On the Index Coding and Caching Problems

Eimear Byrne [1]
(joint work with Marco Calderini [2])

[1]University College Dublin, [2]University of Trento Italy

ALCOMA, March 19, 2015

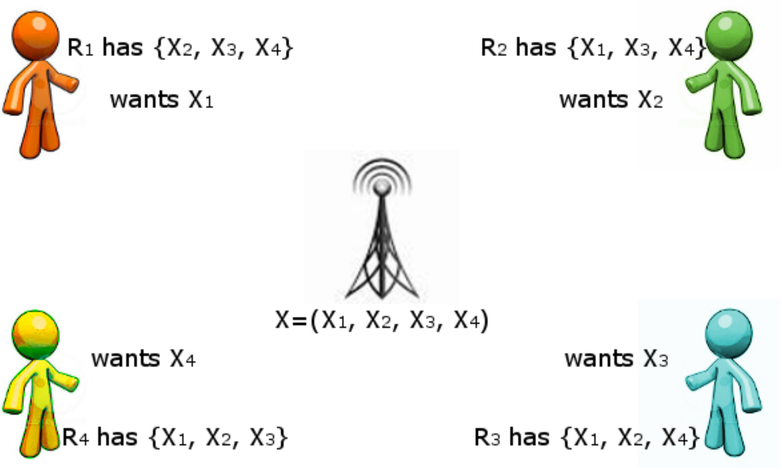
Outline

- The Index Coding with Side Information Problem
- Error Correction in the Index Coding Problem
- Generalizations
  - Coded-Side Information
  - Matrix Channels
- The Coded-Caching Problem
  - Connections to Index Coding
  - Connections to Rank-Distance Codes

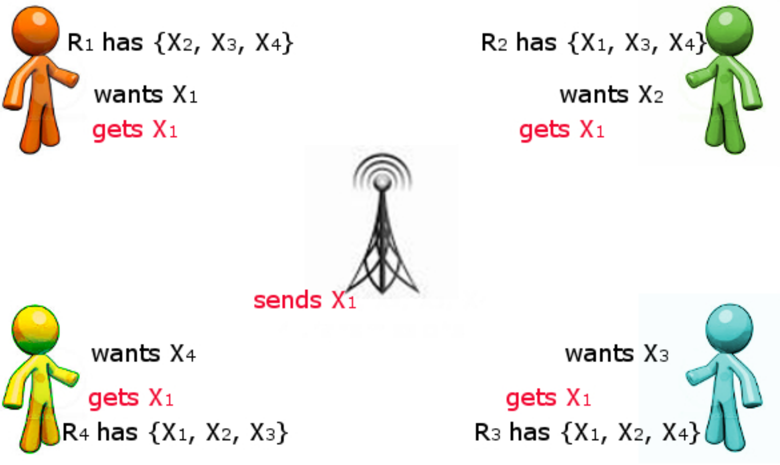
Index Coding with Side Information

- introduced in 2006 by Bar-Yossef, Birk, Jayram & Kol
- has applications to video-on-demand and wireless networks
- equivalent problem to Network Coding
- many approaches to problem from graph theory

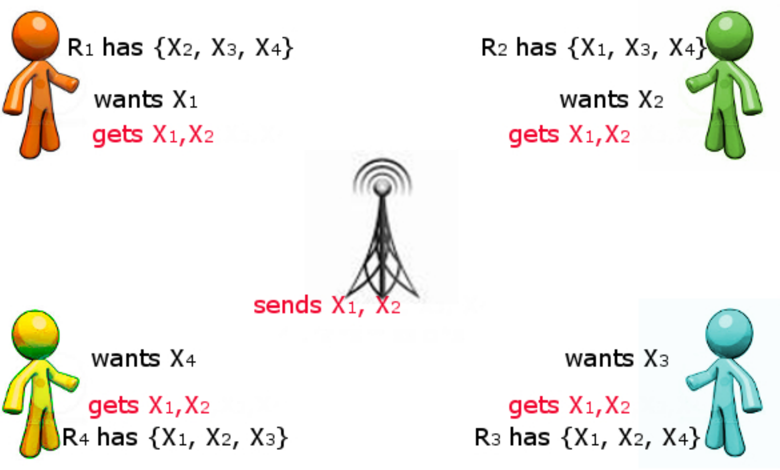
Index Coding with Side Information



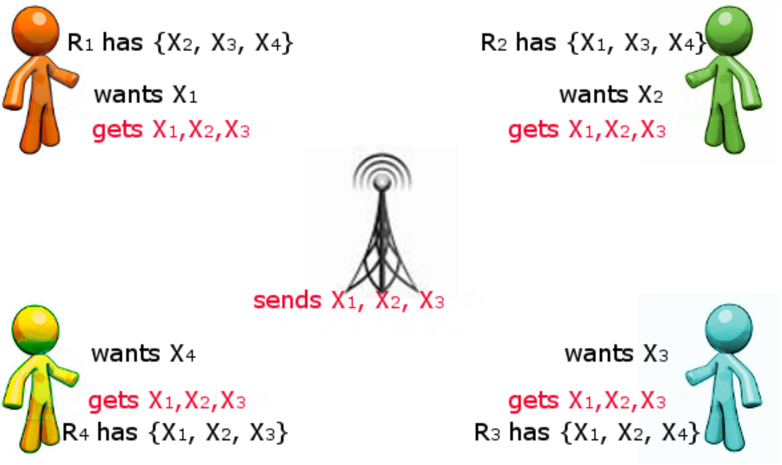
Index Coding with Side Information



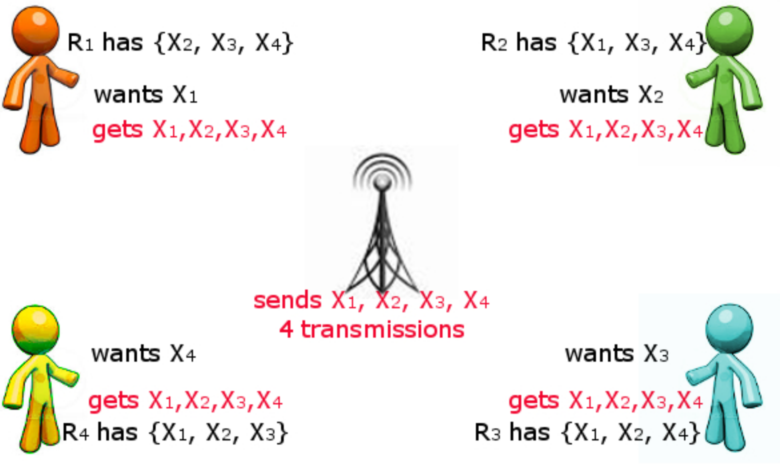
Index Coding with Side Information



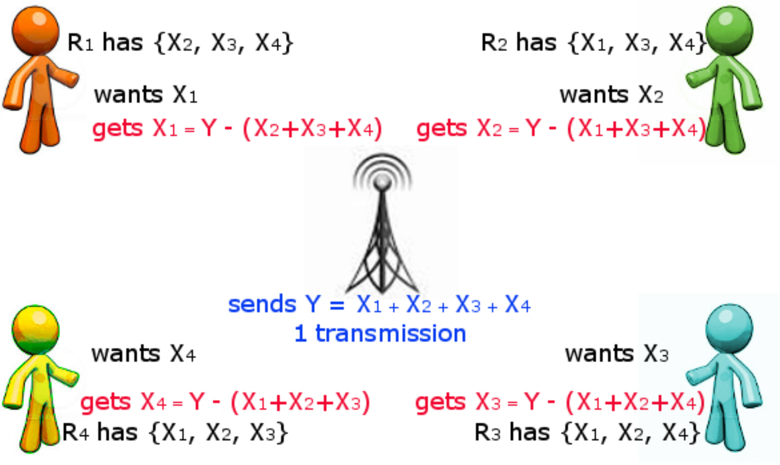
Index Coding with Side Information



Index Coding with Side Information



Index Coding with Side Information



Index Coding with Side-Information (Original Formula)

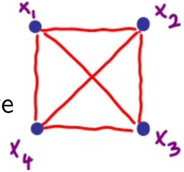
- The sender has a file X split into n packets $X = [X_1, ..., X_n] \in \mathbb{F}_q^n$.
- There are n users $\{1, ..., n\}$.
- User i has side information $\{X_j : j \in S_i\}$.
- User i requests packet X_i.
- $\mathcal{I} = \{S_i : i \in [n]\}$ is an instance of the index coding with side-information problem.

Problem 1 (The Main ICSI Problem)

What is the minimum number of transmissions required by the sender to satisfy all n requests, if encoding of data is permitted?

- Related Structure: the side-information digraph

Index Coding with Side Information



Example 2

Sender has $\{X_1, X_2, X_3, X_4\}, X_i \in \mathbb{F}_2^t$. The receivers have side-information:

$$D_1 = \{X_2, X_3, X_4\}, D_2 = \{X_1, X_3, X_4\},$$

$$D_3 = \{X_1, X_2, X_4\}, D_4 = \{X_1, X_2, X_3\}.$$

Choosing $L = [1, 1, 1, 1]$ the sender broadcasts LX :

$$\begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} \longrightarrow LX = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} = X_1 + X_2 + X_3 + X_4$$

So the minimum number of transmissions is $N = 1$.

The Min-Rank of a Graph

Definition 3

Let G be a directed graph with adjacency matrix $\mathcal{A}$.

$$\mathsf{minrank}_q(G) := \min\{\mathrm{rank}_q(A + I) : \mathrm{Supp}(A) \subset \mathrm{Supp}(\mathcal{A})\}.$$

Theorem 4 (Bar-Yossef, Birk, Jayram, Kol 2006)

The minimum number of transmissions required for a linear index code over $\mathbb{F}_2$ for the instance $\mathcal{I}$ is minrank(G), where G is the side-information graph of $\mathcal{I}$.

- The minrank is NP-hard to compute (Peeters, 1996)

Bounds on the Min-Rank of a Graph

Theorem 5 (Haemers, Haviv & Langberg, Bar-Yossef *et al*)

For every undirected graph G of n vertices over $\mathbb{F}_q$:

- $\alpha(G) \leq \Theta(G) \leq minrank_q(G) \leq \chi(\overline{G})$
- $\Omega(\log n) \leq minrank_q(G(n,p)) \leq \mathcal{O}(n/\log n)$
- *Expected value of $minrank_q(G(n,p))$ is (almost surely) $\Omega(\sqrt{n})$*

- $\alpha(G)$ is the max size of an independent set
- $\Theta(G)$ is the Shannon capacity of G
- $\chi(\overline{G})$ is the chromatic number of $\overline{G}$

Graph Theory

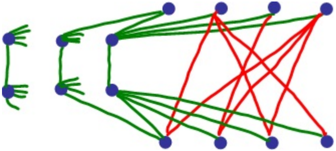
Shanmugam, Dimakis, Langberg, "Graph Theory Versus Minimum Rank for Index Coding," (2014) arXiv.1402.3898
The authors:

- distinguish between 'graph theoretic' and 'algebraic' methods,
- give index coding schemes from graph theory that outperform all known graph theoretic bounds,
- show all known graph theoretic bounds are withing $\log n$ of the chromatic number,
- state that the minrank (algebraic) can outperform the chromatic number by a polynomial factor.

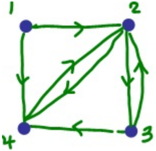
Equivalence of Linear Network and Index Coding

Theorem 6 (El Rouyhab et al 2010)

There exists a linear network code if and only if there exists a perfect linear index code.



Network Code



Index Code

Index Coding with Side-Information (New Formula)

- The sender has a file X split into n packets $X = [X_1, ..., X_n] \in \mathbb{F}_q^n$.
- There are $m \geq n$ users $\{1, ..., m\}$.
- User i has side information $\{X_j : j \in S_i\}$.
- User i requests packet $X_{f(i)}$, some surjection $f : [m] \longrightarrow [n]$.

Problem 7 (The Main ICSI Problem)

What is the minimum number of transmissions required by the sender to satisfy all m requests, if encoding of data is permitted?

- Related Structure: the side-information hypergraph

Data Retrieval

Definition 8

We say that $L \in \mathbb{F}_q^{N\times n}$ represents an linear $\mathcal{I} = (n, m, S, f)$ of the index coding problem with side information indexed by $S = \{S_i : i \in [m]\}$ if for each receiver $i \in [m]$ there is a decoding map

$$D_i : \mathbb{F}_q^N \times \mathbb{F}_q^n \to \mathbb{F}_q,$$

such that for some $A \in \mathbb{F}_q^n, \mathrm{Supp}(A) \subset S_i$

$$D_i(LX, A) = X_{f(i)} \ \forall X \in \mathbb{F}_q^n.$$

Decoding at the Receiver i

Let $A \in \mathbb{F}_q^n$ s.t. $\mathrm{Supp}(A) \subset S_i$. User i knows $AX = \sum_{j \in S_i} A_j X_j$.
Let $B \in \mathbb{F}_q^N$ such that

$$BL = A + e_{f(i)}. \tag{1}$$

Then

$$BLX = AX + e_{f(i)}X = AX + X_{f(i)}.$$

So the existence of a decoder depends on the solvability of (1).

$$D_i(LX, A) = BLX - AX = X_{f(i)}$$

The Min-Rank

Theorem 9 (Dau, Skachek, Chee 2012)

The minimum number of transmissions required for an instance $\mathcal{I} = (n, m, S, f)$ of the index coding problem is

$$\kappa(\mathcal{I}) := \min\{\mathrm{rank}(U + E_f) : \mathrm{Supp}(U_i) \subset S_i, i \in [m]\},$$

where $E_f \in \mathbb{F}_q^{m\times n}$ has each ith row equal to $e_{f(i)}$.

- $\kappa(\mathcal{I})$ is called the minrank of the system.
- $\kappa(\mathcal{I})$ generalizes the minrank of the *side-information graph*
- $\kappa(\mathcal{I})$ is *NP*-hard to compute.

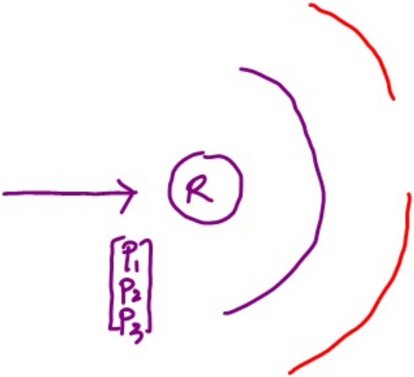
Coded-Side Information

User i wants P_i. The sender transmits a packet at each time slot.

Slot	Sent	User 1?	User 2?	User 3?
1	P_1	N	Y	N
2	P_2	Y	N	N
3	P_3	Y	Y	N
4	$P_1 + P_2$	N	N	Y
5	$P_1 + P_2 + P_3$	Y	Y	Y

After 5 transmissions, all user requests have been satisfied.

Coded-Side Information



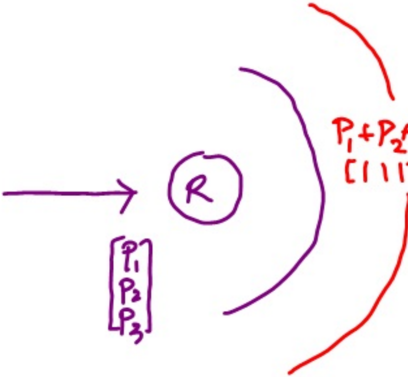
$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

$$\begin{bmatrix} P_2 \\ P_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

$$\begin{bmatrix} P_1 \\ P_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

$$\begin{bmatrix} P_1 + P_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

Coded-Side Information



$$\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

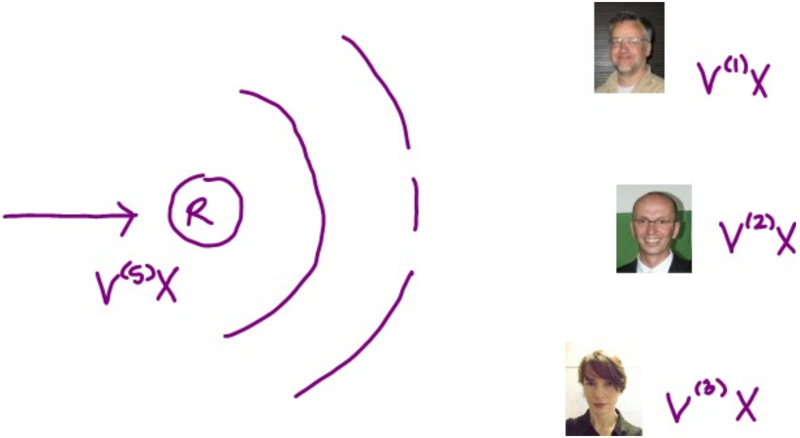
$$P_1+P_2+P_3 = \begin{bmatrix}1 & 1 & 1\end{bmatrix}\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

$$\begin{bmatrix}P_2\\P_3\end{bmatrix} = \begin{bmatrix}0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

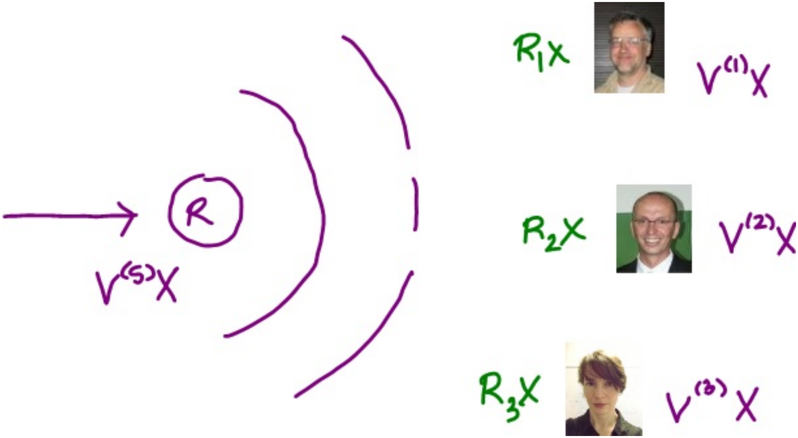
$$\begin{bmatrix}P_1\\P_3\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

$$\begin{bmatrix}P_1+P_2\end{bmatrix} = \begin{bmatrix}1 & 1 & 0\end{bmatrix}\begin{bmatrix}P_1\\P_2\\P_3\end{bmatrix}$$

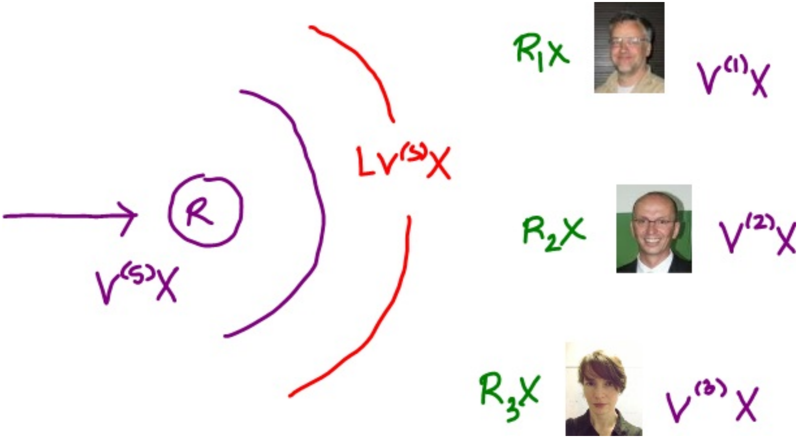
Coded-Side Information



Coded-Side Information



Coded-Side Information



Index-Coding with Coded-Side Information (New 3-in-1)

- $X \in \mathbb{F}_q^{n \times t}$
- The sender has $V^S X \in \mathbb{F}_q^{d_S \times t}$
- User i wants the packet $R_i X \in \mathbb{F}_q^t$,
- User i has side information $(V^{(i)}, V^{(i)} X) \in \mathbb{F}_q^{d_i \times n} \times \mathbb{F}_q^{d_i \times t}$
- The sender transmits $Y = LV^S X \in \mathbb{F}_q^{N \times t}$, some $L \in \mathbb{F}_q^{N \times d_S}$

Objective 1

The sender aims to find an encoding $LV^{(S)}X$ that minimizes N such that the demands of all users satisfied.

Case $t = 1$: Shum, Mingjun, Sung, "Broadcasting with Coded Side Information", IEEE 23rd PIMRC, vol. 89, no. 94, pp. 9-12, 2012.

An Instance of the ICCSI Problem

Definition 10

An instance of the Index Coding with Coded Side Information (ICCSI) problem is a list

$$\mathcal{I} = (t, n, m, \mathcal{X}, \mathcal{X}^S, R),$$

satisfying:

- t, n, m are positive integers,
- $\mathcal{X} = \oplus_{i \in [m]} \mathcal{X}^{(i)}$,
- $\mathcal{X}^{(i)} := \langle V^{(i)} \rangle < \mathbb{F}_q^n$, $\mathrm{dim} \mathcal{X}^{(i)} = d_i$,
- $\mathcal{X}^S := \langle V^{(S)} \rangle < \mathbb{F}_q^n$, $\mathrm{dim} \mathcal{X}^S = d_S$,
- $R \in \mathbb{F}_q^{m \times n}$ has rows $R_i \in \mathbb{F}_q^n$,
- $R_i \in \mathcal{X}^S$, $i \in [m]$.

Linear Index Encoding

Definition 11

Let N be a positive integer. The map

$$E : \mathbb{F}_q^{n \times t} \to \mathbb{F}_q^{N \times t},$$

is an $\mathbb{F}_q$-index code for $\mathcal{I}$ (E is an $\mathcal{I}$-IC) of length N if for each $i \in [m]$ there exists a decoding map

$$D_i : \mathbb{F}_q^{N \times t} \times \mathcal{X}^{(i)} \to \mathbb{F}_q^t,$$

satisfying

$$\forall X \in \mathbb{F}_q^{n \times t} \ : \ D_i(E(X), A) = R_i X,$$

for some $A \in \mathcal{X}^{(i)}$. E is called an $\mathbb{F}_q$-linear $\mathcal{I}$-IC if $E(X) = LV^{(S)}X$ for some $L \in \mathbb{F}_q^{N \times d_S}$. Then L represents the $\mathcal{I}$-IC E.

Decoding Criteria

Lemma 12

$L \in \mathbb{F}_q^{N \times d_s}$ represents an $\mathcal{I}$-IC if and only if for each $i \in [m]$,

$$R_i \in \left\langle \begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix} \right\rangle .$$

User i can compute

$$R_i X = AV^{(i)} X + BLV^{(S)} X,$$

for any $A \in \mathbb{F}_q^{d_i}$, $B \in \mathbb{F}_q^{N}$ satisfying $R_i = AV^{(i)} + BLV^{(S)}$.

The Min-Rank

Lemma 13 (BC)

The length of an optimal $\mathbb{F}_q$-linear $\mathcal{I}$-IC is $\kappa(\mathcal{I}) :=$

$$\min\{\mathrm{rank}(A + R) : A \in \mathbb{F}_q^{m \times n}, A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^S < \mathbb{F}_q^n, \ \forall i \in [m]\}.$$

- $\kappa(\mathcal{I})$ is called the minrank of the instance $\mathcal{I}$.
- $\kappa(\mathcal{I}) = d_{\mathrm{rk}}(R, \mathcal{X} \cap \tilde{\mathcal{X}}) = w_{\mathrm{rk}}(R + (\mathcal{X} \cap \tilde{\mathcal{X}}))$, where $\tilde{\mathcal{X}} = \oplus \mathcal{X}^S$.

The Min-Rank

$m = 6, n = 4, R_i = e_i, i \in [m], R_5 = e_2, R_6 = e_1$ over $\mathbb{F}_2$.

$$V^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$V^{(4)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(6)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R + \mathcal{X} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & * & * \\ * & 0 & 0 & * \\ * & * & 0 & 0 \\ 0 & * & * & 0 \\ * & 0 & * & 0 \\ 0 & * & 0 & * \end{bmatrix} = \begin{bmatrix} 1 & 0 & * & * \\ * & 1 & 0 & * \\ * & * & 1 & 0 \\ 0 & * & * & 1 \\ * & 1 & * & 0 \\ 1 & * & 0 & * \end{bmatrix}$$

The minrank is 3, so $N = 3$ transmissions are required.

Existence of an $\mathcal{I}$-IC

Theorem 14 (BC)

Let $\mathcal{I}$ be an instance of an ICCSI problem and let

$$N = \max\{n - d_i : i \in [m]\}.$$

Suppose that $q > m$. If L is chosen uniformly at random in $\mathbb{F}_q^{N \times d_S}$ then the probability that L represents a linear $\mathcal{I}$-IC is at least $(1 - m/q)^N$.

Corollary 15

If $q > m$ then $\kappa(\mathcal{I}) \leq \max\{n - d_i : i \in [m]\}$.

- Comparable with the Main Network Coding Theorem (see Fragouli & Soljanin *Network Coding Fundamentals*).

The Min-Rank

$m = 6, n = 4, R_i = e_i, i \in [m], R_5 = e_2, R_6 = e_1$ over $\mathbb{F}_3$.

$$V^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$V^{(4)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(6)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$R + \mathcal{X} = \begin{bmatrix} 1 & 0 & * & * \\ * & 1 & 0 & * \\ * & * & 1 & 0 \\ 0 & * & * & 1 \\ * & 1 & * & 0 \\ 1 & * & 0 & * \end{bmatrix} \text{ contains } \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \end{bmatrix}.$$

$R + \mathcal{X}$ has minrank $2 = N = n - d_i$ over $\mathbb{F}_3$.

Bounds on the Min-Rank

- Can we improve the bound $\kappa(\mathcal{I}) \leq \max\{n - d_i : i \in [m]\},\ q > m$?
- An $\mathcal{I}$-IC of length N exists if and only if, for all $i \in [m]$,

$$(R_i + \mathcal{X}^{(i)}) \cap \mathcal{L} \neq \emptyset$$

where $\mathcal{L} = \langle LV^{(S)} \rangle$.

Problem 16

Find an upper bound on the number of N-dimensional subspaces $\mathcal{L}$ that miss $R_i + \mathcal{X}^{(i)}$ for at least one value of $i \in [m]$.

Bounds on the Min-Rank

Using incidence matrices of designs we can construct $\mathcal{I}$ and compute bounds on $\kappa(\mathcal{I})$.

Theorem 17

(BC) There exist $\mathcal{I}$-IC satisfying

- $\kappa(\mathcal{I}) \leq \frac{m+1}{2}$ *(2-(n, k, λ) design),*
- $\kappa(\mathcal{I}) = \frac{p^2+p+1}{2}$ *(projective plane of order $p = 2, 3$).*

Index Coding with Errors

Dau, Skachek, Chee, "Error Correction for Index Coding With Side Information," IEEE Trans on Inform. Th, (59), 3, 2013.

The authors:

- introduced index coding with error correction,
- gave several bounds on the length of an optimal δ-error index code,
- gave a decoding algorithm based on syndrome decoding.

Error-Correction for Coded-Side Information

Definition 18

Let $\mathcal{M} \subset \mathbb{F}_q^{n\times t}$ be the message space.

$$E : \mathbb{F}_q^{n\times t} \to \mathbb{F}_q^{N\times t},$$

is a δ-error correcting code for $\mathcal{I}$ of length N (E is $(\mathcal{I},\delta)$-ECIC), if for each i $\exists$ a decoding map

$$D_i : \mathbb{F}_q^{N\times t} \times \mathcal{X}^{(i)} \to \mathbb{F}_q^{t},$$

such that for some $A \in \mathcal{X}^{(i)}$.

$$D_i(E(X) + W, A) = R_i X$$

for all $X \in \mathcal{M}$ and $W \in \mathbb{F}_q^{N\times t}$, $w(W) \leq \delta$.
E is linear if $E(X) = LV^{(S)}X$ for some $L \in \mathbb{F}_q^{N\times d_S}$.

Decoding Criterion

Theorem 19 (BC)

Let $\mathcal{I}$ be an instance of an ICCSI problem and let N be a positive integer. A matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents a linear $(\mathcal{I}, \delta)$-ECIC if and only if for all $i \in [m]$

$$w\left(LV^{(S)}(X - X')\right) \geq 2\delta + 1,$$

for all $X, X' \in \mathcal{M}$ such that $X - X' \in \mathcal{Z}^{(i)}$.

- $\mathcal{Z}^{(i)} = \{Z \in \mathbb{F}_q^{n \times t} : V^{(i)}X = 0, R_i X \neq 0\}$

Bounds on the Optimal Length of an ECIC: $t = 1$

- $\mathcal{N}(\mathcal{I}, \delta) =$ optimal length N of an δ-error correcting $\mathcal{I}$.
- $N(k, d) =$ optimal length ℓ of a $\mathbb{F}_q$-$[\ell, k, d]$ code
- $\mathcal{J}(\mathcal{I}) := \{U < \mathbb{F}_q^n : U \backslash \{0\} \subset \cup_{i \in [m]} \mathcal{Z}^{(i)}\}$.
- $\alpha(\mathcal{I}) := \max\{\dim U : U \in \mathcal{J}(\mathcal{I})\}$
- $\alpha(\mathcal{I})$ generalizes the notion of an independent set.

Theorem 20 (BC)

Let $\mathcal{I}$ be an instance of the ICCSI problem with $t = 1$. Then

- $N(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta)$,
- $\alpha(\mathcal{I}) \leq \kappa(\mathcal{I})$.

Further Bounds..

Theorem 21 (BC)

Let $\mathcal{I}$ be an instance of the ICCSI problem with $t = 1$. Then

- $\mathcal{N}(\mathcal{I}, \delta) \leq N(\kappa(\mathcal{I}), 2\delta + 1)$ *(κ-bound),*
- $\kappa_q(\mathcal{I}) + 2\delta \leq \mathcal{N}_q(\mathcal{I}, \delta)$ *(Singleton Bound),*
- *if* $q \geq \kappa(\mathcal{I}) + 2\delta - 1$ *then* $\mathcal{N}(\mathcal{I}, \delta) = \kappa(\mathcal{I}) + 2\delta$*,*
- *there exists an* $\mathbb{F}_q$*-linear* $(\mathcal{I}, \delta)$*-ECIC if*

$$N > n - d - 1 + \log_q(m(q-1)V_q(N, 2\delta)),$$

where $d = \min\{d_i : i \in [m]\}$*.*

Bounds on the Optimal Length of an ECIC: $t > 1$

- $\mathcal{N}(\mathcal{I}, \delta) =$ optimal length N of an δ-error correcting $\mathcal{I}$.
- $N(t, \log_q M, d)$ is the least integer N s.t. $\exists$ a code in $\mathbb{F}_q^{N \times t}$ of minimum rank distance d and size M.
- $\mathcal{J}(\mathcal{I}) := \{U \subset \mathbb{F}_q^{n \times t} : X - X' \in \mathcal{Z}_\delta^{(i)}$ some i, any $X, X' \in U\}$.
- $\alpha(\mathcal{I}) := \max\{\log_q |U| : U \in \mathcal{J}(\mathcal{I})\}$
- $\alpha(\mathcal{I})$ generalizes the notion of an independent set.

Theorem 22 (BC)

Let $\mathcal{I}$ be an instance of the ICCSI problem with $t > 1$. Then

- $N(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta)$,
- $\mathcal{N}(\mathcal{I}, \delta) \geq \frac{\alpha(\mathcal{I})}{t} + 2\delta$ *if* $t \geq N(t, \alpha(\mathcal{I}), 2\delta + 1)$,
- $\mathcal{N}(\mathcal{I}, \delta) \geq \frac{\alpha(\mathcal{I})}{t - 2\delta}$ *if* $t \leq N(t, \alpha(\mathcal{I}), 2\delta + 1)$,
- $\alpha(\mathcal{I}) \leq \kappa(\mathcal{I})$.

Decoding

- For Hamming errors a variation of syndrome decoding can be used (high complexity).
- Adding further redundancy to the system, we can use a simple matrix decoder (Silva et al 2010) to correct rank-metric errors in linear time.

Decoding Over the Matrix Channel

The sender transmits:

$$A = \begin{pmatrix} 0_{\delta\times\delta} & 0_{\delta\times t} \\ 0_{N\times\delta} & LV^{(S)}X \end{pmatrix},$$

The error matrix has the form

$$W = \begin{pmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{pmatrix},$$

and $\mathrm{rank}(W_{11}) = \mathrm{rank}(W) = r \leq \delta$. The receivers get

$$W = \begin{pmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} + LV^{(S)}X \end{pmatrix} - - > \begin{pmatrix} W_{11} & W_{12} \\ 0 & LV^{(S)}X \end{pmatrix}.$$

Decoding

1. Choose $A \in \mathbb{F}_q^{d_i}$.
2. Solve $R_i + AV^{(i)} = BLV^S$ for some $B \in \mathbb{F}_q^N$.
3. Compute $R_i X = BY - AV^{(i)} X$.

In other words, the decoder computes $M = [G|H]$, the reduced-row echelon form of the matrix

$$\begin{bmatrix} V^{(i)} & V^{(i)}X \\ LV^{(S)} & Y \end{bmatrix}$$

and solves for Z in $ZA = R_i$ to retrieve $R_i X = ZB$.

Side-Information Coverings

Lemma 23 (BC)

Given $t, n, m, \mathcal{X}$, there exists an encoding of length N satisfying every possible request R if and only if

$$\begin{aligned} N &\geq \max\{\min\{\mathrm{rank}(U+R) : U \in \mathcal{X}\}, R \in \mathbb{F}_q^{m\times n}\} \\ &= \max\{\min\{d_{\mathrm{rk}}(R,U) : U \in \mathcal{X}\}, R \in \mathbb{F}_q^{m\times n}\} \\ &= \max\{d_{\mathrm{rk}}(R,\mathcal{X}), R \in \mathbb{F}_q^{m\times n}\} \\ &= \rho_{\mathrm{rk}}(\mathcal{X}) \end{aligned}$$

$=$ the rank-metric covering radius of $\mathcal{X} = \mathcal{X}^{(1)} \oplus \cdots \oplus \mathcal{X}^{(m)}$.

The Caching Problem

M. A. Maddah-Ali, U. Niesen, "Fundamental Limits of Caching," arXiv.1209.5807.

- m users seek all or part of a file $X \in \mathbb{F}_q^{n\times t}$
- Each user has storage capacity d_i.
- Placement phase: the sender places data in each user's cache during low-traffic times.
- Delivery phase: the sender broadcasts data according to users demands.
- User requests are unknown to the sender at the placement phase.

Problem 24

How should data files be placed in order to minimize transmissions during delivery?

A Caching Strategy

- There are m users each with storage capacity d_i, $i \in [m]$.
- Choose $\mathcal{X} = \oplus_{i\in[m]}\mathcal{X}^{(i)}$ s.t.
  - $\dim \mathcal{X}^{(i)} = d_i$
  - $\mathcal{X}$ has optimal covering rank radius N
- Place $\mathcal{X}^{(i)}$ in User i's cache.
- Then at the delivery phase all possible users' requests can be satisfied with N transmissions.

Problem 25

Construct codes $\mathcal{X}$ with low covering radius.

Final Remarks

- There is an analogue of the ICSI problem for subspace codes. Each user i has some side information $\mathcal{X}^{(i)} < \mathbb{F}_q^n$ and the sender transmits $V < \mathrm{rowsp}(X)$ such that a requested 1-dimensional subspace of $\mathrm{rowsp}(X)$ is contained in $V + \mathcal{X}^{(i)}$.
- How should the ICSI problem be modelled for implementation with MRD codes?
- What bounds and caching schemes in the caching problem can be obtained via algebraic codes for the rank metric?