Peer-to-Peer Networks

10 Fast Download

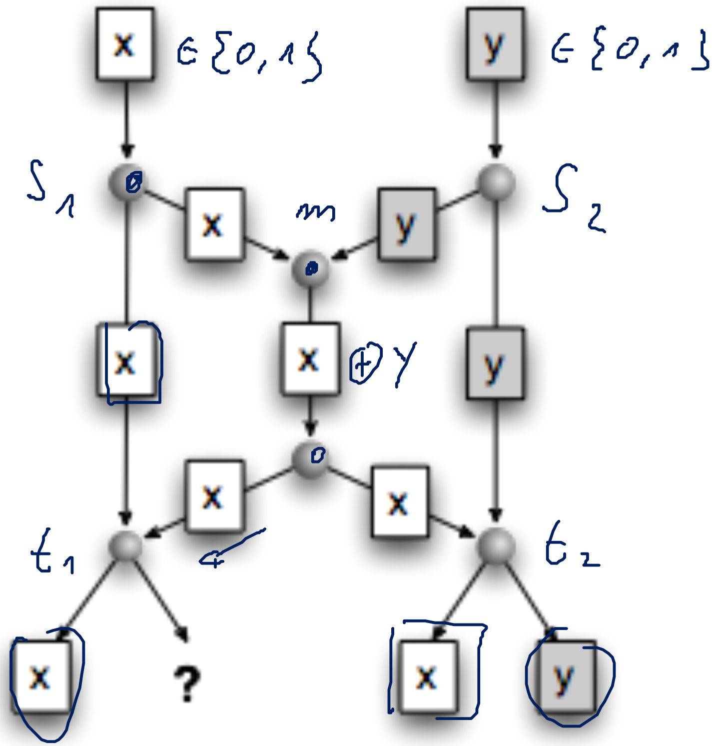
Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of Freiburg

CoNe Freiburg

Network Coding

- R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow", (IEEE Transactions on Information Theory, IT-46, pp. 1204-1216, 2000)

- Example
  - Bits x and y need to be transmitted
  - Every line transmits one bit
  - If only bits are transmitted
    - then only x or y can be transmitted in the middle?
  - By using X we can have both results at the outputs

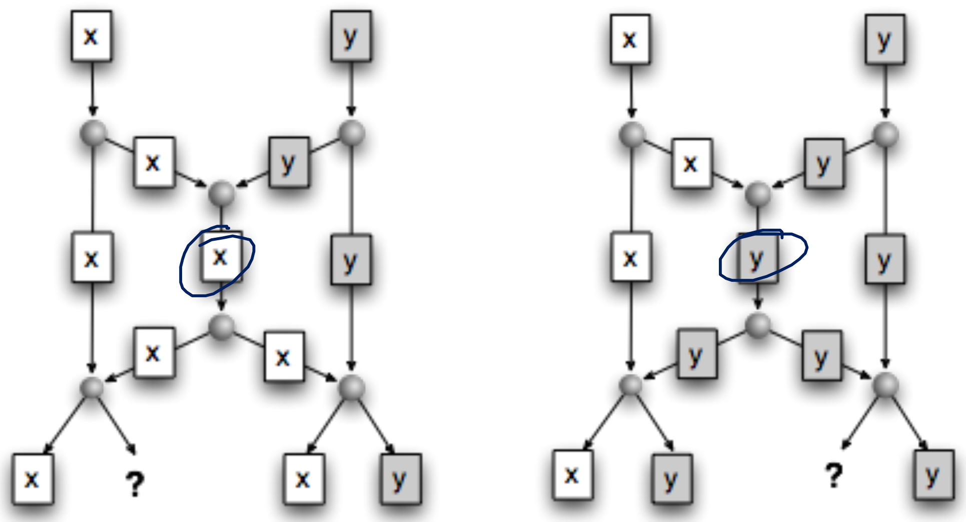


UNI FREIBURG

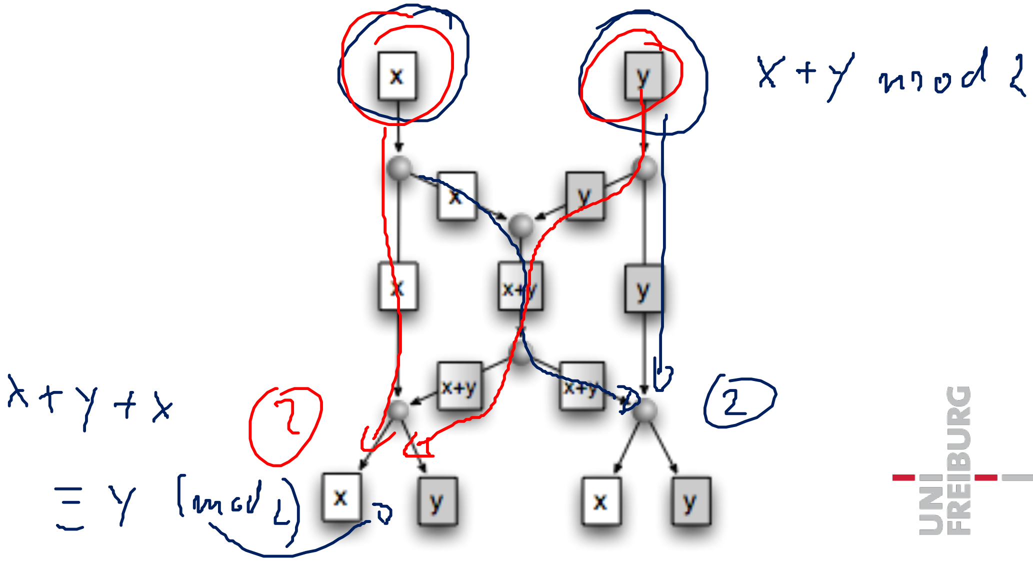
Network Coding

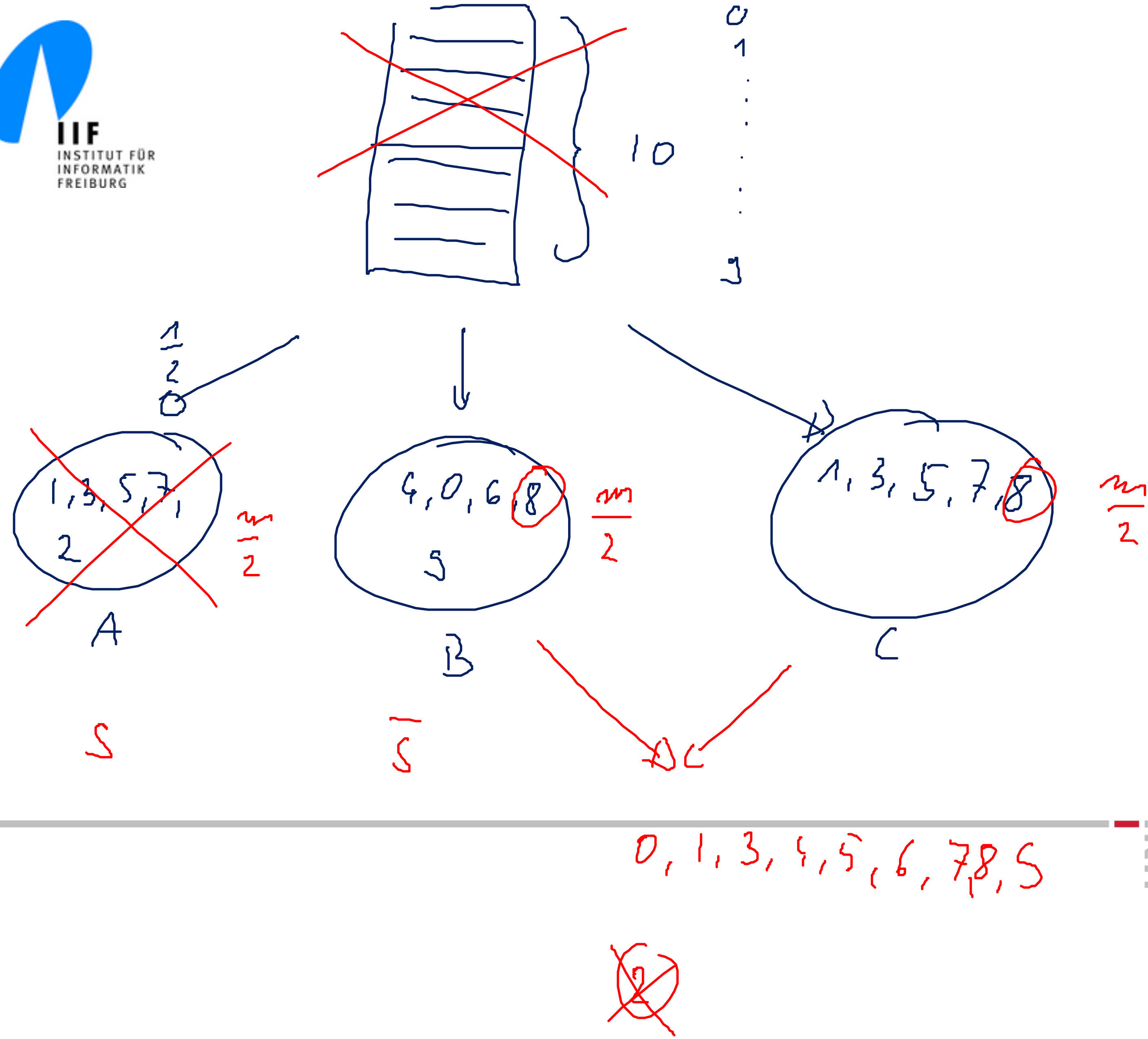
$1 + 1 \equiv 2 \equiv 0 \pmod 2$

- R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow", (IEEE Transactions on Information Theory, IT-46, pp. 1204-1216, 2000)



- Theorem [Ahlswede et al.]
  - There is a network code for each graph such that each node receives as much information as the maximum flow of the corresponding flow problem





0
1
9
10
1
2
0
1,3,5,7,
2
A
4,0,6,8
9
B
1,3,5,7,8
C
m/2
S
0,1,3,4,5,6,7,8,9

$$F = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \quad \in \{0,1\}^4$$

(mod 17)

$$\boxed{1\cdot b_1 + 2\cdot b_2 + 3\cdot b_3 + 17\cdot b_4 + \dots + 5\cdot b_n = c_1}$$

Finite Field $\{0, \dots, 2^m - 1\}$

$GF[2^m]$

$a \cdot b \pmod 2$

AND

Galois

$a + b \mathrel{\hat{=}}$ bitwise xor

$a \cdot b \mathrel{\hat{=}}$ multiply

two pol. mod. pol.

$=$ CRC

$a \cdot b, \quad a \cdot \boxed{b^{-1}}, \quad a + b, \quad a - b$

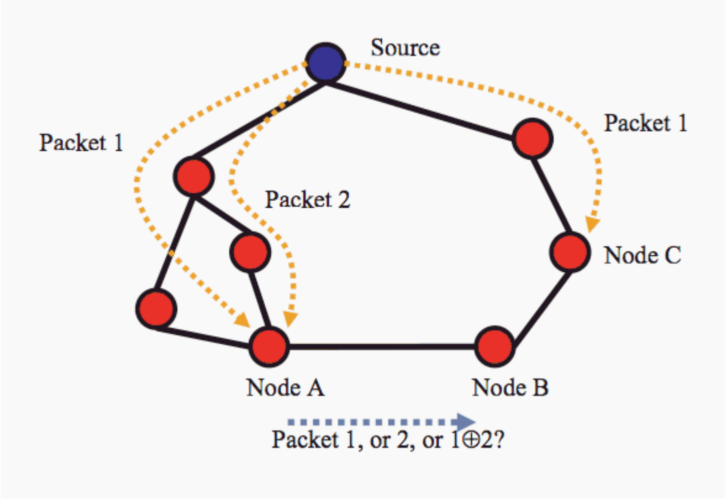
$a + b = b + a \qquad a \cdot b = b \cdot a$

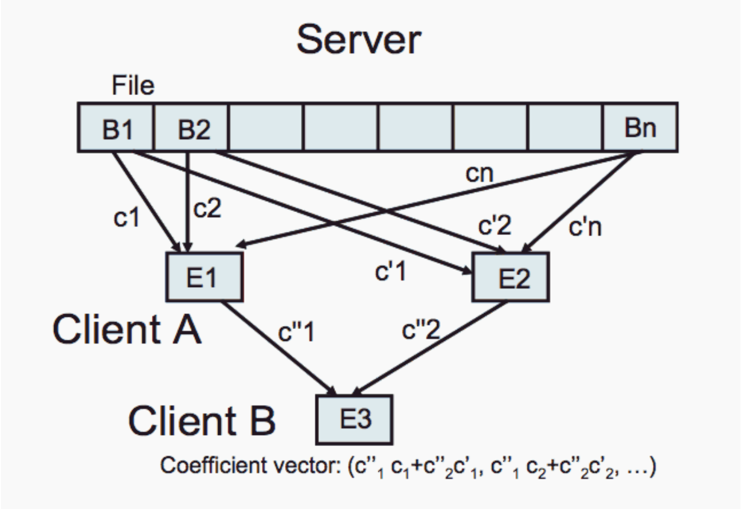
$a(b+c) = ab + ac$

} finite field

Practical Network Coding Avalanche

- Christos Gkantsidis, Pablo Rodriguez Rodriguez, 2005
- Goal
  - Overcoming the Coupon-Collector-Problem
    - a file of m parts can be always reconstructed if at least m network codes have been received
  - Optimal transmission of files within the available bandwidth
- Method
  - Use codes as linear combinations of a file
    - Produced code contains the vector and the variables
  - During the distribution the linear combination are re-combined to new parts
  - The receiver collects the linear combinations
  - and reconstructs the original file using matrix operations





$$\left.\begin{bmatrix} b_1 \\ \vdots \\ b_{10} \end{bmatrix}\right\} m$$

$$c_1 = k_1 \cdot b_1 + k_2 \cdot b_2 + k_3 \cdot b_3 \dots k_{10} \cdot b_{10}$$

k_i : randomly chosen

$$= \sum_{i=1}^{m} r_i \cdot b_i$$

$c_1 \; c_2 \; c_3 \; c_4 \; c_5$

~~$c_6 \; c_7 \; c_8 \; c_9 \; c_{10}$~~

$c_{11} \; c_{12} \; c_{13} \; c_{14} \; c_{15}$

$$\boxed{\text{random}} \rightarrow \begin{pmatrix} r_{11} & r_{12} & \dots & \\ r_{21} & & & \\ & & M & \\ & & & r_{mm} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$$

$$\underline{M} \cdot \vec{b} = \underline{\vec{c}}$$

$$\vec{b} = M^{-1} \cdot \vec{c}$$

Coding and Decoding

$$\sum_{j=1}^{m} r_{ij} \cdot x_j$$

$$\parallel$$

- File: $x_1, x_2, \ldots, x_m$
- Codes: $y_1, y_2, \ldots, y_m$
- Random Variables r_{ij}

$$(r_{i1} r_{i2} \ldots r_{im}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = y_i$$

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

- If the matrix is invertable then

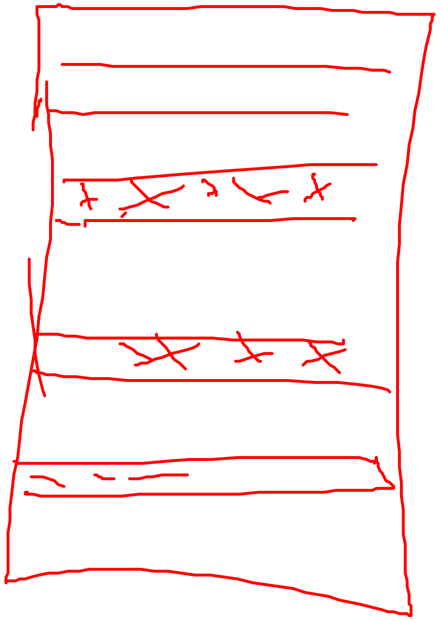
$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} r_{11} & \cdots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mm} \end{pmatrix}^{-1} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

$b = |GF|$ size of the field

$\vec{a}, \vec{b}$

$\vec{c} = 3 \cdot \vec{a} + 4\vec{b}$

→ $\vec{c}$ is linearly dependent from $\vec{a}, \vec{b}$



$m-1$

1	1	2	3	4
2	2	4	6	5
3	3	1	0	0
	⋮			
	3	1	2	5	0

Prob that it the row is dependent

$$\frac{1}{b} \cdot \frac{1}{b} \cdots \frac{1}{b} = \frac{1}{b^{m-1}}$$

$$\frac{1}{b^{m-2}}$$

$$\frac{1}{b}$$

$$\boxed{\left(1 - \frac{1}{b}\right)} \cdot \left(1 - \frac{1}{b^2}\right)\left(1 - \frac{1}{b^3}\right) \dots \approx \frac{1}{2} \cdot \left(1 - \frac{1}{b}\right) \quad b \geq 4$$

$$\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{8}\right) \dots = 0.28\dots \quad \boxed{b = 2}$$

Prob that the last row is independent

Speed of Network-Coding

- Comparison
  - Network-Coding (NC) versus
  - Local-Rarest (LR) and
  - Local-Rarest+Forward-Error-Correction (LR +FEC)