Construction of Optimal Linear Codes

Axel Kohnert

Thurnau April 2005

Bayreuth University

kohnert@uni-bayreuth.de

www.mathe2.uni-bayreuth.de

Construction of Sometimes Optimal Linear Codes

Axel Kohnert

Thurnau April 2005

Bayreuth University
kohnert@uni-bayreuth.de
www.mathe2.uni-bayreuth.de

UNIVERSITÄT BAYREUTH

Linear Code

A *linear* (n, k, q) *code* C is a $k-$dimensional subspace of the vectorspace $GF(q)^n$.

Linear Code

A *linear* (n, k, q) *code* C is a $k-$dimensional subspace of the vectorspace $GF(q)^n$.

The *generator matrix* Γ of a linear (n, k, q) code C is a $k \times n$ matrix where each row is a basis element of the code C.

Linear Code

A *linear* (n,k,q) *code* C is a $k-$dimensional subspace of the vectorspace $GF(q)^n$.

The *generator matrix* Γ of a linear (n,k,q) code C is a $k \times n$ matrix where each row is a basis element of the code C.

$$C = \{v\Gamma : v \in GF(q)^k\}$$

Minimum Distance

The minimum distance of a linear code is the minimum number of nonzero entries (=weight) of all nonzero codewords.

Minimum Distance

The minimum distance of a linear code is the minimum number of nonzero entries (=weight) of all nonzero codewords.

We want to find generator matrices Γ of good codes, this means the weight $wt(v\Gamma)$ is high for all nonzero $v \in GF(q)^k$.

Minimum Distance

The minimum distance of a linear code is the minimum number of nonzero entries (=weight) of all nonzero codewords.

We want to find generator matrices Γ of good codes, this means the weight $wt(v\Gamma)$ is high for all nonzero $v \in GF(q)^k$.

A linear code is called *optimal* if the minimum distance is at the upper bound, so no better linear code for (n, k, q) is possible, and the upper bound could be met.

Minimum Distance Matrix

We build a matrix M whose columns are labeled by the possible columns γ of the generator matrix. Rows are labeled by the nonzero $v \in GF(q)^k$ which produce after the multiplication with the generator matrix the codewords of the code.

UNIVERSITÄT BAYREUTH

Minimum Distance Matrix

$$M = \boxed{}$$

Minimum Distance Matrix

$$\begin{array}{ccc} & \gamma & \\ & \downarrow & \\ M = & \boxed{M_{v,\gamma}} & \leftarrow v \end{array}$$

Minimum Distance Matrix

$$\begin{array}{ccc} & \gamma & \\ & \downarrow & \\ M = & \boxed{\quad M_{v,\gamma} \quad} & \leftarrow v \end{array}$$

$$M_{v,\gamma} = \begin{cases} 1 & v\gamma = 0 \\ 0 & v\gamma \neq 0 \end{cases}$$

Diophantine System of Equations

We interested in an integral (or $0/1$) solution $x = (x_1, \ldots, x_{q^k-1})$ of the system

$$\begin{array}{llll} (1) & Mx & \leq & \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix} \\ (2) & \sum x_i & = & n \end{array}$$

Diophantine System of Equations

We interested in an integral (or $0/1$) solution $x = (x_1, \ldots, x_{q^k-1})$ of the system

$$
\begin{array}{llll}
(1) & Mx & \leq & \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix} \\
(2) & \sum x_i & = & n
\end{array}
$$

A solution corresponds via selection of columns of the generator matrix to an (n, k, q) code with minimum distance $\geq d$.

Projective Geometry

As we are computing scalar products, the 0/nonzero property is invariant under scalar multiplication, so we can label rows and columns by $1-$dimensional subspaces of $GF(q)^k$.

Projective Geometry

As we are computing scalar products, the 0/nonzero property is invariant under scalar multiplication, so we can label rows and columns by $1-$dimensional subspaces of $GF(q)^k$.

M is after this reduction the incidence matrix between the $1-$dimensional subspaces and the $(k-1)-$ dimensional subspaces of $GF(q)^k$.

Automorphisms

We now further reduce the size of the system of equations by prescribing a groups of automorphisms, this method corresponds to choosing complete orbits of subgroups of $GL(k, q)$ on the $1-$dimensional subspaces as possible columns of the generator matrix.

Automorphisms

We now further reduce the size of the system of equations by prescribing a groups of automorphisms, this method corresponds to choosing complete orbits of subgroups of $GL(k,q)$ on the $1-$dimensional subspaces as possible columns of the generator matrix.

This further reduces the number of columns, in our system of equations, as the dimension is now the number of orbits.

Reduction

The defining property of the incidence matrix

$$M_{U,V} = 1 \iff U \leq V$$

is invariant under the automorphisms.

Reduction

The defining property of the incidence matrix

$$M_{U,V} = 1 \iff U \leq V$$

is invariant under the automorphisms.

This also reduces the number of rows in the same way, the dimension is also the number of orbits.

Example

We computed a new $(103, 5, 8)$code with minimum distance 84.

UNIVERSITÄT BAYREUTH

Example

We computed a new $(103, 5, 8)$code with minimum distance 84.

$$q^k - 1$$

$$32767$$

UNIVERSITÄT BAYREUTH

Example

We computed a new $(103, 5, 8)$code with minimum distance 84.

$$q^k - 1 \qquad\qquad \frac{q^k-1}{q-1}$$

$$32767 \quad \rightarrow \quad 4681$$

Example

We computed a new $(103,5,8)$code with minimum distance 84.

$$q^k-1 \qquad \frac{q^k-1}{q-1} \qquad \begin{pmatrix} 7 & & & & \\ & & 7 & & \\ & 7 & & & \\ & & & & 7 \\ & & & 7 & \end{pmatrix}\begin{pmatrix} 4 & & & & \\ & 5 & & & \\ & & 6 & & \\ & & & 5 & \\ & & & & 4 \end{pmatrix}$$

$$32767 \quad \rightarrow \quad 4681 \quad \rightarrow$$

Example

We computed a new $(103, 5, 8)$code with minimum distance 84.

$$q^k - 1 \qquad \frac{q^k-1}{q-1} \qquad \begin{pmatrix} 7 & & & & \\ & & 7 & & \\ & 7 & & & \\ & & & & 7 \\ & & & 7 & \end{pmatrix}\begin{pmatrix} 4 & & & & \\ & 5 & & & \\ & & 6 & & \\ & & & 5 & \\ & & & & 4 \end{pmatrix}$$

$$32767 \quad \rightarrow \quad 4681 \quad \rightarrow \quad 62$$

Searching for Groups

We use random subgroups of $GL(k, q)$.

- Permutation groups
- Blockdiagonal
- Monomial
- random cyclic generator

Searching for Groups

We use random subgroups of $GL(k, q)$.

- Permutation groups
- Blockdiagonal
- Monomial
- random cyclic generator

Limits on orbit sizes, number of orbits, ...

Results

Using this method we computed over 400 new codes for $q \in \{2, 3, 4, 5, 7, 8, 9\}$, i.e. codes better than the previous lower bound.

Results

Using this method we computed over 400 new codes for $q \in \{2,3,4,5,7,8,9\}$, i.e. codes better than the previous lower bound.

Among these there are more than 50 optimal codes.

Results

Ternary Codes (q=3)

k	n	d		k	n	d		k	n	d
6	191	**126**		7	46	26		8	64	37
	201	131			59	34			65	37
	202	132			60	**36**			200	126
	217	142			61	36			205	128
	219	**144**			222	144			224	141
					243	156			225	141
									226	142
									227	143
									228	144

Last update on March, 22 2005

Results

Code details

best found code with parameters
q=3 k=7 n=60
minimum distance = 36

this is new optimal code

the previous bounds were 34/36
this is a projective code

We used the prescribed group of **automorphisms** with the following generators

0	0	2	0	0	0	0
2	0	0	0	0	0	0
0	2	0	0	0	0	0
0	0	0	0	0	2	0
0	0	0	2	0	0	0
0	0	0	0	2	0	0
0	0	0	0	0	0	2

1	0	0	0	0	0	0
0	2	0	0	0	0	0
0	0	2	0	0	0	0
0	0	0	1	0	0	0
0	0	0	0	1	0	0
0	0	0	0	0	2	0
0	0	0	0	0	0	2

Results

This group make 67 orbits of sizes:

1	3	6	6	12	4	4	4	3	6	6	12	6	12	12	24	6	12	12	24	12	24	24	24	24	6	12	12	24	12	12	12	24	24	24

The solution of the corresponding linear system of equations was found after less than 22 seconds:

0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Results

This produces the following **generator matrix**

0	0	0	0	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
0	0	0	0	0	0	0	0	2	2	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	1	1	1	1	2	2
0	0	0	0	0	0	2	2	0	0	0	0	2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1	0	0	0	0	0	0	0	0	2	2
0	0	0	0	2	2	0	0	0	0	0	0	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	0	0
0	0	2	2	0	0	0	0	0	0	0	0	2	2	1	1	1	1	2	2	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
2	2	0	0	0	0	0	0	0	0	0	0	2	1	2	1	2	1	2	1	2	1	2	1	1	2	1	2	2	2	1	1	1	1	2	2	1	2
2	1	2	1	2	1	2	1	2	1	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2

Which is a code with the following weight distribution

$1y^{60}+742x^{36}y^{24}+444x^{39}y^{21}+564x^{42}y^{18}+400x^{45}y^{15}+24x^{48}y^{12}+12x^{51}y^{9}$

Last Page

Thank you very much for your attention.

- M. Braun, A. Kohnert, A. Wassermann: Optimal Linear Codes From Matrix Groups, submitted, 2004
- list of new codes including generator matrix and weight distribution:
  http://linearcodes.uni-bayreuth.de
- A. E. Brouwer has current bounds:
  http://www.win.tue.nl/~aeb/voorlincod.html