Algebraisches Internet

Axel Kohnert

Braunschweig Mai 2010

Universität Bayreuth

axel.kohnert@uni-bayreuth.de

UNIVERSITÄT BAYREUTH

Übersicht

- Designs
- Network Codes
- Konstruktion
- Decodieren

I - Designs

Design

- Menge von v Punkten

Design

- Menge von v Punkten
- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)

Design

- Menge von v Punkten
- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)
- $t-(v,k,\lambda)$ Design

Design

- Menge von v Punkten
- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)
- $t-(v,k,\lambda)$ Design
  Jeder Block hat k Punkte
  Jede $t-$Menge von Punkten ist in genau λ Blöcken

Design

- Menge von v Punkten

  a, b, c, d, e, f, g
- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)

- $t - (v, k, \lambda)$ Design
  Jeder Block hat k Punkte
  Jede $t-$Menge von Punkten ist in genau λ Blöcken

Design

- Menge von v Punkten

  a, b, c, d, e, f, g

- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)

  $abe, adg, acf, bcg, bdf, cde, efg$

- $t-(v,k,\lambda)$ Design
  Jeder Block hat k Punkte
  Jede $t-$Menge von Punkten ist in genau λ Blöcken

Design

- Menge von v Punkten

  a, b, c, d, e, f, g

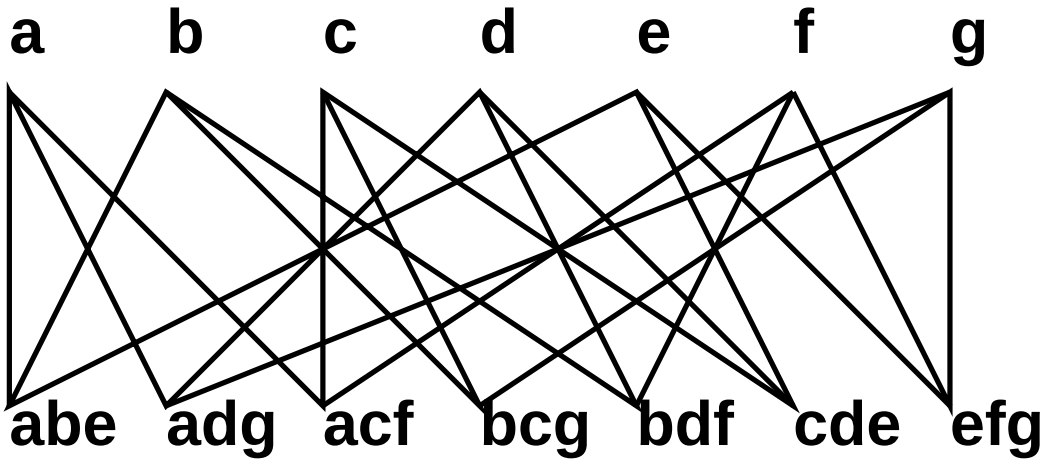
- Menge $\mathcal{B}$ von Blöcken (Block = Menge von Punkten)

  $abe, adg, acf, bcg, bdf, cde, efg$

- $t-(v,k,\lambda)$ Design
  Jeder Block hat k Punkte
  Jede $t-$Menge von Punkten ist in genau λ Blöcken

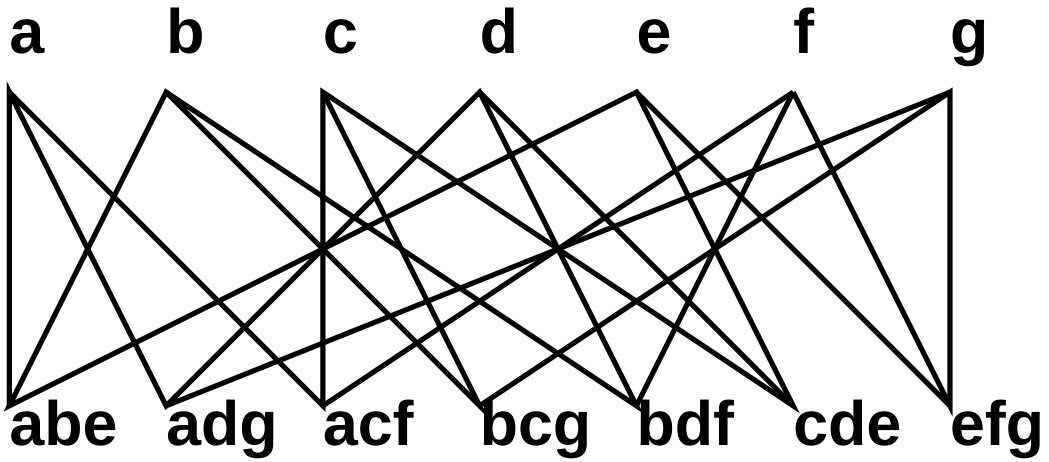
  $2-(7,3,1)$ Design

Designs



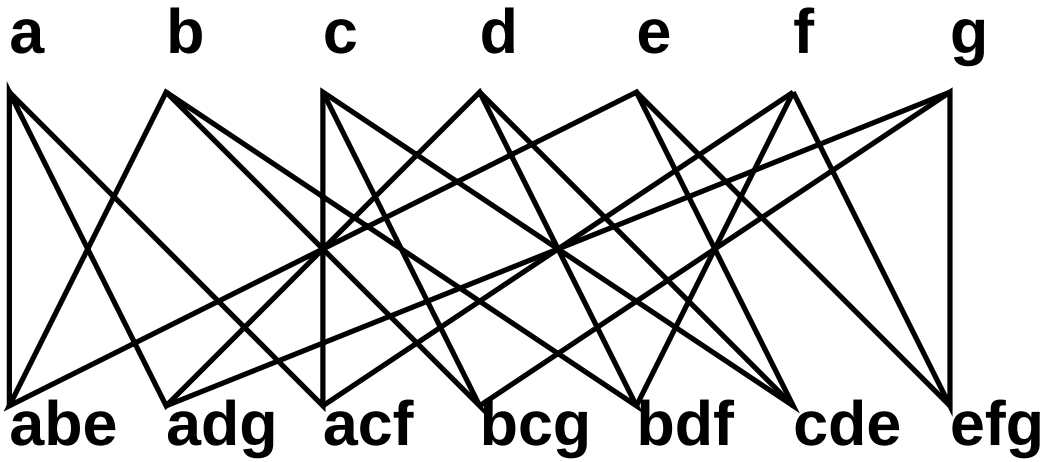
UNIVERSITÄT BAYREUTH

Heawood Graph

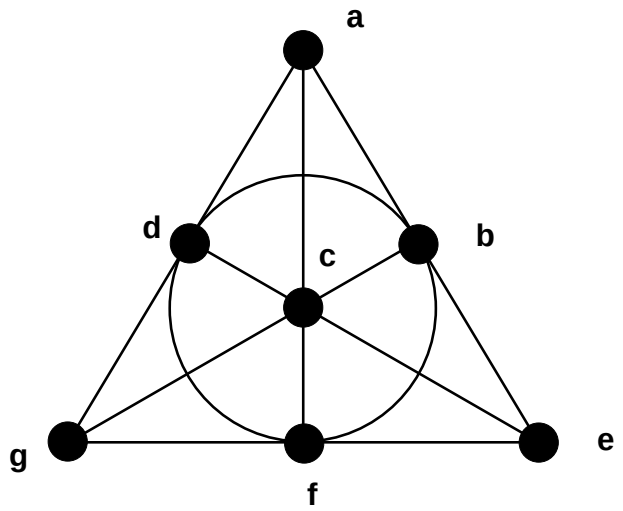


Designs

Heawood Graph



Fano Ebene



Designs über endlichen Körper

- Menge von v Punkten
- Menge von $k-$Blöcken
- $t-(v,k,\lambda)$ Design
  Jede $t-$Menge von Punkten in genau λ Blöcken

Designs über endlichen Körper

- ~~Menge von v Punkten~~
  Vektorraum $GF(q)^v$
- Menge von $k-$Blöcken

- $t-(v,k,\lambda)$ Design
  Jede $t-$Menge von Punkten in genau λ Blöcken

Designs über endlichen Körper

- ~~Menge von v Punkten~~
  Vektorraum $GF(q)^v$
- ~~Menge von $k-$ Blöcken~~
  Menge $\mathcal{B}$ von $k-$dimensionalen Unterräumen von $GF(q)^v$
- $t-(v,k,\lambda)$ Design
  Jede $t-$Menge von Punkten in genau λ Blöcken

Designs über endlichen Körper

- ~~Menge von v Punkten~~
  Vektorraum $GF(q)^v$
- ~~Menge von $k-$ Blöcken~~
  Menge $\mathcal{B}$ von $k-$dimensionalen Unterräumen von $GF(q)^v$
- ~~$t-(v,k,\lambda)$ Design~~
  ~~Jede $t-$ Menge von Punkten in genau λ Blöcken~~
  $t-(v,k,\lambda)$ $q-$Design
  jeder $t-$dimensionale Unterraum in genau λ der $k-$dimensionalen Räume aus $\mathcal{B}$

aktueller Stand

bekannt:

- Thomas (1987): untersuchte als erster $2-$Designs
- Braun, Kerber, Laue (2005): erste $3-$design

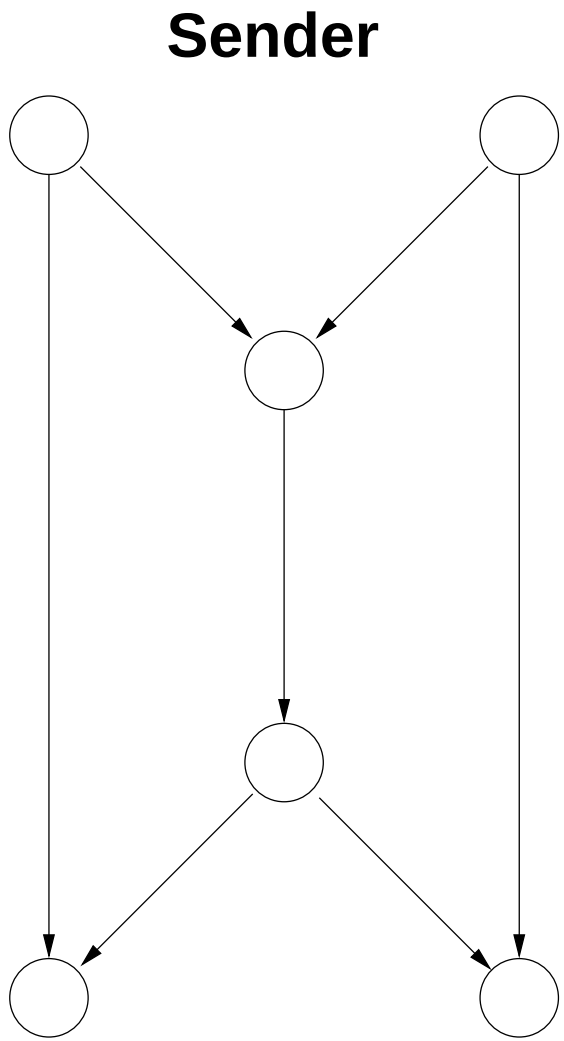
gesucht:

- $q-$analog der Fano Ebene?
- Steinersysteme ? $(\lambda = 1)$
- $t > 3$?

UNIVERSITÄT BAYREUTH

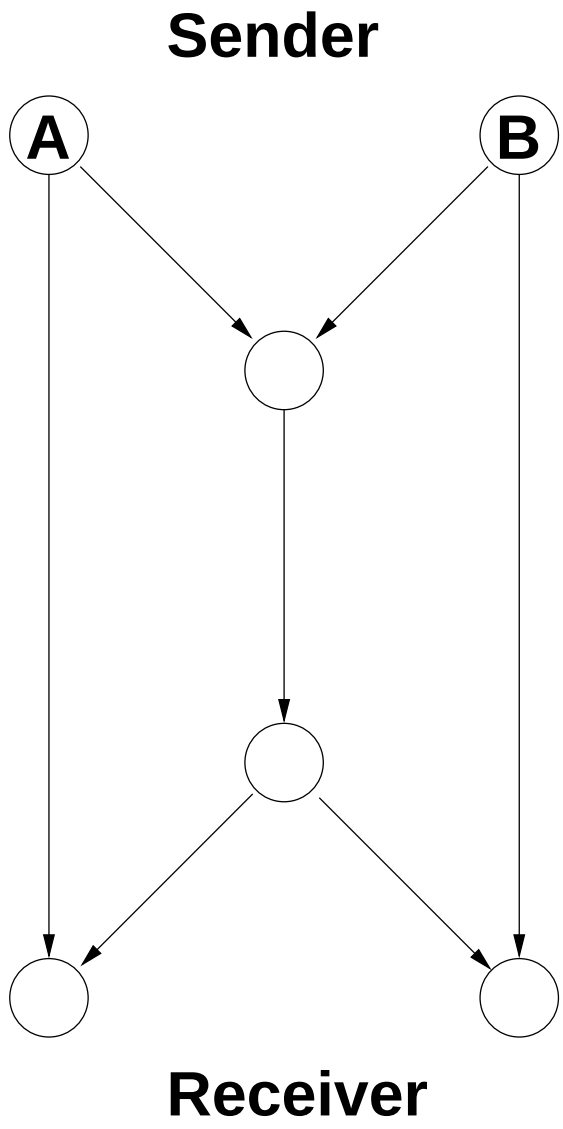
II - Network Codes

Network Codes



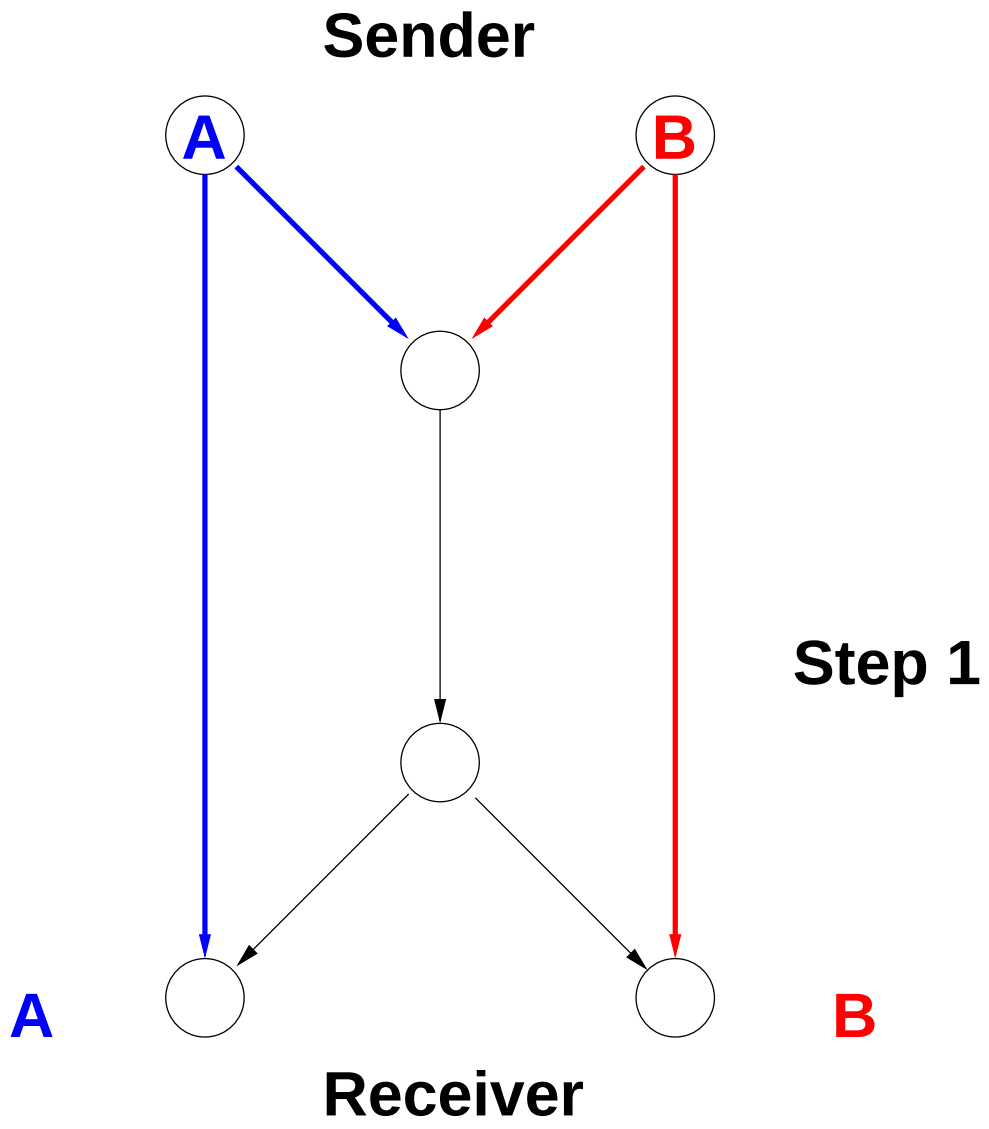
UNIVERSITÄT BAYREUTH

Network Codes



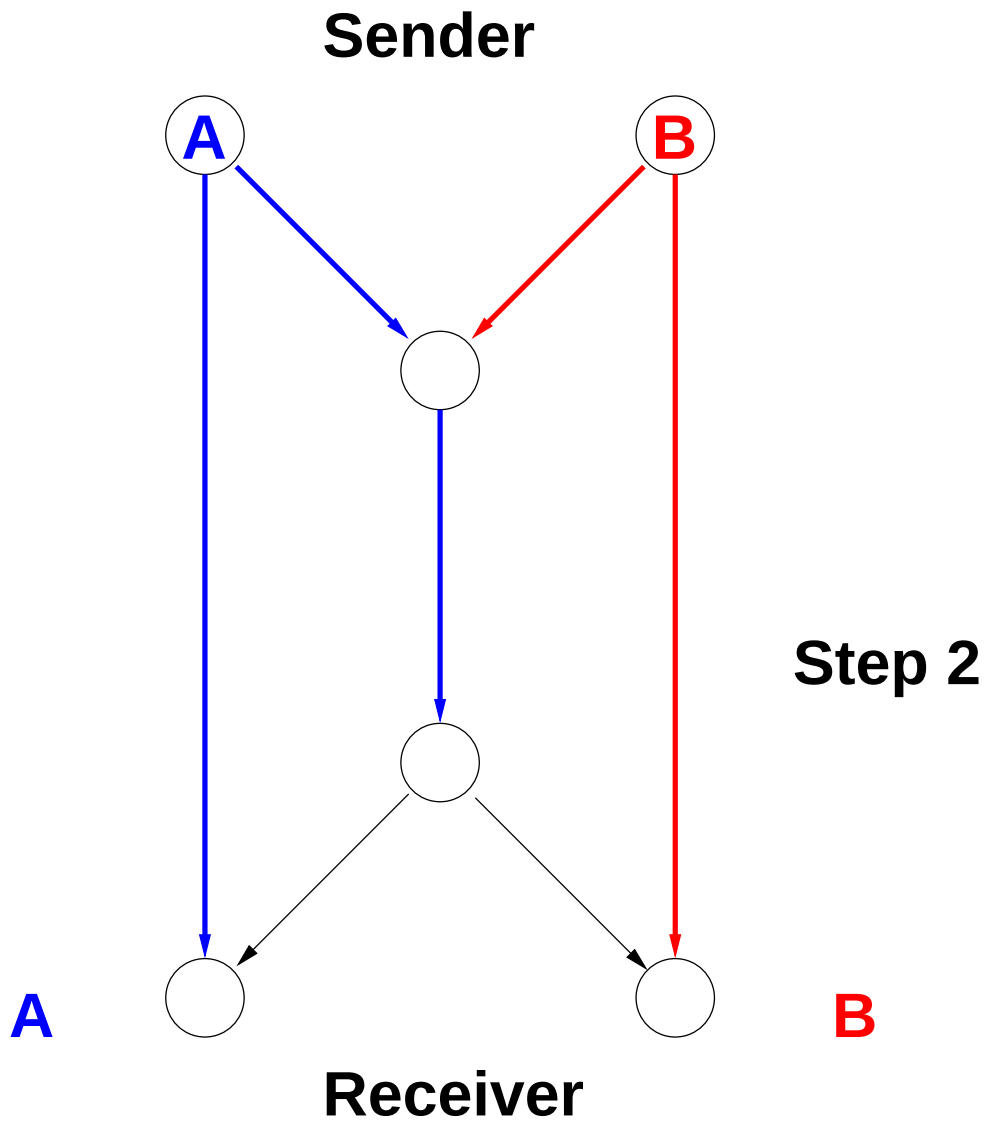
UNIVERSITÄT BAYREUTH

Network Codes

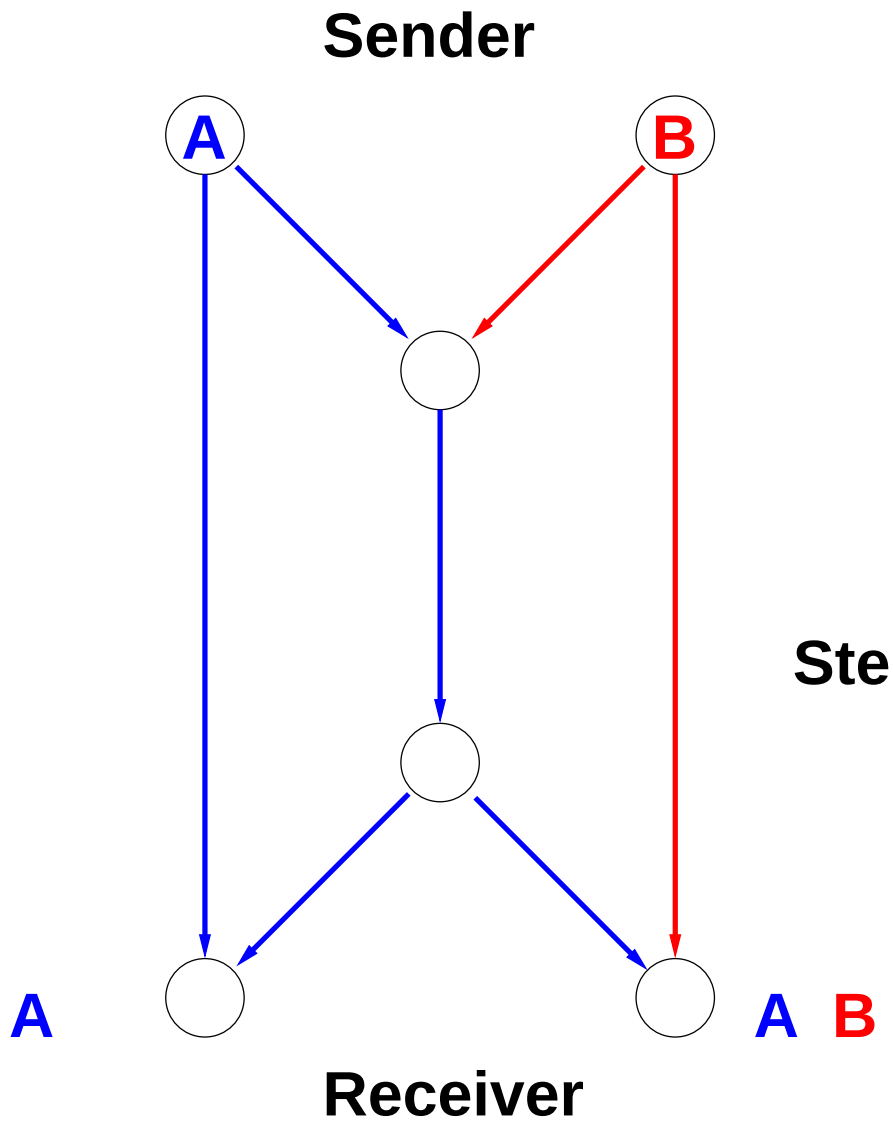


UNIVERSITÄT BAYREUTH

Network Codes

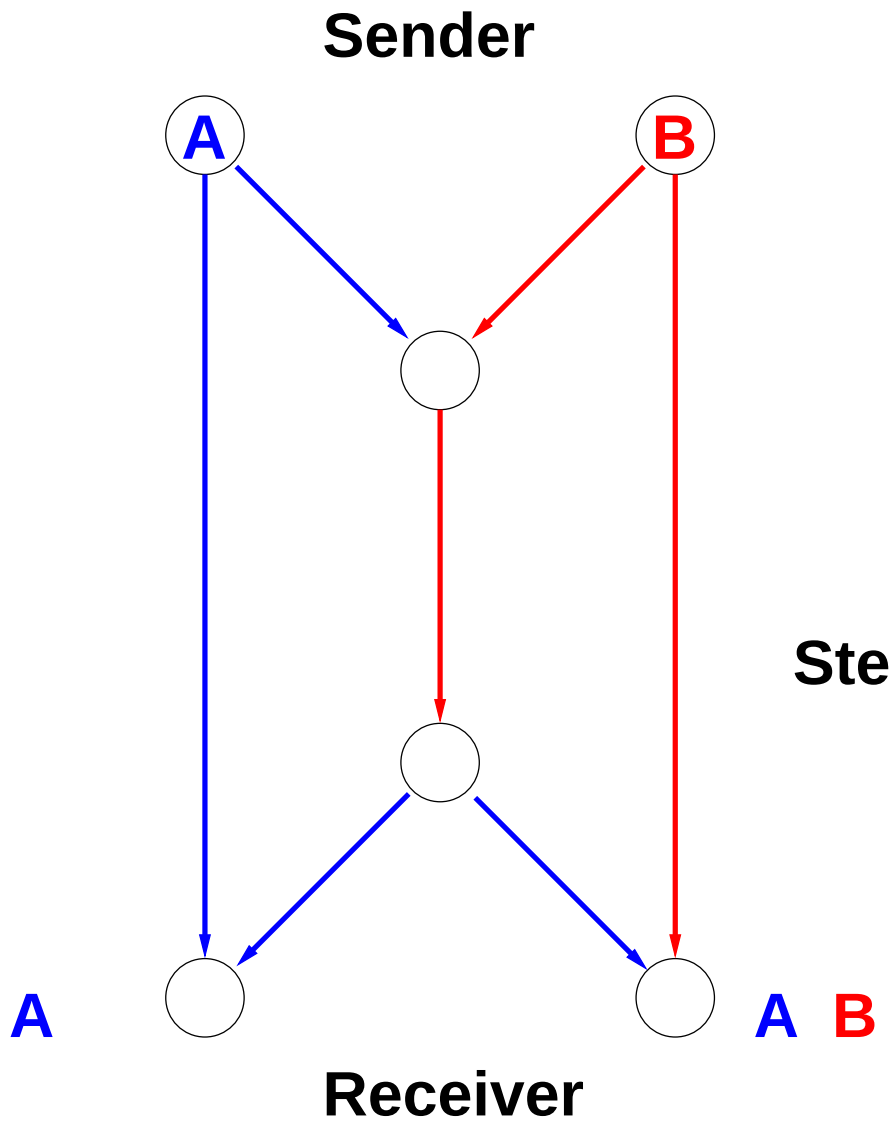


Network Codes



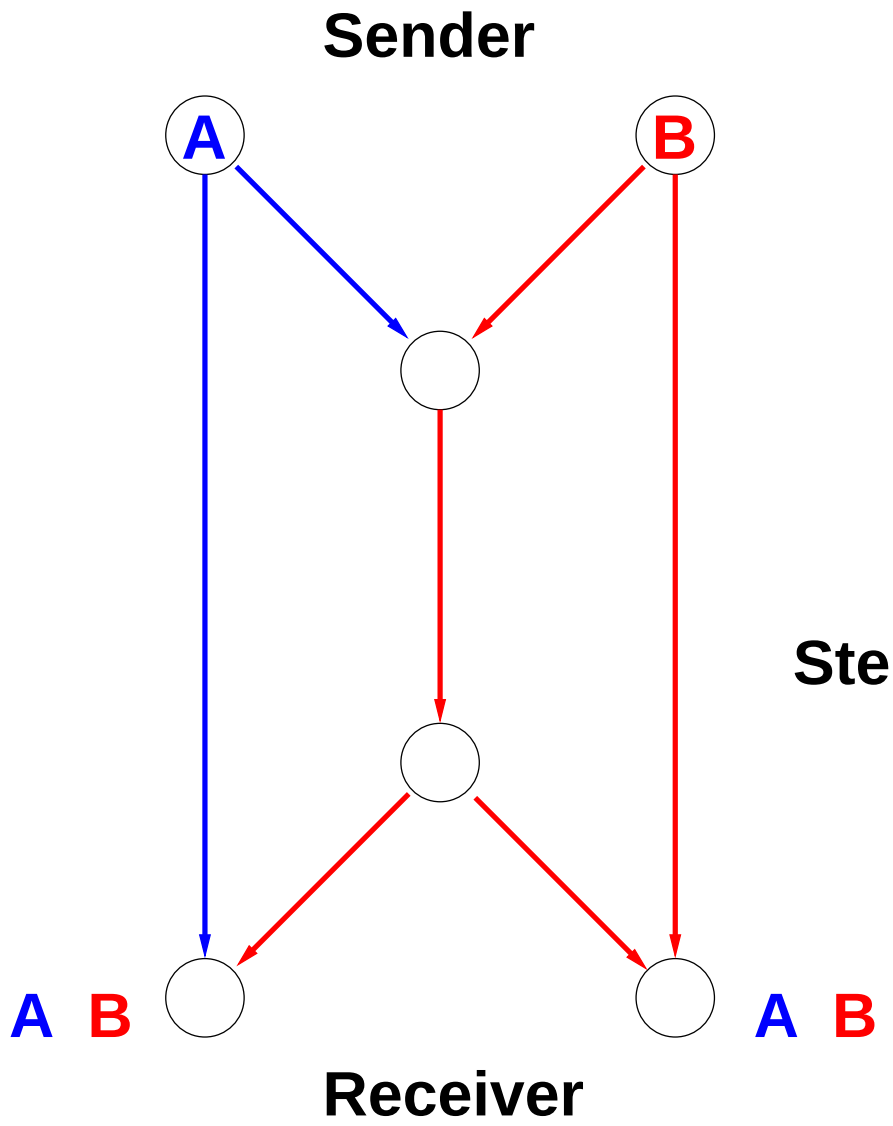
UNIVERSITÄT BAYREUTH

Network Codes

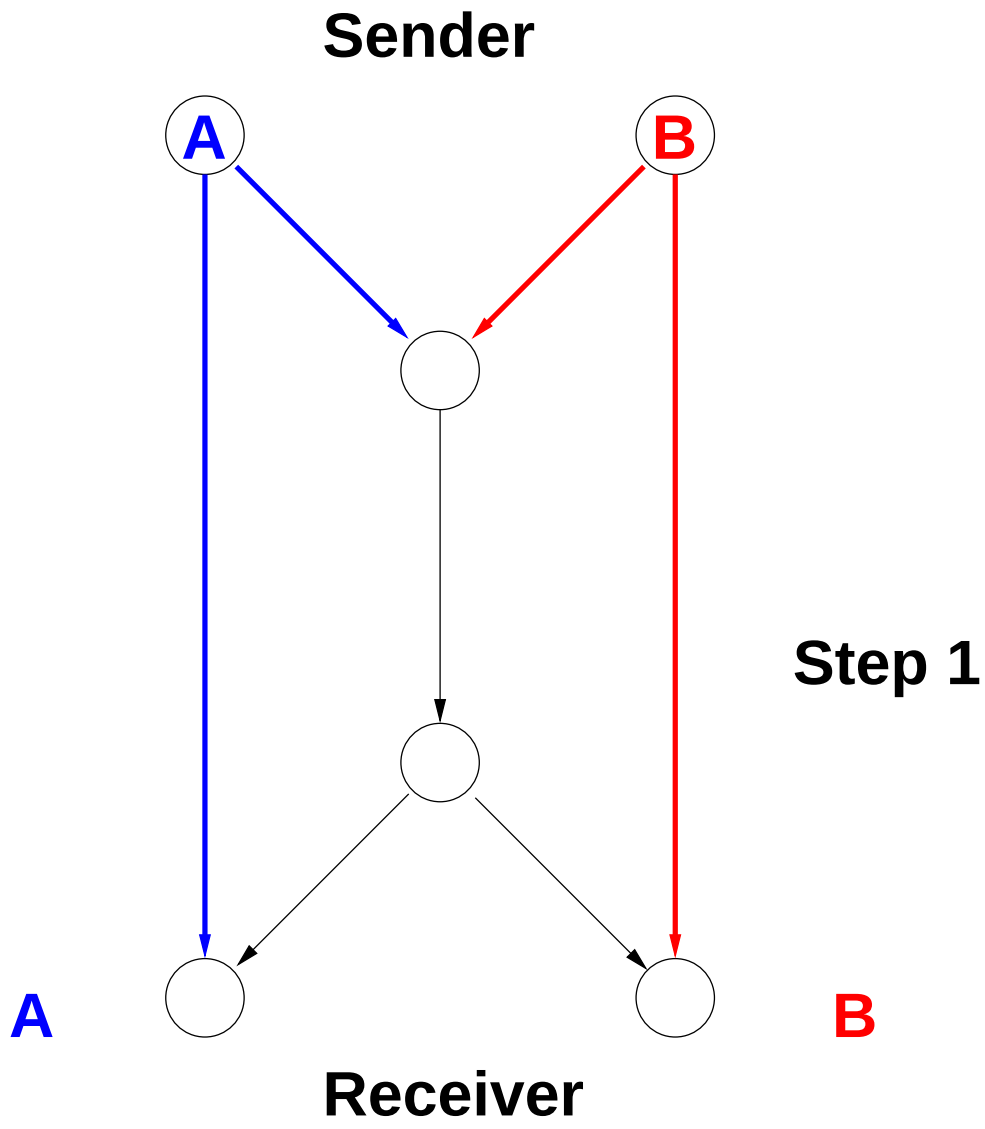


UNIVERSITÄT BAYREUTH

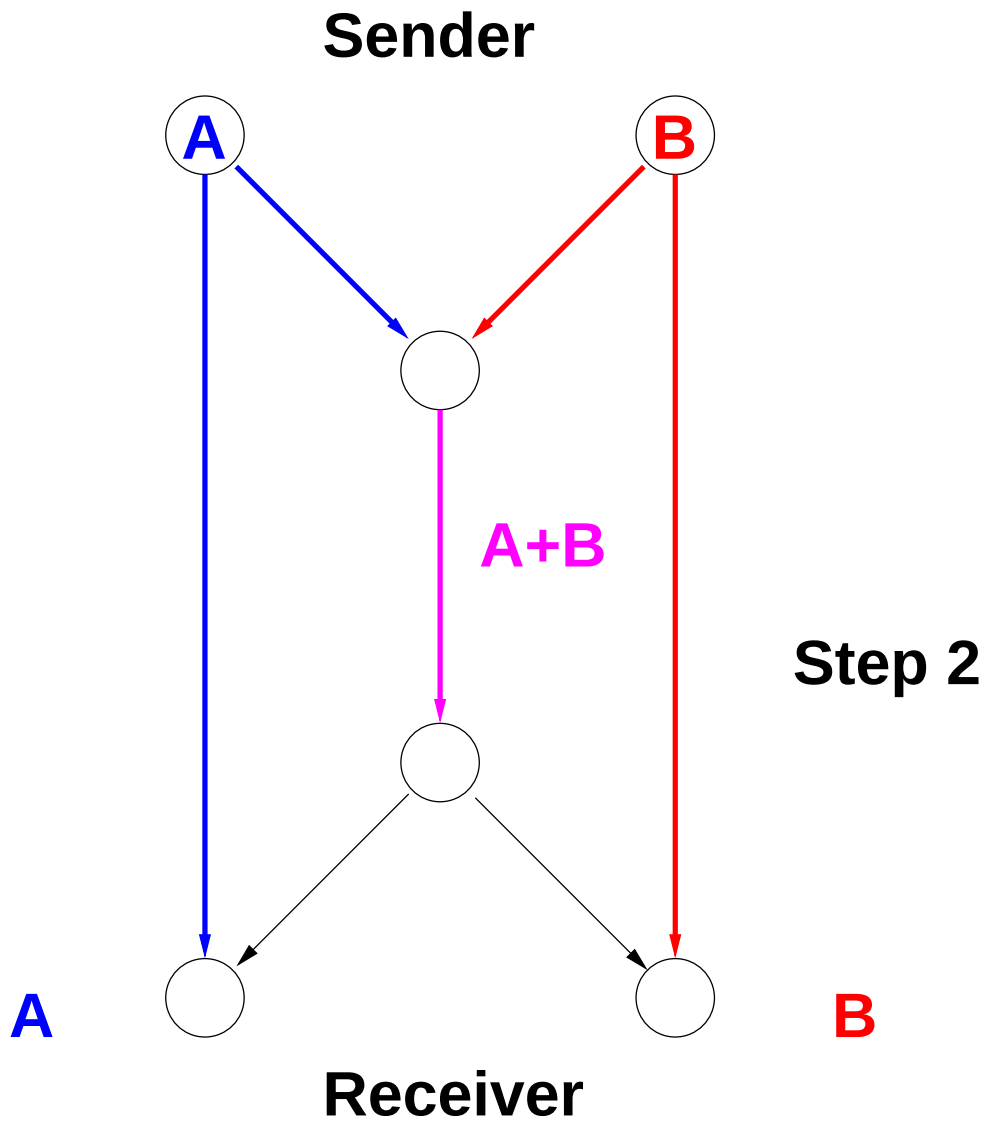
Network Codes



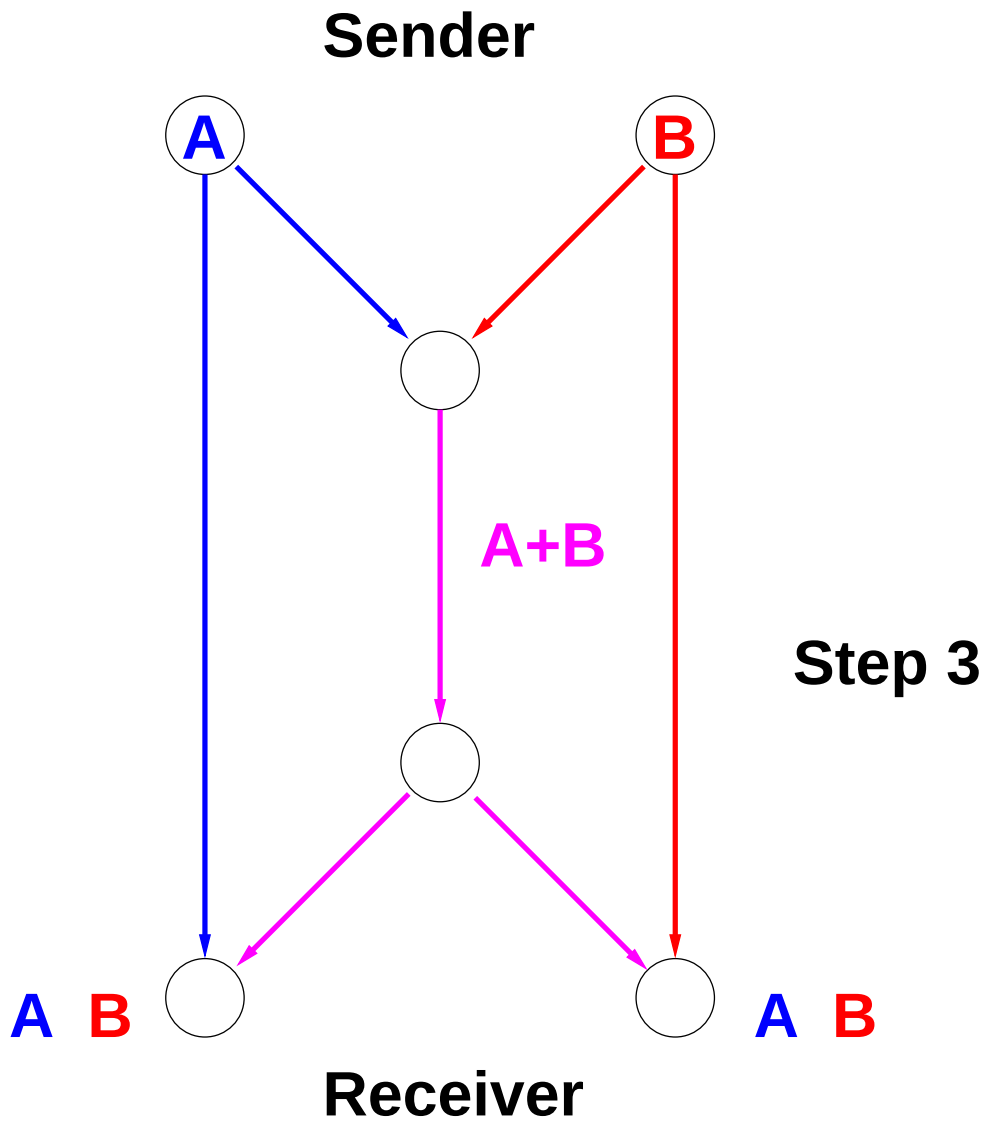
Network Codes



Network Codes



Network Codes



UNIVERSITÄT BAYREUTH

Network Codes

Modell (Kötter, Kschischang)
Nachricht:

- Vektorraum V

Network Codes

Modell (Kötter, Kschischang)
Nachricht:

- Vektorraum V

Knoten im Netzwerk:

- empfängt mehrere $v_i \in V$
- sendet zufällig Linearkombination der v_i= EXOR

Fehlerkorrigierende Network Codes

Codewort:

- Unterraum von $GF(q)^v$

Fehlerkorrigierende Network Codes

Codewort:

- Unterraum von $GF(q)^v$

Distanz d:

- Abstand im Hasse-Diagramm der Unterräume von $GF(q)^v$= Linearer Verband

Fehlerkorrigierende Network Codes

Codewort:

- Unterraum von $GF(q)^v$

Distanz d:

- Abstand im Hasse-Diagramm der Unterräume von $GF(q)^v$= Linearer Verband

$U, W < GF(q)^v$:

$$d(U,W) = dim(U) + dim(W) - 2dim(U \cap W)$$

UNIVERSITÄT BAYREUTH

Fehlerkorrigierende Network Codes

für festes d:

Finde eine Menge von Unterräumen in $GF(q)^v$ mit paarweisen Abstand $\geq d$

Fehlerkorrigierende Network Codes

für festes d:

> Finde eine Menge von Unterräumen in $GF(q)^v$ mit paarweisen Abstand $\geq d$

zusätzliche feste Dimension k der Unterräume:

> Finde eine Menge von $k-$dimensionalen Unterräumen in $GF(q)^v$ mit paarweisen Abstand $\geq 2d$

Fehlerkorrigierende Network Codes

für festes d:

> Finde eine Menge von Unterräumen in $GF(q)^v$ mit paarweisen Abstand $\geq d$

zusätzliche feste Dimension k der Unterräume:

> Finde eine Menge von $k-$dimensionalen Unterräumen in $GF(q)^v$ mit paarweisen Abstand $\geq 2d$

'constant dimension codes' $\approx q-$ Analog der 'constant weight codes'

Codes und Designs

Aus einem $t-(v,k,1)\ q-$Design erhält man einen constant dimension code mit Minimaldistanz $2(k-(t-1))$ da der paarweise Schnitt Dimension $\leq t-1$ hat.

Codes und Designs

Aus einem $t-(v,k,1)$ $q-$Design erhält man einen constant dimension code mit Minimaldistanz $2(k-(t-1))$ da der paarweise Schnitt Dimension $\leq t-1$ hat.

Finde $k-$dim. Räume in $GF(q)^v$ sodass jeder $t-$dim. Raum in genau 1 $k-$Raum ist
= Steiner system = perfekter Code

Codes und Designs

Aus einem $t-(v,k,1)$ $q-$Design erhält man einen constant dimension code mit Minimaldistanz $2(k-(t-1))$ da der paarweise Schnitt Dimension $\leq t-1$ hat.

Finde $k-$dim. Räume in $GF(q)^v$ sodass jeder $t-$dim. Raum in genau 1 $k-$Raum ist
= Steiner system = perfekter Code

Finde $k-$dim. Räume in $GF(q)^v$ sodass jeder $t-$dim. Raum in höchstens 1 $k-$Raum ist
= fehlerkorrigierender network code

aktueller Stand

Definiere $A_q(v,k,d)$ als die maximale Anzahl von Codewörtern eines constant dimension codes mit Minimaldistanz d, Dimension k, und Grundraum = $GF(q)^v$

aktueller Stand

Definiere $A_q(v,k,d)$ als die maximale Anzahl von Codewörtern eines constant dimension codes mit Minimaldistanz d, Dimension k, und Grundraum = $GF(q)^v$

offene Probleme:

- untere (Konstruktion) und obere Schranken für $A_q(v,k,d)$
- Konstruktion 'guter' codes
- sehr interessant: $A_2(7,3,4)$ = Fano Ebene

III - Konstruktion

Problem

Finde $k-$dim. Räume in $GF(q)^v$ sodass jeder $t-$dim. Raum in höchstens 1 $k-$Raum ist
= fehlerkorrigierender network code

Problem

Finde $k-$dim. Räume in $GF(q)^v$ sodass jeder $t-$dim. Raum in höchstens 1 $k-$Raum ist
= fehlerkorrigierender network code

D:= Inzidenz Matrix zwischen $k-$Räumen und $t-$Räumen in $GF(q)^v$

$$D_{U,V} := \begin{cases} 1 & t\text{-Raum } U \text{ ist in } k- \text{ Raum } W \text{ enthalten} \\ 0 & \text{sonst} \end{cases}$$

Problem der kombinatorischen Optimierung

Finde $0/1$-Lösung $x = (x_1, \ldots, x_s)$ sodass

Problem der kombinatorischen Optimierung

Finde $0/1$-Lösung $x = (x_1, \ldots, x_s)$ sodass

- $x_1 + \ldots + x_s$ möglichst groß und

Problem der kombinatorischen Optimierung

Finde $0/1$-Lösung $x = (x_1, \ldots, x_s)$ sodass

- $x_1 + \ldots + x_s$ möglichst groß und
- $Dx^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

Problem der kombinatorischen Optimierung

Finde $0/1$-Lösung $x = (x_1, \ldots, x_s)$ sodass

- $x_1 + \ldots + x_s$ möglichst groß und
- $Dx^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

Lösung = charakteristischer Vektor eines network codes mit Minimaldistanz $\geq 2(k - t + 1)$.

Automorphismen

Automorphismus φ von $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$

Betrachte $G < Aut(GF(q)^v)$

Automorphismen

Automorphismus φ von $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$

Betrachte $G < Aut(GF(q)^v)$

- schrumpfe Matrix D indem man Spalten addiert, die im gleichen $G-$Orbit auf den $k-$Räumen (=Spalten-labels)

$\Rightarrow$ Zeilen innerhalb eines $G-$Orbits auf den $t-$Räumen sind gleich

Automorphismen

Automorphismus φ von $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$
Betrachte $G < Aut(GF(q)^v)$

- schrumpfe Matrix D indem man Spalten addiert, die im gleichen $G-$Orbit auf den $k-$Räumen (=Spalten-labels)

$\Rightarrow$ Zeilen innerhalb eines $G-$Orbits auf den $t-$Räumen sind gleich

- D^G :=geschrumpfte Matrix

$\Rightarrow$Anzahl Spalten = Anzahl Orbits von $k-$Räumen
Anzahl Zeilen = Anzahl Orbits von $t-$Räumen

Geschrumpfte Problem

$b_1, \ldots, b_m$ Orbitgrößen auf $k-$Räumen. Finde $0/1$-Lösung $x = (x_1, \ldots, x_m)$ sodass

Geschrumpfte Problem

$b_1, \ldots, b_m$ Orbitgrößen auf $k-$Räumen. Finde $0/1$-Lösung $x = (x_1, \ldots, x_m)$ sodass

- $b_1 x_1 + \ldots + b_m x_m$ möglichst groß und

Geschrumpfte Problem

$b_1, \ldots, b_m$ Orbitgrößen auf $k-$Räumen. Finde $0/1$-Lösung $x = (x_1, \ldots, x_m)$ sodass

- $b_1 x_1 + \ldots + b_m x_m$ möglichst groß und
- $D^G x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

Geschrumpfte Problem

$b_1, \ldots, b_m$ Orbitgrößen auf $k-$Räumen. Finde $0/1$-Lösung $x = (x_1, \ldots, x_m)$ sodass

- $b_1 x_1 + \ldots + b_m x_m$ möglichst groß und
- $D^G x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

Lösung = Network code mit vorgeschriebenen Automorphismen und Minimaldistanz $\geq 2(k - t + 1)$.

Ergebnisse (binär)

v	k	number of codewords: new	old	d
6	3	77	71	4
7	3	304	294	4
8	3	1275	1164	4
9	3	5621	4657	4
10	3	21483	18631	4
11	3	79833	74531	4
12	3	315315	298139	4

Offene Probleme

- real world $v = 100$
- Vollständiges System mit Encoding/Decoding
- schnelle Algorithmen für die Berechnung von D^G

IV - Decodieren

Neue Sichtweise

Singer Zyklus als Gruppe von Automorphismen wurde erfolgreich verwendet.

Neue Sichtweise

Singer Zyklus als Gruppe von Automorphismen wurde erfolgreich verwendet.
Neue Sichtweise:

- statt $GF(2)^v$ als Grundraum, Körper $GF(2^v)$
- Spezialfall $k = 3$
- Spezialfall $t = 2$, zwei Unterräume haben höchstens ein Nichtnullelement gemeinsam
- Singerzykel = Multiplikation mit Erzeuger ω der Einheitengruppe $GF(2^v)^*$.

Beschreibung Orbit

- Ein $3-$Raum = 7 Elemente aus $GF(2^v)^*$= $\{\omega^{i_1}, \ldots, \omega^{i_7}\}$

Beschreibung Orbit

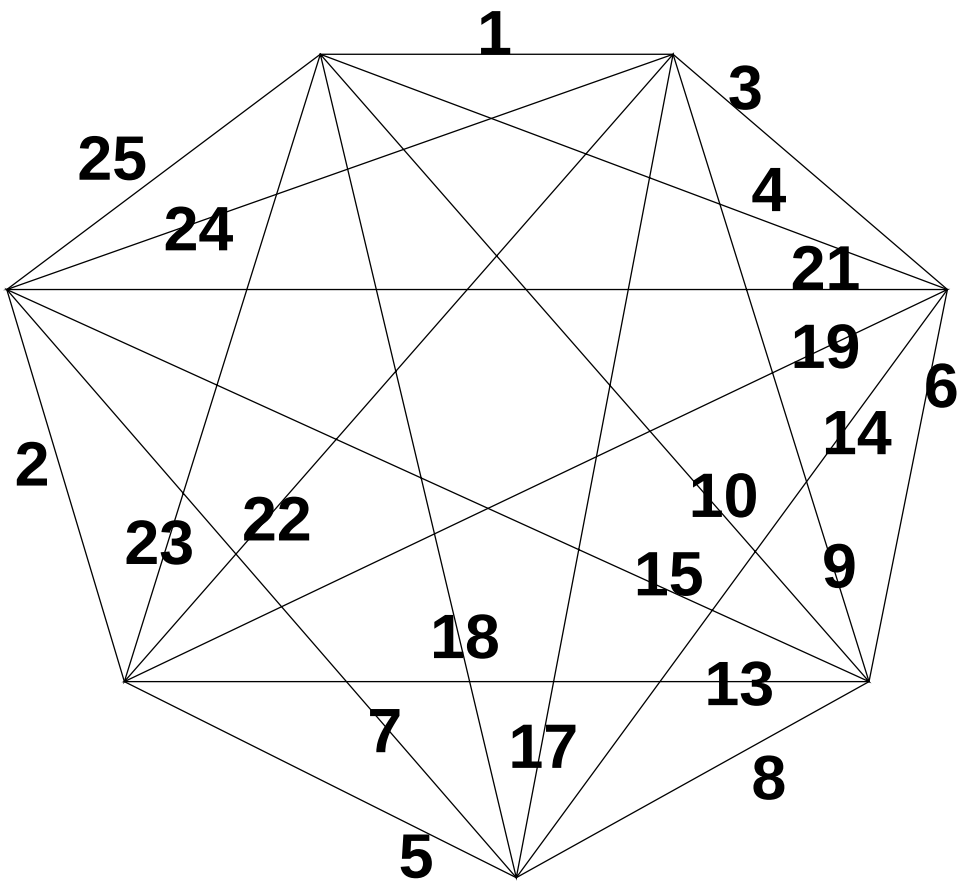
- Ein $3-$Raum = 7 Elemente aus $GF(2^v)^*$= $\{\omega^{i_1},\ldots,\omega^{i_7}\}$
- Gruppenoperation ist Multiplikation mit ω, Orbit =$\{\ \{\omega^{i_1},\ldots,\omega^{i_7}\},\{\omega^{i_1+1},\ldots,\omega^{i_7+1}\},\ldots\}$

Beschreibung Orbit

- Ein $3-$Raum = 7 Elemente aus $GF(2^v)^*$= $\{\omega^{i_1},\ldots,\omega^{i_7}\}$
- Gruppenoperation ist Multiplikation mit ω, Orbit =$\{\ \{\omega^{i_1},\ldots,\omega^{i_7}\},\{\omega^{i_1+1},\ldots,\omega^{i_7+1}\},\ldots\}$
- invariant bleiben die $7\cdot 6$ paarweisen Quotienten innerhalb des $k-$Raums (Vorteil Körper)

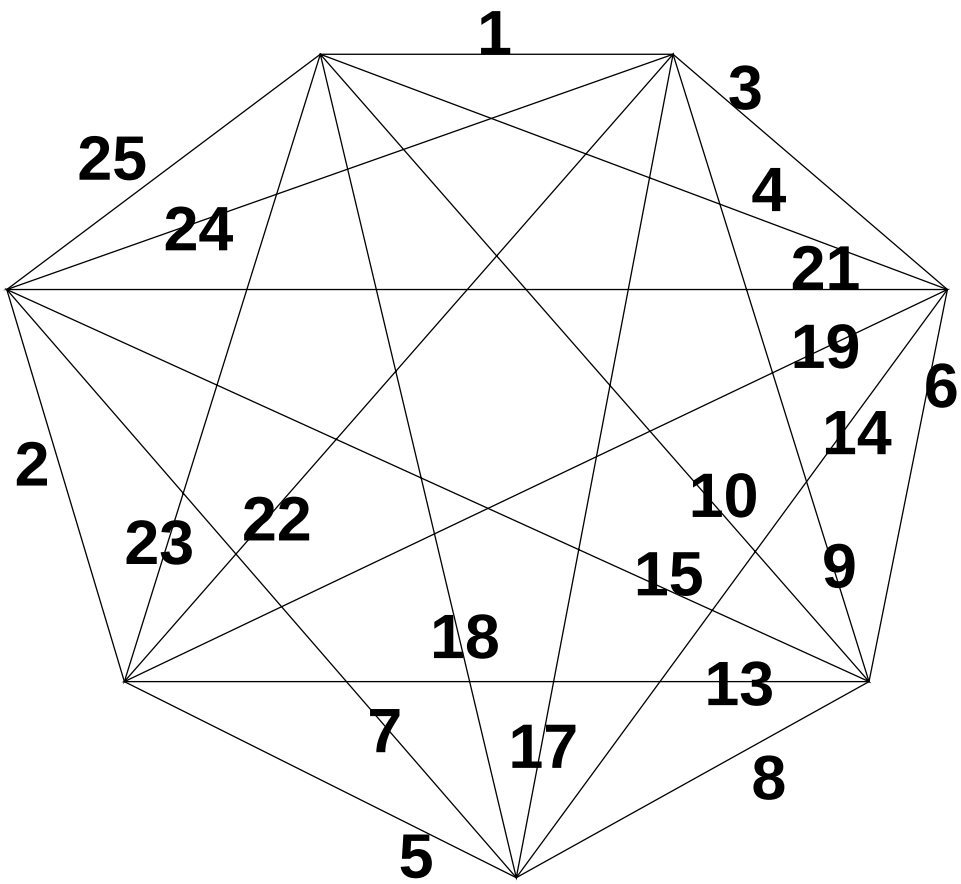
Beschreibung Orbit

$G_O =$



Beschreibung Orbit

$G_O =$



Die $3-$Räume des Orbits schneiden paarweise maximal $1-$dimensional $\Longleftrightarrow$ alle Quotienten sind verschieden

Beschreibung Orbit

Finde jetzt möglichst viele Singerorbits auf den $3-$Räumen, sodass alle paarweisen Quotienten verschieden sind. Dann bildet die Vereinigung der Bahnen einen Code mit Minimaldistanz 4. Für größere Werte:

v	k	n =Orbits für Code	Anzahl Codewörter	$d_S = 2d$
15	3	555	$555 \cdot \left(2^{15}-1\right) = 18185685$	4
16	3	1056	69204960	4
17	3	2108	276297668	4
18	3	4032	1056960576	4

Decodieren

- Spezialfall $n = 1$,
  d.h. nur ein Orbit des Singerzykels als Code.
- Anzahl Codewörter = $2^v - 1$
- gesendet wurde ein $3-$Raum $V < GF(2^v)$

Decodieren

- Spezialfall $n = 1$,
  d.h. nur ein Orbit des Singerzykels als Code.
- Anzahl Codewörter = $2^v - 1$
- gesendet wurde ein $3-$Raum $V < GF(2^v)$

Zwei Fehler sind bei $d = 4$ zu beheben:

- Error (d.h. empfangen wurde ein $4-$Raum $U > V$)
- Erasure (d.h. empfangen wurde ein $2-$Raum $U < V$)

Erasure

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $2-$Raum $U = \{x_1, x_2, x_3, 0\}$

Erasure

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $2-$Raum $U = \{x_1, x_2, x_3, 0\}$
- Bestimme den Quotienten x_1 / x_2.

Erasure

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $2-$Raum $U = \{x_1, x_2, x_3, 0\}$
- Bestimme den Quotienten x_1 / x_2.
- Damit identifiziert man zwei Knoten aus dem Graphen G_O

Erasure

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $2-$Raum $U = \{x_1, x_2, x_3, 0\}$
- Bestimme den Quotienten x_1 / x_2.
- Damit identifiziert man zwei Knoten aus dem Graphen G_O
- Mit einer weiteren Multiplikationen mit einem Kantenlabel aus G_O erhält man einen dritten Basisvektor

Erasure

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $2-$Raum $U = \{x_1, x_2, x_3, 0\}$
- Bestimme den Quotienten x_1 / x_2.
- Damit identifiziert man zwei Knoten aus dem Graphen G_O
- Mit einer weiteren Multiplikationen mit einem Kantenlabel aus G_O erhält man einen dritten Basisvektor
- Aufwand: eine Multiplikation und eine Division in $GF(2^v)$

Error

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $4-$Raum U

Error

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $4-$Raum U
- Wähle einen beliebigen $3-$Unterraum $W < U$, wir wissen dass $W \cap V$ mindestens $2-$dimensional ist

Error

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $4-$Raum U
- Wähle einen beliebigen $3-$Unterraum $W < U$, wir wissen dass $W \cap V$ mindestens $2-$dimensional ist
- Betrachte die sieben $2-$dimensionalen Unterräume von W

Error

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $4-$Raum U
- Wähle einen beliebigen $3-$Unterraum $W < U$, wir wissen dass $W \cap V$ mindestens $2-$dimensional ist
- Betrachte die sieben $2-$dimensionalen Unterräume von W
- In einem dieser Unterräume funktioniert die Erasure Variante

Error

- Gesendet wurde ein $3-$Raum V, empfangen wurde ein $4-$Raum U
- Wähle einen beliebigen $3-$Unterraum $W < U$, wir wissen dass $W \cap V$ mindestens $2-$dimensional ist
- Betrachte die sieben $2-$dimensionalen Unterräume von W
- In einem dieser Unterräume funktioniert die Erasure Variante
- Aufwand: 7 Multiplikationen und 7 Divisionen

Allgemeiner

- Das geht auch mit n statt einem Orbit
- Das geht auch für $k > 3$
- Das geht auch für $t > 2$

Literatur

A.S. Elsenhans, A. Kohnert, A. Wassermann: *Construction of Codes for Network Coding* , Proceedings MTNS 2010.

T. Etzion, N. Silberstein: several papers on arxiv.org

A. Kohnert, S. Kurz: *Construction of Large Constant Dimension Codes With a Prescribed Minimum Distance*, LNCS, 2008.

R. Kötter, F. Kschischang: *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory, **54**, 3579–3590, 2008.

Literatur

A.S. Elsenhans, A. Kohnert, A. Wassermann: *Construction of Codes for Network Coding* , Proceedings MTNS 2010.

T. Etzion, N. Silberstein: several papers on arxiv.org

A. Kohnert, S. Kurz: *Construction of Large Constant Dimension Codes With a Prescribed Minimum Distance*, LNCS, 2008.

R. Kötter, F. Kschischang: *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory, **54**, 3579–3590, 2008.

Danke.