Bounds for Batch Codes with Restricted Query Size

Hui Zhang and Vitaly Skachek

ISIT 2016, Barcelona, Spain

12 July 2016

Supported by the research grants PUT405 and IUT2-1 from the Estonian Research Council, and by the COST Action IC1104 on random network coding and designs over $\mathbb{F}_q$.

Definition of Batch Codes

- Proposed in the crypto community for:
  - Load balancing.

Definition of Batch Codes

- Proposed in the crypto community for:
    - Load balancing.
    - Private information retrieval.

Definition of Batch Codes

- Proposed in the crypto community for:
  - Load balancing.
  - Private information retrieval.

Definition [Ishai *et al.* 2004]

$\mathcal{C}$ is an $(k, N, t, n, \nu)_\Sigma$ batch code over Σ if it encodes any string $\mathbf{x} = (x_1, x_2, \cdots, x_k) \in \Sigma^k$ into n strings (buckets) of total length N over Σ, namely $\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n$, such that for each t-tuple (batch) of (not neccessarily distinct) indices $i_1, i_2, \cdots, i_t \in [k]$, the symbols $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$ can be retrieved by t users, respectively, by reading $\leq \nu$ symbols from each bucket, such that x_{i_ℓ} is recovered from the symbols read by the ℓ-th user alone.

Definition of Batch Codes

- Proposed in the crypto community for:
  - Load balancing.
  - Private information retrieval.

Definition [Ishai *et al.* 2004]

$\mathcal{C}$ is an $(k, N, t, n, \nu)_\Sigma$ batch code over Σ if it encodes any string $\mathbf{x} = (x_1, x_2, \cdots, x_k) \in \Sigma^k$ into n strings (buckets) of total length N over Σ, namely $\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n$, such that for each t-tuple (batch) of (not neccessarily distinct) indices $i_1, i_2, \cdots, i_t \in [k]$, the symbols $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$ can be retrieved by t users, respectively, by reading $\leq \nu$ symbols from each bucket, such that x_{i_ℓ} is recovered from the symbols read by the ℓ-th user alone.

• Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Batch codes and their applications," *Proc. 36th ACM Symposium on Theory of Computing (STOC)*, June 2004, Chicago, IL.

Related Work

- Combinatorial Batch Codes

• M. Paterson, D. Stinson, and R. Wei, "Combinatorial batch codes," *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 13–27, 2009.

• R.A. Brualdi, K. Kiernan, S.A. Meyer, and M.W. Schroeder, "Combinatorial batch codes and transversal matroids," *Advances in Mathematics of Communications*, vol. 4, no. 3, pp. 419–431, 2010.

• C. Bujtás and Z. Tuza, "Combinatorial batch codes: extremal problems under Hall-type conditions," *Electronic Notes in Discrete Mathematics*, vol. 38, pp. 201–206, 2011.

• S. Bhattacharya, S. Ruj, and B. Roy, "Combinatorial batch codes: a lower bound and optimal constructions," *Advances in Mathematics of Communications*, vol. 6, no. 2, pp. 165–174, 2012.

• N. Silberstein and A. Gál, "Optimal combinatorial batch codes based on block designs," *Designs, Codes and Cryptography,* vol. 78, no. 2, pp 409-424, Feb. 2016.

Linear Batch Codes

- $\nu = 1$: only one symbol is read from each bucket.

Linear Batch Codes

- $\nu = 1$: only one symbol is read from each bucket.
- A batch code is *linear*, if every symbol in every bucket is a linear combination of the information symbols.

Linear Batch Codes

- $\nu = 1$: only one symbol is read from each bucket.
- A batch code is *linear*, if every symbol in every bucket is a linear combination of the information symbols.
- We consider *linear codes* with $\nu = 1$ and $N = n$: each bucket contains just one symbol in $\mathbb{F}_q$.

Linear Batch Codes

- $\nu = 1$: only one symbol is read from each bucket.
- A batch code is *linear*, if every symbol in every bucket is a linear combination of the information symbols.
- We consider *linear codes* with $\nu = 1$ and $N = n$: each bucket contains just one symbol in $\mathbb{F}_q$.

- Let $\mathbf{x} = (x_1, x_2, \cdots, x_k)$ be an information string.
- Let $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ be an encoding of $\mathbf{x}$.
- Each encoded symbol y_i, $i \in [n]$, is written as $y_i = \sum_{j=1}^{k} g_{j,i} x_j$.
- Generator matrix: $\mathbf{G} = \left(g_{j,i}\right)_{j\in[k], i\in[n]}$; the encoding is $\mathbf{y} = \mathbf{x}\mathbf{G}$.

Linear Batch Codes

- $\nu = 1$: only one symbol is read from each bucket.
- A batch code is *linear*, if every symbol in every bucket is a linear combination of the information symbols.
- We consider *linear codes* with $\nu = 1$ and $N = n$: each bucket contains just one symbol in $\mathbb{F}_q$.

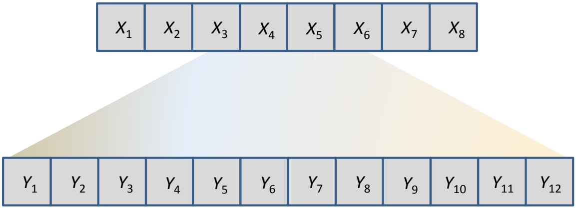
- Let $\mathbf{x} = (x_1, x_2, \cdots, x_k)$ be an information string.
- Let $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ be an encoding of $\mathbf{x}$.
- Each encoded symbol y_i, $i \in [n]$, is written as $y_i = \sum_{j=1}^{k} g_{j,i} x_j$.
- Generator matrix: $\mathbf{G} = \left(g_{j,i} \right)_{j \in [k], i \in [n]}$; the encoding is $\mathbf{y} = \mathbf{x}\mathbf{G}$.

• H. Lipmaa and V. Skachek, "Linear batch codes," *Proc. 4th International Castle Meeting on Coding Theory and Applications*, Palmela, Portugal, September 2014. http://arxiv.org/abs/1404.2796

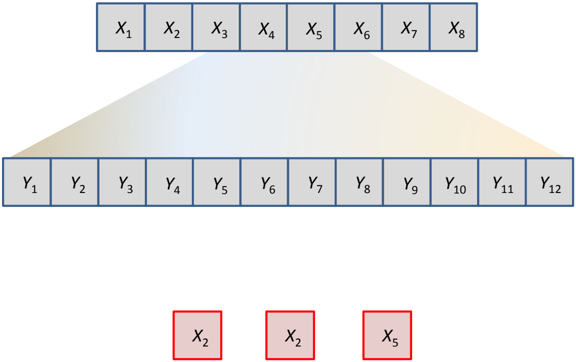
Example: Linear Batch Codes

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8

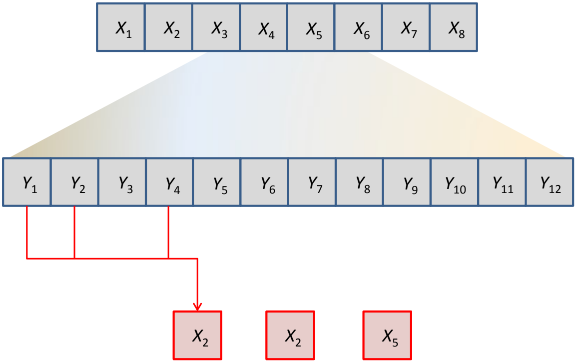
Example: Linear Batch Codes



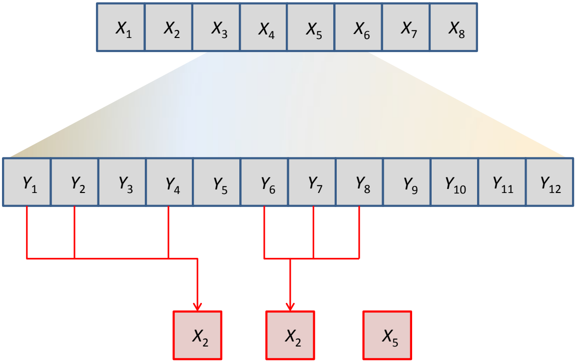
Example: Linear Batch Codes



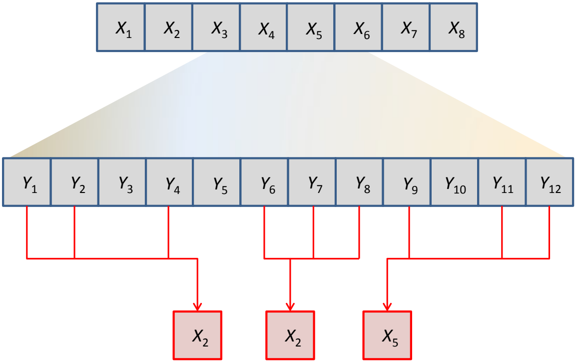
Example: Linear Batch Codes



Example: Linear Batch Codes



Example: Linear Batch Codes



Related Work

- Switch Codes

  • Z. Wang, O. Shaked, Y. Cassuto, and J. Bruck, "Codes for network switches," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, July 2013.

  • Z. Wang, H.M. Kiah, and Y. Cassuto, "Optimal binary switch codes with small query size," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pp. 636–640, June 2015.

  • Y.M. Chee, F. Gao, S.T.H. Teo, and H. Zhang, "Combinatorial systematic switch codes," *Proc. IEEE International Symposium on Information Theory (ISIT),* Hong Kong, China, pp. 241–245, June 2015.

Related Work

- Switch Codes

  • Z. Wang, O. Shaked, Y. Cassuto, and J. Bruck, "Codes for network switches," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, July 2013.

  • Z. Wang, H.M. Kiah, and Y. Cassuto, "Optimal binary switch codes with small query size," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pp. 636–640, June 2015.

  • Y.M. Chee, F. Gao, S.T.H. Teo, and H. Zhang, "Combinatorial systematic switch codes," *Proc. IEEE International Symposium on Information Theory (ISIT),* Hong Kong, China, pp. 241–245, June 2015.

- Connection to Distributed Data Storage

  • A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 681–685, June-July 2014.

  • N. Silberstein, "Fractional repetition and erasure batch codes", *Proc. 4th International Castle Meeting on Coding Theory and Applications,* Palmela, Portugal, September 2014.

Related Work

- Switch Codes

  • Z. Wang, O. Shaked, Y. Cassuto, and J. Bruck, "Codes for network switches," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, July 2013.

  • Z. Wang, H.M. Kiah, and Y. Cassuto, "Optimal binary switch codes with small query size," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pp. 636–640, June 2015.

  • Y.M. Chee, F. Gao, S.T.H. Teo, and H. Zhang, "Combinatorial systematic switch codes," *Proc. IEEE International Symposium on Information Theory (ISIT),* Hong Kong, China, pp. 241–245, June 2015.

- Connection to Distributed Data Storage

  • A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 681–685, June-July 2014.

  • N. Silberstein, "Fractional repetition and erasure batch codes", *Proc. 4th International Castle Meeting on Coding Theory and Applications,* Palmela, Portugal, September 2014.

- Graph-based Constructions

  • A.G. Dimakis, A. Gál, A.S. Rawat, and Z. Song, "Batch codes through dense graphs without short cycles", *IEEE Trans. on Inform. Theory*, vol. 62, no. 4, pp. 1592 - 1604, Apr. 2016.

Related Work

Switch Codes

• Z. Wang, O. Shaked, Y. Cassuto, and J. Bruck, "Codes for network switches," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, July 2013.

• Z. Wang, H.M. Kiah, and Y. Cassuto, "Optimal binary switch codes with small query size," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pp. 636–640, June 2015.

• Y.M. Chee, F. Gao, S.T.H. Teo, and H. Zhang, "Combinatorial systematic switch codes," *Proc. IEEE International Symposium on Information Theory (ISIT),* Hong Kong, China, pp. 241–245, June 2015.

Connection to Distributed Data Storage

• A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 681–685, June-July 2014.

• N. Silberstein, "Fractional repetition and erasure batch codes", *Proc. 4th International Castle Meeting on Coding Theory and Applications,* Palmela, Portugal, September 2014.

Graph-based Constructions

• A.G. Dimakis, A. Gál, A.S. Rawat, and Z. Song, "Batch codes through dense graphs without short cycles", *IEEE Trans. on Inform. Theory*, vol. 62, no. 4, pp. 1592 - 1604, Apr. 2016.

Codes for Private Information Retrieval

• A. Fazeli, A. Vardy, and E. Yaakobi, "PIR with low storage overhead: coding instead of replication," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pp. 2852 - 2856, June 2015. `http://arxiv.org/abs/1505.06241`

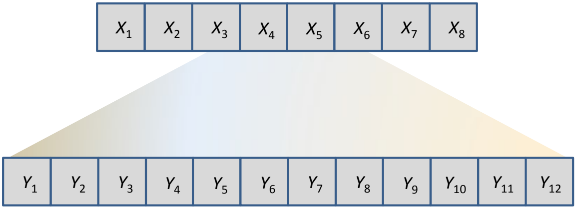
- Locally Repairable Codes

  • A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. on Inform. Theory*, vol. 56, no. 9, pp. 4539-4551, Sept. 2010.

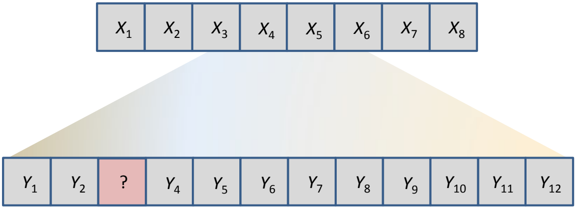
Example: Locally Repairable Codes

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8

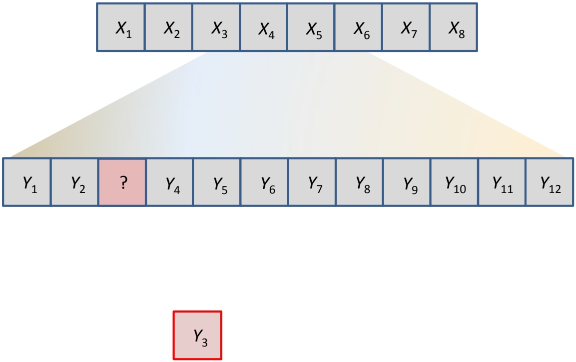
Example: Locally Repairable Codes



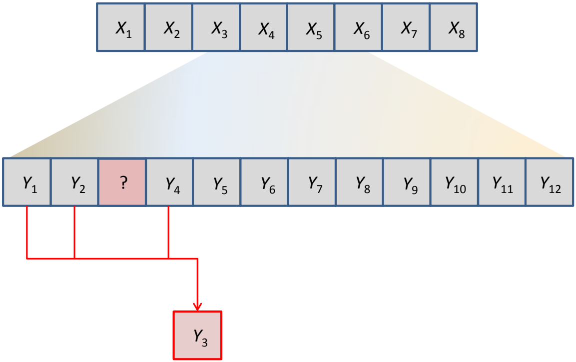
Example: Locally Repairable Codes



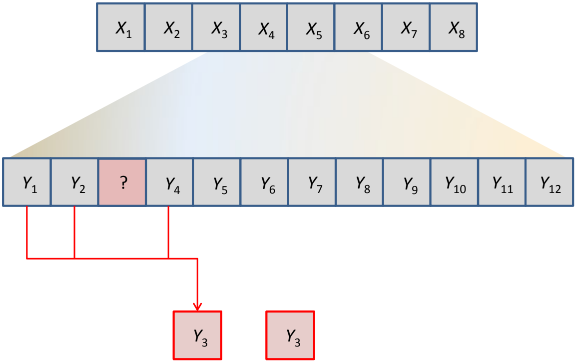
Example: Locally Repairable Codes



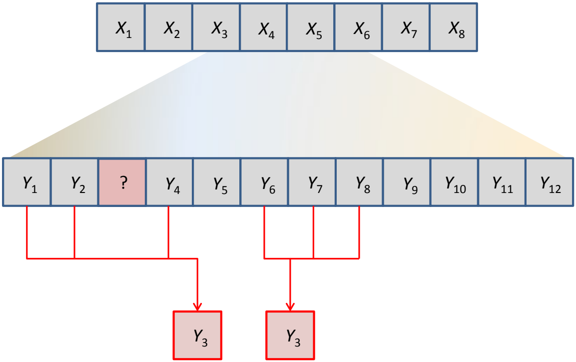
Example: Locally Repairable Codes



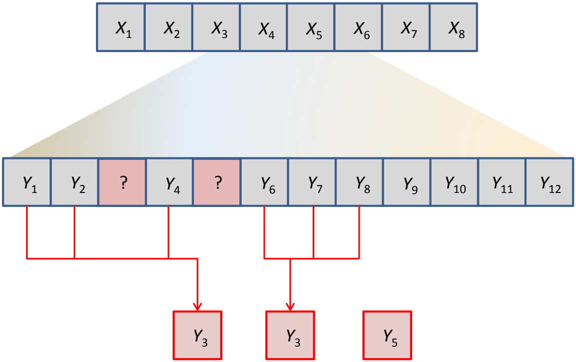
Example: Locally Repairable Codes



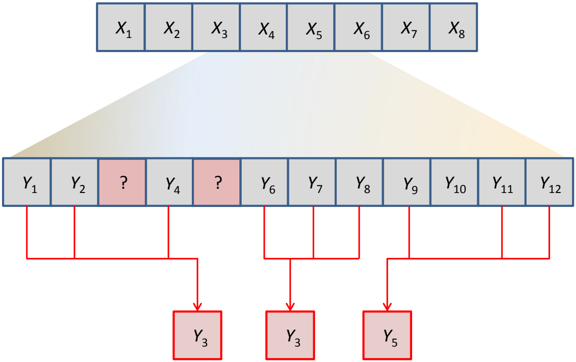
Example: Locally Repairable Codes



Example: Locally Repairable Codes



Example: Locally Repairable Codes



Batch Codes vs. Locally Repairable Codes

- Support different types of requests.

Batch Codes vs. Locally Repairable Codes

- Support different types of requests.
- There are examples of batch codes with **small locality** , which have **large locality** as LRCs. There are examples of LRCs with **small locality**, which have **large locality** as batch codes.

Batch Codes vs. Locally Repairable Codes

- Support different types of requests.
- There are examples of batch codes with **small locality** , which have **large locality** as LRCs. There are examples of LRCs with **small locality**, which have **large locality** as batch codes.
- **Systematic** LRCs for recovery of information part with availability are equivalent to **systematic** linear batch codes.

Batch Codes vs. Locally Repairable Codes

- Support different types of requests.
- There are examples of batch codes with **small locality** , which have **large locality** as LRCs. There are examples of LRCs with **small locality**, which have **large locality** as batch codes.
- **Systematic** LRCs for recovery of information part with availability are equivalent to **systematic** linear batch codes.

• A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 681–685, June-July 2014.

Batch Codes vs. Locally Repairable Codes

- Support different types of requests.
- There are examples of batch codes with **small locality** , which have **large locality** as LRCs. There are examples of LRCs with **small locality**, which have **large locality** as batch codes.
- **Systematic** LRCs for recovery of information part with availability are equivalent to **systematic** linear batch codes.
- The new results hold for **non-systematic** batch codes too.

• A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 681–685, June-July 2014.

Batch Codes vs. Locally Repairable Codes

- Support different types of requests.
- There are examples of batch codes with **small locality** , which have **large locality** as LRCs. There are examples of LRCs with **small locality**, which have **large locality** as batch codes.
- **Systematic** LRCs for recovery of information part with availability are equivalent to **systematic** linear batch codes.
- The new results hold for **non-systematic** batch codes too.
- Different choices of encoding mapping define **different** batch codes.

• A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 681–685, June-July 2014.

Distributed Storage Systems

- Locally Repairable Codes

  • A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. on Inform. Theory,* vol. 56, no. 9, pp. 4539-4551, Sept. 2010.

Distributed Storage Systems

- Locally Repairable Codes

• A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” *IEEE Trans. on Inform. Theory,* vol. 56, no. 9, pp. 4539-4551, Sept. 2010.

- Bounds on the Parameters of LRC Codes

• P. Gopalan, C. Huang, H. Simitchi, and S. Yekhanin, “On the locality of codeword symbols,” *IEEE Trans. on Inform. Theory,* vol. 58, no. 11, pp. 6925-6934, Nov. 2012.

• M. Forbes and S. Yekhanin, “On the locality of codeword sysmbols in non-linear codes,” *Discrete Math*, vol. 324, pp. 78–84, 2014.

• A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, “Locality and availability in distributed storage,” *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 681–685, June-July 2014.

• A. Wang and Z. Zhang, “Repair locality with multiple erasure tolerance,” *IEEE Trans. on Inform. Theory,* vol. 60, no. 11, pp. 6979 - 6987, Nov. 2014.

• A. S. Rawat, A. Mazumdar, and S. Vishwanath, “Cooperative local repair in distributed storage,” *EURASIP Journal on Adv. in Signal Processing,* Dec. 2015.

• I. Tamo and A. Barg, “Bounds on locally recoverable codes with multiple recovering sets,” *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 691-695, June-July 2014.

Restricted Query Size

Definition

A *primitive* (k, n, r, t) *batch code* $\mathcal{C}$ *with restricted query size* over an alphabet Σ encodes a string $\mathbf{x} \in \Sigma^k$ into a string $\mathbf{y} = \mathcal{C}(\mathbf{x}) \in \Sigma^n$, such that for all multisets of indices $\{i_1, i_2, \ldots, i_t\}$, where all $i_j \in [k]$, each of the entries $x_{i_1}, x_{i_2}, \ldots, x_{i_t}$ can be retrieved independently of each other by reading at most r symbols of $\mathbf{y}$.

Main Theorem

Lemma

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code over $\mathbb{F}$, $\mathbf{x} \in \mathbb{F}^k$, $\mathbf{y} = \mathcal{C}(\mathbf{x})$. Let $S_1, S_2, \cdots, S_t \subseteq [n]$ be t disjoint recovery sets for the coordinate x_i. Then, there exist indices $\ell_2 \in S_2$, $\ell_3 \in S_3$, $\cdots$, $\ell_t \in S_t$, such that if we fix the values of all coordinates of $\mathbf{y}$ indexed by the sets $S_1, S_2 \backslash \{\ell_2\}, S_3 \backslash \{\ell_3\}, \cdots, S_t \backslash \{\ell_t\}$, then the values of the coordinates of $\mathbf{y}$ indexed by $\{\ell_2, \ell_3, \cdots, \ell_t\}$ are uniquely determined.

Main Theorem

Lemma

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code over $\mathbb{F}$, $\mathbf{x} \in \mathbb{F}^k$, $\mathbf{y} = \mathcal{C}(\mathbf{x})$. Let $S_1, S_2, \cdots, S_t \subseteq [n]$ be t disjoint recovery sets for the coordinate x_i. Then, there exist indices $\ell_2 \in S_2$, $\ell_3 \in S_3$, $\cdots$, $\ell_t \in S_t$, such that if we fix the values of all coordinates of $\mathbf{y}$ indexed by the sets $S_1, S_2 \backslash \{\ell_2\}, S_3 \backslash \{\ell_3\}, \cdots, S_t \backslash \{\ell_t\}$, then the values of the coordinates of $\mathbf{y}$ indexed by $\{\ell_2, \ell_3, \cdots, \ell_t\}$ are uniquely determined.

Theorem

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code over $\mathbb{F}$ with the minimum distance d. Then,

$$d \leq n - k - (t-1)\left(\left\lceil \frac{k}{rt - t + 1} \right\rceil - 1\right) + 1 \,.$$

Input: linear (k, n, r, t) batch code $\mathcal{C}$

1: $\mathcal{C}_0 = \mathcal{C}$

2: $j = 0$

3: while $|\mathcal{C}_j| > 1$ do

4: $j = j + 1$

5: Choose the multiset $\{i_j^1, i_j^2, \ldots, i_j^t\} \subseteq [k]$ and disjoint subsets $S_j^1, \ldots, S_j^t \in [n]$, where S_j^ℓ is a recovery set for the information bit i_j^ℓ, such that there exist at least two codewords in $\mathcal{C}_{j-1}$ that differ in (at least) one coordinate

6: Let $\boldsymbol{\sigma}_j \in \Sigma^{|S_j|}$ be the most frequent element in the multiset $\{\mathbf{x}|_{S_j} : \mathbf{x} \in \mathcal{C}_{j-1}\}$, where $S_j = S_j^1 \cup \cdots \cup S_j^t$

7: Define $\mathcal{C}_j \triangleq \{\mathbf{x} : \mathbf{x} \in \mathcal{C}_{j-1}, \mathbf{x}|_{S_j} = \boldsymbol{\sigma}_j\}$

8: end while

Output: $\mathcal{C}_{j-1}$

Extensions of the Main Theorem

Corollary

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code over $\mathbb{F}$ with the minimum distance d. Then,

$$n \geq \max_{1 \leq \beta \leq t, \beta \in \mathbb{N}} \left\{ (\beta - 1) \left(\left\lceil \frac{k}{r\beta - \beta + 1} \right\rceil - 1 \right) + k + d - 1 \right\} .$$

Extensions of the Main Theorem

Corollary

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code over $\mathbb{F}$ with the minimum distance d. Then,

$$n \geq \max_{1 \leq \beta \leq t, \beta \in \mathbb{N}} \left\{ (\beta - 1) \left(\left\lceil \frac{k}{r\beta - \beta + 1} \right\rceil - 1 \right) + k + d - 1 \right\} .$$

Corollary

Let $\mathcal{C}$ be a linear systematic (k, n, r, t) batch code over $\mathbb{F}$ with the minimum distance d. Then,

$$n \geq \max_{2 \leq \beta \leq t, \beta \in \mathbb{N}} \left\{ (\beta - 1) \left(\left\lceil \frac{k}{r\beta - \beta - r + 2} \right\rceil - 1 \right) + k + d - 1 \right\} .$$

Example

Consider a batch code, which is the $[7, 3, 4]_2$ simplex code. The code, formed by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

is a $(3, 7, 2, 4)$ batch code with $d = 4$. Here $r = 2$ and $t = 4$.

Example

Consider a batch code, which is the $[7, 3, 4]_2$ simplex code. The code, formed by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} ,$$

is a $(3, 7, 2, 4)$ batch code with $d = 4$. Here $r = 2$ and $t = 4$. Pick $\beta = 2$. The RHS in the Main Theorem is

$$(2 - 1)\left(\left\lceil \frac{3}{2 \cdot 2 - 2 - 2 + 2} \right\rceil - 1\right) + 3 + 4 - 1 = 7 ,$$

and therefore the bound is attained with equality.

Example

Consider a batch code, which is the $[7, 3, 4]_2$ simplex code. The code, formed by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

is a $(3, 7, 2, 4)$ batch code with $d = 4$. Here $r = 2$ and $t = 4$. Pick $\beta = 2$. The RHS in the Main Theorem is

$$(2 - 1)\left(\left\lceil \frac{3}{2 \cdot 2 - 2 - 2 + 2} \right\rceil - 1\right) + 3 + 4 - 1 = 7 ,$$

and therefore the bound is attained with equality.

• Z. Wang, H. M. Kiah, and Y. Cassuto, "Optimal binary switch codes with small query size," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, pages 636–640, June 2015.

Further Improvements

- Assume that $\mu_j = 1$ for all $1 \leq j \leq \tau$ (i.e. in each step i of the algorithm, the set S_i recovers multiple copies of one symbol).
- Additionally, assume that

$$k \geq 2(rt - t + 1) + 1 \ .$$

- Let ϵ and λ be some positive integers,

$$
\begin{aligned}
\mathbb{A} &= \mathbb{A}(k, r, d, \beta, \epsilon) \\
&\triangleq (\beta - 1)\left(\left\lceil \frac{k+\epsilon}{r\beta - \beta + 1} \right\rceil - 1\right) + k + d - 1 , \\
\mathbb{B} &= \mathbb{B}(k, r, d, \beta, \lambda) \\
&\triangleq (\beta - 1)\left(\left\lceil \frac{k+\lambda}{r\beta - \beta + 1} \right\rceil - 1\right) + k + d - 1 , \\
\mathbb{C} &= \mathbb{C}(k, r, \beta, \lambda, \epsilon) \\
&\triangleq (r\beta - \lambda + 1)k - \binom{k}{2}(\epsilon - 1) .
\end{aligned}
$$

Improved Bound

Theorem

Let $\mathcal{C}$ be a linear (k, n, r, t) batch code with the minimum distance d. Then,

$$n \geq \max_{\beta \in \mathbb{N} \cap \left[1, \min\left\{t, \left\lfloor \frac{k-3}{2(r-1)} \right\rfloor\right\}\right]} \left\{ \max_{\epsilon, \lambda \in \mathbb{N} \cap [1, r\beta - \beta]} \{\min \{\mathbb{A}, \mathbb{B}, \mathbb{C}\}\} \right\} .$$

Example

Take $k = 12$, $r = 2$ and $t = 3$. The maximum of the right-hand side is obtained when $\beta = 3$. For that selection of parameters, we have

$$n \geq 15 + d \geq 18 \ .$$

At the same time, by taking $\beta = 3$, $\lambda = 1$ and $\epsilon = 1$, we obtain that

$$\mathbb{A} = \mathbb{B} = 17 + d \quad \text{and} \quad \mathbb{C} = 6 \cdot 12 - 0 = 72 \ ,$$

and so

$$n \geq \min\{17 + d, 72\} \geq 20 \ .$$

Thank you!

Questions?