A Tight Rate Bound and Matching Construction for Locally Recoverable Codes with Sequential Recovery

S. B. Balaji, Ganesh R. Kini and P. Vijay Kumar[1]

ECE Dept., Indian Institute of Science, Bangalore

Information Theory and Applications Workshop
Catamaran Resort, San Diego, February 13, 2017

[1] P. Vijay Kumar is a Professor in ECE at IISc and an Adjunct Research Professor at USC.

Thanks to Alon and the other organizers for the invite...

Parameters of Interest

All codes are linear codes over $\mathbb{F}_q$.

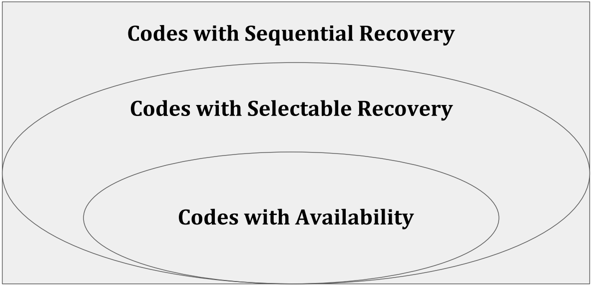
q	field size
n	Block length
k	dimension
R	$= (k/n) =$ rate
$d_{\min}$	minimum distance

t	maximum number of erasures from which local recovery is desired
r	maximum number of code symbols contacted for recovery of a single erased symbol

Various Local Approaches to Multiple-Erasure Recovery

Approach	Explanation
Availability	Each code symbol is protected by a set of parity checks that includes a set of t orthogonal parity checks, each of weight $\leq (r+1)$
Sequential Recovery	Given a set of $\leq t$ erased code symbols, there exists a parity check for at least one code symbol, of weight $\leq (r+1)$ which does not include any of the other code symbols
Selectable Recovery	For any given set of $(t-1)$ other erasures, each code symbol is protected by a parity check of weight $\leq (r+1)$, that does not include any of these other code symbols
Cooperative Recovery	Given a set of t erasures, there exists a set of r code symbols using which one can recover from these t erasures

Codes with Locality For Multiple Erasures



Sequential Recovery Results

- A tight upper bound on rate R for any $(r \geq 3,\ t \geq 2)$
- Matching binary-code construction

Codes with Locality for Sequential Recovery

Definition

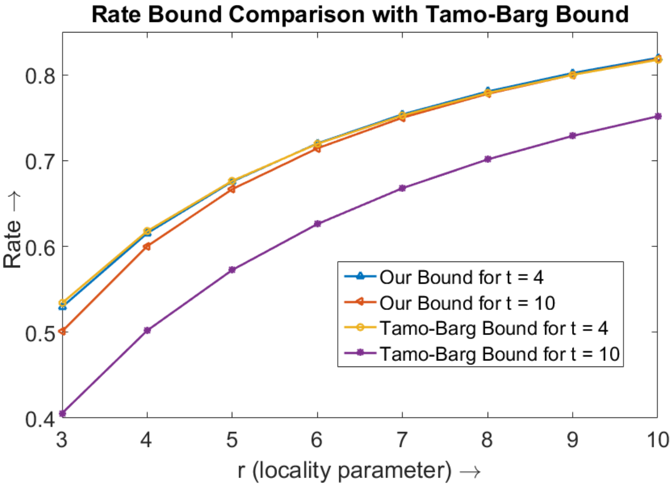
An $[n, k]$ code over $\mathbb{F}_q$ is a

code with sequential recovery from t erasures having locality r

if for any set of $s \leq t$ erased symbols, $\{c_{\sigma_1}, ..., c_{\sigma_s}\}$, there exists a codeword $\underline{h}$ in the dual code, of Hamming weight $\leq r + 1$, such that $\text{supp}(\underline{h}) \cap \{\sigma_1, ..., \sigma_s\} = 1$.

We denote the above defined codes as $(n, k, r, t)_{seq}$ codes.

Motivation:
Improved Rate (in comparison with availability)



The (Tight) Upper Bound on Rate

Theorem

Rate Bound: *Let $\mathcal{C}$ be an $(n, k, r, t)_{seq}$ code over a field $\mathbb{F}_q$. Let $r \geq 3$. Then*

$$\frac{k}{n} \leq \frac{r^{\frac{t}{2}}}{r^{\frac{t}{2}} + 2\sum_{i=0}^{\frac{t}{2}-1} r^i} \quad \textit{for } t \textit{ an even integer,} \tag{1}$$

$$\frac{k}{n} \leq \frac{r^s}{r^s + 2\sum_{i=1}^{s-1} r^i + 1} \quad \textit{for } t \textit{ an odd integer,} \tag{2}$$

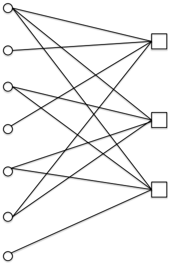
where $s = \frac{t+1}{2}$.

Bound for $t = 2, 3, 4, 5, 6, 7$

t	Bound	t	Bound
2	$\frac{r}{r+2}$	3	$\frac{r^2}{r^2+2r+1}$
4	$\frac{r^2}{r^2+2r+2}$	5	$\frac{r^3}{r^3+2r^2+2r+1}$
6	$\frac{r^3}{r^3+2r^2+2r+2}$	7	$\frac{r^4}{r^4+2r^3+2r^2+2r+1}$

Rawat et. al. Construction for Codes with Sequential Recovery

1. r+1-regular bipartite graph, girth $\geq t+1$ [a]
2. edge are code symbols, node are parity checks,
3. Rate is $\frac{r-1}{r+1} + \frac{1}{n}$.
4. Rate meets our rate bound when a Moore graph of degree $r+1$ and girth $t+1$ exists.
5. Such Moore graphs are shown to not exist for $t \notin \{2,3,4,5,7,11\}$ for any $r \geq 2$.
6. Thus the construction is not rate-optimal in most cases.



[a] A. Rawat, A. Mazumdar, and S. Vishwanath, "On cooperative local repair in distributed storage, " in Information Sciences and Systems (CISS), 2014 48th Annual Conference on, 2014, pp. 1?5.

Conjecture on Rate

The following conjecture on the rate of an $(n, k, r, t)_{seq}$ code was given by Song[2] et al.

$$\frac{k}{n} \leq \frac{1}{1+\sum_{i=1}^{m} \frac{a_i}{r^i}},$$
$$a_i \geq 0, \quad a_i \in \mathbb{Z}, \quad \sum_{i=1}^{m} a_i = t, \quad m = \lceil log_r(k) \rceil.$$

- Our rate bound verifies this general conjecture,

- More specific bounds were conjectured for $t = 5, 6$
- The $t = 5$ bound was verified to be correct, the $t = 6$ case, the conjecture turned out to be incorrect .

[2] Song, Cai, Yuen, "On sequential locally repairable codes," arXiv preprint arXiv:1610.09767, 2016.

Proof (restrict to a sub matrix of H_{full})

Let H_{full} be the parity-check matrix of the $[n, k, r, t]_{\text{seq}}$ code.

$$H_{\text{full}} \;\Rightarrow\; \text{Rowspace}\,(H_{\text{full}})$$

$$\Downarrow$$

$$\text{restrict to subspace } S \text{ spanned by rows of } w_H(\cdot) \leq (r+1)$$

$$\Downarrow$$

$$\text{select basis with } w_H(\cdot) \leq (r+1) \text{ for } S\text{: } \{\underline{h}_1^t, \underline{h}_2^t, \cdots \underline{h}_m^t\}$$

$$\Downarrow$$

$$\text{Set } H \;=\; \begin{bmatrix} \underline{h}_1^t \\ \underline{h}_2^t \\ \vdots \\ \underline{h}_m^t \end{bmatrix}.$$

Proof (choose columns of low Hamming weight)

$$H = \begin{bmatrix} \underline{h}_1^t \\ \underline{h}_2^t \\ \vdots \\ \underline{h}_m^t \end{bmatrix} \Rightarrow \text{(each row of } H \text{ has Hamming weight} \leq (r+1))$$

- Our interest is in maximizing rate
- i.e., maximizing n for given redundancy m
- Hence choose as many columns of low Hamming weight as possible

Proof
(after some work, for t even, arrive at form below)

$$
H = \left[\begin{array}{c|c|c|c|c|c|c|c|c}
D_0 & A_1 & 0 & 0 & \dots & 0 & 0 & 0 & \\ \cline{1-8}
0 & D_1 & A_2 & 0 & \dots & 0 & 0 & 0 & \\ \cline{1-8}
0 & 0 & D_2 & A_3 & \dots & 0 & 0 & 0 & \\ \cline{1-8}
0 & 0 & 0 & D_3 & \dots & 0 & 0 & 0 & \\ \cline{1-8}
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & E \\ \cline{1-8}
0 & 0 & 0 & 0 & \dots & A_{\frac{t}{2}-2} & 0 & 0 & \\ \cline{1-8}
0 & 0 & 0 & 0 & \dots & D_{\frac{t}{2}-2} & A_{\frac{t}{2}-1} & 0 & \\ \cline{1-8}
0 & 0 & 0 & 0 & \dots & 0 & D_{\frac{t}{2}-1} & & \\ \cline{1-7}
0 & 0 & 0 & 0 & \dots & 0 & 0 & C &
\end{array}\right]
$$

- $\{D_i\}$ are diagonal and $\{A_i\}$ have column weight 1
- each row of $\{A_i\}$ has Hamming weight $\leq r$
- $\{C\}$ has column weight 2 and $\{E\}$ has column weight ≥ 3

- this form leads to the bound

Proof
(if equality holds in the bound, we must have:)

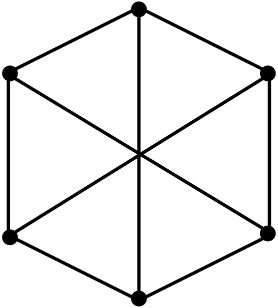
$$H = \left[\begin{array}{c|c|c|c|c|c|c|c}
D_0 & A_1 & 0 & 0 & \dots & 0 & 0 & 0 \\ \hline
0 & D_1 & A_2 & 0 & \dots & 0 & 0 & 0 \\ \hline
0 & 0 & D_2 & A_3 & \dots & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & D_3 & \dots & 0 & 0 & 0 \\ \hline
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \hline
0 & 0 & 0 & 0 & \dots & A_{\frac{t}{2}-2} & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & \dots & D_{\frac{t}{2}-2} & A_{\frac{t}{2}-1} & 0 \\ \hline
0 & 0 & 0 & 0 & \dots & 0 & D_{\frac{t}{2}-1} & C
\end{array}\right]$$

- each row of $\{A_i\}$ has Hamming weight $= r$
- there is no matrix E

Example: PC Matrix of Rate-Optimal ($r = 3, t = 2$) Code (Regular Graph)

$$
\begin{aligned}
H &= [D_0 \mid A_1] \\
&= \left[\begin{array}{cccccc|ccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1
\end{array}\right]
\end{aligned}
$$

Regular Graph Interpretation of $(r = 3, t = 2)$ Rate-Optimal Code



- Edges correspond to symbols
- Nodes correspond to parity-symbols
- Thus this code is an $[n = 15,\ k = 9,\ r = 3,\ t = 2]$ code

- A regular graph for any r will lead to a rate-optimal $(t = 2)$ code

Rate-Optimal Product Code ($t = 3$, $r = 4$)

c_{11}	c_{12}	c_{13}	c_{14}	c_{15}
c_{21}	c_{22}	c_{23}	c_{24}	c_{25}
c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
c_{41}	c_{42}	c_{43}	c_{44}	c_{45}
c_{51}	c_{52}	c_{53}	c_{54}	c_{55}

Figure: Code array.

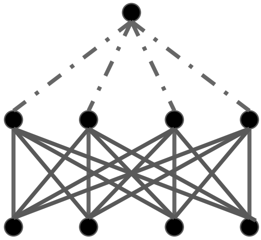


Figure: Graphical representation.

- Thus this code is an $[n = 25,\ k = 16,\ r = 4,\ t = 3]$ code
- A $2D$ product code for any r will lead to a rate-optimal ($t = 3$) code

Product Code: Parity Check Matrix

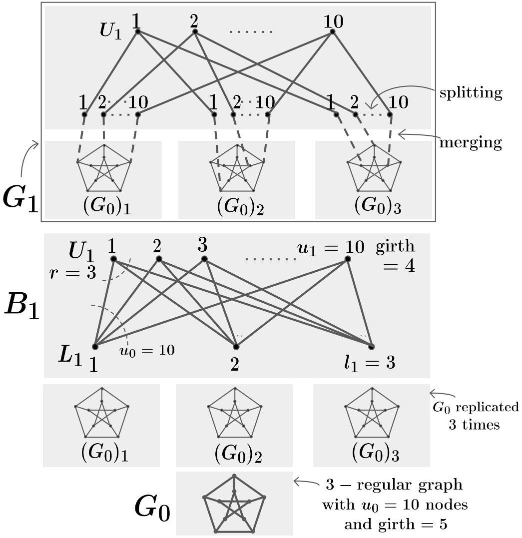
$$H = \left[\begin{array}{ccccc|cccccccccccccccccccc}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right]$$

(this matrix also conforms to the form

$$H = \begin{bmatrix} D_0 & A_1 \\ 0 & D_1 \end{bmatrix},$$

in the proof of the theorem)

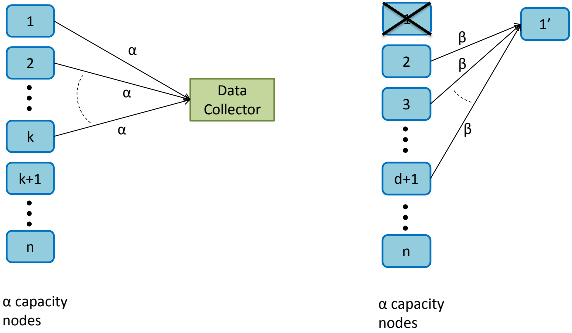
A Binary Rate-Optimal Code ($t = 4, r = 3$)



Regenerating Codes

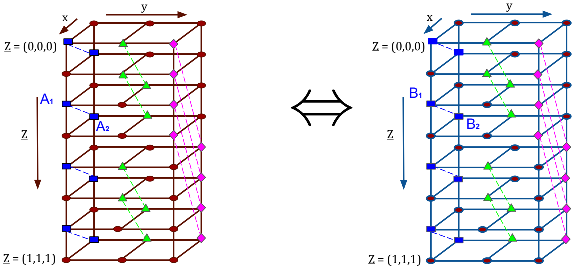
Regenerating Codes - Formal Definition

Parameters: $(\ (n, k, d), \ (\alpha, \beta), \ B, \ \mathbb{F}_q \ )$



- Data to be recovered by connecting to any k of n nodes
- Nodes to be repaired by connecting to any d nodes, downloading β symbols from each node; ($d\beta <<$ file size B)

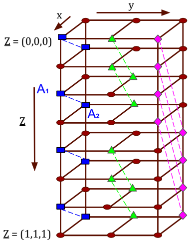
A Recent High-Rate MSR Code Construction with $d < (n-1)$



- A simple interpretation as being obtained through a pairwise, symbol transformation from a layered RS code (left)
- ... followed by an RS code across symbols within a node
- extends the Ye-Barg construction...

- Min Ye, Alexander Barg, "Explicit constructions of optimal-access MDS codes with nearly optimal sub-packetization," arXiv:1605.08630v1, 27 May 2016.
- Birenjith Sasidharan, Myna Vajha, P. Vijay Kumar, "An Explicit, Coupled-Layer Construction of a High-Rate MSR Code with Low Sub-Packetization Level, Small Field Size and $d < (n-1)$," arXiv:1701.07447v1, 25 Jan 2017.

A Recent High-Rate MSR Code Construction with $d < (n-1)$



- Rate as close to 1 as desired
- Field size comparable to that of an RS code of same block length
- Sub-packetization level comparable to that of the Ye-Barg construction
- $d < (n-1)$
- Explicit with uniform, all-symbol repair

- Birenjith Sasidharan, Myna Vajha, P. Vijay Kumar, "An Explicit, Coupled-Layer Construction of a High-Rate MSR Code with Low Sub-Packetization Level, Small Field Size and $d < (n-1)$," arXiv:1701.07447v1, 25 Jan 2017.

Thanks!