Large Constant Dimension Codes

Axel Kohnert

Ghent May 2009

Bayreuth University Germany

axel.kohnert@uni-bayreuth.de

UNIVERSITÄT
BAYREUTH

- Designs
- Network Codes
- Construction

Designs

Designs

- a set of v points

Designs

- a set of v points
- a set of blocks (block = set of points)

UNIVERSITÄT BAYREUTH

Designs

- a set of v points
- a set of blocks (block = set of points)
- $t-(v,k,\lambda)$ Design

UNIVERSITÄT BAYREUTH

Designs

- a set of v points
- a set of blocks (block = set of points)
- $t-(v,k,\lambda)$ Design
  each block is a $k-$set
  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT BAYREUTH

Designs

- a set of v points

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

- a set of blocks (block = set of points)

- $t-(v,k,\lambda)$ Design

  each block is a $k-$set

  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT BAYREUTH

Designs

- a set of v points

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

- a set of blocks (block = set of points)

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

- $t-(v,k,\lambda)$ Design
  each block is a $k-$set
  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT BAYREUTH

Designs

- a set of v points

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

- a set of blocks (block = set of points)

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

- $t-(v,k,\lambda)$ Design
  each block is a $k-$set
  each $t-$set of points is in exactly λ blocks

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

UNIVERSITÄT
BAYREUTH

Designs over Finite Fields

- a set of v points

- a set of $k-$blocks

- $t-(v,k,\lambda)$ Design
  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT BAYREUTH

Designs over Finite Fields

- ~~a set of v points~~

  linear $v-$space $GF(q)^v$
- a set of $k-$blocks

- $t-(v,k,\lambda)$ Design

  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT
BAYREUTH

Designs over Finite Fields

- ~~a set of v points~~

  linear $v-$space $GF(q)^v$

- ~~a set of $k-$blocks~~

  a set of $k-$spaces in $GF(q)^v$

- $t-(v,k,\lambda)$ Design

  each $t-$set of points is in exactly λ blocks

UNIVERSITÄT BAYREUTH

Designs over Finite Fields

- ~~a set of v points~~

  linear $v-$space $GF(q)^v$

- ~~a set of $k-$blocks~~

  a set of $k-$spaces in $GF(q)^v$

- ~~$t-(v,k,\lambda)$ Design~~
  ~~each $t-$set of points is in exactly λ blocks~~

  $t-(v,k,\lambda)$ $q-$Design
  each $t-$space of $GF(q)^v$ is in exactly
  λ of the $k-$spaces

UNIVERSITÄT BAYREUTH

Current State

known:

- Thomas (1987): first to study, $2-$designs
- Braun, Kerber, Laue (2005): first $3-$design

open problems:

- $q-$analog of the Fano plane?
- Steiner systems ? $(\lambda = 1)$
- $t > 3$?

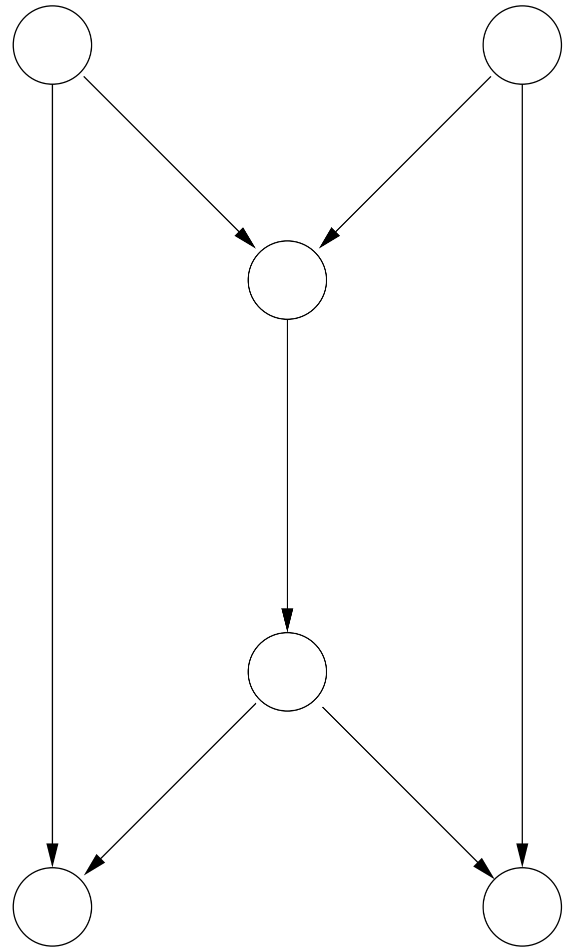
UNIVERSITÄT BAYREUTH

Network Codes

UNIVERSITÄT
BAYREUTH

Network Codes

Sender

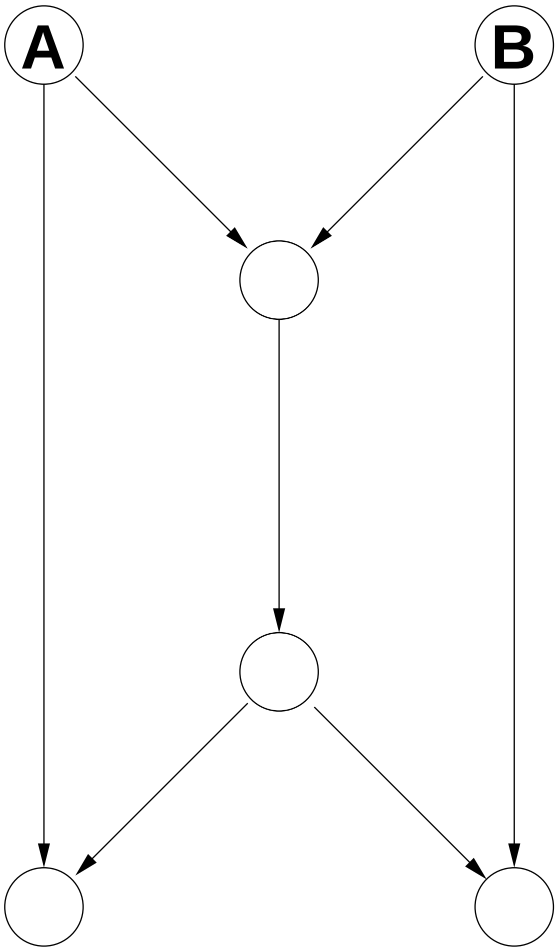


Receiver

UNIVERSITÄT
BAYREUTH

Network Codes

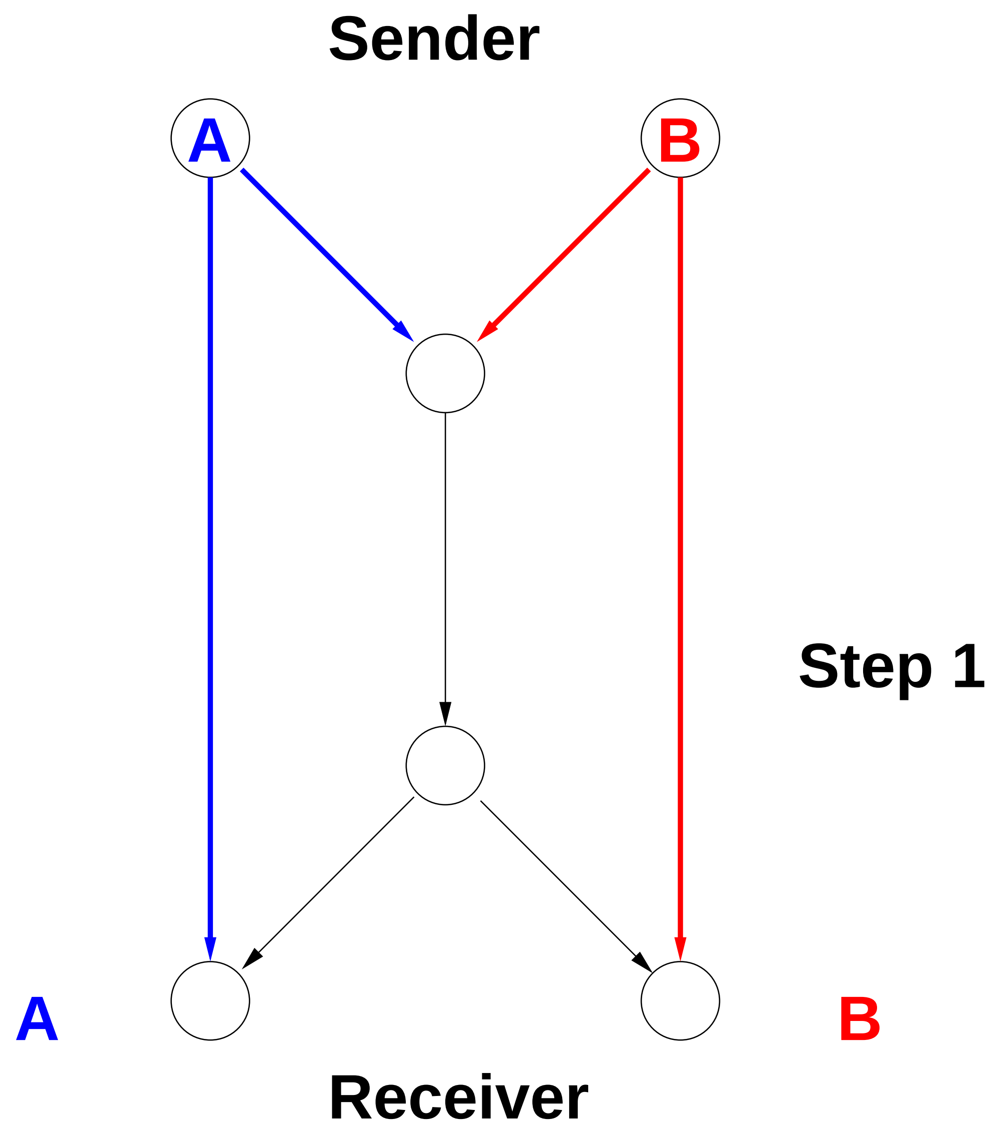
Sender



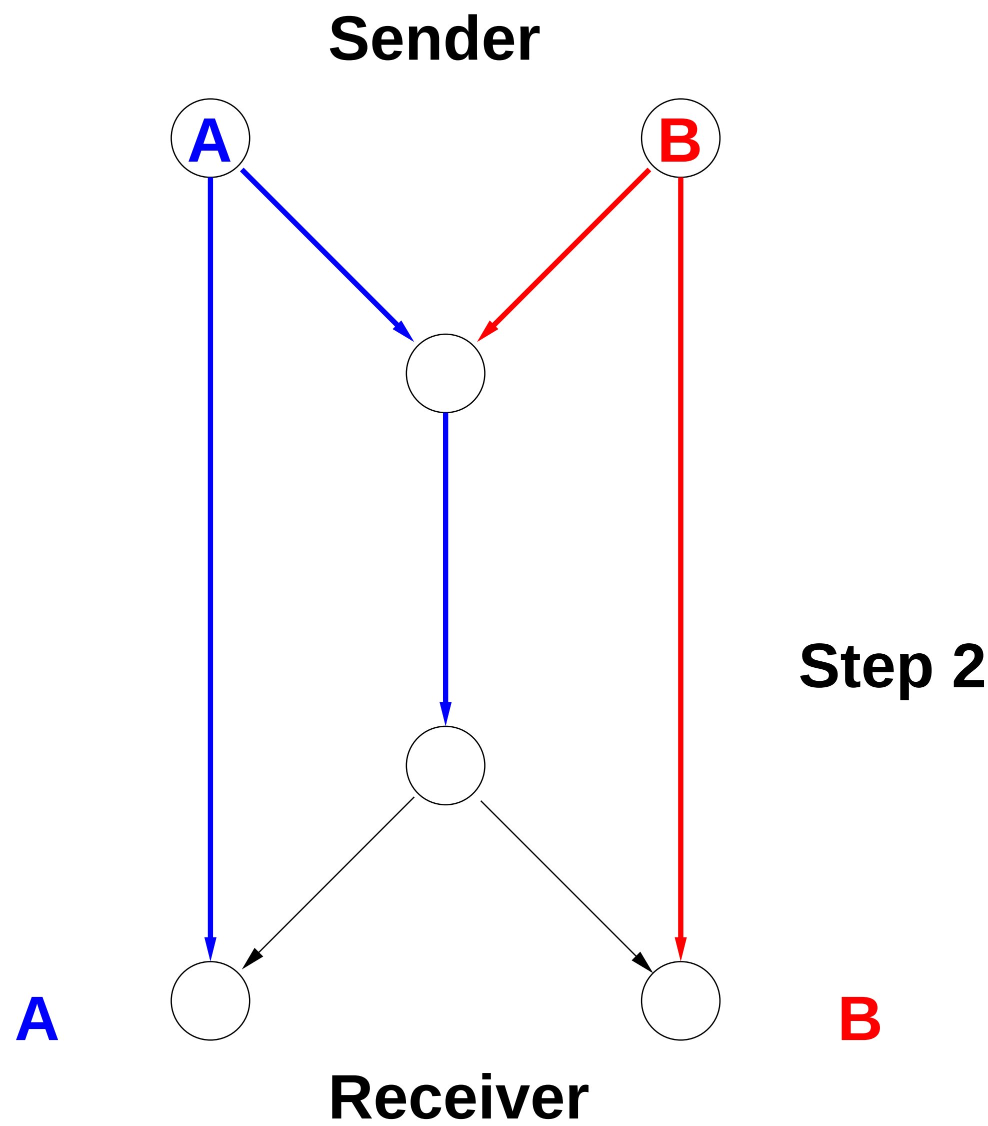
Receiver

UNIVERSITÄT
BAYREUTH

Network Codes

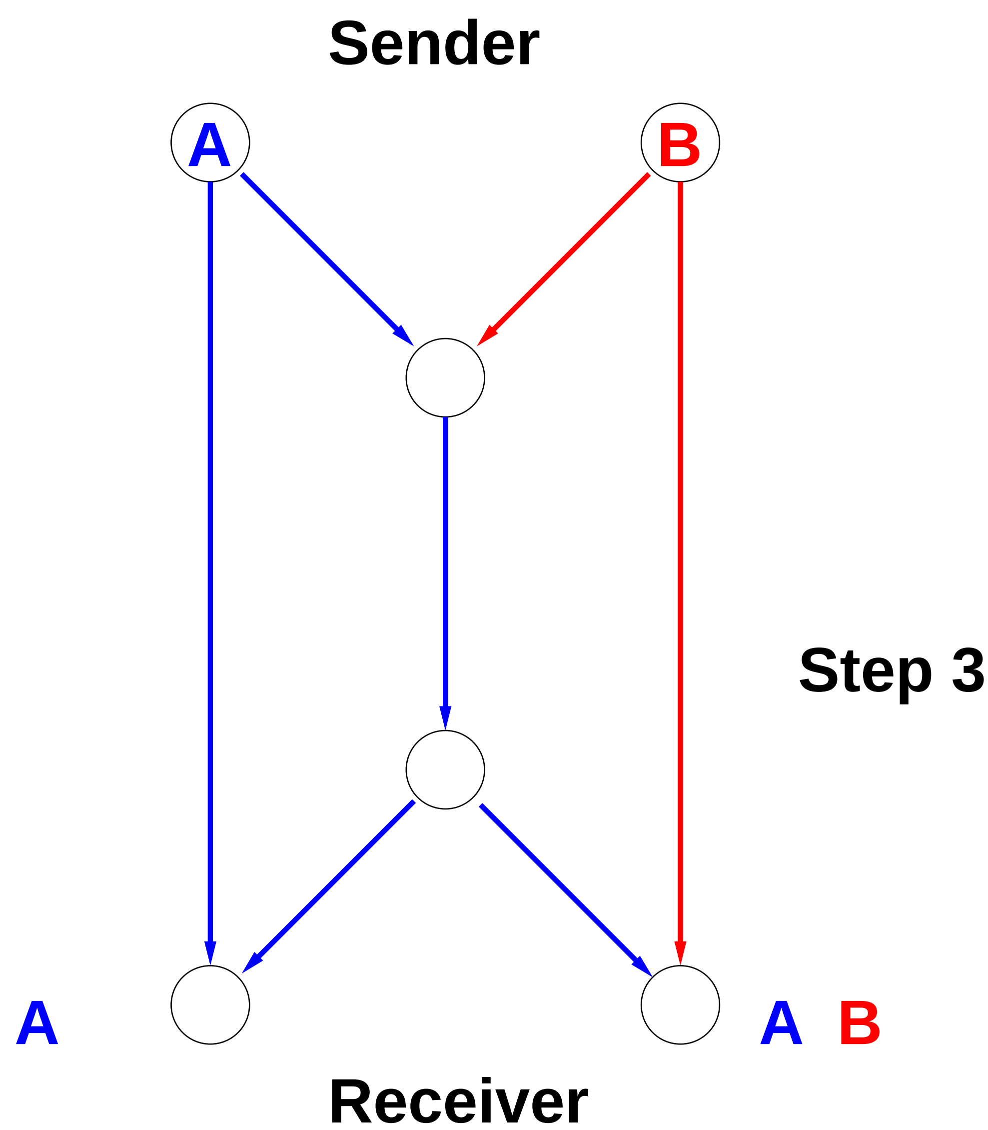


Network Codes



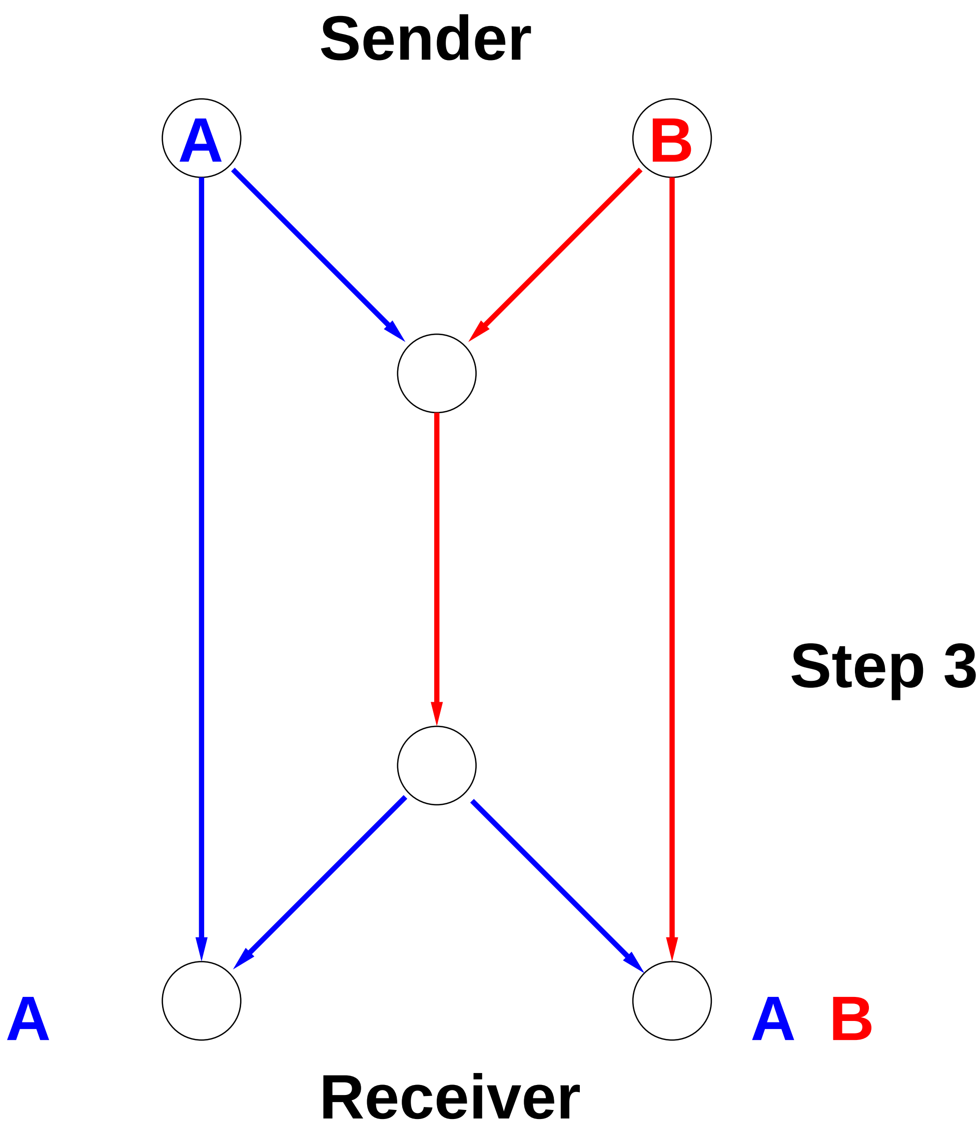
UNIVERSITÄT BAYREUTH

Network Codes



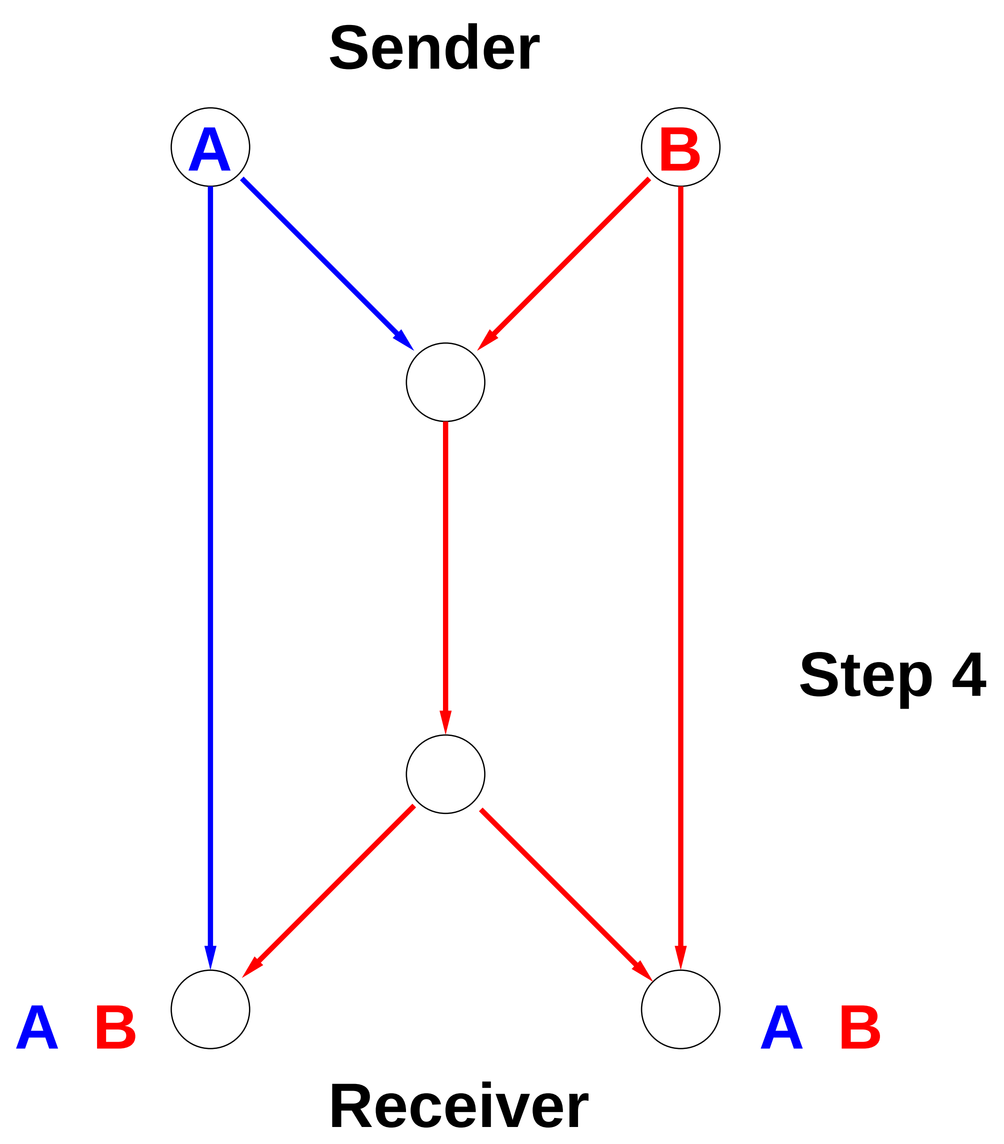
UNIVERSITÄT BAYREUTH

Network Codes



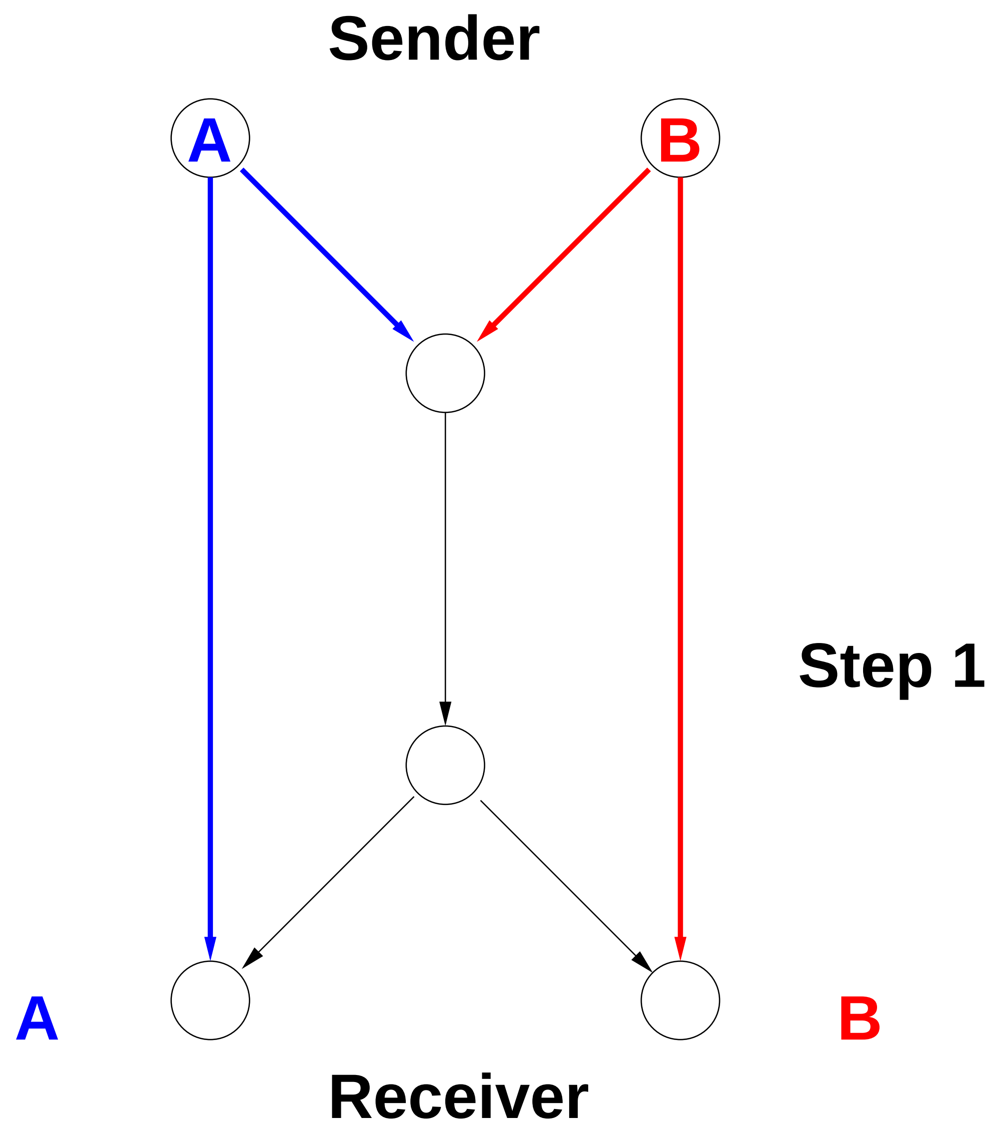
UNIVERSITÄT BAYREUTH

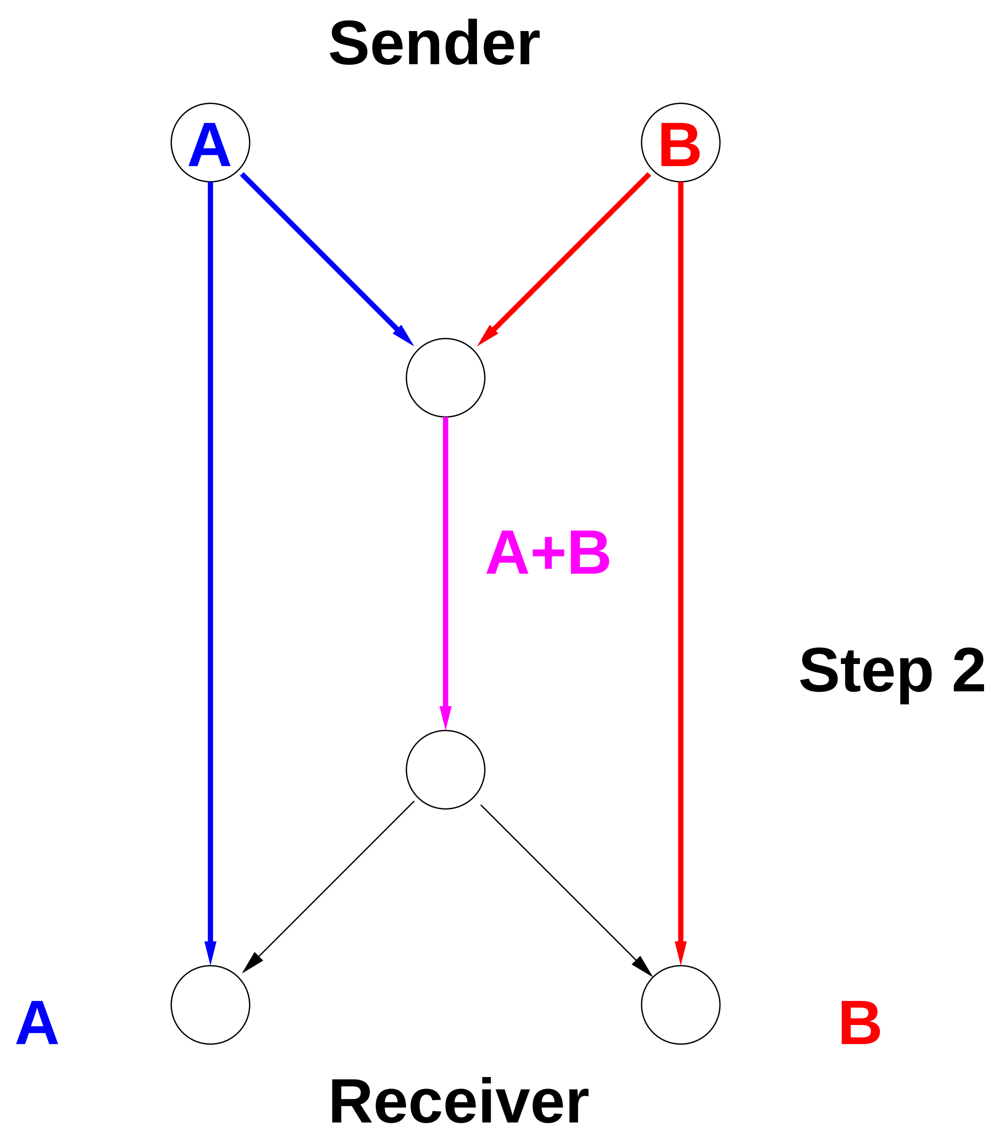
Network Codes

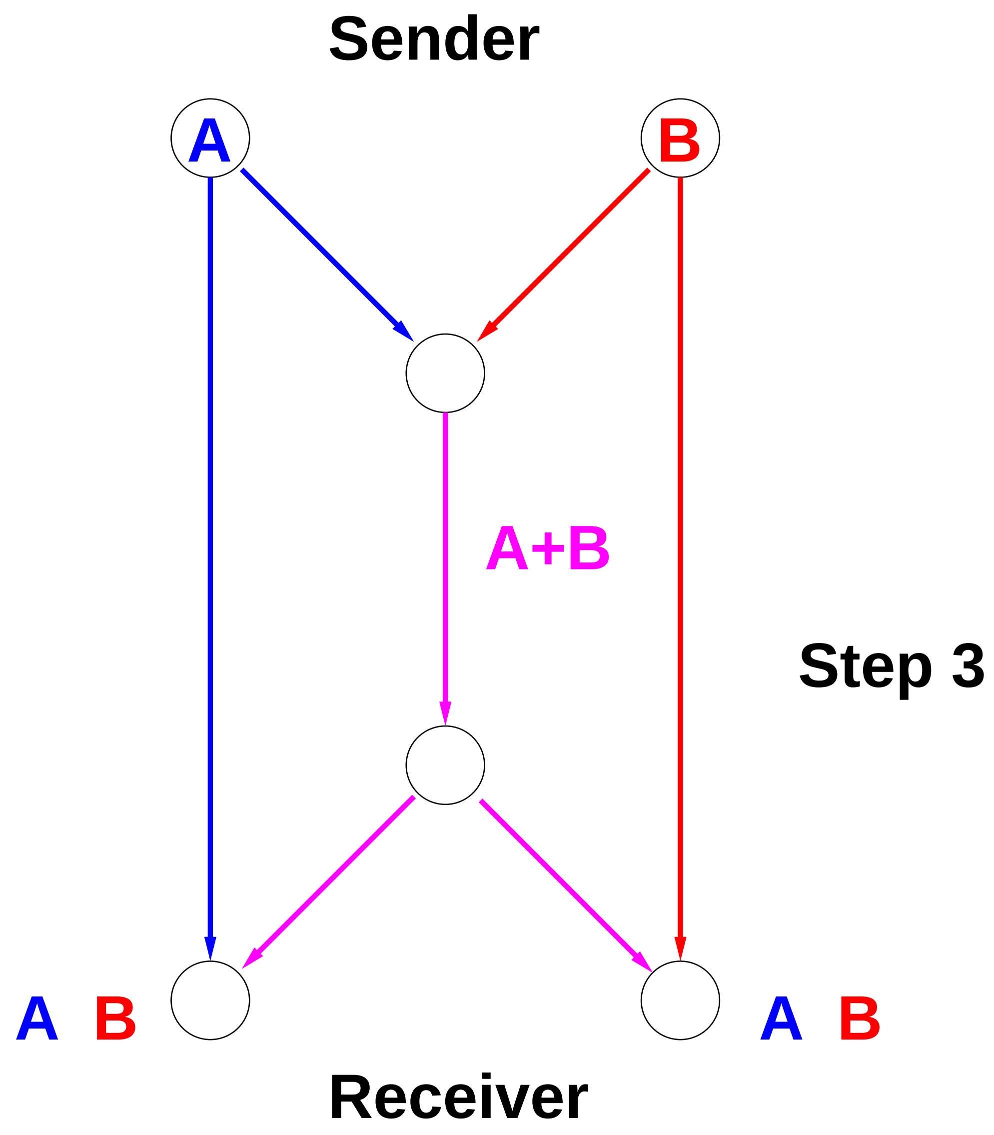


UNIVERSITÄT BAYREUTH

Network Codes




Sender
A
B
A+B
Step 2
A
B
Receiver



UNIVERSITÄT BAYREUTH

Network Codes

message:

- linear space

Network Codes

message:

- linear space

single node:

- receives vectors
- sends some linear combination of the incoming vectors

UNIVERSITÄT
BAYREUTH

Error-Correcting Network Codes

codeword:

- linear subspace of $GF(q)^v$

UNIVERSITÄT
BAYREUTH

Error-Correcting Network Codes

codeword:

- linear subspace of $GF(q)^v$

distance d:

- distance in the Hasse diagram of the linear lattice of all subspaces of $GF(q)^v$

UNIVERSITÄT BAYREUTH

Error-Correcting Network Codes

codeword:

- linear subspace of $GF(q)^v$

distance d:

- distance in the Hasse diagram of the linear lattice of all subspaces of $GF(q)^v$

U, W subspace of $GF(q)^v$:

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

UNIVERSITÄT
BAYREUTH

Error-Correcting Network Codes

fix minimum distance d:

$$\boxed{\text{Find a set of subspaces in } GF(q)^v \text{ such that the pairwise distance is at least } d}$$

Error-Correcting Network Codes

fix minimum distance d:

> Find a set of subspaces in $GF(q)^v$ such that the pairwise distance is at least d

fix also dimension k of the subspaces:

> Find a set of $k-$subspaces in $GF(q)^v$ such that the pairwise distance is at least $2d$

Error-Correcting Network Codes

fix minimum distance d:

$$\boxed{\text{Find a set of subspaces in } GF(q)^v \text{ such that the pairwise distance is at least } d}$$

fix also dimension k of the subspaces:

$$\boxed{\text{Find a set of } k\text{−subspaces in } GF(q)^v \text{ such that the pairwise distance is at least } 2d}$$

constant dimension codes $\approx q-$ analogue of constant weight codes

UNIVERSITÄT
BAYREUTH

Given a $t-(v,k,1)$ $q-$design we get a constant dimension code with minimum distance $2(k-(t-1))$ as the intersection of two codewords has dimension $\leq t-1$.

Codes and Designs

Given a $t-(v,k,1)$ $q-$design we get a constant dimension code with minimum distance $2(k-(t-1))$ as the intersection of two codewords has dimension $\leq t-1$.

Find a set of $k-$subspaces in $GF(q)^v$ such that each $t-$subspace is in exactly 1 $k-$subspace
= Steiner system = prefect code

Codes and Designs

Given a $t-(v,k,1)$ $q-$design we get a constant dimension code with minimum distance $2(k-(t-1))$ as the intersection of two codewords has dimension $\leq t-1$.

Find a set of $k-$subspaces in $GF(q)^v$ such that each $t-$subspace is in exactly 1 $k-$subspace = Steiner system = prefect code

Find a set of $k-$subspaces in $GF(q)^v$ such that each $t-$subspace is in at most 1 $k-$subspace = error-correcting network code

UNIVERSITÄT BAYREUTH

Current State

Define $A_q(v, k, d)$ as the maximal size (= number of codewords) of a constant dimension code with minimum distance d, dimension of codewords = k, and ambient space = $GF(q)^v$

Current State

Define $A_q(v,k,d)$ as the maximal size (= number of codewords) of a constant dimension code with minimum distance d, dimension of codewords = k, and ambient space = $GF(q)^v$

open problems:

- find lower and upper bounds for $A_q(v,k,d)$
- find constructions of ’good’ codes
- special case $A_2(7,3,4)$ = Fano plane

UNIVERSITÄT BAYREUTH

Construction

Problem

Find a set of $k-$subspaces in $GF(q)^v$ such that each $t-$subspace is in at most 1 $k-$subspace
= error-correcting network code

Problem

Find a set of $k-$subspaces in $GF(q)^v$ such that each $t-$subspace is in at most 1 $k-$subspace
= error-correcting network code

D:= incidence matrix between $k-$spaces and $t-$spaces in $GF(q)^v$

$$D_{U,V} := \begin{cases} 1 & t\text{-space } U \text{ is subspace of } k-\text{ space } W \\ 0 & \text{else} \end{cases}$$

Problem

Combinatorial optimization problem

Find a $0/1$-solution $x = (x_1, \ldots, x_s)$ such that

UNIVERSITÄT BAYREUTH

Problem

Combinatorial optimization problem

Find a $0/1$-solution $x = (x_1, \ldots, x_s)$ such that

- $x_1 + \ldots + x_s$ as large as possible

Problem

Combinatorial optimization problem

Find a $0/1$-solution $x = (x_1, \ldots, x_s)$ such that

- $x_1 + \ldots + x_s$ as large as possible
- $Dx^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

UNIVERSITÄT BAYREUTH

Problem

Combinatorial optimization problem

Find a $0/1$-solution $x = (x_1, \ldots, x_s)$ such that

- $x_1 + \ldots + x_s$ as large as possible
- $Dx^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

solution = network code with minimum distance $2(k - t + 1)$.

UNIVERSITÄT BAYREUTH

Automorphisms

Automorphism φ on $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$

G subgroup of $Aut(GF(q)^v)$

UNIVERSITÄT BAYREUTH

Automorphisms

Automorphism φ on $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$
G subgroup of $Aut(GF(q)^v)$

- shrink matrix D by: adding columns of elements in the same orbit of G on the $k-$spaces

$\Rightarrow$ rows of elements in the same orbit on the $t-$spaces are identical

Automorphisms

Automorphism φ on $GF(q)^v$: $U < W \iff U^\varphi < W^\varphi$
G subgroup of $Aut(GF(q)^v)$

- shrink matrix D by: adding columns of elements in the same orbit of G on the $k-$spaces

$\Rightarrow$ rows of elements in the same orbit on the $t-$spaces are identical

- D^G :=shrinked matrix

$\Rightarrow$number of columns = number of orbits on $k-$spaces
number of rows = number of orbits on $t-$spaces

Reduced Problem

$b_1, \ldots, b_m$ orbit sizes on $k-$spaces. Find a $0/1$-solution $x = (x_1, \ldots, x_m)$ such that

UNIVERSITÄT BAYREUTH

Reduced Problem

$b_1, \ldots, b_m$ orbit sizes on $k-$spaces. Find a $0/1$-solution $x = (x_1, \ldots, x_m)$ such that

- $b_1 x_1 + \ldots + b_m x_m$ as large as possible

UNIVERSITÄT
BAYREUTH

Reduced Problem

$b_1, \ldots, b_m$ orbit sizes on $k-$spaces. Find a $0/1$-solution $x = (x_1, \ldots, x_m)$ such that

- $b_1 x_1 + \ldots + b_m x_m$ as large as possible
- $D^G x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

UNIVERSITÄT
BAYREUTH

Reduced Problem

$b_1, \ldots, b_m$ orbit sizes on $k-$spaces. Find a $0/1$-solution $x = (x_1, \ldots, x_m)$ such that

- $b_1 x_1 + \ldots + b_m x_m$ as large as possible
- $D^G x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

solution = network code with prescribed automorphisms and minimum distance $2(k - t + 1)$.

UNIVERSITÄT BAYREUTH

Results (binary)

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

UNIVERSITÄT
BAYREUTH

Open Problems

- real world $v = 100$
- complete system with encoding and decoding

Last Page

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.

Thank you very much for your attention.

UNIVERSITÄT BAYREUTH