Construction of Two-Weight Codes

Axel Kohnert

Tokyo November 2005

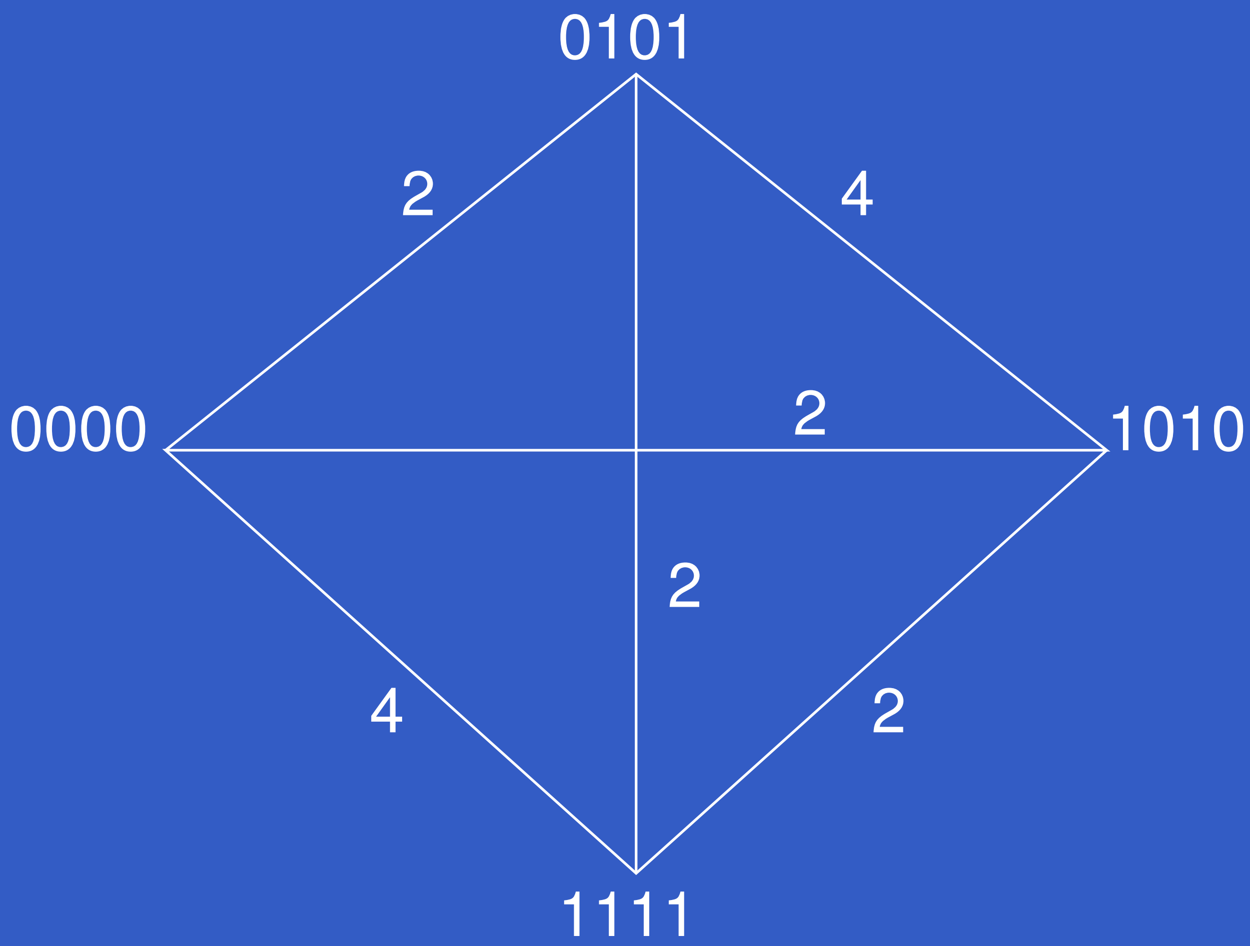
Bayreuth University Germany

axel.kohnert@uni-bayreuth.de

linearcodes.uni-bayreuth.de

UNIVERSITÄT BAYREUTH

Coding Theory



Coding Theory

Hamming distance $d_H(x, y)$=number of places with different letters in two codewords x and y.

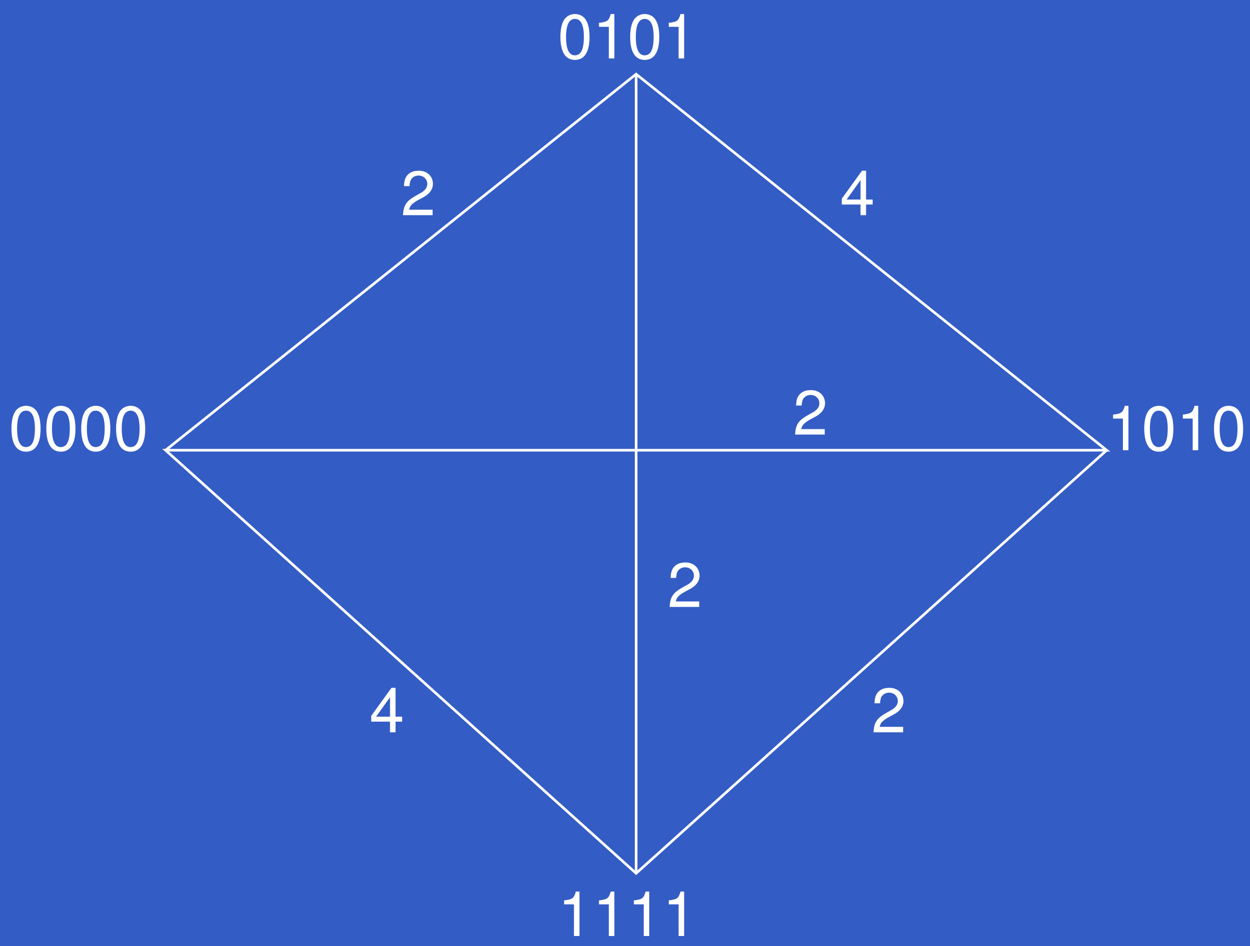
Minimum distance = minimum of $d_H(x, y)$ for all pairs of codewords.

Error correcting capability is measured by the minimum distance.

Linear Code

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

Linear Code



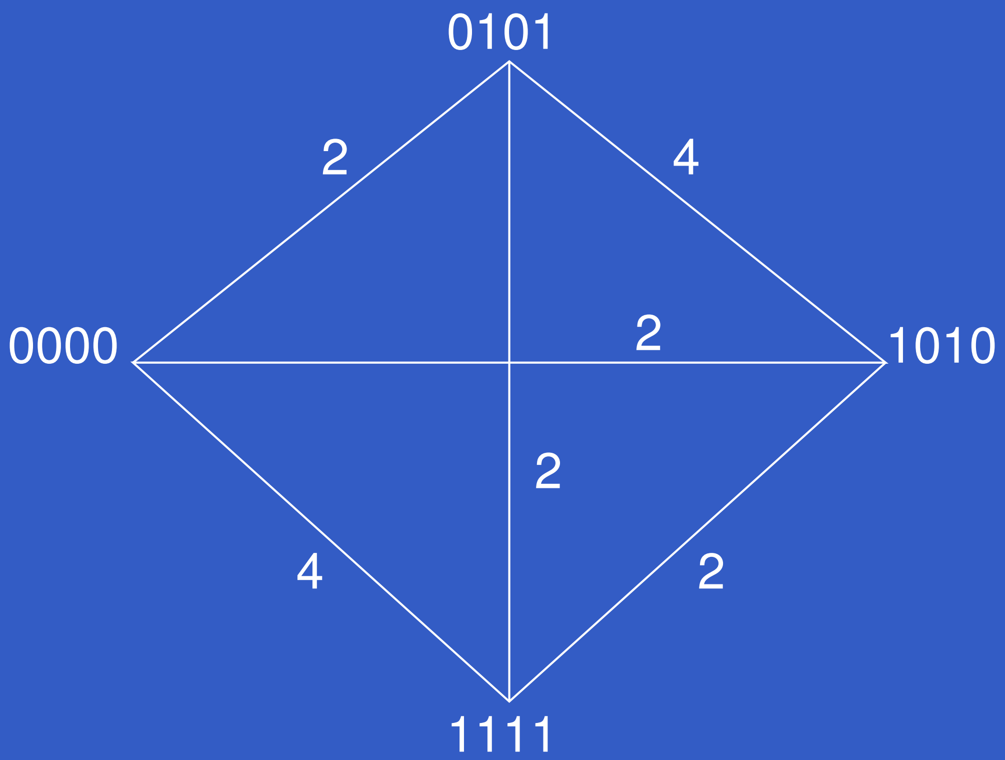
Linear Code

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

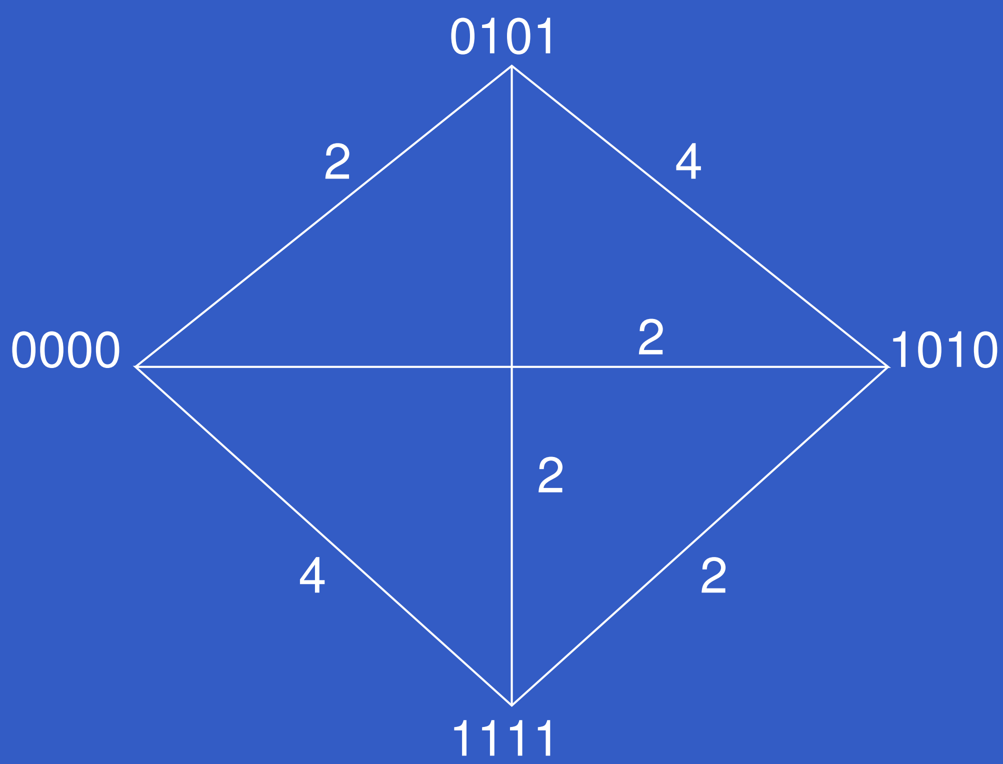
The **generator matrix** Γ of a linear $[n, k; q]$ code C is a $k \times n$ matrix where each row is a basis element of the code C.

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

Linear Code



Linear Code



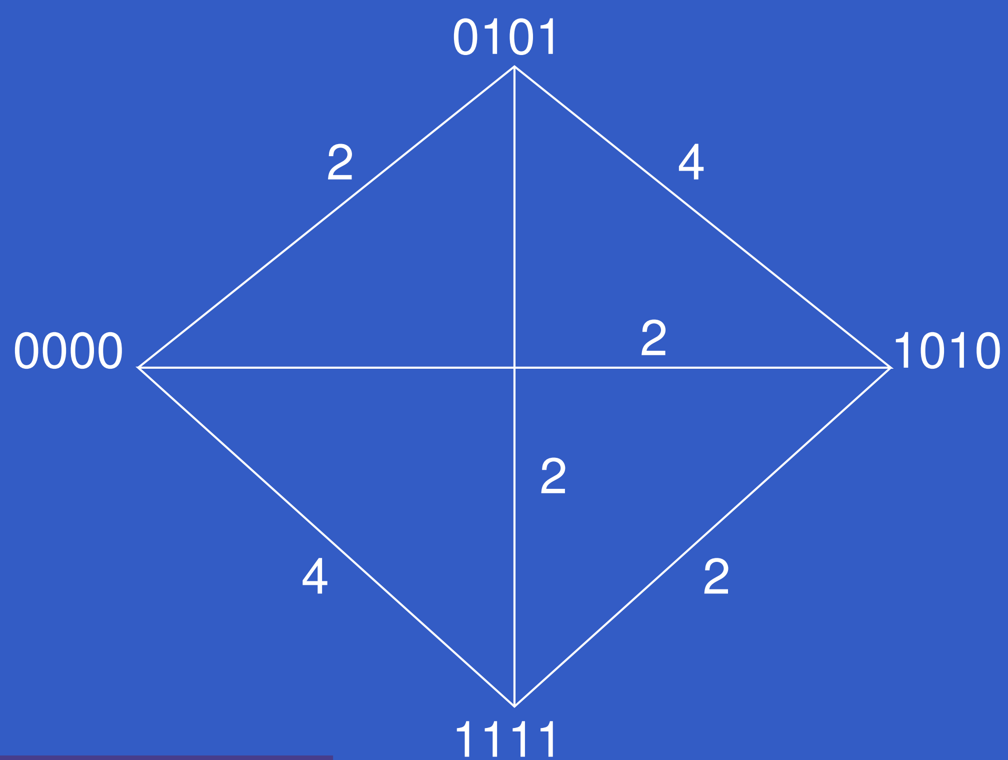
$$\Gamma = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Minimum Distance

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

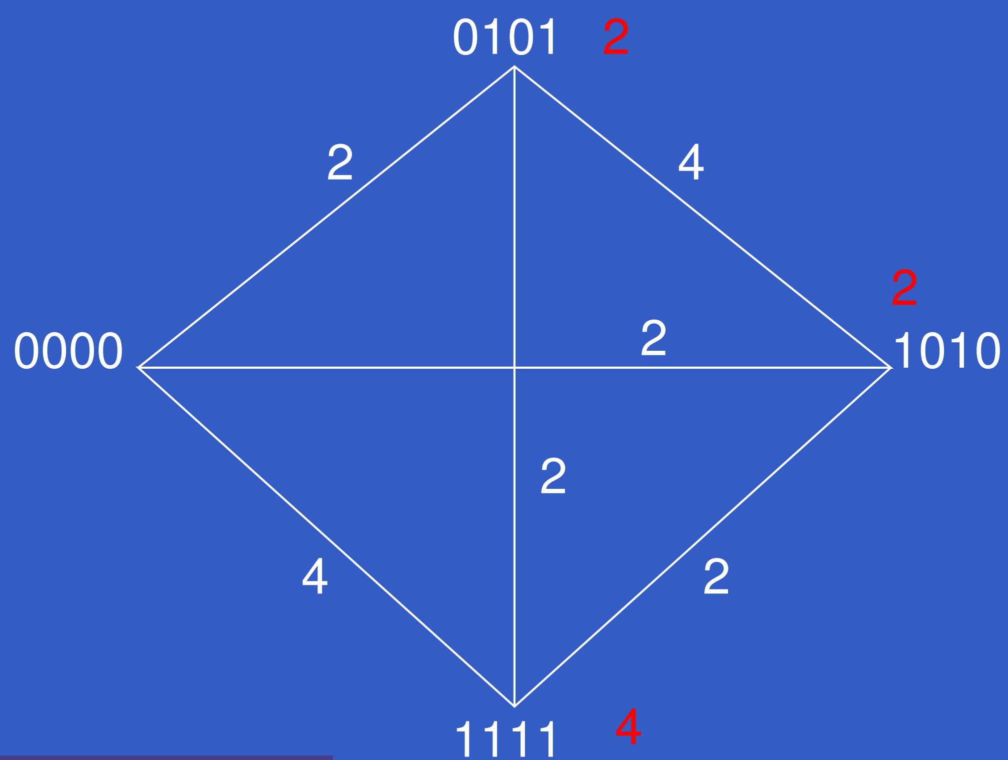
Minimum Distance

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



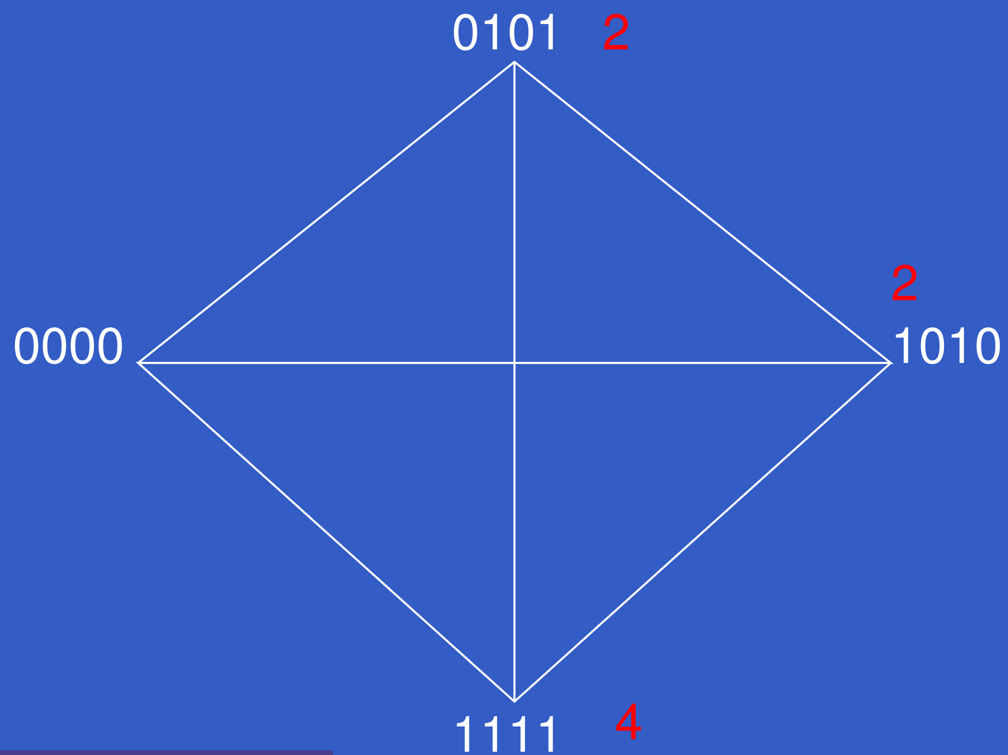
Minimum Distance

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.



UNIVERSITÄT BAYREUTH

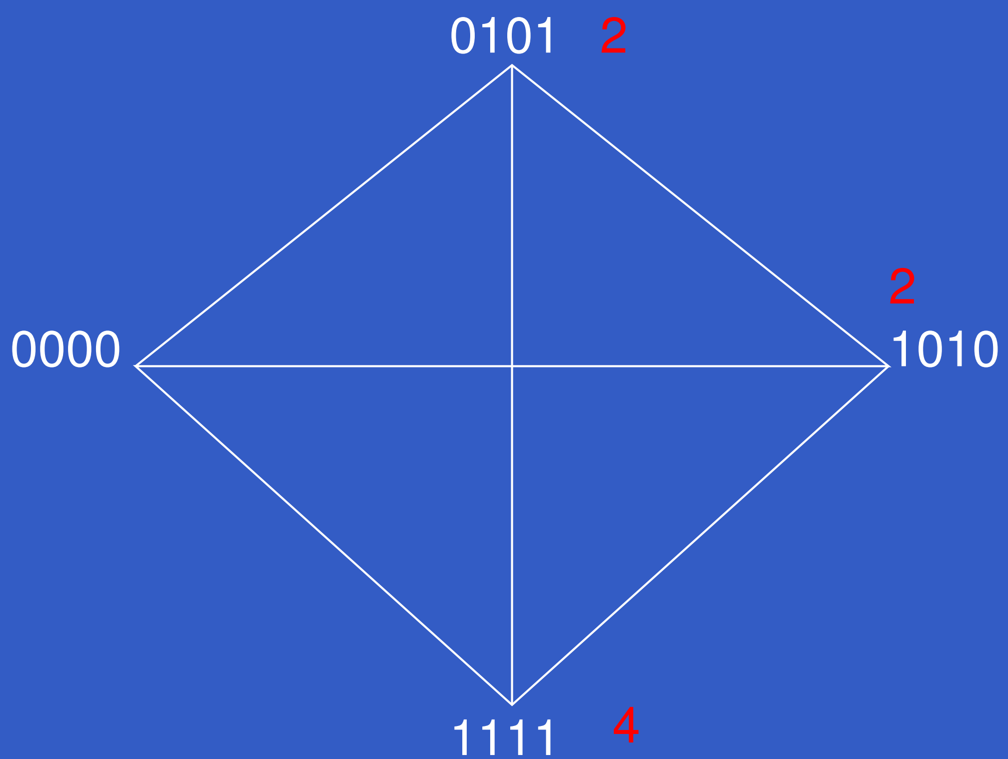
Weight Enumerator

Weight enumerator $A_C(z) := \sum A_i z^i$ where A_i is the number of codewords in C of weight i.

UNIVERSITÄT BAYREUTH

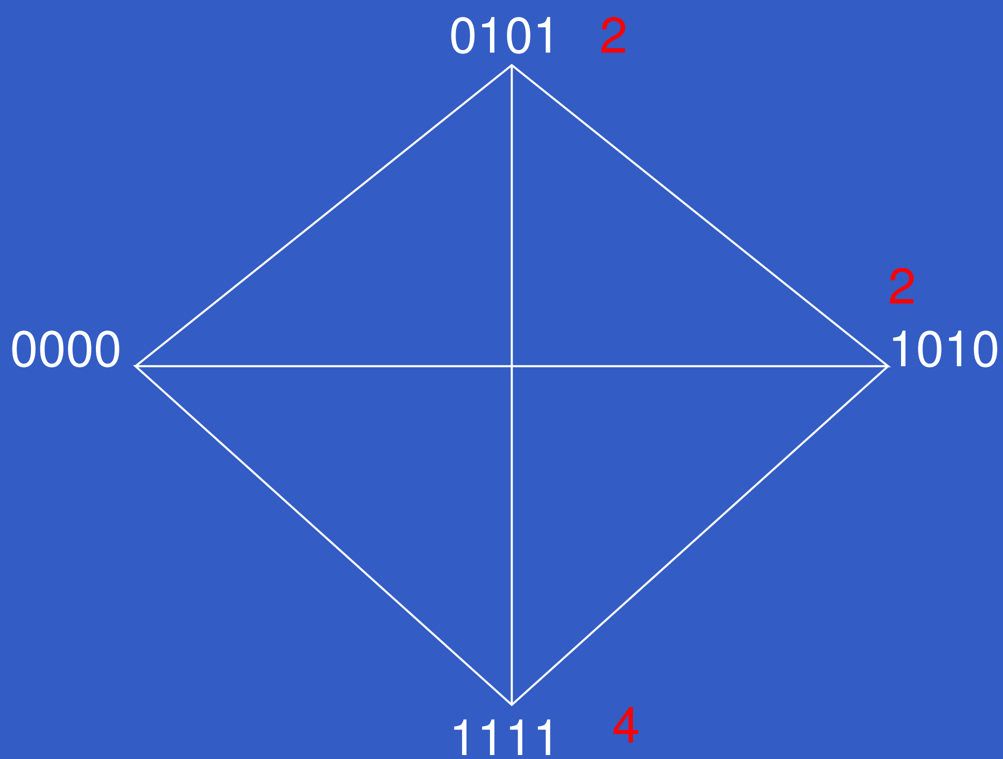
Weight Enumerator

Weight enumerator $A_C(z) := \sum A_i z^i$ where A_i is the number of codewords in C of weight i.



Weight Enumerator

Weight enumerator $A_C(z) := \sum A_i z^i$ where A_i is the number of codewords in C of weight i.



$$A_C = z^0 + 2z^2 + z^4$$

Two-Weight Code

This is a (linear) code with only two different nonzero weights w_1 and $w_2 (w_1 < w_2)$.

$$
\begin{matrix}
0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1
\end{matrix}
$$

Two-Weight Code

This is a (linear) code with only two different nonzero weights w_1 and $w_2 (w_1 < w_2)$.

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{array} \quad \Gamma = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

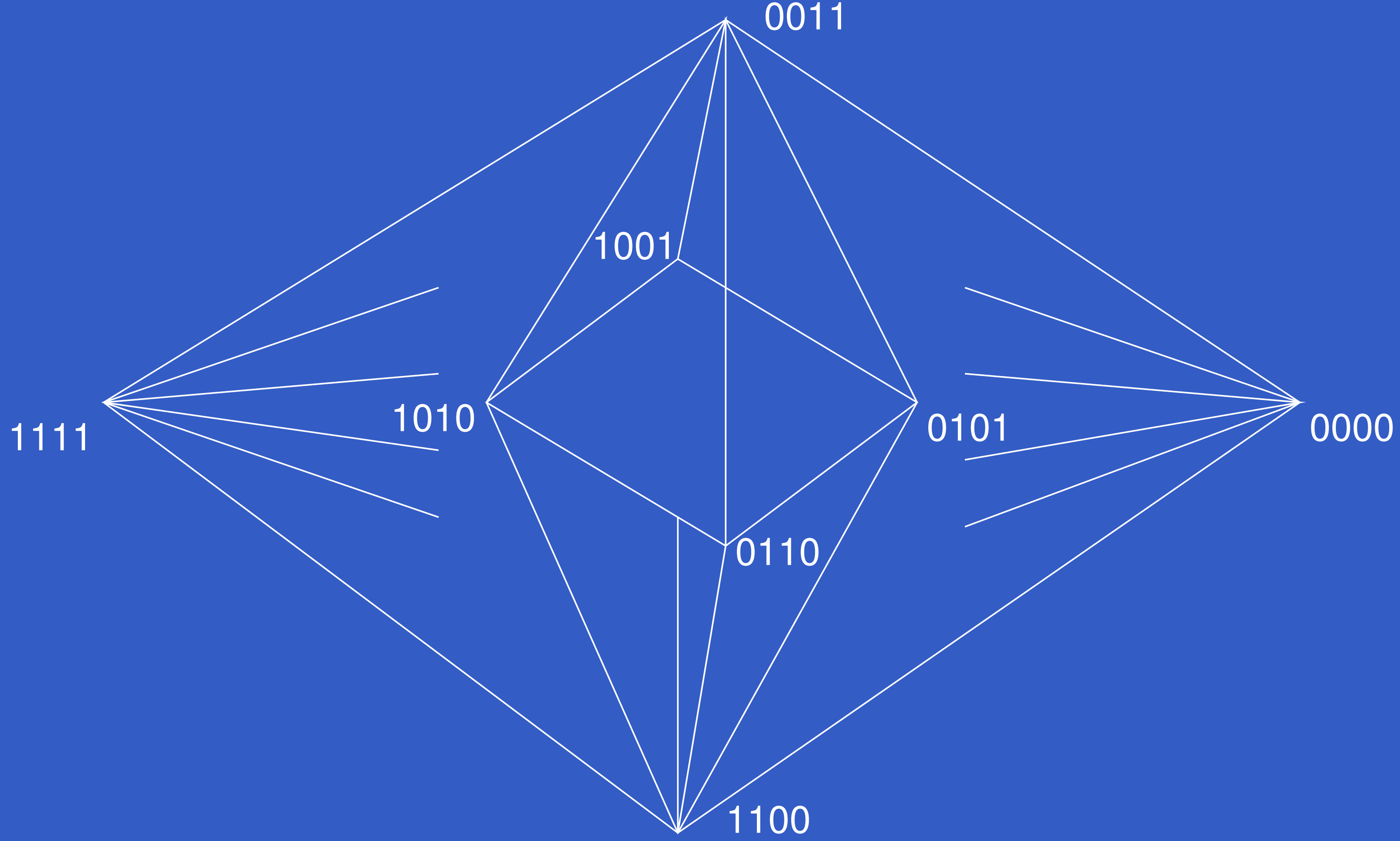
Two-Weight Code

This is a (linear) code with only two different nonzero weights w_1 and $w_2 (w_1 < w_2)$.

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix} \quad \Gamma = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} A_C = z^0 + 6z^2 + z^4$$

Two-Weight Code

Visualization of a two-weight code C by a graph G_C



Graph G_C of a Two-Weight Code

Given a code C with the two nonzero weights w_1 and w_2

Graph G_C of a Two-Weight Code

Given a code C with the two nonzero weights w_1 and w_2

vertices = codewords

UNIVERSITÄT BAYREUTH

Graph G_C of a Two-Weight Code

Given a code C with the two nonzero weights w_1 and w_2

vertices = codewords

edge between x and y if $d_H(x, y) = w_1$

Properties of G_C

G_C is a **regular** graph.

Properties of G_C

G_C is a **regular** graph.

G_C is **strongly regular** [DELSARTE], i.e. the number of common neighbors of a pair x, y of vertices depends only on the fact whether x and y are adjacent or not.

Strongly Regular Graphs

A strongly regular graph is (partially) described by four parameters (N, K, λ, μ)

N= number of vertices

K= degree

λ = number of common neighbors of adjacent vertices

μ = number of common neighbors of non-adjacent vertices

Construction

To construct a two-weight $[n, k; q]$ code we construct a corresponding generator matrix Γ.

Construction

To construct a two-weight $[n, k; q]$ code we construct a corresponding generator matrix Γ.

The codewords of a two-weight code have $n - w_1$ or $n - w_2$ zeros.

Construction

To construct a two-weight $[n, k; q]$ code we construct a corresponding generator matrix Γ.

The codewords of a two-weight code have $n - w_1$ or $n - w_2$ zeros.

We have to control the number of zeros in the codewords.

Construction

A codeword c is given by a product:

$$v\Gamma = c. \qquad\qquad (v \in GF(q)^k)$$

Construction

A codeword c is given by a product:

$$v\Gamma = c. \qquad (v \in GF(q)^k)$$

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 give after multiplication with the generator matrix the codewords of the two-weight code.

Weight Matrix

$$M = \boxed{}$$

Weight Matrix

$$\gamma \in GF(q)^k$$

$$\downarrow$$

$$M = \boxed{M_{v,\gamma}} \leftarrow v \in GF(q)^k$$

Weight Matrix

$$\gamma \in GF(q)^k$$

$$\downarrow$$

$$M = \boxed{\quad M_{v,\gamma} \quad} \leftarrow v \in GF(q)^k$$

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

Diophantine System of Equations

Now a two-weight code corresponds to a $0/1$ solution $x = (x_1, \ldots, x_{q^k-1})$ of the system

$$
\begin{array}{lccc}
(1) & Mx & = & \begin{pmatrix} n - w_1 \text{ or } n - w_2 \\ \vdots \\ n - w_1 \text{ or } n - w_2 \end{pmatrix} \\
 & & & \\
(2) & \sum x_i & = & n
\end{array}
$$

UNIVERSITÄT BAYREUTH

Diophantine System of Equations

$$\left[\begin{array}{c|ccccc} & w_1 - w_2 & 0 & \dots & 0 & 0 \\ & 0 & \ddots & 0 & & 0 \\ M & \vdots & 0 & w_1 - w_2 & 0 & \vdots \\ & 0 & & 0 & \ddots & 0 \\ & 0 & 0 & \dots & 0 & w_1 - w_2 \\ \hline 1 \dots 1 & 0 & \dots & 0 & \dots & 0 \end{array}\right] x = \left[\begin{array}{c} n - w_1 \\ \vdots \\ \\ \vdots \\ n - w_1 \\ \hline n \end{array}\right]$$

Diophantine System of Equations

$$
\left[\begin{array}{c|ccccc}
 & w_1 - w_2 & 0 & \dots & 0 & 0 \\
 & 0 & \ddots & 0 & & 0 \\
M & \vdots & 0 & w_1 - w_2 & 0 & \vdots \\
 & 0 & & 0 & \ddots & 0 \\
 & 0 & 0 & \dots & 0 & w_1 - w_2 \\
\hline
1 \dots 1 & 0 & \dots & 0 & \dots & 0
\end{array}\right] x = \left[\begin{array}{c}
n - w_1 \\
\vdots \\
\\
\vdots \\
n - w_1 \\
\hline
n
\end{array}\right]
$$

To solve this system we use an LLL-variant of A. Wassermann.

Diophantine System of Equations

We are interested in a $0/1$ solution $x = (x_1, \ldots, x_{q^k-1}, \ldots, x_{2(q^k-1)})$ of the system.

Diophantine System of Equations

We are interested in a $0/1$ solution $x = (x_1, \ldots, x_{q^k-1}, \ldots, x_{2(q^k-1)})$ of the system.

The first half $x = (x_1, \ldots, x_{q^k-1})$ of a solution corresponds via selection of columns of the generator matrix to an $[n, k; q]$ two-weight code with weights w_1 and w_2.

UNIVERSITÄT BAYREUTH

Diophantine System of Equations

We are interested in a $0/1$ solution $x = (x_1, \ldots, x_{q^k-1}, \ldots, x_{2(q^k-1)})$ of the system.

The first half $x = (x_1, \ldots, x_{q^k-1})$ of a solution corresponds via selection of columns of the generator matrix to an $[n, k; q]$ two-weight code with weights w_1 and w_2.

The second half $x = (x_{q^k}, \ldots, x_{2(q^k-1)})$ contains the information on the weight enumerator.

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 $GF(q)^k$.

UNIVERSITÄT BAYREUTH

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 $GF(q)^k$.

UNIVERSITÄT BAYREUTH

3 Different Languages

We can study the same object in 3 different settings:

- Two-Weight Codes
- Strongly Regular Graphs
- Point-Sets in the Projective Geometry

Automorphisms

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

Automorphisms

We further reduce the size of the system by prescribing a group of automorphisms, this method corresponds to choosing complete orbits of subgroups of $PGL(k, q)$ 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 height is also the number of orbits.

UNIVERSITÄT BAYREUTH

Example

We computed a new $[738, 8; 3]$ two-weight code with nonzero weights 486 and 513.

Example

We computed a new $[738, 8; 3]$ two-weight code with nonzero weights 486 and 513.

$$q^k - 1$$

$$6560$$

UNIVERSITÄT BAYREUTH

Example

We computed a new $[738, 8; 3]$ two-weight code with nonzero weights 486 and 513.

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

$$6560 \quad \longrightarrow \quad 3280$$

Example

We computed a new $[738, 8; 3]$ two-weight code with nonzero weights 486 and 513.

$$q^k - 1 \qquad \frac{q^k-1}{q-1} \qquad \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 \\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 & 0 & 2 & 2 & 0 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \end{pmatrix}$$

$$6560 \quad \longrightarrow \quad 3280 \quad \longrightarrow$$

Example

We computed a new $[738, 8; 3]$ two-weight code with nonzero weights 486 and 513.

$$q^k - 1 \qquad \frac{q^k-1}{q-1} \qquad \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 \\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 & 0 & 2 & 2 & 0 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \end{pmatrix}$$

$6560 \quad \longrightarrow \quad 3280 \quad \longrightarrow \quad 40$ orbits

Searching for Groups

We use different subgroups of $PGL(k, q)$.

- random cyclic generator (like above example)
- Permutation groups
- Blockdiagonal
- Monomial

Searching for Groups

We use different subgroups of $PGL(k, q)$.

- random cyclic generator (like above example)
- Permutation groups
- Blockdiagonal
- Monomial

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

Results

Using this method we computed several new two-weight codes.

Results

Using this method we computed several new two-weight codes.

Among these there are also distance-optimal codes.

Results

Some new two-weight codes

two-weight code					strongly regular graph			
n	k	q	w_1	w_2	N	K	λ	μ
140	6	3	90	99	729	280	103	110
198*	10	2	96	112	1024	198	22	42
...								

UNIVERSITÄT BAYREUTH

Last Page

Thank you very much for your attention.

- A. Kohnert: Construction of Two-Weight Codes, in preparation
- M. Braun, A. Kohnert, A. Wassermann: Optimal Linear Codes From Matrix Groups, IEEE Information Theory, 2005

Last Page

Thank you very much for your attention.

- list of new codes including generator matrix and weight enumerator:
  http://linearcodes.uni-bayreuth.de
- A. E. Brouwer has a list (not online) of known parameters:
  http://www.win.tue.nl/~aeb/