New Bound for Batch Codes with Restricted Query Size

Vitaly Skachek

Joint work with **Hui Zhang**

COST Action IC1104 Workshop
Dubrovnik, 7 April 2016

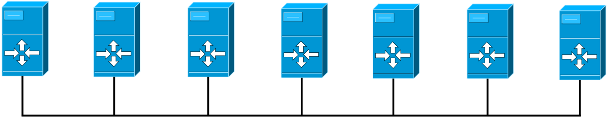
Supported by the research grants PUT405 and IUT2-1 from the Estonian Research Council and by the COST Action IC1104 on random network coding and designs over $\mathbb{F}_q$.

Distributed storage systems

- Enormous amounts of data are stored in a huge number of servers.
- Occasionally servers fail.
- Failed server is replaced and the data has to be copied to the new server.

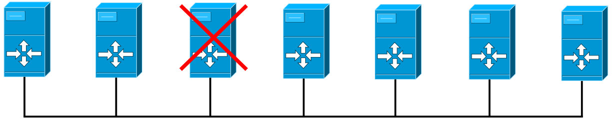
Distributed storage systems

- Enormous amounts of data are stored in a huge number of servers.
- Occasionally servers fail.
- Failed server is replaced and the data has to be copied to the new server.



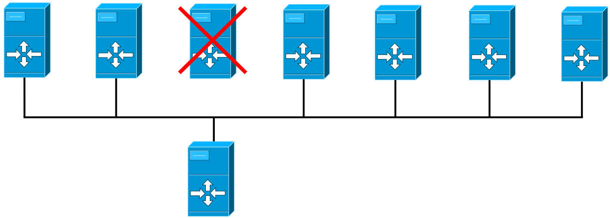
Distributed storage systems

- Enormous amounts of data are stored in a huge number of servers.
- Occasionally servers fail.
- Failed server is replaced and the data has to be copied to the new server.

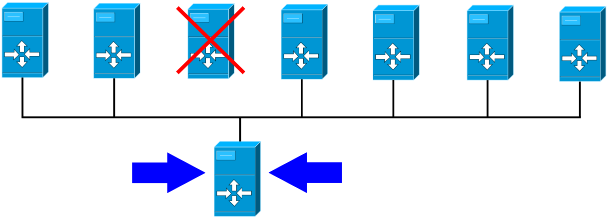


Distributed storage systems

- Enormous amounts of data are stored in a huge number of servers.
- Occasionally servers fail.
- Failed server is replaced and the data has to be copied to the new server.



- Enormous amounts of data are stored in a huge number of servers.
- Occasionally servers fail.
- Failed server is replaced and the data has to be copied to the new server.



Locally repairable codes

- Consideration: minimize amount of transferred data.
- Proposed in [Dimakis, Godfrey, Wu, Wainwright, Ramchandran 2008].

Locally repairable codes

- Consideration: minimize amount of transferred data.
- Proposed in [Dimakis, Godfrey, Wu, Wainwright, Ramchandran 2008].

- Erasure-correcting codes!
- Additional property: erasures can be recovered by using a small number of other symbols (locality).

Locally repairable codes

- Consideration: minimize amount of transferred data.
- Proposed in [Dimakis, Godfrey, Wu, Wainwright, Ramchandran 2008].

- Erasure-correcting codes!
- Additional property: erasures can be recovered by using a small number of other symbols (locality).

0	1	0	0	1	0	1	1	0

Locally repairable codes

- Consideration: minimize amount of transferred data.
- Proposed in [Dimakis, Godfrey, Wu, Wainwright, Ramchandran 2008].

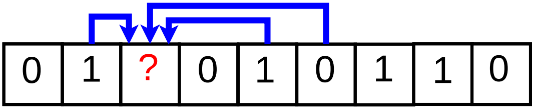
- Erasure-correcting codes!
- Additional property: erasures can be recovered by using a small number of other symbols (locality).

0	1	?	0	1	0	1	1	0

Locally repairable codes

- Consideration: minimize amount of transferred data.
- Proposed in [Dimakis, Godfrey, Wu, Wainwright, Ramchandran 2008].

- Erasure-correcting codes!
- Additional property: erasures can be recovered by using a small number of other symbols (locality).



Batch codes

- Proposed in [Ishai, Kushilevitz, Ostrovsky, Sahai 2004].
- Can be used in:
  - Load balancing.
  - Private information retrieval.
  - Distributed storage systems.

Batch codes

- Proposed in [Ishai, Kushilevitz, Ostrovsky, Sahai 2004].
- Can be used in:
  - Load balancing.
  - Private information retrieval.
  - Distributed storage systems.

Constructions:

- [Ishai *et al.* 2004]: algebraic, expander graphs, subsets, RM codes, locally-decodable codes

Prior art

Design-based constructions and bounds:

- [Stinson, Wei, Paterson 2009]
- [Brualdi, Kiernan, Meyer, Schroeder 2010]
- [Bujtas, Tuza 2011]
- [Bhattacharya, Ruj, Roy 2012]
- [Silberstein, Gal 2013]

Prior art

Design-based constructions and bounds:

- [Stinson, Wei, Paterson 2009]
- [Brualdi, Kiernan, Meyer, Schroeder 2010]
- [Bujtas, Tuza 2011]
- [Bhattacharya, Ruj, Roy 2012]
- [Silberstein, Gal 2013]

Application to distributed storage:

- [Rawat, Papailiopoulos, Dimakis, Vishwanath 2014]
- [Silberstein 2014]

Prior art

Design-based constructions and bounds:

- [Stinson, Wei, Paterson 2009]
- [Brualdi, Kiernan, Meyer, Schroeder 2010]
- [Bujtas, Tuza 2011]
- [Bhattacharya, Ruj, Roy 2012]
- [Silberstein, Gal 2013]

Application to distributed storage:

- [Rawat, Papailiopoulos, Dimakis, Vishwanath 2014]
- [Silberstein 2014]

Constructions and bounds:

- [Lipmaa, Skachek 2014]
- [Dimakis, Gal, Rawat, Song 2014]

Prior art

Design-based constructions and bounds:

- [Stinson, Wei, Paterson 2009]
- [Brualdi, Kiernan, Meyer, Schroeder 2010]
- [Bujtas, Tuza 2011]
- [Bhattacharya, Ruj, Roy 2012]
- [Silberstein, Gal 2013]

Application to distributed storage:

- [Rawat, Papailiopoulos, Dimakis, Vishwanath 2014]
- [Silberstein 2014]

Constructions and bounds:

- [Lipmaa, Skachek 2014]
- [Dimakis, Gal, Rawat, Song 2014]

Private information retrieval:

- [Fazeli Vardy Yaakobi 2015]

Batch codes

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.

Batch codes

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

If $\nu = 1$, then we use notation $(k, N, t, n)_\Sigma$ for it. Only one symbol is read from each bucket.

Batch codes

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

If $\nu = 1$, then we use notation $(k, N, t, n)_\Sigma$ for it. Only one symbol is read from each bucket.

Definition

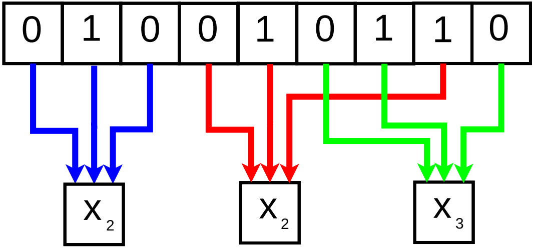
An $(k, N, t, n, \nu)_q$ batch code is *linear*, if every symbol in every bucket is a linear combination of original symbols.

Small buckets

In what follows, consider *linear codes* with $\nu = 1$ and $N = n$: each encoded bucket contains just one symbol in $\mathbb{F}_q$.

Small buckets

In what follows, consider *linear codes* with $\nu = 1$ and $N = n$: each encoded bucket contains just one symbol in $\mathbb{F}_q$.



Linear batch codes

For simplicity we refer to a linear $(k, N = n, t, n)_q$ batch code as $[n, k, t]_q$ batch code.

Linear batch codes

For simplicity we refer to a linear $(k, N = n, t, n)_q$ batch code as $[n, k, t]_q$ batch code.

- 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 $y_i = \sum_{j=1}^{k} g_{j,i} x_j$.
- Form the matrix $\mathbf{G}$:

$$\mathbf{G} = \left(g_{j,i} \right)_{j \in [k], i \in [n]} ;$$

the encoding is $\mathbf{y} = \mathbf{x}\mathbf{G}$.

Retrieval

Theorem

Let $\mathcal{C}$ be an $[n, k, t]_q$ batch code. It is possible to retrieve $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$ simultaneously if and only if there exist t non-intersecting sets $T_1, T_2, \cdots, T_t$ of indices of columns in $\mathbf{G}$, and for T_r there exists a linear combination of columns of $\mathbf{G}$ indexed by that set, which equals to the column vector $\mathbf{e}_{i_r}^T$, for all $r \in [t]$.

Retrieval

Theorem

Let $\mathcal{C}$ be an $[n, k, t]_q$ batch code. It is possible to retrieve $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$ simultaneously if and only if there exist t non-intersecting sets $T_1, T_2, \cdots, T_t$ of indices of columns in $\mathbf{G}$, and for T_r there exists a linear combination of columns of $\mathbf{G}$ indexed by that set, which equals to the column vector $\mathbf{e}_{i_r}^T$, for all $r \in [t]$.

Example

[Ishai *et al.* 2004] Consider the following linear binary batch code $\mathcal{C}$ whose 4×9 generator matrix is given by

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Retrieval (cont.)

Example

Let $\mathbf{x} = (x_1, x_2, x_3, x_4)$, $\mathbf{y} = \mathbf{x}\mathbf{G}$.
Assume that we want to retrieve the values of (x_1, x_1, x_2, x_2). We can retrieve (x_1, x_1, x_2, x_2) from the following set of equations:

$$\left\{ \begin{array}{rcl} x_1 & = & y_1 \\ x_1 & = & y_2 + y_3 \\ x_2 & = & y_5 + y_8 \\ x_2 & = & y_4 + y_6 + y_7 + y_9 \end{array} \right. .$$

It is straightforward to verify that any 4-tuple $(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4})$, where $i_1, i_2, i_3, i_4 \in [4]$, can be retrieved by using columns indexed by some four non-intersecting sets of indices in $[9]$. Therefore, the code $\mathcal{C}$ is a $[9, 4, 4]_2$ batch code.

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 $\mathbf{y}$.

Related Works

- [Gopalan, Huang, Simitci, Yekhanin 2012]
- [Forbes, Yekhanin 2014]
- [Rawat, Papailiopoulos, Dimakis, Vishwanath 2010]
- [Rawat, Mazumdar, Vishwanath 2014]
- [Tamo, Barg 2014]

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,

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

Algorithm

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 codes, which are obtained by taking $[7, 3, 4]$ simplex codes. It was shown in [Wang Kiah Cassuto 2015] that the linear 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 the minimum distance $d = 4$. Here $r = 2$ and $t = 4$.

Pick $\beta = 2$. The right-hand side in the Main Theorem can be re-written as

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

and therefore the bound is attained with equality for $\beta = 2$.

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,

Further Improvements (cont.)

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

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

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

and so

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

Thank you!

Questions?