

# Constructing Two-weight Codes with Prescribed Groups of Automorphisms

---

-updated version August 2007

Axel Kohnert

*Lehrstuhl Mathematik II  
Universität Bayreuth  
95440 Bayreuth  
Deutschland*

## Introduction

We are interested in the construction of linear  $[n, k; q]$  two-weight codes. A linear code is a  $k$ -dimensional subspace  $C$  of the  $n$ -dimensional vector space  $GF(q)^n$  over the finite field  $GF(q)$  with  $q$  elements. The  $q^k$  codewords of length  $n$  are the elements of the subspace, they are written as row vectors. The weight of a codeword  $c$  is the number of nonzero components of the vector  $c \in GF(q)^n$ . In the case of a two-weight code  $C$  the nonzero elements of  $C$  have only two different weights  $w_1$  and  $w_2$  with  $w_1 < w_2$ .

Two-weight codes are an interesting object, as there are connections to objects in different areas of mathematics like strongly regular graphs, partial geometries and projective point sets. But two-weight codes are also interesting in the area of coding theory itself (e.g. uniformly packed codes) and have been studied intensively [11]. Delsarte [12] was the first to study the connections between two-weight codes, strongly regular graphs and projective point-sets. A survey of this relationship was given later by Calderbank and Kantor [10].

## Projective Point Sets

To formulate a two-weight code as a solution of a Diophantine system of equations we use in a first step a well known equivalence between linear two-weight  $[n, k; q]$  codes and point sets in the projective space  $PG(k-1, q)$ . A linear  $[n, k; q]$  code  $C$  is described by a generator matrix, i.e. a  $k \times n$  matrix over  $GF(q)$  whose row-space is the subspace  $C$ . If we assume that the columns of a generator matrix are pairwise linearly independent, we can take the columns of the generator matrix as a set (no multiple points as columns are linearly independent) of points in  $PG(k-1, q)$ . Because of this correspondence such a linear code is called *projective*. Using this correspondence it is well-known [10] that the weights of the code become the intersection numbers between the projective point set and the hyperplanes of  $PG(k-1, q)$ . In the case of a two-weight code the corresponding point set  $\Omega$  has the property that every hyperplane meets  $\Omega$  in  $n - w_1$  or  $n - w_2$  points. Such a point set is called a  $(n, k, n - w_1, n - w_2)$  point set. To construct projective two-weight codes we construct the corresponding point sets.

The next step is to formulate the construction of the point set as a solution of a Diophantine system of linear equations. For this let  $M$  be the point - hyperplane incidence matrix of  $PG(k-1, q)$ . Incidence is given by the subset relation between subspaces of  $GF(q)^k$ .  $M$  is a  $p \times p$  square matrix, where  $p$  is the number of points. The columns are labeled by the points and rows are labeled by the hyperplanes. This incidence matrix  $M$  can be used to formulate the construction of the point set as a solution of a system of equations.

**Theorem 1** *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  $x = (x_1, \dots, x_p)$  of the*

*Diophantine system of  $p + 1$  linear equations:*

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

$$(2) \quad \sum_{i=1, \dots, p} x_i = n.$$

An entry  $x_i$  equal to one in the solution says that the corresponding point labeling the  $i$ -th column of  $M$  is part of the  $(n, k, n - w_1, n - w_2)$  point set. The first  $p$  equations given in a closed matrix notation ensure that there are only two intersection numbers. The last equation ensures that point set has order  $n$ .

To solve this system using the computer we transfer it in the following form, where  $J$  is a  $p \times p$  diagonal matrix with the entry  $(w_2 - w_1)$  on the diagonal:

**Corollary 2** *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  $(x, y) = (x_1, \dots, x_p, y_1, \dots, y_p)$  of the Diophantine system of  $p + 1$  linear equations:*

$$(1) \quad (M, J)(x, y)^T = \begin{pmatrix} n - w_1 \\ \vdots \\ n - w_1 \end{pmatrix}$$

$$(2) \quad \sum_{i=1, \dots, p} x_i = n.$$

Here  $(M, J)$  denotes the  $p \times 2p$  block matrix built from matrices  $M$  and  $J$ . An entry  $y_i$  equal to one says that the  $i$ -th point (which is in the point set given by the solution  $x$ ) is met by  $n - w_2$  hyperplanes, an entry  $y_i$  equal to zero says that this point is met by  $n - w_1$  hyperplanes. The limiting factor for computation of a solution is the size (=number of rows) of the incidence matrix which is  $(q^k - 1)/(q - 1)$ . Solving the corresponding Diophantine system of equations is only possible for small dimensions. Therefore we apply a well-known method [1,20] to shrink this system by prescribing a group of automorphisms, i.e.

a subgroup of the general linear group  $GL(k, q)$ . This will be described in the next section. This method to reduce the size of the system of equations by prescribing automorphisms has since the first use in 1976 by Kramer and Mesner [21] been successfully applied in several cases like design theory [3,21],  $q$ -analoga of designs [9], arcs [7] and the construction of distance-optimal codes [5,6]. Already in [14] the author constructed new distance optimal codes by combining orbits.

### **Two-weight Codes with Prescribed Projective Groups**

We no longer search for an arbitrary solution, which corresponds to a selection of columns of the generator matrix or equivalently to a selection of points in a projective point set. In the reduced system an entry equal to one in the first half of the solution corresponds to a selection of a complete orbit of points under the action (multiplication) of a subgroup  $G$  of  $GL(k, q)$ . In the language of linear codes this means that the linear code has  $G$  as a subgroup in its group of automorphisms. For the incidence matrix  $M$  the selection of complete orbits of points corresponds to the addition of columns corresponding to the points in the orbit. This reduces the size of the matrix  $M$  to one, where the number of columns is the number of orbits. The action of  $G$  on the points induces an action on subspaces, and this action preserves incidence in the following sense:

**Lemma 3** Denote by  $B \cdot v$  the action of a matrix  $B \in G < GL(k, q)$  on a subspace  $v$  of  $GF(q)^k$ . Let  $p$  be a point of  $PG(k - 1, q)$  and  $H$  be a hyperplane in  $PG(k - 1, q)$ . Then we have for all matrices  $B$  :

$$p \subset H \iff B \cdot p \subset B \cdot H.$$

Because of this property the rows labeled by the hyperplanes in an orbit of  $G$  are identical after the column reduction. This shrinks the square matrix  $M$  of size  $(q^k - 1)/(q - 1)$  to a square matrix  $M^G$  of a smaller size  $m$ . Where  $m$  is the number of orbits. The rows of  $M^G$  are labeled by the orbits  $\Omega_1, \dots, \Omega_m$  of  $G$  on the hyperplanes, the columns are labeled by the orbits  $\omega_1, \dots, \omega_m$  of  $G$  on the points. For an entry in  $M^G$  we have

$$M_{i,j}^G = |\{p \in \omega_j : p \subset H_i\}|$$

for an arbitrary representative  $H_i \in \Omega_i$ . This allows us to give a version of the above corollary 2 in the case of a prescribed group of automorphisms.

**Theorem 4** *There is an  $(n, k, n - w_1, n - w_2)$  point set in  $PG(k - 1, q)$  with a subgroup  $G < GL(k, q)$  of automorphisms if and only if there is a  $(0/1)$ -solution  $(x, y)$  of the Diophantine system of linear equations:*

$$(1) (M^G, J^G)(x, y)^T = \begin{pmatrix} n - w_1 \\ \vdots \\ n - w_1 \end{pmatrix}$$

$$(2) \quad \sum_{i=1, \dots, m} |\omega_i| = n$$

Such a solution is a vector of length  $2m$  where  $m$  is the number of orbits of  $G$  on the points (resp. hyperplanes) in  $PG(k - 1, q)$ . An entry  $x_i$  equal to one says that the corresponding orbit is part of the  $(n, k, n - w_1, n - w_2)$  point set. The  $0/1$  distribution in  $y$  says, like in the case of corollary 2, how many hyperplanes meet the points from the corresponding  $i$ -th orbit.

## Results

To apply theorem 4 we need to know the two weights  $w_1$  and  $w_2$  of the linear code. As we are looking for projective codes, no two columns of the generator matrix are linearly dependent, so we know that the minimum distance of the dual code is at least 3. This allows to use the first 3 MacWilliams [1] identities to get candidates for the two weights. Using these candidates we apply theorem 4 for several subgroups of  $GL(k, q)$ . A last crucial step is the use of an effective algorithm [25] by A. Wassermann for the solution of the reduced Diophantine system of linear equations.

It is known [10,12] that a projective two-weight code can be used to define a strongly regular graph. A strongly regular graph is a  $K$ -regular graph with  $N$  vertices and each pair of adjacent vertices has  $\lambda$  common neighbors, and each pair of non-adjacent vertices has  $\mu$  common neighbors.

In the following tables we give the parameters of the two-weight codes we found using our method together with parameters of the corresponding strongly regular graph. Our table extends the results in [15] which used backtracking algorithms to construct all possible generator matrices. They got all inequivalent projective two weight codes. We were able to compute some (not all) two-weight codes for larger parameters. The left part of the tables below gives the parameters of the code, the fourth column the minimum weight together with the number of codewords of this weight, the fifth column the same information for the second weight. The next four columns give the parameters  $N, K, \lambda, \mu$  of the corresponding strongly regular graph. In the last column we give information on the found code, in the case of already known codes we give a citation or a method of construction already given in [10]. An entry 'known' or some reference different from a construction in [10] means that the corresponding strongly regular graph was known before. This does not necessarily mean that the code was already known.

Optimal codes (minimum distance meets some known upper bound) are marked with \*.

The author thanks Andries Brouwer who helped to compare the parameters with his database of two-weight codes/strongly regular graphs. We list the constructed two-weight codes for given  $q, k$  up to  $n = \left\lfloor \frac{q^k-1}{4} \right\rfloor$  which is half the number of all possible points. We do not list codes known from the SU2 construction of [10].

*Table 1: Binary codes of dimension 8*

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
51*	8	2	24(204)	32(51)	256	51	2	12	known
60	8	2	24(60)	32(195)	256	60	20	12	SU2,FE1
68*	8	2	32(187)	40(68)	256	68	12	20	FE1
85*	8	2	40(170)	48(85)	256	85	24	30	known
102*	8	2	48(153)	56(102)	256	102	38	42	known
119	8	2	56(136)	64(119)	256	119	54	56	RT2
128*	8	2	64(254)	128(1)	256	128	0	128	CY2,SU1

*Table 2: Binary codes of dimension 9*

The codes for  $n = 70$  and  $n = 196$  were found by Bierbrauer/Edel in 1997. (update Aug. 07)

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
70*	9	2	32(315)	40(196)	512	70	6	10	[4]
73*	9	2	32(219)	40(292)	512	73	12	10	[17]
196*	9	2	96(441)	112(70)	512	196	60	84	[4]
219	9	2	96(73)	112(438)	512	219	106	84	[17]
256*	9	2	128(510)	256(1)	512	256	0	256	SU1

Table 3: Binary codes of dimension 10

The code for  $n = 198$  may be a new optimal two-weight code, the strongly regular graph was known.

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
198*	10	2	96(825)	112(198)	1024	198	22	42	new
231*	10	2	112(792)	128(231)	1024	231	38	56	[13]
264*	10	2	128(759)	144(264)	1024	264	56	72	FE1
297	10	2	144(726)	160(297)	1024	297	76	90	[13]
330	10	2	160(693)	176(330)	1024	330	98	110	[13]
363	10	2	176(660)	192(363)	1024	363	122	132	[13]
396	10	2	192(627)	208(396)	1024	396	148	156	[13]
429	10	2	208(594)	224(429)	1024	429	176	182	[13]
462	10	2	224(561)	240(462)	1024	462	206	210	[13]
495	10	2	240(528)	256(495)	1024	495	238	240	known
512	10	2	256(1022)	512(1)	1024	512	0	512	SU1

Table 4: Binary codes of dimension 11

There are no new codes.

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
276	11	2	128(759)	144(1288)	2048	276	44	36	RT5
759	11	2	352(276)	384(1771)	2048	759	310	264	RT5d
1024	11	2	512(2046)	1024(1)	2048	1024	0	1024	SU1

Table 5: Binary codes of dimension 12

We list codes different from the construction SU2. 'new' means that the strongly regular graph and the two weight code are both new.

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
234*	12	2	112(2808)	128(1287)	4096	234	2	14	FE3
270	12	2	128(2295)	144(2184)	4096	270	14	18	known
273	12	2	128(1911)	144(2184)	4096	273	20	18	[22]
455*	12	2	224(3640)	256(455)	4096	455	6	56	known
780	12	2	384(3315)	416(780)	4096	780	116	156	known
845	12	2	416(3250)	448(845)	4096	845	144	182	new
910	12	2	448(3185)	480(910)	4096	910	174	210	new
975	12	2	480(3120)	512(975)	4096	975	206	240	known
1040	12	2	512(3055)	544(1040)	4096	1040	240	272	known
1105	12	2	544(2990)	576(1105)	4096	1105	276	306	new
1170	12	2	576(2925)	608(1170)	4096	1170	314	342	[24]
1300	12	2	640(2795)	672(1300)	4096	1300	396	420	new
1365	12	2	672(2730)	704(1365)	4096	1365	440	462	known
1430	12	2	704(2665)	736(1430)	4096	1430	486	506	new
1495	12	2	736(2600)	768(1495)	4096	1495	534	552	new
1560	12	2	768(2535)	800(1560)	4096	1560	584	600	known
1625	12	2	800(2470)	832(1625)	4096	1625	636	650	new
1690	12	2	832(2405)	864(1690)	4096	1690	690	702	new
1755	12	2	864(2340)	896(1755)	4096	1755	746	756	new
1800*	12	2	896(3825)	960(270)	4096	1800	728	840	known
1820	12	2	896(2275)	928(1820)	4096	1820	804	812	new
1885	12	2	928(2210)	960(1885)	4096	1885	864	870	new
1911	12	2	896(273)	960(3822)	4096	1911	950	840	[22]
1950	12	2	960(2145)	992(1950)	4096	1950	926	930	new
2015	12	2	992(2080)	1024(2015)	4096	2015	990	992	known
2048	12	2	1024(4094)	2048(1)	4096	2048	0	2048	SU1

Table 6: Ternary codes of dimension 5

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	info
11	5	3	6(132)	9(110)	243	22	1	2	known
55	5	3	36(220)	45(22)	243	110	37	60	known

Table 7: Ternary codes of dimension 6

There is no new two-weight code, but we mention references to the found codes.

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	
56	6	3	36(616)	45(112)	729	112	1	20	FE2
84	6	3	54(560)	63(168)	729	168	27	42	[18]
98	6	3	63(532)	72(196)	729	196	43	56	[18]
112	6	3	72(504)	81(224)	729	224	61	72	RT2
126	6	3	81(476)	90(252)	729	252	81	90	RT2,FE1
140	6	3	90(286)	99(280)	729	280	103	110	DeResmini
154	6	3	99(420)	108(308)	729	308	127	132	[19,14]
168	6	3	108(392)	117(336)	729	336	153	156	[23]

We found no new ternary two-weight codes of dimension 7, the only parameters were those from the construction SU1.

Table 8: Ternary codes of dimension 8

'new' means that the strongly regular graph and the two weight code are both new.

$n$	$k$	$q$	$w_1$	$w_2$	$N$	$K$	$\lambda$	$\mu$	
328*	8	3	216(5904)	243(656)	6561	656	7	72	known
656	8	3	432(5248)	459(1312)	6561	1312	223	272	known
738	8	3	486(5087)	513(1476)	6561	1476	297	342	known
820	8	3	540(4920)	567(1640)	6561	1640	379	420	new
902	8	3	594(4756)	621(1804)	6561	1804	469	506	new
984	8	3	648(4592)	675(1968)	6561	1968	567	600	new
1066	8	3	702(4428)	729(2132)	6561	2132	673	702	known
1107	8	3	729(4346)	756(2214)	6561	2214	729	756	known
1148	8	3	756(4264)	783(2296)	6561	2296	787	812	[22]
1189	8	3	783(4182)	810(2378)	6561	2378	847	870	new
1230	8	3	810(4100)	837(2460)	6561	2460	909	930	new
1271	8	3	837(4018)	864(2542)	6561	2542	973	992	new
1312	8	3	864(3936)	891(2624)	6561	2624	1039	1056	known
1353	8	3	891(3854)	918(2706)	6561	2706	1107	1122	new
1394	8	3	918(3772)	945(2788)	6561	2788	1177	1190	new
1435	8	3	945(3690)	972(2870)	6561	2870	1249	1260	[22]
1476	8	3	972(3608)	999(2952)	6561	2952	1323	1332	known
1517	8	3	999(3526)	1026(3034)	6561	3034	1399	1406	new
1558	8	3	1026(3444)	1053(3116)	6561	3116	1477	1482	new
1599	8	3	1053(3362)	1080(3198)	6561	3198	1557	1560	new

A more detailed version of these tables (together with generator matrices and the used group of automorphisms) can be found at the URL: <http://linearcodes.uni-bayreuth.de/twoweight/>.

### Concluding remark

There is the construction SU2 of Calderbank/Kantor [10] which gives two-weight codes for a series of parameters. Looking at the results for the pairs  $(q, k) = (2, 12), (3, 6), (3, 8)$  (see tables 5,7,8) suggests that

there might be a similar series sharing the same weights of the SU2-two-weight codes, but having different lengths of the codewords. For example in the case  $q = 3$  and  $k = 8$  the construction SU2 gives codes with weights  $w_1, w_2$  and length  $n$ :

$$w_1 = 27 \cdot i, w_2 = 27 + w_1, n = 40 + 40 \cdot i \quad (i = 1, \dots, 40).$$

The above table 8 indicates that we found two-weight codes for nearly all pairs of weights of this SU2 series but for a different length  $n = 41 \cdot i$  starting with  $i = 8$ .

## References

- [1] A. Betten, M. Braun, H. Friepertinger, A. Kerber, A. Kohnert and A. Wassermann: *Error Correcting Linear Codes*, Springer 2006.
- [2] A. Betten, R. Laue and A. Wassermann: *Simple 7-Designs with Small Parameters*. *Journal of Combinatorial Designs* 7, pp. 79-94, 1999
- [3] A. Betten, A. Kerber, A. Kohnert, R. Laue and A. Wassermann: *The discovery of simple 7-designs with automorphism group  $P\Gamma L(2, 32)$* . *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995, *Lect. Notes Comput. Sci.* 948, pp. 131-145, 1995.
- [4] J. Bierbrauer and Y. Edel: *A family of 2-weight codes related to BCH-codes*. *J. Comb. Des.* Vol. 5, pp. 391-396, 1997.
- [5] M. Braun: *Construction of Linear Codes with Large Minimum Distance*. *IEEE Transactions on Information Theory*, Vol.50, pp. 1687-1691, 2004.
- [6] M. Braun, A. Kohnert and A. Wassermann: *Optimal Linear Codes From Matrix Groups*, *IEEE Transactions on Information Theory*, Vol. 51, pp. 4247-4251, 2005.
- [7] M. Braun, A. Kohnert and A. Wassermann: *Construction of  $(n,r)$ -arcs in  $PG(2,q)$* , *Innovations in Incidence Geometry* 1, pp. 133-141, 2005.
- [8] M. Braun: *Construction of a point-cyclic resolution in  $PG(9,2)$* , *Innovations in Incidence Geometry* 3, pp. 33-50, 2006.
- [9] M. Braun, A. Kerber and R Laue: *Systematic Construction of  $q$ -Analogues of Designs*, *Des. Codes Cryptography* 34, pp. 55-70, 2005
- [10] R. Calderbank and W. M. Kantor, *The Geometry of Two-Weight Codes*, *Bull. London Math. Soc.* 18, pp. 97-122, 1986.
- [11] F. De Clerk and M. Delanote, *Two-Weight Codes, Partial Geometries and Steiner Systems*, *Des. Codes Cryptography* 21, pp. 87-98, 2000.

- [12] P. Delsarte, *Weights of linear codes and strongly regular normed spaces*, Discrete Math. 4, pp. 47-64, 1972.
- [13] L. A. Dissett, *Combinatorial and Computational Aspects of Finite Geometries*, Ph. D. Thesis, University of Toronto, 2000.
- [14] M. van Eupen, *Some New results for Ternary Linear Codes of Dimension 5 and 6*, IEEE Transactions on Information Theory, Vol.41, pp. 2048-2051, 1995.
- [15] V. Fack, I. Bouyukliev, W. Willems and J. Winne, *Projective two-weight codes with small parameters and their corresponding graphs*, Proceedings OC2005, Pamprovo 2005, pp. 139-145, 2005.
- [16] V. Fack, I. Bouyukliev, W. Willems and J. Winne, *Projective two-weight codes with small parameters and their corresponding graphs*, preprint 25p., August 2005.
- [17] F. Fiedler and M. Klin, *A strongly regular graph with the parameters (512, 73, 438, 12, 10) and its dual graph*. Preprint. MATH-AL-7-1998, Technische Universität Dresden, July 1998, 23 pp.
- [18] T. A. Gulliver, *Two new optimal ternary two-weight codes and strongly regular graphs*, Discrete Math. 149, pp. 83-92, 1996.
- [19] T. A. Gulliver, *A new two-weight code and strongly regular graph*, Appl. Math. Lett. 9, pp. 17-20, 1996.
- [20] A. Kerber: *Applied Finite Group Actions*, Springer, 1999.
- [21] E. S. Kramer and D. M. Mesner, *t-Designs on Hypergraphs*, Discrete Math. 15, pp. 263-296, 1976.
- [22] C. L. M. de Lange, *Some New Cyclotomic Strongly Regular Graphs*, J. Algebr. Comb. 4, pp. 329 - 330, 1995.
- [23] T. Penttila and G. F. Royle, *Sets of type (m, n) in the affine and projective planes of order nine*. Des. Codes Cryptography 6, pp. 229-245, 1995.
- [24] M. de Resmini and G. Migliori, *A 78-set of Type (2, 6) in PG(2, 16)*, Ars Comb. 22, pp. 73 - 75, 1986.
- [25] A. Wassermann: *Finding Simple t-Designs with Enumeration Techniques*, Journal of Combinatorial Designs 6, pp. 79-90, 1998.