

# Construction of Two-Weight Codes

Axel Kohnert

Tokyo November 2005

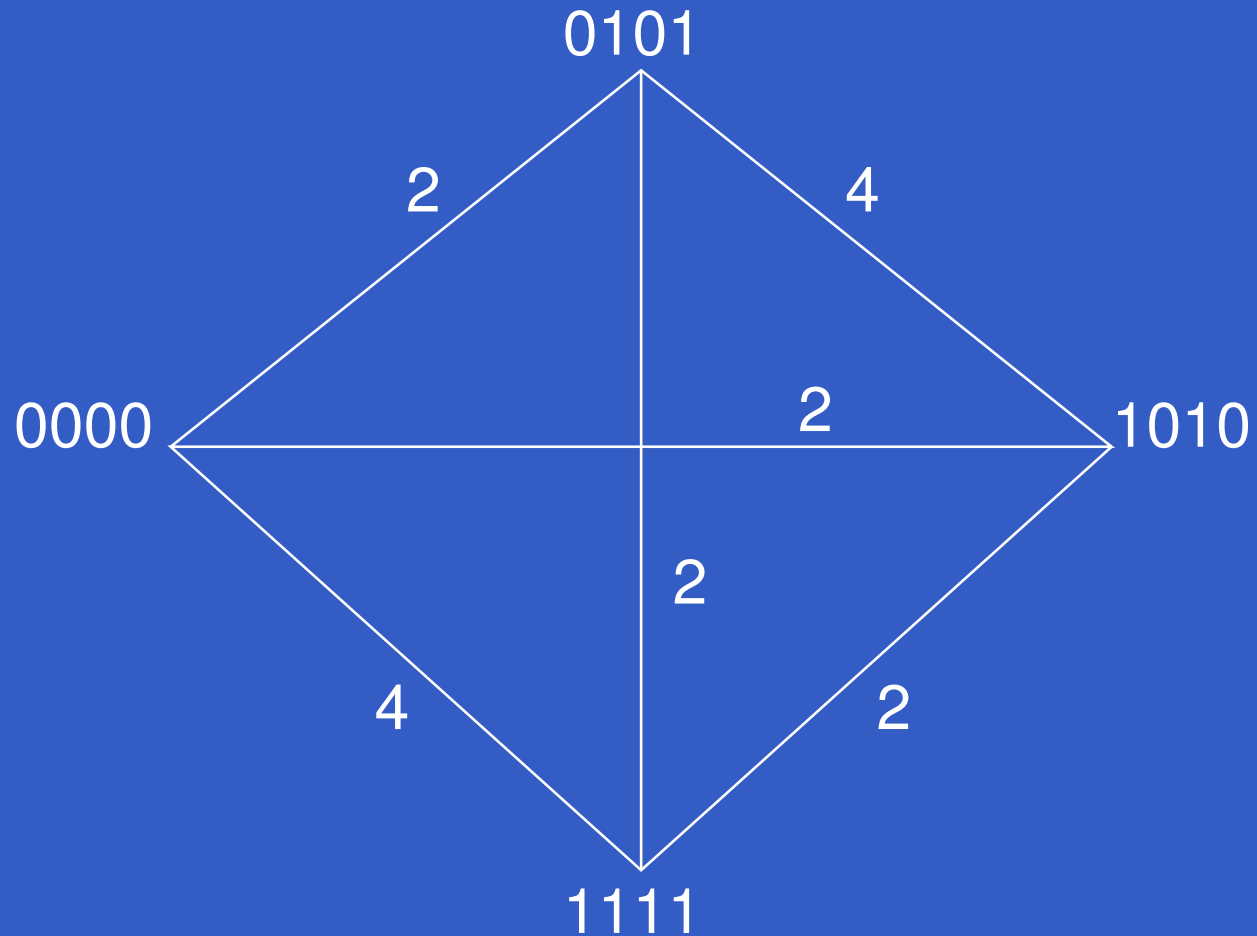
Bayreuth University Germany

[axel.kohnert@uni-bayreuth.de](mailto:axel.kohnert@uni-bayreuth.de)

[linearcodes.uni-bayreuth.de](http://linearcodes.uni-bayreuth.de)



# Coding Theory



# Coding Theory

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

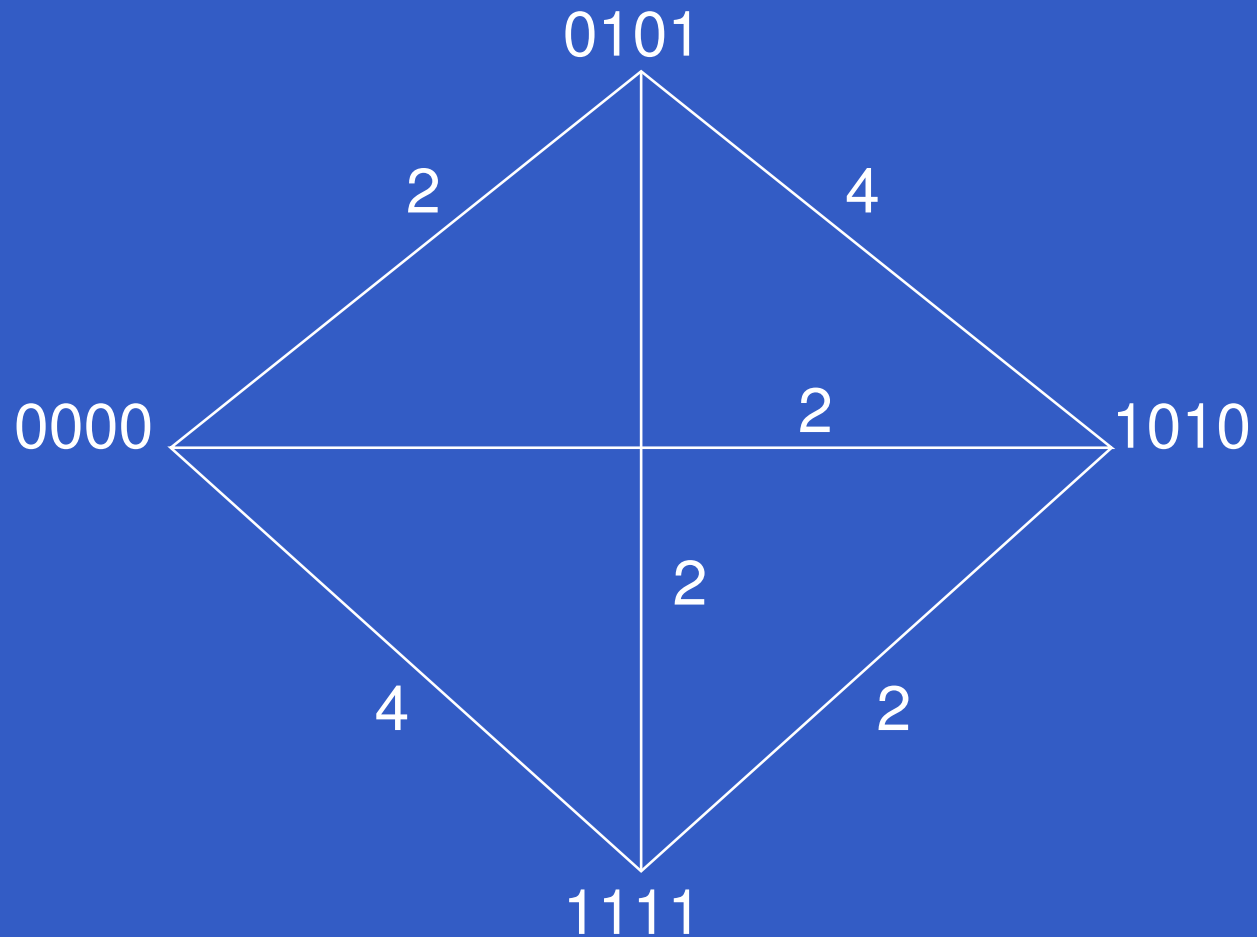
**Minimum distance** = minimum of  $d_H(x, y)$  for all pairs of codewords.

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



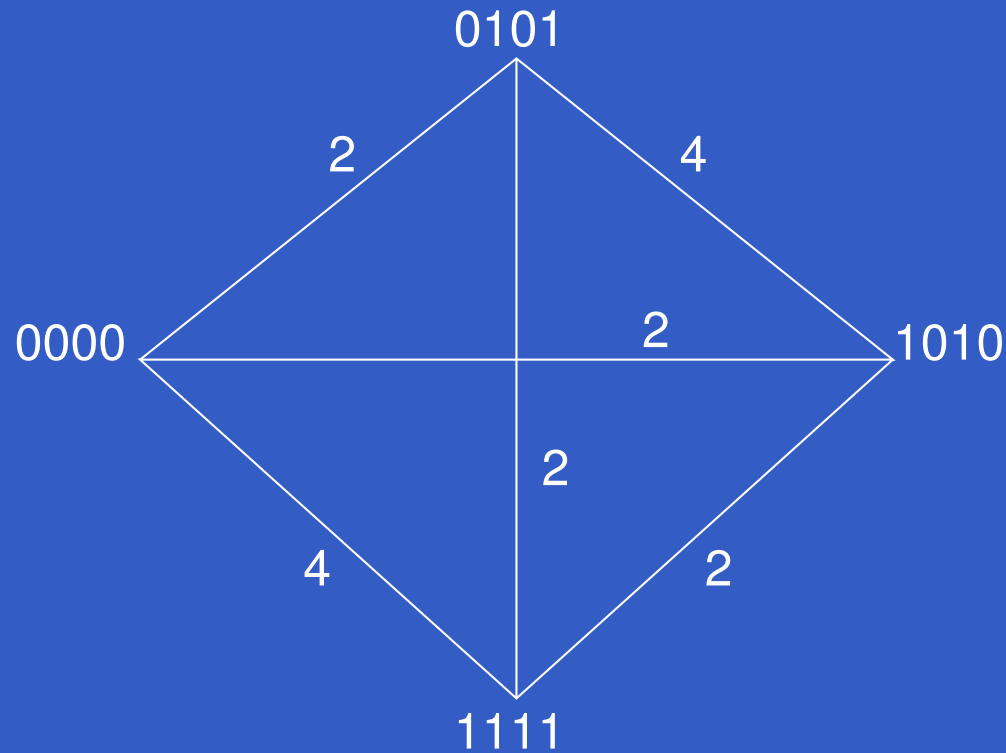
# Linear Code

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

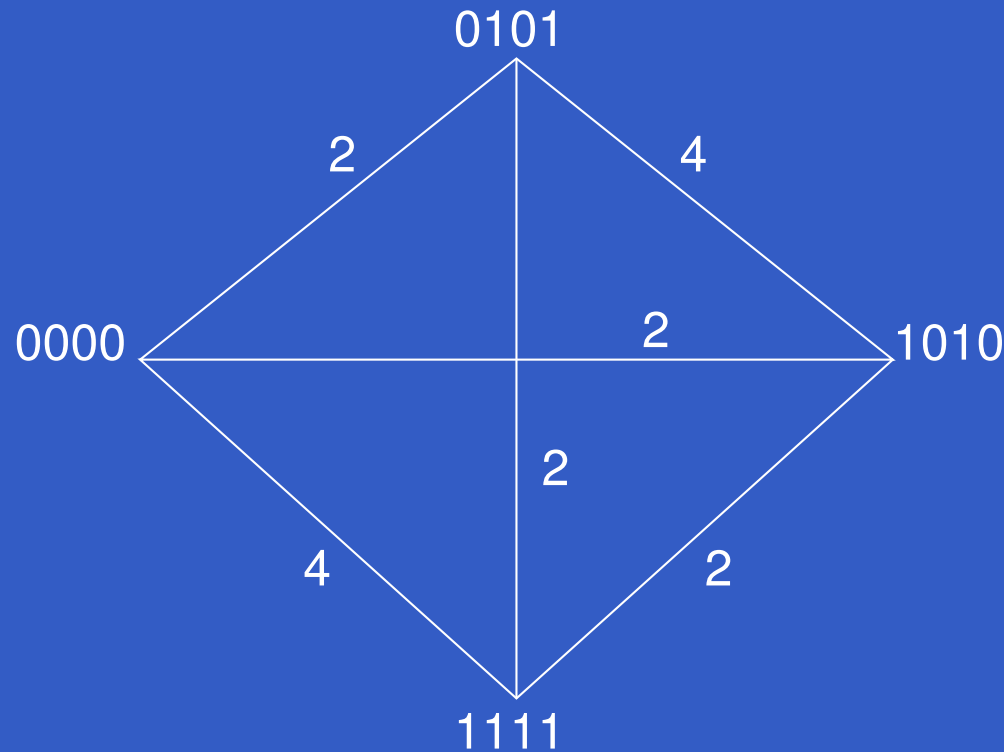
The **generator matrix**  $\Gamma$  of a linear  $[n, k; q]$  code  $C$  is a  $k \times n$  matrix where each row is a basis element of the code  $C$ .

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

# Linear Code



# Linear Code



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

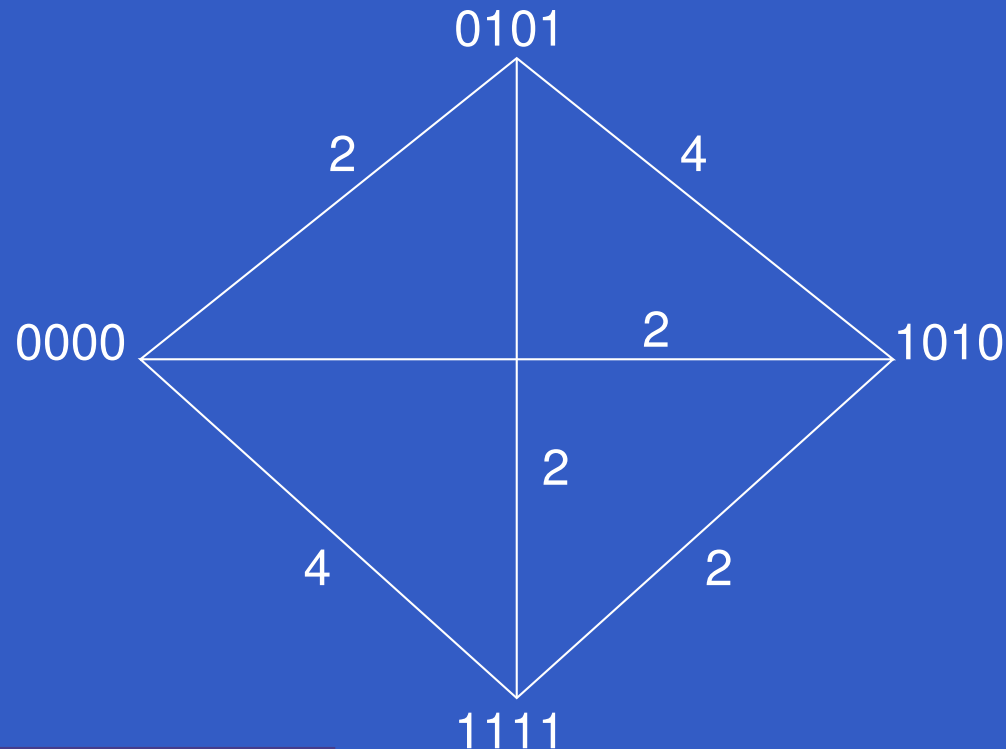


# Minimum Distance

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

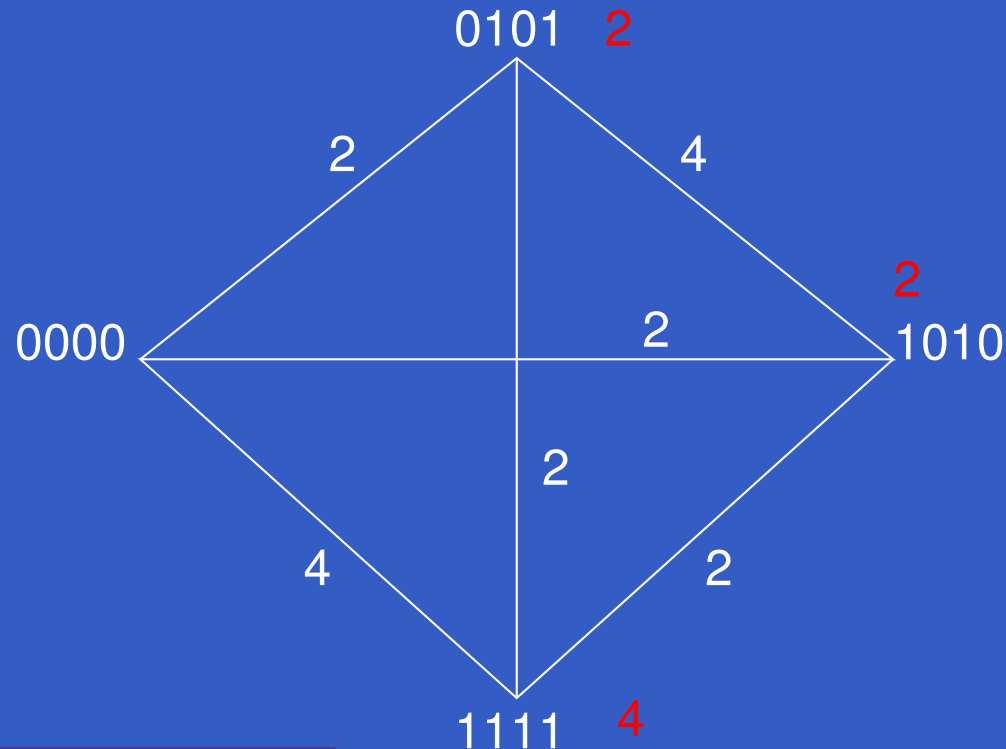
# Minimum Distance

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



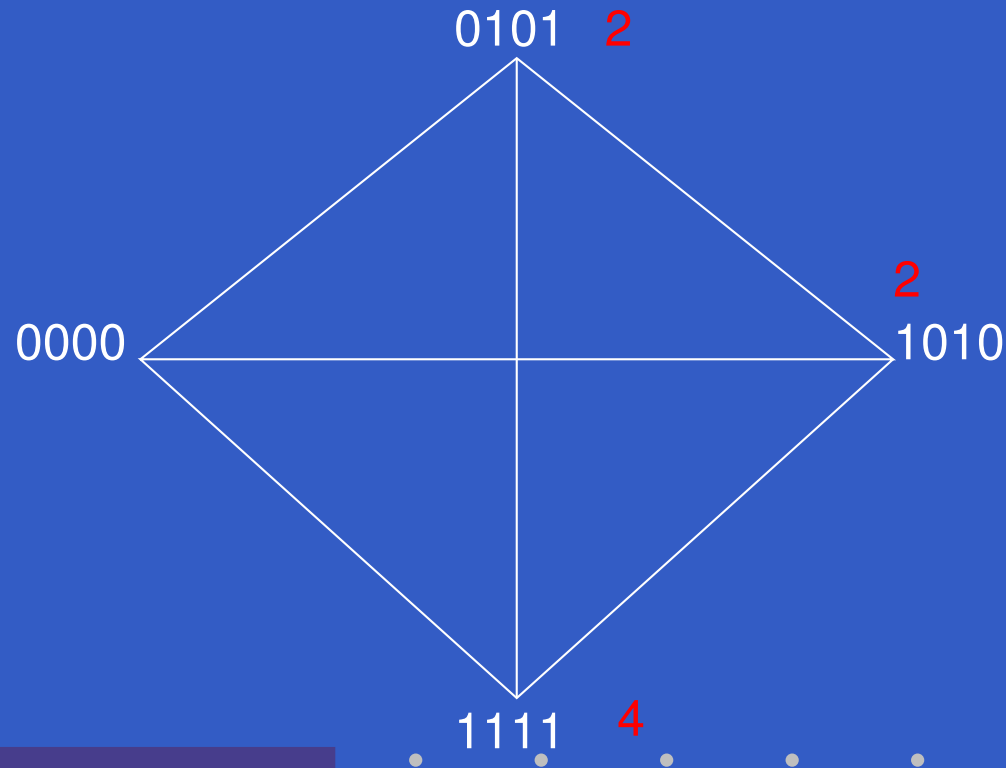
# Minimum Distance

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.

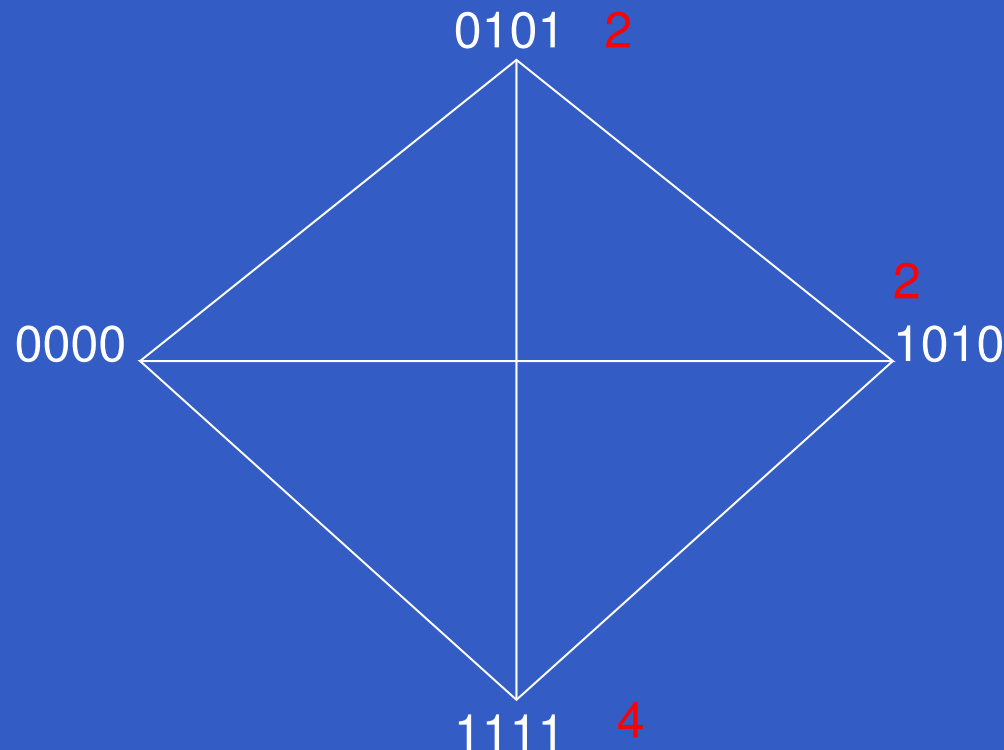


# Weight Enumerator

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

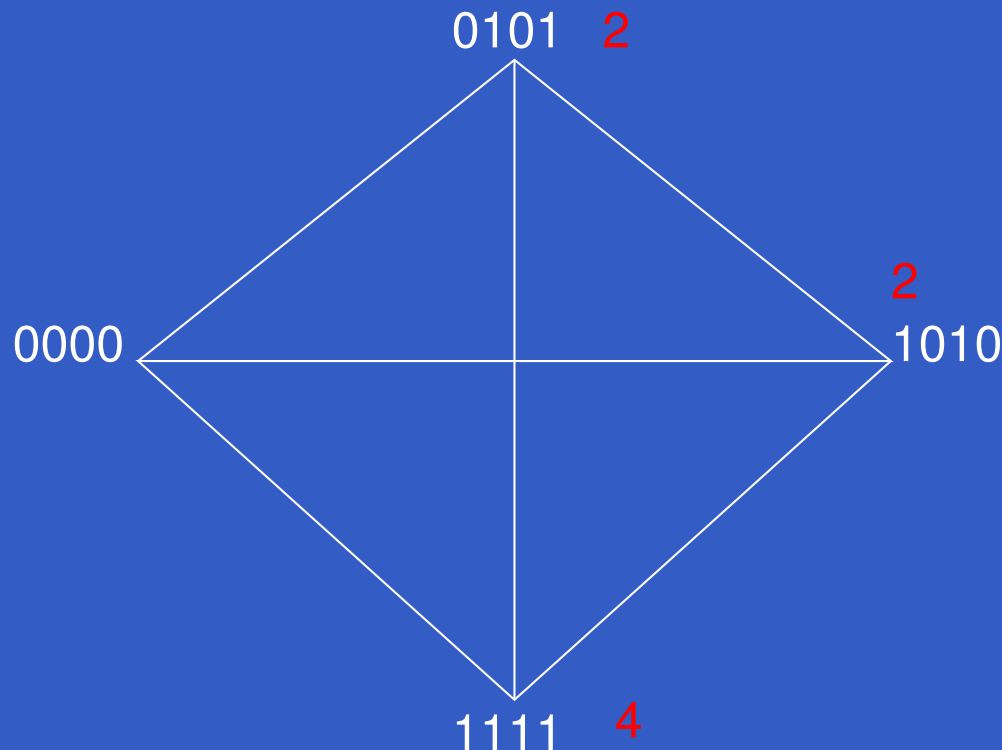
# Weight Enumerator

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



# 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  $w_2$  ( $w_1 < w_2$ ).

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



# Two-Weight Code

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

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

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

# Two-Weight Code

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

0 0 0 0

1 1 0 0

1 0 1 0

1 0 0 1

0 1 1 0

0 1 0 1

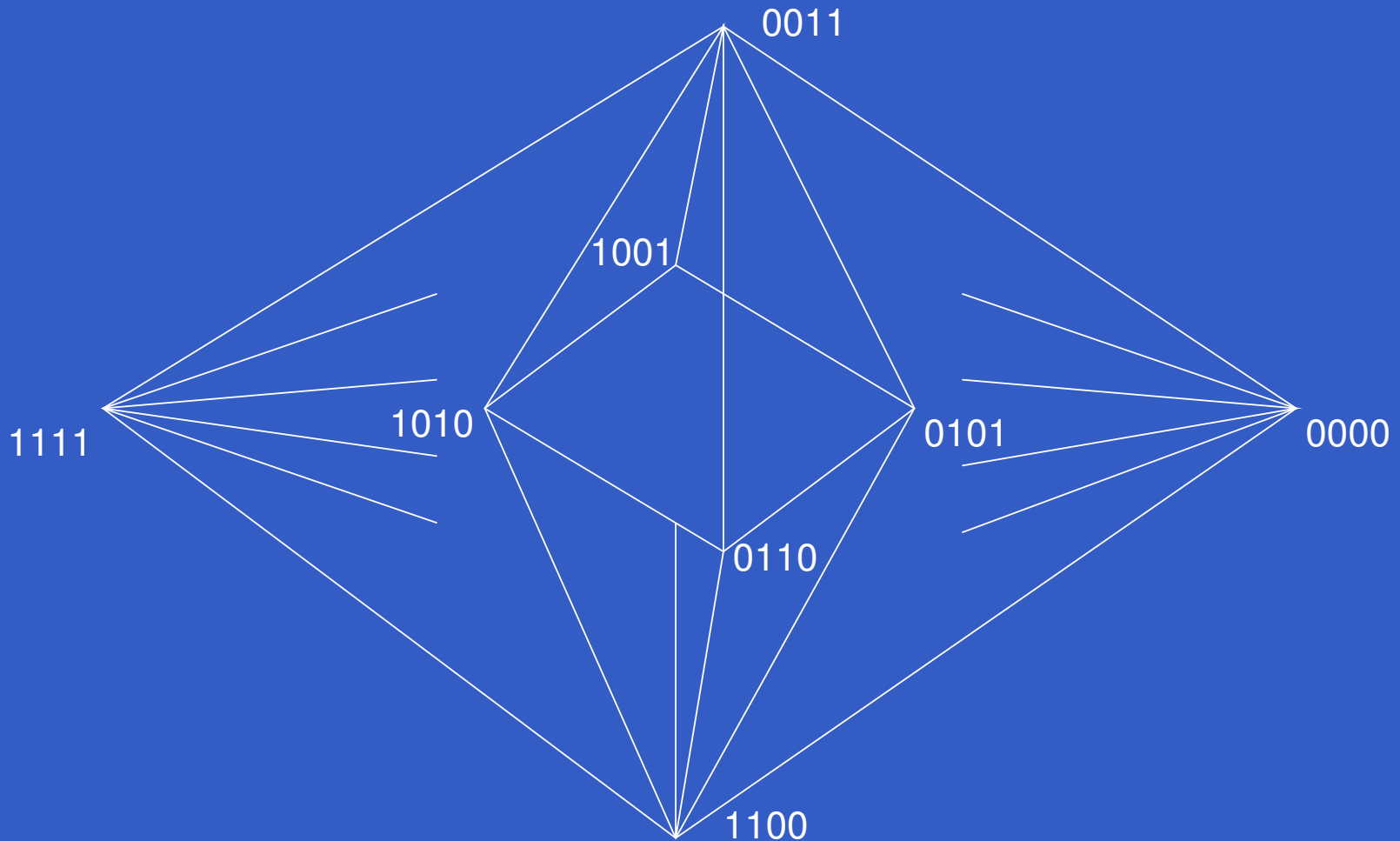
0 0 1 1

1 1 1 1

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

# 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

# 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  $(N, K, \lambda, \mu)$

$N =$  number of vertices

$K =$  degree

$\lambda =$  number of common neighbors of adjacent vertices

$\mu =$  number of common neighbors of non-adjacent vertices



# Construction

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

# Construction

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

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  $\Gamma$ .

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:

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

# Construction

A codeword  $c$  is given by a product:

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

We build a matrix  $M$  whose columns are labeled by the possible columns  $\gamma$  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

$M =$



# Weight Matrix

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



$$M =$$

$$M_{v, \gamma}$$

$$\leftarrow v \in GF(q)^k$$



# Weight Matrix

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



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

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

# Diophantine System of Equations

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

$$(1) \quad Mx = \begin{pmatrix} n - w_1 \text{ or } n - w_2 \\ \vdots \\ n - w_1 \text{ or } n - w_2 \end{pmatrix}$$

$$(2) \quad \sum x_i = n$$

# Diophantine System of Equations

$M$	$w_1 - w_2$	0	...	0	0	$x =$	$n - w_1$
	0	...	0	0	0		⋮
	⋮	0	$w_1 - w_2$	0	⋮		⋮
	0	0	0	...	0		$n - w_1$
	0	0	...	0	$w_1 - w_2$		$n - w_1$
$1 \dots 1$	0	...	1	0	...	0	$n$

# Diophantine System of Equations

$$\begin{array}{c|cccccc}
 & w_1 - w_2 & 0 & \dots & 0 & 0 \\
 \hline
 M & 0 & \ddots & 0 & 0 & 0 \\
 & \vdots & 0 & w_1 - w_2 & 0 & \vdots \\
 & 0 & 0 & 0 & \ddots & 0 \\
 & 0 & 0 & \dots & 0 & w_1 - w_2 \\
 \hline
 1 \dots 1 & 0 & \dots & 1 & 0 & \dots & 0
 \end{array}
 \quad x = \begin{array}{c}
 n - w_1 \\
 \vdots \\
 \vdots \\
 n - w_1 \\
 \hline
 n
 \end{array}$$

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

# Diophantine System of Equations

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

# Diophantine System of Equations

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

The first half  $x = (x_1, \dots, x_{q^k-1})$  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  $w_2$ .

# Diophantine System of Equations

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

The first half  $x = (x_1, \dots, x_{q^k-1})$  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  $x = (x_{q^k}, \dots, x_{2(q^k-1)})$  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  $GF(q)^k$ .



# 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  $GF(q)^k$ .



# 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.

# 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





# Example

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

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

$$6560 \rightarrow 3280$$

# Example

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

$$q^k - 1$$

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

$$6560 \rightarrow 3280 \rightarrow$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 \\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 & 0 & 2 & 2 & 0 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \end{pmatrix}$$

# Example

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

$$q^k - 1$$

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

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 \\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 & 0 & 2 & 2 & 0 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 \end{pmatrix}$$

$$6560 \rightarrow 3280 \rightarrow 40 \text{ orbits}$$

# 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			
$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$
140	6	3	90	99	729	280	103	110
198*	10	2	96	112	1024	198	22	42
...								



# 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/>