Algorithms for Radio Networks

Network Coding

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Christian Schindelhauer
Network Coding

- R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung

Example
- Bits x and y are to be transferred
- Each edge carries only a bit
- If bits are transferred as is
  - then both x and y cannot be received either on the left or right side
Network Coding

- Example
  - Bits x and y are to be transferred
  - Each edge carries only a bit
  - If bits are transferred as is
    - then both x and y cannot be received either on the left or right side
Network Coding

Solution

- Transfer Xor A+B on the middle edge

\[
\begin{array}{c|c|c}
\text{XOR} & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0
\end{array}
\]

\[
\begin{align*}
x + x &= 0 \\
x + y &= y + x \\
(x + y) + z &= x + (y + z)
\end{align*}
\]

\[
\begin{align*}
x + x + y &= y \\
x + y + y &= x
\end{align*}
\]
Network Coding and Flow

- Theorem [Ahlsweide et al.]
  - For each graph there exists a network code such that each sink can receive as many bits as the maximum flow allows for each sink.
Linear Codes for Network Coding

- **Koetter, Médard**
  - Beyond Routing: An Algebraic Approach to Network Coding

- **Task**
  - Efficiently compute the network code

- **Solution**
  - Linear codes can always solve network coding

- **Practical Network Coding**
  - With high probability even random linear combinations suffice
Application Areas

- **Satellite Communication**
  - Preliminary work was published there

- **Peer-to-Peer networks**
  - Better information flow better than previous protocols
  - But too inefficient to displace prevalent protocols, e.g. Bittorrent

- **WLAN**
  - Xor in the Air, COPE
    - Simple network code improves flow

- **Ad-Hoc Networks, Wireless Sensor Networks, ...**
Coding and Decoding

\( y_i = x_1 \cdot r_{i1} + x_2 \cdot r_{i2} + \ldots + x_m \cdot r_{im} \)

- **Original message**: \( x_1, x_2, \ldots, x_m \)
- **Coding packet**: \( y_1, y_2, \ldots, y_m \)
- **Random variable** \( r_{ij} \)

Then:

\[
\begin{pmatrix}
  r_{11} & \cdots & r_{1m} \\
  \vdots & \ddots & \vdots \\
  r_{m1} & \cdots & r_{mm}
\end{pmatrix}
\begin{pmatrix}
  x_1 \\
  \vdots \\
  x_m
\end{pmatrix}
= 
\begin{pmatrix}
  y_1 \\
  \vdots \\
  y_m
\end{pmatrix}
\]

- If the matrix \( (r_{ij}) \) is invertible

\[
\begin{pmatrix}
  x_1 \\
  \vdots \\
  x_m
\end{pmatrix}
= 
\begin{pmatrix}
  r_{11} & \cdots & r_{1m} \\
  \vdots & \ddots & \vdots \\
  r_{m1} & \cdots & r_{mm}
\end{pmatrix}^{-1}
\begin{pmatrix}
  y_1 \\
  \vdots \\
  y_m
\end{pmatrix}
\]
Inverse of a Random Matrix

- **Theorem**
  - If the numbers of an \( m \times m \) Matrix are chosen randomly from a finite field with \( b \) elements, then the matrix is invertable with probability of at least
  
  \[
  1 - \sum_{i=1}^{m} \frac{1}{b^i}
  \]

- **Idea: Consider Galois-Field GF\([2^k]\)**
  - Computation is efficient
  - Binary representation of data straight-forward
Galois Field

- $GF(2^w)$ = finite field with $2^w$ elements
  - elements are binary strings of length $w$
  - $0 = 0^w$ neutral element of addition
  - $1 = 0^{w-1}$ neutral element of multiplication
- $u + v =$ bit-wise Xor of strings
  - z.B. $0101 + 1100 = 1001$
- $a \cdot b =$ product of polynomials modulo a given irreducible polynomial and modulo 2
  - i.e. $(a_{w-1} \ldots a_1 a_0)(b_{w-1} \ldots b_1 b_0) =$
    $((a_0 + a_1 x + \ldots + a_{w-1} x^{w-1})(b_0 + b_1 x + \ldots + b_{w-1} x^{w-1}) \mod q(x)) \mod 2)$
Example: GF(2^2)

\[ q(x) = x^2 + x + 1 \]

<table>
<thead>
<tr>
<th>Generator of GF(4)</th>
<th>Polynomial in GF(4)</th>
<th>Binary Representation in GF(4)</th>
<th>Decimal Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>00</td>
<td>0</td>
</tr>
<tr>
<td>( x^0 )</td>
<td>1</td>
<td>01</td>
<td>1</td>
</tr>
<tr>
<td>( x^1 )</td>
<td>( x )</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>( x^2 )</td>
<td>( x + 1 )</td>
<td>11</td>
<td>3</td>
</tr>
</tbody>
</table>

\[ 1 \cdot x + 0 \cdot x^0 = 10 \]
**Example: \( \text{GF}(2^2) \)**

<table>
<thead>
<tr>
<th></th>
<th>0 = 00</th>
<th>1 = 01</th>
<th>2 = 10</th>
<th>3 = 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>1 = 01</td>
<td>01</td>
<td>00</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>2 = 10</td>
<td>10</td>
<td>11</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>3 = 11</td>
<td>11</td>
<td>10</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>
### Example: GF($2^2$)

$q(x) = x^2 + x + 1$

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x^2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>x</td>
<td>x^2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>x^2</td>
<td>1</td>
<td>x</td>
</tr>
</tbody>
</table>
Irreducible Polynomial

- Irreducible polynomial cannot be factorized
  - Irreducible polynomial \( x^2 + 1 = (x+1)^2 \mod 2 \)
- Irreducible polynomials
  - \( w=2 \): \( x^2 + x + 1 \)
  - \( w=4 \): \( x^4 + x + 1 \)
  - \( w=8 \): \( x^8 + x^4 + x^3 + x^2 + 1 \)
  - \( w=16 \): \( x^{16} + x^{12} + x^3 + x + 1 \)
  - \( w=32 \): \( x^{32} + x^{22} + x^2 + x + 1 \)
  - \( w=64 \): \( x^{64} + x^4 + x^3 + x + 1 \)
Fast Multiplication

- **Power law**
  - Consider \(\{2^0, 2^1, 2^2, \ldots\}\)
  - \(= \{x^0, x^1, x^2, x^3, \ldots\}\)
  - \(= \exp(0), \exp(1), \ldots\)

- \(\exp(x+y) = \exp(x) \exp(y)\)

- **Inverse function:** \(\log(\exp(x)) = x\)
  - \(\log(x \cdot y) = \log(x) + \log(y)\)

- \(x \cdot y = \exp(\log(x) + \log(y))\)
  - Caution: in the exponent standard addition

- **Tables store exponential function and logarithm**

\[\begin{align*}
2^8 \cdot 2^8 &= 2^{16} \\
2^{16} \cdot 2^{16} &= 2^{32}
\end{align*}\]
Example: GF(16)

\[ q(x) = x^4 + x + 1 \]

\[
\begin{array}{|c|cccccccccccccccc|}
\hline
x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
\hline
\text{exp}(x) & 1 & x & x^2 & x^3 & 1+x & x+x^2 & x^2+x^3 & 1+x+ x^3 & 1+x^2 & x+x^3 & 1+x^2+x^3 & 1+x+x^2+x^3 & 1+x^2 & 1+x^3 \\
\hline
\text{exp}(x) & 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 5 & 10 & 7 & 14 & 15 & 13 & 9 & 1 \\
\hline
\end{array}
\]

\[
\begin{array}{|c|cccccccccccccccc|}
\hline
x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
\hline
\text{log}(x) & 0 & 1 & 4 & 2 & 8 & 5 & 10 & 3 & 14 & 9 & 7 & 6 & 13 & 11 & 12 \\
\hline
\end{array}
\]

- \( 5 \cdot 12 = \exp(\log(5)+\log(12)) = \exp(8+6) = \exp(14) = 9 \)
- \( 7 \cdot 9 = \exp(\log(7)+\log(9)) = \exp(10+14) = \exp(24) = \exp(24-15) = \exp(9) = 10 \)

\[
a \cdot b = \exp(\log(a) + \log(b)) = \exp(\log(a \cdot b)) = \exp(\log(a) + \log(b))
\]
Special Case GF[2]

- **Network Coding in GF[2]**
  - Boolean Algebra
    - $x + y = x \text{ XOR } y$
    - $x \cdot y = x \text{ AND } y$

- **Example**
  - Xor in the Air
  - Multicasting in Ad-Hoc Networks

- **Disadvantage**
  - Full potential of network coding is unused

- **Advantage**
  - Transparent, intuitiv and very efficient
Multicasting in Ad Hoc Networks

- Wu, Chou, Sun-Yuan,
  - Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006

- Multicast
  - Distribute message from one node to a given set of nodes

- Cost measure
  - Each one-hop broadcast costs an energy unit

![Multicast Diagram]

12 messages
SPT
10 messages
min Steiner tree

Target A
Target B

Broadcast

\[ x_1 + x_2 \]
Beispiel

- Traditionell, es kostet 5 Energie-Einheiten für eine Multicast-Nachricht.
Traditionally,
• it costs 5 energy units for a multicast message
Example

- **Network coding**
  - 9 energy units for 2 messages
  - Average of 4.5

- **Without network coding**
  - 5 units for one multicast message
Multicasting in Ad Hoc Networks

- Solution of the minimal energy multicasting problem without network coding is NP-hard
  - Less than constant factor approximation is NP-hard
  - Requires calculation of the discrete Steiner tree
Condition for Network Coding

- Messages allow flow of the size of the desired number of messages
  - from the sources to each individual sink
- If such flows are guaranteed, network coding can be applied
- Size of the flows describe energy consumption
Computational Complexity

- **Algorithm**
  - Collect all available link information
  - Formulate as linear program
  - Approximation of the solution

- With the help of network coding, the maximum throughput can be approximated arbitrarily well in polynomial time
Example Demand

Wu, Chou, Sun-Yuan, Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006
Example Multicasting with minimal Energy

Wu, Chou, Sun-Yuan, Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006
Multicasting with Network Coding

Wu, Chou, Sun-Yuan, Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006
Discussion

- **Options**
  - Energy model can customized

- **Limitations**
  - Network coding is not described
  - Central algorithm
  - Any change in the communication requires recalculation
Xors in the Air

- Katti, Hu, Katabi, Médard, Crowcroft
  - XORs in the Air: Practical Wireless Network Coding
- Problem
  - Maximize throughput in ad-hoc network
  - Multihop messages cause interference
- Solution
  - Uses only XORs of multiple messages
  - Local, opportunistic algorithm
Xors in the Air

- **Problem**
  - Multihop messages cause interferences

- **Example**
  - Traditional: 4 messages to send
    - a message from A to B
    - and a message from B to A

<table>
<thead>
<tr>
<th>Round</th>
<th>A</th>
<th>Relay</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>![Message 1](Message 1)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>![Message 1](Message 1)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>![Message 2](Message 2)</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>![Message 2](Message 2)</td>
</tr>
</tbody>
</table>
Xors in the Air

- **Problem**
  - Multihop messages cause interferences

- **Example**
  - Traditional: 4 messages to send
    - a message from A to B
    - and a message from B to A
  - Network Coding
    - 3 messages suffice

**Diagram**

- **Round 1**
  - Message $x_1$ from A to Relay

- **Round 2**
  - Message $x_2$ from Relay to B
  - Message $x_1$ from A to Relay

- **Round 3**
  - Message $x_1 \oplus x_2$ from Relay to B
  - Message $x_1 \oplus x_2$ from A to Relay

**Equation**

$1 \quad x_1 \quad x_1 \oplus x_2 \quad x_1 \oplus x_2$

$2 \quad x_2 \quad x_2$

$3 \quad x_1 \oplus x_2 \quad x_1 \oplus x_2$
Coding Opportunistically
COPE

- Consider of multiple communication paths
  - Opportunistic coding of messages by Xor

- Utilization of the broadcast medium
  - listening to the channel
  - all (even foreign) messages are buffered
  - buffered messages are used for decoding

- Context messages
  - announcement of level of knowledge
  - neighbors can generate code adapted to the receiver’s knowledge

- Guess the level of knowledge of neighbors
Opportunistic Coding

known messages

known messages

known messages

messages to be send

receivers

A
B
C
D

P_1
P_2
P_3
P_4

A
C
C
D

P_1
P_3

P_1
P_4

P_1
P_4

P_1
P_3

P_3
P_4
Oppportunistic Coding

- Messages to be send: $P_1, P_2, P_3, P_4$
- Receivers: A, C, C, D
- Known messages:
  - A: $P_3, P_4$
  - C: $P_1, P_4$
  - D: $P_1, P_3$
Opportunistic Coding

Known messages:
- A
- C
- D

Messages to be sent:
- P_1
- P_2
- P_3
- P_4

The diagram illustrates how messages are sent and received within a network, utilizing opportunistic coding to optimize the transmission of data.
Opportunistic Coding

A diagram illustrating the concept of opportunistic coding in radio networks. The network consists of nodes A, B, C, and D, each with known messages: P_1, P_3, and P_4 for node A; P_1 and P_4 for node C; and P_3 for node D. Node B is the recipient node with messages to be sent: P_1, P_2, P_3, and P_4. The diagram shows how messages can be combined and sent efficiently across the network.
Codings Gain

<table>
<thead>
<tr>
<th>Topology</th>
<th>Coding Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-chain</td>
<td>1,333...</td>
</tr>
<tr>
<td>X</td>
<td>1,333...</td>
</tr>
<tr>
<td>Cross</td>
<td>1,666...</td>
</tr>
<tr>
<td>Infinite Chain</td>
<td>2</td>
</tr>
<tr>
<td>Infinite Wheel</td>
<td>2</td>
</tr>
</tbody>
</table>
Summary Network Coding

Figure 12—COPE can provide a several-fold (3-4x) increase in the throughput of wireless Ad hoc networks. Results are for UDP flows with randomly picked source-destination pairs, Poisson arrivals, and heavy-tail size distribution.

Wu, Chou, Sun-Yuan, Minimum-Energy Multicast in Mobile Ad hoc Networks using Network Coding, 2006
Network Coding

- **Benefit**
  - Network throughput can be increased
    - COPE
  - Reduction of energy consumption
  - Higher robustness, small error rate
  - Applications in peer-to-peer networks, wireless sensor networks

- **Problems**
  - complex encoding
  - sometimes high computational cost
  - difficult organization
Algorithms for Radio Networks

Network Coding

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Christian Schindelhauer
\[ x_1 \cdot v_1 + x_2 \cdot v_2 = y_1 \]
\[ x_1 \cdot v_3 + x_2 \cdot v_4 = y_2 \]
\[ x_3 \cdot v_5 + x_4 \cdot v_6 = y_3 \]
\[ y_1 \cdot v_7 + y_2 \cdot v_8 = y_6 \]
\[
\begin{pmatrix}
1 & 0 \\
0 & 1 \\
\end{pmatrix}
\begin{pmatrix}
x \\
y \\
\end{pmatrix}
=
\begin{pmatrix}
x \\
x + y \\
\end{pmatrix}
\]

\[M = \begin{pmatrix}
1 & 0 \\
0 & 1 \\
\end{pmatrix}\]

\[M = \begin{pmatrix}
1 & 0 \\
0 & 0 \\
\end{pmatrix}\]

\[M^{-1} = \begin{pmatrix}
1 & 0 \\
0 & 0 \\
\end{pmatrix}\]

\[\gamma \ast u(M) = 1\]

\[M \cdot M^{-1} = \begin{pmatrix}
1 & 0 \\
0 & 0 \\
\end{pmatrix}\]
\( \text{rank}(M') = n - 1 \)

\[ P[\text{rank}(M) = n] = \sum_{i=0}^{n} \frac{1}{2} \]

\[ P[\text{rank}(k) < n] \geq \frac{1}{2} \]
\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 4 & 6 \\
3 & 0 & 3 & 6 & 2 \\
\end{array}
\]

\[
2 \cdot 4 = 8 \pmod{7}
\]

\[\equiv 1\]

\[
(\mod 7)
\]
\[ 6 + [2] \]

\[ -1 = 1 \]

\[ \begin{array}{c|ccc}
+ & 0 & 1 & 0 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 \\
\end{array} \]

\[ \begin{array}{c|ccc}
\times & 0 & 1 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 \\
\end{array} \]

\[ \begin{array}{c|ccc}
- & 0 & 1 & 0 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 \\
\end{array} \]

\[ 0 - 1 = x \]

\[ 0 = x + 1 \]

\[ 1 = x + \frac{1}{0} \]

\[ \land \equiv x \]

5
\[ 372 = 2 \cdot 10^0 + 7 \cdot 10^1 + 3 \cdot 10^2 \]

\[ 372 \cdot 123 = 2 \cdot 3 \cdot 10^0 + 2 \cdot 2 \cdot 10^1 \]

\[ (a_0 \cdot q^0 + a_1 \cdot q^1 + \ldots) \cdot (b_0 \cdot q^0 + \ldots) = \sum a_i \cdot b_j \cdot q^{i+j} \]

\[ (c_0 \cdot q^0 + c_1 \cdot q^1 + \ldots) \cdot (d_0 \cdot q^0 + \ldots) \]

\[ dw \cdot q^u \ldots \]
\[ \begin{align*}
    x^2 + 1 &= (x+1)^2 = x^2 + (x + x) + 1 \\
    x^2 + x + 1 &= \\
    x^2 &= x \cdot x \\
    x^3 + x + 1 &= (x+1)(x^2 + x + 1) \\
    101110_2 : 111 &= 0100_2 \\
    \hline
    101 & \\
    \hline
    101 & \\
    \hline
    101 & \\
    \hline
    101 & \\
    \hline
    0104 & \\
    \hline
    110111 & \\
    \hline
    x^4 + 3x^3 + x^2 + 1 &= 10111_2 \quad \text{Mod: 0000}
\end{align*} \]