Peer-to-Peer Networks

11 Network Coding

Arne Vater
Technical Faculty
Computer Networks and Telematics
University of Freiburg
Network Flow

- How can network flow be optimized?
  - two data bits
    - x, y
  - two sender
    - S₁, S₂
  - two receiver
    - R₁, R₂
  - link capacity 1
  - deliver both bits to both receiver
Network Flow
Network Flow

- Simple transmission of bits allows maximal flow 3
  - minimal cut = 3
  - middle edge is bottleneck
- Can we do better?
Network Coding

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

Solution
- Send Xor of x and y on the middle edge
Network Coding

- Theorem [Ahlswede et al.]
  - For each graph there exists a network code such that each sink can receive as many information as allowed by the maximum flow to that sink.
Linear Network Codes

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

- Goal
  - finding those codes for network coding

- Solution
  - linear combinations are sufficient for any network coding
    - even random linear combinations in Practical Network Coding for peer-to-peer networks
Application Areas

- Satellite communication
  - preliminary work
- WLAN
  - Xor in the Air, COPE
    - simple network code improves network flow
- Ad hoc networks
- Sensor networks
- Peer-to-peer networks
Coding and Decoding

- Original message: $x_1, x_2, \ldots, x_n$
- Code packets: $b_1, b_2, \ldots, b_n$
- Random linear coefficient $c_{ij}$

Thus

$$
\begin{pmatrix}
c_{11} & \cdots & c_{1n} \\
\vdots & \ddots & \vdots \\
c_{n1} & \cdots & c_{nn}
\end{pmatrix}
\begin{pmatrix}
x_1 \\
\vdots \\
x_n
\end{pmatrix}
=
\begin{pmatrix}
b_1 \\
\vdots \\
b_n
\end{pmatrix}
$$

If matrix $(c_{ij})$ is invertible then:

$$
\begin{pmatrix}
x_1 \\
\vdots \\
x_n
\end{pmatrix}
=
\begin{pmatrix}
c_{11} & \cdots & c_{1n} \\
\vdots & \ddots & \vdots \\
c_{n1} & \cdots & c_{nn}
\end{pmatrix}^{-1}
\begin{pmatrix}
b_1 \\
\vdots \\
b_n
\end{pmatrix}
$$
Inverse of Random Matrix

- **Theorem**
  - If the values of an $n \times n$ matrix are randomly chosen from a finite field with $s$ elements, then the matrix is invertible with probability at least
  \[
  1 - \sum_{i=1}^{n} \frac{1}{s^i}
  \]

- **Problem**
  - Numbers become larger with each calculation
Galois Fields

- Idea: Use Galois field $GF[2^w]$
  - efficient computation
  - power of two suits binary data representation
- $GF[2^w] = \text{finite field with } 2^w \text{ elements}$
  - elements are binary strings with length $w$
  - $0 = 0^w$ identity element for addition
  - $1 = 0^{w-1}1$ identity element for multiplication
- $u + v = \text{bit-wise Xor}$
  - i.e. $0101 + 1100 = 1001$
- $a \cdot b = \text{polynom product modulo an irreducible polynom and modulo } 2$
  - i.e.
    $$ (a_{w-1}...a_1a_0)(b_{w-1}...b_1b_0) = $$
    $$ (\left(\left(a_0 + a_1x + ... + a_{w-1}x^{w-1}\right) \left(b_0 + b_1x + ... + b_{w-1}x^{w-1}\right) \mod q(x)\right) \mod 2 $$
### Example: GF[$2^2$]

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></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>
Why is $x^2 = x + 1$?

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

$x^2 \mod x^2 + x + 1 = $
Example: 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>

bit-wise Xor
Example: GF[2^2]

<table>
<thead>
<tr>
<th>*</th>
<th>0 = 0</th>
<th>1 = 1</th>
<th>2 = x</th>
<th>3 = x^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 = 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 = 1</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x^2</td>
</tr>
<tr>
<td>2 = x</td>
<td>0</td>
<td>x</td>
<td>x^2</td>
<td>1</td>
</tr>
<tr>
<td>3 = x^2</td>
<td>0</td>
<td>x^2</td>
<td>1</td>
<td>x</td>
</tr>
</tbody>
</table>
Why is $x^3 = 1$?
- $x^2 = x + 1$
- $x + x = 0$

$x^3 =$
Irreducible Polynomials

- Irreducible polynomials are non-decomposable
  - 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: $x^{64} + x^4 + x^3 + x + 1$

- Decomposable polynom: $x^2 + 1 = (x + 1)^2 \mod 2$
Fast Multiplication

- Power laws
  - \( \{2^0, 2^1, 2^2, \ldots\} \)
  - \( \{x^0, x^1, x^2, x^3, \ldots\} \)
  - \( \text{exp}(0), \text{exp}(1), \text{exp}(2), \ldots \)

- \( \text{exp}(x + y) = \text{exp}(x) \cdot \text{exp}(y) \)

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

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

- Values for exponential and logarithmic function stored in lookup tables
Example: GF[16]

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

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

\[ x \cdot y = \exp(\log(x) + \log(y)) \]
Special Case: GF[2]

- **Boolean algebra**
  - $x + y = x \text{ XOR } y$
  - $x \cdot y = x \text{ AND } y$
Peer-to-Peer Networks
11 Network Coding

Arne Vater
Technical Faculty
Computer Networks and Telematics
University of Freiburg