Two-Weight Codes with prescribed Symmetries

AXEL KOHNERT
Mathematisches Institut, Universität Bayreuth
D–95440 Bayreuth, Germany
(axel.kohnert@uni–bayreuth.de)

1. Linear Codes

Linear $[n, k, q]$ codes are k–dimensional subspaces C of the n–dimensional vectorspace $GF(q)^n$. They are described by a generator matrix, i.e. a matrix whose rows are a basis of C.

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

is a generator matrix of a $[4, 3, 2]$–code. The elements of the space are the codewords. In the above example these are the 8 words:

$$0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111.$$

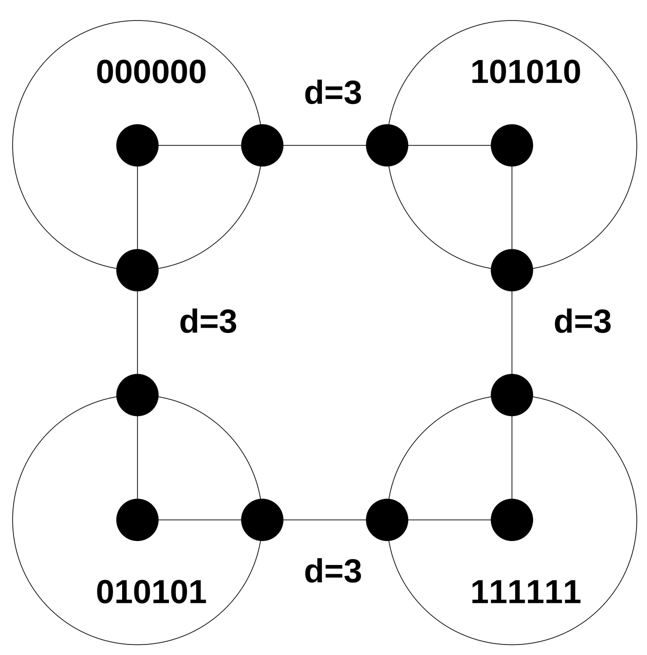
We get these codewords if we multiply

$$v\Gamma$$

for all 8 vectors $v \in GF(q)^k$. Codes are used for the correction of errors during the transmission over a noisy channel, the number of entries where two codewords differ is called the Hamming distance between these two codewords. This is the number of errors which must be made during the transmission to change one codeword into the other. The minimum distance d of a code is the minimum of distance between all pairs of codewords. A code with minimum distance d allows the correction of $\lfloor d/2 \rfloor$ errors.

Example

The following 4-word code allows the correction of 1 error.

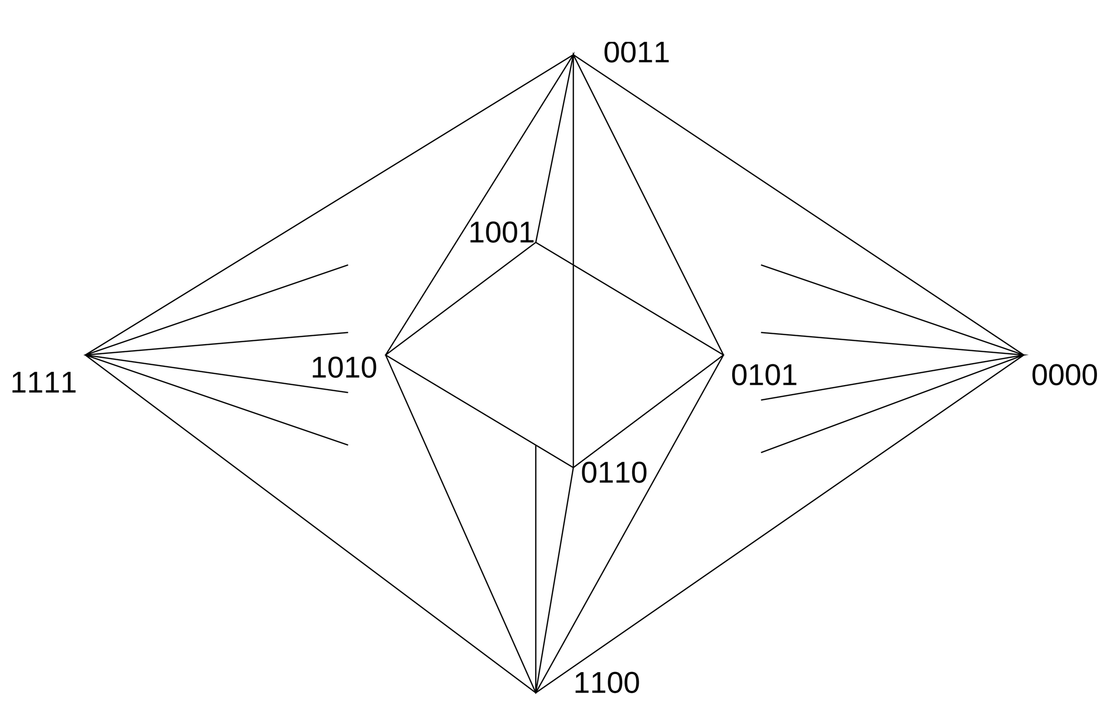


In the case of a linear code we know, that the difference (in the vector space) is again a codeword, therefore the Hamming distance is the number of nonzero entries in the difference codeword. The number of nozero entries is called the *weight* of the codeword. For a linear code the minimum distance is equal to the minimum weight of the nonzero codewords. A *two-weight* code is a code where the nonzero codewords only have two different weights.

2. Strongly Regular Graphs

There is a connection between two-weight codes and graph theory given by the following graph which can be defined for any linear two-weight code with the two weights say w_1 and w_2. The vertices of the graph are the N codewords and two vertices are connected if their Hamming distance is w_1. In the above 8-word code for $w_1 = 2$ this the following graph:

Example



This graph is a so-called *strongly regular* graph which has some nice properties, it is

1. *regular*, this means every vertex has the same number K of neighbors, and
2. the number of common neighbors for any pair of vertices depends only on the question whether these two vertices are connected or not. This is described by the two parameters λ(=common neighbors of adjacent vertices) and μ (for non-adjacent vertices)

Above example has parameters $8, 6, 6, 6$. Strongly regular graphs are very interesting objects and people are searching for them as they know feasible parameters N, K, λ, μ from algebra but sometimes there is no known method for the construction of such a graph.

3. Finite Projective Geometry

The connection to the finite projective geometry is given by the generator matrix. The columns of the generator matrix are points (=one-dimensional subspaces of $GF(q)^k$) in $PG(k-1, q)$. As long as we have different points (= two columns of the generator matrix are linearily independent) we can take the generator matrix as a set of points. Such codes are called *projective* because of this correspondence. The interseting point is that the weight and therefore also the minimum distance can be formulated in the context of the geometry setting.

$$c = v\Gamma \text{ is a codeword of weight } d$$
$$\Longleftrightarrow$$
$$\text{the hyperplane orthogonal to } v \text{ contains } n-d \text{ of the the points given by } \Gamma$$

Because of this property the construction of a linear code with given weights can be seen as the selection of points in $PG(k-1, q)$ with certain intersection properties. For this construction we define the incidence matrix M between points and hyperplanes in $PG(k-1, q)$. This square matrix has rows labeled by the hyperplanes and columns labeled by points.

$$M_{i,j} := \begin{cases} 1 & \text{hyperplane } i \text{ contains the point } j \\ 0 & \text{otherwise} \end{cases}$$

Using this matrix the construction of a two-weight code with weights w_1 and w_2 corresponds to a selection of columns, such that the row sum is $n - w_1$ or $n - w_2$. The corresponding system of points in $PG(k-1, q)$ is called an $(n, k, n-w_1, n-w_2)$ point set.

4. Diophantine System

We summarize the construction of a two-weight code with the following:

Theorem: There is an $(n, k, n-w_1, n-w_2)$ point set in $PG(k-1, q)$ if and only if there is a $(0/1)-$solution x of the Diophantine system of linear equations:

$$\left[\begin{array}{c|ccccc} & w_2-w_1 & 0 & \dots & 0 & 0 \\ & 0 & \ddots & 0 & & 0 \\ M & \vdots & 0 & w_2-w_1 & 0 & \vdots \\ & 0 & & 0 & \ddots & 0 \\ & 0 & 0 & \dots & 0 & w_2-w_1 \\ \hline 1\dots1 & & & 0\dots0 & & \end{array}\right] x = \left[\begin{array}{c} n-w_1 \\ \vdots \\ \\ \vdots \\ n-w_1 \\ \hline n \end{array}\right]$$

The advantage of this description is that we have an effective method at hand for the solution of such a Diophantine system of equations. It is an modified version of the LLL-algorithm made available by Alfred Wassermann. Using this we can solve systems with up to 400 columns.

5. Automorphisms

To construct codes in cases, where the size is too big, a common method is to prescribe a group G of automorphisms, i.e. elements from $GL(k, q)$ acting on the points. In this case we condense the matrix M by adding up columns which are elements of the same orbit under G.

After this first step of the reduction there are identical lines which correspond to the hyperplanes in the orbit of the automorphism on the hyperplanes. This allows the recution of rows. After there is again are square matrix, we denote by M^G. Above theorem becomes now:

Theorem: There is an $(n, k, n-w_1, n-w_2)$ point set in $PG(k-1, q)$ with a group $G < GL(k, q)$ of automorphisms if and only if there is a $(0/1)-$solution x of the Diophantine system of linear equations:

$$\left[\begin{array}{c|ccccc} & w_2-w_1 & 0 & \dots & 0 & 0 \\ & 0 & \ddots & 0 & & 0 \\ M^G & \vdots & 0 & w_2-w_1 & 0 & \vdots \\ & 0 & & 0 & \ddots & 0 \\ & 0 & 0 & \dots & 0 & w_2-w_1 \\ \hline |\omega_1|\dots|\omega_m| & & & 0\dots0 & & \end{array}\right] x = \left[\begin{array}{c} n-w_1 \\ \vdots \\ \\ \vdots \\ n-w_1 \\ \hline n \end{array}\right]$$

6. Binary Codes

We give a list of newly found binary two-weight codes together with the parameters of the corresponding strongly regular graphs.

n	k	q	w_1	w_2	N	K	λ	μ
70*	9	2	32(315)	40(196)	512	70	6	10
196*	9	2	96(441)	112(70)	512	196	60	84
198*	10	2	96(825)	112(198)	1024	198	22	42
234*	12	2	112(2808)	128(1287)	4096	234	2	14
270	12	2	128(2295)	144(2184)	4096	270	14	18
273	12	2	128(1911)	144(2184)	4096	273	20	18
455*	12	2	224(3640)	256(455)	4096	455	6	56
780	12	2	384(3315)	416(780)	4096	780	116	156
845	12	2	416(3250)	448(845)	4096	845	144	182
910	12	2	448(3185)	480(910)	4096	910	174	210
975	12	2	480(3120)	512(975)	4096	975	206	240
1040	12	2	512(3055)	544(1040)	4096	1040	240	272
1105	12	2	544(2990)	576(1105)	4096	1105	276	306
1170	12	2	576(2925)	608(1170)	4096	1170	314	342
1300	12	2	640(2795)	672(1300)	4096	1300	396	420
1365	12	2	672(2730)	704(1365)	4096	1365	440	462
1430	12	2	704(2665)	736(1430)	4096	1430	486	506
1495	12	2	736(2600)	768(1495)	4096	1495	534	552
1560	12	2	768(2535)	800(1560)	4096	1560	584	600
1625	12	2	800(2470)	832(1625)	4096	1625	636	650
1690	12	2	832(2405)	864(1690)	4096	1690	690	702
1755	12	2	864(2340)	896(1755)	4096	1755	746	756
1800*	12	2	896(3825)	960(270)	4096	1800	728	840
1820	12	2	896(2275)	928(1820)	4096	1820	804	812
1885	12	2	928(2210)	960(1885)	4096	1885	864	870
1950	12	2	960(2145)	992(1950)	4096	1950	926	930
2015	12	2	992(2080)	1024(2015)	4096	2015	990	992

7. Ternary Codes

n	k	q	w_1	w_2	N	K	λ	μ
328*	8	3	216(5904)	243(656)	6561	656	7	72
656	8	3	432(5248)	459(1312)	6561	1312	223	272
738	8	3	486(5087)	513(1476)	6561	1476	297	342
820	8	3	540(4920)	567(1640)	6561	1640	379	420
902	8	3	594(4756)	621(1804)	6561	1804	469	506
984	8	3	648(4592)	675(1968)	6561	1968	567	600
1066	8	3	702(4428)	729(2132)	6561	2132	673	702
1107	8	3	729(4346)	756(2214)	6561	2214	729	756
1148	8	3	756(4264)	783(2296)	6561	2296	787	812
1189	8	3	783(4182)	810(2378)	6561	2378	847	870
1230	8	3	810(4100)	837(2460)	6561	2460	909	930
1271	8	3	837(4018)	864(2542)	6561	2542	973	992
1312	8	3	864(3936)	891(2624)	6561	2624	1039	1056
1353	8	3	891(3854)	918(2706)	6561	2706	1107	1122
1394	8	3	918(3772)	945(2788)	6561	2788	1177	1190
1435	8	3	945(3690)	972(2870)	6561	2870	1249	1260
1476	8	3	972(3608)	999(2952)	6561	2952	1323	1332
1517	8	3	999(3526)	1026(3034)	6561	3034	1399	1406
1558	8	3	1026(3444)	1053(3116)	6561	3116	1477	1482
1599	8	3	1053(3362)	1080(3198)	6561	3198	1557	1560

8. References

[1] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann: Error Correcting Linear Codes, Springer 2006.

[2] R. Calderbank and W. M. Kantor, *The Geometry of Two-Weight Codes*, Bull. London Math. Soc. 18, pp. 97-122, 1986.

[3] A. Wassermann: *Finding Simple t-Designs with Enumeration Techniques*, Journal of Combinatorial Designs 6, pp. 79-90, 1998.