ON GRAPH-BASED BATCH AND PIR CODES

Ago-Erik Riet, agoerik@ut.ee
Institute of mathematics and statistics, University of Tartu

joint work with Vitaly Skachek and Eldho K. Thomas

Latvian-Estonian joint Computer Science Theory Days 2018
Rīga, Latvia

13 October 2018

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 $\boldsymbol{x} = (x_1, x_2, \cdots, x_k) \in \Sigma^k$ into n strings (buckets) of total length N over Σ, namely $\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n$, 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.

Motivation

- Private information retrieval (PIR) codes can be used for multi-server private information retrieval to reduce the storage overhead [Fazeli, Vardy, Yaakobi].
- Batch codes can be used to access hot data which is distributed over several servers, to balance load [Ishai, Kushilevitz, Ostrovsky, Sahai].
- Up to t clients must be able to access pairwise disjoint sets of servers to retrieve an information vector $(x_{i_1}, \ldots, x_{i_t})$ (a multiset of information symbols) for batch codes and $(x_i, \ldots, x_i)$ (any one information symbol t times) for PIR codes.

• **A. Fazeli, A. Vardy, and E. Yaakobi,** "PIR with low storage overhead: coding instead of replication", *2015 IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, pp. 2852-2856, 2015.
• **Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai,** "Batch codes and their applications", *Proc. 36th ACM Symp. on Theory of Computing*, Chicago, IL, 2004.

Linear (computational) PIR/batch codes

- The code is a systematic linear code over $\mathbb{F}_q$ such that each parity symbol is a fixed linear combination (over $\mathbb{F}_q$) of a subset of information symbols (with non-zero coefficients).

Linear (computational) PIR/batch codes

- Let $\boldsymbol{x} = (x_1, x_2, \cdots, x_k)$ be an information string.
- Let $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$ be an encoding of $\boldsymbol{x}$.
- Each encoded symbol y_i, $i \in [n]$, is written as $y_i = \sum_{j=1}^{k} g_{j,i} x_j$.
- Generator matrix: $[\boldsymbol{I}|\boldsymbol{G}]$ where $\boldsymbol{G} = \left(g_{j,i}\right)_{j\in[k], i\in[n]}$; the encoding is $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G}$.
- If $E = \{x_1, \ldots, x_k\}$ (information symbols),
- $V = \{y_1, \ldots, y_n\}$ (parity symbols),
- $\{x_j, y_i\} \in I$ (an edge) iff $g_{j,i} \neq 0$
- bipartite graph $G(E, V, I)$ (left part E, right part V, edge set I).

Graph-based and asynchronous PIR/batch codes

- [Rawat, Song, Dimakis, Gal] showed that if $G(E, V, I)$ has girth (length of shortest cycle) ≥ 6, resp. ≥ 8 and $\forall i : \deg(x_i) \geq t - 1$ then the graph represents a PIR, resp. batch code with parameter t.
- Call the codes graph-based.
- OBSERVATION (R., Skachek, Thomas). Graph-based (PIR and) batch codes are moreover asynchronous, meaning if queries $x_{i_1}, \ldots, x_{i_{j-1}}, x_{i_{j+1}}, \ldots, x_{i_t}$ are being served and query x_{i_j} has been finished serving, it is possible to find a disjoint set of servers to serve any new (possibly different) query $x_{i_{t+1}}$.

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

Hypergraphs and graph-based PIR/batch codes

- Upon removing edges from $G(E, V, I)$ to equalize all left degrees to $t-1$ (changing the original code), girth cannot decrease.
- Define the corresponding (multi)hypergraph $\mathcal{F}(V, E)$ by identifying an $e \in E$ with the set $\{v \mid \{e, v\} \in I\}$. It will be $(t-1)$-uniform, or a $(t-1)$-graph.
- For PIR codes (Berge girth at least 3) it is equivalently a 2-$(|V|, t-1, 1)$ packing design.
- For batch codes (Berge girth at least 4) we prove that an extremal hypergraph for the $(3r-3, 3)$-problem can be modified to be an extremal hypergraph with Berge girth at least 4:

Hypergraph $(6,3)$-problem

- [Brown, Erdős and Sós] asked for $F^{(r)}(\eta;\kappa,s)$, the maximum number of hyperedges of an r-graph on η vertices whose no set of κ vertices contains s or more hyperedges, for fixed r,κ,s.
- [Ruzsa and Szemerédi] essentially solved first open case $F^{(3)}(\eta;6,3)$, known as the $(6,3)$-problem.
- [Erdős, Frankl and Rödl] essentially found $F^{(r)}(\eta;3r-3,3)$, solving the $(3r-3,3)$-problem.
- We use their solution for constructions and bounds for redundancy of graph-based batch codes.

• **W. G. Brown, P. Erdős, and V.T. Sós,** "Some extremal problems on r-graphs", *New Directions in the Theory of Graphs, 3rd Ann. Arbor Conference on Graph Theory*, Academic Press, pp. 55–63, 1973.
• **W. G. Brown, P. Erdős, and V.T. Sós,** "On the existence of triangulated spheres in 3-graphs and related problems", *Periodica Mathematica Hungaria*, vol. 3, pp. 221–228, 1973.
• **I.Z. Ruzsa, E. Szemerédi,** "Triple systems with no six points carrying three triangles", *Coll. Math. Soc. Janos Bolyai*, no. 18, pp. 939–945, 1978.
• **P. Erdös, P. Frankl, V. Rödl,** "The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent", *Graphs and Combinatorics*, vol. 2, No. 1, pp. 113–121, 1986..

Hypergraph $(6,3)$-problem

- We use constructions and bounds by Erdős, Frankl and Rödl for constructions, and bounds for redundancy, of graph-based batch codes.
- THEOREM (R., Skachek, Thomas). An r-graph with no 3 hyperedges contained in any set of $3r-3$ vertices, can be modified slightly, so that it has no Berge 2- or 3-cycle. An r-graph with no Berge 2- or 3-cycles already has no 3 hyperedges contained in any set of $3r-3$ vertices. Therefore,

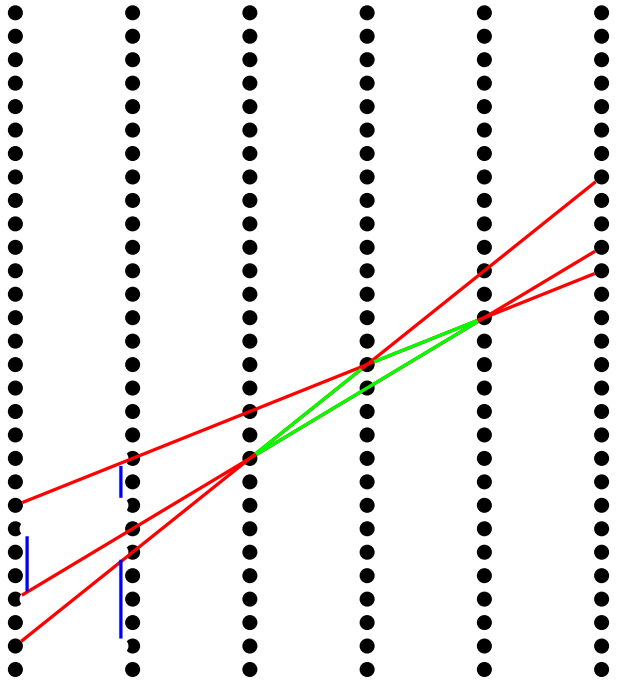
$$F^{(r)}(\eta; 3r-3, 3) = B^{(r)}(\eta; 4)$$

where $B^{(r)}(\eta; 4)$ is the maximum number of hyperedges in an r-graph with Berge girth at least 4.

• **P. Erdös, P. Frankl, V. Rödl,** "The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent", *Graphs and Combinatorics*, vol. 2, No. 1, pp. 113–121, 1986..

Erdős, Frankl and Rödl construction

- Arrange vertices as an $\lfloor \eta / r \rfloor$-by-r-grid. Each hyperedge is a line of r points with restricted slopes.



- 3 slopes, elements (4,3,2) in an arithmetic progression of length r would give rise to a (Berge) triangle.

Erdős, Frankl and Rödl construction

- [Behrend] constructed a big subset of $\{1, 2, \ldots, N\}$ containing no 3-term arithmetic progression.
- Erdős, Frankl and Rödl modified this contstruction, giving a big subset $A \subseteq \{1, 2, \ldots, N\}$, containing no 3 terms of any r-term arithmetic progression.
- In the grid, use only lines with slopes from A.
- The resulting hypergraph $\mathcal{F}(V, E)$ has no (Berge) 2- or 3-cycles.
- The respective bipartite incidence graph $G(E, V, I)$ has girth at least 8, giving rise to a graph-based batch code.

• **F.A. Behrend** "On sets of integers which contain no three elements in arithmetic progression", *Nat. Acad. Sci.*, no. 23, pp. 331–332, 1946.
• **P. Erdös, P. Frankl, V. Rödl,** "The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent", *Graphs and Combinatorics*, vol. 2, No. 1, pp. 113–121, 1986.

Erdős, Frankl and Rödl construction and bound

- This construction gives at least order of $\eta^{2-\epsilon}$ hyperedges for any $\epsilon > 0$.
- Reminder: there are $\eta = n - k$ parity symbols/vertices and $k = \eta^{2-\epsilon}$ information symbols/hyperedges and $t = r + 1 \geq 4$.
- Batch code redundancy $\rho = n - k$ is $O(k^{1/(2-\epsilon)})$.
- Erdős, Frankl and Rödl use an early version of Szemerédi's Regularity Lemma to bound the number of hyperdges to $o(\eta^2)$, so $\lim \frac{\rho}{\sqrt{k}} \to \infty$ for redundancy ρ of graph-based batch codes.

• **J. Komlós, A. Shokoufandeh, M. Simonovits, and E. Szemerédi** "The Regularity Lemma and Its Applications in Graph Theory", in: G. Khosrovshahi, A. Shokoufandeh, and A. Shokrollahi(eds) "Theoretical Aspects of Computer Science", Springer, pp. 84–112, 2002.
• **P. Erdös, P. Frankl, V. Rödl,** "The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent", *Graphs and Combinatorics*, vol. 2, No. 1, pp. 113–121, 1986.

Case $r = t - 1 = 2$

- For 2-graphs (graphs) we need to avoid multiple-edges and 3-cycles.
- The maximum number of edges in a graph on η vertices with no triangles is $\frac{\eta^2}{4}$, given by Mantel's (Turán's) Theorem.
- The complete bipartite graph $\mathcal{F}(V, E) = K_{\lfloor \eta/2 \rfloor, \lceil \eta/2 \rceil}$ attains this bound.
- Can construct the bipartite incidence graph $G(E, V, I)$ which is left-regular of degree 2 and has girth ≥ 8.
- For graph-based batch codes this gives redundancy

$$\rho = n - k = \Theta(\sqrt{k}).$$

Packing designs and PIR codes

- An r-graph with no (Berge) 2-cycles (a linear r-graph) is equivalently a 2-$(\eta, r, 1)$ packing design.
- Vertices – points; hyperedges – blocks. Defining condition: no two points in more than one block.
- So packing designs give rise to PIR codes with $\eta = n - k$ parity symbols, "number of blocks" $= k$ information symbols and $r = t - 1$.

Packing designs and PIR codes

- If $D(\eta, r)$ is the maximum number of blocks, then [Horsley] observed [Keevash] has proved, for big enough η, it is the largest possible, attaining the [Johnson] bounds. From [Keevash] but also already from [Wilson]:

$$\lim_{\eta \to \infty} \frac{D(\eta, r)}{\binom{\eta}{2} / \binom{r}{2}} = 1.$$

- $\eta = n - k$, $D(\eta, r) = k$, redundancy for PIR codes

$$\rho = n - k = \Theta(\sqrt{k}).$$

• **D. Horsley,** "Generalising Fisher's inequality to coverings and packings", *Combinatorica*, vol. 37, no. 4, pp. 673–696, Aug. 2017.
• **P. Keevash,** "The existence of designs", arXiv:1401.3665, Feb. 2018.
• **S. M. Johnson,** "A new upper bound for error-correcting codes", *IRE Trans. IT-8*, pp. 203–207, 1962.
• **R. M. Wilson,** "An existence theory for pairwise balanced designs I. Composition theorems and morphisms", *J. Combin. Theory Ser. A*, vol. 13, pp. 220–245, 1972.
• **R. M. Wilson,** "An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures", *J. Combin. Theory Ser. A*, vol. 13, pp. 246–273, 1972.
• **R. M. Wilson,** "An existence theory for pairwise balanced designs III. Proof of the existence conjectures", *J. Combin. Theory Ser. A*, vol. 18, pp. 71–79, 1975.

Packing designs and PIR codes

- For very small r, many constructions of Steiner 2-designs are known. It is possible to forget a small number of points/parity symbols and take a Steiner 2-design on the rest.

• **W. H. Mills, and R. C. Mullin,** "Coverings and packings", in: *"Contemporary Design Theory"*, (Eds. J. H. Dinitz and D. R. Stinson), Wiley, pp. 371–399, 1992.

Open questions

- [Rao, Vardy] proved redundancy $\rho = \Omega(\sqrt{k})$ for PIR codes for t=3. This also holds for $t \geq 3$ and for batch codes for $t \geq 3$.
- [Vardy, Yaakobi] showed for batch codes $\rho = O(\sqrt{k})$ for $t = 3, 4$ and $\rho = O(\sqrt{k} \log k)$ for $t \geq 5$.
- Note there is a gap for $t = 4$ between $O(\sqrt{k})$ and $\omega(\sqrt{k})$ general/graph-based asynchronous batch codes.
- For $t \geq 4$ what is the asymptotics of optimal redundancy for graph-based asynchronous batch codes?
- Is there a gap for $t \geq 5$ between optimal redundancy of general batch codes $(O(\sqrt{k} \log k))$ and graph-based asynchronous batch codes $(O(k^{1/(2-\epsilon)})$ and $\omega(\sqrt{k}))$?

• **S. Rao and A. Vardy,** "Lower Bound on the Redundancy of PIR Codes", arXiv:1605.01869, May 2016.
• **A. Vardy and E. Yaakobi,** "Constructions of batch codes with near-optimal redundancy", *Proc. ISIT*, Barcelona, pp. 1197-1201, July 2016.

Thank you!

Paldies!