q-analogs of combinatorial designs and network codes

Axel Kohnert

Zürich October 20, 2010

University of Bayreuth

axel.kohnert@uni-bayreuth.de

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

UNIVERSITÄT BAYREUTH

- Combinatorial Designs
- Network Codes
- Large Network Codes

I - Combinatorial Designs

Combinatorial Designs

- a set of v points

Combinatorial Designs

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

UNIVERSITÄT BAYREUTH

Combinatorial Designs

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

UNIVERSITÄT
BAYREUTH

Combinatorial 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

Combinatorial 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

Combinatorial 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

Combinatorial Designs

- a set of v points

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

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

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

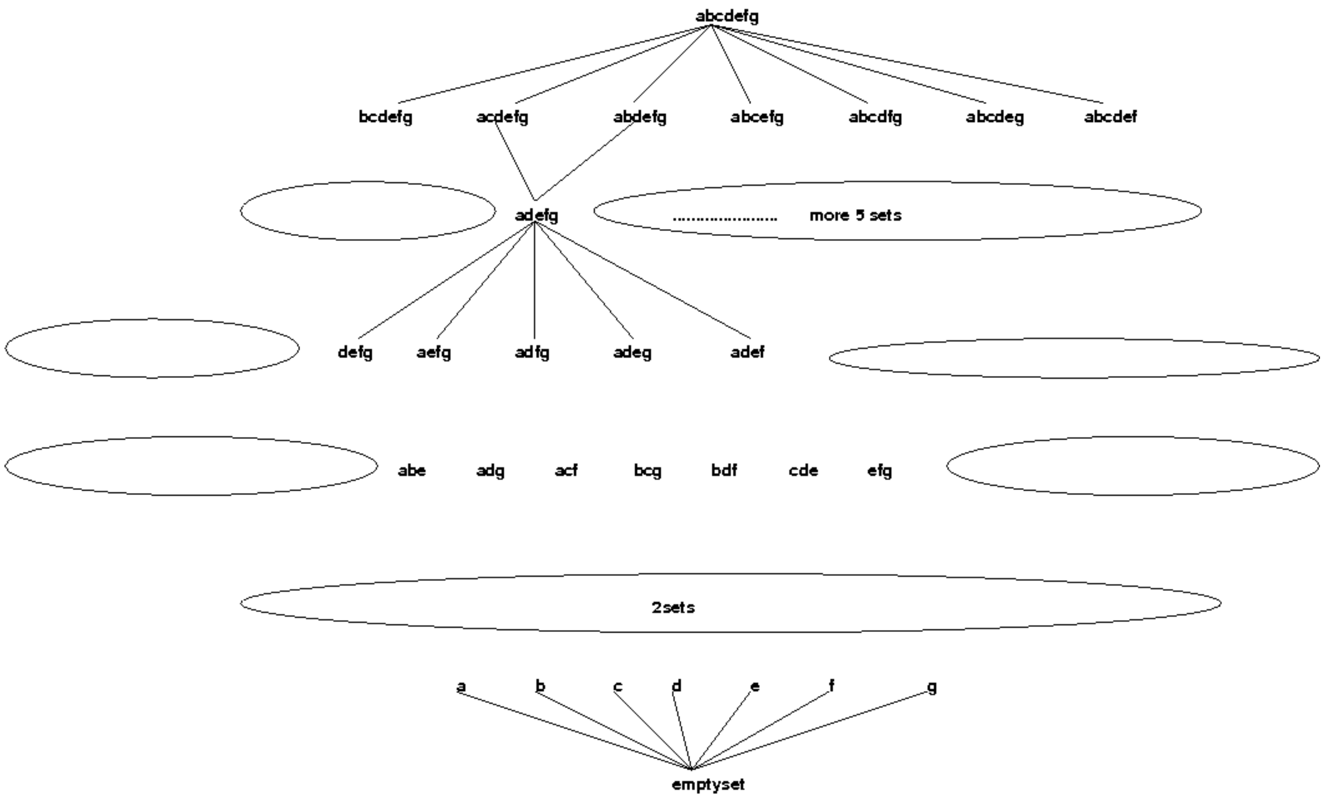
- $t - (v, k, \lambda)$ Design
  each block is a $k-$set
  each $t-$set of points is in exactly λ blocks

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

UNIVERSITÄT BAYREUTH

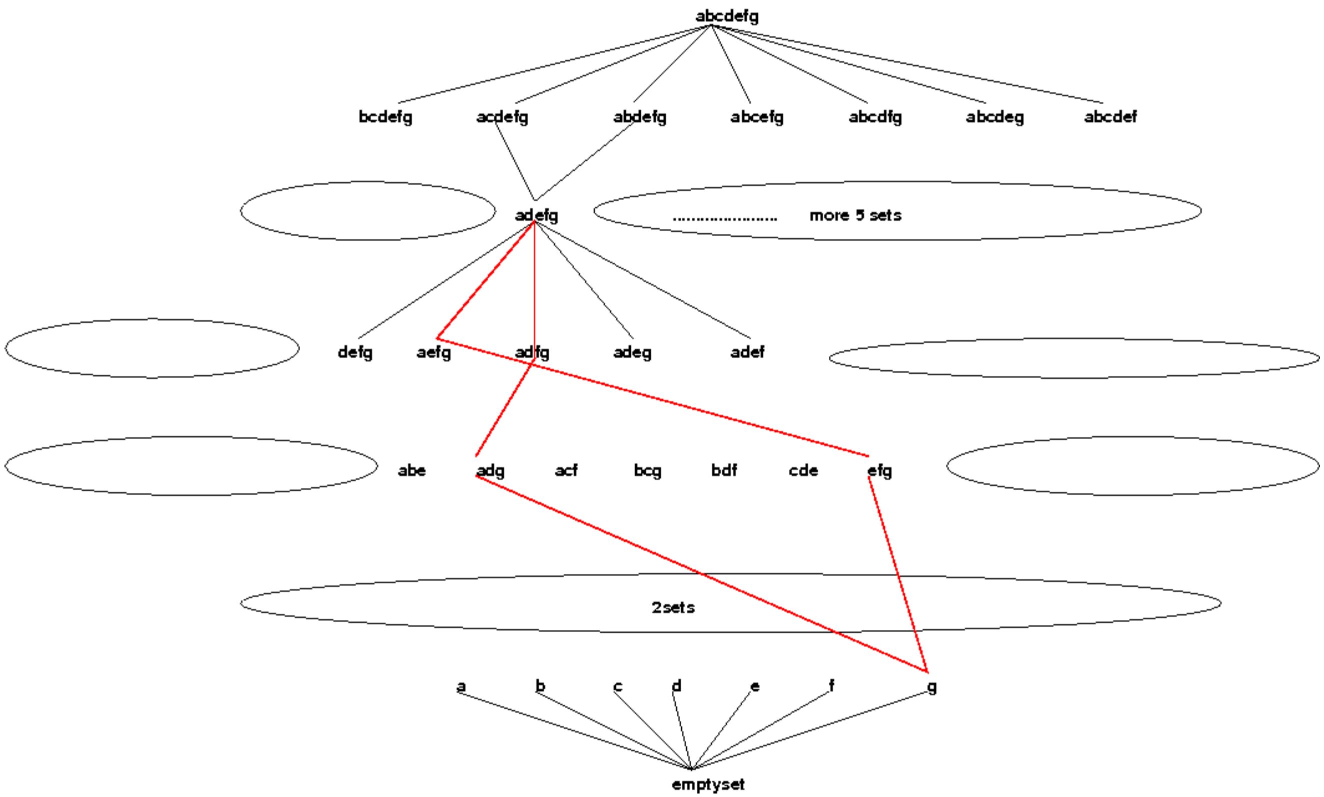
Combinatorial Designs

This is a selection problem in the lattice of all subsets of $\{a, b, c, d, e, f, g\}$



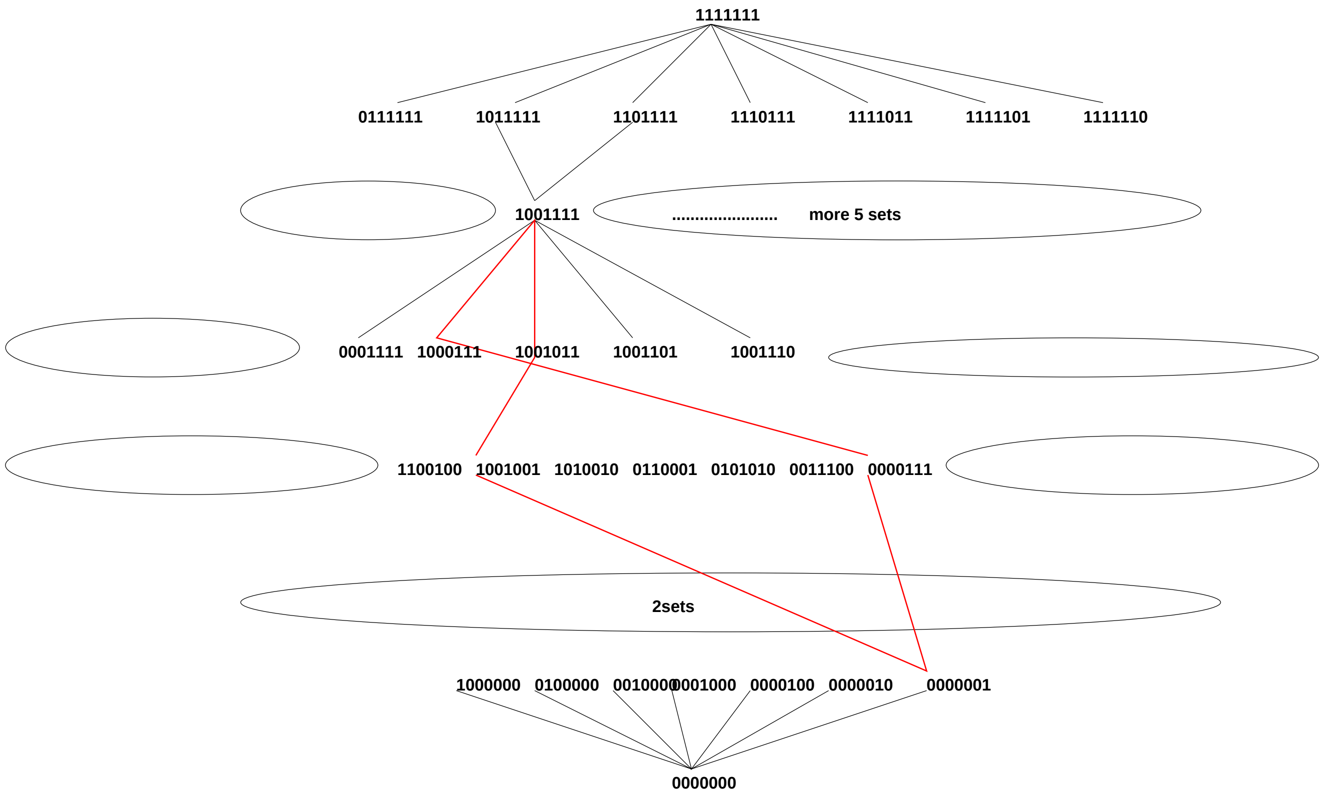
Combinatorial Designs

This is a selection problem in the lattice of all subsets of $\{a,b,c,d,e,f,g\}$



UNIVERSITÄT BAYREUTH

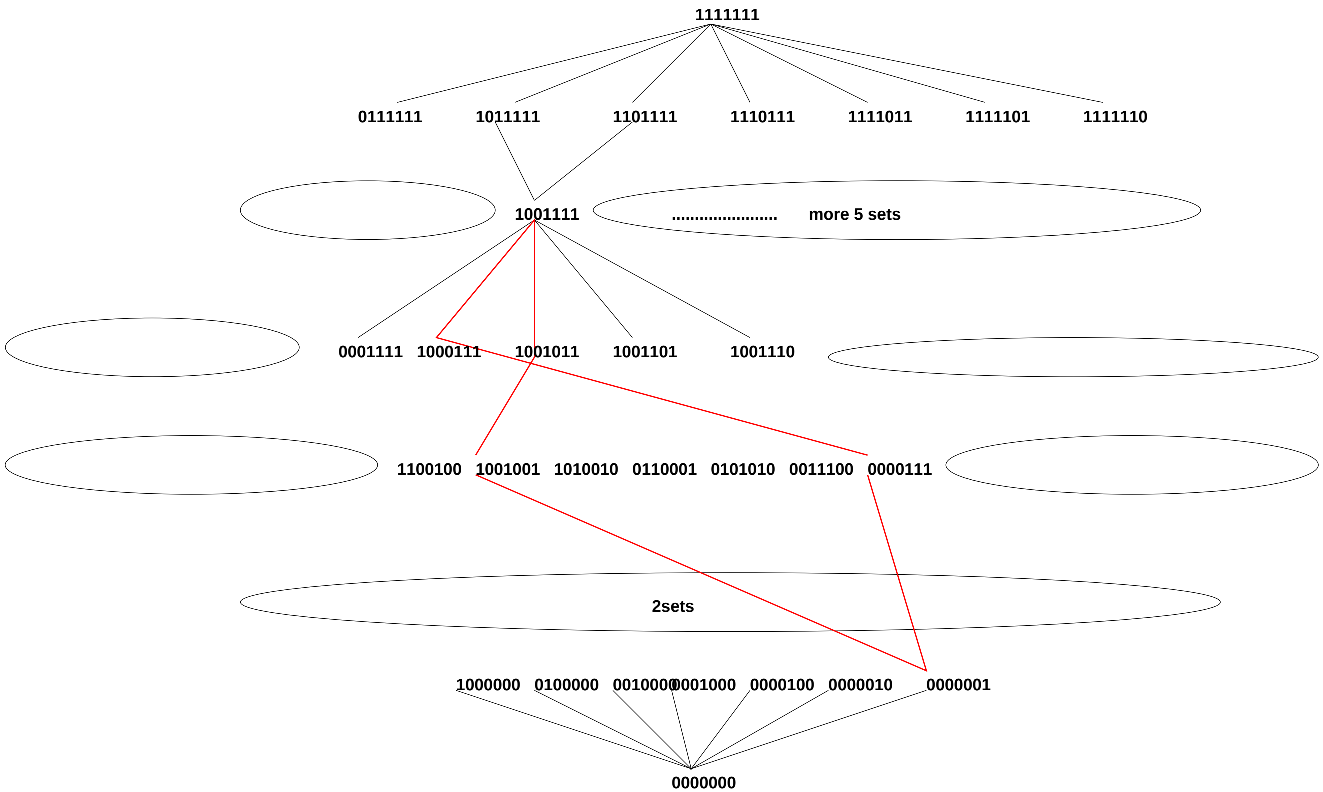
Combinatorial Designs



This is a selection problem in the lattice of all subsets of $\{a, b, c, d, e, f, g\}$=1111111

UNIVERSITÄT BAYREUTH

Combinatorial Designs

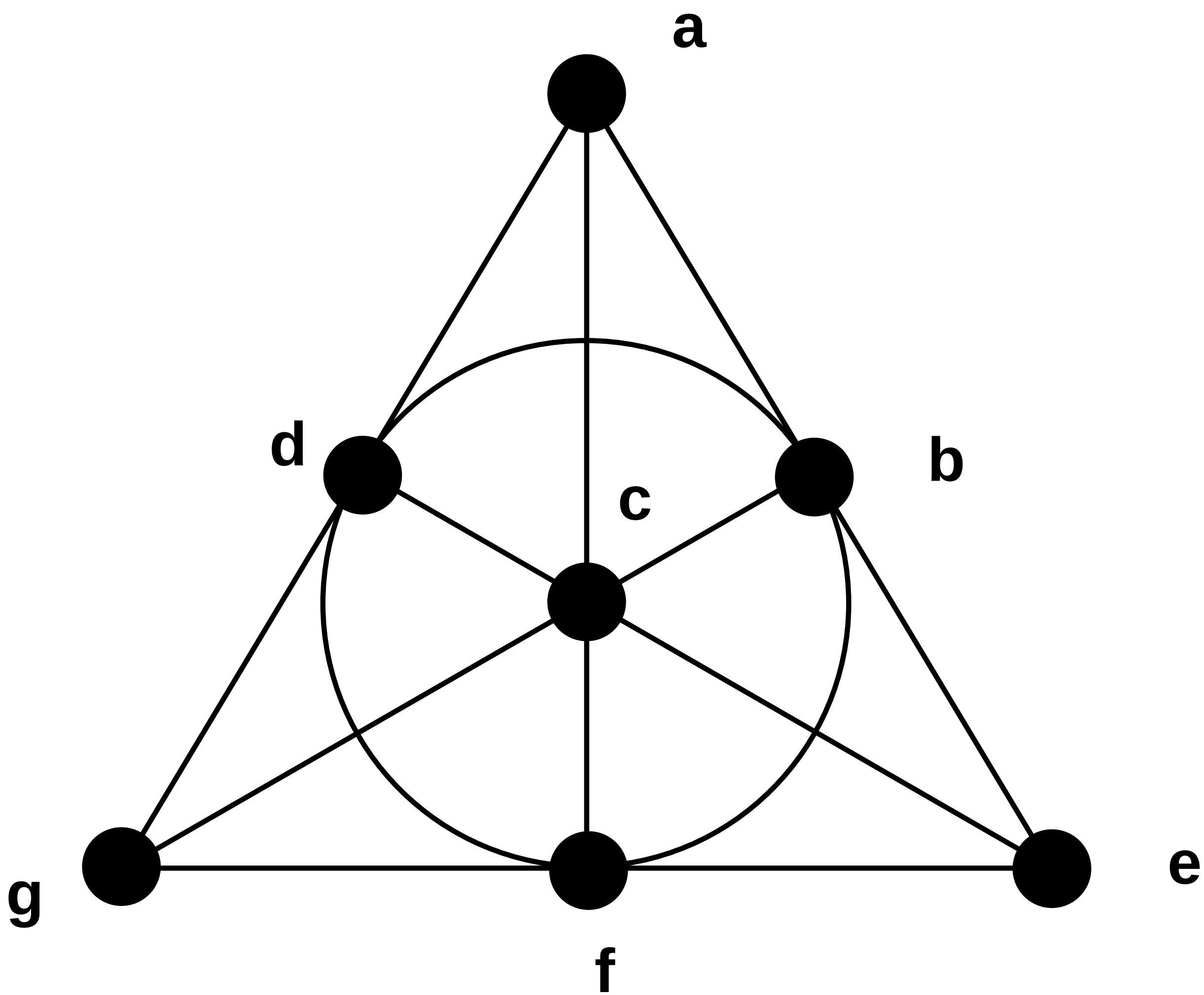


This is a selection problem in the ~~lattice of all subsets of $\{a,b,c,d,e,f,g\}$=1111111~~=Hamming Graph

UNIVERSITÄT BAYREUTH

Combinatorial Designs

Fano plane



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 $\mathbb{F}_q^v$
- 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 $\mathbb{F}_q^v$
- ~~a set of $k-$blocks~~

  a set of $k-$spaces in $\mathbb{F}_q^v$
- $t-(v,k,\lambda)$ 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 $\mathbb{F}_q^v$

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

  a set of $k-$spaces in $\mathbb{F}_q^v$

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

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

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

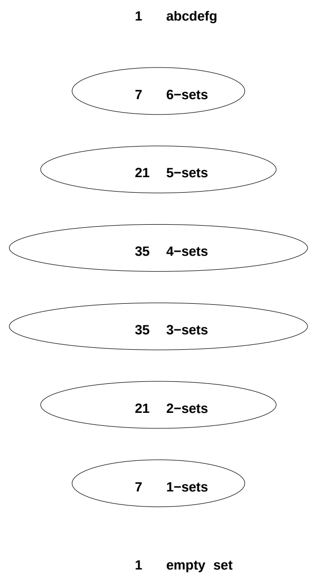
  each $t-$space of $\mathbb{F}_q^v$ is in exactly

  λ of the chosen $k-$spaces

UNIVERSITÄT BAYREUTH

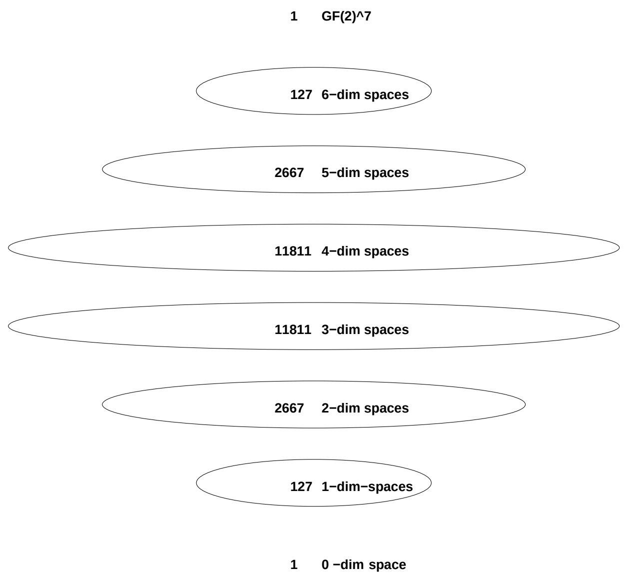
Combinatorial Designs

- A selection problem in the 'Linear Lattice' of all subspaces of $\mathbb{F}_q^v$.



UNIVERSITÄT BAYREUTH

- A selection problem in the 'Linear Lattice' of all subspaces of $\mathbb{F}_q^v$.



size given by the q-binomial coefficients $\begin{bmatrix} v \\ k \end{bmatrix}_q$:= number of the $k-$subspaces of $\mathbb{F}_q^v$.

UNIVERSITÄT BAYREUTH

Current State

known:

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

open problems:

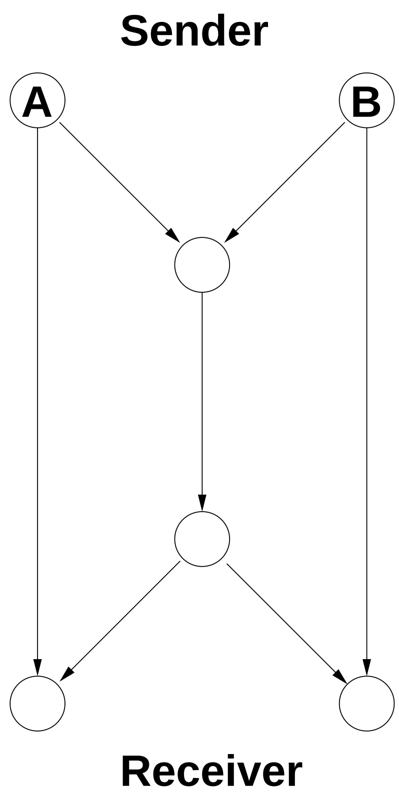
- $q-$analog of the Fano plane?
- Steiner systems ? ($\lambda = 1$)
- $t > 3$? (up to $t = 9$ in classical case)

UNIVERSITÄT BAYREUTH

II - Network Codes

Network Codes

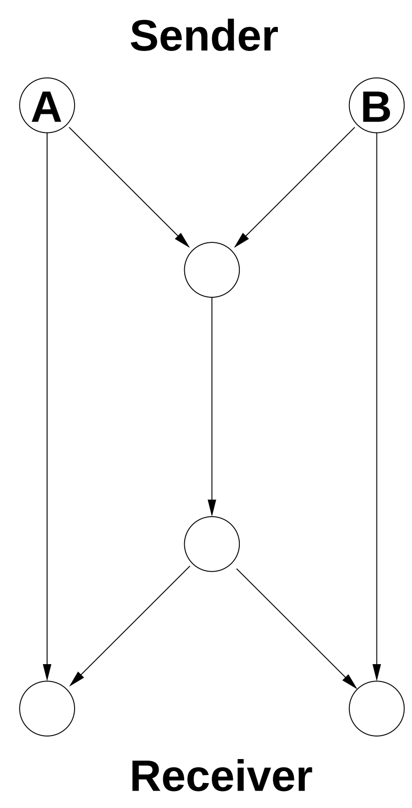
Model (Kötter, Kschischang)



Network Codes

Model (Kötter, Kschischang)
one codeword:

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



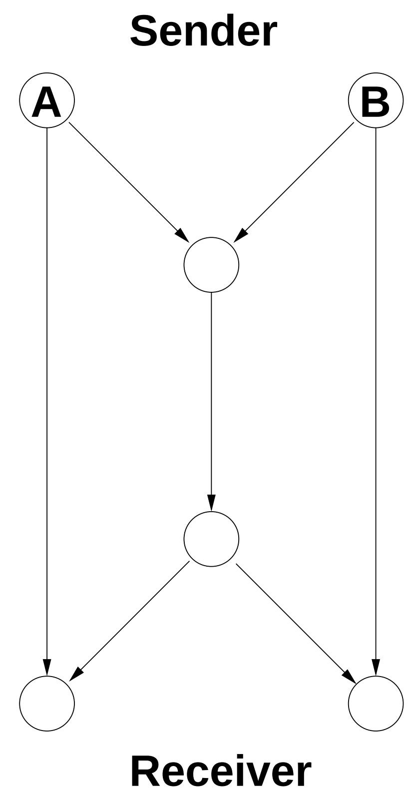
Network Codes

Model (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)



Error Correcting Network Codes

codeword:

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

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:

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

fix also dimension k of the subspaces:

find a set of $k-$dimensional subspaces of $\mathbb{F}_2^v$ 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

Construction

original problem

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

Construction

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

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

Construction

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

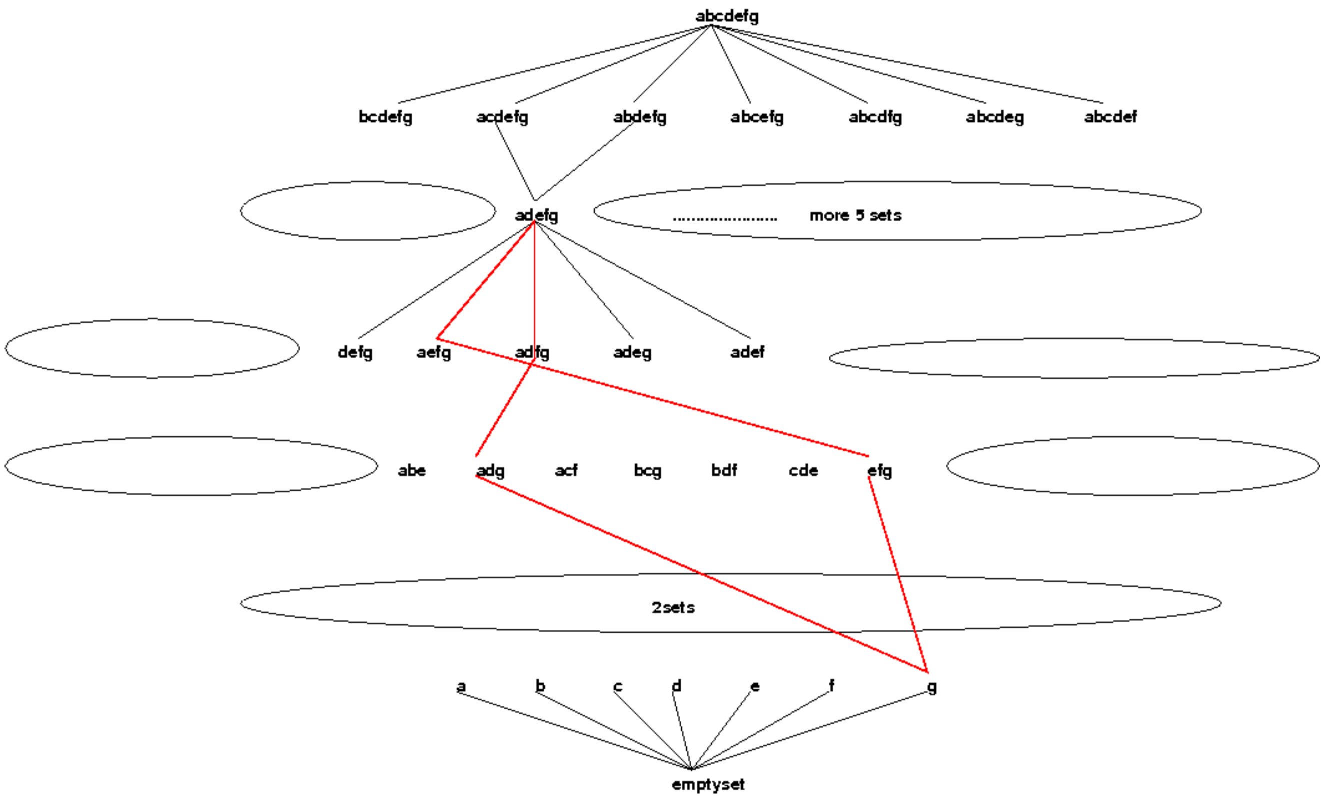
$$\boxed{\text{find } k-\text{dim. subspaces } \{V_1, \ldots, V_b\} \text{ in } \mathbb{F}_2^v \text{ such that the pairwise intersection is at most } 1-\text{dimensional}}$$

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

UNIVERSITÄT BAYREUTH

Combinatorial Designs

This is a selection problem in the lattice of all subsets of $\{a, b, c, d, e, f, g\}$



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

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 $S = (\mathbb{F}_{2^v})^*$ 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 $S = (\mathbb{F}_{2^v})^*$ 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 $\{u_1, \ldots, u_{2^k-1}, 0\} < \mathbb{F}_2^v$

UNIVERSITÄT BAYREUTH

Description of Singer orbit

- Given a $k-$dimensional space $\{u_1, \ldots, u_{2^k-1}, 0\} < \mathbb{F}_2^v$
- take $\{u_1, \ldots, u_{2^k-1}\}$ as elements in the field $\mathbb{F}_{2^v}$
- action of S is multiplication in $\mathbb{F}_{2^v}$

UNIVERSITÄT BAYREUTH

Description of Singer orbit

- Given a $k-$dimensional space $\{u_1, \ldots, u_{2^k-1}, 0\} < \mathbb{F}_2^v$
- take $\{u_1, \ldots, u_{2^k-1}\}$ as elements in the field $\mathbb{F}_{2^v}$
- 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 $\{u_1, \ldots, u_{2^k-1}, 0\} < \mathbb{F}_2^v$
- take $\{u_1, \ldots, u_{2^k-1}\}$ as elements in the field $\mathbb{F}_{2^v}$
- 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 $2\binom{k}{2}$quotients

UNIVERSITÄT BAYREUTH

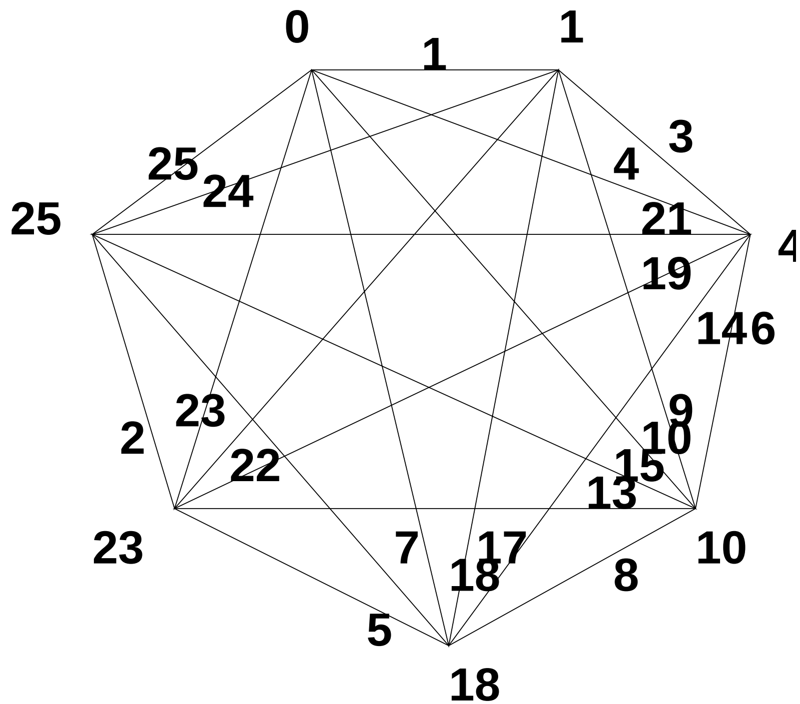
Example

$k = 3$, $3-$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



good orbits

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

UNIVERSITÄT BAYREUTH

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 $\geq 2(k-1)$

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 $\geq 2(k-1)$

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

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

UNIVERSITÄT BAYREUTH

results

v	k	b	number of codewords	$2d$
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

Decoding

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

Decoding

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

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

- one erasure (we received a $2-$space $U < V$)
- one error (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
- find the edge $\overrightarrow{x_1 x_2}$ with label x_1/x_2 in the orbit graph G_O

Erasure

- received a $2-$space $U = \{x_1, x_2, x_3, 0\} < V$
- compute x_1/x_2
- find the edge $\overrightarrow{x_1 x_2}$ with label x_1/x_2 in the 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
- find the edge $\overrightarrow{x_1 x_2}$ with label x_1/x_2 in the 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 (ux_1) and one division (x_1/x_2) in $\mathbb{F}_{2^v}$

Error

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

UNIVERSITÄT BAYREUTH

Error

- we received a $4-$space $U > V$
- choose a random $3-$subspace $W < U$,

UNIVERSITÄT BAYREUTH

Error

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

Error

- we 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

UNIVERSITÄT BAYREUTH

Error

- we 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
- at least 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 U

UNIVERSITÄT BAYREUTH

Error

- we 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
- at least 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 U
- worst case costs: 7 divisions and 7 multiplications

Generalisations

- It works for $b > 1$, you have to store the representing quotient-set for each orbit

Generalisations

- It works for $b > 1$, you have to store the representing quotient-set for each orbit
- It works for $k > 3$, the number of $2-$subspaces is increasing

UNIVERSITÄT BAYREUTH

Generalisations

- It works for $b > 1$, you have to store the representing quotient-set for each orbit
- It works for $k > 3$, the number of $2-$subspaces is increasing
- It works for all finite fields

UNIVERSITÄT
BAYREUTH

III - Large Network Codes

UNIVERSITÄT BAYREUTH

good orbits

- Restrict to codes from good orbits = intersection of two $k-$dim. codewords in the Singer orbit is at most one-dimensional.

UNIVERSITÄT BAYREUTH

good orbits

- Restrict to codes from good orbits = intersection of two $k-$dim. codewords in the Singer orbit is at most one-dimensional.
- Describe a 'bad' basis (representing a non good orbit) as a $\mathbb{F}_{2^v}$ -solution $b_1, \ldots, b_k$ of at least one of the equations for identical quotients:

$$\frac{l_a}{l_b} = \frac{l_c}{l_d}$$

with l_i one of the $\left(2^k - 1\right)$ nonzero $\mathbb{F}_2-$linear combination of the b_j.

UNIVERSITÄT BAYREUTH

good orbits

- at most $(2^k - 1)^4$ equations

UNIVERSITÄT BAYREUTH

good orbits

- at most $(2^k - 1)^4$ equations
- one equation has at most $2\ (2^v - 1)^{k-1}$ solutions

good orbits

- at most $(2^k - 1)^4$ equations
- one equation has at most $2\ (2^v - 1)^{k-1}$ solutions
- number of bad bases ($<(2^k - 1)^4 \cdot 2 \cdot (2^v - 1)^{k-1}$) is slower increasing (with increasing v) than the number of all bases (about $(2^v - 1)^k$)

UNIVERSITÄT BAYREUTH

good orbits

- number of equations can be reduced from $(2^k - 1)^4$

UNIVERSITÄT
BAYREUTH

good orbits

- number of equations can be reduced from $(2^k - 1)^4$
- to $\begin{bmatrix} k \\ 2 \end{bmatrix}_2 + 28 \begin{bmatrix} k \\ 3 \end{bmatrix}_2 + 280 \begin{bmatrix} k \\ 4 \end{bmatrix}_2$

UNIVERSITÄT BAYREUTH

good orbits

- number of equations can be reduced from $(2^k-1)^4$
- to $\begin{bmatrix} k \\ 2 \end{bmatrix}_2 + 28 \begin{bmatrix} k \\ 3 \end{bmatrix}_2 + 280 \begin{bmatrix} k \\ 4 \end{bmatrix}_2$

Lemma: for $v > 4k-6$ there are good orbits.

UNIVERSITÄT BAYREUTH

combinable orbits

- given one good orbit again only a ’small’ number of orbits are excluded

UNIVERSITÄT BAYREUTH

combinable orbits

- given one good orbit again only a ’small’ number of orbits are excluded
- same argument: a small number of equations with a small number of solutions

UNIVERSITÄT BAYREUTH

combinable orbits

- given one good orbit again only a ’small’ number of orbits are excluded
- same argument: a small number of equations with a small number of solutions
- a naive greedy algorithm then already gives a huge number of combinable orbits

UNIVERSITÄT BAYREUTH

combinable orbits

- given one good orbit again only a ’small’ number of orbits are excluded
- same argument: a small number of equations with a small number of solutions
- a naive greedy algorithm then already gives a huge number of combinable orbits
- e.g. $k = 3, v = 64$ gives 10^{16} orbits of $2^{64} - 1$ codewords

UNIVERSITÄT BAYREUTH

combinable orbits

- given one good orbit again only a 'small' number of orbits are excluded
- same argument: a small number of equations with a small number of solutions
- a naive greedy algorithm then already gives a huge number of combinable orbits
- e.g. $k = 3, v = 64$ gives 10^{16} orbits of $2^{64} - 1$ codewords
- e.g. $k = 4$, $v = 128$ gives 10^{34} orbits of $2^{128} - 1$ codewords

coding/decoding

- using the idea described for a single orbit we now have to store a representative for each of the 10^{large} orbits

UNIVERSITÄT BAYREUTH

coding/decoding

- using the idea described for a single orbit we now have to store a representative for each of the 10^{large} orbits
- a much better idea is needed to avoid storing this huge number of quotient sets

new construction

- new idea: use a systematic way to find (and label) combinable orbits (not a naive greedy algorithm)

UNIVERSITÄT BAYREUTH

new construction

- new idea: use a systematic way to find (and label) combinable orbits (not a naive greedy algorithm)
- to construct a code with $k-$dimensional codewords in $\mathbb{F}_{2^{2v}}$ we start with k affine lines in $\mathbb{F}_{2^{2v}}$

UNIVERSITÄT BAYREUTH

new construction

- new idea: use a systematic way to find (and label) combinable orbits (not a naive greedy algorithm)
- to construct a code with $k-$dimensional codewords in $\mathbb{F}_{2^{2v}}$ we start with k affine lines in $\mathbb{F}_{2^{2v}}$
- for each line we have a map $b_i : \mathbb{F}_{2^v} \longrightarrow \mathbb{F}_{2^{2v}} : t \mapsto a_i + s_i t$ for some $a_i, s_i \in \mathbb{F}_{2^{2v}}$

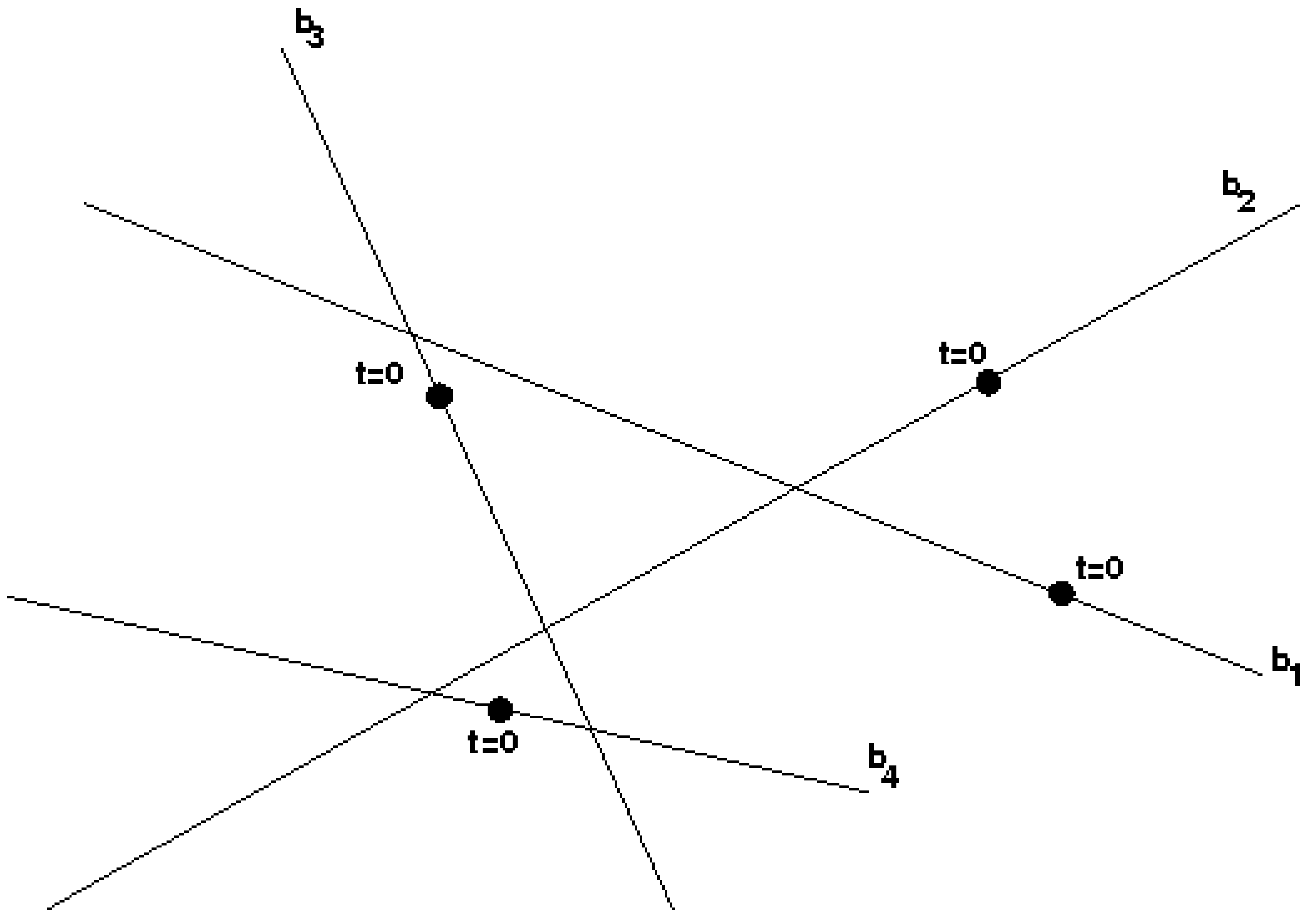
UNIVERSITÄT BAYREUTH

new construction

- new idea: use a systematic way to find (and label) combinable orbits (not a naive greedy algorithm)
- to construct a code with $k-$dimensional codewords in $\mathbb{F}_{2^{2v}}$ we start with k affine lines in $\mathbb{F}_{2^{2v}}$
- for each line we have a map $b_i : \mathbb{F}_{2^v} \longrightarrow \mathbb{F}_{2^{2v}} : t \mapsto a_i + s_i t$ for some $a_i, s_i \in \mathbb{F}_{2^{2v}}$
- idea: use t to label the 2^v $k-$dimensional subspaces $\langle b_1(t), \ldots, b_k(t) \rangle$

UNIVERSITÄT BAYREUTH

new construction



new construction

- we have to make sure, that the k points on the line a linearily independent

new construction

- we have to make sure, that the k points on the line a linearily independent
- similar argument gives: for a fixed set of parameters a_i, s_i the number of independent points is at least $2^v - 2^k + 1$, in praxis independent for all t.

UNIVERSITÄT BAYREUTH

new construction

- we have to make sure, that the k points on the line a linearily independent
- similar argument gives: for a fixed set of parameters a_i, s_i the number of independent points is at least $2^v - 2^k + 1$, in praxis independent for all t.
- now look at the orbits of each space

UNIVERSITÄT BAYREUTH

new construction

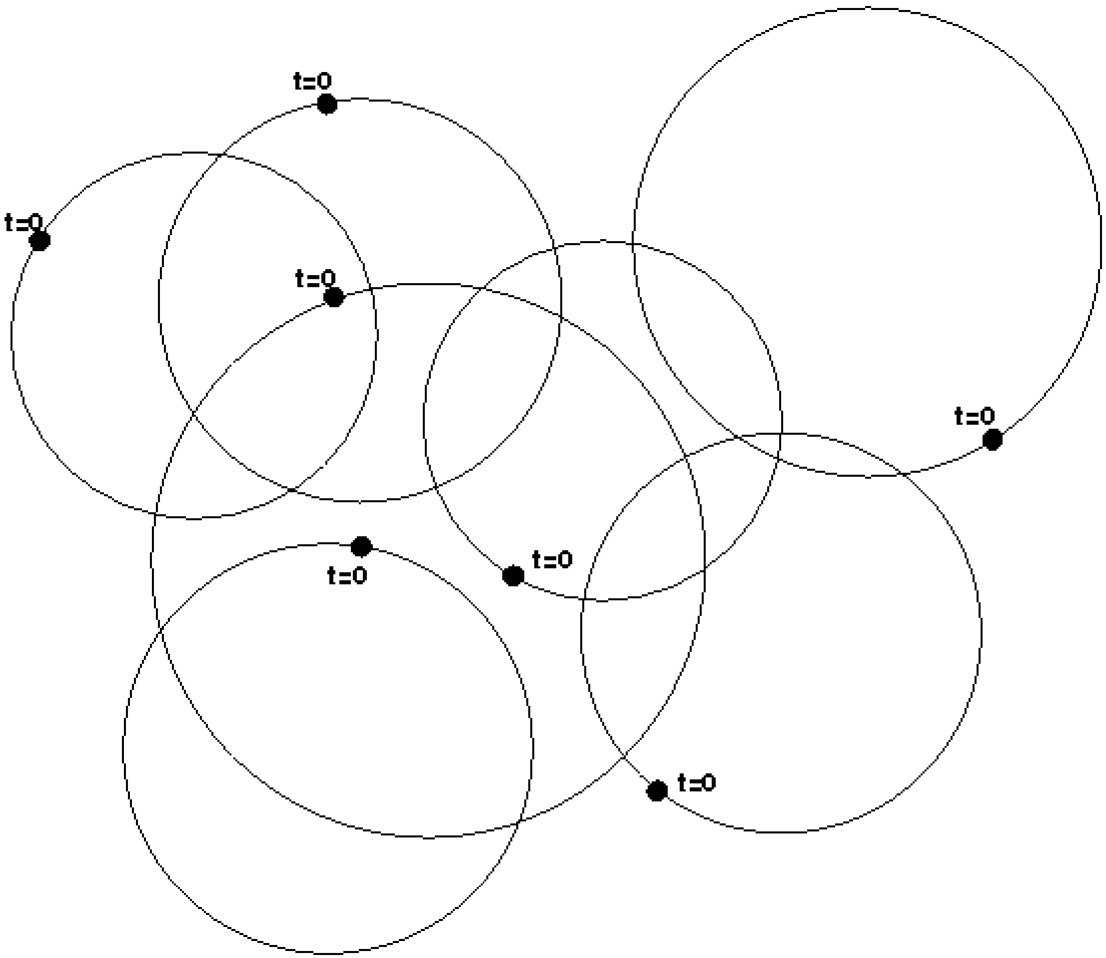
- we have to make sure, that the k points on the line a linearily independent
- similar argument gives: for a fixed set of parameters a_i, s_i the number of independent points is at least $2^v - 2^k + 1$, in praxis independent for all t.
- now look at the orbits of each space
- to check whether good and combinable we have to look at the $(2^k - 1)(2^k - 2)$ quotients

$$t \longmapsto \frac{l_i(b_1(t), \ldots, b_k(t))}{l_j(b_1(t), \ldots, b_k(t))}$$

UNIVERSITÄT
BAYREUTH

new construction

- these are circles in the Miquelian inversive plane (finite analogue of Riemann sphere)



UNIVERSITÄT BAYREUTH

new construction

- the non-combinable condition corresponds to a intersection of two circles with the extra condition, that intersection must happen for the same value of t.

UNIVERSITÄT BAYREUTH

new construction

- the non-combinable condition corresponds to a intersection of two circles with the extra condition, that intersection must happen for the same value of t.
- we call this set of parameters the exceptional set of the code (given by the k lines (= pairs a_i, s_i))

UNIVERSITÄT BAYREUTH

new construction

- the non-combinable condition corresponds to a intersection of two circles with the extra condition, that intersection must happen for the same value of t.
- we call this set of parameters the exceptional set of the code (given by the k lines (= pairs a_i, s_i))
- $k = 3$, $2v = 64$, experiment gave an example with an exceptional set of only 234 parameters. This gives a code of minimum distance 4 and $(2^{64} - 1)(2^{32} - 234)$ codewords

UNIVERSITÄT BAYREUTH

new construction

- the non-combinable condition corresponds to a intersection of two circles with the extra condition, that intersection must happen for the same value of t.
- we call this set of parameters the exceptional set of the code (given by the k lines (= pairs a_i, s_i))
- $k = 3$, $2v = 64$, experiment gave an example with an exceptional set of only 234 parameters. This gives a code of minimum distance 4 and $(2^{64} - 1)(2^{32} - 234)$ codewords
- $k = 4$, $2v = 128$, smallest exceptional set had 7044 elements –> Code with $(2^{128} - 1)(2^{64} - 7044)$ codewords

UNIVERSITÄT BAYREUTH

encoding/decoding

- central idea is to prepare a ’backup code’ for the small exceptional set

UNIVERSITÄT BAYREUTH

encoding/decoding

- central idea is to prepare a ’backup code’ for the small exceptional set
- prepare two codes C_1 and a backup code C_2 (i.e. use random affine lines and compute the exceptional sets, which must be disjoint)

encoding/decoding

- central idea is to prepare a ’backup code’ for the small exceptional set
- prepare two codes C_1 and a backup code C_2 (i.e. use random affine lines and compute the exceptional sets, which must be disjoint)
- now use C_2 if parameter t is from the exceptional set of C_1, check that for these cases the quotients of C_2 are not in C_1

encoding/decoding

- central idea is to prepare a 'backup code' for the small exceptional set
- prepare two codes C_1 and a backup code C_2 (i.e. use random affine lines and compute the exceptional sets, which must be disjoint)
- now use C_2 if parameter t is from the exceptional set of C_1, check that for these cases the quotients of C_2 are not in C_1
- prepare one further parameter t_0 such that the corresponding code in C_2 is combinable

UNIVERSITÄT BAYREUTH

encoding/decoding

- central idea is to prepare a ’backup code’ for the small exceptional set
- prepare two codes C_1 and a backup code C_2 (i.e. use random affine lines and compute the exceptional sets, which must be disjoint)
- now use C_2 if parameter t is from the exceptional set of C_1, check that for these cases the quotients of C_2 are not in C_1
- prepare one further parameter t_0 such that the corresponding code in C_2 is combinable
- we have $2^v + 1$ combinable Singer orbits each of length $2^{2v} - 1$

UNIVERSITÄT BAYREUTH

encoding/decoding

For encoding we will transform a bitsequence $(t, z) \in \mathbb{F}_{2^v} \times \mathbb{F}_{2^{2v}}$ into a $k-$dim subspace of $\mathbb{F}_{2^{2v}}$.

encoding/decoding

For encoding we will transform a bitsequence $(t, z) \in \mathbb{F}_{2^v} \times \mathbb{F}_{2^{2v}}$ into a $k-$dim subspace of $\mathbb{F}_{2^{2v}}$.

- t is the parameter to select the orbit (typically in C_1, in the exceptionally case from C_2)

UNIVERSITÄT BAYREUTH

encoding/decoding

For encoding we will transform a bitsequence $(t,z) \in \mathbb{F}_{2^v} \times \mathbb{F}_{2^{2v}}$ into a $k-$dim subspace of $\mathbb{F}_{2^{2v}}$.

- t is the parameter to select the orbit (typically in C_1, in the exceptionally case from C_2)
- choose the proper subspace from the orbit by multiplying with $z \neq 0$

encoding/decoding

For encoding we will transform a bitsequence $(t, z) \in \mathbb{F}_{2^v} \times \mathbb{F}_{2^{2v}}$ into a $k-$dim subspace of $\mathbb{F}_{2^{2v}}$.

- t is the parameter to select the orbit (typically in C_1, in the exceptionally case from C_2)
- choose the proper subspace from the orbit by multiplying with $z \neq 0$
- if z is zero use an space from the orbit with parameter t_0 in C_2 and encode by $(t_0, t11 \ldots 11)$

UNIVERSITÄT BAYREUTH

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)

UNIVERSITÄT BAYREUTH

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)
- compute one quotient x in Z

UNIVERSITÄT BAYREUTH

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)
- compute one quotient x in Z
- compute for each circle in the quotient space the parameter t giving the quotient x, this identifies the orbit

UNIVERSITÄT
BAYREUTH

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)
- compute one quotient x in Z
- compute for each circle in the quotient space the parameter t giving the quotient x, this identifies the orbit
- a division in $\mathbb{F}_{2^{2v}}$ gives the translation factor z inside the orbit giving the decoding candidate W

UNIVERSITÄT BAYREUTH

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)
- compute one quotient x in Z
- compute for each circle in the quotient space the parameter t giving the quotient x, this identifies the orbit
- a division in $\mathbb{F}_{2^{2v}}$ gives the translation factor z inside the orbit giving the decoding candidate W
- check that $dim(W \cap U) \geq k - 2$

encoding/decoding

For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2v}}$

- loop over all $2-$dim subspaces Z (unique to the codewords)
- compute one quotient x in Z
- compute for each circle in the quotient space the parameter t giving the quotient x, this identifies the orbit
- a division in $\mathbb{F}_{2^{2v}}$ gives the translation factor z inside the orbit giving the decoding candidate W
- check that $dim(W \cap U) \geq k-2$
- return t, z with special care for the case $t = t_0$

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