Projective two-weight codes with small parameters and their corresponding graphs

V. Fack[*], I. Bouyukliev[†], W. Willems[‡], J. Winne[§]

14th April 2005

Submitted to Proceedings of OC'2005,
Fourth International Workshop on Optimal Codes and Related Topics,
Bulgaria, June 2005

1 Introduction

Let $\mathrm{GF}(q)^n$ be the n-dimensional vector space over the Galois field $\mathrm{GF}(q)$. The *Hamming distance* between two vectors of $\mathrm{GF}(q)^n$ is defined to be the number of coordinates in which they differ. A *q-ary linear $[n,k,d;q]$-code* is a k-dimensional linear subspace of $\mathrm{GF}(q)^n$ with minimum distance d. Let $n(k,d)$ denote the smallest value of n for which an $[n,k,d]$-code exists. An $[n(k,d),k,d]$-code is called *optimal*. A *generator matrix G* of a linear $[n,k;q]$-code C is any matrix of rank k over $\mathrm{GF}(q)$ with rows from C.

Let C_1 and C_2 be two linear $[n,k;q]$-codes. They are said to be *equivalent* if the codewords of C_2 can be obtained from the codewords of C_1 via a finite sequence of transformations of the following types: (1) permutation on the set of coordinate positions; (2) multiplication of the elements in a given position by a non-zero element of $\mathrm{GF}(q)$; (3) application of a field automorphism to the elements in all coordinate positions. An *automorphism* of a linear code C is a sequence of transformations of type (1)-(3) which maps each codeword of C onto a codeword of C. All the automorphisms of a code C form a group, which is called the *automorphism group* $\mathrm{Aut}(C)$ of the code C.

A linear code is called *projective* if no two columns of the generator matrix are linearly dependent. The *weight* $w(x)$ of a codeword x is defined as the number of the non-zero entries of x. The *weight enumerator* of C is $W_C(y) = \sum_{i=0}^{n} A_i y^i$ where A_i is

[*] Corresponding author. Department of Applied Mathematics and Computer Science, Ghent University, Belgium. E-mail: Veerle.Fack@UGent.be

[†] Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003. Institute of Mathematics and Informatics, Bulgarian Academy of Sciences. E-mail: iliya@moi.math.bas.bg

[‡] Institut fr Algebra und Geometrie, Otto-von-Guericke-Universitt, Magdeburg, Germany. E-mail: wolfgang.willems@mathematik.uni-magdeburg.de

[§] Department of Applied Mathematics and Computer Science, Ghent University, Belgium. E-mail: Joost.Winne@UGent.be the number of codewords of weight i in C. A *two-weight code* is a code which has only two non-zero weights w_1 and w_2.

Many people have studied projective two-weight codes (PTW) but not much is known about their properties. Some of the known classification results are related to optimal codes. In the binary case Tonchev [12] enumerated PTW [27,6,12;2] and [36,6,16;2] codes. In [9] Hamada and Helleseth found all inequivalent codes with parameters [15,4,9;3]. The uniqueness of the [56,6,36;3] code is proved in [10]. There are some other sporadic results.

Projective two-weight codes are related to other combinatorial objects, such as caps in projective spaces, combinatorial designs, etc. Moreover all these codes correspond to strongly regular graphs [7]. A *strongly regular graph* (SRG) with parameters (v, K, λ, μ) is a finite simple graph on v vertices, regular of degree K, and such that any two distinct vertices have λ common neighbours when they are adjacent and μ common neighbours when they are non-adjacent. Table 5.9 in [1] gives an overview of known strongly regular graphs and their properties, for relatively small parameter sets. Some of these graphs come from projective two-weight codes, the existence of which can be checked in [6].

Our contribution in this paper is a study of some properties of projective two-weight codes, their classification for small parameters and a study of their relation with strongly regular graphs, all of which might shed additional light on the general structure of projective two-weight codes.

2 Some properties of PTW codes

The following two lemmas present some basic results on the weights of PTW codes. In their proofs we use the fact that the simplex codes and McDonald codes are unique with their parameters [8]. A code is *even* (resp. *doubly-even*) if the weights of all codewords are divisible by 2 (resp. 4).

Lemma 1 *All binary projective two-weight codes are even except the* $[2^k-2, k, 2^{k-1}-1, 2^{k-1}]$ *McDonald codes. Moreover, at least one of the nonzero weights is doubly-even.*

Lemma 2 *All projective two-weight codes have weights which are multiples of the characteristic of the field except the* $[(q^k-q)/(q-1), k, q^{k-1}-1, q^{k-1}]$ *McDonald codes.*

Two vectors in $\mathrm{GF}(q)^n$ are said to be *orthogonal* if their inner product is 0. The set of vectors of $\mathrm{GF}(q)^n$ orthogonal to all codewords of C is called the *orthogonal code* $C^\perp$ to C. It is well-known that the code $C^\perp$ is a linear $[n, n-k; q]$ code. If $C \subseteq C^\perp$, then the code C is called *self-orthogonal.*

Lemma 3 *All doubly-even binary codes are self-orthogonal and all even quaternary codes are Hermitian self-orthogonal.*

In [2], Brouwer and Van Eupen described a correspondence between projective codes and two-weight codes (see also [8]). Let C be a projective $[n, k, d; q]$-code with nonzero weights $w_1, w_2, \ldots, w_s$ and generator matrix G . For α and β such that $\alpha w_i + \beta$

are nonnegative integers for all i, we can define a dual transform, say C^*, of C in the following way. Consider all nonzero vectors $v \in F_q^k$ for which the corresponding points in $PG(k-1)$ are different. A matrix G^* is constructed so that it contains as column vectors all such vectors v taken $w(v.G) \times \alpha + \beta$ times. This matrix G^* is the generator matrix of a two-weight code $C^*_{\alpha,\beta}$ which we call the *projective dual* of C.

Let C be a two-weight projective code with weights w_1 and w_2. Choose $\alpha_1 = \frac{1}{w_2-w_1}$, $\beta_1 = \frac{-w_1}{w_2-w_1}$ and $\alpha_2 = \frac{1}{w_1-w_2}$, $\beta_2 = \frac{-w_2}{w_1-w_2}$ in the above construction. In the first case we take all codewords of weight w_2 ones and we take no codeword of weight w_1. In the second case we change the weights.

The code C is said to be *projective self-dual* if it is equivalent to either $C^*_{\alpha_1,\beta_1}$ or $C^*_{\alpha_2,\beta_2}$. The code C is said to be *formally projective self-dual* if either $C^*_{\alpha_1,\beta_1}$ or $C^*_{\alpha_2,\beta_2}$ has the same length, dimension and weight set as C. Let $w_1 < w_2$ and let take the codewords of weight w_1 for the projective dual code. Then the projective dual code has length A_{w_1} and hence $A_{w_1} = n$.

Theorem 1 *If C is a formally projective self-dual code and C^* is its projective dual then their automorphism groups are isomorphic.*

As the length, dimension, weight distribution of the two codes are the same and their automorphism groups are isomorphic we can suppose that these codes are equivalent. Till these days for all known examples of formally projective self-dual codes the two codes are equivalent. But we obtained many new formally projective self-dual codes for which the code and its projective dual are not equivalent.

3 Computational results

Since a linear code is completely determined by its generator matrix it suffices to construct the generator matrices by means of a backtracking algorithm.

An important aspect in this algorithm is to construct all *inequivalent* linear codes with given length, dimension and minimum distance. Straightforward strategies excluding a lot of equivalent solutions consist in fixing a part of the generator matrix and in constructing the matrix in such a way that its columns are lexicographically ordered. More advanced strategies use ideas from [3] and [11] which give a canonical labelling and the automorphism group of the codes. For more information we refer to [5].

Moreover there are some specific restrictions for constructing PTW codes such as restrictions on the set of possible weights and restrictions coming from the projectivity.

In Tables 1 and 2 we present our results for binary and ternary PTW codes. For more results (codes over GF(4) and GF(5)) we refer to [4].

4 PTW codes and strongly regular graphs

There are strong connections between projective two-weight codes and strongly regular graphs. One such connection is given by Delsarte [7] (see also [6, Theorem 5.7]). Let w_1 and w_2 (where $w_1 < w_2$) be the weights of a q-ary projective two-weight code C

of length n and dimension k. To C we associate a graph $\Gamma(C)$ on $v = q^k$ vertices as follows. The vertices of the graph are identified with the codewords and two vertices corresponding to codewords x and y are adjacent iff $d(x,y) = w_1$. Then $\Gamma(C)$ is a strongly regular graph [7, Theorem 2].

Another construction follows from Calderbank and Kantor [6]. As vertices we take the points of the k-dimensional vectorspace $\mathrm{GF}(q)^k$. Such a vector defines a linear combination of the n-dimensional vectors of a generator matrix G of a projective two-weight code C corresponding to a codeword from the code. Two points p and q are joined by an edge iff $p - q$ is a multiple of a column in G. The graph $\Gamma'(C)$ obtained in this way is strongly regular [6, Theorems 3.1 and 3.2].

In Tables 3 and 4 we present results for strongly regular graphs obtained from binary and ternary PTW codes. For more results (strongly regular graphs from PTW codes over GF(4) and GF(5)) we refer to [4].

Acknowledgement. This work was finished during a visit of I. Bouyukliev in the Institute for Algebra and Geometry of the Otto-von-Gruericke-University Magdeburg. He would like to thank his hosts for the nice working conditions and hospitality.

References

[1] A.E. Brouwer, “Strongly regular graphs”, In: *CRC Handbook of Combinatorial Designs*, C.Colbourn and J.Dinitz eds., CRC Press, New York, 1996.

[2] A.E. Brouwer and M. van Eupen, “The correspondence between projective codes and 2-weight codes”, *Designs, Codes and Cryptography* **11** (1997) 262–266.

[3] I. Bouyukliev, “An algorithm for finding isomorphisms of codes”, In: *Proceedings of the International Workshop OCRT, Sunny Beach, Bulgaria* (2001) 35–41.

[4] I. Bouyukliev, V. Fack, W. Willems, J. Winne, “Projective two-weight codes with small parameters and their corresponding graphs”, in preparation.

[5] I. Bouyukliev and J. Simonis, “Some new results for optimal ternary linear codes”, *IEEE Trans. Inform. Theory* **48** (2002) 981–985.

[6] A.R. Calderbank and W.M. Kantor, “The geometry of two-weight codes”, *Bull. London Math. Soc.* **18** (1986) 97–122.

[7] P. Delsarte, “Weights of linear codes and strongly regular normed spaces”, *Discrete Math.* **3** (1972) 47–64.

[8] S. Dodunekov and J. Simonis, “Codes and projective multisets”, *Electron. J. Combin.* **5** no. 1 (1998) 23 pp. (electronic).

[9] N. Hamada and T. Helleseth, “A characterization of some $\{3v_2+v_3, 3v_1+v_2; 3, 3\}$-minihypers and some [15,4,9;3]-codes with $B_2 = 0$”, *J. Stat. Plann. Infer.* **56** (1996) 129–146.

[10] R. Hill, “Caps and codes”, *Discrete Math.* **22** (1978) 111–137.

[11] B.D. McKay, “Practical graph isomorphism”, *Congr. Numer.* **30** (1981) 45–87.

[12] V.D. Tonchev, “The uniformly packed binary [27,21,3] and [35,29,3] codes”, *Discrete Math.* **149** (1996) 283–288.

Table 1: Binary projective two-weight codes. For each code we list: (1) parameters of the code; (2) how far it stays from the Griesmer bound (optimal codes are marked with '*'); (3) weight enumerator; (4) number of nonequivalent codes; (5) number of projective self-dual codes; (6) order of the automorphism groups of the code; (7) information about the known examples in [6] (one example); (8) additional information about classification results.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$[5,4,2;2]$	0 *	$1+10z^2+5z^4$	1	1	$120,$		
$[6,4,2;2]$	1	$1+6z^2+9z^4$	1	1	$72,$	SU2	
$[14,6,4;2]$	4	$1+14z^4+49z^8$	1	1	$56448,$	SU2	
$[21,6,8;2]$	4	$1+21z^8+42z^{12}$	2	2	$336,1008,$	SU2	
$[27,6,12;2]$	2	$1+36z^{12}+27z^{16}$	5	5	$24,120,160,384,$ $51840,$	RT2	[12]
$[28,6,12;2]$	3	$1+28z^{12}+35z^{16}$	7	7	$24,120,84,96,$ $1344,384,40320,$	SU2	[12]
$[30,8,8;2]$	11	$1+30z^8+225z^{16}$	1	1	$812851200,$	CY4	
$[45,8,16;2]$	11	$1+45z^{16}+210z^{24}$	2	2	$120960,3628800,$	CY4	
$[51,8,24;2]$	1 *	$1+204z^{24}+51z^{32}$	1	1	$48960,$		
$[60,8,24;2]$	10	$1+60z^{24}+195z^{32}$	12	12	$192,16,24,32,40,$ $96,14400,576,120,$ $288,4320,720,$	CY4	
$[68,8,32;2]$	3 *	$1+187z^{32}+68z^{40}$	41	29	$2^7,6^2,48^3,12,192,$ $96,16320,1^{15},3^3,$ $4^4,8^2,16,$		

Table 2: Ternary projective two-weight codes. Legend: see Table 1.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$[10,4,6;3]$	0 *	$1+60z^6+20z^9$	1	1	$2880,$		
$[12,4,6;3]$	2	$1+24z^6+56z^9$	2	2	$288,1152,$	CY4	
$[15,4,9;3]$	1 *	$1+50z^9+30z^{12}$	2	2	$72,1440,$		[9]
$[16,4,9;3]$	2	$1+32z^9+48z^{12}$	4	4	$144^2,2304,64,$	CY4	
$[20,4,12;3]$	1	$1+40z^{12}+40z^{15}$	4	4	$24,480,128,160,$	CY4	
$[11,5,6;3]$	0 *	$1+132z^6+110z^9$	1	0	$15840,$		
$[55,5,36;3]$	0 *	$1+220z^{36}+22z^{45}$	1	0	$15840,$		[10]
$[56,6,36;3]$	0 *	$1+616z^{36}+112z^{45}$	1	1	$80640,$		[10]

Table 3: Strongly regular graphs corresponding to binary PTW codes.

SRG parameters	PTW parameters	$\lvert Aut(\Gamma)\rvert$	2-rank(Γ)
$(16, 5, 0, 2)$	$[5, 4, 2; 2]$	1920,	16,
$(16, 6, 2, 2)$	$[6, 4, 2; 2]$	1152,	6,
$(64, 14, 6, 2)$	$[14, 6, 4; 2]$	3251404800,	14,
$(64, 21, 8, 6)$	$[21, 6, 8; 2]$	21504,64512,	64,64,
$(64, 27, 10, 12)$	$[27, 6, 12; 2]$	1536,7680,10240,73728,	64,64,64,64,
		3317760,	64,
$(64, 28, 12, 12)$	$[28, 6, 12; 2]$	1536,7680,5376,6144,	14,12,14,12,
		2580480,24576,2580480,	8,8,8,
$(256, 30, 14, 2)$	$[30, 8, 8; 2]$	9223372036854775807,	30,
$(256, 45, 16, 6)$	$[45, 8, 16; 2]$	30965760,928972800,	256,256,
$(256, 51, 2, 12)$	$[51, 8, 24; 2]$	12533760,	256,
$(256, 60, 20, 12)$	$[60, 8, 24; 2]$	49152,4096,6144,8192,	38,42,42,42,
		10240,24576,3686400,147456,	42,40,36,40,
		30720,73728,1105920,184320,	42,42,38,40,
$(256, 68, 12, 20)$	$[68, 8, 32; 2]$	512,1536,12288,3072,	44,44,40,40,
		49152,24576,4177920,256,	36,38,36,46,
		256,768,256,256,	44,42,44,44,
		256,512,256,256,	44,42,42,46,
		512,256,768,1024,	44,46,44,42,
		512,256,256,512,	44,46,44,42,
		2048,256,256,256,	42,46,42,42,
		512,1024,512,256,	44,42,44,44,
		1024,256,2048,1024,	42,44,42,42,
		768,1536,4096,12288,	44,38,38,36,
		12288,	38,

Table 4: Strongly regular graphs corresponding to ternary PTW codes.

SRG parameters	PTW parameters	$\lvert Aut(\Gamma)\rvert$	2-rank(Γ)
$(81, 20, 1, 6)$	$[10, 4, 6; 3]$	233280,	81,
$(81, 24, 9, 6)$	$[12, 4, 6; 3]$	23328,93312,	19,19,
$(81, 30, 9, 12)$	$[15, 4, 9; 3]$	5832,116640,	19,19,
$(81, 32, 13, 12)$	$[16, 4, 9; 3]$	11664,11664,186624,5184,	81,81,81,81,
$(81, 40, 19, 20)$	$[20, 4, 12; 3]$	1944,38880,10368,12960,	81,81,81,81,
$(243, 22, 1, 2)$	$[11, 5, 6; 3]$	3849120,	243,
$(243, 110, 37, 60)$	$[55, 5, 36; 3]$	3849120,	243,
$(729, 112, 1, 20)$	$[56, 6, 36; 3]$	58786560,	729,