Construction of Codes for Network Coding

Axel Kohnert

Budapest MTNS July 2010

University of Bayreuth

axel.kohnert@uni-bayreuth.de

(joint work with A.S. Elsenhans, A. Wassermann)

UNIVERSITÄT
BAYREUTH

Agenda

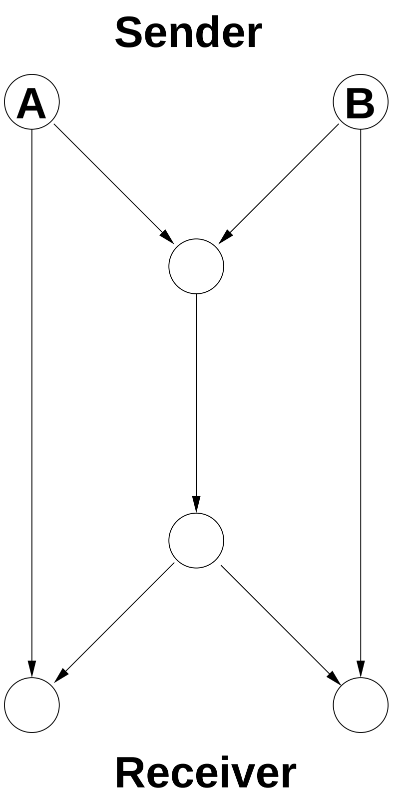
- Network Codes
- Finding Codes (construction)
- Using Codes (decoding)

I - Network Codes

UNIVERSITÄT
BAYREUTH

Network Codes

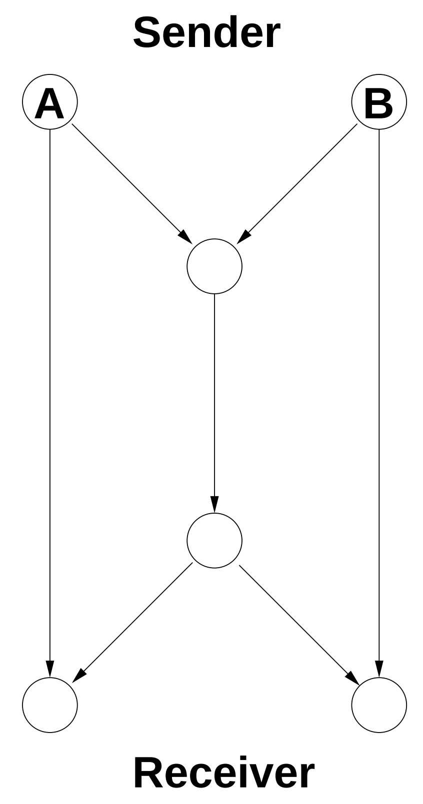
Modell (Kötter, Kschischang)



Network Codes

Modell (Kötter, Kschischang)
one codeword:

- vectorspace $V < \mathbb{F}_2^v$



UNIVERSITÄT BAYREUTH

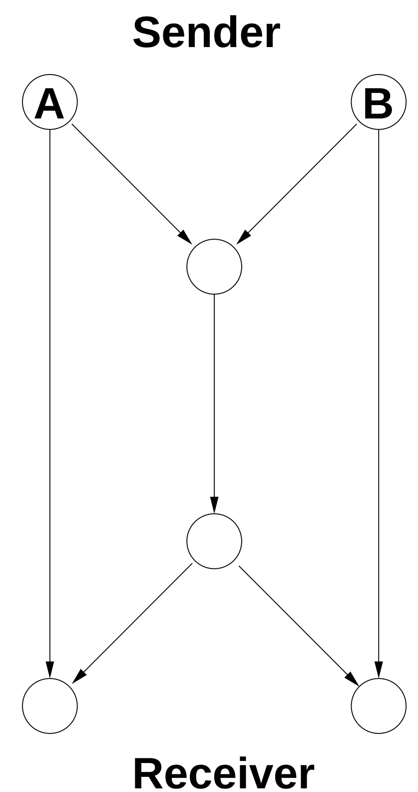
Network Codes

Modell (Kötter, Kschischang)
one codeword:

- vectorspace $V < \mathbb{F}_2^v$

one vertex in the network:

- receives several $v_i \in V$
- sends random combination of the v_i (= EXOR)



UNIVERSITÄT BAYREUTH

Error Correcting Network Codes

codeword:

- subspace of $\mathbb{F}_2^v$

Error Correcting Network Codes

codeword:

- subspace of $\mathbb{F}_2^v$

distance d:

- graph theoretic distance in the Hasse diagram of the subspace lattice of $\mathbb{F}_2^v$

UNIVERSITÄT BAYREUTH

Error Correcting Network Codes

codeword:

- subspace of $\mathbb{F}_2^v$

distance d:

- graph theoretic distance in the Hasse diagram of the subspace lattice of $\mathbb{F}_2^v$

$U, W < \mathbb{F}_2^v$:

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

UNIVERSITÄT BAYREUTH

Error Correcting Network Codes

for a fixed d:

$$\boxed{\text{find a set of subspaces of } \mathbb{F}_2^v \text{ with pairwise distances } \geq d}$$

UNIVERSITÄT BAYREUTH

Error Correcting Network Codes

for a fixed d:

$\boxed{\text{find a set of subspaces of } \mathbb{F}_2^v \text{ with pairwise distances} \geq d}$

fix also dimension k of the subspaces:

$\boxed{\text{find a set of } k-\text{dimensional subspaces of } \mathbb{F}_2^v \text{ with pairwise distances} \geq 2d}$

UNIVERSITÄT
BAYREUTH

Error Correcting Network Codes

for a fixed d:

$$\boxed{\text{find a set of subspaces of } \mathbb{F}_2^v \text{ with pairwise distances} \geq d}$$

fix also dimension k of the subspaces:

$$\boxed{\text{find a set of } k-\text{dimensional subspaces of } \mathbb{F}_2^v \text{ with pairwise distances} \geq 2d}$$

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

UNIVERSITÄT BAYREUTH

II - Construction

UNIVERSITÄT
BAYREUTH

Problem

original problem

$$\boxed{\text{find a set of } k-\text{dimensional subspaces of } \mathbb{F}_2^v \text{ with pairwise distances } \geq 2d}$$

UNIVERSITÄT BAYREUTH

Problem

original problem

$$\boxed{\text{find a set of } k-\text{dimensional subspaces of } \mathbb{F}_2^v \text{ with pairwise distances } \geq 2d}$$

modified version

$$\boxed{\text{find } k-\text{dim. subspaces } \{V_1, \dots, V_b\} \text{ in } \mathbb{F}_2^v \text{ such that the pairwise intersection is at most } 1-\text{dimensional}}$$

UNIVERSITÄT
BAYREUTH

Problem

original problem

$$\boxed{\text{find a set of } k\text{−dimensional subspaces of } \mathbb{F}_2^v \text{ with pairwise distances } \geq 2d}$$

modified version

$$\boxed{\text{find } k\text{−dim. subspaces } \{V_1, \ldots, V_b\} \text{ in } \mathbb{F}_2^v \text{ such that the pairwise intersection is at most } 1\text{−dimensional}}$$

$\Rightarrow$ code with minimum distance $\geq 2(k-1)$

Singer Cycle

- On $\mathbb{F}_2^v$ acts the Singer cycle S
- i.e. multiplication in $\mathbb{F}_{2^v}$ with non-zero elements

UNIVERSITÄT BAYREUTH

Singer Cycle

- On $\mathbb{F}_2^v$ acts the Singer cycle S
- i.e. multiplication in $\mathbb{F}_{2^v}$ with non-zero elements
- inducing action of S on the $k-$spaces

UNIVERSITÄT BAYREUTH

Singer Cycle

- On $\mathbb{F}_2^v$ acts the Singer cycle S
- i.e. multiplication in $\mathbb{F}_{2^v}$ with non-zero elements
- inducing action of S on the $k-$spaces

find a Singer orbit O on the $k-$dim. subspaces of $\mathbb{F}_2^v$ such that the pairwise intersection of the $V_i \in O$ is at most $1-$dimensional

UNIVERSITÄT BAYREUTH

Singer Cycle

- typical Singer orbit on $k-$spaces has $2^v - 1$ elements
- like in the case of the action on $\mathbb{F}_2^v$

UNIVERSITÄT BAYREUTH

Singer Cycle

- typical Singer orbit on $k-$spaces has $2^v - 1$ elements
- like in the case of the action on $\mathbb{F}_2^v$
- for v large enough there are 'good' orbits having above $1-$dim. intersection property

UNIVERSITÄT BAYREUTH

Singer Cycle

- typical Singer orbit on $k-$spaces has $2^v - 1$ elements
- like in the case of the action on $\mathbb{F}_2^v$
- for v large enough there are 'good' orbits having above $1-$dim. intersection property
- good orbit $\Rightarrow$ code with $2^v - 1$ codewords and minimum distance $\geq 2(k-1)$

UNIVERSITÄT BAYREUTH

Description of Singer orbit

- Given a $k-$dimensional space $V < \mathbb{F}_2^v$
- take all the nonzero vectors $\{u_1, \ldots, u_{2^k-1}\}$
- action of S is multiplication in $\mathbb{F}_{2^v}$

UNIVERSITÄT BAYREUTH

Description of Singer orbit

- Given a $k-$dimensional space $V < \mathbb{F}_2^v$
- take all the nonzero vectors $\{u_1, \ldots, u_{2^k-1}\}$
- action of S is multiplication in $\mathbb{F}_{2^v}$
- pairwise quotients u_i/u_j are invariant under the action of S

UNIVERSITÄT BAYREUTH

Description of Singer orbit

- Given a $k-$dimensional space $V < \mathbb{F}_2^v$
- take all the nonzero vectors $\{u_1, \ldots, u_{2^k-1}\}$
- action of S is multiplication in $\mathbb{F}_{2^v}$
- pairwise quotients u_i/u_j are invariant under the action of S
- describe a complete orbit by the pairwise quotients

UNIVERSITÄT BAYREUTH

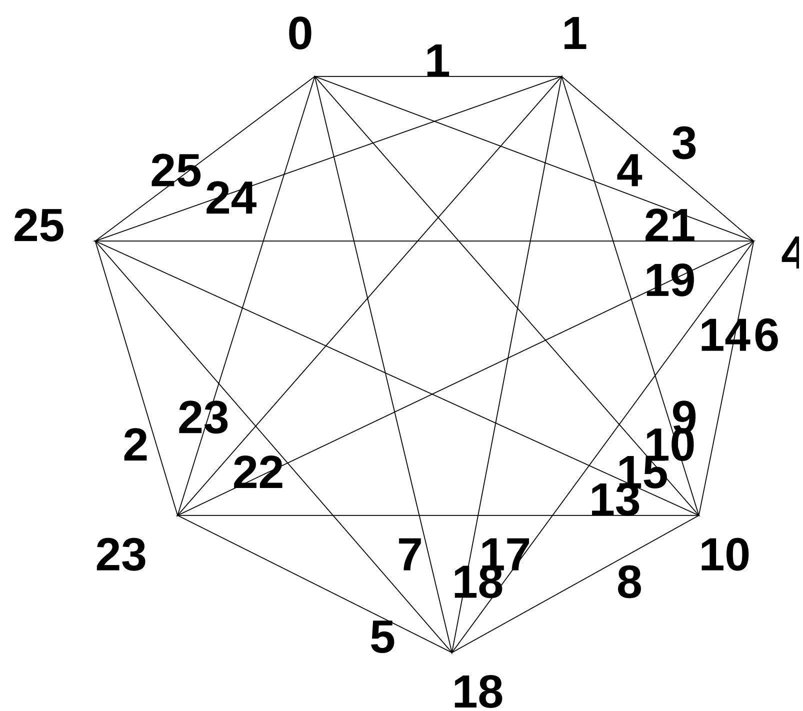
Example

$k = 3$, $3-$space = $\{0, 1, 4, 10, 18, 23, 25\}$
= exponents of a generator of $\mathbb{F}_{2^v}^*$ (only for the example)

UNIVERSITÄT BAYREUTH

Example

$k = 3$, $3-$space = $\{0, 1, 4, 10, 18, 23, 25\}$
= exponents of a generator of $\mathbb{F}_{2^v}^*$ (only for the example)
orbit graph G_O



UNIVERSITÄT
BAYREUTH

Lemma: O is a good orbit $\iff$ all the pairwise quotients are different

good orbits

Lemma: O is a good orbit $\iff$ all the pairwise quotients are different

$$\boxed{\begin{array}{c}\text{find a } k\text{−dim. subspace of } \mathbb{F}_2^v \text{ such that the} \\ \text{pairwise quotients are all different}\end{array}}$$

$\Rightarrow$code with $2^v - 1$ codewords and minimum distance $\geq 2(k-1)$

UNIVERSITÄT BAYREUTH

good orbits

Lemma: O is a good orbit $\iff$ all the pairwise quotients are different

$$\boxed{\text{find a } k\text{-dim. subspace of } \mathbb{F}_2^v \text{ such that the pairwise quotients are all different}}$$

$\Rightarrow$code with $2^v - 1$ codewords and minimum distance $\geq 2(k-1)$

$$\boxed{\text{find a set } \{V_1, \ldots, V_b\} \text{ of } k\text{-dim. subspace of } \mathbb{F}_2^v \text{ such that all the pairwise quotients are all different}}$$

$\Rightarrow$ code with $b\,(2^v - 1)$ codewords and minimum distance $\geq 2(k-1)$

UNIVERSITÄT BAYREUTH

results

v	k	b	number of codewords	$d_S = 2d$
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

UNIVERSITÄT BAYREUTH

III - Decoding

Decoding

- special case $b = 1$
- number of codewords $2^v - 1$
- message is a $3-$space $V < \mathbb{F}_2^v$

UNIVERSITÄT
BAYREUTH

Decoding

- special case $b = 1$
- number of codewords $2^v - 1$
- message is a $3-$space $V < \mathbb{F}_2^v$

as $d = 4$: two possible cases in decoding:

- erasure (we received a $2-$space $U < V$)
- error (i.e. we received a $4-$space $U > V$)

UNIVERSITÄT BAYREUTH

Erasure

- received a 2$-$space $U = \{x_1, x_2, x_3, 0\} < V$

UNIVERSITÄT
BAYREUTH

Erasure

- received a $2-$space $U = \{x_1, x_2, x_3, 0\} < V$
- compute x_1/x_2.

UNIVERSITÄT BAYREUTH

Erasure

- received a $2-$space $U = \{x_1, x_2, x_3, 0\} < V$
- compute x_1 / x_2.
- identify an edge $\{x_1, x_2\}$ in orbit graph G_O

UNIVERSITÄT BAYREUTH

Erasure

- received a $2-$space $U = \{x_1, x_2, x_3, 0\} < V$
- compute x_1/x_2.
- identify an edge $\{x_1, x_2\}$ in orbit graph G_O
- multiply x_1 with an edgelabel u from G_O giving a third base element ux_1 of $V = \langle x_1, x_2, ux_1\rangle$

UNIVERSITÄT
BAYREUTH

Erasure

- received a $2-$space $U = \{x_1, x_2, x_3, 0\} < V$
- compute x_1/x_2.
- identify an edge $\{x_1, x_2\}$ in orbit graph G_O
- multiply x_1 with an edgelabel u from G_O giving a third base element ux_1 of $V = \langle x_1, x_2, ux_1\rangle$
- costs: one multiplication and one division in $\mathbb{F}_{2^v}$

UNIVERSITÄT
BAYREUTH

Error

- received a $4-$space $U > V$

UNIVERSITÄT
BAYREUTH

Error

- received a $4-$space $U > V$
- choose a random $3-$subspace $W < U$, we know: $W \cap V$ is at least $2-$dimensional

UNIVERSITÄT BAYREUTH

Error

- received a $4-$space $U > V$
- choose a random $3-$subspace $W < U$, we know: $W \cap V$ is at least $2-$dimensional
- loop over the $7 \quad 2-$dim subspaces of W

Error

- received a $4-$space $U > V$
- choose a random $3-$subspace $W < U$, we know: $W \cap V$ is at least $2-$dimensional
- loop over the $7 \quad 2-$dim subspaces of W
- one of it is a $2-$dim subspace of V and we can apply the erasure algorithm, including a check whether the third constructed vector is in V

UNIVERSITÄT BAYREUTH

Error

- received a $4-$space $U > V$
- choose a random $3-$subspace $W < U$, we know: $W \cap V$ is at least $2-$dimensional
- loop over the $7 \quad 2-$dim subspaces of W
- one of it is a $2-$dim subspace of V and we can apply the erasure algorithm, including a check whether the third constructed vector is in V
- worst case costs: 7 divisions and 7 multiplications

Generalisations

- it works for $b > 1$
- it works for $k > 3$

UNIVERSITÄT
BAYREUTH

Bibliography

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

A.S. Elsenhans, A. Kohnert: *Constructing Network Codes using Möbius Transformations*, in preperation

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

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.

UNIVERSITÄT BAYREUTH

Bibliography

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

A.S. Elsenhans, A. Kohnert: *Constructing Network Codes using Möbius Transformations*, in preperation

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

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

UNIVERSITÄT BAYREUTH