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)
Agenda

- 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)
Combinatorial Designs

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

\( 2 - (7, 3, 1) \) design
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 \( \{a, b, c, d, e, f, g\} \).
This is a selection problem in the lattice of all subsets of \( \{a, b, c, d, e, f, g\} \) = 1111111
This is a selection problem in the lattice of all subsets of \(\{a, b, c, d, e, f, g\}\) = 1111111 = Hamming Graph
Combinatorial Designs

Fano plane

a

b
d
e
c
f

g
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 \( \lambda \) blocks
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 $\lambda$ blocks
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 \( \lambda \) blocks
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 \( \lambda \) blocks
- \( t-(v,k,\lambda) \) \( q \)-Design
  each \( t \)-space of \( \mathbb{F}_q^v \) is in exactly \( \lambda \) of the chosen \( k \)-spaces
Combinatorial Designs

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

```
  1  abcdefg
 7  6-sets
21  5-sets
35  4-sets
35  3-sets
21  2-sets
 7  1-sets
 1  empty set
```
Combinatorial Designs

- 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 \( \mathbb{F}_q^v \).
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)
II - Network Codes
Network Codes

Model (Kötter, Kschischang)
Model (Kötter, Kschischang) one codeword:

- vectorspace $V \subset \mathbb{F}_2^q$
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)
codeword:
- subspace of $\mathbb{F}_2^\nu$
Error Correcting Network Codes

codeword:
  • subspace of $\mathbb{F}_2^\nu$

distance $d$:
  • graph theoretic distance in the Hasse diagram of the subspace lattice of $\mathbb{F}_2^\nu$
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 $\mathbb{F}_2^v$

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

$$d(U, W) = \dim(U) + \dim(W) - 2\dim(U \cap W)$$
Error Correcting Network Codes

for a fixed $d$:

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

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

fix also dimension $k$ of the subspaces:

find a set of $k$–dimensional subspaces of $\mathbb{F}_2^\nu$ with pairwise distances $\geq 2d$
for a fixed $d$:

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

fix also dimension $k$ of the subspaces:

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

constant dimension codes $\approx q$– analog of constant weight codes
Construction

original problem

find a set of \( k \)-dimensional subspaces of \( \mathbb{F}_q^2 \) with pairwise distances \( \geq 2d \)
Construction

original problem

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

modified version

find $k$–dim. subspaces $\{V_1, \ldots, V_b\}$ in $\mathbb{F}_2^q$ such that
the pairwise intersection is at most 1–dimensional
**Construction**

**original problem**

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

**modified version**

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

$\Rightarrow$ code with minimum distance $\geq 2(k - 1)$
This is a selection problem in the lattice of all subsets of \( \{a, b, c, d, e, f, g\} \)
Singer Cycle

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

i.e. multiplication in $\mathbb{F}_{2^\nu}$ with non-zero elements

inducing action of $S = (\mathbb{F}_{2^\nu})^*$ on the $k$–spaces
Singer Cycle

- On $\mathbb{F}_2^\nu$ acts the Singer cycle $S$
- i.e. multiplication in $\mathbb{F}_2^\nu$ with non-zero elements
- inducing action of $S = (\mathbb{F}_2^\nu)^*$ on the $k$–spaces

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

- typical Singer orbit on $k$-spaces has $2^\nu - 1$ elements
- like in the case of the action on $\mathbb{F}_2^\nu$
• 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
• 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 $\geq 2(k - 1)$
Description of Singer orbit

• Given a \( k \)-dimensional space \( \{u_1, \ldots, u_{2^k - 1}, 0\} \) < \( \mathbb{F}_2^\nu \)
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 $\mathbb{F}_2^v$
Description of Singer orbit

- Given a $k$-dimensional space \( \{u_1, \ldots, u_{2^k-1}, 0\} \subset \mathbb{F}_2^v \)
- 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 \( S \)
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 $2^k \choose 2$ quotients
Example

\[ k = 3 \text{, } 3\text{-}\text{space} = \{0, 1, 4, 10, 18, 23, 25\} \]

= exponents of a generator of \( \mathbb{F}_{2^v}^* \) (only for the 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 \( G_O \)
Lemma: \( O \) is a good orbit \iff all the pairwise quotients are different
Lemma: $O$ is a good orbit $\iff$ all the pairwise quotients are different

find a $k$–dim. subspace of $\mathbb{F}_2^\nu$ such that the pairwise quotients are all different

$\Rightarrow$ code with $2^\nu - 1$ codewords and minimum distance $\geq 2(k - 1)$
Lemma: $O$ is a good orbit $\iff$ all the pairwise quotients are different

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

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

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

$\Rightarrow$ code with $b(2^v - 1)$ codewords and minimum distance $\geq 2(k - 1)$
<table>
<thead>
<tr>
<th>$v$</th>
<th>$k$</th>
<th>$b$</th>
<th>number of codewords</th>
<th>$2d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>3</td>
<td>555</td>
<td>$555 \cdot (2^{15} - 1) = 18185685$</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>3</td>
<td>1056</td>
<td>69204960</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>3</td>
<td>2108</td>
<td>276297668</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>4032</td>
<td>1056960576</td>
<td>4</td>
</tr>
</tbody>
</table>
• 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 \( V < F_2^v \)

as \( d = 4 \): two possible cases in decoding:
  - one erasure (we received a 2-space \( U < V \))
  - one error (we received a 4-space \( U > V \))
Erasure

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

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

- received a 2−space \( U = \{x_1, x_2, x_3, 0\} < V \)
- compute \( x_1/x_2 \)
- find the edge \( \overrightarrow{x_1x_2} \) 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 \( \overrightarrow{x_1x_2} \) 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 \( V = \langle x_1, x_2, ux_1 \rangle \)
• received a 2-space $U = \{x_1, x_2, x_3, 0\} < V$
• compute $x_1 / x_2$
• find the edge $\overrightarrow{x_1x_2}$ 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 $\mathbb{F}_{2^v}$
• we received a 4-space $U > V$
• we received a 4–space $U > V$
• choose a random 3–subspace $W < U$, 
• we received a 4–space $U > V$
• choose a random 3–subspace $W < U$,
• we know: $W \cap V$ is at least 2–dimensional
• 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 $7$ $2$–dim subspaces of $W$
• 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 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 $U$
• 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 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
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
III - Large Network Codes
good orbits

- Restrict to codes from good orbits = intersection of two $k$–dim. codewords in the Singer orbit is at most one-dimensional.
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 $(2^k - 1)$ nonzero $\mathbb{F}_2$–linear combination of the $b_j$. 
good orbits

- at most \((2^k - 1)^4\) equations
good orbits

- at most \((2^k - 1)^4\) equations
- one equation has at most \(2 (2^\nu - 1)^{k-1}\) 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 \((2^v - 1)^k\))
good orbits

• number of equations can be reduced from

\((2^k - 1)^4\)
good orbits

- number of equations can be reduced from $(2^k - 1)^4$
- to $\left[ \begin{array}{c} k \\ 2 \end{array} \right]_2 + 28 \left[ \begin{array}{c} k \\ 3 \end{array} \right]_2 + 280 \left[ \begin{array}{c} k \\ 4 \end{array} \right]_2$
good orbits

- number of equations can be reduced from 
  \((2^k - 1)^4\)
  
- to \[ \left( \begin{array}{c} k \\ 2 \end{array} \right)^2 + 28 \left( \begin{array}{c} k \\ 3 \end{array} \right)^2 + 280 \left( \begin{array}{c} k \\ 4 \end{array} \right)^2 \]

Lemma: for \( \nu > 4k - 6 \) there are good orbits.
combinable orbits

- given one good orbit again only a ’small’ number of orbits are excluded
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
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
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
• 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
• using the idea described for a single orbit we now have to store a representative for each of the $10^{large}$ orbits
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)
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 \(\mathbb{F}_{2^v}\) we start with \(k\) affine lines in \(\mathbb{F}_{2^v}\)
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 $\mathbb{F}_{2^v}$ we start with $k$ affine lines in $\mathbb{F}_{2^v}$
- for each line we have a map
  \[ b_i : \mathbb{F}_{2^v} \to \mathbb{F}_{2^v} : t \mapsto a_i + s_i t \text{ for some } a_i, s_i \in \mathbb{F}_{2^v} \]
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 $\mathbb{F}_{2^v}$ we start with $k$ affine lines in $\mathbb{F}_{2^v}$

• for each line we have a map $b_i : \mathbb{F}_{2^v} \to \mathbb{F}_{2^v} : t \mapsto a_i + s_it$ for some $a_i, s_i \in \mathbb{F}_{2^v}$

• idea: use $t$ to label the $2^v$ $k$–dimensional subspaces $\langle b_1(t), \ldots, b_k(t) \rangle$
new construction
new construction

- we have to make sure, that the $k$ points on the line are linearly 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 $t$. 
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
new construction

• we have to make sure, that the $k$ points on the line are linearly 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

\[
    t \mapsto \frac{l_i(b_1(t), \ldots, b_k(t))}{l_j(b_1(t), \ldots, b_k(t))}
\]
new construction

- these are circles in the Miquelian inversive plane (finite analogue of Riemann sphere)
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 $t$. 
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 \( a_i, s_i \)).
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 \( a_i, s_i \))

• \( k = 3, 2\nu = 64 \), 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
new construction

- the non-combinable condition corresponds to an 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 $\rightarrow$ Code with $(2^{128} - 1)(2^{64} - 7044)$ codewords
encoding/decoding

- central idea is to prepare a 'backup code' for the small exceptional set
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 $C_1$
• 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
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 $2^{2^v} - 1$
For encoding we will transform a bitsequence \((t, z) \in \mathbb{F}_{2^v} \times \mathbb{F}_{2^v} \) into a \(k\)–dim subspace of \(\mathbb{F}_{2^v}\).
For encoding we will transform a bitsequence \((t, z) \in F_{2^v} \times F_{2^{2v}}\) into a \(k\)-dim subspace of \(F_{2^{2v}}\).

- \(t\) is the parameter to select the orbit (typically in \(C_1\), in the exceptionally case from \(C_2\))
For encoding we will transform a bitsequence \((t, z) \in F_{2^v} \times F_{2^v}\) into a \(k\)-dim subspace of \(F_{2^v}\).

- \(t\) 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 \(k-\text{dim}\) 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 \((t_0, t11 \ldots 11)\)
For decoding we use the ideas from the easier case of a single orbit. We received a space $U \subset \mathbb{F}_{2^v}$
For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^{2\nu}}$

- loop over all 2–dim subspaces $Z$ (unique to the codewords)
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 $Z$
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
For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^v}$

- 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 $\mathbb{F}_{2^v}$ gives the translation factor $z$ inside the orbit giving the decoding candidate $W$
For decoding we use the ideas from the easier case of a single orbit. We received a space $U < \mathbb{F}_{2^v}$

- 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 $\mathbb{F}_{2^v}$ gives the translation factor $z$ inside the orbit giving the decoding candidate $W$
- check that $\text{dim}(W \cap U) \geq k - 2$
encoding/decoding

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

- 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 $\mathbb{F}_{2^v}$ 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 $t = t_0$
T. Etzion, N. Silberstein: several papers on arxiv.org on constant dimension codes
T. Etzion, N. Silberstein: several papers on arxiv.org on constant dimension codes.

Thank you