Quadratic Residue codes, rank three groups and PBIBDs

Minjia Shi, Shukai Wang, Tor Helleseth, Patrick Solé

Quadratic Residue codes, rank three groups and PBIBDs

Minjia Shi[*], Shukai Wang[†], Tor Helleseth[‡], Patrick Solé[§¶]

Abstract

The automorphism group of the Zetterberg code Z of length 17 (also a quadratic residue code) is a rank three group whose orbits on the coordinate pairs determine two strongly regular graphs equivalent to the Paley graph attached to the prime 17. As a consequence, codewords of a given weight of Z are the characteristic vectors of the blocks of a PBIBD with two associate classes of cyclic type. More generally, this construction of PBIBDs is extended to quadratic residue codes of length $\equiv 1 \pmod 8$, to the adjacency codes of triangular and lattice graphs, and to the adjacency codes of various rank three graphs. A remarkable fact is the existence of 2-designs held by the quadratic residue code of length 41 for code weights 9 and 10.

Keywords: Rank three groups, cyclic codes, Strongly Regular Graphs

AMS Math Sc. Cl. (2010): 94 B15, 05 E30, 62K10

1 Introduction

There is an old and well-known connection between codes and designs [7]. Many classical codes hold 2-designs, and some of them, like the Golay codes,

[*]smjwcl.good@163.com

[†]wangshukai_2017@163.com

[‡]Tor.Helleseth@uib.no

[§]sole@enst.fr

[¶]MS and SW are with Anhui University, Hefei, China.TH is with Bergen University, Bergen, Norway. PS is with Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France.

5-designs. The relations between Partially Balanced Incomplete Block designs (PBIBD for short) and codes, have been documented in several publications [6, 14, 15, 16, 18].

PBIBDs are of practical use in statistics [1, 4], and at the origin of the study of association schemes in algebraic combinatorics.

In this note, we give an example of a classical code that constructs eight such designs, the parameters of which are not all in the tables of [4]. The corresponding two-class association scheme is the metric scheme of the Paley strongly regular graph (SRG) [5] on 17 vertices. The proof relies on the fact that the automorphism group of the Zetterberg code of length 17 is a rank three group. These groups were historically involved in the classification of finite simple groups [8]. They were also employed to construct SRG's [5]. Chapter 11 of [5] is dedicated to them.

This symmetry argument is generalized in the following way. Any binary code left invariant under a rank three group holds PBIBDs. An infinite class of examples is obtained by considering quadratic residue codes of length $\equiv 1 \pmod 8$. This requires the determination of their automorphism group from [13, Chap. 17]. Of special interest is the quadratic residue code of length 41, whose codewords of length 9 hold a $2-(41,9,18)$ design; the codewords of length 10 holding a $2-(41,10,72)$ design. The existence of these designs cannot be explained by the Assmus-Mattson theorem, nor by the direct group action argument of [13, p. 308]. It can however, be given a proof by using the techniques of [16, §3.5].

Examples of rank three graphs of combinatorial interest include the triangular and lattice graphs. These graphs are diameter two instances of the Johnson and Hamming graphs, respectively. The 2-designs arising in these graphs can be used to construct unequal error protection codes [15, 16]. More examples are found by combining the information in [5, §11.5], and in [12].

The material is arranged in the following way. The next section collects the definitions and notions required to understand the following sections. Section 3 studies the example of the Zetterberg code of length 17 in great detail. Section 4 generalizes this example to quadratic residue codes, adjacency codes of triangular codes, lattice codes and other rank three graphs. Section 5 addresses the adjacency codes of various SRGs. Section 6 concludes the article.

2 Background material

2.1 Permutation groups

Let G be a permutation group acting on a finite set X. We will denote by x^G the unique orbit under the group G that contains $x \in X$. The group G will be called a *rank three group* if and only if it is transitive on X and any one point stabilizer has three orbits on X including the trivial one. In other words, it has three orbits (classical called *orbitals*) on the cartesian product $X \times X$ including the diagonal. The transposition induces a pairing on orbitals. If an orbital O is self-paired then the graph (X, O) is symmetric and strongly regular.

2.2 Association schemes

An *association scheme* on a set X with s classes is a partition of the cartesian product $X \times X = \cup_{i=0}^{s} R_i$ with the following properties.

1. $R_0 = \{(x, x) \mid x \in X\}$;
2. $(x, y) \in R_k$ if and only if $(y, x) \in R_k$;
3. If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$, is an integer p_{ij}^k that depends on i, j, k but not on the special choice of x and y.

A consequence of axiom 3 is that each graph R_i is regular of degree v_i, say. In this note, we will restrict ourselves to *two-class association schemes* that is to say the case of $s = 2$. In that case the graph (X, R_1) is called *strongly regular* (shortly SRG). An association scheme is *cyclic* if it is translation invariant under a cyclic group. In other words, X is the additive group of a residue class ring $\mathbb{Z}_v$ for some integer v, and the relations are of the form

$$(x, y) \in R_k \Leftrightarrow x - y \in E_k$$

for some $E_k \subset X$.

2.3 Designs

A PBIBD with two associate classes of parameters $(b, v, k, r, \lambda_1, \lambda_2)$ is an incidence structure $(\mathcal{P}, \mathcal{B}, I)$ satisfying the following axioms.

1. The set $\mathcal{P}$ has v points;
2. The set $\mathcal{B}$ has b blocks;
3. Each block is incident to k points;
4. Each point is incident to r blocks;
5. There is a two-class association scheme on $\mathcal{P}$ such that two i-associate points are both incident to exactly λ_i blocks for $i = 1, 2$.

A similar definition exists for s associates but in this note we will focus on the case $s = 2$. Note that the case $\lambda_1 = \lambda_2 = \lambda$ is that of a $2-(v, k, \lambda)$ design. There is a classification of PBIBD into types depending if the association scheme is

1. group divisible;
2. triangular;
3. Latin square type;
4. cyclic;
5. partial geometry type;
6. miscellaneous.

2.4 Codes

Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field of order 2. A binary code of length n is a $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$. The *weight* of a vector of $\mathbb{F}_2^n$ is the number of its nonzero coordinates. The *weight distribution* of a code C is the sequence A_w of number of codewords of C of weight w. It is written in Magma [20] notation as the list with generic element $\langle w, A_w \rangle$ where w ranges over the weights of C. A binary code is *cyclic* if it is invariant under the cyclic shift. Cyclic codes are in one to one correspondence with ideals of the residue class ring $\mathbb{F}_2[x]/(x^n - 1)$. The generator polynomial of a cyclic code is the generator of the corresponding ideal. The *Quadratic residue codes* are the cyclic codes of

length p, which is an odd prime defined for $p \equiv \pm 1 \pmod 8$ by the generator polynomial of degree $\frac{p-1}{2}$

$$\prod_{r=1}^{\frac{p-1}{2}}(x - \alpha^{2r}),$$

where α is a primitive root of order p. Since 2 is a quadratic residue modulo an odd prime p, this polynomial is indeed in $\mathbb{F}_2[x]$. See [11, Chap.16] for background.

The *automorphism* group of a binary code of length n is a subgroup of the symmetric group on n coordinate places that leave the code wholly invariant.

3 The Zetterberg code

3.1 Construction

Let $q = 16$, and $K = \mathbb{F}_{q^2}$. Define $U = \{x \in K \mid x^{q+1} = 1\} = \langle \alpha \rangle$, where α is a primitive root of order 17 in the multiplicative group of K. The coordinates of the codewords of the binary Zetterberg code Z are naturally indexed by U. The columns of its parity-check matrix can be identified with elements of U under the standard isomorphism $K \cong (\mathbb{F}_2)^8$. Thus $H = [1, \alpha, \alpha^2, \ldots, \alpha^{16}]$. The Zetterberg code is in fact a classical cyclic code [11, p. 206], [2, p. 161]. Its parameters are $[17, 9, 5]$ and its weight distribution is computed in Magma [20] as

$$[\langle 0, 1\rangle, \langle 5, 34\rangle, \langle 6, 68\rangle, \langle 7, 68\rangle, \langle 8, 85\rangle,$$
$$\langle 9, 85\rangle, \langle 10, 68\rangle, \langle 11, 68\rangle, \langle 12, 34\rangle, \langle 17, 1\rangle].$$

3.2 Symmetry

The permutation group G of Z is of order $2^3 \times 17$ generated by the shift $x \mapsto \alpha x$ and the squaring $x \mapsto x^2$. Consider the group action on the set P of pairs of indices. Define the sets

- $A = \{1, 2\}^G$,
- $B = \{1, 8\}^G$.

It can be checked that A and B are disjoint, and both with size $68 = \binom{17}{2}/2$. Thus their union is $P = A \bigcup B$.

Theorem 1 *For every weight $w \in \{5, 6, \ldots, 12\}$ of Z, there are two constants λ and μ such that each pair in A (resp. B) is covered by λ (resp. μ) codewords of Z of weight w. Further $68(\lambda + \mu) = A_w\binom{w}{2}$.*

Proof. The first statement is immediate by group action. The second statement is immediate by double counting. ∎

The constants can be computed in Magma and are listed in the following table.

Table 1: The value of λ, μ

w	5	6	7	8	9	10	11	12
λ	2	7	9	16	21	21	27	16
μ	3	8	12	19	24	24	28	17

Theorem 2 *The graph on $[1..17]$ with edge set A (resp. B) is strongly regular, and isomorphic to the Paley graph attached to the prime 17.*

Proof. Write $A' = (1, 2)^G$ and $B' = (1, 8)^G$. It can be checked exhaustively that

$$\{\{x, y\} \mid (x, y) \in A'\} = A,$$

and likewise,

$$\{\{x, y\} \mid (x, y) \in B'\} = B.$$

This means that G is a rank three group and therefore the said graphs form a pair of complementary SRGs by [5, §1.1.5]. By [19], there is a unique SRG on 17 vertices. It is the Cayley graph on the cyclic group $\mathbb{Z}_{17}$ with generating set the quadratic residues. ∎

We conclude this section with the following result.

Theorem 3 *For any weight w of Z, the codewords of weight w hold a PBIBD of cyclic type with two associates of parameters*

$$v = 17,\ b = A_w,\ r = \frac{A_w w}{17},\ \lambda,\ \mu,$$

where the constants λ, μ, depend on w and are given in Table 1.

Proof. The design property follows by Theorem 1. The two-class association scheme is the one attached to the SRG of Theorem 2. Since this graph is circulant, the scheme is cyclic. Since G is transitive the replication number r is well-defined, and obtained from the fact that each block has size w. ∎

Remark 1 The parameters for $w \neq 5, 8, 9$ do not appear in Table VII-A of [4, p. 448].

4 Generalizations

The following result is immediate. Its proof is omitted.

Theorem 4 *If C is a binary code with automorphism group G that is a rank three group, then codewords of given weight hold a PBIBD.*

A case of application would be the code spanned by the adjacency matrix of the SRG attached to such a group. See Table 10 A in [8].

In the following examples, the groups of the codes involved are either rank three or doubly transitive.

4.1 Quadratic residue codes

Observing that Z is nothing else than the quadratic residue code of length 17, we generalize the observation that the group G is rank three to some quadratic residue codes.

Theorem 5 *If C is a binary quadratic residue code of length which is a prime $p \neq 7, 23$, then the permutation group of C is a rank three group.*

Proof. (sketch) By [13, chap. 17, Th. 6.7 (v) a.], the automorphism group of the extended quadratic residue code of length $p + 1$ is, under that hypothesis, isomorphic to $PSL(2, p)$. By [11, chap. 16, Th. 10], that group is generated by S, V, T where S is the cyclic shift. The other two generators V, T are given by $V : x \mapsto \rho^2 x$ (where $\mathbb{F}_p^\times = \langle \rho \rangle$) and $T : x \mapsto -\frac{1}{x}$.

We see that they fix the origin. Hence they generate the automorphism group of C. It can be checked that the two non-trivial orbits are, respectively,

the set of quadratic residues, and the set of non-residues. ∎

What happens when $p = 7$ or $p = 23$ is that the permutation group of C is 2-transitive. In particular, when $p = 23$ that group is the Matthieu group M_{23}, which is even four-transitive.

Note that when $p \equiv -1 \pmod 8$, the quadratic residues do not lead to a Paley graph, but give a symmetric Paley-Hadamard design. Thus the result in this paragraph can be used to generate PBIBDs only when $p \equiv 1 \pmod 8$.

For $n = 41$ we find 2-designs in weights $9, 10$ and their complements $31 = 41 - 10, 32 = 41 - 9$. None of these designs can be explained by the standard group action argument of [13, p. 308], or by the Assmus-Mattson theorem [11, Chap. 6, Th. 29]. It can be explained by the theorems of [16, §3.5], in particular Theorem 3.5.1 for weight 9, and Theorem 3.5.3 for weight 10. By similar arguments the codes invariant under Higman-Sims, or Hoffman Singleton in [17] can be shown to hold 2-designs. It would be interesting to know if the 3-design of [3] can be explained in the same way. The weight distribution of the code is $[\langle 0,1\rangle, \langle 9,410\rangle, \langle 10,1312\rangle, \langle 11,3034\rangle, \langle 12,7585\rangle, \langle 13,16605\rangle, \langle 14,33210\rangle, \langle 15,60024\rangle, \langle 16,97539\rangle, \langle 17,146370\rangle, \langle 18,195160\rangle, \langle 19,232060\rangle, \langle 20,255266\rangle, \langle 21,255266\rangle, \langle 22,232060\rangle, \langle 23,195160\rangle, \langle 24,146370\rangle, \langle 25,97539\rangle, \langle 26,60024\rangle, \langle 27,33210\rangle, \langle 28,16605\rangle, \langle 29,7585\rangle, \langle 30,3034\rangle, \langle 31,1312\rangle, \langle 32,410\rangle, \langle 41,1\rangle]$.

The parameters of the PBIBD are as follows.

w	9	10	11	12	13	14	15	16	17
λ	18	72	203	610	1575	3681	7668	14256	24234
μ	18	72	204	611	1584	3690	7704	14292	24318

w	18	19	20	21	22	23	24
λ	36372	48330	59084	65310	65310	60172	49224
μ	36456	48456	59210	65436	65436	60256	49308

w	25	26	27	28	29	30	31	32
λ	35667	23772	14211	7650	3755	1609	744	248
μ	35703	23808	14220	7659	3756	1610	744	248

4.2 Triangular graphs

The triangular graph, of order $\binom{n}{2}$, is the line graph of the complete graph K_n. The graph is distance transitive as being the Johnson graph $J(n, 2)$ as by [5, 1.2.2]. The adjacency code has parameters $[\binom{n}{2}, n-1]$, by [9, §4.1],

or by [16, Lemma 3.6.6]. For $n = 5$ to 12, the automorphism groups of the adjacency codes are all rank three except for $n = 6$, where the group is 2-transitive and we obtain 2-designs.

- $n = 5, [\langle 0, 1\rangle, \langle 4, 5\rangle, \langle 6, 10\rangle]$

w	4	6
λ	0	3
μ	1	4

- $n = 6, [\langle 0, 1\rangle, \langle 8, 15\rangle]$

  The code is the $[15, 4, 8]$ Simplex code. We obtain a $2-(15, 8, 4)$ design.

- $n = 7, [\langle 0, 1\rangle, \langle 6, 7\rangle, \langle 10, 21\rangle, \langle 12, 35\rangle]$

w	6	10	12
λ	0	4	10
μ	1	5	12

- $n = 8, [\langle 0, 1\rangle, \langle 12, 28\rangle, \langle 16, 35\rangle]$

w	12	16
λ	4	10
μ	6	12

- $n = 9, [\langle 0, 1\rangle, \langle 8, 9\rangle, \langle 14, 36\rangle, \langle 18, 84\rangle, \langle 20, 126\rangle]$

w	8	14	18	20
λ	0	4	20	35
μ	1	7	21	40

- $n = 10, [\langle 0, 1\rangle, \langle 16, 45\rangle, \langle 24, 210\rangle]$

w	16	24
λ	4	56
μ	8	60

- $n = 11, [\langle 0, 1\rangle, \langle 10, 11\rangle, \langle 18, 55\rangle, \langle 24, 165\rangle, \langle 28, 330\rangle, \langle 30, 462\rangle]$

w	10	18	24	28	30
λ	0	4	28	84	126
μ	1	9	36	84	140

- $n = 12, [\langle 0, 1\rangle, \langle 20, 66\rangle, \langle 32, 495\rangle, \langle 36, 462\rangle]$

w	20	32	36
λ	4	112	126
μ	10	120	140

- $n = 13, [\langle 0, 1\rangle, \langle 12, 13\rangle, \langle 22, 78\rangle, \langle 30, 286\rangle, \langle 36, 715\rangle, \langle 40, 1287\rangle, \langle 42, 1716\rangle]$

w	12	22	30	36	40	42
λ	0	4	36	144	330	462
μ	1	11	55	165	336	504

- $n = 14, [\langle 0, 1\rangle, \langle 24, 91\rangle, \langle 40, 1001\rangle, \langle 48, 3003\rangle]$

w	24	40	48
λ	4	180	792
μ	12	220	840

- $n = 15, [\langle 0, 1\rangle, \langle 14, 15\rangle, \langle 26, 105\rangle, \langle 36, 455\rangle, \langle 44, 1365\rangle, \langle 50, 3003\rangle, \langle 54, 5005\rangle, \langle 56, 6435\rangle]$

w	14	26	36	44	50	54	56
λ	0	4	44	220	660	1287	1716
μ	1	13	78	286	715	1320	1848

- $n = 16, [\langle 0, 1\rangle, \langle 28, 120\rangle, \langle 48, 1820\rangle, \langle 60, 8008\rangle, \langle 64, 6435\rangle]$

w	28	48	60	64
λ	4	264	1980	1716
μ	14	364	2002	1848

- $n = 17, [\langle 0, 1\rangle, \langle 16, 17\rangle, \langle 30, 136\rangle, \langle 42, 680\rangle, \langle 52, 2380\rangle, \langle 60, 6188\rangle, \langle 66, 12376\rangle, \langle 70, 19448\rangle, \langle 72, 24310\rangle]$

w	16	30	42	52	60	66	70	72
λ	0	4	52	312	1144	2860	5005	6435
μ	1	15	105	455	1365	3003	5148	6864

- $n = 18, [\langle 0, 1\rangle, \langle 32, 153\rangle, \langle 56, 3060\rangle, \langle 72, 18564\rangle, \langle 80, 43758\rangle]$

w	32	56	72	80
λ	4	364	4004	11440
μ	16	560	4368	12012

- $n = 19, [\langle 0, 1\rangle, \langle 18, 19\rangle, \langle 34, 171\rangle, \langle 48, 969\rangle, \langle 60, 3876\rangle, \langle 70, 11628\rangle, \langle 78, 27132\rangle, \langle 84, 50388\rangle, \langle 88, 75582\rangle, \langle 90, 92378\rangle]$

w	18	34	48	60	70	78	84	88	90
λ	0	4	60	420	1820	5460	12012	19448	24310
μ	1	17	136	680	2380	6188	12376	20020	25740

- $n = 20, [\langle 0, 1\rangle, \langle 36, 190\rangle, \langle 64, 4845\rangle, \langle 84, 38760\rangle, \langle 96, 125970\rangle, \langle 100, 92378\rangle]$

w	36	64	84	96	100
λ	4	480	7280	31824	24310
μ	18	846	8568	32032	25740

- $n = 21, [\langle 0, 1\rangle, \langle 20, 21\rangle, \langle 38, 210\rangle, \langle 54, 1330\rangle, \langle 68, 5985\rangle, \langle 80, 20349\rangle, \langle 90, 54264\rangle, \langle 98, 116280\rangle, \langle 104, 203490\rangle, \langle 108, 293930\rangle, \langle 110, 352716\rangle]$

w	20	38	54	68	80	90	98	104	108	110
λ	0	4	68	544	2720	9520	24752	49504	75582	92378
μ	1	19	171	969	3876	11628	27132	50388	77792	97240

- $n = 22, [\langle 0, 1\rangle, \langle 40, 231\rangle, \langle 72, 7315\rangle, \langle 96, 74613\rangle, \langle 112, 319770\rangle, \langle 120, 646646\rangle]$

w	40	72	96	112	120
λ	4	612	12240	74256	167960
μ	20	1140	15504	77520	175032

- $n = 23, [\langle 0, 1\rangle, \langle 22, 23\rangle, \langle 42, 253\rangle, \langle 60, 1771\rangle, \langle 76, 8855\rangle, \langle 90, 33649\rangle, \langle 102, 100947\rangle, \langle 112, 245157\rangle, \langle 120, 490314\rangle, \langle 126, 817190\rangle, \langle 130, 1144066\rangle, \langle 132, 1352078\rangle]$

w	22	42	60	76	90	102	112	120	126	130	132
λ	0	4	76	684	3876	15504	46512	108528	201552	293930	352716
μ	1	21	210	1330	5985	20349	54264	116280	203490	302328	369512

4.3 Lattice graphs

The lattice graph of order m^2 is the line graph of the complete bipartite graph $K_{m,m}$. It can be seen to be the same as the Hamming graph $H(2, m)$. Thus it is distance transitive [5, 1.2.3]. The code has parameters $[m^2, 2(m-1), 2(m-1)]$ by [10].

Proposition 1 *The minimum weight codewords hold a* $2-(m^2, 2(m-1), m-2, 2)$ *PBIBD.*

Proof. The minimum weight vectors are the m^2 row vectors of the adjacency matrix. The support $s(z)$ of the row $r(z)$ indexed by z are the graph vertices at distance 1 from z. Given a pair of position $\{x, y\}$, the number of z such that $\{x, y\} \subset s(z)$ is equal to the number of z's at distance 1 from both x and y. This number in turn by strong regularity depend only on the distance of x to y. Thus it equals $m - 2$ or 2. ∎

- $m = 5, [\langle 0, 1\rangle, \langle 8, 25\rangle, \langle 10, 20\rangle, \langle 12, 100\rangle, \langle 14, 100\rangle, \langle 20, 10\rangle]$

w	8	10	12	14	20
λ	2	2	18	30	6
μ	3	5	24	31	7

- $m = 6, [\langle 0, 1\rangle, \langle 10, 36\rangle, \langle 12, 30\rangle, \langle 16, 225\rangle, \langle 18, 440\rangle, \langle 20, 225\rangle, \langle 24, 30\rangle, \langle 26, 36\rangle, \langle 36, 1\rangle]$

w	10	12	16	18	20	24	26	36
λ	2	2	40	104	65	12	18	1
μ	4	6	44	108	69	16	20	1

- $m = 7, [\langle 0, 1\rangle, \langle 12, 49\rangle, \langle 14, 42\rangle, \langle 20, 441\rangle, \langle 22, 490\rangle, \langle 24, 1225\rangle, \langle 26, 1470\rangle, \langle 28, 70\rangle, \langle 32, 294\rangle, \langle 42, 14\rangle]$

w	12	14	20	22	24	26	28	32	42
λ	2	2	70	90	250	395	20	120	10
μ	5	7	75	115	300	410	30	136	11

- $m = 8, [\langle 0, 1\rangle, \langle 14, 64\rangle, \langle 16, 56\rangle, \langle 24, 784\rangle, \langle 26, 896\rangle, \langle 30, 3136\rangle, \langle 32, 6510\rangle, \langle 34, 3136\rangle, \langle 38, 896\rangle, \langle 40, 784\rangle, \langle 48, 56\rangle, \langle 50, 64\rangle, \langle 64, 1\rangle]$

w	14	16	24	26	30	32	34	38	40	48	50	64
λ	2	2	102	132	630	1555	826	300	298	30	38	1
μ	6	8	126	188	690	1615	886	356	322	36	42	1

- $m = 9, [\langle 0, 1\rangle, \langle 16, 81\rangle, \langle 18, 72\rangle, \langle 28, 1296\rangle, \langle 30, 1512\rangle, \langle 36, 7308\rangle, \langle 38, 9072\rangle, \langle 40, 15876\rangle, \langle 42, 21168\rangle, \langle 44, 2268\rangle, \langle 48, 6048\rangle, \langle 54, 168\rangle, \langle 58, 648\rangle, \langle 72, 18\rangle]$

w	16	18	28	30	36	38	40	42	44	48	54	58	72
λ	2	2	140	182	1414	1932	3430	5390	630	2072	70	322	14
μ	7	9	196	287	1449	2114	3920	5684	791	2240	91	365	15

- $m = 10, [\langle 0, 1\rangle, \langle 18, 100\rangle, \langle 20, 90\rangle, \langle 32, 2025\rangle, \langle 34, 2400\rangle, \langle 40, 420\rangle, \langle 42, 14400\rangle, \langle 44, 18900\rangle, \langle 48, 44100\rangle, \langle 50, 97272\rangle, \langle 52, 44100\rangle, \langle 56, 18900\rangle, \langle 58, 14400\rangle, \langle 60, 420\rangle, \langle 66, 2400\rangle, \langle 68, 2025\rangle, \langle 80, 90\rangle, \langle 82, 100\rangle, \langle 100, 1\rangle]$

w	18	20	32	34	40	42	44	48	50
λ	2	2	184	240	56	2464	3500	9408	23408
μ	8	10	288	416	112	2688	4116	10192	24220

w	52	56	58	60	66	68	80	82	100
λ, μ	11172	5768	4768	140	1008	913	56	66	1
λ, μ	11956	6384	4992	196	1184	1017	64	72	1

5 Various SRGs

In the following examples, we have proceeded as follows. We have computed the $\mathbb{F}_2$-linear span of various SRGs from [12]. If the automorphism group of that code is a rank three group, then we have computed the parameters of the attached PBIBD. Some information on the graphs can be inferred from [5, §11.5].

- $n = 9, [\langle 0, 1\rangle, \langle 4, 9\rangle, \langle 6, 6\rangle]$
  The SRG is a lattice graph, equivalent to the Paley graph with the same parameters.

w	4	6
λ	1	2
μ	2	3

- $n = 10, [\langle 0, 1\rangle, \langle 3, 10\rangle, \langle 4, 15\rangle, \langle 5, 12\rangle, \langle 6, 15\rangle, \langle 7, 10\rangle, \langle 10, 1\rangle]$
  The SRG is the celebrated Petersen graph.

w	3	4	5	6	7
λ	0	2	2	5	4
μ	1	2	4	5	5

- $n = 16, [\langle 0, 1\rangle, \langle 6, 16\rangle, \langle 8, 30\rangle, \langle 10, 16\rangle, \langle 16, 1\rangle]$
  The two SRGs $(16, 6, 2, 2)$ have equivalent adjacency codes, both with a doubly transitive automorphism group of order 11520.

- $n = 17, [\langle 0, 1\rangle, \langle 6, 68\rangle, \langle 8, 85\rangle, \langle 10, 68\rangle, \langle 12, 34\rangle]$
  The SRG is a Paley graph. The $[17, 8, 6]$ adjacency code is actually the dual of the quadratic residue code $[17, 9, 5]$.

w	6	8	10	12
λ	7	16	21	16
μ	8	19	24	17

- $n = 21, [\langle 0, 1\rangle, \langle 4, 105\rangle, \langle 6, 805\rangle, \langle 8, 3255\rangle, \langle 10, 5481\rangle, \langle 12, 4515\rangle, \langle 14, 1935\rangle, \langle 16, 252\rangle, \langle 18, 35\rangle]$
  The SRG is a triangle graph.

w	4	6	8	10	12	14	16	18
λ	2	57	424	1159	1412	838	144	25
μ	4	58	444	1190	1426	839	144	26

From now on, we indicate the parameters of the SRG as $(v - k - \lambda - \mu)$.

- $(27 - 10 - 1 - 5), [\langle 0, 1\rangle, \langle 2, 351\rangle, \langle 4, 17550\rangle, \langle 6, 296010\rangle, \langle 8, 2220075\rangle, \langle 10, 8436285\rangle, \langle 12, 17383860\rangle, \langle 14, 20058300\rangle, \langle 16, 13037895\rangle, \langle 18, 4686825\rangle, \langle 20, 888030\rangle, \langle 22, 80730\rangle, \langle 24, 2925\rangle, \langle 26, 27\rangle]$

w	2	4	6	8	10	12	14
λ	1	300	12650	177100	1081575	3268760	5200300

w	16	18	20	22	24	26
λ	4457400	2042975	480700	53130	2300	25

- $(36{-}14{-}4{-}6), [\langle 0, 1\rangle, \langle 14, 36\rangle, \langle 16, 63\rangle, \langle 18, 56\rangle, \langle 20, 63\rangle, \langle 22, 36\rangle, \langle 36, 1\rangle]$
  Here is the 180-th SRG with $v = 36$ in [12].

w	14	16	18	20	22
λ	4	12	12	19	12
μ	6	12	16	19	14

- $(40{-}12{-}2{-}4), [\langle 0, 1\rangle, \langle 12, 40\rangle, \langle 16, 135\rangle, \langle 20, 672\rangle, \langle 24, 135\rangle, \langle 28, 40\rangle, \langle 40, 1\rangle]$
  Here is the 6-th SRG with $v = 40$ in [12].

w	12	16	20	24	28
λ	2	18	160	45	18
μ	4	22	172	49	20

- $(40 - 12 - 2 - 4), [\langle 0, 1\rangle, \langle 8, 45\rangle, \langle 12, 1120\rangle, \langle 16, 15570\rangle, \langle 20, 32064\rangle, \langle 24, 15570\rangle, \langle 28, 1120\rangle, \langle 32, 45\rangle, \langle 40, 1\rangle]$
  Here is the 26-th SRG with $v = 40$ in [12].

w	8	12	16	20	24	28	32
λ	1	92	2394	7808	5508	540	28
μ	3	96	2396	7816	5510	544	30

6 Conclusion

In this work, we have constructed more than a thousand examples of PBIBDs with two associate classes held by binary codes with a rank three automorphism group. We could have constructed twice as many PBIBDs by simply considering the dual code, which has a different weight distribution in general. One possible extension would be to consider codes over other fields or rings. In another direction, allowing for more than two orbits on pairs of coordinates could lead to more examples of PBIBDs. For instance, the Zetterberg code of length 65 can be shown to hold PBIBDs with three associate classes.

References

[1] R. A. Bailey, *Association Schemes: designed experiments, algebra and combinatorics,* Cambridge studies in advanced math 84, Cambridge University Press, (2004), Cambridge.

[2] J. Bierbrauer, *Introduction to Coding Theory*, 2nd edition, CRC Press, (2017), Boca Raton, FL, USA.

[3] A. Bonnecaze, P. Solé, The extended binary quadratic residue code of length 42 holds a 3-design, Joural of Combinatorial designs, (2021), `https://doi.org/10.1002/jcd.21782`

[4] R. C. Bose, W. H. Clatworthy, S. S. Shrikhande, Table of PBIBDs with two associate classes, Technical bulletin (North Carolina Agricultural Experiment Station), (1954), no. 107.

[5] A. E. Brouwer, H. Van Maldeghem, *Fragments of a text on strongly regular graphs*, available from `https://www.win.tue.nl/~aeb/`

[6] D. Crnković, M. Maksimović, B. G. Rodrigues, S. Rukavina, Self-orthogonal codes from the strongly regular graphs on up to 40 vertices, Advances in Mathematics of Communications, (2016), 10:555–582.

[7] C. Ding, *Designs from linear codes*, World Scientific (2018) Singapore.

[8] R. Griess, *Twelve Sporadic Groups*, Springer, (1998).

[9] W. H. Haemers, R. Peeters, J. M. van Rijckevorsel, Binary codes of strongly regular graphs, Designs, Codes and Cryptography, (1999), 17:187–209.

[10] J. D. Key, P. Seneviratne, Permutation decoding for binary codes from lattice graphs, Discrete Mathematics, (2008), 308:2862–2867.

[11] F. J. MacWilliams, N. J. A. Sloane, *The theory of Error Correcting Codes*, North-Holland, Amsterdam, (1981).

[12] E. Spence, adjacency matrices of SRGs on at most 64 vertices `http://www.maths.gla.ac.uk/ es/srgraphs.php`

[13] V. S. Pless, W. C. Huffman,*Handbook of Coding theory*, North Holland, (1998), Amsterdam.

[14] V. D. Tonchev, On block designs arising from rank three graphs, J. Statist. Plannning and Inference, (1981), 5:399–403.

[15] V. D. Tonchev, Rank 3 graphs, block designs and unequal error protection codes, Problems of Information Transmission, (1981), 27:19–25.

[16] V. D. Tonchev, *Combinatorial configurations*, New York, Wiley, (1988).

[17] V. D. Tonchev, Binary codes derived from the Hoffman-Singleton and Higman-Sims graphs, IEEE Transactions on Information Theory, (1997), 43:1021–1025.

[18] V. D. Tonchev, Error correcting codes from graphs, Discrete Mathematics, (2002), 257:549–557.

[19] Table of Strongly regular graphs, `https://www.win.tue.nl/~ aeb/graphs/srg/`

[20] `http://magma.maths.usyd.edu.au/calc/`