# ILP techniques for binary subspace codes

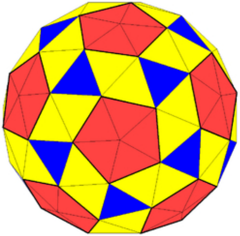

Sascha Kurz
University of Bayreuth
sascha.kurz@uni-bayreuth.de

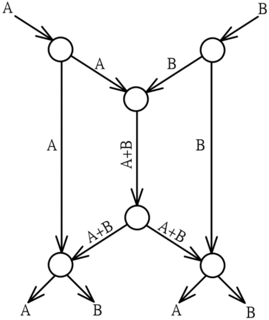
joint work with

Thomas Honold
Zhejiang University
honold@zju.edu.cn

and

Michael Kiermaier
University of Bayreuth
michael.kiermaier@uni-bayreuth.de




Algebraic combinatorics and applications (ALCOMA), Kloster Banz, Germany, 15.-20.03.2015

# Subspace Codes

- codeword: subspace of $\mathbb{F}_q^v$
- distance $d$: graph theoretic distance in the Hasse diagram of the subspace lattice of $\mathbb{F}_q^v$; $U, W \le \mathbb{F}_q^v$:

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

- problem: find a *large* set of subspaces of $\mathbb{F}_q^v$ with pairwise distances $\ge d$
- constant dimension code: all codewords have dimension $k$

# Algorithmic approaches for the determination of the maximum cardinality

**Reference**

Axel Kohnert and S.K. (2008): Construction of large constant dimension codes with a prescribed minimum distance.
In: Calmet, Jacques (Eds.): Mathematical Methods in Computer Science Springer 31-42.

# Algorithmic approaches for the determination of the maximum cardinality

- formulation as a clique problem in a graph (subspaces are vertices, two vertices are connected by an edge iff their distance is $\geq d$) $\rightsquigarrow$ `cliquer` (ask Patric)

**Reference**

Axel Kohnert and S.K. (2008): Construction of large constant dimension codes with a prescribed minimum distance.
In: Calmet, Jacques (Eds.): Mathematical Methods in Computer Science Springer 31-42.

# Algorithmic approaches for the determination of the maximum cardinality

- formulation as a clique problem in a graph (subspaces are vertices, two vertices are connected by an edge iff their distance is $\geq d$) $\rightsquigarrow$ `cliquer` (ask Patric)
- formulation as a Diophantine equation system (using slack variables) $\rightsquigarrow$ `LLL based solver` (ask Alfred)

**Reference**

Axel Kohnert and S.K. (2008): Construction of large constant dimension codes with a prescribed minimum distance.
In: Calmet, Jacques (Eds.): Mathematical Methods in Computer Science Springer 31-42.

# Algorithmic approaches for the determination of the maximum cardinality

- formulation as a clique problem in a graph (subspaces are vertices, two vertices are connected by an edge iff their distance is $\geq d$) $\rightsquigarrow$ `cliquer` (ask Patric)
- formulation as a Diophantine equation system (using slack variables) $\rightsquigarrow$ `LLL based solver` (ask Alfred)
- formulation as an Integer Linear Program (chosen subspaces are variables) $\rightsquigarrow$ e.g. `CPLEX`, `Gurobi` (this talk)

**Reference** (sorry, no use of automorphisms here. . . )

Axel Kohnert and S.K. (2008): Construction of large constant dimension codes with a prescribed minimum distance.
In: Calmet, Jacques (Eds.): Mathematical Methods in Computer Science Springer 31-42.

# An example

**Honold, Kiermaier, and K. (2015)**

The maximum cardinality of a constant dimension code with parameters $q = 2$, $v = 6$, $k = 3$, and minimal distance $d = 4$ is 77. There are exactly 5 non-isomorphic extremal codes. Some of these can be generalized to arbitrary $q$.

# An example

**Honold, Kiermaier, and K. (2015)**

The maximum cardinality of a constant dimension code with parameters $q = 2$, $v = 6$, $k = 3$, and minimal distance $d = 4$ is 77. There are exactly 5 non-isomorphic extremal codes. Some of these can be generalized to arbitrary $q$.

Given the corresponding graph $G = (V, E)$ we can formulate

$$\begin{aligned} \max \quad & \sum_{v \in V} x_v \\ \text{s.t.} \quad & x_u + x_v \le 1 \quad \forall \{u, v\} \in \overline{E} = \binom{V}{2} \backslash E \\ & x_v \in \{0, 1\} \quad \forall v \in V \quad (x_v \in [0, 1] \quad \forall v \in V) \end{aligned}$$

# An example

**Honold, Kiermaier, and K. (2015)**

The maximum cardinality of a constant dimension code with parameters $q = 2$, $v = 6$, $k = 3$, and minimal distance $d = 4$ is 77. There are exactly 5 non-isomorphic extremal codes. Some of these can be generalized to arbitrary $q$.

Given the corresponding graph $G = (V, E)$ we can formulate

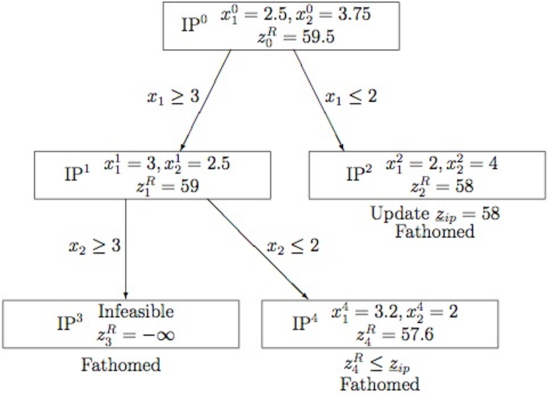
$$\begin{aligned} \max \quad & \sum_{v \in V} x_v \\ \text{s.t.} \quad & x_u + x_v \leq 1 \quad \forall \{u, v\} \in \overline{E} = \binom{V}{2} \setminus E \\ & x_v \in \{0, 1\} \quad \forall v \in V \quad (x_v \in [0, 1] \quad \forall v \in V) \end{aligned}$$

- solution time of the LP-relaxation: 5 seconds $\rightsquigarrow$ 93
- solution time of the ILP: hopeless

# Branch & Bound

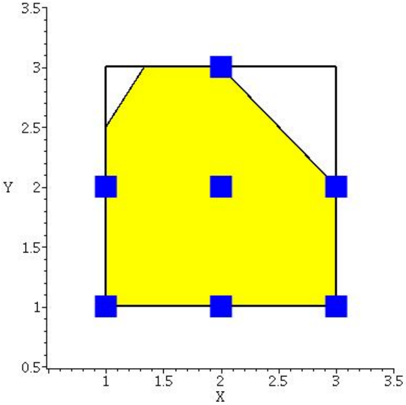
max $\quad 13x_1 + 8x_2$

s.t. $\quad x_1 + 2x_2 \leq 10,\ 5x_1 + 2x_2 \leq 20,\ x_1, x_2 \in \mathbb{Z}_{\geq 0}$



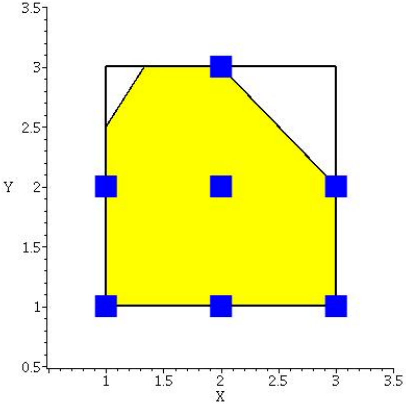
# Polyhedral descriptions

$$2Y - 3X \leq 2$$
$$X + Y \leq 5$$
$$1 \leq X \leq 3$$
$$1 \leq Y \leq 3$$
$$X, Y \in \mathbb{Z}$$



# Polyhedral descriptions

$$2Y - 3X \leq 2$$
$$X + Y \leq 5$$
$$1 \leq X \leq 3$$
$$1 \leq Y \leq 3$$
$$X, Y \in \mathbb{Z}$$




Add the valid constraint $-X + Y \leq 1$

# A perfect polyhedral description

$2Y - 3X \leq 2$

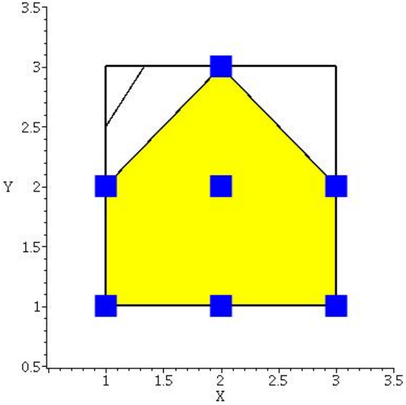
$X + Y \leq 5$

$-X + Y \leq 1$

$1 \leq X \leq 3$

$1 \leq Y \leq 3$

$X, Y \in \mathbb{Z}$




The LP-relaxation coincides with the ILP formulation!

($2Y - 3X \leq 2$ is superfluous.)

# A better polyhedral description for our example

- use independent set constraints:
  $\sum_{v \in I} x_v \leq 1$ for an independent set $I$

$$\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E, \dim(E)=3} x_E \leq 1 \quad \forall U \leq \mathbb{F}_2^6 \,:\, \dim(U) = 2$$

  solution time of the LP-relaxation: 3 seconds $\rightsquigarrow$ 93

# A better polyhedral description for our example

- use independent set constraints:
  $\sum_{v \in I} x_v \leq 1$ for an independent set $I$
  $$\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E, \dim(E)=3} x_E \leq 1 \quad \forall U \leq \mathbb{F}_2^6 \,:\, \dim(U) = 2$$
  solution time of the LP-relaxation: 3 seconds $\rightsquigarrow$ 93
- use sub-graph constraints:
  $\sum_{v \in G'} x_v \leq \alpha(G')$ for a subgraph $G' \leq G$
  $$\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E, \dim(E)=3} x_E \leq 9 \quad \forall U \leq \mathbb{F}_2^6 \,:\, \dim(U) = 1$$
  solution time of the LP-relaxation: 1.5 seconds $\rightsquigarrow$ 81

# Symmetry kills the ILP solver...

**Symmetry group**

$GL(6,2)$ of order 20 158 709 760

# Symmetry kills the ILP solver…

## Symmetry group

$GL(6, 2)$ of order 20 158 709 760

## General approach

- identify some appropriate (geometric) sub-configuration
- generate all sub-configurations up to isomorphism
- prescribe each of the sub-configurations (each one separately, Step 1)
- exclude all sub-configurations (Step 2)

# Appropriate sub-configurations

## 9-configurations

A subset of the code consisting of 9 planes passing through a common point $P$.

$$\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E,\, \dim(E)=3} x_E = 9 \text{ where } U \leq \mathbb{F}_2^6 \;:\; \dim(U) = 1$$

Up to isomorphism there are just four 9-configurations.

## 17-configurations

A subset of size 17 consisting of two 9-configurations with a common codeword.
There are 12 770 isomorphism types of 17-configurations.

# Another example – the mixed dimensional case

**Problem**

Determine the maximum sizes $A_2(6, d)$ of binary ($q = 2$) "mixed-dimension" subspace codes with packet length $v = 6$ and minimum subspace distance $d \in \{1, 2, 3, 4, 5, 6\}$.

# Another example – the mixed dimensional case

## Problem

Determine the maximum sizes $A_2(6, d)$ of binary ($q = 2$) "mixed-dimension" subspace codes with packet length $v = 6$ and minimum subspace distance $d \in \{1, 2, 3, 4, 5, 6\}$.

## Trivial case

- $d = 1$: take all subspaces $\rightsquigarrow$ 2825

## Easy cases (theoretical and computational)

- $d = 2$: take all subspaces of odd dimension $\rightsquigarrow$ 1521; for the upper bound a result of Ahlswede and Aydinian (On error control codes for random network coding, 2009) can be used
- $d = 5, 6$: plane spreads $\rightsquigarrow$ 9

# Valid inequalities for $d = 4$

$$\sum_{E \le \mathbb{F}_2^6 \,:\, U \le E,\, \dim(E)=3} x_E \le 1 \quad \forall U \le \mathbb{F}_2^6 \,:\, \dim(U) = 2$$

$$\sum_{E \le \mathbb{F}_2^6 \,:\, E \le U,\, \dim(E)=3} x_E \le 1 \quad \forall U \le \mathbb{F}_2^6 \,:\, \dim(U) = 4$$

$$\sum_{E \le \mathbb{F}_2^6 \,:\, U \le E,\, \dim(E)\le 5} x_E \le 9 \quad \forall U \le \mathbb{F}_2^6 \,:\, \dim(U) = 1$$

$$\sum_{E \le \mathbb{F}_2^6 \,:\, E \le U,\, \dim(E)\ge 1} x_E \le 9 \quad \forall U \le \mathbb{F}_2^6 \,:\, \dim(U) = 5$$

$$\sum_{P \le U \,:\, \dim(P)=1} x_P + x_U + x_{U'} + \sum_{E \le \mathbb{F}_2^6 \,:\, U \le E,\, \dim(E)=3} x_E \le 1 \quad \forall U \le U' \le \mathbb{F}_2^6 \,:\, \dim(U) = 2,\, \dim(U') = 4$$

$$\ldots$$

Several further inequalities can be stated. In the literature the problem is known as Erdős-Ko-Rado sets.

# Appropriate sub-configurations for $d = 4$

- 9-configurations
- 17-configurations
- *something* that still needs to be discovered… (or just prescribing a few points)

# Excluding 17-configurations

- let $U, U' \leq \mathbb{F}_2^6$, $\dim(U) = \dim(U') = 1$; $\mathcal{C}$ the entire code
- $\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E,\, \dim(E)=3} x_E \leq 9$ (affects 155 $x_E$; $S_1$)
- $\sum_{E \leq \mathbb{F}_2^6 \,:\, U' \leq E,\, \dim(E)=3} x_E \leq 9$ (affects 155 $x_E$; $S_2$)
- we consider the three-dimensional subspaces $E$ with either $U \leq E$ or $U' \leq E$ (295 cases; $S_1 \cup S_2$) for $U \neq U'$

# Excluding 17-configurations

- let $U, U' \leq \mathbb{F}_2^6$, $\dim(U) = \dim(U') = 1$; $\mathcal{C}$ the entire code
- $\sum_{E \leq \mathbb{F}_2^6 \,:\, U \leq E, \dim(E)=3} x_E \leq 9$ (affects 155 $x_E$; $S_1$)
- $\sum_{E \leq \mathbb{F}_2^6 \,:\, U' \leq E, \dim(E)=3} x_E \leq 9$ (affects 155 $x_E$; $S_2$)
- we consider the three-dimensional subspaces $E$ with either $U \leq E$ or $U' \leq E$ (295 cases; $S_1 \cup S_2$) for $U \neq U'$
- if $\mathcal{C} \cap S_1 \cap S_2 \neq \emptyset$ then $|\mathcal{C} \cap (S_1 \cup S_2)| \leq 16$ (no 17-configuration)
- if $\mathcal{C} \cap S_1 \cap S_2 = \emptyset$ then $|\mathcal{C} \cap (S_1 \cup S_2)| \leq 18$
- $|\mathcal{C} \cap S_1 \cap S_2| \leq 1$

# Excluding 17-configurations

- let $U, U' \le \mathbb{F}_2^6$, $\dim(U) = \dim(U') = 1$; $\mathcal{C}$ the entire code
- $\sum_{E \le \mathbb{F}_2^6 \,:\, U \le E, \dim(E)=3} x_E \le 9$ (affects 155 $x_E$; $S_1$)
- $\sum_{E \le \mathbb{F}_2^6 \,:\, U' \le E, \dim(E)=3} x_E \le 9$ (affects 155 $x_E$; $S_2$)
- we consider the three-dimensional subspaces $E$ with either $U \le E$ or $U' \le E$ (295 cases; $S_1 \cup S_2$) for $U \ne U'$
- if $\mathcal{C} \cap S_1 \cap S_2 \ne \emptyset$ then $|\mathcal{C} \cap (S_1 \cup S_2)| \le 16$ (no 17-configuration)
- if $\mathcal{C} \cap S_1 \cap S_2 = \emptyset$ then $|\mathcal{C} \cap (S_1 \cup S_2)| \le 18$
- $|\mathcal{C} \cap S_1 \cap S_2| \le 1$

$$\sum_{E \in S_1 \cap S_2} 3x_E \; + \sum_{E \in (S_1 \cup S_2) \setminus (S_1 \cap S_2)} 1x_E \;\le\; 18$$

(Big-$M$ constraint for conditional inequalities.)

# Results for $d = 4$

- prescribe a 17-configuration $\rightsquigarrow$ 77 (only 3-dimensional subspaces are used)
- prescribe a 9-configuration, exclude 17-configurations $\rightsquigarrow$ $\leq$ 74 (even using the LP relaxation)
- exclude 9-configurations $\rightsquigarrow$ 51 ... 98 (another sub-configuration to kill symmetry is needed)

**Summary**

The maximum cardinality for $d = 4$ lies between 77 and 98.

(Of course the exact upper bound is 77 and the already classified 5 isomorphism types are the complete list of extremal codes.)

# Results for $d = 3$

- an example of cardinality 104 has been found
- prescribe a 17-configuration $\rightsquigarrow$ (not completed yet)
- prescribe a 9-configuration, exclude 17-configurations $\rightsquigarrow$ $\leq 97 \ldots 114$ (still too weak)
- exclude 9-configurations $\rightsquigarrow$ $\leq 119$ (still very weak)

**Summary**

The maximum cardinality for $d = 3$ lies between 104 and 119.

(We do not know the exact answer yet. The previously best known bounds were, up to our knowledge, 85 and 123.)

# Results for $d = 3$

- an example of cardinality 104 has been found
- prescribe a 17-configuration $\rightsquigarrow$ (not completed yet)
- prescribe a 9-configuration, exclude 17-configurations $\rightsquigarrow$ $\leq 97 \ldots 114$ (still too weak)
- exclude 9-configurations $\rightsquigarrow$ $\leq 119$ (still very weak)

**Summary**

The maximum cardinality for $d = 3$ lies between 104 and 119.
(We do not know the exact answer yet. The previously best known bounds were, up to our knowledge, 85 and 123.)

Thank you very much for your attention!