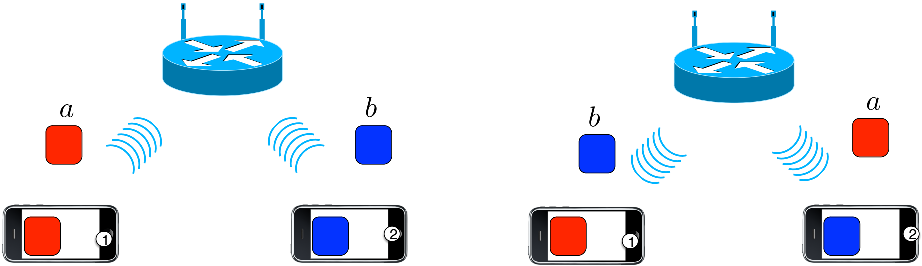
# Wireless Network Coding: Algorithms, Analysis, and Applications

A. Sprintson

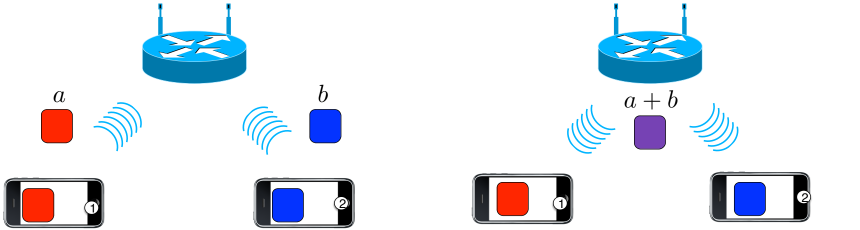
Department of Electrical and Computer Engineering
Texas A&M

CUHK, Hong Kong
Nov. 10, 2014

# Wireless Network Coding

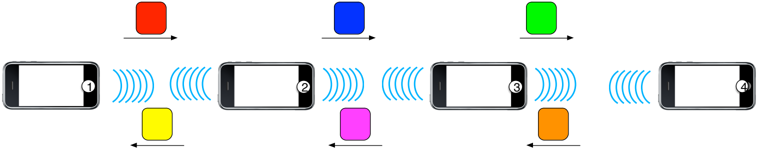


# Wireless Network Coding



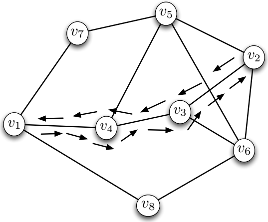
# Reverse Carpooling

- Leverage the broadcast properties of the wireless medium
- Flow in the opposite direction is (almost) free

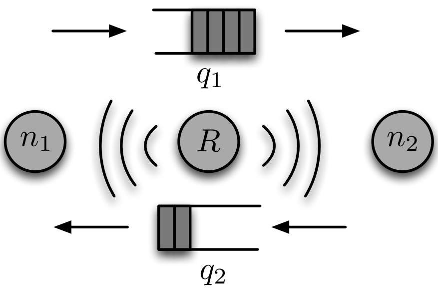


# Reverse Carpooling

- The network coding technique allows to send packets in opposite direction with little extra cost
- How to encourage flows to use carpool lines?

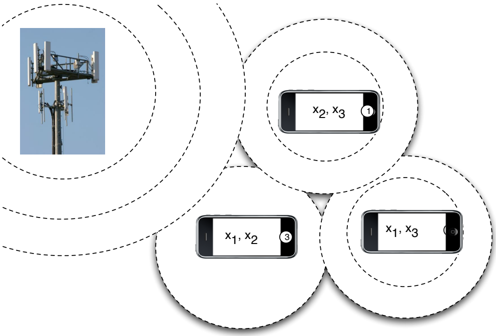


# Code or wait?



# Heterogenous Wireless Networks

- Clients might be interested in the same data
- Data is broadcast from an external source
- Clients receive missing packets from their peers using local links

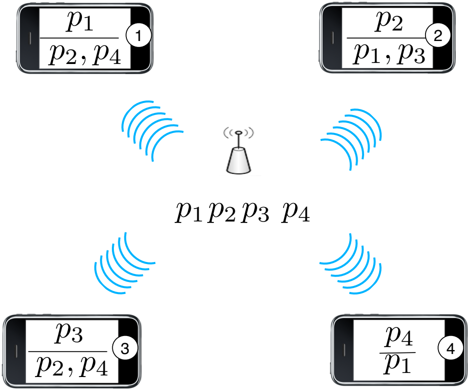



Keller et al. MicroCast: Cooperative Video Streaming on Smartphones. In Proceedings of MobiSys '12

# Index Coding Problem

# Index Coding Problem

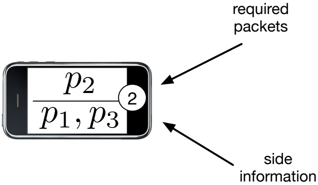
- A set of $m$ packets $P = \{p_1, \ldots, p_m\}$ needs to be delivered to $n$ clients $C = \{c_1, \ldots, c_n\}$




Y. Birk and T. Kol, *"Coding-on-demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients,"* INFOCOM 98.

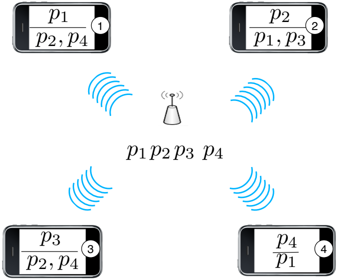
# Index Coding Problem (cont.)

- Each client $c_i \in C$ is associated with two subsets:
  - $W(c_i) \subseteq P$ - the "wants" set, i.e., the set of messages required by $c_i$.
  - $H(c_i) \subseteq P$ - the "has" set, i.e., the set of messages available at $c_i$ (side information)



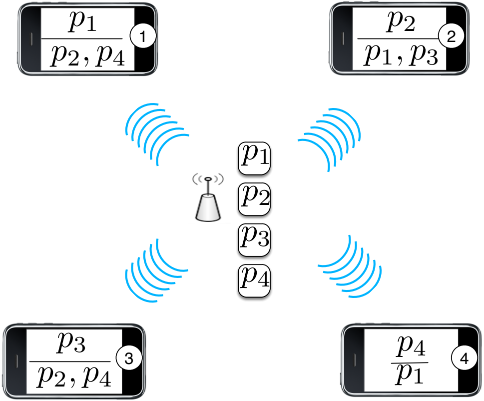
# Index Coding Problem

- The server uses a lossless broadcast channel
- Each packet is a combination of packets
- Goal: find an encoding scheme that satisfies all clients with minimum number of transmissions.



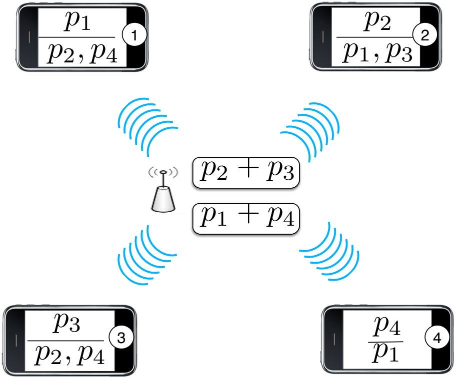
# Index Coding Problem

- Option 1: transmit four uncoded packets

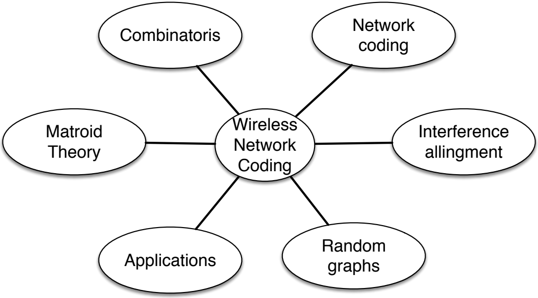


# Index Coding Problem

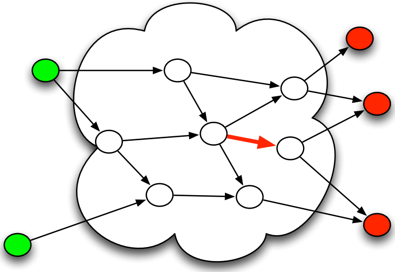
- Option 1: transmit four uncoded packets
- Option 2: mix packets to take advantage of available side information



# Wireless Network Coding and Related Areas



# Relation between Index and Network Coding

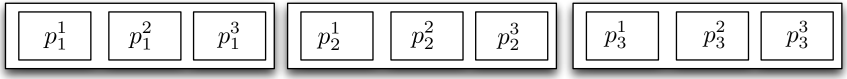


- All links have an infinite capacity except for the bottleneck link

H. Maleki, V. Cadambe, S. Jafar “Index Coding- An Interference Alignment Perspective.”

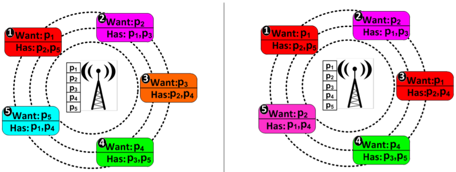
# Linear Solution

- If $\Sigma$ is a field and the encoding and decoding functions are linear we say that the instance has a $(k, \mu)$-linear solution over $\Sigma$.
- If, in addition, $k = 1$ we say that the instance has a $(1, \mu)$-scalar linear solution over $\Sigma$.
- $\frac{k}{\mu}$ - transmission rate
- $\mu' = \frac{\mu}{k}$ - normalized number of transmissions



# Multiple Unicast vs. Multiple Multicast

- Multiple unicast - each packet is requested by a single client
- Multiple multicast (groupcast) - a packet can be requested by several clients
- Equivalence for linear coding has recently been established by Maleki et al.

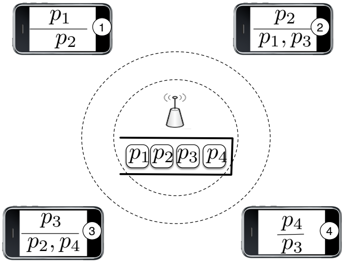


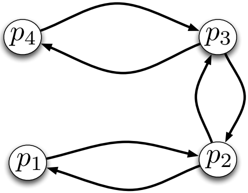

Multiple Unicast

Multiple Multicast

# Multiple Unicast case

- Dependency (side information) graph $G$



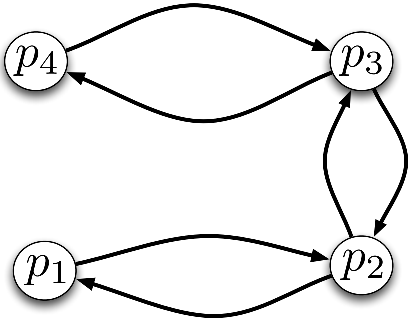

- $(i, j)$ is an edge iff $c_i$ knows the value of $p_i$

# Dependency Graph

- Maximum Induced Acyclic Subgraph ($MAIS(G)$) as the maximum acyclic induced subgraph of $G$.
- Observation:

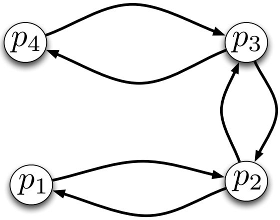
$$\mu \geq |MAIS(G)|$$

$$\mu' \geq |MAIS(G)|$$



# Multiple Unicast case

- $A_G$- the adjacency matrix for $G$, $A_G = \begin{bmatrix} 1 & X & 0 & 0 \\ X & 1 & X & 0 \\ 0 & X & 1 & X \\ 0 & 0 & X & 1 \end{bmatrix}$
- $\begin{bmatrix} u_1 \\ \dots \\ u_r \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
- Client $c_i$ can decode from $p_1 + p_2$ (row 1) since it knows $p_2$ and $p_4$



# Multiple Unicast case

- $A_G$- the adjacency matrix for $G$,
- $\begin{bmatrix} u_1 \\ \dots \\ u_r \end{bmatrix}$ - basis for $\mathrm{rows}(A_G + I)$, sending $\begin{bmatrix} u_1 \\ \dots \\ u_r \end{bmatrix} \begin{bmatrix} p_1 \\ \dots \\ p_k \end{bmatrix}$
- Decoding

$$((A_G + I) \cdot P)_i = p_i + \sum_{j \in N_G^+(i)} p_j$$

  hence $c_i$ can decode $p_i$
- Conclusion $\mu \leq \mathrm{rank}_q(A_G + I)$
- For any spanning subgraph $H \subseteq G$, it holds that $\mu \leq \mathrm{rank}_q(A_H + I)$

# Min-Rank problem

- Given a matrix
  - Non-zero diagonal
  - Do-not cares
  - All other entries are zeros
- Minimize the rank of the matrix

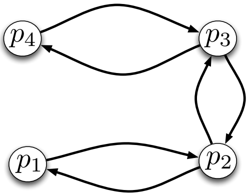
| | $p_1$ | $p_2$ | $p_3$ | $p_4$ |
|---|---|---|---|---|
| $p_1$ | 1 | X | | X |
| $p_2$ | X | 1 | X | |
| $p_3$ | | X | 1 | X |
| $p_4$ | X | | X | 1 |

- $$OPT \leq \min_{H \subset G} \mathrm{rank}_q(A_H + I) =: \mathrm{minrk}_q(G)$$
- $\mathrm{minrk}_q(G)$ - the optimal size of scalar linear code over $GF(q)$

# Minimum Rank Problem

- Given a matrix
  - Non-zero diagonal
  - Do-not cares
  - All other entries are zeros
- Minimize the rank of the matrix

$$A_G = \begin{bmatrix} 1 & X & 0 & 0 \\ X & 1 & X & 0 \\ 0 & X & 1 & X \\ 0 & 0 & X & 1 \end{bmatrix}$$



# Min-Rank problem

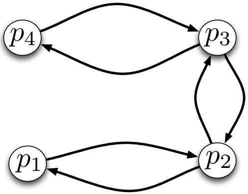
$$\begin{bmatrix} 1 & X & 0 & 0 \\ X & 1 & X & 0 \\ 0 & X & 1 & X \\ 0 & 0 & X & 1 \end{bmatrix}$$

$$OPT \leq \min_{A \text{ fits } G} \text{rank}_q(A) =: \text{minrk}_q(G)$$

- $\text{minrk}_q(G)$ - the optimal size of scalar linear code over $GF(q)$

# Scalar Linear Codes

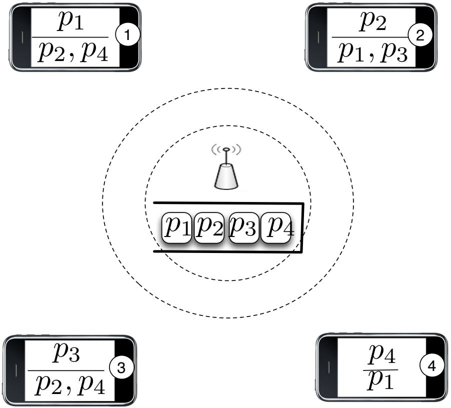
$$A_G = \begin{bmatrix} 1 & X & 0 & 0 \\ X & 1 & X & 0 \\ 0 & X & 1 & X \\ 0 & 0 & X & 1 \end{bmatrix}$$




$$OPT \leq \mathrm{minrk}_q(G)$$

$\mathrm{minrk}_q(G)$ - the optimal size of scalar linear code over $GF(q)$

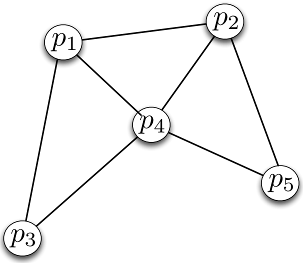
# Relation to Min-Rank problem




| | $p_1$ | $p_2$ | $p_3$ | $p_4$ |
|---|---|---|---|---|
| $p_1$ | 1 | X | | X |
| $p_2$ | X | 1 | X | |
| $p_3$ | | X | 1 | X |
| $p_4$ | X | | | 1 |

# Dependency Graph - Acyclic Case

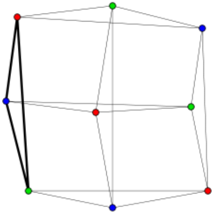
- $\alpha(G)$ - independence number of $G$
- $\bar{\chi}(G)$ - clique-cover number of $G$

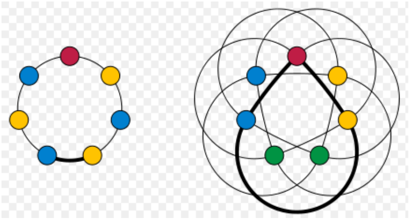



$$\alpha(G) \le \mu' \le \mu = \mathrm{minrk}_q(G) \le \mathrm{minrk}_2(G) \le \bar{\chi}(G)$$

# Special cases

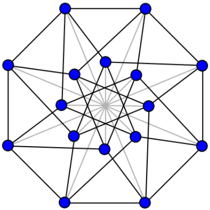
- For certain types of graphs $\mu = \mathrm{minrk}_2(G)$
  - Perfect graphs
  - Odd holes (odd-length cycles of length at least 5)
  - Odd anti-holes (complements of odd holes)





# Impact of field size

- There exists a family of graphs such that
  - $\mathrm{minrk}_2(G) \geq n^{1-\epsilon}$
  - $\mathrm{minrk}_p(G) \leq n^{\epsilon}$
- Using Ramsey graphs for the construction.



Lubetzky, E. and Stav, U. 2007. Non-Linear Index Coding Outperforming the Linear Optimum.

N. Alon, The Shannon capacity of a union

# Linear vs. Non-linear

- Theorem: There exists an explicit family of index coding instances with $n$ messages and some fixed $\epsilon > 0$ such that the non-linear rate is $\Omega(n^{\epsilon})$ times larger than the linear rate.

---

Blasiak, R. Kleinberg, and E. Lubetzky, Lexicographic Products and the Power of Non- Linear Network Coding, Proc. of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011).

# Index Coding Complexity

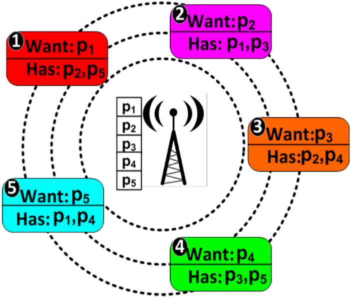
- Let $\frac{k}{\mu}$ be an optimal rate, then
- Finding an approximation solution of rate $\alpha\frac{k}{\mu}$ is "hard" for any constant $\alpha \leq 1$
  - Finding such codes would solve a long-standing problem in graph coloring
  - Relies on the Unique Game Conjecture
- Result applies to scalar linear, vector linear, and non-linear encoding functions

---

M. Langberg and A. Sprintson. "On the Hardness of Approximating the Network Coding Capacity", IEEE Transactions on Information Theory, vol. 57, no.2, pp.1008-1014, Feb. 2011

# Complimentary Index Coding

- Goal: Maximize the number of transmission, i.e., $n - \mu$
  - Maximize the benefit obtained by employing the network coding technique.




$$p_1 + p_2$$
$$p_3 + p_4$$
$$p_5$$

  - Two transmissions are "saved" in this scenario.

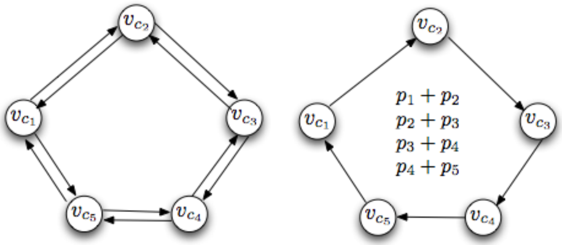
# Complimentary Index Coding

- Clearly, the problem is NP-hard
- Multiple unicast
  - Approximation ratios of $\Omega(\sqrt{n} \cdot \log n \log\log n)$ and $\Omega(\log n \cdot \log\log n)$ for scalar and vector linear solutions, respectively.
- Multiple Multicast
  - NP-hard to find an approximate solution

Chaudhry, Sprintson, Langberg, "On the Complementary Index Coding Problem."

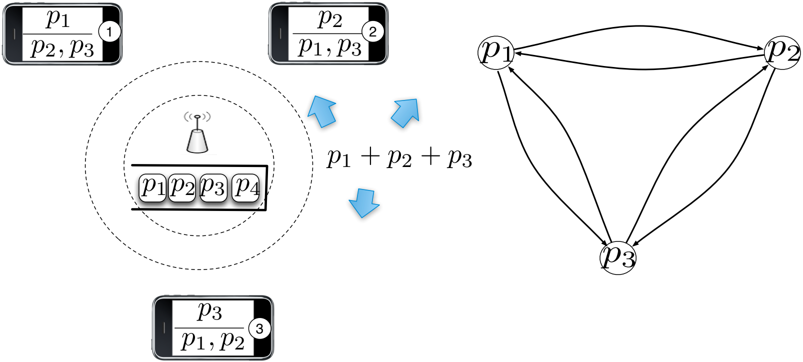
# Complimentary Index Coding

- Intuition: a cycle in the dependency graph allows to “save” one transmission
- Feedback vertex set provides an upper bound on the maximum number of “saved” transmissions
- Finding vertex-disjoint cycle packing can result in an approximate solution.



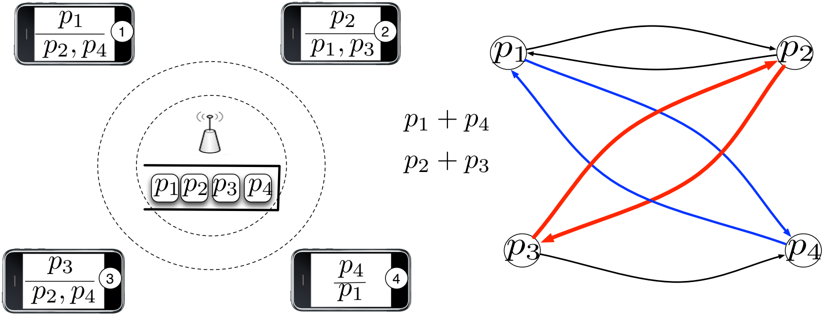
# Heuristic approaches

- Observation: All nodes in a clique can be satisfied by one transmission



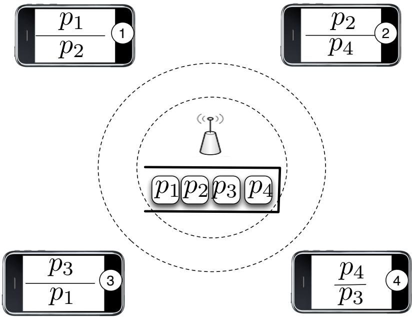
# Heuristic: minimum clique cover

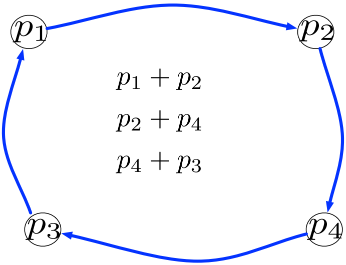
- Find a minimal set of cliques that cover all nodes in the network



# Heuristic: maximum cycle cover

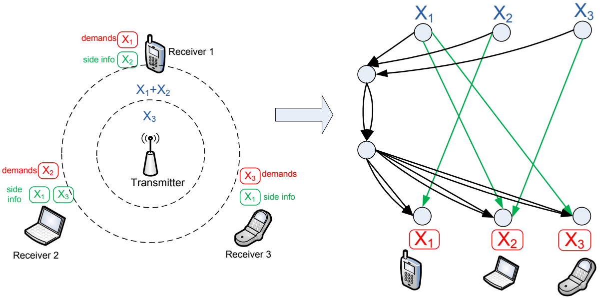
- Each cycle allows to "save" one transmission



# Relation between Index and Network Coding

# Equivalence to Linear Network Coding

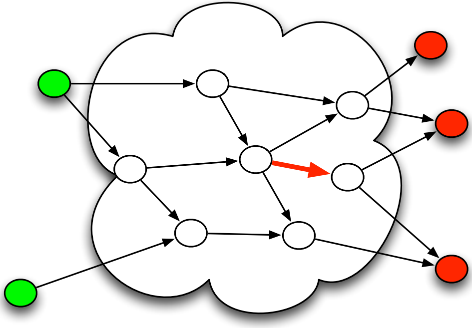



## Theorem

*Given a network $\mathcal{N}$ with $m$ edges, there exists an instance of the Index Coding problem $\mathcal{I}(\mathcal{N})$ such that $\mathcal{N}$ admits a vector linear network code of dimension $n$ over $GF(q)$ iff $\mathcal{I}(\mathcal{N})$ has an optimal linear index code with the same properties and consisting of $nm$ transmissions.*

S. El Rouayheb, A. Sprintson and C. N. Georghiades, "*On the Relation Between the Index Coding and the Network Coding Problems,*" ISIT, 2008

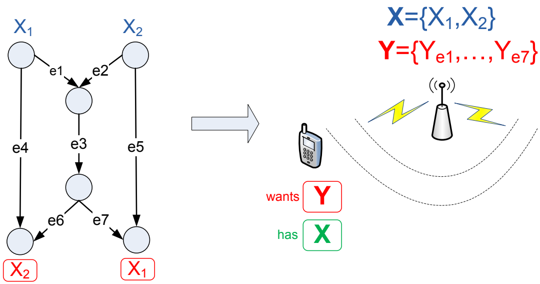
# Relation between Index and Network Coding



- All links have an infinite capacity except for the bottleneck link

H. Maleki, V. Cadambe, S. Jafar “Index Coding- An Interference Alignment Perspective.”

# Reduction technique

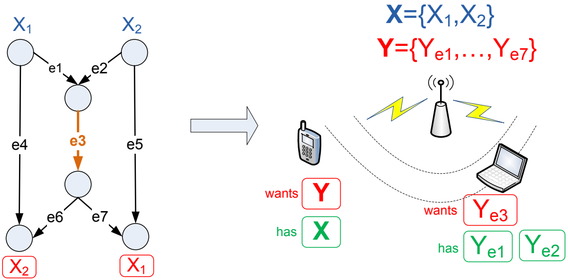



- Transmitter has two sets of sources $X$ and $Y$
- The first receiver makes the Index Code "diagonalizable", and can be put in the following form:

$$Y_{e1} + f_{e1}(X), Y_{e2} + f_{e2}(X), \dots, Y_{e7} + f_{e7}(X)$$

- We want to show that each function $f_{ei}$ can be used in the network code as the encoding function on edge $e_i$

# Sketch of Proof

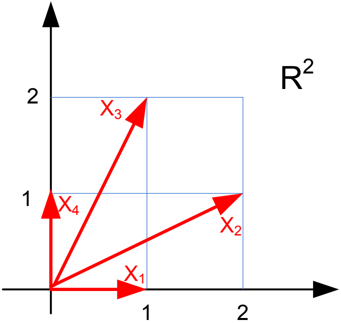



- For each network edge, we add a new receiver
- This receiver will used the first three transmitted signals, i.e.

$$Y_{e1} + f_{e1}(X), Y_{e2} + f_{e2}(X) \text{ and } Y_{e3} + f_{e3}(X)$$

- He can decode $Y_{e3}$ only if $f_{e3}(X)$ is a linear combination of $f_{e1}(X)$ and $f_{e2}(X)$

# Properties of Linear Independence




| Linearly Independent Subsets |
| --- |
| $\{X_1\}, \{X_2\}, \{X_3\}, \{X_4\}$<br>$\{X_1, X_2\}, \{X_1, X_3\}, \{X_2, X_3\}$<br>$\{X_2, X_4\}, \{X_3, X_4\}$ |

The linearly independent sets satisfy the following conditions:

- If $A$ is ind. and $A' \subseteq A$, then $A'$ is ind.
- $A$, $B$ ind. and $|A| < |B|$,then $\exists e \in B \setminus A$ s.t. $A \cup \{e\}$ is ind.

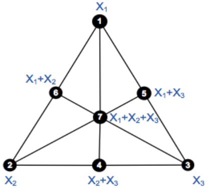
# Matroids as Abstraction of Linear Independence

A matroid $\mathcal{M}(E, \mathcal{I})$ is a couple formed by:

- A finite set $E$, called ground set of the matroid
- A collection $\mathcal{I}$ of subsets of $E$ s.t:

1. (I1) $\emptyset \in \mathcal{I}$
2. (I2) If $A \in \mathcal{I}$ and $A' \subseteq A$, then $A' \in \mathcal{I}$
3. (I3) $A, B \in \mathcal{I}$ and $|A| < |B|$,then $\exists e \in B \setminus A$ s.t. $A \cup \{e\} \in \mathcal{I}$

A subset of $E$ that belongs to $\mathcal{I}$ is called independent; otherwise it is called dependent.




Linear Representation of the Non-Fano Matroid over $GF(3)$.

$X_1, X_2, X_3$ canonical basis of $GF(3)^3$

### Definition

A matroid $\mathcal{M}(E, \mathcal{I})$ of rank $k$ is linearly representable over a field $\mathbb{F}$ if

- There exists a set $S$ of vectors in $\mathbb{F}^k$
- And a bijection $\phi : E \to S$ s.t. $\forall A \subseteq E$, $A \in \mathcal{I} \Leftrightarrow \phi(A)$ is linearly independent

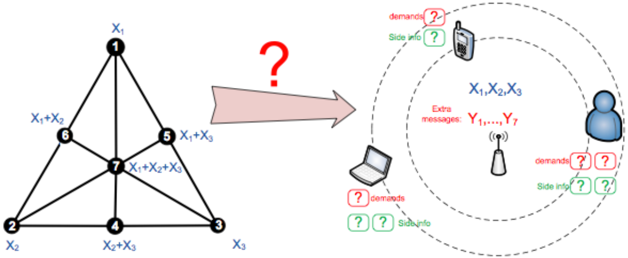
# Reduction from Matroids

- Given a matroid, we build a network that reflects ALL the matroid dependencies and independencies
- Let $\mathcal{M}(Y, \mathcal{I})$ be a matroid
- We construct an instance of the Index Coding problem $\mathcal{N}(\mathcal{M})$ s.t.

**Theorem**

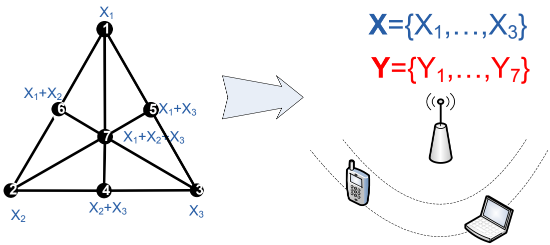
*The network $\mathcal{N}(\mathcal{M})$ has a vector linear network code of dimension $n$ over $GF(q)$ iff the matroid $\mathcal{M}$ has an $n$-linear representation over the same field.*

# Proof Idea

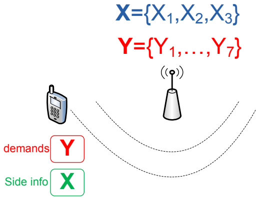



- Build a reduction from the Matroid representation problem to the Index Coding problem
- Add extra messages in the Index Coding problem to gain more degrees of freedom

# Proof Outline: Transmitter




- Let $\mathcal{M}(Y, r)$ be a matroid of rank $k$ where $Y = \{Y_1, \ldots, Y_m\}$
- In the equivalent Index Coding Problem, the transmitter has two sets of messages
  1. $X = \{X_1, \ldots, X_k\}$ corresponding to the matroid representation
  2. $Y = \{Y_1, \ldots, Y_m\}$ extra messages corresponding to the matroid ground set

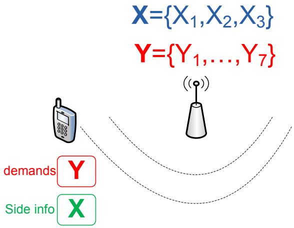



Optimal Index Code:

$$g_1(X,Y) = a_{11}X_1 + a_{12}X_2 + a_{13}X_3 + b_{11}Y_1 + \cdots + b_{17}Y_7$$
$$g_2(X,Y) = a_{21}X_1 + a_{22}X_2 + a_{23}X_3 + b_{21}Y_1 + \cdots + b_{27}Y_7$$
$$\vdots$$
$$g_7(X,Y) = a_{71}X_1 + a_{72}X_2 + a_{73}X_3 + b_{71}Y_1 + \cdots + b_{77}Y_7$$

- We add a receiver having the set $X$ as side info and demanding the messages in $Y$
- A lower bound on the number of transmissions is then $|Y| = 7$
- This receiver is able to decode $Y$ iff Matrix $[a_{ij}]$ is invertible

# Proof Outline: Diagonal Form




Optimal Index Code:

$$g'_1(X,Y) = Y_1 + \underbrace{c_{11}X_1 + c_{12}X_2 + c_{13}X_3}_{f_1(X)}$$

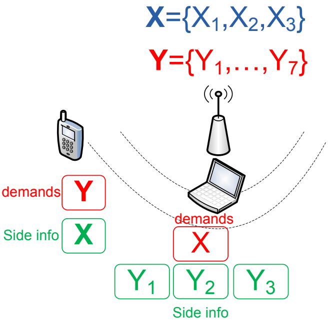
$$g'_2(X,Y) = Y_2 + \underbrace{c_{21}X_1 + c_{22}X_2 + c_{23}X_3}_{f_2(X)}$$

$$\vdots$$

$$g'_7(X,Y) = Y_7 + \underbrace{c_{71}X_1 + c_{72}X_2 + c_{73}X_3}_{f_7(X)}$$

- We want to show that the functions $f_i(X)$ give a linear representation of the matroid

# Proof Outline: Independent Sets




Index Code:

~~$Y_1$~~ + $f_1(X)$

~~$Y_2$~~ + $f_2(X)$

~~$Y_3$~~ + $f_3(X)$

.

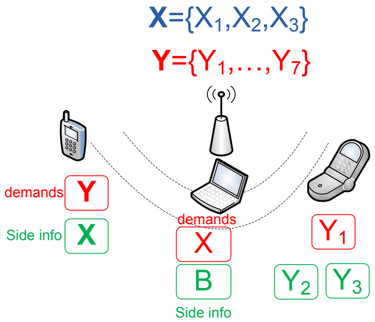
.

.

$Y_7 + f_7(X)$

- Let $B = \{Y_1, Y_2, Y_3\} \subseteq Y$ be a base
- The corresponding receiver can get $f_1(X), f_2(X), f_3(X)$ from the transmitted signals
- He can decode the $X$'s iff $f_1(X), f_2(X), f_3(X)$ are linearly independent

# Proof Outline: Dependent Sets




Index Code:

$Y_1 + f_1(X)$

$Y_2 + f_2(X)$

$Y_3 + f_3(X)$

.

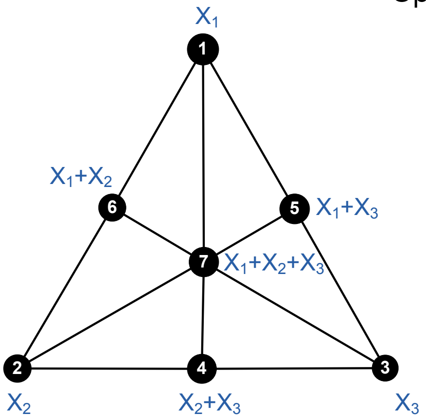
.

.

$Y_7 + f_7(X)$

- $C \subseteq Y$ is a dependent set.
- For example, let $C = \{Y_1, Y_2, Y_3\}$
- The corresponding receiver can decode $f_2(X)$ and $f_3(X)$
- He can decode $Y_1$ only iff $f_1(X)$ is a linear combination of $f_2(X)$ and $f_3(X)$

# Example

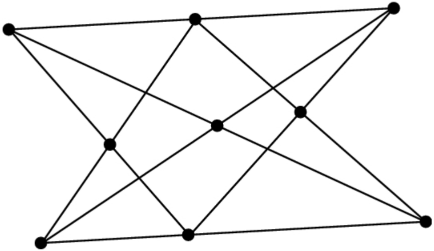



Optimal Index Code:

$$Y_1 + X_1$$
$$Y_2 + X_2$$
$$Y_3 + X_3$$
$$Y_4 + X_2 + X_3$$
$$Y_5 + X_1 + X_3$$
$$Y_6 + X_1 + X_2$$
$$Y_7 + X_1 + X_2 + X_3$$

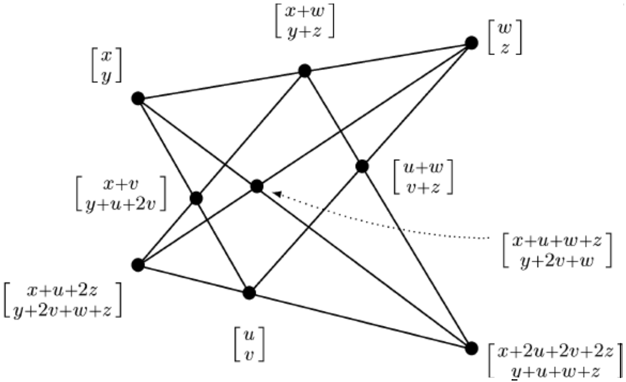
# Applications

- A reduction for a non-Pappus matroid can be used to show that vector linear coding outperforms scalar coding



S. El Rouayheb, A. Sprintson, and C. Georghiades, “On the Index Coding Problem and Its Relation to Network Coding and Matroid Theory,”

# Example: The Non-Pappus Matroid




The Non-Pappus matroid is not linearly representable but has a 2-linear representation over $GF(3)$

F. Matus, *"Matroid representations by partitions"*, Discrete Mathematics, 1999

# Leveraging reduction, it can be shown that:

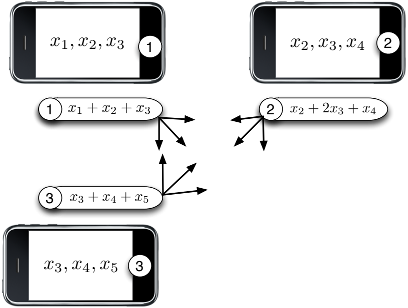
1. Vector linear codes have better performance than scalar codes for certain instances of the index coding problem.
2. Effros et al. showed equivalence between network and index codes for general (non-linear) encoding and decoding functions.
    1. Any efficient scheme that solves the index coding problem can be used for solving the more general network coding problem.

M. Effros, S. El Rouayheb, and M. Langberg, “An equivalence between network coding and index coding,” ISIT’13

# Cooperative Data Exchange

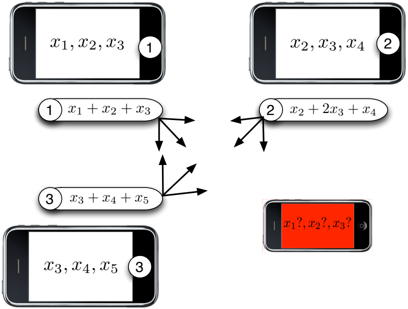
# Cooperative Data Exchange Problem

- Clients need to share their local packets with other clients
- Clients use a lossless broadcast channel
- One packet or function of packet is broadcasted at each time slot.



# Eavesdropper

- Wants to obtain information about packets held by the clients
- Has access to any data transmitted over the broadcast channel



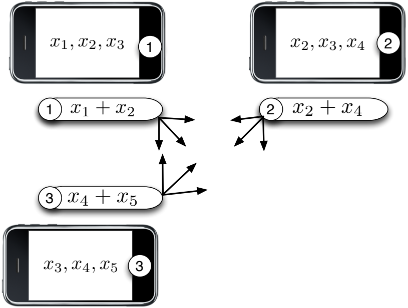
# Weak Security

- $X = \{X_i\}$: set of original packets
- $P = \{P_i\}$: transmitted packets
  - Packet $P_i$ is a linear combination of packets in $X$
- Strong security requirement

$$I(X; P) = 0$$

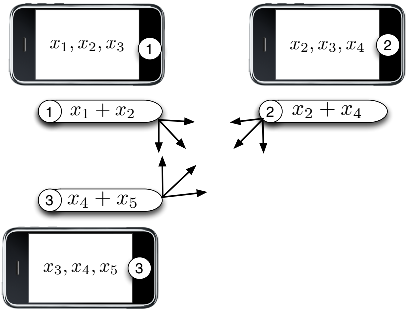
- Weak security requirement

$$I(X_i; P) = 0$$



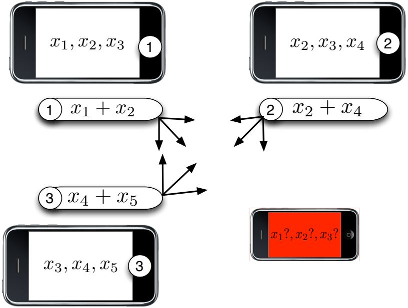
# $g$-weak Security

- Strong security requirement $I(X; P) = 0$
- Weak security requirement $I(X_i; P) = 0$
- $g$-weak security: for each subset $S$ of $X$ of size $g$ or less it holds that
$$I(S; P) = 0$$



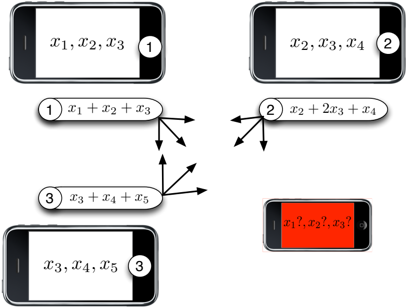
# Example

- Eavesdropper can only get value of $x_1 + x_2$, $x_2 + x_4$, and $x_4 + x_5$,
  - cannot get value of the original packets $x_1, \cdots, x_4$
  - this solution is 1-weakly secure



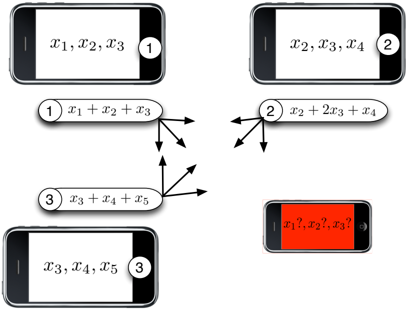
# Example (cont.)

- Eavesdropper cannot obtain a combination of any two original packets
- This solution is 2-weakly secure



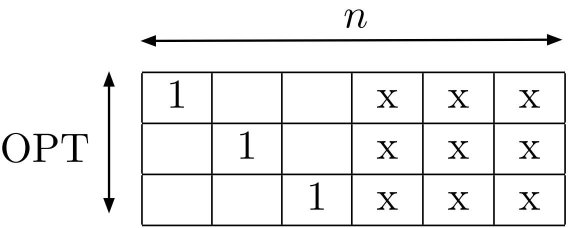
# Adversary with prior side information

- If an eavesdropper that has access to at most $g-1$ packets, it will not be able to obtain any additional packets



# Matrix completion problem

- $n$ columns, $OPT$ rows
- Goal: construct a code that maximizes minimum distance
- There are well-known construction, e.g., Reed-Solomon codes
- Optimal code (MDS) achieves $n - OPT + 1$



# Matrix completion problem

- Our case: constraints on the code construction
  - Due to the side information available at the clients
- When is it possible to complete the matrix so it will satisfy the MDS condition?
  - When it does not contain an all zero submatrix of size $a \times b$, such that $a + b \geq OPT + 1$

$n$

OPT

| | | | | | |
|---|---|---|---|---|---|
| x | x | 0 | 0 | x | x |
| 0 | 0 | x | x | x | x |
| x | x | x | x | 0 | 0 |

# Matrix completion problem

- If an all zero submatrix of size $a \times b$, such that $a + b \geq OPT + 1$ exists, then it is not possible to complete the matrix to MDS

OPT-1 (rows 2–3), 2 (columns 1–2)

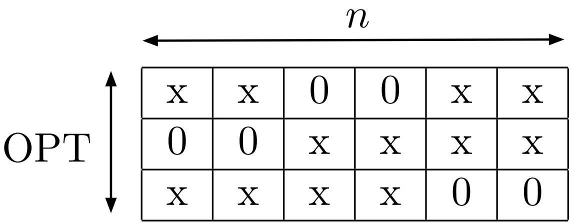
| | | | | | |
|---|---|---|---|---|---|
| x | x | 0 | 0 | x | x |
| 0 | 0 | x | x | x | x |
| 0 | 0 | x | x | x | x |

1 (column 1), OPT-1 (rows 1–3)

| | | | | | |
|---|---|---|---|---|---|
| 0 | x | 0 | x | x | x |
| 0 | x | x | x | 0 | x |
| 0 | 0 | x | x | x | x |

# Matrix completion problem

- Our case: constraints on the code construction
  - Due to the side information available at the clients
- Random code works with high probability
  - Hard to check since finding a minimum distance is an NP-hard problem



# Theorem

- Can achieve the distance

$$n - OPT + 1$$

  - with high probability at least $1 - \binom{n}{OPT} \frac{OPT}{q}$
  - requires field size $\binom{q>n}{OPT} OPT$

$n$

OPT

| | | | | | |
|---|---|---|---|---|---|
| x | x | 0 | 0 | x | x |
| 0 | 0 | x | x | x | x |
| x | x | x | x | 0 | 0 |

# Deterministic algorithm

- Use matrix completion
  - Fill $i^{th}$ entry of the matrix with a value if $GF(2^i) \subset GF(2^{i-1})$
  - Determinant of any $OPT \times OPT$ matrix is guaranteed to be full rank

$n$ (columns) × OPT (rows)

| | | | | | |
|---|---|---|---|---|---|
| x | x | 0 | 0 | x | x |
| 0 | 0 | x | x | x | x |
| x | x | x | x | 0 | 0 |

# Structured Codes

- Can we use standard codes, e.g., Reed-Solomon
- Then, perform a linear transformation to complete the matrix?
- Generalized Reed-Solomon code

$$G = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\mu-1} & \alpha_2^{\mu-1} & \dots & \alpha_n^{\mu-1} \end{bmatrix}.$$

# Structured Codes

- Can we use standard codes, e.g., Reed-Solomon
- Then, perform a linear transformation to complete the matrix?
- Generalized Reed-Solomon code

$$\begin{bmatrix} X & X & X & X & 0 & 0 \\ X & X & 0 & 0 & X & X \\ 0 & 0 & X & X & X & X \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 & \alpha_6^2 \end{bmatrix}$$

- Unfortunately, the transformation matrix is not guaranteed to be full-rank

# Negative example

- A negative example:

$$\begin{bmatrix} 0 & 0 & \alpha^5 & \alpha^5 & \alpha^4 & \alpha^4 \\ \alpha & \alpha & 0 & 0 & \alpha^3 & \alpha^3 \\ \alpha^6 & \alpha^6 & \alpha^2 & \alpha^2 & 0 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & \alpha^3 & \alpha^3 \\ 1 & \alpha^6 & \alpha^6 \\ 1 & \alpha^5 & \alpha^5 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 \\ \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha & \alpha^3 \end{bmatrix}$$

$\alpha$: primitive element of $GF(8)$ with primitive polynomial $x^3 + x + 1$

# Randomized algorithm

- Idea: use Randomized Reed-Solomon code
- The code will work with high probability
- Key: Show that matrix $T$ is not identically equal to zero.

$$\begin{bmatrix} X & X & X & X & 0 & 0 \\ X & X & 0 & 0 & X & X \\ 0 & 0 & X & X & X & X \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 & \alpha_6^2 \end{bmatrix}$$

# Conjecture

- If the configuration matrix can be completed to MDS,
  - i.e., it does not contain a zero submatrix of dimension $a \times b$ such that $a + b \geq OPT + 1$
- Then the determinant of $T$ is not identically equal to zero

$$\begin{bmatrix} X & X & X & X & 0 & 0 \\ X & X & 0 & 0 & X & X \\ 0 & 0 & X & X & X & X \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 & \alpha_6^2 \end{bmatrix}$$

# Conclusion

- Fascinating research field
  - Requires methods and tools from different areas
- Establishing connections between different research problems
- Structural solutions vs. randomized algorithms
- Impact on practical applications