

Construction of Linear Codes with Prescribed Primal and Dual Minimum Distance

Axel Kohnert

Magdeburg November 2007

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

- Coding Theory
- Geometry
- Modelling
- Application

Coding Theory



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

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

- linear $[n, k]_q$ -code $C = k$ -dimensional subspace of $GF(q)^n$
- dual code $C^\perp =$ dual space $= [n, n - k]_q$ -code
- Hamming weight $w(v) =$ number of non-zero coordinates

- linear $[n, k]_q$ -code $C = k$ -dimensional subspace of $GF(q)^n$
- dual code $C^\perp =$ dual space $= [n, n - k]_q$ -code
- Hamming weight $w(v) =$ number of non-zero coordinates
- 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 $= [n, n - k]_q$ -code
- Hamming weight $w(v) =$ number of non-zero coordinates
- Hamming distance $d(v, w) =$ number of different coordinates $= w(v - w)$
- Minimum distance $= \min\{d(v, w) : v \neq w \in C\} = \min\{w(v) : v \in C \setminus \{0\}\}$

- generator matrix, rows are a basis of C

- generator matrix, rows are a basis of C
- check matrix, generator matrix of C^\perp

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

Search for code C with prescribed:

Search for code C with prescribed:

- field size q

Search for code C with prescribed:

- field size q
- length n

Search for code C with prescribed:

- field size q
- length n
- dimension k

Search for code C with prescribed:

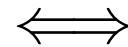
- field size q
- length n
- dimension k
- minimum distance d

Search for code C with prescribed:

- field size q
- length n
- dimension k
- minimum distance d
- dual minimum distance d^\perp

known:

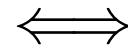
An $[n, k]_q$ -code C has minimum distance $\geq d$



each $(d - 1)$ -set of columns of a check matrix of C is linearly independent

known:

An $[n, k]_q$ -code C has minimum distance $\geq d$



each $(d - 1)$ -set of columns of a check matrix of C is linearly independent

This allows to control the dual minimum distance given a generator matrix

Geometry



- code-quality does not change if we reorder the columns

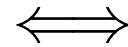
- code-quality does not change if we reorder the columns
- code-quality does not change if we multiply columns with non-zero field elements

- code-quality does not change if we reorder the columns
- code-quality does not change if we multiply columns with non-zero field elements
- generator matrix = set of 1–dim subspaces of $GF(q)^k$

- code-quality does not change if we reorder the columns
- code-quality does not change if we multiply columns with non-zero field elements
- generator matrix = set of 1–dim subspaces of $GF(q)^k$
- code = point (multi-)set in the projective geometry $PG(k - 1, q)$

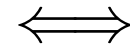
- code-quality does not change if we reorder the columns
- code-quality does not change if we multiply columns with non-zero field elements
- generator matrix = set of 1–dim subspaces of $GF(q)^k$
- code = point (multi-)set in the projective geometry $PG(k - 1, q)$
- points (=0–flat), lines (=1–flat), hyper-plane (= $(k - 2)$ –flat)

- minimum distance $\geq d$



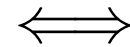
at most $n - d$ points in any hyper-plane

- minimum distance $\geq d$



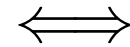
at most $n - d$ points in any hyper-plane

- dual minimum distance ≥ 3



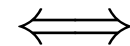
no 2 columns dependent

- minimum distance $\geq d$

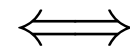


at most $n - d$ points in any hyper-plane

- dual minimum distance ≥ 3



no 2 columns dependent



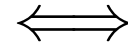
no multiset of points

in general:



in general:

dual distance $\geq d^\perp$



no $(d^\perp - 1)$ points on a $(d^\perp - 3)$ -flat

Search for code C with prescribed:

- field size q
- length n
- dimension k
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q
 PG over field $GF(q)$
- length n
- dimension k
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q
 PG over field $GF(q)$
- length n
cardinality of the point set
- dimension k
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q
 PG over field $GF(q)$
- length n
cardinality of the point set
- dimension k
points in $PG(k-1, q)$
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q
 PG over field $GF(q)$
- length n
cardinality of the point set
- dimension k
points in $PG(k-1, q)$
- minimum distance d
intersection number with hyper-planes
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q
 PG over field $GF(q)$
- length n
cardinality of the point set
- dimension k
points in $PG(k-1, q)$
- minimum distance d
intersection number with hyper-planes
- dual minimum distance d^\perp
intersection number with $(d^\perp - 3)$ -flats

Modelling



To find codes=point-sets with the help of the computer use:

find n points from the set of all points in $PG(k-1, q)$

=

0/1 solution of a system with $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ variables $(x_i)_{i=1, \dots}$

Search for code C with prescribed:

- field size q , dimension k
- length n
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q , dimension k
number of variables
- length n
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q , dimension k
number of variables
- length n
 $\sum x_i = n$
- minimum distance d
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q , dimension k
number of variables
- length n
 $\sum x_i = n$
- minimum distance d
for each hyperplane with points x_{i_1}, x_{i_2}, \dots
 $x_{i_1} + x_{i_2} + \dots \leq n - d$
- dual minimum distance d^\perp

Search for code C with prescribed:

- field size q , dimension k
number of variables
- length n
 $\sum x_i = n$
- minimum distance d
for each hyperplane with points x_{i_1}, x_{i_2}, \dots
 $x_{i_1} + x_{i_2} + \dots \leq n - d$
- dual minimum distance d^\perp
for each $(d^\perp - 3)$ -flat with points x_{j_1}, x_{j_2}, \dots
 $x_{j_1} + x_{j_2} + \dots < d^\perp - 1$

- Diophantine system of linear equations

equations

length n	$\sum x_i$	$=$	n
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$

- Diophantine system of linear equations

length n	$\sum x_i$	$=$	n	# equations 1
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$	
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$	

- Diophantine system of linear equations

length n	$\sum x_i$	$=$	n
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$

equations

1

#points

- Diophantine system of linear equations

length n	$\sum x_i$	$=$	n	# equations 1
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$	#points
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$	$\#(d^\perp - 3)$ -flats

- Diophantine system of linear equations

length n	$\sum x_i$	$=$	n	# equations
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$	#points
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$	$\#(d^\perp - 3)$ -flats

- number of variables = number of points

- Diophantine system of linear equations

length n	$\sum x_i$	$=$	n	# equations 1
distance d	$x_{i_1} + x_{i_2} + \dots$	\leq	$n - d$	#points
dual d^\perp	$x_{j_1} + x_{j_2} + \dots$	$<$	$d^\perp - 1$	$\#(d^\perp - 3)$ -flats

- number of variables = number of points
- Too large: $q = 2, k = 11,$
2047 points, $d^\perp = 4, 698027$ lines

Reduce the Problem

search now for solutions with special properties

Reduce the Problem

search now for solutions with special properties

- action of $G < PGL(k - 1, q)$ on $PG(k - 1, q)$
- columns (points of $PG(k - 1, q)$) are the orbits
- number of variables = number of orbits
- solution has $\phi \in G$ as an automorphism

Reduce the Problem

search now for solutions with special properties

- action of $G < PGL(k - 1, q)$ on $PG(k - 1, q)$
- columns (points of $PG(k - 1, q)$) are the orbits
- number of variables = number of orbits
- solution has $\phi \in G$ as an automorphism
- automorphism $\phi \in G$ is incidence - preserving
- point p in flat $f \iff \phi(p) \in \phi(f)$

Reduce the Problem

- rows corresponding to flats in the same orbit are identical

Reduce the Problem

- rows corresponding to flats in the same orbit are identical
- automorphisms also reduce the number of rows

Reduce the Problem

- rows corresponding to flats in the same orbit are identical
- automorphisms also reduce the number of rows
- size of the system of equations is now the number of orbits

Application



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

- Boolean ($q = 2$) function: $GF(2)^s \rightarrow GF(2)$
- Definition: a function $f : GF(2)^s \rightarrow GF(2)$ 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.

- Boolean ($q = 2$) function: $GF(2)^s \rightarrow GF(2)$
- Definition: a function $f : GF(2)^s \rightarrow GF(2)$ 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.
- $f : GF(2)^s \rightarrow GF(2)$ 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.

- Theorem:Kurosawa et al.

Given an $[n, k, d]_2$ -code with dual distance d^\perp , we get a Boolean Funktion $GF(2)^{2n} \rightarrow GF(2)$ satisfying $EPC(d^\perp - 1)$ of order $d - 1$.

Thank you very much for your attention.

