Construction of codes for cryptographic purposes using groups of automorphisms

Axel Kohnert
Vlora May 2008

Bayreuth University Germany
axel.kohnert@uni-bayreuth.de

UNIVERSITÄT BAYREUTH

Overview

Overview

- Boolean functions in cyptography: which are the good ones?

Overview

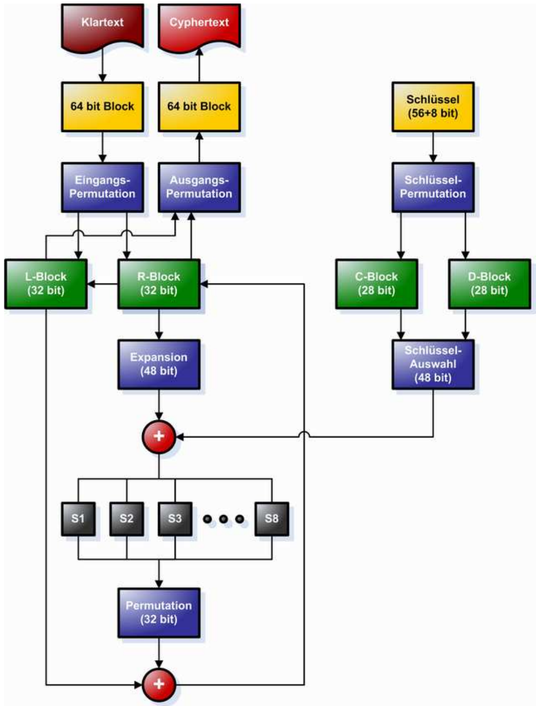
- Boolean functions in cyptography: which are the good ones?
- Construction of good cryptographic functions: use linear codes.

Overview

- Boolean functions in cyptography: which are the good ones?
- Construction of good cryptographic functions: use linear codes.
- Construction of linear codes providing good cryptographic functions.

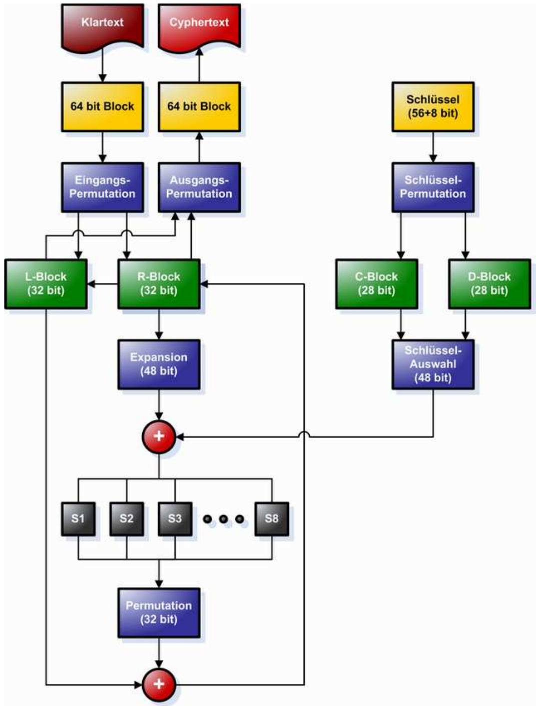
- Boolean function: $GF(2)^s \rightarrow GF(2)$

- Boolean function: $GF(2)^s \rightarrow GF(2)$



-

- Boolean function: $GF(2)^s \rightarrow GF(2)$

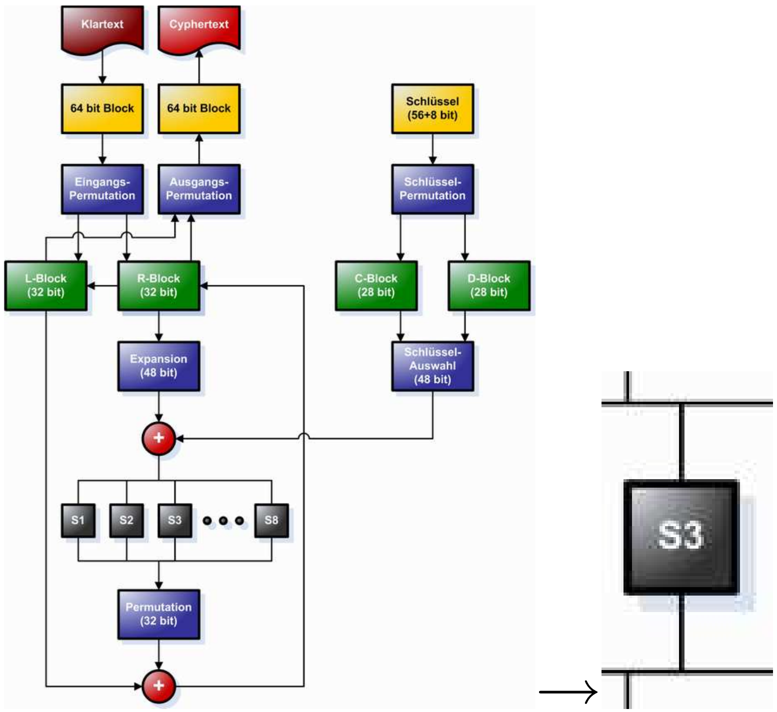


$\longrightarrow$

-

UNIVERSITÄT BAYREUTH

- Boolean function: $GF(2)^s \rightarrow GF(2)$

- 

- SBOX = substituting s input bits by l output bits = set of l Boolean functions

- Security of a Boolean function $f : GF(2)^s \rightarrow GF(2)$

- Security of a Boolean function $f : GF(2)^s \to GF(2)$
- Definition: a function $f : GF(2)^s \to GF(2)$ is $m-$**resilient** if we can fix any set of m input bits $(m < s)$ and the reduced function with only 2^{s-m} different inputs gives 0 and 1 equally often.

- Security of a Boolean function $f : GF(2)^s \to GF(2)$
- Definition: a function $f : GF(2)^s \to GF(2)$ is $m-$**resilient** if we can fix any set of m input bits $(m < s)$ and the reduced function with only 2^{s-m} different inputs gives 0 and 1 equally often.
- $f : GF(2)^s \to GF(2)$ satisfies the **extended propagation criteria** $EPC(l)$ of order m if for each Δ with $1 \leq wt(\Delta) \leq l$ the difference function $f(x) + f(x + \Delta)$ is $m-$resilient.

- This definition is motivated by possible attacks against Boolean functions representing S-boxes.

- This definition is motivated by possible attacks against Boolean functions representing S-boxes.
- There are several constructions known.

- linear $[n,k]_q$-code C = $k-$dimensional subspace of $GF(q)^n$

Linear Codes and Cryptography

- linear $[n,k]_q$-code C = $k-$dimensional subspace of $GF(q)^n$
- dual code $C^\perp$= dual space = $\{v \in GF(q)^n : cv^T = 0$ for all $c \in C\}$ is an $[n, n-k]_q$-code

UNIVERSITÄT BAYREUTH

Linear Codes and Cryptography

- linear $[n,k]_q$-code C = $k-$dimensional subspace of $GF(q)^n$
- dual code $C^{\perp}$= dual space = $\{v \in GF(q)^n : cv^T = 0$ for all $c \in C\}$ is an $[n, n-k]_q$-code
- Hamming weight $w(v)$ = number of non-zero coordinates of the codeword v

UNIVERSITÄT BAYREUTH

- linear $[n,k]_q$-code C = $k-$dimensional subspace of $GF(q)^n$
- dual code $C^\perp$= dual space = $\{v \in GF(q)^n : cv^T = 0$ for all $c \in C\}$ is an $[n, n-k]_q$-code
- Hamming weight $w(v)$ = number of non-zero coordinates of the codeword v
- Hamming distance $d(v,w)$ = number of different coordinates = $w(v-w)$

- linear $[n, k]_q$-code C = $k-$dimensional subspace of $GF(q)^n$
- dual code $C^{\perp}$= dual space = $\{v \in GF(q)^n : cv^T = 0$ for all $c \in C\}$ is an $[n, n-k]_q$-code
- Hamming weight $w(v)$ = number of non-zero coordinates of the codeword v
- Hamming distance $d(v, w)$ = number of different coordinates = $w(v - w)$
- Minimum distance = $min\{d(v, w) : v \neq w \in C\}$ = $min\{w(v) : v \in C\backslash 0\}$

- generator matrix Γ, rows are a basis of C

Linear Codes and Cryptography

- generator matrix Γ, rows are a basis of C
- check matrix, generator matrix of $C^{\perp}$

Linear Codes and Cryptography

- generator matrix Γ, rows are a basis of C
- check matrix, generator matrix of $C^\perp$
- dual distance $d^\perp$= minimum distance of $C^\perp$

UNIVERSITÄT BAYREUTH

Linear Codes and Cryptography

- generator matrix Γ, rows are a basis of C
- check matrix, generator matrix of $C^\perp$
- dual distance $d^\perp$= minimum distance of $C^\perp$
- primal distance d = minimum distance of C

UNIVERSITÄT BAYREUTH

- **Theorem**:Kurosawa et al.
  From an $[n, k]_2-$code C with primal distance d and dual distance $d^{\perp}$, we get a Boolean Funktion f :$GF(2)^{2n} \to GF(2)$ satisfying $EPC(d^{\perp} - 1)$ of order $d - 1$.

- **Theorem**:Kurosawa et al.
  From an $[n,k]_2-$code C with primal distance d and dual distance $d^{\perp}$, we get a Boolean Funktion $f: GF(2)^{2n} \to GF(2)$ satisfying $EPC(d^{\perp}-1)$ of order $d-1$.

- Let Γ be a generator matrix of C, then

$$f : (x_1, \ldots, x_n, x_{n+1}, \ldots x_{2n}) \mapsto$$
$$(x_1, \ldots, x_n)(\Gamma^T \cdot \Gamma)(x_{n+1}, \ldots, x_{2n})$$

Construction of Linear Codes

- Describe linear codes using finite projective geometry

UNIVERSITÄT BAYREUTH

Construction of Linear Codes

- Describe linear codes using finite projective geometry

- Describe primal distance using finite projective geometry

Construction of Linear Codes

- Describe linear codes using finite projective geometry
- Describe primal distance using finite projective geometry
- Describe dual distance using finite projective geometry

Construction of Linear Codes

- $[n,k]_q$- code C with generator matrix
  $\Gamma = (\gamma_1, \ldots, \gamma_n)$.

UNIVERSITÄT BAYREUTH

Construction of Linear Codes

- $[n,k]_q$- code C with generator matrix $\Gamma = (\gamma_1, \dots, \gamma_n)\,.$
- Multiplication of a column γ_i by a nonzero field element or permuting the columns gives an equivalent code.

UNIVERSITÄT BAYREUTH

Construction of Linear Codes

- $[n,k]_q$- code C with generator matrix $\Gamma = (\gamma_1, \ldots, \gamma_n)$.
- Multiplication of a column γ_i by a nonzero field element or permuting the columns gives an equivalent code.
- Work with the $n-$set $\{\gamma_1, \ldots, \gamma_n\}$ of columns up to multiplication with a nonzero scalar.

Construction of Linear Codes

- $[n,k]_q$- code C with generator matrix $\Gamma = (\gamma_1, \ldots, \gamma_n)$.
- Multiplication of a column γ_i by a nonzero field element or permuting the columns gives an equivalent code.
- Work with the $n-$set $\{\gamma_1, \ldots, \gamma_n\}$ of columns up to multiplication with a nonzero scalar.
- $C \leftrightarrow$set of n points $\{\gamma_1, \ldots, \gamma_n\}$in finite projective geometry $PG(k-1,q)$

Construction of Linear Codes

- generator matrix $\Gamma = (\gamma_1, \ldots, \gamma_n)\,.$

UNIVERSITÄT BAYREUTH

Construction of Linear Codes

- generator matrix $\Gamma = (\gamma_1, \ldots, \gamma_n)$.
- codeword $c = v \cdot \Gamma = v\gamma_1, \ldots, v\gamma_n$ given by n inner products with $v \in GF(q)^k$

UNIVERSITÄT BAYREUTH

Construction of Linear Codes

- generator matrix $\Gamma = (\gamma_1, \ldots, \gamma_n)$.
- codeword $c = v \cdot \Gamma = v\gamma_1, \ldots, v\gamma_n$ given by n inner products with $v \in GF(q)^k$
- weight of c is invariant under scalar multiplication of v with a nonzero field element

Construction of Linear Codes

- generator matrix $\Gamma = (\gamma_1, \dots, \gamma_n)$.
- codeword $c = v \cdot \Gamma = v\gamma_1, \dots, v\gamma_n$ given by n inner products with $v \in GF(q)^k$
- weight of c is invariant under scalar multiplication of v with a nonzero field element
- to get all codewords $c = v \cdot \Gamma$ up to scalar multiplicaton loop v over all points from $PG(k-1, q)$

UNIVERSITÄT BAYREUTH

Minimum Weight

- weight of a codeword $c = v\Gamma = v\gamma_1, \ldots, v\gamma_n$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ s.t. $c\gamma_i \neq 0$

Minimum Weight

- weight of a codeword $c = v\Gamma = v\gamma_1, \ldots, v\gamma_n$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ s.t. $c\gamma_i \neq 0$
- weight of a codeword $v\Gamma$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are not orthogonal to v

UNIVERSITÄT BAYREUTH

Minimum Weight

- weight of a codeword $c = v\Gamma = v\gamma_1, \ldots, v\gamma_n$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ s.t. $c\gamma_i \neq 0$
- weight of a codeword $v\Gamma$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are not orthogonal to v
- weight of a codeword $v\Gamma$ is $n-$ number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are orthogonal to v

UNIVERSITÄT BAYREUTH

Minimum Weight

- weight of a codeword $c = v\Gamma = v\gamma_1, \ldots, v\gamma_n$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ s.t. $c\gamma_i \neq 0$
- weight of a codeword $v\Gamma$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are not orthogonal to v
- weight of a codeword $v\Gamma$ is $n-$ number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are orthogonal to v
- weight of a codeword $v\Gamma$ is $n-$ number of points from $\{\gamma_1, \ldots, \gamma_n\}$ in the hyperplane $v^\perp$

Minimum Weight

- weight of a codeword $c = v\Gamma = v\gamma_1, \ldots, v\gamma_n$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ s.t. $c\gamma_i \neq 0$
- weight of a codeword $v\Gamma$ is the number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are not orthogonal to v
- weight of a codeword $v\Gamma$ is $n-$ number of points from $\{\gamma_1, \ldots, \gamma_n\}$ which are orthogonal to v
- weight of a codeword $v\Gamma$ is $n-$ number of points from $\{\gamma_1, \ldots, \gamma_n\}$ in the hyperplane $v^\perp$
- minimum weight $\geq d$ iff each hyperplane $v^\perp$ contains $\leq n-d$ points from $\{\gamma_1, \ldots, \gamma_n\}$.

UNIVERSITÄT BAYREUTH

Incidence System

- use this point - hyperplane incidence property to describe the minimum distance by a linear Diophantine system

Incidence System

- use this point - hyperplane incidence property to describe the minimum distance by a linear Diophantine system
- $D :=$incidence matrix between points (=columns) and hyperplanes (=rows) of $PG(k-1,q)$

UNIVERSITÄT BAYREUTH

Incidence System

- use this point - hyperplane incidence property to describe the minimum distance by a linear Diophantine system
- $D :=$incidence matrix between points (=columns) and hyperplanes (=rows) of $PG(k-1, q)$
- D is a $m \times m$ $(0/1)-$matrix where $m :=$number of points in $PG(k-1, q)$

UNIVERSITÄT BAYREUTH

Theorem: There is a $[n, k, \geq d]_q-$code iff there is an integral solution $x = (x_1, \ldots, x_m)^T$ with $x_i \geq 0$ of

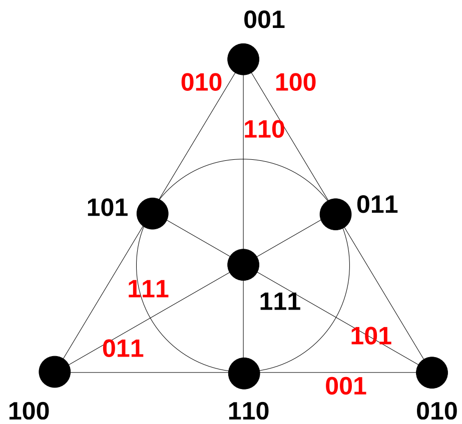
1. $\sum x_i = n$
2. $Dx \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix}$

Small Example

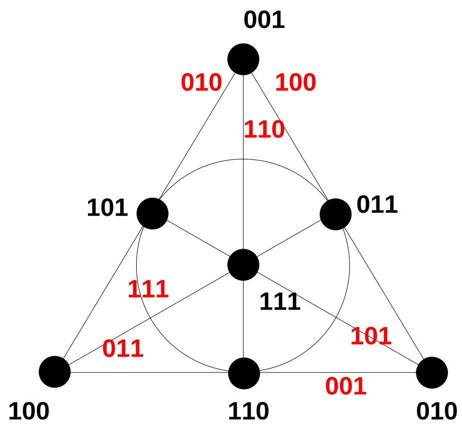
Construction of a $[4,3,2]_2-$code. Working in $PG(2,2)$.

UNIVERSITÄT BAYREUTH

Construction of a $[4,3,2]_2-$code. Working in $PG(2,2)$.



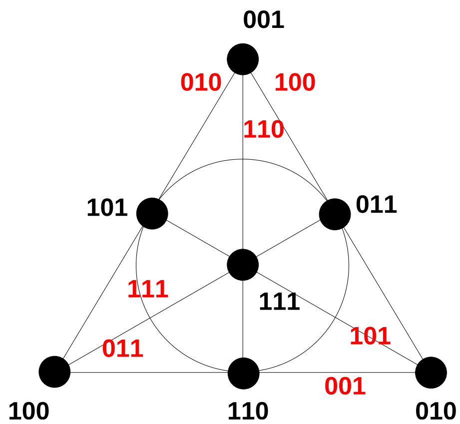
Construction of a $[4,3,2]_2-$code. Working in $PG(2,2)$.



$\longrightarrow D =$

	001	010	011	100	101	110	111
001	0	1	0	1	0	1	0
010	1	0	0	1	1	0	0
011	0	0	1	1	0	0	1
100	1	1	1	0	0	0	0
101	0	1	0	0	1	0	1
110	1	0	0	0	0	1	1
111	0	0	1	0	1	1	0

Construction of a $[4,3,2]_2-$code. Working in $PG(2,2)$.



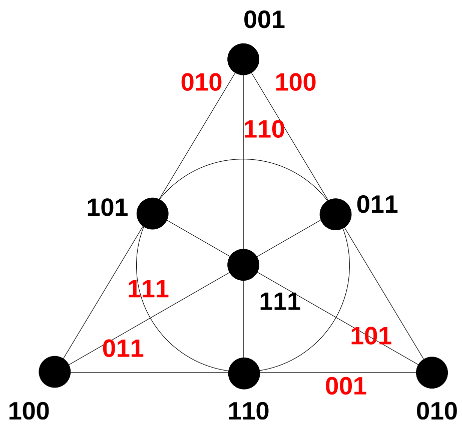
$\rightarrow D =$

	001	010	011	100	101	110	111
001	0	1	0	1	0	1	0
010	1	0	0	1	1	0	0
011	0	0	1	1	0	0	1
100	1	1	1	0	0	0	0
101	0	1	0	0	1	0	1
110	1	0	0	0	0	1	1
111	0	0	1	0	1	1	0

Find 4 columns such that in each row the sum is at most 2

Small Example

Construction of a $[4,3,2]_2-$code. Working in $PG(2,2)$.



$\rightarrow D =$

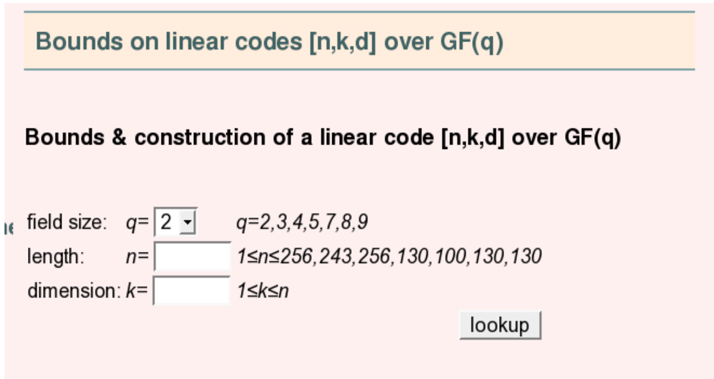
	001	010	011	100	101	110	111
001	0	1	0	1	0	1	0
010	1	0	0	1	1	0	0
011	0	0	1	1	0	0	1
100	1	1	1	0	0	0	0
101	0	1	0	0	1	0	1
110	1	0	0	0	0	1	1
111	0	0	1	0	1	1	0

Find 4 columns such that in each row the sum is at most 2

column $1, 2, 5, 6$ gives generator matrix $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

UNIVERSITÄT BAYREUTH

Database of best minimum distance possible:
www.codetables.de


Bounds on linear codes [n,k,d] over GF(q)

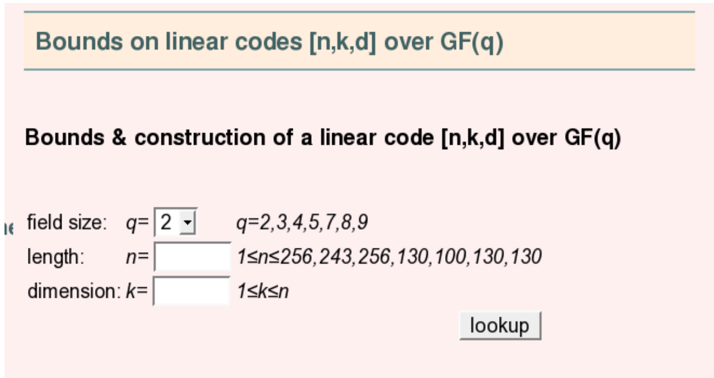
Bounds & construction of a linear code [n,k,d] over GF(q)

field size:	*q*=	2	*q*=2,3,4,5,7,8,9
length:	*n*=		1≤*n*≤256,243,256,130,100,130,130
dimension:	*k*=		1≤*k*≤*n*

lookup

Real Example

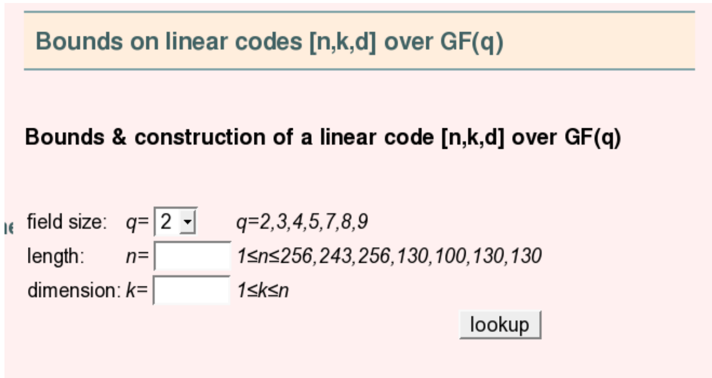
Database of best minimum distance possible:
www.codetables.de



real example: $q = 5$ $k = 7$ $n = 26$, size of D = $(5^7 - 1)/4$=19531

Real Example

Database of best minimum distance possible: www.codetables.de



real example: $q = 5$ $k = 7$ $n = 26$, size of D = $(5^7 - 1)/4$=19531

$\binom{19531}{26}$ = $88305459316602033393836441203136554503445356602753992\dots$ selections of columns

Automorphisms

- Prescribe automorphisms $\{M \in PGL(k-1,q)\}$ of a point set corresponding to a solution.

Automorphisms

- Prescribe automorphisms $\{M \in PGL(k-1,q)\}$ of a point set corresponding to a solution.
- A point set $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ has an automorphism M iff $M\gamma_i \in \Gamma$ for all γ_i

UNIVERSITÄT BAYREUTH

Automorphisms

- Prescribe automorphisms $\{M \in PGL(k-1,q)\}$ of a point set corresponding to a solution.
- A point set $\Gamma = \{\gamma_1, \dots, \gamma_n\}$ has an automorphism M iff $M\gamma_i \in \Gamma$ for all γ_i
- A solution is now built by orbits of the group G generated by $\{M\}$.

Automorphisms

- Prescribe automorphisms $\{M \in PGL(k-1,q)\}$ of a point set corresponding to a solution.
- A point set $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ has an automorphism M iff $M\gamma_i \in \Gamma$ for all γ_i
- A solution is now built by orbits of the group G generated by $\{M\}$.
- The size of D can be reduced by adding up columns corresponding to points of an orbit under G.

Automorphisms

- Automorphisms M are compatible with the incidence structure:

UNIVERSITÄT BAYREUTH

Automorphisms

- Automorphisms M are compatible with the incidence structure:
- for a point p and a line (hyperplane,...) L we have

$$p \in L \iff Mp \in ML$$

UNIVERSITÄT BAYREUTH

Automorphisms

- Automorphisms M are compatible with the incidence structure:
- for a point p and a line (hyperplane,...) L we have

$$p \in L \iff Mp \in ML$$

- Rows of D corresponding to hyperplanes in the same orbit are equal after adding up the columns

Automorphisms

- Automorphisms M are compatible with the incidence structure:
- for a point p and a line (hyperplane,...) L we have

$$p \in L \iff Mp \in ML$$

- Rows of D corresponding to hyperplanes in the same orbit are equal after adding up the columns
- We remove duplicate rows =:D^G

Automorphisms

- Automorphisms M are compatible with the incidence structure:
- for a point p and a line (hyperplane,...) L we have

$$p \in L \iff Mp \in ML$$

- Rows of D corresponding to hyperplanes in the same orbit are equal after adding up the columns
- We remove duplicate rows =:D^G
- D^G is a square matrix, size = number of orbits on points = number of orbits on hyperplanes

Theorem(Braun,K,Wassermann):
Let $G < PGL(k-1,q)$ with m orbits on the points of $PG(k-1,q)$. There is an $[n,k]_q-$code with primal distance d and with symmetries from G iff there is an integral solution $x = (x_1,\ldots,x_m)^T$with $x_i \geq 0$ of

1) $\sum \omega_i x_i = n$ 2) $D^G x \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix}$

where ω_i is the size of the $i-$th orbit of G on the points of $PG(k-1,q)$.

www.codetables.de

Bounds on linear codes [26,7] over GF(5)

lower bound: 16
upper bound: 16

Construction

Construction type: **Kohnert**

```
Construction of a linear
code [26,7,16] over GF(5):
[1]:  [26, 7, 16] Linear Code over GF(5)
      Code found by Axel Kohnert
Construction from a stored generator matrix

last modified: 2008-05-05
```

number of orbits = 1695
orbits of size $12, 6, 4, 3, 1$
4 orbits used to build the generator matrix

known:
An $[n,k]_q-$code C has primal distance $\geq d \iff$ each $(d-1)-$set of columns of a check matrix of C is linearly independent

Dual Distance

known:
An $[n,k]_q-$code C has primal distance $\geq d \iff$ each $(d-1)-$set of columns of a check matrix of C is linearly independent

dual version:
An $[n,k]_q-$code C has dual distance $\geq d^\perp \iff$ each $(d^\perp - 1)-$set of columns of a generator matrix of C is linearly independent

Example $d^{\perp} = 4$

$d^{\perp} = 4:$ no 3 points on a line of $PG(k-1,q)$.
$D_2:$ incidence matrix between points (columns) and lines (rows) of $PG(k-1,q)$.

$d^\perp = 4$: no 3 points on a line of $PG(k-1, q)$.
D_2 : incidence matrix between points (columns) and lines (rows) of $PG(k-1, q)$.

Theorem:
There is an $[n, k]_q$–code with $d^\perp \geq 4$ iff there is an integral solution $x = (x_1, \ldots, x_m)^T$ with $x_i \geq 0$ of

1) $\sum x_i = n$ 2) $D_2 x \leq \begin{pmatrix} 2 \\ \vdots \\ 2 \end{pmatrix}$

$d^{\perp} = 4$: no 3 points on a line of $PG(k-1,q)$.

D_2 : incidence matrix between points (columns) and lines (rows) of $PG(k-1,q)$.

Theorem:

There is an $[n,k]_q-$code with $d^{\perp} \geq 4$ iff there is an integral solution $x = (x_1, \ldots, x_m)^T$ with $x_i \geq 0$ of

1) $\sum x_i = n$ 2) $D_2 x \leq \begin{pmatrix} 2 \\ \vdots \\ 2 \end{pmatrix}$

This is a general method to prescribe primal and dual distance. And you can use automorphisms again.

typical **Theorem**:
There is an $[n,k]_q-$code with primal distance d and dual distance 5 and with symmetries from G iff there is an integral solution $x=(x_1,\ldots,x_m)^T$with $x_i \geq 0$ of

$$1)\ \sum \omega_i x_i = n \qquad 2)\ D^G x \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix} \qquad 3)\ D^G_3 x \leq \begin{pmatrix} 3 \\ \vdots \\ 3 \end{pmatrix}$$

UNIVERSITÄT BAYREUTH

Matsumoto et al. (2006) defined the number $N(d, d^{\perp})$ as the minimal length of a linear binary code with minimum distance d and dual distance $d^{\perp}$. Using above construction we got codes giving new upper bounds.

$d \backslash d^{\perp}$	3	4	5	6	7	8
3	6	–				
4	7	8				
5	11	13	16			
6	12	14	17	18		
7	14	15	19 – 20	20 – 21	22	
8	15	16	20 – 21	21 – 22	23	24

Results in Projective Geometry

Caps in projective geometry $PG(k-1,q)$ are codes having dual distance 4. The optimal cap problem is the search for a code with dual distance 4 and maximal length n.

In the case $q=3$ and $k=7$ we found several new $[112,7]_3-$codes with dual distance 4.

UNIVERSITÄT BAYREUTH

Last Page

- linearcodes.uni-bayreuth.de
- Betten, Braun, Fripertinger, Kerber, Kohnert, Wassermann: Error-Correcting Linear Codes - Classification by Isometry and Applications , ACM Vol. 18, Springer 2006, 42.75 Euro til end of July
- Matsumoto et al.: Primal-dual distance bounds of linear codes with application to cryptography, IEEE Trans. Inform. Theory 52 (2006), 4251–4256

Last Page

- linearcodes.uni-bayreuth.de
- Betten, Braun, Fripertinger, Kerber, Kohnert, Wassermann: Error-Correcting Linear Codes - Classification by Isometry and Applications , ACM Vol. 18, Springer 2006, 42.75 Euro til end of July
- Matsumoto et al.: Primal-dual distance bounds of linear codes with application to cryptography, IEEE Trans. Inform. Theory 52 (2006), 4251–4256

Thank you very much for your attention.

UNIVERSITÄT BAYREUTH