ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

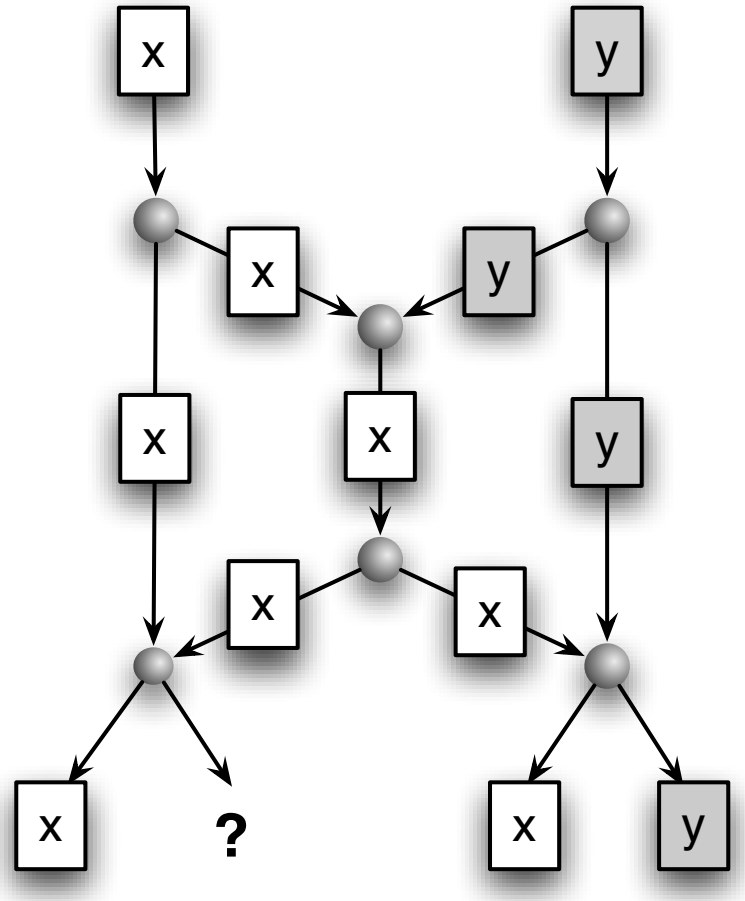
Algorithmen für drahtlose Netzwerke

Netzwerk-Kodierung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

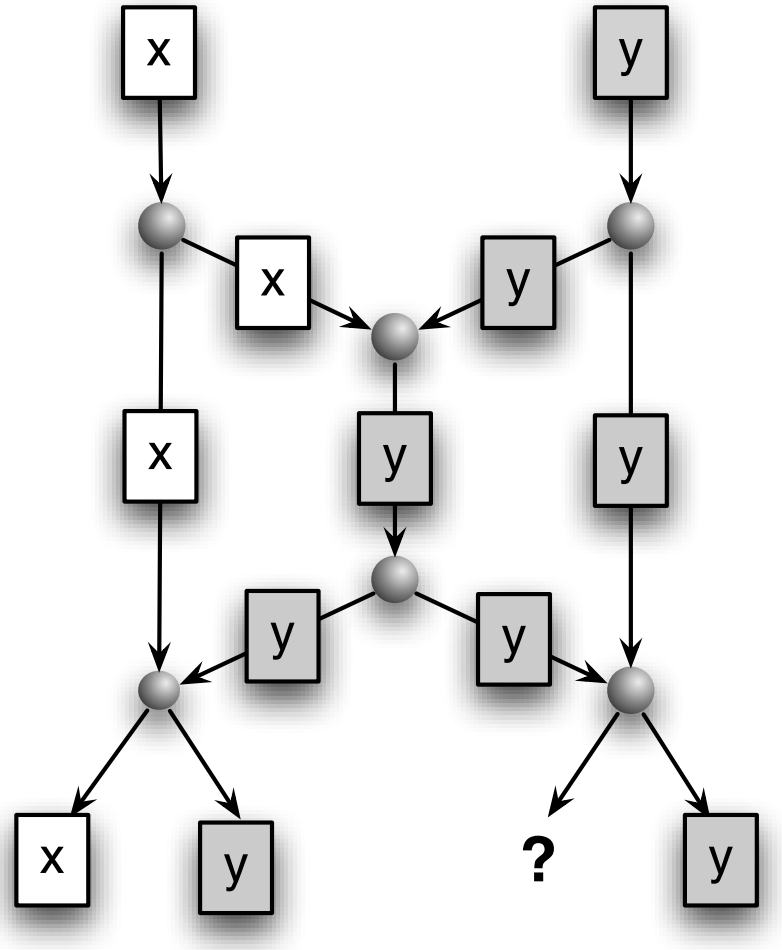
Netzwerk-Kodierung

- **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)
- **Beispiel:**
  - Bits x und y sollen übertragen werden
  - Jede Kante überträgt nur ein Bit
  - Falls die Bits nicht verändert werden dürfen
    - dann können x und y entweder auf der linken oder rechten Seite empfangen werden



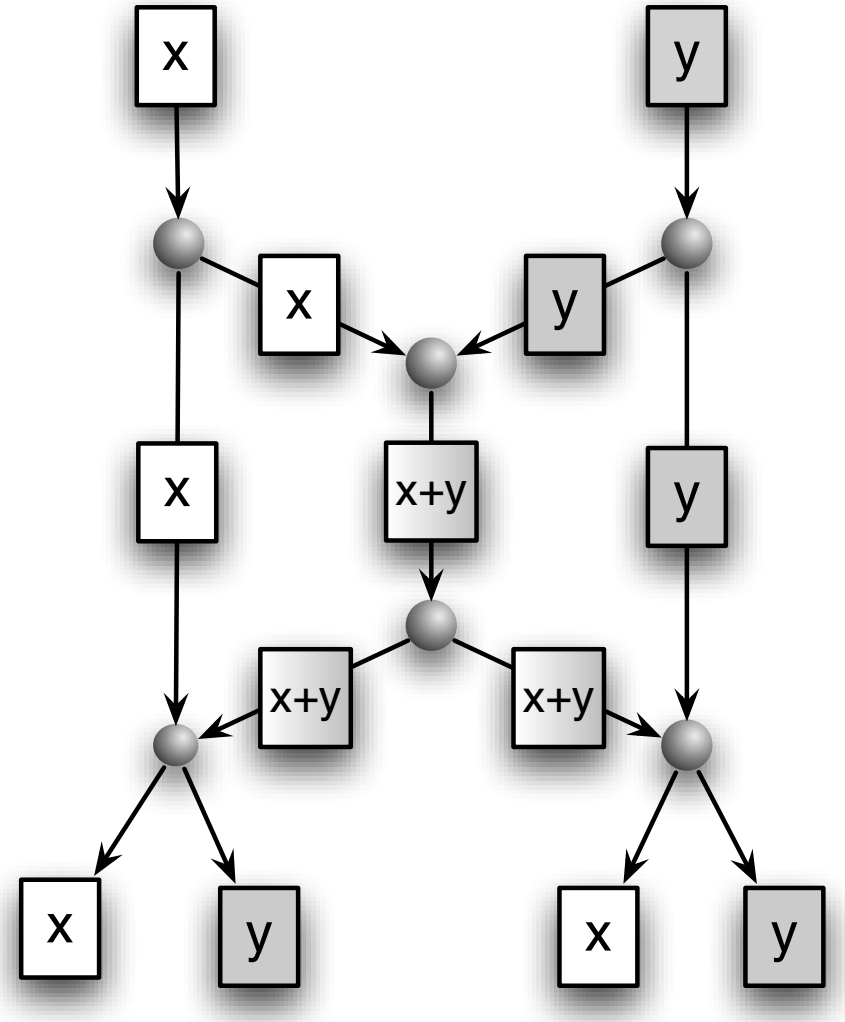
Netzwerk-Kodierung

- **Beispiel:**
  - Bits x und y sollen übertragen werden
  - Jede Kante überträgt nur ein Bit
  - Falls die Bits nicht verändert werden dürfen
    - dann können x und y entweder auf der linken oder rechten Seite empfangen werden



Netzwerk-Kodierung

- **Lösung: Berechne Xor A+B auf der Mittelkante**



Network Coding and Flow

- **Theorem [Ahlswede et al.]**
  - Für jeden Graph gibt es einen Netzwerk-Code, so dass jede Senke so viel Information empfangen kann, wie es der maximale Fluss für jede Senke erlaubt.

Lineare Codes für Network Coding

- **Koetter, Médard**
  - Beyond Routing: An Algebraic Approach to Network Coding
- **Ziel**
  - Bestimmung konkreter Codes für Netzwerk-Kodierung
- **Lösung**
  - Lineare Codes können Netzwerk-Koding immer lösen
- **Practical Network Coding**
  - In Peer-to-Peer-Netzwerken genügen sogar schon zufällige Linearkombinationen

Anwendungsgebiete

- **Satellitenkommunikation**
  - Vorarbeiten für Netzwerk-Kodierung dort gefunden
- **Peer-to-Peer-Netzwerke**
  - Vom Informationsfluss besser als bisherige Protokolle
  - Aber zu rechenaufwändig um z.B. Bittorrent zu verdrängen
- **WLAN**
  - Xor in the Air, COPE
    - Einfacher Netzwerk-Code verbessert Fluss
- **Ad-Hoc-Netzwerke, Sensor-Netzwerke, u.v.a.**

Kodierung und Dekodierung

- **Originalnachricht: x_1, x_2, ..., x_m**
- **Kodierte Pakete: y_1,y_2,...,y_m**
- **Zufallsvariablen r_{ij}**
- **Somit**

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

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

- **Falls die Matrix (r_{ij}) invertierbar ist:**

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

Inverse einer Zufallsmatrix

- **Theorem**
  - Falls die Zahlen einer m x m Matrix zufällig gewählt werden aus einem endlichen Körper mit b Elementen, dann ist die Matrix invertierbar mit Wahrscheinlichkeit mindestens

$$1 - \sum_{i=1}^{m} \frac{1}{b^i}$$

- **Idee: Wähle Galois-Körper GF[2^k]**
  - Berechnung effizient möglich
  - Zweierpotenzen passen zur binären Darstellung von Daten

Galois Körper

- **GF(2^w) = Endlicher Körper mit 2^w Elementen**
  - Elemente sind binäre Zeichenketten der Länge w
  - 0 = 0^w neutrales Element der Addition
  - 1 = $0^{w-1}1$ neutrales Element der Multiplikation
- **u + v = bitweises Xor der Zeichenkett**
  - z.B. 0101 + 1100 = 1001
- **a b = Produkt der Polynome modulo eines irreduziblen Polynoms und modulo 2**
  - i.e. (a_{w-1} ... a_1 a_0) (b_{w-1} ... b_1 b_0) =

$$((a_0 + a_1 x + \ldots + a_{w-1}x^{w-1})(b_0 + b_1 x + \ldots + b_{w-1}x^{w-1}) \bmod q(x)) \bmod 2)$$

Beispiel: GF(2^2)

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

Erzeugendes Element von GF(4)	Polynom in GF(4)	Binäre Darstellung in GF(4)	Dezimale Darstellung
0	0	00	0
x^0	1	01	1
x^1	x	10	2
x^2	x+1	11	3

Beispiel: GF(2^2)

+	0 = 00	1 = 01	2 = 10	3 = 11
0 =00	00	01	10	11
1 =01	01	00	11	10
2 =10	10	11	00	01
3 =11	11	10	01	00

Beispiel: GF(2^2)

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

*	0 = 0	1 = 1	2 = x	3 = x^2
0 = 0	0	0	0	0
1 = 1	0	1	x	x^2
2 = x	0	x	x^2	1
3 = x^2	0	x^2	1	x

Irreduzible Polynome

- **Irreduzible Polynome können nicht zerlegt werden**
  - Zerlegbares Polynom: $x^2+1 = (x+1)^2 \bmod 2$
- **Irreduzible Polynome**
  - 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: $x^{64}+x^4+x^3+x+1$

Schnelle Multiplikation

- **Potenzgesetze**
  - Betrachte: $\{2^0, 2^1, 2^2, ...\}$
  - $= \{x^0, x^1, x^2, x^3, ...$
  - $= \exp(0), \exp(1), ...$
- **$\exp(x+y) = \exp(x) \exp(y)$**
- **Inverse Funktion: $\log(\exp(x)) = x$**
  - $\log(x \cdot y) = \log(x) + \log(y)$
- **$x\ y = \exp(\log(x) + \log(y))$**
  - Achtung: im Exponenten normale Addition
- **Tabellen speichern Exponentialfunktion und Logarithmen**

Beispiel: GF(16)

$q(x) = x^4+x+1$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
exp(x)	1	x	x^2	x^3	1+x	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1
exp(x)	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
log(x)	0	1	4	2	8	5	10	3	14	9	7	6	13	11	12

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

Spezialfall GF[2]

- **Netzwerk-Kodierung wird oft in GF[2] berechnet**
  - Boolesche Algebra:
    - x + y = x XOR y
    - x y = x AND y
- **Beispiele**
  - Xor in the Air
  - Multicasting in Ad-Hoc-Netzwerken
- **Nachteil:**
  - Volle Fähigkeit der Netzwerk-Kodierung bleibt ungenutzt
- **Vorteil:**
  - Transparent, intuitiv und sehr effizient

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer