A network coding tutorial

Tracey Ho
Center for the Mathematics of Information
California Institute of Technology
Introduction – Network Coding

- Generalization of traditional store & forward
- Information can be operated on in network, not just transported
- Powerful framework for considering theoretical and operational issues in networking

“...a fresh and sharp tool that has the potential to open up stagnant fundamental areas of research”

– Dr. Ralf Koetter, the Network Coding Home Page
A multicast example
A multicast example
A multicast example

[ACL Y00]
A multicast example

[ACL Y00]
1. Determining feasibility of a network connection problem

- non-multicast: ?
- multicast:
  - min-cut max-flow bound satisfied for each receiver [ACLY00]
  - transfer matrix \( A(I - F)^{-1}B_\beta^T \) for each receiver \( \beta \) is non-singular [KM01]
Algebraic network coding [KM01]

- Multi-source multicast
- Information transmitted as vectors of $n$ bits
- Coding in finite field $\mathbb{F}_{2^n}$

Data Stream

\[
\begin{array}{|c|c|c|}
\hline
\text{n bits} & \text{n bits} & \text{.} \\
\hline
\end{array}
\]

Element of $\mathbb{F}_{2^n}$
Algebraic network coding [KM01]

$Y_j \rightarrow v \rightarrow Y_k$

Coefficients $\{a_{i,j}, f_{l,j}, b_{\beta i,l}\}$ give network-constrained transfer matrices $(A, F, \{B\}_{\beta})$, a network code.

$M_{\beta} = A(I - F)^{-1}B^T_{\beta}$ gives transfer function from sources to outputs [KM01]:

\[
\begin{bmatrix}
X_1 \\
X_2 \\
. . . \\
X_r
\end{bmatrix}
\overset{M_{\beta}}{\rightarrow}
\begin{bmatrix}
Z_{\beta,1} \\
Z_{\beta,2} \\
. . . \\
Z_{\beta,r}
\end{bmatrix}
\]
Algebraic network coding [KM01]

$Y_j \rightarrow Y_k$

source $X_i$
originating at $v$

$g \beta \rightarrow$
receiver

$\beta = a_{i,l} X_i + f_{j,l} Y_j + f_{k,l} Y_k$

$g \beta$ output

$Z_{\beta,i} = b_{\beta i,k} Y_j + b_{\beta i,k} Y_k$

$\{a_{i,j}, f_{l,j}, b_{\beta i,l}\}$
Coefficients give network-constrained transfer matrices ($A, F, \{B_{\beta}\}$), a network code

$M_{\beta} = A(I - F)^{-1}B_{\beta}^T$
Matrix gives transfer function from sources to outputs [KM01]:

$[X_1 \ X_2 \ldots X_r] M_{\beta} = [Z_{\beta,1} \ Z_{\beta,2} \ldots Z_{\beta,r}]$
Algebraic network coding [KM01]

source $X_i$
originating at $v$

$Y_i = a_{i,l} X_i + f_{j,l} Y_j + f_{k,l} Y_k$

Matrix $M_\beta = A (I - F)^{-1} B^T$ gives transfer function from sources to outputs [KM01]:

\[
\begin{bmatrix}
X_1 \\
X_2 \\
\vdots \\
X_r
\end{bmatrix}
\times
\begin{bmatrix}
Z_{\beta,1} \\
Z_{\beta,2} \\
\vdots \\
Z_{\beta,r}
\end{bmatrix}
\]
Algebraic network coding [KM01]

Y_j \rightarrow Y_k \quad \text{source } X_i \\
\quad \text{originating at } v \\
Y_i = a_{i,l} X_i + f_{j,l} Y_j \\
\quad + f_{k,l} Y_k \\

Y_j \rightarrow Y_k \quad \text{receiver } \beta 

\frac{\text{Coefficients } \{a_{i,j}, f_{l,j}, b_{\beta i,k}\}}{\text{give network-constrained transfer matrices } (A, F, \{B_{\beta}\}), \text{ a network code}} \\

M_{\beta} = A(I - F)^{-1}B_{\beta}^{T} \\
\text{gives transfer function from sources to outputs [KM01]:} \\
\begin{bmatrix}
X_1 \\
X_2 \\
\vdots \\
X_r
\end{bmatrix} \\
M_{\beta} = \\
\begin{bmatrix}
Z_{\beta,1} \\
Z_{\beta,2} \\
\vdots \\
Z_{\beta,r}
\end{bmatrix}
Algebraic network coding [KM01]

\[ Y_j \rightarrow Y_k \text{ source } X_i \text{ originating at } v \]

\[ Y_l = a_{i,l}X_i + f_{j,l}Y_j + f_{k,l}Y_k \]

\[ Y_j \rightarrow Y_k \text{ receiver } \beta \]

Output \[ Z_{\beta,i} = b_{\beta,i,k}Y_j + b_{\beta,i,k}Y_k \]
Algebraic network coding [KM01]

- Coefficients \{a_{i,j}, f_{l,j}, b_{\beta_{i,l}}\} give network-constrained transfer matrices \((A, F, \{B_{\beta}\})\), a network code
- Matrix \(M_{\beta} = A(I - F)^{-1}B_{\beta}^T\) gives transfer function from sources to outputs [KM01]:

\[
[X_1 \ X_2 \ldots X_r] M_{\beta} = [Z_{\beta,1} \ Z_{\beta,2} \ldots Z_{\beta,r}]
\]
Algebraic network coding [KM01]

- Coefficients \( \{a_{i,j}, f_{l,j}, b_{\beta_i,l}\} \) give network-constrained transfer matrices \((A, F, \{B_\beta\})\), a network code.

- Matrix \( M_\beta = A(I - DF)^{-1}B_\beta^T \) gives transfer function from sources to outputs [KM01]:

\[
\begin{bmatrix}
X_1 & X_2 & \cdots & X_r
\end{bmatrix}
\begin{bmatrix}
M_\beta
\end{bmatrix}
= 
\begin{bmatrix}
Z_{\beta,1} & Z_{\beta,2} & \cdots & Z_{\beta,r}
\end{bmatrix}
\]
1. Determining feasibility of a network connection problem

- non-multicast: ?
- multicast:
  - min-cut max-flow bound satisfied for each receiver [ACLY00]
  - transfer matrix \( A(I - F)^{-1}B^T_\beta \) for each receiver \( \beta \) is non-singular [KM01]
2. Types of network codes needed

- multicast: linear [LY03], algebraic [KM01] sufficient
- non-multicast: nonlinear codes may be needed [DFZ04]
3. Constructing linear multicast network codes

Centralized

- general graphs: set code coefficient values sequentially, keeping the transfer matrix determinant polynomial nonzero [KM01]
- acyclic graphs: consider subgraph consisting of flow solutions to individual receivers [SET03, JCJ03]
  - set coefficient values in ancestral ordering, maintaining a full rank “frontier set” for each receiver

Decentralized

- general graphs: randomized linear network coding [HKMKE03]
- acyclic graphs, two sources: subtree decomposition and token distribution [FSS04]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03,JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
Polynomial-time deterministic construction for acyclic graphs [SET03, JCJ03]
3. Constructing linear multicast network codes

Centralized

- general graphs: set code coefficient values sequentially, keeping the transfer matrix determinant polynomial nonzero [KM01]
- acyclic graphs: consider subgraph consisting of flow solutions to individual receivers [SET03, JCJ03]
  - set coefficient values in ancestral ordering, maintaining a full rank “frontier set” for each receiver

Decentralized

- general graphs: randomized linear network coding [HKMKE03]
- acyclic graphs, two sources: subtree decomposition and token distribution [FSS04]
Distributed random linear network coding

- Interior network nodes independently choose random linear mappings from inputs to outputs
- Coefficients of aggregate effect communicated to receivers

\[
\begin{align*}
y_j &= 2X_1 + X_2 \\
[2 & 1 0]
\end{align*}
\]
Distributed random linear network coding

- Interior network nodes independently choose random linear mappings from inputs to outputs
- Coefficients of aggregate effect communicated to receivers

\[
\begin{align*}
X_1 & \rightarrow \ X_2 \quad \text{with} \quad y_j = 2X_1 + X_2 \\
\quad & \rightarrow \ X_3 \\
& \quad \text{and} \quad y_k = X_2 \\
& \quad \text{with} \quad \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}
\end{align*}
\]

\[
\begin{align*}
\begin{bmatrix} 2 & 1 & 0 \end{bmatrix} &\begin{bmatrix} 3X_3 + 2y_j + y_k \\
3[0 0 1] + 2[2 1 0] + [0 1 0] = [4 3 3]
\end{align*}
\]
Distributed random linear network coding

- Interior network nodes independently choose random linear mappings from inputs to outputs
- Coefficients of aggregate effect communicated to receivers

\[
\begin{align*}
X_1 & \rightarrow X_1 \\
X_2 & \rightarrow X_2 \\
X_3 & \rightarrow \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} + 2 \begin{bmatrix} 2 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 3 & 3 \end{bmatrix}
\end{align*}
\]

- Receiver nodes can decode if they receive as many independent linear combinations as the number of source processes
Success probability

Theorem (HKMKE03, HMSEK03). For a feasible $d$-receiver multicast connection problem on a network with

- independent or linearly correlated sources
- a network code in which code coefficients $a_{i,j}$, $f_{i,j}$ for $\eta$ links are chosen independently and uniformly over $\mathbb{F}_{q}$

the success probability is at least $(1 - d/q)^{\eta}$ for $q > d$.

Error bound is of the order of the inverse of the field size $q = 2^{n}$, so error probability decreases exponentially with codeword length $n$. 
4. Choosing a minimum-cost coding subgraph

- Suppose each link \((a, b)\) has cost \(C_{ab}(g_{ab})\) and capacity \(R_{ab}\)
- linear or convex optimization

Minimize \(\sum_{ab} C_{ab}(g_{ab})\) subject to

\[
\lambda_i = \sum_b f_{ib}^{\beta} - \sum_a f_{ai}^{\beta} \quad \forall \ i, \beta \neq i
\]

\[
\sum_i \lambda_i = \sum_a f_{a\beta}^{\beta} \quad \forall \ \beta \in T
\]

\[
0 \leq f_{ab}^{\beta} \leq g_{ab} \leq R_{ab} \quad \forall \ a, b, \beta \in T
\]

where \(\lambda_i\) is the source rate at node \(i\)
5. Throughput advantage of network coding

- directed wired networks, multicast: $O(\log |V|)$ [SET03]
- directed wired networks, multiple unicasts: $O(|V|)$ [LL04]
- undirected wired networks, multicast: 2 [LL04]
- undirected wired networks, multiple unicasts: conjectured to be 1 [LL04]
Throughput advantage in directed wired networks, multicast [SET03]
Throughput advantage in directed wired networks, multicast [SET03]

- coding rate: $h$
- routing rate: $2$

Proof:
- suppose source tries to send $2n$ symbols $b_1, \ldots, b_{2n}$ in $n$ steps
- at most $2hn$ symbols can be sent to relay nodes in $n$ steps
- let $U_i$ be the subset of relay nodes receiving $b_i$
- since $U_1 + \ldots U_{2n} \leq 2hn$, there is an $i$ for which $|U_i| \leq h$
- any sink not connected to a node in $U_i$ does not receive $b_i$
Throughput advantage in directed wired networks, multiple unicasts [LL04]
6. Network coding in wireless

- Additional elements to consider:
  - Dependence of topology on transmit powers, medium access, etc.
  - Wireless multicast advantage

- Network coding can offer advantages in throughput and energy:

\[
\begin{align*}
&w \\
&t & b_1 & u \\
&w & b_2 & w \\
&y & b_1 & z \\
&z & b_2 & u \\
&y & b_1 + b_2 & z
\end{align*}
\]
7. Complexity advantage of network coding

- Multicast throughput:
  - integral/fractional routing: integral/fractional Steiner tree packing (NP complete)
  - network coding: P

- Minimum-energy multicast/broadcast:
  - routing: NP complete
  - network coding: P [LMHK04]
Applications of network coding

Network capacity / optimization

- Achieving capacity [ACLY00]
- Minimizing cost/energy [WCK04,LMHK04]
- Distributed compression [HMEK04]

Network operations

- Analysis of network management [HMK02]
- Error correction [CY02a]
- Decentralized robust network operation [HKMKE03]

Network security

- Wiretapping [CY02b]
- Byzantine fault detection [HLKMEK04]
Decentralized robust network operation using randomized network coding

- Decentralized scenarios

<table>
<thead>
<tr>
<th>Receiver position</th>
<th>(2,4)</th>
<th>(4,4)</th>
<th>(8,10)</th>
<th>(10,10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Randomized flooding upper bound</td>
<td>0.563</td>
<td>0.672</td>
<td>0.667</td>
<td>0.667</td>
</tr>
<tr>
<td>Randomized Coding $F_{26}$ lower bound</td>
<td>0.882</td>
<td>0.827</td>
<td>0.604</td>
<td>0.567</td>
</tr>
<tr>
<td>$F_{28}$ lower bound</td>
<td>0.969</td>
<td>0.954</td>
<td>0.882</td>
<td>0.868</td>
</tr>
</tbody>
</table>

- Online algorithms in dynamically varying environments
- Experimental demonstration on ISP graphs [CWJ03]
**Byzantine security**

- Robustness against faulty/malicious components with arbitrary behavior, e.g.
  - dropping packets
  - misdirecting packets
  - sending spurious information
- Abstraction as Byzantine generals problem [LSP82]
- Byzantine robustness in networking [P88, MR97, KMM98, CL99]
Byzantine detection with network coding

Distributed randomized network coding can be extended to detect Byzantine behavior

- Small computational and communication overhead
  - small number of hash bits included with each packet, calculated as simple polynomial function of data

- Require only that a Byzantine attacker does not design and supply modified packets with complete knowledge of other nodes’ packets
Byzantine modification detection scheme

- Suppose each packet contains $\theta$ data symbols $x_1, \ldots, x_\theta$ and $\phi \leq \theta$ hash symbols $y_1, \ldots, y_\phi$
- Consider the function $\pi(x_1, \ldots, x_k) = x_1^2 + \cdots + x_{k+1}^k$, and set

$$
\begin{array}{c|c|c|c}
1 & k & 2k \\
\hline
x_1 & x_2 & \cdots \\
\hline
\pi & \pi & \pi \\
\downarrow & \downarrow & \downarrow \\
y_1 & y_2 & y_3
\end{array}
$$

where $k = \left\lceil \frac{\theta}{\phi} \right\rceil$ is a design parameter trading off overhead against detection probability
Detection probability

Theorem (HLKMEK04). If the receiver gets $s$ genuine packets, then the detection probability is at least $1 - \left( \frac{k+1}{q} \right)^s$.

- E.g. With 2% overhead ($k = 50$), code length=7, $s = 5$, the detection probability is 98.9%.
- with 1% overhead ($k = 100$), code length=8, $s = 5$, the detection probability is 99.0%.
Distributed compression of correlated sources

- Distributed randomized network coding can remove or add redundancy according to network capacity
Background – Slepian-Wolf

- Separate encoding of two correlated sources for a single receiver

- Achievable rate region found by Slepian and Wolf, 73

- Error exponents for linear coding found by Csiszar, 82
Coding and decoding

• randomized linear network coding over vectors of bits in $\mathbb{F}_2$

$$Y_{ncj}^i \rightarrow Y_{ncj}^j \rightarrow Y_{ncj}^k$$

source $X_i$ originating at $v$

$$Y_{ncl}^i = \Upsilon_{1,3}X_{ni}^i + \Psi_{1,3}Y_{ncj}^i + \Psi_{2,3}Y_{ncj}^j$$

• receivers perform minimum entropy or maximum a posteriori probability decoding
Distributed compression problem

Consider

- two sources of rates $r_1, r_2$ whose output values in each unit time period are i.i.d. with distribution $Q$.
- linear network coding in $\mathbb{F}_2$ over vectors of $nr_i$ bits from each source

Define

- $m_1$ and $m_2$ the min cut capacities between the receiver and each source respectively
- $m_3$ the min cut capacity between the receiver and both sources
- $L$ the maximum source-receiver path length
Theorem (HMEK04). The error probability at each receiver using minimum entropy or maximum a posteriori probability decoding is at most $\sum_{i=1}^{3} p_{e}^i$, where

$$p_{e}^i \leq \exp \left\{ -n \min_{X_1, X_2} \left( D(P_{X_1 X_2} || Q) + m_i \left( 1 - \frac{1}{n} \log L - H(X_i | X_{\bar{i}}) \right) \right) + 2^{r_1 + r_2 + r_i} \log(n + 1) \right\} \text{ for } i = 1, 2$$

$$p_{e}^3 \leq \exp \left\{ -n \min_{X_1, X_2} \left( D(P_{X_1 X_2} || Q) + m_3 \left( 1 - \frac{1}{n} \log L - H(X_1 X_2) \right) \right) + 2^{2r_1 + 2r_2} \log(n + 1) \right\}$$

- Generalizes error exponents for linear Slepian-Wolf coding [Csi82]
Conclusions

• Network coding is potentially useful in many aspects of practical and theoretical networking

• Multicast in wired networks is well understood (algebraic codes suffice, efficient algorithms for constructing optimal solutions)

• Advantages exist for non-multicast, wireless settings, but many interesting questions remain
Further work

- Richer wireless network models: variable rates, correlated link variations
- Distributed, adaptive resource optimization and scheduling algorithms for networks with concurrent multicast and unicast connections
- Use of network coding in conjunction with signal combination or cooperation at the physical layer
The End

- My web page: http://www.mit.edu/~trace
- Network coding homepage: http://www.networkcoding.info
Proof outline

• Recall transfer matrix \( M_\beta = A(I - F)^{-1}B_\beta^T \) for each receiver \( \beta \) must be non-singular

• We show an equivalent condition connected with bipartite matching: the Edmonds matrices

\[
\begin{bmatrix}
A & 0 \\
I - F & B_\beta^T
\end{bmatrix}
\]

(in the acyclic delay-free case) or

\[
\begin{bmatrix}
A & 0 \\
I - DF & B_\beta^T
\end{bmatrix}
\]

(in the case with delays) are non-singular

• This shows that if \( \eta \) links have random coefficients, the determinant polynomial
  – has maximum degree \( \eta \) in the random variables \( \{a_{x,j}, f_{i,j}\} \)
  – is linear in each of these variables
Proof outline (cont’d)

• We want the product of the $d$ receivers’ determinant polynomials to be nonzero

• We can show inductively, using the Schwartz-Zippel Theorem, that for any polynomial $P \in \mathbb{F}[\xi_1, \xi_2, \ldots]$ of degree $\leq d\eta$, in which each $\xi_i$ has exponent at most $d$, if $\xi_1, \xi_2, \ldots$ are chosen independently and uniformly at random from $\mathbb{F}_q \subseteq \mathbb{F}$, then $P = 0$ with probability at most $1 - (1 - d/q)^\eta$ for $d < q$

• Particular form of the determinant polynomials gives rise to a tighter bound than the Schwartz-Zippel bound for general polynomials of the same total degree
Improvement with spare capacity

Theorem. Consider multicasting independent or linearly correlated sources of joint entropy rate $r$ on an acyclic graph with minimum redundancy $y$, i.e. deletion of any $y$ links in the network preserves feasibility. At any receiver, successful reception occurs with probability at least

$$\sum_{x=r}^{r+y} \binom{r+y}{x} \left(1 - \frac{1}{q}\right)^L x \left(1 - \left(1 - \frac{1}{q}\right)^L\right)^{r+y-x}$$

where $L$ is the longest source-receiver path in the network.

- Proof uses Theorem ??
Analysis

• Let $M$ be the matrix whose $i^{th}$ row $m_i$ represents the concatenation of the data and corresponding hash value for packet $i$

• Suppose the receiver tries to decode using
  – $s$ unmodified packets, represented as $C_a [M|I]$, where the $i^{th}$ row of the coefficient matrix $C_a$ is the vector of code coefficients of the $i^{th}$ packet
  – $r - s$ modified packets, represented by $[C_b M + V | C_b]$, where $V$ is an arbitrary matrix
Analysis (cont’d)

• Let $C = \begin{bmatrix} \frac{C_a}{C_b} \end{bmatrix}$

• Decoding is equivalent to pre-multiplying the matrix

$$
\begin{bmatrix}
C_aM & C_a \\
C_bM + V & C_b
\end{bmatrix}
$$

with $C^{-1}$, which gives

$$
\begin{bmatrix}
M + C^{-1} \begin{bmatrix} 0 \\ V \end{bmatrix} & I
\end{bmatrix}
$$

• Consider any fixed $C_b$ and $V$. Since the receiver decodes only when it has a full rank set of packets, possible values of $C_a$ are such that $C$ is non-singular
Analysis (cont’d)

We can show that

- for each of $\geq s$ packets, the attacker knows only that the decoded value will be one of $q^{\text{rank}(V)}$ possibilities

$$\left\{ m_i + \sum_{j=1}^{\text{rank}(V)} \gamma_{i,j} u_j \mid \gamma_{i,j} \in \mathbb{F}_q \right\}$$

- at most $k + 1$ out of the $q$ vectors in a set $\{ u + \gamma v \mid \gamma \in \mathbb{F}_q \}$, where $u = (u_1, \ldots, u_{k+1})$ is a fixed length-$(k+1)$ vector and $v = (v_1, \ldots, v_{k+1})$ a fixed nonzero length-$(k+1)$ vector, can satisfy the property that the last element of the vector equals the hash of the first $k$ elements.
Outline

• Network coding tutorial
• Randomized linear network coding
  – Decentralized robust network operation
  – Byzantine fault detection
  – Distributed compression [HMEK04]
Outline of proof of Theorem 48

- Error probability $\leq \sum_{i=1}^{3} p_e^i$, where
  - $p_e^i$, $i = 1, 2$, is the probability of error in $X_i$ only
  - $p_e^3$ is the probability of error in both $X_1, X_2$

- Proof approach using method of types similar to that in [Csi82]

- Type $P_x$ of a vector $x$ is the empirical distribution of elements in the vector

- Bound error probabilities by summing over sequences of different joint types $P_{X_1\tilde{X}_1X_2\tilde{X}_2}$
Proof outline (cont’d)

• probability of source vector of type $(x_1, x_2) \in \mathcal{X}_1 \mathcal{X}_2$

$$Q^n(x_1x_2) = \exp\{-n(D(P_{X_1X_2}||Q) + H(X_1X_2))\}$$

• decoding conditions
  – minimum entropy decoder:

$$H(\tilde{X}_1\tilde{X}_2) \leq H(X_1X_2)$$

  – maximum a posteriori probability decoder:

$$D(P_{\tilde{X}_1\tilde{X}_2}||Q) + H(\tilde{X}_1\tilde{X}_2) \leq D(P_{X_1X_2}||Q) + H(X_1X_2)$$
Proof outline (cont’d)

• Define
  
  - $P_i, i = 1, 2$, the probability that $(x_i, x_i^c), (\tilde{x}_i, x_i^c)$, where $x_i \neq \tilde{x}_i$, give the same signals at the receiver
  
  - $P_3$, the probability that $(x_1, x_2), (\tilde{x}_1, \tilde{x}_2)$, where $x_1 \neq \tilde{x}_1, x_2 \neq \tilde{x}_2$, give the same signals at the receiver

• Two distinct input values are mapped to the same value on a link of capacity $c$ with probability $\frac{1}{2n^c}$

• We can show by induction on the minimum cut capacities $m_i$ that

$$P_i \leq \left(1 - (1 - \frac{1}{2^n})^L\right)^{m_i} \leq \left(\frac{L}{2^n}\right)^{m_i}$$
Proof outline (cont’d)

Bound error probabilities by summing over

- sets of joint types

\[
P^i_n = \left\{ \begin{array}{l}
\{ P_{X_1 \tilde{X}_1 X_2 \hat{X}_2} \mid \tilde{X}_1 \neq X_1, \hat{X}_2 = X_2 \} \quad i = 1 \\
\{ P_{X_1 \tilde{X}_1 X_2 \hat{X}_2} \mid \tilde{X}_1 = X_1, \hat{X}_2 \neq X_2 \} \quad i = 2 \\
\{ P_{X_1 \tilde{X}_1 X_2 \hat{X}_2} \mid \tilde{X}_1 \neq X_1, \tilde{X}_2 \neq X_2 \} \quad i = 3 
\end{array} \right.
\]

where \( X_i, \tilde{X}_i \in \mathbb{F}_2^{mr_i} \)

- sequences of each type

\[
\mathcal{T}_{X_1 X_2} = \left\{ \begin{bmatrix} x_1 & x_2 \end{bmatrix} \in \mathbb{F}_2^{n(r_1+r_2)} \mid P_{x_1 x_2} = P_{X_1 X_2} \right\}
\]

\[
\mathcal{T}_{\tilde{X}_1 \tilde{X}_2} | X_1 X_2(x_1 x_2) = \left\{ \begin{bmatrix} \tilde{x}_1 & \tilde{x}_2 \end{bmatrix} \in \mathbb{F}_2^{n(r_1+r_2)} \mid P_{\tilde{x}_1 \tilde{x}_2} = P_{\tilde{X}_1 \tilde{X}_2} \right\}
\]

\[
P_{\tilde{x}_1 \tilde{x}_2 x_1 x_2} = P_{\tilde{X}_1 \tilde{X}_2 X_1 X_2}
\]
Proof outline (cont’d)

We also use the cardinality bounds

$$|\mathcal{P}_n^1| < (n + 1)^{2^{2r_1+r_2}}$$

$$|\mathcal{P}_n^2| < (n + 1)^{2^{r_1+2r_2}}$$

$$|\mathcal{P}_n^3| < (n + 1)^{2^{2r_1+2r_2}}$$

$$|\mathcal{I}_{X_1X_2}| \leq \exp\{nH(X_1X_2)\}$$

$$|\mathcal{I}_{\tilde{X}_1\tilde{X}_2|X_1X_2}(x_1x_2)| \leq \exp\{nH(\tilde{X}_1\tilde{X}_2|X_1X_2)\}$$
Distributed random routing scheme RR:

- The source node sends one process in both directions on one axis and the other process in both directions along the other axis.

- A node receiving information on one link sends the same information on its three other links (these are nodes along the grid axes passing through the source node).

- A node receiving signals on two links sends one of the incoming signals on one of its two other links with equal probability, and the other signal on the remaining link.

The probability that a receiver located at grid position \((x, y)\) relative to the source receives both source processes is at most

\[
\frac{1 + 2|x - y| + 1(4\min(|x|, |y|) - 1 - 1)/3}{2|x| + |y| - 2}
\]
Distributed random coding scheme RC:

- The source node sends one process in both directions on one axis and the other process in both directions along the other axis.

- A node receiving information on one link sends the same information on its three other links.

- A node receiving signals on two links sends a random linear combination of the source signals on each of its two other links.

The probability that a receiver located at grid position \((x, y)\) relative to the source can decode both source processes is at least 

\[(1 - 1/q)^2(x+y-2).\]