Codes for networks

Ralf Koetter
ralf.koetter@tum.de
Codes for networks

Ralf Koetter
ralf.koetter@tum.de

Collaborators:
M. Medard, M. Effros, D. Traskov, D. Lun, N. Ratnakar,
F. Kschischang, R. Yeung, T. Lutz, M. Thakur, G. Zeitler .....
Acknowledgements:


A channel is a probabilistic device with input and output alphabet $A, R$ and a “channel law” $p(Y|X)$. 

\[ X \in C \subset A^n \quad \text{Channel} \quad Y \in R^n \]
Codes for networks:

A code for a network reduces the network to a channel, capturing the end-to-end characteristics of the network.
- wireline, wireless
- errors, erasures
- packet switched networks
- network coded or not?
Outline of the talk

-- Network coding
-- Modeling network coded networks as “channels”
-- Codes for networks
-- Metrics and constructions
-- Some consequences
Wireless Network Coding..
Wireless Network Coding...
Wireless Network Coding...
Wireless Network Coding
Wireless Network Coding
Wireless Network Coding

BETTER IS...
Wireless Network Coding

BETTER IS....
Wireless Network Coding

BETTER IS....this! Three channel uses only
Network Coding

The wireless situation
The wireless situation — congested areas in the network are better utilized: packets use “car pooling”
Network coding.... the standard example

The wireless butterfly (two-way relay channel)

The “butterfly” example
IEEE-IT, vol. 46, pp 1204-1216, 2000
Some categories

The (to date) three forms of network coding:

- **Combinatorial network coding**
  
  R. Dougherty, C. Freiling, K. Zeger, 
  Insufficiency of linear coding in network 
  information flow, IEEE-IT 
  
  field size, structure of networks, 
  matroidal solutions, entropic vectors, 
  
  “....diabolically constructed networks....”  
  (M.Sudan)

- **Opportunistic network coding for medium access**

S. Katti, H. Rahul, W.Hu, D. Katabi, M. 
Medard, J. Crowcroft 
XORs in The Air: Practical Wireless 
Network Coding

exploiting dynamic and localized multicast opportunities, 
protocol issues, how proactive can we do this,.....
The (to date) three forms of network coding:

- **Combinatorial network coding**
  
  R. Dougherty, C. Freiling, K. Zeger, Insufficiency of linear coding in network information flow, IEEE-IT
  
  field size, structure of networks, matroidal solutions, entropic vectors,
  
  “....diabolically constructed networks....”
  (M.Sudan)

- **Opportunistic network coding for medium access**

S. Katti, H. Rahul, W.Hu, D. Katabi, M. Medard, J. Crowcroft
XORs in The Air: Practical Wireless Network Coding

exploiting dynamic and localized multicast opportunities, protocol issues, how proactive can we do this,.....
The (to date) three forms of network coding:

- **Combinatorial network coding**
  
  R. Dougherty, C. Freiling, K. Zeger, 
  Insufficiency of linear coding in network information flow, IEEE-IT
  
  field size, structure of networks, 
  matroidal solutions, entropic vectors, 
  “....diabolically constructed networks....”
  (M.Sudan)

- **Opportunistic network coding for medium access**

  S. Katti, H. Rahul, W.Hu, D. Katabi, M. Medard, J. Crowcroft
  XORs in The Air: Practical Wireless Network Coding
  
  exploiting dynamic and localized multicast opportunities, 
  protocol issues, how proactive can we do this,.....
Random linear network coding

In random network coding (multicast, gossip content distribution, distributed storage, broadcast) the information packets are interpreted as vectors over a finite field which are linearly combined with randomly chosen coefficients from that field. The approach will achieve the capacity region of the network with high probability.

All operations at network nodes are assumed linear!

\[
Y(e_3) = \sum_i \alpha_i X(v, i) + \sum_{j=1,2} \beta_j Y(e_j)
\]

\[
Z(v, j) = \sum_{j=1}^n \epsilon_j Y(e_j).
\]

Note that in random network coding the choice of code and operation of each node is chosen completely decentralized and does not require any centralized management!
The defining property of network coding is that nodes in a network are allowed to form outgoing symbols from incoming symbols in any way — not only time-multiplexing of data streams.

⇒

The goal of network coding is to provide a receiver $R$ with enough evidence to solve an inference problem concerning the data that it wants to receive $⇒ H(X_R|Y_R) = 0$" is the goal

Network coding breaks with the transportation model:

A bit is not a car!
We consider coding on packet erasure networks

A prototype toy example:

End-to-end coding (LT codes) achieves a “throughput” of \((1-\epsilon)^2\)
“Classically” one would decode and re-encode at the center node.
- long latency
- potentially significant complexity

Random network coding solution:

Random network coding also achieves the capacity of $1 - \epsilon$ without additional complexity or delay!
The network model with random linear network coding.

Packets \( \{p_1, p_2, \ldots, p_M\}, p_i \in F_q^N \) are injected and \( y_1, y_2, \ldots, y_L \) are received.

\[ y_j = \sum_{i=1}^{M} h_{j,i} p_i \]
The network model.

Packets \( \{ p_1, p_2, \ldots, p_M \} \), \( p_i \in F_q^N \) are injected, \( y_1, y_2, \ldots, y_L \) are received, also erroneous packets \( e_1, e_2, \ldots, e_t \) are injected.

\[
y_j = \sum_{i=1}^{M} h_{j,i} p_i + \sum_{t=1}^{T} g_{j,t} e_t
\]
The network model....

\[ y = Hp + Ge \]

- \( p \) is an \( M \times N \) matrix over \( F_q \) whose rows are \( p_1, p_2, \ldots, p_M \).
- \( e \) is an \( T \times N \) matrix over \( F_q \) whose rows are \( e_1, e_2, \ldots, e_T \).
- \( H \) is a random \( L \times M \) matrix over \( F_q \).
- \( G \) is a random \( L \times T \) matrix over \( F_q \).

\[ y_j = \sum_{i=1}^{M} h_{j,i} p_i + \sum_{t=1}^{T} g_{j,t} e_t \]
Any single error $e_i$ is likely to distort every output $y_j$. 

$F_q$-linear MIMO network:

$$y = Hp + Ge$$
Any single error $e_i$ is likely to distort every output $y_j$.

A random matrix $H$ leaves the row-space of matrix $p$ unchanged.

$=>$

the only possibility to transmit information through such a channel is by encoding the information in the choice of the row-space generated by $p$. 

$y = Hp + Ge$
Modeling the end-to-end behavior of a network as a channel:

- a point-to-point connection (also multicast)

The dimension of $V$ may be smaller than the dimension of $U$. A loss in dimension occurs if some packets are dropped or the min-cut is just not sufficient.

In addition $V$ may contain an error space $E$ --- the equivalent of an additive error
Let $W$ be an $N$-dimensional vector space over $F_q^N$. (Transmitted and received packets are elements of $W$.)

Let $\mathcal{P}(W)$ denote the set of all subspaces of $W$ (sometimes called the projective geometry of $W$).

**Definition**

An *operator channel* associated with ambient space $W$ is a channel with input and output alphabet $\mathcal{P}(W)$. The channel input $V$ and channel output $U$ are related as

$$U = \mathcal{H}_k(V) \oplus E$$

where $\mathcal{H}_k$ is an erasure operator, $E \in \mathcal{P}(W)$ is an arbitrary error space and $\oplus$ denotes direct sum. If $\text{dim}(V) \leq k$, then $\mathcal{H}_k(V) = V$; otherwise $\mathcal{H}_k(V)$ acts to project $V$ onto a randomly chosen $k$-dimensional subspace of $V$. 
A distance for networks

Let $A$ and $B$ be subspaces of $W$.

The distance between $A$ and $B$ is defined as

$$d(A, B) := \dim(A + B) - \dim(A \cap B).$$

$d(A, B)$ is equal to the minimal number of insertions and deletions of generators that are required to transform a basis for $A$ into a basis for $B$.

(Analogous to Hamming distance in classical coding theory, which is equal to the minimum number of symbol changes required to transform a vector $A$ into a vector $B$.)
Definition

A code for an operator channel with ambient space $W \simeq F_q^N$ is a nonempty subset of $\mathcal{P}(W)$.

- The size of a code $\mathcal{C}$ is denoted $|\mathcal{C}|$.
- The minimum distance of $\mathcal{C}$ is denoted by
  \[ D(\mathcal{C}) = \min_{X,Y \in \mathcal{C}, X \neq Y} d(X,Y) \]
- The maximum dimension of elements of $\mathcal{C}$ is denoted by
  \[ \ell(\mathcal{C}) = \max_{X \in \mathcal{C}} \dim(X) \]

We say that $\mathcal{C}$ is a $q$-ary code of type $(N, \ell(\mathcal{C}), \log_q |\mathcal{C}|, D(\mathcal{C}))$. 
**Definition**

A *code* for an operator channel with ambient space $W \simeq F_q^N$ is a nonempty subset of $\mathcal{P}(W)$.

- The size of a code $\mathcal{C}$ is denoted $|\mathcal{C}|$.
- The minimum distance of $\mathcal{C}$ is denoted by
  $$D(\mathcal{C}) = \min_{X, Y \in \mathcal{C}, X \neq Y} d(X, Y)$$
- The maximum dimension of elements of $\mathcal{C}$ is denoted by
  $$\ell(\mathcal{C}) = \max_{X \in \mathcal{C}} \dim(X)$$

We say that $\mathcal{C}$ is a *q-ary code of type* $(N, \ell(\mathcal{C}), \log_q |\mathcal{C}|, D(\mathcal{C}))$.

**Definition**

A *minimum distance decoder* for $\mathcal{C}$ takes the output $U$ of an operator channel and returns a nearest codeword $V \in \mathcal{C}$, i.e., a codeword $V$ satisfying, for all $X \in \mathcal{C}$, $d(U, V) \leq d(U, X)$. 
Theorem

Assume we use a code $C$ for transmission over an operator channel. Let $V \in C$ be transmitted, and let

$$U = \mathcal{H}_k(V) \oplus E$$

be received, where $\dim(E) = t$. Let $\rho = (\ell(C) - k)_+$ denote the maximum number of erasures induced by the channel. If

$$2(t + \rho) < D(C),$$

then a minimum distance decoder for $C$ will produce the transmitted space $V$ from the received space $U$.

Proof: standard application of the triangle inequality.

Remark: “erasures” (i.e., deletion of desired dimensions) cost the same as “errors” (i.e., insertion of undesired dimensions).
Let $C$ be an $(N, \ell, \log_q |C|, D)$ code. Transmission of a basis for a codeword requires transmission of up to $N\ell$ $q$-ary symbols.

**Definition**

The *rate* of a $(N, \ell, \log_q |C|, D)$ code is

$$R = \frac{\log_q |C|}{N\ell}.$$

We also introduce the normalized parameters:

- the normalized weight: $\lambda = \ell/N \in [0, 1]$
- the normalized minimum distance $\delta = D/2\ell \in [0, 1]$
Example
(Classical “uncoded” network coding.)
Let $\mathcal{C}_1 \subset \mathcal{P}(W, \ell)$ be the set of spaces $U$ having a generator matrix of the form $[I|A]$, where $I$ is the $\ell \times \ell$ identity matrix.

This is a code of type $(N, \ell, \ell(N - \ell), 2)$ with normalized weight $\lambda = \ell/N$ and rate $R = 1 - \lambda$.

Example
(“uncoded” network coding with strictly more codewords.)
Let $\mathcal{C}_2$ be $\mathcal{P}(W, \ell)$ itself.

This is a code of type $(N, \ell, \log_q |\mathcal{P}(W, \ell)|, 2)$ with strictly more codewords than $\mathcal{C}_1$.

Example
(“uncoded” network coding with even more codewords)
Let $\mathcal{C}_3 = \bigcup_{i=1}^{\ell} \mathcal{P}(W, i)$. 

Let $F_q$ be a finite field and let $F$ be an extension field.

**Definition**

A polynomial $L(x) \in F[x]$ is called a *linearized polynomial* with respect to $F_q$ if

$$L(x) = \sum_{i=0}^{d} a_i x^{q^i}, \ a_i \in F.$$
We may regard any extension $K$ of $F$ as a vector space over $F_q$. The map taking $\beta \in K$ to $L(\beta) \in K$ is linear w.r.t. $F_q$, i.e., for all $\beta_1, \beta_2 \in K$ and all $\lambda_1, \lambda_2 \in F_q$, 

$$L(\lambda_1 \beta_1 + \lambda_2 \beta_2) = \lambda_1 L(\beta_1) + \lambda_2 L(\beta_2).$$

If $K$ is large enough to contain all the zeros of $L(x)$. The zeros of $L(x)$ then correspond to the kernel of $L(x)$ regarded as a linear map, and hence they form a subspace of $K$. Conversely, each subspace of $K$ corresponds to some linearized polynomial over $K$.

Roughly speaking . . .

linearized polynomials are to subspaces as polynomials are to points.
Setup:

$F_q$ is a finite field, $F = F_q^m$ is an extension field of $F_q$, regarded as a vector space of dimension $m$ over $F_q$. Let $\alpha_1, \ldots, \alpha_\ell \in F$ be a set of linearly independent elements, that span a vector space $A$ of dimension $\ell$ over $F_q$.

The User ...

... provides $k$ elements $u_0, u_1, \ldots, u_{k-1}$ in $F$; this is the message to be sent.
The Encoder . . .

. . . forms the linearized polynomial

\[ f(x) = \sum_{i=0}^{k-1} u_i x^{q^i} \]

and evaluates \( f(x) \) at the \( \ell \) points \( \alpha_1, \ldots, \alpha_\ell \) to form

\[ \beta(i) = f(\alpha_i), \ i = 1, \ldots, \ell. \]

The set of pairs \( (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_\ell, \beta_\ell) \) is clearly a set of linearly independent vectors in \( A \times F \cong F_q^{\ell+m} \), and so is a basis for a vector space \( V \) of dimension \( \ell \). (The ambient space \( W \) is \( F_q^{\ell+m} \).)

The Transmitter . . .

. . . sends (a basis for) \( V \) over the operator channel.
Each pair $\alpha_i, \beta_i$ may be regarded as a zero of the bivariate polynomial $y - f(x)$. In fact, since $f(x)$ is linearized, every element of $V$ is a zero of $y - f(x)$, since, for all $\lambda_1, \ldots, \lambda_\ell \in F_q$,

$$
\sum_{i=1}^{\ell} \lambda_i \beta_i - f \left( \sum_{i=1}^{\ell} \lambda_i \alpha_i \right) = \sum_{i=1}^{\ell} \lambda_i \beta_i - \sum_{i=1}^{\ell} \lambda_i f(\alpha_i)
$$

$$
= \sum_{i=1}^{\ell} \lambda_i (\beta_i - f(\alpha_i))
$$

$$
= 0
$$

which shows that $\sum_{i=1}^{\ell} \lambda_i (\alpha_i, \beta_i)$ is a zero of $y - f(x)$.

Each distinct message polynomial gives rise to a distinct codeword, hence $|C| = q^{mk}$. Thus $C$ is of type $(\ell + m, \ell, mk, D)$ with rate

$$
R = \frac{mk}{\ell(\ell + m)} = \frac{k}{\ell} \frac{m}{m + \ell}.
$$
Theorem

\[ D(C) = 2(\ell - k + 1) \]

Proof: Let \( U \) and \( V \) be two spaces obtained from distinct linearized polynomials \( f_1(x) \) and \( f_2(x) \), respectively. Suppose that \( U \cap V \) has dimension \( a \). This means it is possible to find \( a \) linearly independent elements \( (\alpha'_1, \beta'_1), (\alpha'_2, \beta'_2), \ldots, (\alpha'_a, \beta'_a) \) such that \( f_1(\alpha'_i) = f_2(\alpha'_i) = \beta_i \). It is easy to show that \( \alpha'_1, \ldots, \alpha'_a \) must themselves be linearly independent. If \( a \geq k \), then we would have two linearized polynomials of degree less than \( q^k \) that agree on \( a \) linearly independent points, which is only possible if the two polynomials coincide. Thus \( a \leq k - 1 \), so

\[ d(U, V) = 2(\ell - a) \geq 2(\ell - k + 1). \]
This construction yields codes of type \((\ell + m, \ell, mk, 2(\ell - k + 1))\). In terms of normalized parameters, we find that

\[
R = (1 - \lambda)(1 - \delta + \frac{1}{\lambda N})
\]

which has the same asymptotic behavior as the Singleton bound.
Suppose that $V$ is sent and $U$, a space of dimension $\ell'$ is received. Let $(x_i, y_i), i = 1, \ldots, \ell'$ be a basis for $U$. Decoding may proceed as follows.

1. Construct a bivariate interpolating polynomial

$$Q(x, y) = \Lambda(y) + \Omega(x)$$

such that $Q(x_i, y_i) = 0$ for $i = 0, \ldots, \ell'$ with $\Lambda(y)$ is a monic linearized polynomial of degree $q^t$ and $\Omega(x)$ is a linearized polynomial of degree at most $t + k - 1$, where $t = \lceil (\ell' - k)/2 \rceil$. [Such a polynomial can be proved to exist.]
2. Note that

\[
Q(x, f(x)) = \Lambda(x) \otimes f(x) + \Omega(x)
\]

\[
= \Lambda(y - f(x)) + Q(x, f(x)).
\]

If few enough errors occur, then \(Q(x, f(x))\) will have many zeros (more than its degree), and so \(Q(x, f(x))\) will be the zero polynomial, in which case \(Q(x, y) = \Lambda(y - f(x))\) will have \(y - f(x)\) as a factor.

3. \(f(x)\) can be recovered via a division operation in the ring of linearized polynomials, to recover \(f(x)\).
The operation of packet switched networks with packet erasures and/or errors can be handled with codes for the operator channel:

\[ U = \mathcal{H}_k(V) \oplus E \]

A Reed Solomon type code construction achieves the optimal trade-off between rate and error/erasure protection.

The complexity per information symbol behaves as \( O(\sqrt{n}) \) for packet size \( n \).

**Correspondences:**

<table>
<thead>
<tr>
<th>Classical channel</th>
<th>Operator Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C \subseteq F_q^n )</td>
<td>( C \subseteq \mathcal{P}(W) )</td>
</tr>
<tr>
<td>codeword ( c \in C )</td>
<td>codespace ( V \in C )</td>
</tr>
<tr>
<td>( \min d_H(c, c') )</td>
<td>( \max U \cap U' )</td>
</tr>
<tr>
<td>codelength ( n )</td>
<td>virtual code length ( q^n )</td>
</tr>
<tr>
<td>( t &lt; D/2 )</td>
<td>( t &lt; \text{depends on setup} )</td>
</tr>
</tbody>
</table>
More consequences of representing a network by $U = \mathcal{H}_k(V) \oplus E$

**Capacity:**
\[
C = \max_{p(V)} I(U;V)
\]

At a subspace dimension of $L$ and an error-space dimension of $T$ the capacity achieving distribution is a uniform density over $L$-$T$ dimensional subspaces of $N$-dimensional ambient space.

\[
C = \left(1 - \frac{L}{N}\right) \left(1 - \frac{T}{L}\right)
\]

If $k$ and $\text{dim}(E)$ are both random variables we can still compute the *capacity* of the network and the capacity achieving distribution. The interplay of $k$ and $L$ depends on the network in question.
More consequences of representing a network by

Networks and the broadcast channel

The network is statistically degraded if \( \dim(\bar{E}) \geq \dim(E) \) and \( \bar{k} \leq k \)

In this case the rate region is given as:

\[
R_2 \leq I(U, W) \quad R_1 \leq I(\bar{U} ; V | W) \\
\text{(under the usual characterizations of the r.v. } U, \bar{U}, V, W )
\]

This characterization includes priority transmission setups etc.
Constructing a two priority scheme

**Setup:**

\( F_q \) is a finite field, \( F = F_{q^m} \) is an extension field of \( F_q \), regarded as a vector space of dimension \( m \) over \( F_q \). Let \( \alpha_1, \ldots, \alpha_\ell \in F \) be a set of linearly independent elements, that span a vector space \( A \) of dimension \( \ell \) over \( F_q \).

**The User . . .**

. . . provides \( k \) elements \( u_0, u_1, \ldots, u_{k-1} \) in \( F \); this is the first part of the message to be sent.

**The User . . .**

. . . provides \( k' < k \) elements \( v_0, v_1, \ldots, v_{k'-1} \) in \( F \); this is the second part of the message to be sent.
The Encoder . . .

. . . forms the linearized polynomial

\[ f(x) = \sum_{i=0}^{k-1} u_i x^{q^i}, \quad f'(x) = \sum_{i=0}^{k'-1} v_i x^{q^i} \]

and evaluates \( f(x) \) and \( f'(x) \) at the \( \ell \) points \( \alpha_1, \ldots, \alpha_\ell \) to form

\[ \beta(i) = f(\alpha_i), \quad \gamma(i) = f'(\alpha_i) \quad i = 1, \ldots, \ell. \]

The set of pairs \( (\alpha_1, \beta_1, \gamma_1), (\alpha_2, \beta_2, \gamma_2), \ldots, (\alpha_\ell, \beta_\ell, \gamma_\ell) \) is clearly a set of linearly independent vectors in \( A \times F \cong F_{q^\ell+m} \), and so is a basis for a vector space \( V \) of dimension \( \ell \). (The ambient space \( W \) is \( F_{q^{\ell+m}} \).)

The Transmitter . . .

. . . sends (a basis for) \( V \) over the operator channel.
- The end-to-end characterization of a packet switched, network coded, erasure and/or error network leads to a characterization

\[ U = \mathcal{H}_k(V) \oplus E \]

-- This becomes a simple discrete memoryless channel with the set of subspaces of a vector space as in- and output alphabet

-- We can efficiently code for such a channel introducing a new coding problem

-- Furthermore this characterization of a network makes information theoretic concepts and multiterminal information theory applicable in a broader context
Thank you!
Network coding.... common assumptions

\( C(e) = 1 \) (links are noiseless and have the same capacity)
\( H(X_i) = 1 \) (sources have the same rate)
The \( X_i \) are mutually independent.

At nodes we implement deterministic functions.
Network coding... linear network coding

All operations at network nodes are assumed linear!

\[ Y(e_3) = \sum_i \alpha_i X(v, i) + \sum_{j=1,2} \beta_j Y(e_j) \]

\[ Z(v, j) = \sum_{j=1}^{n} \varepsilon_j Y(e_j). \]
Network coding... linear network coding

\[
\begin{align*}
Y(e_1) &= \alpha_{1,e_1}X_1 + \alpha_{2,e_1}X_2 \\
Y(e_2) &= \alpha_{1,e_2}X_1 + \alpha_{2,e_2}X_2 \\
Y(e_3) &= \beta_{e_1,e_3}Y(e_1) \\
Y(e_4) &= \beta_{e_1,e_4}Y(e_1) \\
Y(e_5) &= \beta_{e_2,e_5}Y(e_2) + \beta_{e_3,e_5}Y(e_3) \\
Z_1 &= \varepsilon_{e_4,1}Y(e_4) + \varepsilon_{e_5,1}Y(e_5) \\
Z_2 &= \varepsilon_{e_4,2}Y(e_4) + \varepsilon_{e_5,2}Y(e_5)
\end{align*}
\]
Network coding... linear network coding

In matrix form (after solving the linear system)

\[
\begin{pmatrix}
Z_1 \\
Z_2
\end{pmatrix}
= \begin{pmatrix}
\varepsilon_{e_4,1} & \varepsilon_{e_5,1} \\
\varepsilon_{e_4,2} & \varepsilon_{e_5,2}
\end{pmatrix}
\begin{pmatrix}
\beta_{e_1,e_4} & 0 \\
\beta_{e_1,e_3} & \beta_{e_3,e_5}
\end{pmatrix}
\begin{pmatrix}
\alpha_{1,e_1} & \alpha_{1,e_2} \\
\alpha_{2,e_1} & \alpha_{2,e_2}
\end{pmatrix}
\begin{pmatrix}
X_1 \\
X_2
\end{pmatrix}
\]

We define three matrices \( A, G, B \)

The main question becomes: Is \( G \) invertible?

We collect all parameters as: \( \underline{\xi} = (\xi_1, \xi_2, \ldots) = (\ldots, \alpha_{e,l}, \ldots, \beta_{e',e}, \ldots, \varepsilon_{e',j}, \ldots) \)
Network coding... linear network coding

\[ z = M \bar{x} = B \cdot G^T \cdot A \bar{x} \]

where the entries in \( B, G, A \) are functions of the weights \( \ldots, \alpha_{e,l}, \ldots, \beta_{e',e}, \ldots, \varepsilon_e \)

\[ \xi = (\xi_1, \xi_2, \ldots) = (\ldots, \alpha_{e,l}, \ldots, \beta_{e',e}, \ldots, \varepsilon_{e',j}, \ldots) \]

For acyclic networks the elements of \( G \) (and hence \( M \)) are polynomial functions in variables \( \xi = (\xi_1, \xi_2, \ldots) \)

⇒ an algebraic characterization of flows...
$C = \{(v, u_1, \mathcal{X}(v)), (v, u_2, \mathcal{X}(v)), \ldots, (v, u_K, \mathcal{X}(v))\}$

$M$ is a $|\mathcal{X}(v)| \times K|\mathcal{X}(v)|$ matrix.

$m_i(\xi) = \det(M_i(\xi))$

Choose the coefficients in $\mathbb{F}$ so that all $m_i(\xi)$ are unequal to zero.

Find a solution of $\prod_i m_i(\xi) \neq 0$
The “main” network coding theorem

* Assume we want to transmit a source with entropy rate $R$.

* The maximal entropy rate that we can generate at any receiver is equal to the min-cut between the source and this receiver.

* Using network coding functions that mix data efficiently enough we can achieve the maximal entropy rate simultaneously at each receiver.

The multicast capacity is determined by the min-cut in the network and is achievable with random network coding.
Random network coding

\[ Y(e_3) = \sum_i \alpha_i X(v, i) + \sum_{j=1,2} \beta_j Y(e_j) \]

\[ Z(v, j) = \sum_{j=1}^n \varepsilon_j Y(e_j). \]

Operations are over a finite field \( \mathbb{F}_{2^m} \) with randomly chosen coefficients. The compound effect of all the choices can be efficiently communicated in a packet header.
Random network coding

In random network coding for multicast, (content distribution, distributed storage, broadcast) the information packets are linearly combined with randomly chosen coefficients from a field. The approach will achieve the capacity region of the network with high probability.

Note that in random network coding the choice of code and operation of each node is chosen completely decentralized and does not require any centralized management!

- If every node in a network forwards random combinations of packets, we will flood the network with information.....

- If we can combine network coding with an efficient resource allocation scheme that only forwards information on properly chosen links with proper rates we can avoid the flooding problem

- Network optimization and the multicast...........................
Multicast and packing/flow problems

The original multicast problem has an interpretation as “random network coding”

Interpretation as packing of overlapping distribution trees

Interpretation as packing of overlapping source destination flows

We hence have a chance to formulate the multicast problem as a flow problem.....
Multicast and packing/flow problems

Utilizing the flow formulation we can solve a linear program:

**Minimize** the sum of cost-max flow product for each edge

**subject to:** Observe the flow conservation at intermediate network nodes for each receiver individually
An LP problem for the multicast

If we assume a proportional cost assignment we obtain the following LP

\[
\text{minimize } \sum_{(i,j) \in A} a_{ij} z_{ij} \\
\text{subject to } c_{ij} \geq z_{ij}, \quad \forall (i, j) \in A \\
z_{ij} \geq x_{ij}^{(t)} \geq 0, \quad \forall (i, j) \in A, \; t \in T \\
\sum_{\{j \mid (i, j) \in A\}} x_{ij}^{(t)} - \sum_{\{j \mid (j, i) \in A\}} x_{ji}^{(t)} = \sigma_i^{(t)}, \quad \forall i \in \mathcal{N}, \; t \in T
\]
What we achieved so far.....

- A main benefit of network coding is the formulation of the multicast problem as a problem of “overlapping packing of flows”

- This makes it possible to integrate network optimization and resource allocation techniques with multicast applications!

- The resulting linear (convex) programs can be efficiently solved by iterative distributed algorithms

- At the same time random network coding provides a way to construct the network code in a distributed way

.... the multicast problem enters the realm of network optimization....
Some plots...

Rocketfuel's view of the AT&T backbone....
www.cs.washington.edu/research/networking/rocketfuel/
### Some numbers...

<table>
<thead>
<tr>
<th>Network</th>
<th>Approach</th>
<th>2 sinks</th>
<th>4 sinks</th>
<th>8 sinks</th>
<th>16 sinks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telstra (au)</td>
<td>DST approximation</td>
<td>17.0</td>
<td>28.9</td>
<td>41.7</td>
<td>62.8</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>13.5</td>
<td>21.5</td>
<td>32.8</td>
<td>48.0</td>
</tr>
<tr>
<td>Sprint (us)</td>
<td>DST approximation</td>
<td>30.2</td>
<td>46.5</td>
<td>71.6</td>
<td>127.4</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>22.3</td>
<td>35.5</td>
<td>56.4</td>
<td>103.6</td>
</tr>
<tr>
<td>Ebone (eu)</td>
<td>DST approximation</td>
<td>28.2</td>
<td>43.0</td>
<td>69.7</td>
<td>115.3</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>20.7</td>
<td>32.4</td>
<td>50.4</td>
<td>77.8</td>
</tr>
<tr>
<td>Tiscali (eu)</td>
<td>DST approximation</td>
<td>32.6</td>
<td>49.9</td>
<td>78.4</td>
<td>121.7</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>24.5</td>
<td>37.7</td>
<td>57.7</td>
<td>81.7</td>
</tr>
<tr>
<td>Exodus (us)</td>
<td>DST approximation</td>
<td>43.8</td>
<td>62.7</td>
<td>91.2</td>
<td>116.0</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>33.4</td>
<td>49.1</td>
<td>68.0</td>
<td>92.9</td>
</tr>
<tr>
<td>Abovenet (us)</td>
<td>DST approximation</td>
<td>27.2</td>
<td>42.8</td>
<td>67.3</td>
<td>75.0</td>
</tr>
<tr>
<td></td>
<td>Network coding</td>
<td>21.8</td>
<td>33.8</td>
<td>60.0</td>
<td>67.3</td>
</tr>
</tbody>
</table>
Network codes as the “better” LT codes

We consider coding on packet erasure networks

A prototype toy example:

End-to-end coding (LT codes) achieves a “capacity” of \((1-e)^2\)
Network codes as the “better” LT codes

“Classically” one would decode and re-encode at the center node.
• long latency
• potentially significant complexity

Random network coding solution:

Random network coding also achieves the capacity of 1-e without complexity or delay!
Network codes as the “better” LT codes

Average number of transmissions required per packet in random networks of varying size. Sources and sinks were chosen randomly according to a uniform distribution. Paths or subgraphs were chosen in each random instance to minimize the total number of transmissions required, except in the cases of end-to-end retransmission and end-to-end coding, where they were chosen to minimize the number of transmissions required by the source node.
Summary

Network coding is a multifaceted phenomenon with three significant contributions:

- The rate region enlargement -> the butterfly example
- The possibility to cast classically hard problems, i.e. the multicast, as standard optimization problems
- Network codes as the “better” fountain code ...
- The joint optimization of the channel access and the network coded multicast is a particular intriguing area of research

THANK YOU
Summary

Network coding is a multifaceted phenomenon with three significant contributions:

- The rate region enlargement -> the butterfly example
- The possibility to cast classically hard problems, i.e. the multicast, as standard optimization problems
- Network codes as the “better” fountain code ...
- The joint optimization of the channel access and the network coded multicast is a particular intriguing area of research

THANK YOU
Summary

Network coding is a multifaceted phenomenon with three significant contributions:

- The rate region enlargement -> the butterfly example

- The possibility to cast classically hard problems, i.e. the multicast, as standard optimization problems

- Network codes as the “better” fountain code ...

- The joint optimization of the channel access and the network coded multicast is a particular intriguing area of research

THANK YOU
A simple (?) question

What is the capacity of a noiseless two hop network with simple links transmitting one bit per unit time.

Each individual link is an error free when it is “on”

The joint distribution of Input $X$ and Output $Y$ is:

<table>
<thead>
<tr>
<th>$P(X, Y)$; $X, Y$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1/2</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1/2</td>
</tr>
</tbody>
</table>
A simple (?) question

assuming the half-duplex constraint on binary bit pipes

X1 and X2 cannot be nonzero simultaneously, X1, X2 assume values in \{1, -1, NS\}

The conditional probability \(P(Y_1|X_1, X_2)\):

| \(Y_1, |X_1, X_2\) | \(N, N\) | \(N, 0\) | \(N, 1\) | \(0, N\) | \(0, 0\) | \(0, 1\) | \(1, N\) | \(1, 0\) | \(1, 1\) |
|----------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| \(E\)                | 1     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| 0                    | 0     | 1     | 0     | 1     | 1     | 0     | 0     | 1     | 0     |
| 1                    | 0     | 0     | 1     | 0     | 0     | 1     | 1     | 0     | 1     |

assuming the half-duplex constraint on binary bit pipes

If \(X_2\) is “on” we have \(Y_1 = X_2\) otherwise \(Y_1 = X_1\)
A simple (?) question

X1 and X2 cannot be nonzero simultaneously, X1,X2 assume values in {1,0,N}

The conditional probability P(Y1|X1,X2):

<table>
<thead>
<tr>
<th>Y1,</th>
<th>X1, X2</th>
<th>N, N</th>
<th>N, 0</th>
<th>N, 1</th>
<th>0, N</th>
<th>0, 0</th>
<th>0, 1</th>
<th>1, N</th>
<th>1, 0</th>
<th>1, 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

assuming the half-duplex constraint on binary bit pipes

This conditional pdf satisfies the conditions for a physically degraded relay channel (Cover & Thomas; G. Kramer)

with capacity:

\[
P(Y_2, Y_1|X_1, X_2) = P(Y_1|X_1, X_2)P(Y_2|Y_1, X_2)
\]

\[
\sup_{P(X_1, X_2)} \min\{I(X_1, X_2; Y), I(X; Y_1|X_1)\}
\]

The capacity of the binary input half duplex chain of two links is 1.1388 bits/channel use
A simple (?) question

three information bits grouped as 0 and 10
A simple (?) question

Timeslot 1

Timeslot 2

Timeslot 3

Timeslot 4
A simple (?) question

Timeslot 1

Timeslot 2

Timeslot 3

Timeslot 4
A simple (?) question

Timeslot 1

Timeslot 2

Timeslot 3

Timeslot 4
A simple (?) question

Timeslot 1

010N

Timeslot 2

1N11

N0NN

11 10 01 00

Timeslot 3

N100

1NNN

11 10 01 00

Timeslot 4

110N

NNNN1

11 10 01 00
A simple (?) question

This strategy achieves 0.75 bit per channel use while respecting the half-duplex constraint. The crucial step is to allow memory in $X_1$ and $X_2$. Allowing for more memory eventually hits a limit of 1.138 bit per channel use.
For a chain of links with half-duplex constraints the capacity converges to 1 bit per channel use.

The dependencies of all link inputs have to be carefully balanced in order to achieve this.
For a gaussian half-duplex channel ($N_0 << P_2$):

\[ Y_1 = \begin{cases} 
X_1 + N_1 & X_2 = NS \\
X_2 + N_0 & \text{otherwise}
\end{cases} \]

Capacity: \( \frac{1}{2} E[1-T](\log(1+\text{SNR}_1/E[1-T])) \) where $T$ is a Bernoulli r.v. satisfying:

\[
\frac{1}{2}(1 - E[T])(\log(1 + \text{SNR}_1/(1 - E[T]))) = \max_{f_X:E[X^2]/E[T]=P_2} h(N_2 + E[X])
\]
The wireless butterfly (incarnation II)

Half-duplex and interference constraint

Without network coding and time-sharing: 0.25 bits/(unit time x connections)
With network coding and time sharing: 0.33 bits/(unit time x connections)
With network coding and half-duplex constraint: ≥ 0.57 bits/(unit time x connections)
The wireless situation
The wireless situation — congested areas in the network are better utilized: packets use “car pooling”
Network coding.... some thoughts and talk outline

• Network coding is most often understood in the context of a rate region enlargement (the “main” theorem)

• Network coding also provides the opportunity to utilize optimization theory to plan resource allocation in networks

• A third benefit of network coding is the use as rateless codes in a packet erasure network.

• It is the combination of these three features that makes network coding a powerful tool.
Multicast and packing/flow problems

Utilizing the flow formulation we can solve a linear program:

Minimize the sum of cost-max flow product for each edge

subject to:

Observe the flow conservation at intermediate network nodes for each receiver individually
Multicast and packing/flow problems

Utilizing the flow formulation we can solve a linear program:

**Minimize** the sum of cost-max flow product for each edge

**subject to:** Observe the flow conservation at intermediate network nodes for each receiver individually
Multicast and packing/flow problems

Utilizing the flow formulation we can solve a linear program:

**Minimize** the sum of cost-max flow product for each edge

**subject to:** Observe the flow conservation at intermediate network nodes for each receiver individually

\[
\begin{align*}
\text{minimize} & \quad \sum_{(i,j) \in A} a_{ij} z_{ij} \\
\text{subject to} & \quad c_{ij} \geq z_{ij}, \quad \forall (i, j) \in A \\
& \quad z_{ij} \geq x_{ij}^{(t)} \geq 0, \quad \forall (i, j) \in A, \ t \in T \\
& \quad \sum_{\{j \mid (i, j) \in A\}} x_{ij}^{(t)} - \sum_{\{j \mid (j, i) \in A\}} x_{ji}^{(t)} = \sigma_{i}^{(t)}, \forall i \in N, \ t \in T
\end{align*}
\]
Codes for networks

Ralf Koetter
ralf.koetter@tum.de