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

Iliya Bouyukliev*

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,

P.O. Box 323, 5000 V. Tarnovo, Bulgaria,

iliya@moi.math.bas.bg, http://www.moi.math.bas.bg/∼iliya/

Veerle Fack†

Research Group on Combinatorial Algorithms and Algorithmic Graph Theory,

Department of Applied Mathematics and Computer Science, Ghent University,

Krijgslaan 281–S9, B–9000 Ghent, Belgium,

Veerle.Fack@UGent.be, http://caagt.ugent.be/∼vfack/

Wolfgang Willems

Institut für Algebra und Geometrie, Otto-von-Guericke-Universität,

Postfach 4120, D-39016 Magdeburg, Germany,

wolfgang.willems@mathematik.uni-magdeburg.de, http://fma2.math.uni-magdeburg.de/∼willems/

Joost Winne‡

Research Group on Combinatorial Algorithms and Algorithmic Graph Theory,

Department of Applied Mathematics and Computer Science, Ghent University,

Krijgslaan 281–S9, B–9000 Ghent, Belgium,

Joost.Winne@UGent.be, http://allserv.ugent.be/∼jpwinne/

14th April 2006

Abstract

Projective two-weight codes with relatively small parameters are enumerated up to equivalence. Some properties of codes and related strongly-regular graphs are presented.

*Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003.

†Corresponding author

‡The author thanks the Fund for Scientific Research – Flanders (Belgium) for a Research grant.

1 Introduction

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the Galois field $\mathbb{F}_q$. The *Hamming distance* between two vectors of $\mathbb{F}_q^n$ is defined as the number of coordinates in which they differ. A *q-ary linear $[n, k, d]_q$ code* is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum distance d. A *generator matrix* G of a linear code $[n, k]$ code C is any matrix of rank k (over $\mathbb{F}_q$) 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 of coordinate positions; (2) multiplication of the elements in a given position by a non-zero element of $\mathbb{F}_q$; (3) application of a field automorphism to the elements in all coordinate positions. An *automorphism* of a linear code C is a finite sequence of transformations of type (1)–(3), which map each codeword of C onto a codeword of C. The set of automorphisms of a code C form a group which is called the *automorphism group* of the code C and denoted by $\mathrm{Aut}(C)$. Clearly, $\mathrm{Aut}(C)$ is the semidirect product of a group of monomial matrices by a Galois group.

A linear $[n, k]$ code is called *projective* if no two columns of a generator matrix G are linearly dependent, i.e., if the columns of G are pairwise different points in a projective $(k-1)$-dimensional space.

The *weight* $w(x)$ of a word $x \in \mathbb{F}_q^n$ is defined as the number of non-zero entries of x. We define the *weight enumerator* of C as $W_C(y) = \sum_{i=0}^{n} A_i y^i$ where A_i denotes the number of codewords of weight i in C. A *two-weight code* is a code which has exactly two non-zero weights, say w_1 and w_2.

The dual of a two-weight code belongs to the important family of uniformly packed codes [29]. It has been studied in many papers. There are some infinite classes of such codes [15], [22], [28] etc.. A good survey may be found in [11].

Many people have studied projective two-weight codes (PTW) but not much is really known about their properties. Some of the known classification results are related to optimal codes. In the binary case Tonchev [26] enumerated $[27, 6, 12]_2$ and $[36, 6, 16]_2$ PTW codes. In [18] Hamada and Helleseth found all inequivalent codes with parameters $[15, 4, 9]_3$. The uniqueness of a $[56, 6, 36]_3$ code is proved in [19].

For all q a $[q^2 + 1, 4, q(q-1)]$ code is known to exist. Moreover such a code is a PTW code with $d = w_1 = q(q-1)$ and $w_2 = q^2$. The columns of such a code form an *ovoid* in the 3-dimensional projective space [16]. Since for q odd an ovoid is an elliptic quadric, a result of Barlotti [1] and Panella [25], a $[q^2 + 1, 4, q(q-1)]$ code is unique if the underlying field has odd characteristic. In case q is an odd power of 2 there are ovoids, discovered by Tits, which are not equivalent to elliptic quadrics (see [30], Kapitel 2.6). However all $[q^2 + 1, 4, q(q-1)]$ codes have the same weight distribution.

Our contribution in this paper is the classification of projective two-weight codes for small parameters and the study of their properties and relations which might shed additional light on the general structure.

Projective two-weight codes are related to other combinatorial objects, such as caps in projective spaces, combinatorial designs, etc. Furthermore all such codes correspond to strongly regular graphs [12]. A *strongly regular graph* (SRG) with parameters (v, K, λ, μ) is a finite simple graph with v vertices which is regular of degree K, and any two distinct vertices have λ common neighbours if they are adjacent and μ common neighbours if they are non-adjacent.

Table 5.9 in [8] 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 [11]. In this paper we enumerate all codes mentioned in this table, except binary codes of dimension 8 and length > 68, as well as some additional codes over $\mathbb{F}_5$. Moreover we summarize some properties of these codes and their corresponding graphs.

2 Preliminaries

2.1 Optimality and residual codes

Many of the PTW codes have a large minimum distance. 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*.

One of the main problems in algebraic coding theory is to determine $n(k,d)$ for all values of k and d. A general lower bound on $n(k,d)$ has been proved by Griesmer [17]. He showed that

$$n(k,d) \geq g(k,d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil ,$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$.

We study how far the constructed codes are away from the Griesmer bound, how many of them meet the bound, and which of them are optimal.

Let G be a generator matrix of a linear $[n,k,d]_q$ code C. Then the *residual code* $Res(C,c)$ of C with respect to the codeword c is the code generated by the restriction of G to the columns i in which c has zero entries, i.e., $c_i = 0$.

Lemma 1 [13] *Suppose that C is an $[n,k,d]$ code over $\mathbb{F}_q$ and that $c \in C$ has weight w where $d > w(q-1)/q$. Then $Res(C,c)$ is an $[n-w, k-1, d']$ code with $d' \geq d - w + \lceil w/q \rceil$.*

2.2 Orthogonality

The *Euclidean inner product* of two vectors $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$ is defined by

$$\langle u\,, v\rangle \, = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

For codes over $\mathbb{F}_q$ where q is an even power of a prime p one can consider another type of inner product, the Hermitian inner product. The *Hermitian inner product* of two vectors $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$ is defined by

$$\langle u\,, v\rangle \, = u_1\bar{v}_1 + u_2\bar{v}_2 + \cdots + u_n\bar{v}_n,$$

where $\bar{v}_i = v_i^{\sqrt{q}}$ for $v_i \in \mathbb{F}_q$. Consequently, for $q = 4$, the Hermitian inner product is given by

$$\langle u\,, v\rangle \;= u_1 v_1^2 + u_2 v_2^2 + \cdots + u_n v_n^2.$$

In the binary and ternary case we consider the Euclidean inner product and in the quaternary case (like in most other studies) the Hermitian inner product.

Every inner product in $\mathbb{F}_q^n$ defines an orthogonality: Two vectors are said to be *orthogonal* if their inner product is 0. The set of all vectors of $\mathbb{F}_q^n$ orthogonal to all codewords of C is called the *orthogonal code* $C^\perp$ to C, i.e.,

$$C^\perp = \{x \in \mathbb{F}_q^n \mid \langle x\,, y\rangle \;= 0 \text{ for any } y \in C\}.$$

It is well-known that $C^\perp$ is a linear $[n, n-k]_q$ code.

A generator matrix of the code $C^\perp$, orthogonal to C, is a *parity check matrix* for C which we denote by $\mathbf{H}_C$.

If $C \subseteq C^\perp$ then C is called *self-orthogonal*.

3 PTW codes – orthogonality and weights

If the weigths of all codewords of C are divisible by $r \in \mathbb{N}$ we call C an r-divisible code. Likewise, in particular in characteristic 2, we call a code *even* (resp. *doubly-even*) if the weights of all codewords are divisible by 2 (resp. 4). In this section we will use the fact that the simplex codes and MacDonald codes are unique with respect to their parameters [14]. Note that a $[(q^k - q)/(q-1), k, q^{k-1} - 1]$ MacDonald code has a generator matrix whose columns consist of all points but one of the projective space $PG(k-1, q)$.

Proposition 2 *Let q be a power of the prime p. Then all projective two-weight codes of dimension $k \geq 3$ are p-divisible except the $[(q^k - q)/(q-1), k, q^{k-1} - 1]$ MacDonald codes whose weights are $q^{k-1} - 1$ and q^{k-1}.*

Proof. Let C be a projective $[n, k]$ two-weight code over $\mathbb{F}_q$ with weights w_1 and w_2. If A_i resp. B_i $(i = 0, \ldots, n)$ denotes the weight distribution of C resp. $C^\perp$ then, by the MacWilliams identies, we have

$$|C| B_k = \sum_{i=0}^{n} A_i\, K_k(i) \qquad (k = 0, \ldots, n)$$

where $K_k(i)$ are Krawtchouk polynomials. Since C is a projective code we get $0 = B_1 = B_2$. Thus

$$\begin{aligned}
q^k = q^k B_0 &= K_0(0) + A_{w_1} K_0(w_1) + K_0(w_2) A_{w_2}, \\
0 = q^k B_1 &= K_1(0) + A_{w_1} K_1(w_1) + K_1(w_2) A_{w_2}, \\
0 = q^k B_2 &= K_2(0) + A_{w_1} K_2(w_1) + K_2(w_2) A_{w_2}.
\end{aligned}$$

¿From these equations one easily derives

$$q^{k-2}(q-1)n^2 - q^{k-2}(q(w_1+w_2)-1)n + \frac{(q^k-1)w_1w_2}{q-1} = 0,$$

hence $q^{k-2} \mid w_1w_2$. Note that p divides w_1 or w_2 (since $k \geq 3$), but not both since otherwise we are done. Thus we may assume that $q \nmid w_2$ and $q \mid w_1$.
Let $\mathbb{F}_q = \{0 = \alpha_0, 1 = \alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$. Suppose that

$$x = (\underbrace{1111\ldots1111}_{a_1+\cdots+a_{q-1}+a_0}\underbrace{00\ldots0}_{b}00\ldots0)$$

and

$$y = (\underbrace{11\ldots11}_{a_1}\underbrace{\alpha_2\ldots\alpha_2}_{a_2}\ldots,\underbrace{\alpha_{q-1}\ldots\alpha_{q-1}}_{a_{q-1}}\underbrace{00\ldots0}_{a_0}\underbrace{11\ldots1}_{b}00\ldots0)$$

are codewords in C. We put $a = a_1 + \cdots + a_{q-1}$ and $w_2 = a + a_0 = \mathrm{wt}(x)$.
(1) We claim that $b = \frac{w_1}{q}$.
Suppose that

$$\mathrm{wt}(\alpha_{i_1}x - y) = \mathrm{wt}(\alpha_{i_2}x - y) = \cdots = \mathrm{wt}(\alpha_{i_s}x - y) = w_1$$

and

$$\mathrm{wt}(\alpha_{j_1}x - y) = \mathrm{wt}(\alpha_{j_2}x - y) = \cdots = \mathrm{wt}(\alpha_{j_m}x - y) = w_2$$

where $\{\alpha_{i_1}, \ldots, \alpha_{i_s}, \alpha_{j_1}, \ldots, \alpha_{j_m}\} = \mathbb{F}_q^*$, hence $s + m = q - 1$. Since

$$\mathrm{wt}(\alpha_l x - y) = a + a_0 + b - a_l$$

we have $a_{i_1} = \cdots = a_{i_s} = a + a_0 + b - w_1$ and $a_{j_1} = \cdots = a_{j_m} = a + a_0 + b - w_2$. Furthermore, the equation

$$a_{i_1} + \cdots + a_{i_s} + a_{j_1} + \cdots + a_{j_m} = a$$

implies

$$a = s(a + a_0 + b - w_1) + m(a + a_0 + b - w_2) = (q-1)(a + a_0 + b) - sw_1 - mw_2.$$

If $a + b = w_2$ then $a_0 = b = w_2 - a$ and therefore

$$a = (q-1)(a + 2w_2 - 2a) - sw_1 - mw_2 = (2q - 2 - m)w_2 - (q-1)a - sw_1.$$

Thus we get

$$(*) \qquad qa = (q - 1 + s)w_2 - sw_1.$$

Since $p \nmid w_2$ and $q \mid w_1$ we have $q \mid (s-1)$ and therefore $s = 1$ as $s \leq q - 1$. By $(*)$ we get (up to equivalence) that

$$a = w_2 - \frac{w_1}{q},$$

hence

$$b = w_2 - a = \frac{w_1}{q}.$$

In case $a + b = w_1$ we have $a_0 = w_2 - a$ and $b = w_1 - a$. Therefore

$$a = (q-1)(a + w_2 + w_1 - 2a) - sw_1 - mw_2 = (q-1-m)w_2 + (q-1-s)w_1 - (q-1)a,$$

hence

$$qa = (q-1-m)w_2 + (q-1-s)w_1.$$

Since $p \nmid w_2$ and $q \mid w_1$ we obtain $q \mid (q-1-m)$. This implies $m = q-1$ and $s = 0$. It follows that $a = \frac{q-1}{q}w_1$. Since $a + b = w_1$ we get again $b = \frac{w_1}{q}$.

(2) We claim that $w_1 = q^{k-1}$ and $w_2 = n - \frac{q^{k-1}-1}{q-1}$.

By (1), the residual code $\mathrm{Res}(C, x)$ is a 1-weight projective code of length $n - w_2$ with the only non-zero weight $\frac{w_1}{q}$. By a well-known result of Bonisoli [2] $\mathrm{Res}(C, x)$ must be a Simplex code. Let x be the first row of a generator matrix G of C. Next we show that the dimension of $\mathrm{Res}(C, x)$ is equal to $k-1$. If not, then the code defined by the second up to the last row of G contains a codeword $c \neq 0$ with non-zero entries only in the first w_2 positions. Clearly, $c \neq \alpha x$ for any $\alpha \in \mathbb{F}_q$ since otherwise G has rank smaller than k. Thus, for some $\alpha \in F_q^*$ the vector $\alpha x - c$ is not 0 and has a weight smaller than w_2. It follows that $\mathrm{wt}(\alpha x - c) = w_1 < w_2$ and

$$w_1 = \mathrm{wt}(\alpha x - c) = \mathrm{wt}(x) + \mathrm{wt}(c) - 2|\{i \mid c_i = \alpha\}|.$$

Since p does not divide both w_1 and w_2 we get from Corollary 2 of [12] that $w_2 = w_1 + 1$. Therefore

$$w_2 - 1 = w_2 + \mathrm{wt}(c) - 2|\{i \mid c_i = \alpha\}|.$$

Suppose that $\mathrm{wt}(c) = w_2$. Then $|\{i \mid c_i = \alpha\}| = (w_2+1)/2$. Thus there exists a further element, say $\beta \neq \alpha$, with $|\{i \mid c_i = \beta\}| = (w_2+1)/2$, a contradiction. Now suppose that $\mathrm{wt}(c) = w_1 = w_2 - 1$. Then $|\{i \mid c_i = \alpha\}| = w_2/2$. This forces obviously $w_2 - 1 = w_1 = w_2/2$, hence $w_2 = 2$. Thus we obtain $q \mid w_1 < w_2 = 2$, a final contradiction. Thus we have shown that $\mathrm{Res}(C, x)$ is the

$$[\frac{q^{k-1}-1}{q-1}, k-1, q^{k-2}]$$

Simplex code. In particular $\frac{w_1}{q} = q^{k-2}$, hence $w_1 = q^{k-1}$. Since w_2 is equal to n minus the length of $\mathrm{Res}(C, x)$ we get $w_2 = n - \frac{q^{k-1}-1}{q-1}$.

(3) Finally we show that C is a MacDonald code.

By Corollary 2 of [12], we have $w_2 = w_1 \pm 1$. Suppose that $w_2 = w_1 + 1$. Then, by (2),

$$n = \frac{q^{k-1}-1}{q-1} + w_2 = 1 + q + \ldots + q^{k-2} + q^{k-1} + 1 = \frac{q^k - 1}{q-1} + 1,$$

a contradiction since C is projective. Thus we get

$$q^{k-1} - 1 = w_1 - 1 = w_2 = n - \frac{q^{k-1} - 1}{q - 1}$$

which implies $n = \frac{q^k - q}{q-1}$. This proves that C is a projective $[\frac{q^k-q}{q-1}, k, q^{k-1} - 1]$ code with weights q^{k-1} and $q^{k-1} - 1$. This code is known to be a MacDonald code. $\square$

Corollary 3 *All binary projective two-weight codes of dimension at least* 3 *are even except the* $[2^k - 2, k, 2^{k-1} - 1]$ *MacDonald codes. Moreover, at least one of the non-zero weights is doubly-even.*

Proof. According to Proposition 2 we only have to show that one of the nonzero weights is doubly-even. This follows immediately from Corollary 2 in [12] since the code is even. $\square$

To prove the next lemma we need the following notation. For two binary vectors x and y we define $x * y$ as the vector which has a 1 exactly at those positions in which both x and y have a 1.

Proposition 4 *A binary projective two-weight code of dimension at least* 3 *is self-orthogonal if and only if it is doubly-even.*

Proof. Let C be a binary projective $[n, k]$ two-weight code with weights w_1 and w_2. Note that for $c, c' \in C$ we have

$$\mathrm{wt}(c + c') = \mathrm{wt}(c) + \mathrm{wt}(c') - 2\mathrm{wt}(c * c').$$

Thus if C is doubly-even then $2 \mid \mathrm{wt}(c * c')$ which proves that c and c' are orthogonal.

Now suppose that C is self-orthogonal. Thus $\mathrm{wt}(c + c') = \mathrm{wt}(c) + \mathrm{wt}(c') \bmod 4$ which means that the natural map

$$\mathrm{wt} : C \to 2\mathbb{Z}/4\mathbb{Z}$$

is a group homomorphism. Consequently the subset C_0 of doubly-even words of C is a subspace. Suppose that $C_0 < C$. By Corollary 3, we have $C_0 \neq 0$. Thus $|C_0| = 2^{k-1}$. If A_{w_i} denotes the number of codewords of weight w_i where w_1 is doubly-even then $A_{w_1} = 2^{k-1} - 1$ and $A_{w_2} = 2^{k-1}$. Counting the entries 1 of all codewords of C we obtain

$$(2^{k-1} - 1)w_1 + 2^{k-1}w_2 = 2^{k-1}n.$$

Thus $2^{k-1} \mid w_1$ and since $w_1 \leq n \leq 2^k - 1$ we get $w_1 = 2^{k-1}$. This shows that $n = 2^{k-1} - 1 + w_2$. Since $k \geq 3$ and $w_1/2$ odd we obtain $n \equiv 1 \bmod 4$. On the other hand, the same argument applied to C_0 shows that

$$(2^{k-1} - 1)2^{k-1} = (2^{k-1} - 1)w_1 = e2^{k-2}$$

where $e = |\{i \mid (c_1, \ldots, c_n) \in C_0,\ c_i \neq 0\}|$. It follows $e = 2^k - 2$. The condition $n \equiv 1 \bmod 4$ now forces $n \geq 2^k + 1$, contradicting the projectivity of C. $\square$

The following lemma which we need in the sequel seems to be known. For the reader's convenience we include a proof here.

Lemma 5 *A quaternary code is Hermitian self-orthogonal if and only if it is even.*

Proof. For a codeword $x = (x_1, x_2, \ldots, x_n)$ in a quaternary Hermitian self-orthogonal code we have

$$\langle x\,, x\rangle\ = x_1^3 + x_2^3 + \cdots + x_n^3 = \mathrm{wt}(x) \pmod 2.$$

Since $\langle x\,, x\rangle\ = 0$ we get $\mathrm{wt}(x) \equiv 0 \pmod 2$.

We now prove that the property C being even implies self-orthogonality. Let C be an even quaternary code and let $x, y \in C$. Since for quaternary codes equivalence preserves self-orthogonality we may assume that

$$x = (\underbrace{11\ldots11}_{a+b+c+d}\underbrace{00\ldots0}_{e}00\ldots0)$$

and

$$y = (\underbrace{11\ldots11}_{a}\underbrace{\omega\ldots\omega}_{b}\underbrace{\omega^2\ldots\omega^2}_{c}\underbrace{00\ldots0}_{d}\underbrace{11\ldots1}_{e}00\ldots0)$$

where $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. As

$$\mathrm{wt}(x) \equiv \mathrm{wt}(y) \equiv \mathrm{wt}(x+y) \equiv \mathrm{wt}(x+\omega y) \equiv \mathrm{wt}(x+\omega^2 y) \equiv 0 \pmod 2$$

we have

$$a+b+c+d \equiv a+b+c+e \equiv b+c+d+e \equiv a+b+d+e \equiv a+c+d+e \equiv 0 \pmod 2.$$

Hence $a \equiv b \equiv c \equiv d \equiv e \pmod 2$. The inner product is given by

$$\langle x\,, y\rangle\ = \underbrace{1+\cdots+1}_{a} + \underbrace{\omega^2+\cdots+\omega^2}_{b} + \underbrace{\omega+\cdots+\omega}_{c},$$

which sums up to 0 if $a \equiv b \equiv c \equiv 0 \pmod 2$, and to $1+\omega+\omega^2$ if $a \equiv b \equiv c \equiv 1 \pmod 2$. Since $1+\omega+\omega^2 = 0$ we have in each case $\langle x\,, y\rangle\ = 0$. Thus C is Hermitian self-orthogonal. $\square$

4 Formally projective self-dual codes

In [10], Brouwer and Van Eupen described a correspondence between special projective and two-weight codes (see also [14]). Let C be a projective $[n,k,d]$ code over $\mathbb{F}_q$ with nonzero weights $w_1, w_2, \ldots, w_s$ and generator matrix G. For real numbers α and β such that $\alpha w_i + \beta$ are nonnegative integers for all i we can define a dual transform C^* of C in the following way. Consider all nonzero vectors $v \in \mathbb{F}_q^k$ for which the corresponding points in $PG(k-1)$ are different. Now we take all such $v's$ and write them with multiplicity $\mathrm{wt}(vG)\alpha + \beta$ as columns in a matrix which we denote by G^*. Note that 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

$$\alpha_1 = \frac{1}{w_2 - w_1},\ \beta_1 = \frac{-w_1}{w_2 - w_1} \text{ and } \alpha_2 = \frac{1}{w_1 - w_2},\ \beta_2 = \frac{-w_2}{w_1 - w_2}$$

in the above construction. In the first case we take all codewords of weight w_2 exactly once and no codeword of weight w_1. The second case covers the change of the weights. Note that $C^*_{\alpha_1,\beta_1}$ is of length A_{w_2} and $C^*_{\alpha_2,\beta_2}$ of length A_{w_1}.

The code C is called *projective self-dual* if it is equivalent to either $C^*_{\alpha_1,\beta_1}$ or $C^*_{\alpha_2,\beta_2}$. It is called *formally projective self-dual* if either $C^*_{\alpha_1,\beta_1}$ or $C^*_{\alpha_2,\beta_2}$ has the same length and weight distribution as C.

In order to study the automorphism groups of C and its projective dual we need the following lemma.

Lemma 6 *Let q be a power of the prime p. Then the isometry group of $\mathbb{F}_q^n$ with respect to the Hamming distance is the semidirect product*

$$\widehat{M}(n,q) = M(n,q) \cdot Gal(\mathbb{F}_q/\mathbb{F}_p)$$

where $M(n,q)$ denotes the group of monomial matrices of size n over $\mathbb{F}_q$ and $Gal(\mathbb{F}_q/\mathbb{F}_p)$ the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$. Moreover, the multiplication is given by

$$(Q_1\tau_1)(Q_2\tau_2) = (Q_1 Q_2^{\tau_1^{-1}})(\tau_1\tau_2)$$

for $Q_i \in M(n,q)$ and $\tau_i \in Gal(\mathbb{F}_q/\mathbb{F}_p)$. (Here Q^τ denotes the matrix obtained from Q by applying τ to each entry.)

Proof. By definition of an automorphism we only have to check the multiplication rule. If $Q = \mathrm{diag}(a_1, \ldots, a_n)\mathrm{P}(\pi) \in \mathrm{M}(n,q)$ with the permutation matrix $\mathrm{P}(\pi) = (p_{ij})$ where $p_{ij} = 1$ for $i = \pi j$ and 0 otherwise then

$$(x_1, \ldots, x_n)Q\tau = (a_{\pi 1}^\tau x_{\pi 1}^\tau, \ldots, a_{\pi n}^\tau x_{\pi n}^\tau).$$

for any vector $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. With this observation one easily checks the multiplication rule. □

Theorem 7 *If C is a formally projective self-dual code then $Aut(C)$ and $Aut(C^*)$ are isomorphic.*

Proof. (1) Let D be an $m \times n$ matrix whose rows are codewords of C which are pairwise not a multiple of each other and which generate C as vector space. In addition we assume that the set consisting of the rows of D with all their collinear vectors is invariant under $\mathrm{Aut}(C)$. If $Q\tau \in \mathrm{Aut}(C) \leq \widehat{M}(n,q)$ then the matrix $DQ\tau$ can be obtained from D by permuting the rows and multiplying them by nonzero elements of $\mathbb{F}_q$. Thus there is a monomial matrix $P \in \mathrm{M}(m,q)$ such that

$$(*) \qquad P(DQ\tau) = D.$$

By Lemma 6, we have

$$DQ\tau = D^\tau Q^\tau$$

which we freely use in the sequel. Obviously, the matrix P is uniquely determined by $Q\tau$ since D does not contain collinear row vectors. Next we define a multiplication on

$$\mathrm{M}\widehat{M}(m,n,q) = \mathrm{M}(m,q) \times \widehat{M}(n,q)$$

by

$$(P_1, Q_1\tau_1)(P_2, Q_2\tau_2) = (P_2 P_1^{\tau_2}, (Q_1\tau_1)(Q_2\tau_2)) = (P_2 P_1^{\tau_2}, Q_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2)$$

and consider the map

$$\Phi : \mathrm{Aut}(C) \to \mathrm{M}\widehat{M}(m,n,q)$$

given by

$$\Phi(Q\tau) = (P, Q\tau).$$

Let $Q_1\tau_1,\ Q_2\tau_2 \in \mathrm{Aut}(C)$. Hence

$$P_1(DQ_1\tau_1) = D \quad \text{and} \quad P_2(DQ_2\tau_2) = D.$$

We obtain

$$(P_1 D^{\tau_1} Q_1^{\tau_1})(Q_2\tau_2) = P_1^{\tau_2} D^{\tau_1\tau_2} Q_1^{\tau_1\tau_2} Q_2^{\tau_2} = DQ_2\tau_2,$$

and therefore

$$D = P_2(DQ_2\tau_2) = P_2 P_1^{\tau_2} D^{\tau_1\tau_2} Q_1^{\tau_1\tau_2} Q_2^{\tau_2} = (P_2 P_1^{\tau_2})(DQ_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2).$$

Thus

$$\Phi((Q_1\tau_1)(Q_2\tau_2)) = \Phi(Q_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2) = (P_2 P_1^{\tau_2}, Q_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2).$$

On the other hand

$$\Phi(Q_1\tau_1)\Phi(Q_2\tau_2) = (P_1, Q_1\tau_1)(P_2, Q_2\tau_2) = (P_2 P_1^{\tau_2}, Q_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2).$$

This shows that Φ defines a group homomorphism onto its image. Clearly, Φ is a monomorphism since $Q\tau = id$ implies that the corresponding monomial matrix P is the identity as all row vectors of D are pairwise non-collinear. Finally suppose that $PDQ\tau = D$ with $P \in \mathrm{M}(m,q)$ and $Q\tau \in \widehat{M}(n,q)$. Since $DQ\tau = P^{-1}D$ and the rows of D generate C the monomial matrix $Q\tau$ is an automorphism of C. Thus we have proved that

$$\mathrm{Aut}(C) \cong \{(P, Q\tau) \mid (P, Q\tau) \in \mathrm{M}(n,q) \times \widehat{M}(n,q),\ P(DQ\tau) = D\}.$$

(2) Let G be a generator matrix of C and let $g_1, g_2, \ldots, g_k$ be its rows. If $b = (\beta_1, \beta_2, \ldots, \beta_k)$ is a column of G^* then

$$\beta_1 g_1 + \beta_2 g_2 + \cdots + \beta_k g_k$$

is a codeword in C, say of weight w. If C has the same length and weight distribution as $C^*_{\alpha_1,\beta_1}$ then $w = w_2$, and in the other case $w = w_1$. In this way we obtain all n but non-collinear codewords in C of weight w. Hence $(G^*)^t G = D$ where the rows of D are all non-collinear codewords in C of weight w. The matrix D is a square matrix of size n in which all rows have the same weight w. Moreover, all columns of D have also weight w. This can be seen as follows. The number of ones as entries in D is nw. This holds obviously also true for $D^t = G^t G^*$ whose rows are codewords of C^*. Now, if $r > 0$ row vectors of D^t have weight $w_1 \neq w$ then the number of ones in D^t would be $rw_1 + (n-r)w < nw$, a contradiction. Thus the weigths of all row and all column vectors of D are w. Furthermore D generates the whole code C since the rank of both G^* and G is k. Thus by (1),

$$\mathrm{Aut}(C) \cong \{(P, Q\tau) \mid (P, Q\tau) \in \mathrm{M}(n,q) \times \widehat{M}(n,q),\ P(DQ\tau) = D\}.$$

Next we consider $G^t G^* = ((G^*)^t G)^t = D^t$. By the same argument as above

$$\mathrm{Aut}(C^*) \cong \{(P, Q\tau) \mid (P, Q\tau) \in \mathrm{M}(n,q) \times \widehat{M}(n,q),\ P(D^t Q\tau) = D^t\}.$$

Now, if $P(DQ\tau) = D$ then

$$D^t = (PD^\tau Q^\tau)^t = Q^{t\tau} D^{t\tau} P^t) = Q^{t\tau}(D^t P^{t\tau^{-1}} \tau).$$

Clearly, the map

$$\Psi : \mathrm{Aut}(C) \to \mathrm{Aut}(C^*)$$

defined by

$$(P, Q\tau) \to (Q^{t\tau}, P^{t\tau^{-1}} \tau)$$

is a bijection. Finally, we have show that it is a group isomorphism. Note that on one hand side we have

$$\begin{aligned}\Psi((P_1, Q_1\tau_1)(P_2, Q_2\tau_2)) &= \Psi(P_2 P_1^{\tau_2}, Q_1 Q_2^{\tau_1^{-1}} \tau_1\tau_2) \\ &= (Q_2^{t\tau_2} Q_1^{t\tau_1\tau_2}, P_1^{t\tau_1^{-1}} P_2^{t(\tau_1\tau_2)^{-1}} \tau_1\tau_2).\end{aligned}$$

On the other hand

$$\begin{aligned}\Psi((P_1, Q_1\tau_1))\Psi(P_2, Q_2\tau_2) &= ((Q_1^{t\tau_1}, P_1^{t\tau_1^{-1}} \tau_1))((Q_2^{t\tau_2}, P_2^{t\tau_2^{-1}} \tau_2)) \\ &= (Q_2^{t\tau_2} Q_1^{t\tau_1\tau_2}, P_1^{t\tau_1^{-1}} P_2^{t\tau_2^{-1}\tau_1^{-1}} \tau_1\tau_2)\end{aligned}$$

which proves the assertion. □

One might be tempted to conjecture that two formally projective self-dual codes which have isomorphic automorphism groups are equivalent. This is far from being true. Via computer search we obtained many formally projective self-dual codes for which the code and its projective dual are not equivalent.

The tables at the end of this paper indicate which codes are formally projective self-dual as well as those which are projective self-dual.

5 Construction of codes

Clearly, a linear code is completely determined by its generator matrix. So in order to construct codes we may consider their generator matrices G_x.

The main problem we are faced with is to find the list of all inequivalent linear codes of length n, dimension k and minimum distance d via their generator matrices.

Obviously, if we can fix a part of the generator matrix we have to consider less cases. If the fixed part gets larger in size then the number of inequivalent codes may decrease. For the fixed part we can choose the identity matrix of order k for instance, since any code has a generator matrix in systematic form.

In this case a generator matrix is of shape

$$G_x = \left(\begin{array}{c|cccc} \cdots\cdots\cdots & 1 & & & \\ \cdots\cdots\cdots & & 1 & & \\ & & & \ddots & \\ \cdots\cdots\cdots & & & & 1 \end{array} \right).$$

The fixed part can be taken as a generator matrix of a residual code.

Let C be a $[n, k, d]$ code and let C_0 be the residual $\mathrm{Res}(C_x, w)$ with respect to a codeword of weight $w < d + \lceil w/q \rceil$.

Let G_0 be a generator matrix of the $[n', k-1, d']$ code C_0. If $C_0 = \mathrm{Res}(C_x, w)$ then up to equivalence there exists a generator matrix of C_x in the following form

$$G_x = \left(\begin{array}{c|c} 1\ 1\ \ldots\ \ 1 & 0\ \ldots\ 0\ 0 \\ \hline \cdots\cdots\cdots & \\ \cdots\cdots\cdots & G_0 \\ & \\ \cdots\cdots\cdots & \end{array} \right).$$

Note that the rank of G_0 equals $k-1$ since $w < d + \lceil w/q \rceil$ by Lemma 1. We will describe the algorithms only in the binary case. For larger fields the ideas are very similar.

A generator matrix has two parts - a fixed one (called $G_{x-fixed}$) (with rows $u_1, u_2, \ldots, u_{k_{out}}$ of G_0) and a free one (called G_{x-free}) (from position 1 up to position $n - n'$). The first row of G_{x-free} consists of the all one vector. It is rather easy (according to exhaustive search) to find how many ones the second, the third, in general the i-th row can have.

The idea of the algorithm for constructing the i-th row is the following: In the first step we obtain the possible number of ones. In a further step we localize the positions of these ones and in the last step we find the exact positions.

Suppose that the second row contains x_2 entries equal to 1. Without lost of generality we can write these x_2 ones in the first x_2 positions of the second row of G_{x-free}. So the columns of the constructed matrix are lexicographically ordered and we exclude a lot of equivalent solutions. In this step it is not possible to fix the ones in the other rows.

Suppose that we have found the first $t-1$ rows of G_{x-free}. Let us denote them by $v_1, v_2, \ldots, v_{t-1}$. A vector v (lexicographically ordered in the intervals) is called a *solution* for the row i with $i \geq t$ if the matrix with rows $(v_1, u_1), (v_2, u_2), \ldots, (v_{t-1}, u_{t-1}), (v, u_i)$ generates a [n,t,d] code with non-zero weights from a set W. To each such vector we can associate a vector M whose length is equal to the number of intervals and whose coordinates state the number of the ones in the corresponding intervals. If $i = t$ we call the solution *real* otherwise it is called *possible*. All possible solutions strongly depend on the last real solution.

In the algorithm we use two types of equivalencies, one depending on the dimension of the code, the other on real solutions. Let y_1 and y_2 be two real solutions for the t-th row with corresponding codes C_{y_1} and C_{y_2}. These codes are generated by the first t rows of G_x. If $t < k_{out}$ we say that y_1 and y_2 are *equivalent up to extension* if $\sigma_1\sigma_2(C_{y_1}) = C_{y_2}$ for a permutation σ_1 of the first w coordinates and $\sigma_2 \in Aut(C_0)$. If $t = k_{out}$ we have the usual equivalence between linear codes.

We use the following back-track algorithm to find all real solutions for the second row (with the first row fixed) and all real solutions for the $(t+1)$-th row (where the first t rows are fixed) using all possible solutions for the $(t+1)$-th row with fixed $t-1$ rows.

```
var
tree:array  [1..k_out] of integer;
T:integer;

begin
    T:=1;
    tree[T]:=1;
    while T>1 then
   begin
     if (tree[T]>1) and (T<k_out) then
            begin
               tree[T]:=tree[T]-1;
               T:=T+1;
               Find all real solutions for the T-th row with a fixed
               T-1 row (a real solution tree[T-1]+1);
               tree[T]:=all inequivalent real solutions for row T;
```

```
            Find all possible solutions for T+1,T+2,...,k rows with
            fixed T-1 row;
          end
          else
             T:=T-1;
   end
end.
```

An important task of the back-track search is to find inequivalent real solutions in each step. We develop an algorithm using ideas from [5] and [23] which leads to a canonical labelling and produces also the order of the automorphism groups.

For more information the reader is refered to [6].

There are some specific restrictions for the construction of PTW codes. We have restrictions on the set of possible weights. Let C be a binary $[n,k]$ code with the even two weights w_1 and w_2, with $w_2 > w_1$. Then the residual code C_0 will have the following weights: $w_1/2$, $w_2/2$ and $w_2 - w_1/2$. Another restriction comes from the projectivity. In the last step the algorithm has to search only for real solutions which do not contain proportional columns. This fact has a strong impact on the complexity of the algorithm (see [6]).

6 Computational results

Table 5.9 in [8] contains information about known strongly regular graphs (see section 8 for the definition) with not more than 280 vertices. PTW codes of dimension at most 8 in the binary case, and of dimension at most 5 resp. 4 over a field with 3 resp. 4 elements give rise to such strongly regular graphs.

We use the method described in Section 5 which is implemented in the program 'Q-extension' to classify all PTW codes which correspond to strongly regular graphs in the table, except codes of dimension 8 and length greater than 68. Moreover we classify some PTW codes of dimension 4 over the field with 5 elements. Less than three days of CPU time on a 800MHz PC was needed to carry out all the computations.

The results on PTW codes are presented below in Table 1, 2, 3 and 4 for fields with 2, 3, 4 and 5 elements. We list the parameters of the codes, how far they are away from the Griesmer bound, the weight enumerators, the number of non-equivalent codes, the number of projective self-dual codes and the order of the automorphism groups. At several places some further information is included, for instance, known examples from [11] (one example) and additional information about classification results. We also indicate which codes are optimal.

The complete list of codes is available from the authors.

7 PTW codes and other combinatorial structures

This section contains an overview on some known relations between PTW codes and other combinatorial structures.

7.1 Two-weight codes and caps

A two-weight code with dual distance at least 4 corresponds to a cap in a projective space having exactly two intersection numbers with hyperplanes. Codes with parameters $[10, 4, 6]_3$, $[11, 5, 6]_3$, $[56, 6, 36]_3$, $[17, 4, 12]_4$ and $[78, 6, 56]_4$ are of this kind.

7.2 Two-weight codes and 2-designs

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a t-(v, k, λ) design, where t, v, k and λ are non-negative integers, if the following three conditions hold.

(1) $|\mathcal{P}| = v$.

(2) Every block $B \in \mathcal{B}$ is incident with precisely k points.

(3) Every t distinct points are together incident with precisely λ blocks.

By the support of a nonzero vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ we denote the set of indices of its non-zero coordinates, i.e., $\mathrm{supp}(x) = \{i | x_i \neq 0\}$.

We define the (*support*) *design* of a code of length n for a given non-zero weight w in the following way. The points are the n coordinate indices and the blocks consist of the supports of all codewords of weight w. In Table 5 we list all PTW codes considered so far which have a supported 2-design.

7.3 Other specific cases

1. A 2-(v, k, λ) design has *symmetric difference property*, or is an SDP design, if the symmetric difference of any two blocks is either a block or the complement of a block. PTW codes with parameters $[27, 6, 12]_2$, $[28, 6, 12]_2$ and $[35, 6, 16]_2$ give rise to the construction of 2-(28,12,11), 2-(36,16,12) and 2-(64,28,12) SDP designs (see [26]). The designs with symmetric difference property provide a number of links between PTW codes, Reed-Muller codes, difference sets, bent functions and point sets in projective spaces having prescribed intersection numbers with hyperplanes.

2. Codes with the same number of words for each weight were studied by Langevin and Zanotti [21] (see also [4]). Here we classify ternary $[20, 4, 12]$-codes with weight distribution $A_0 = 1, A_{12} = A_{15} = 40$. There are exactly four inequivalent codes. Two of them are not cyclic. It follows that there are *balanced weight distribution* (BWD) *codes* which can not be constructed via a subgroup of the multiplicative group $\mathbb{F}_{q^k}^*$.

3. A code with parameters $[39, 4, 30]_5$ was found in [3]. Other examples with the same parameters were discovered by Van Eupen and Tonchev in [27]. They used $[39, 4, 30]_5$ and $[36, 4, 25]_5$ PTW codes to construct a reversible abelian Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$.

8 PTW codes and strongly regular graphs

There are strong connections between projective two-weight codes and *strongly regular graphs* (SRG). One such connection is given by Delsarte [12]. 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 $\Gamma(C)$ as follows. The vertices of the graph are identified with the $v = q^k$ codewords and two vertices corresponding to x and y are adjacent iff $d(x, y) = w_1$. Then $\Gamma(C)$ is a strongly regular graph [12, Theorem 2].

Another construction is given by Calderbank and Kantor in [11]. As vertices one takes the points of the k-dimensional vector space $\mathbb{F}_q^k$. Each such vector defines a linear combination of the (n-dimensional) row vectors of a generator matrix G of a projective two-weight code C corresponding to a codeword. Two different 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 [11, Theorems 3.1 and 3.2] with the following parameters [11, Corollary 3.7]:

$$\begin{aligned} v &= q^k \,, && (1) \\ K &= n(q-1)\,, && (2) \\ \lambda &= K^2 + 3K - q(w_1 + w_2) - Kq(w_1 + w_2) + q^2 w_1 w_2\,, && (3) \\ \mu &= \frac{q^2 w_1 w_2}{q^k} = K^2 + K - Kq(w_1 + w_2) + q^2 w_1 w_2\,. && (4) \end{aligned}$$

A relation between the two graphs $\Gamma(C)$ and $\Gamma'(C)$ can be obtained from [11, Theorem 5.7] and the definition of the projective dual in Section 4. For a given code C and its projective dual C^*, the graph $\Gamma(C)$ is isomorphic to $\Gamma'(C^*)$. Hence, for projective self-dual codes, the two constructions lead to isomorphic graphs.

In Table 6, 7, 8 and 9 we present results for strongly regular graphs obtained from PTW codes over $\mathbb{F}_q$ for $q = 2, 3, 4$ and 5. We list SRG and PTW parameters as well as the size of automorphism groups and the 2-rank of the graphs.

9 Open problems

(1) Does there exist a two-weight code over F_q of length $n = 3(q^2 + 1)/2$ with weights $3q(q-1)/2$ and $(3q-1)q/2$?
For $q = 3$ two such codes exist and for $q = 5$ there are 8.
(2) Does a $[430, 7, 320]$ code over $\mathbb{F}_4$ exist? If it exists it does not have an automorphism of order 43.

These open problems were stated by H. Ward and R. Hill during the "Euro Workshop on Optimal Codes and Related Topics" in Sunny Beach, Bulgaria, 2001.

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

The authors would like to thank the anonymous referees for valuable remarks and suggestions, and in particular one of the referees for giving a short proof of Lemma 4.

References

[1] A. Barlotti. Un'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital. Ser. III*, 10:498–506, 1955.

[2] A. Bonisoli. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combinatoria*, 18:181–186, 1983.

[3] I. Boukliev. Some new optimal linear codes over F_5. In *Proc. 25th Spring Conference of the Union of Bulgarian Mathematicians, Kazanlak, Bulgaria*, pages 81–85, 1996.

[4] I. Boukliev. Cyclotomic description of some optimal codes. In *Proceedings of the International Workshop ACCT, Pskov, Russia*, pages 52–56, 1998.

[5] I. Bouyukliev. An algorithm for finding isomorphisms of codes. In *Proceedings of the International Workshop OCRT, Sunny Beach, Bulgaria*, pages 35–41, 2001.

[6] I. Bouyukliev and J. Simonis. Some new results for optimal ternary linear codes. *IEEE Trans. Inform. Theory*, 48:981–985, 2002.

[7] A.E. Brouwer. Some new two-weight codes and strongly regular graphs. *Discrete Applied Math.*, 10:111–114, 1985.

[8] A.E. Brouwer. *Strongly regular graphs.* CRC Press, New York, 1996.

[9] A.E. Brouwer. *Bounds on the size of linear codes.* Elsevier, Amsterdam etc., 1998. Online version: http://www.win.tue.nl/math/dw/voorlincod.html.

[10] A.E. Brouwer and E. van Eupen. The correspondence between projective codes and 2-weight codes. *Designs, Codes and Cryptography*, 11:262–266, 1997.

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

[12] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Math.*, 3:47–64, 1972.

[13] S. Dodunekov. Minimal block length of a linear q-ary code with specified dimension and code distance. *Problems Inform. Transmission*, 20:239–249, 1984.

[14] S. Dodunekov and J. Simonis. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998. 23 pp. (electronic).

[15] S.M. Dodunekov and V.I. Jorgov. Distribution of weights of irreducible cyclic codes and strongly regular graphs. *Problems Inform. Transmission*, 16:105–110, 1980.

[16] A. Faldum and W. Willems. A characterization of MMD codes. *IEEE Trans. Inform. Theory*, 44:1555–1558, 1998.

[17] J.H. Griesmer. A bound for error-correcting codes. *I.B.M. J. Res. Develop.*, 4:532–542, 1960.

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

[19] R. Hill. Caps and codes. *Discrete Math.*, 22:111–137, 1978.

[20] I. Landjev. PhD thesis, 2002.

[21] P. Langevin and J.P. Zanotti. Linear codes with balanced weight distribution. *Appl. Algebra Eng. Comm. Comput.*, 6:299–307, 1995.

[22] R.J. McEliece. A class of two-weight codes. *J. P. L. Space Programs Summary, 37-41, Vol.IV*, pages 264–266.

[23] B.D. McKay. Practical graph isomorphism. *Congressus Numerantium*, 30:45–87, 1981.

[24] B.D. McKay. *nauty* user's guide (version 1.5). Technical Report TR-CS-90-02, Computer Science Department, Australian National University, 1990.

[25] G. Panella. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital. Ser. III*, 10:507–513, 1955.

[26] V.D. Tonchev. The uniformly packed binary [27,21,3] and [35,29,3] codes. *Discrete Math.*, 149:283–288, 1996.

[27] M. van Eupen and V. Tonchev. Linear codes and the existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$. In *Proc. ACCT'96, Sozopol, Bulgaria*, pages 295–301, 1996.

[28] J.H. Van Lint and A. Schrijver. Construction of strongly regular graphs, two-weight codes and partialgeometries by finite fields. *Combinatorica*, 1:63–75, 1981.

[29] H.C.A. van Tilborg. *Uniformly packed codes.* PhD thesis, Eindhoven University of Technology, 1976.

[30] W. Willems. *Codierungstheorie.* deGruyter, Berlin, 1999.

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 [11] (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	[26]
$[28,6,12]_2$	3	$1+28z^{12}+35z^{16}$	7	7	$24, 120, 84, 96, 1344, 384, 40320,$	SU2	[26]
$[30,8,8]_2$	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	$72, 1440,$		[18]
$[16,4,9]_3$	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	$15840,$		[19]
$[56,6,36]_3$	0 *	$1+616z^{36}+112z^{45}$	1	1	$80640,$		[19]

Table 3: Quaternary projective two-weight codes. Legend: see Table 1.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$[6, 3, 4]_4$	0 *	$1 + 45z^4 + 18z^6$	1	1	$2160,$		
$[7, 3, 4]_4$	1	$1 + 21z^4 + 42z^6$	1	1	$1008,$	CY4	
$[9, 3, 6]_4$	0 *	$1 + 36z^6 + 27z^8$	1	1	$1296,$	RT3	
$[10, 4, 4]_4$	3	$1 + 30z^4 + 225z^8$	1	1	$259200,$	CY4	
$[15, 4, 8]_4$	3	$1 + 45z^8 + 210z^{12}$	2	2	$2160, 120960,$	CY4	
$[17, 4, 12]_4$	0 *	$1 + 204z^{12} + 51z^{16}$	1	1	$48960,$		[20]
$[20, 4, 12]_4$	3	$1 + 60z^{12} + 195z^{16}$	7	7	$1080, 432, 288, 4320, 576, 720, 120,$	CY4	
$[25, 4, 16]_4$	3	$1 + 75z^{16} + 180z^{20}$	19	19	$144, 576, 288, 2160, 48, 72, 360, 43200, 24^2, 18, 12^2, 60, 36^3, 120, 96,$	CY4	
$[30, 4, 20]_4$	2	$1 + 90z^{20} + 165z^{24}$	68	66	$18^7, 72^2, 24^8, 6^{20}, 3^4, 12^{11}, 288, 144^2, 48^2, 36^2, 216, 4320, 600, 30, 120, 180^2, 720, 9,$	CY4	
$[34, 4, 24]_4$	1 *	$1 + 153z^{24} + 102z^{28}$	84	38	$6^{24}, 3^{32}, 12^7, 18^9, 72^3, 48, 144, 24^3, 36^2, 120, 204,$		
$[35, 4, 24]_4$	2	$1 + 105z^{24} + 150z^{28}$	231	179	$12^{25}, 3^{78}, 6^{68}, 48^4, 72^5, 36^{10}, 24^7, 21, 288, 720, 60^3, 18^9, 216, 1200, 96, 144^2, 9^8, 108, 30, 63, 90^2, 42,$	CY4	
$[40, 4, 28]_4$	2	$1 + 120z^{28} + 135z^{32}$	481	315	$3^{239}, 6^{129}, 9^7, 12^{42}, 48^6, 18^{12}, 36^{10}, 24^{16}, 72^2, 60, 432, 5760, 1152, 576^2, 180^2, 30^2, 144^2, 96, 120^2, 480, 384, 155520,$	CY4	

Table 4: Projective two-weight codes over $\mathbb{F}_5$. Legend: see Table 1.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$[12,4,5]_5$	4	$1+48z^5+576z^{10}$	1	1	$460800,$	CY4	
$[18,4,10]_5$	4	$1+72z^{10}+552z^{15}$	1	1	$2880,$	CY4	
$[24,4,15]_5$	4	$1+96z^{15}+528z^{20}$	7	7	$160,192,128,576,96,$ $3840,4608,$	CY4	
$[26,4,20]_5$	0 *	$1+520z^{20}+104z^{25}$	1	1	$124800,$	RT2	[20]
$[30,4,20]_5$	4	$1+120z^{20}+504z^{25}$	38	38	$8^8,4,32^5,40,16^4,$ $480,48^6,96^2,80,128,$ $288,400,384,9600,160,$ $64,240,800,$	CY4	
$[39,4,30]_5$	0 *	$1+468z^{30}+156z^{35}$	8	8	$4,16,24^2,72,12,$ $48^2,$		

Table 5: Projective two-weight codes and 2-designs

parameters	2-(v,k,λ)
$[5,4,2]_2$	2-(5,2,1)
$[5,4,2]_2$	2-(5,4,3)
$[10,4,6]_3$	2-(10,6,20)
$[10,4,6]_3$	2-(10,9,16)
$[11,5,6]_3$	2-(11,6,36)
$[11,5,6]_3$	2-(11,9,72)
$[56,6,36]_3$	2-(56,36,252)
$[56,6,36]_3$	2-(56,45,72)
$[6,3,4]_4$	2-(6,4,18)
$[6,3,4]_4$	2-(6,6,18)
$[7,3,4]_4$	2-(7,4,6)
$[7,3,4]_4$	2-(7,6,30)
$[9,3,6]_4$	2-(9,6,15)
$[9,3,6]_4$	2-(9,8,21)
$[15,4,8]_4$	2-(15,8,12)
$[15,4,8]_4$	2-(15,12,132)
$[17,4,12]_4$	2-(17,12,99)
$[17,4,12]_4$	2-(17,16,45)
$[26,4,20]_5$	2-(26,20,304)
$[26,4,20]_5$	2-(26,25,96)

Table 6: 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 7: 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,

Table 8: Strongly regular graphs corresponding to quaternary PTW codes. For the cases marked with (*), the full data concerning $|Aut(\Gamma)|$ and 2-rank(Γ) can be found at `http://www.moi.math.bas.bg/~iliya`.

SRG parameters	PTW parameters	$\|Aut(\Gamma)\|$	2-rank(Γ)
$(64, 18, 2, 6)$	$[6, 3, 4]_4$	138240,	14,
$(64, 21, 8, 6)$	$[7, 3, 4]_4$	64512,	64,
$(64, 27, 10, 12)$	$[9, 3, 6]_4$	3317760,	64,
$(256, 30, 14, 2)$	$[10, 4, 4]_4$	9223372036854775807,	30,
$(256, 45, 16, 6)$	$[15, 4, 8]_4$	30965760,30965760,	256,256,
$(256, 51, 2, 12)$	$[17, 4, 12]_4$	12533760,	256,
$(256, 60, 20, 12)$	$[20, 4, 12]_4$	1105920,1105920,73728,1105920,	38,38,42,38,
		147456,3686400,30720,	40,36,42,
$(256, 75, 26, 20)$	$[25, 4, 16]_4$	368640,147456,73728,11059200,	256,256,256,256,
		12288,147456,368640,11059200,	256,256,256,256,
		6144,4608,3072,15360,	256,256,256,256,
		9216,18432,9216,3072,	256,256,256,256,
		6144,30720,24576,	256,256,256,
$(256, 90, 34, 30)$	$[30, 4, 20]_4$	(*)	(*)
$(256, 102, 38, 42)$	$[34, 4, 24]_4$	(*)	(*)
$(256, 105, 44, 42)$	$[35, 4, 24]_4$	(*)	(*)

Table 9: Strongly regular graphs corresponding to PTW codes over $\mathbb{F}_5$.

SRG parameters	PTW parameters	$\lvert Aut(\Gamma)\rvert$	2-rank(Γ)
$(625, 48, 23, 2)$	$[12, 4, 5]_5$	9223372036854775807,	625,
$(625, 72, 25, 6)$	$[18, 4, 10]_5$	1800000,	625,
$(625, 96, 29, 12)$	$[24, 4, 15]_5$	100000,120000,80000,360000,	625,625,625,625,
		60000,2400000,2880000,	625,625,625,
$(625, 104, 3, 20)$	$[26, 4, 20]_5$	78000000,	625,
$(625, 120, 35, 20)$	$[30, 4, 20]_5$	5000,2500,5000,20000,	95,95,95,95,
		5000,5000,5000,20000,	95,95,95,95,
		25000,5000,5000,5000,	95,95,95,95,
		10000,300000,30000,60000,	95,95,91,91,
		50000,10000,10000,30000,	91,95,95,91,
		10000,30000,30000,60000,	93,95,95,91,
		30000,30000,80000,20000,	98,91,91,98,
		180000,250000,240000,6000000,	91,91,98,85,
		100000,20000,20000,40000,	96,98,98,98,
		150000,500000,	96,92,
$(625, 156, 29, 42)$	$[39, 4, 30]_5$	2500,10000,15000,45000,	625,625,625,625,
		7500,15000,30000,30000,	625,625,625,625,