 8, 6]$	5	$\mathcal{R}_{5,4,2} \times \mathcal{D}_{5,5}$
				$[15, 8, 4]$	3	$\mathcal{D}_{5,5} \times \mathcal{D}_{5,3}$
5	8	2	3	$[100, 8, 48]$	47	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,5,2} \times \mathcal{R}_{5,4,2}$
				$[96, 8, 45]$	44	$\mathcal{P}_{5,5,2} \times \mathcal{R}_{5,4,2} \times \mathcal{P}_5$
				$[90, 8, 40]$	39	$\mathcal{R}_{5,5,2} \times \mathcal{P}_5 \times \mathcal{D}_{5,3}$
				$[80, 8, 36]$	35	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,4,2} \times \mathcal{R}_{5,4,2}$
				$[75, 8, 32]$	31	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,5,2} \times \mathcal{D}_{5,3}$
				$[72, 8, 30]$	29	$\mathcal{R}_{5,4,2} \times \mathcal{P}_5 \times \mathcal{D}_{5,3}$
				$[64, 8, 27]$	26	$\mathcal{R}_{5,4,2} \times \mathcal{R}_{5,4,2} \times \mathcal{R}_{5,4,2}$
				$[60, 8, 24]$	23	$\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,4,2} \times \mathcal{D}_{5,3}$
				$[54, 8, 20]$	19	$\mathcal{P}_5 \times \mathcal{D}_{5,3} \times \mathcal{D}_{5,3}$
				$[48, 8, 18]$	17	$\mathcal{R}_{5,4,2} \times \mathcal{R}_{5,4,2} \times \mathcal{D}_{5,3}$
				$[45, 8, 16]$	15	$\mathcal{R}_{5,5,2} \times \mathcal{D}_{5,3} \times \mathcal{D}_{5,3}$
				$[36, 8, 12]$	11	$\mathcal{R}_{5,4,2} \times \mathcal{D}_{5,3} \times \mathcal{D}_{5,3}$
				$[27, 8, 8]$	7	$\mathcal{D}_{5,3} \times \mathcal{D}_{5,3} \times \mathcal{D}_{5,3}$

Constructions

Results for $q = 5, k \in \{9, 10\}$

q	k	r	ℓ	Code	t	Construction
5	9	3	2	$[25, 4, 9]$	8	$\mathcal{R}_{5,5,3} \times \mathcal{R}_{5,5,3}$
				$[20, 4, 6]$	5	$\mathcal{R}_{5,5,3} \times \mathcal{D}_{5,4}$
				$[16, 4, 4]$	3	$\mathcal{D}_{5,4} \times \mathcal{D}_{5,4}$
5	10	5	2	$[36, 6, 10]$	9	$\mathcal{P}_5 \times \mathcal{D}_{5,6}$
				$[30, 6, 8]$	7	$\mathcal{R}_{5,5,2} \times \mathcal{D}_{5,6}$
				$[24, 6, 6]$	5	$\mathcal{R}_{5,4,2} \times \mathcal{D}_{5,6}$
				$[18, 6, 4]$	3	$\mathcal{D}_{5,6} \times \mathcal{D}_{5,3}$

Using BCH codes, we also get the additional parameters:

k	r	ℓ
6	2	2
8	3	2
9	2	2
10	3	2

Resolvable Configurations

Definition

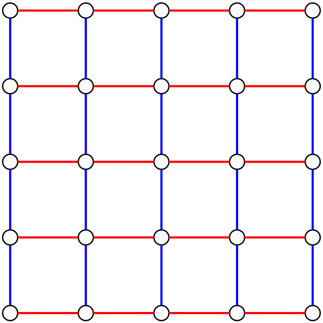
Let P be a set of **points** and $\mathcal{B}$ be a set of **blocks** i.e. subsets of P such that:

- $|P| = v$,
- $|\mathcal{B}| = b$,
- each point is contained in r blocks,
- each block contains k points,
- the blocks can be partitioned into r **parallel classes** where the blocks of each class partition P.

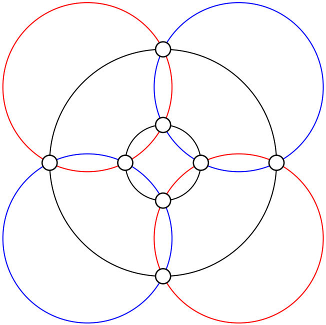
Then $(P, \mathcal{B})$ is said to be a **(v_r, b_k)-resolvable configuration**.

Resolvable Configurations

Examples



(a) A $(25_2, 10_5)$-resolvable configuration



(b) A $(8_3, 6_4)$-resolvable configuration (the Miquel configuration)

Iteration Counting

Overview

Let $\mathcal{C}$ be an SLRC from a resolvable configuration with ℓ parallel classes, consistent block length b, and locality r,

Given a parallel class, say we can recover all the erased points on each line provided that the line has r unerased points. Given some set of unerased points $\mathcal{S}$ such that the full codeword can be recovered, let $I(\mathcal{C} \mid \mathcal{S})$ count (with repetition) the minimum number of necessary parallel classes of $\mathcal{C}$ used sequentially to fully recover the full codeword.

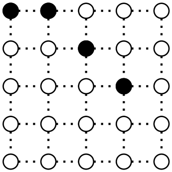
Then let $I(\mathcal{C})$ be the maximum of these over all such sets $\mathcal{S}$.

Since a product of ℓ $[n, k, d]$ MDS codes can be represented as an ℓ-dimensional $n \times \cdots \times n$ grid of points where each line can be fully recovered given $r = k$ unerased vertices, we can also consider the number $I(n, \ell, r)$ specific to this construction.

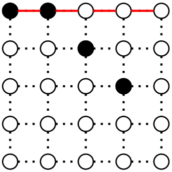
Iteration Counting

Example

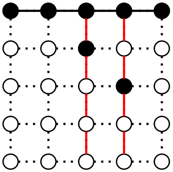
For a square with $n = 5$, $\ell = 2$, and $r = 2$ (e.g. $\mathcal{R}_{5,5,2} \times \mathcal{R}_{5,5,2}$). Black vertices represent un-erased symbols, white represent erased symbols. Red lines indicate the lines being recovered.



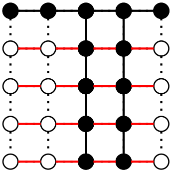
(a) Initial pattern



(b) First iteration



(c) Second iteration



(d) Third iteration

i.e. here $I(\mathcal{C} \mid \mathcal{S}) = 3$ and in fact $I(5, 2, 2) = 3$ so this is a worst-case scenario.

Iteration Counting

Results and Conjectures

- $I(n, 1, r) = 1$ for all n and all r (just a single line).
- $I(n, 2, r) \leq 2r - 1$ for all n and all r.
- $I(3, 3, 2) = 7$ (by brute force checking).
- $I(4, 3, 2) = 10$ (by brute force checking).
- $I(n, 3, 2) = 10$ for all $n \geq 4$ (conjecture).
- $I(3, 4, 2) \geq 14$ (by pathological example).
- $\lim_{n \to \infty} I(n, \ell, r) = \infty$ if $\ell \geq 4$ or if $r \geq 3$ and $\ell \geq 3$ (by specific placement of erasures; conjecture).

Future Work

- Consider other families of codes in the construction.
- Algorithm for finding optimal sequences for recovery.
- Work out more numbers and bounds regarding the iteration counting.
- Consider iteration counting with regards to other resolvable configurations.
- Consider iteration counting when only one vertex can be recovered per r unerased vertices accessed (as opposed to the whole line).

Thank you for your attention!

References I

[1] S. B. Balaji, K. P. Prasanth, and P. Vijay Kumar. “Binary codes with locality for multiple erasures having short block length”. In: *2016 IEEE International Symposium on Information Theory (ISIT)*. 2016, pp. 655–659.

[2] Gábor Gévay. “Resolvable configurations”. In: *Discrete Applied Mathematics* 266 (2019), pp. 319–330.

[3] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*. Vol. 16. Elsevier, 1977.

[4] Lluis Pamies-Juarez, Henk DL Hollmann, and Frédérique Oggier. “Locally repairable codes with multiple repair alternatives”. In: *2013 IEEE international symposium on information theory*. IEEE. 2013, pp. 892–896.

[5] Wentu Song, Kai Cai, Chau Yuen, Kui Cai, and Guangyue Han. “On Sequential Locally Repairable Codes”. In: *IEEE Transactions on Information Theory* 64.5 (2018), pp. 3513–3527.

[6] Yi-Sheng Su. “Design of membership matrices for (r, t)-availability in distributed storage”. In: *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2016, pp. 998–1002.