Periodic Golay pairs and pairwise balanced designs

Dean Crnković (deanc@math.uniri.hr) [1]
Doris Dumičić Danilović (ddumicic@math.uniri.hr) [1]
Ronan Egan (ronan.egan@nuigalway.ie)[2]
and
Andrea Švob * (asvob@math.uniri.hr)[1]
[1] *Department of Mathematics, University of Rijeka, Croatia*
[2] *School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway*

Abstract

In this paper we exploit a relationship between certain pairwise balanced designs with v points and periodic Golay pairs of length v, to classify periodic Golay pairs of length less than 40. In particular we construct all pairwise balanced designs with v points under specific block conditions having an assumed cyclic automorphism group, and using isomorph rejection which is compatible with equivalence of corresponding periodic Golay pairs, we complete a classification up to equivalence. This is done using the theory of orbit matrices, and some compression techniques which apply to complementary sequences. We use similar tools to construct new periodic Golay pairs of lengths greater than 40 where classifications remain incomplete, and demonstrate that under some extra conditions on its automorphism group, a periodic Golay pair of length 90 will not exist. Length 90 remains the smallest length for which existence of a periodic Golay pair is undecided. Some quasi-cyclic self-orthogonal codes are constructed as an added application.

Acknowledgement
The authors thank the anonymous referee for pointing out reference [2], and we thank Dragomir Đoković for helpful communications and clarifications.

AMS classification numbers: 05B30, 05E18, 11B83, 94B05.
Keywords: Periodic Golay pair, pairwise balanced design, self-orthogonal code.

*Corresponding author

1 Introduction and preliminaries

Let $a = [a_0, \ldots, a_{v-1}]$ be a $\{\pm 1\}$-sequence of length v. The *periodic autocorrelation function* of a for a given shift s is defined to be $\mathrm{PAF}_s(a) = \sum_{i=0}^{v-1} a_i a_{i+s}$ where the sequence indices are read modulo v. A pair (a, b) of $\{\pm 1\}$-sequences is a *periodic Golay pair* (PGP) if $\mathrm{PAF}_s(a) + \mathrm{PAF}_s(b) = 0$ for all $1 \leq s \leq v-1$. We denote the set of all PGPs of length v by $\mathrm{PGP}(v)$. PGPs generalize the better known Golay pairs, introduced in [14], which are known to have applications in multislit spectroscopy, signal processing, digital communications and a variety of other areas (see e.g., [18]). PGPs exist in far greater abundance and at lengths where no Golay pairs may exist, but retain many of the properties required for these applications, so they are also of significant value, but are of mathematical interest in their own right too.

A $\mathrm{PGP}(v)$ is used to construct Hadamard matrices of order $2v$ (see e.g., [9]). This fact alone demonstrates that a $\mathrm{PGP}(v)$ for $v > 1$ can exist only if v is even. It is also well known that v must be the sum of two squares. Another less obvious restriction is due to Arasu and Xiang.

Theorem 1.1 (Corollary 3.6, [1]). *If there exists a* $\mathrm{PGP}(v)$ *where* $v = p^t u > 1$, $p \equiv 3 \mod 4$ *is prime, and* $\gcd(p, u) = 1$, *then* $u \geq 2p^{t/2}$.

This proves that no PGP(18) exists. It is possible to compose a $\mathrm{PGP}(v)$ with a Golay pair of length u to construct a $\mathrm{PGP}(uv)$, though Golay pairs of length u are only known to exist for lengths $u = 2^a 10^b 26^c$ for $a, b, c \in \mathbb{N}$, and it is conjectured that no others exist. It is shown in [12] for example, that no Golay pair of length u exists if u has a prime factor congruent to 3 modulo 4. The literature on PGPs is reasonably extensive, we refer the reader to [8, 9, 10] for recent progress, and to the references contained therein for further background. The smallest v for which existence remains undecided is 90.

Let K be a set of positive integers. A pairwise balanced design $\mathrm{PBD}(v, K, \lambda)$ is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$, with the following properties:

- $|\mathcal{P}| = v$,
- if an element of $\mathcal{B}$ is incident with k elements of $\mathcal{P}$, then $k \in K$,
- every pair of distinct elements of $\mathcal{P}$ is incident with exactly λ elements of $\mathcal{B}$.

Elements of $\mathcal{P}$ and $\mathcal{B}$ are called points and blocks respectively. A 2-(v, k, λ) design, also known as a balanced incomplete block design (BIBD), is a $\mathrm{PBD}(v, K, \lambda)$ where $K = \{k\}$. If $\mathcal{D}$ is a 2-design, each point is incident with a constant number of blocks, denoted by r, and called a replication number. If $|\mathcal{B}| = |\mathcal{P}|$ then the 2-(v, k, λ) design is called a symmetric design. An isomorphism from one design to other is a bijective mapping of points to points

and blocks to blocks which preserves incidence. An isomorphism from a design $\mathcal{D}$ onto itself is called an automorphism of $\mathcal{D}$. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group denoted by $\mathrm{Aut}(\mathcal{D})$.

Using the method outlined in [6] we can construct PBDs using orbit matrices. This construction is described in Section 3. By constructing PBDs with appropriate parameters and a presumed cyclic automorphism group, we can construct PGPs. We completely classify PBDs with these conditions which correspond to PGP(v)s for all $v \leq 34$, and we note that there are no periodic Golay pairs of length 36 and 38.

In the next section we define PBDs up to isomorphism in order to carry out our classification up to isomorphism accordingly. Similarly we explicitly define equivalence of PGPs and outline a procedure for efficiently computing the equivalence class of a given pair. We will see that the isomorph rejection used in the construction of PBDs is compatible with equivalence of corresponding PGPs. That is, the isomorph rejection only eliminates PBDs corresponding to equivalent PGPs, so at least one representative from each equivalence class of PGP remains. We then outline the construction of PBDs via orbit matrices in Section 3 and present our computational results in Section 4. As an added application we demonstrate how the objects constructed and related orbit matrices can be used to construct quasi-cyclic self-orthogonal linear codes over suitable finite fields in Section 5.

Computation in this paper consisted of programmes written for Magma [3] and GAP [13].

2 PBDs and periodic Golay pairs

Let $(a, b) \in \mathrm{PGP}(v)$, and let A and B be the circulant matrices with first rows a and b, respectively. Then $\begin{bmatrix} A & B \end{bmatrix}$ is a $v \times 2v$ matrix where the dot product of any two distinct rows is zero, i.e. the top half of a Hadamard matrix. This is only possible if v is even, or if $v = 1$. So by replacing each 1 with 0 and each -1 with 1 in $\begin{bmatrix} A & B \end{bmatrix}$ to get $\begin{bmatrix} A' & B' \end{bmatrix}$ we have an incidence matrix of a pairwise balanced design $\mathrm{PBD}(v, \{k_a, k_b\}, \lambda)$, where k_a and k_b denote the number of entries equal to -1 in a and b respectively. If the blocks label the columns and points label the rows of $\begin{bmatrix} A' & B' \end{bmatrix}$, we have v points, each incident with $r = k_a + k_b$ blocks, and any pair of points is incident with λ blocks. There are $2v$ blocks, the first v being incident with k_a points, the second v incident with k_b points. Orthogonality of rows in $\begin{bmatrix} A & B \end{bmatrix}$ gives that $\lambda = r - \frac{v}{2}$. Further, the cyclic group C_v acts transitively on points and has two orbits on the set of blocks.

Thus by constructing a $\mathrm{PBD}(v, K, \lambda)$ with presumed automorphism group C_v acting transitively on points, we can construct the corresponding PGP.

2.1 Isomorphism of PBDs

During the construction of PBDs with a presumed automorphism group we avoid construction of mutually isomorphic designs. This process is called an isomorph rejection. When constructing PBDs with parameters (v, K, λ) corresponding to periodic Golay pairs (a, b) of length v, and thus having the presumed automorphism group C_v, for isomorph rejection we use the normalizer N of the group C_v in $\mathrm{Sym}(v)$ (see [6]). The elements of N that are not in the centralizer of C_v act in the same way on the sets of blocks corresponding to the sequences a and b, respectively, while the elements of the centralizer can act independently on these two sets of blocks of a $\mathrm{PBD}(v, K, \lambda)$.

2.2 Equivalence of periodic Golay pairs

Given a Golay pair (a, b) of length v, we can construct a new Golay pair of length v by applying certain equivalence operations, see [7] for example. Any two periodic Golay pairs such that one is obtainable from the other through some combination of equivalence operations are members of the same equivalence class. In this section we outline similar operations that when applied to a pair of $\{\pm 1\}$-sequences, preserve the property of being a PGP. Moreover we describe a computational procedure for efficiently computing equivalence classes, which helps to classify the PGPs constructed in this paper. A similar tactic was applied to computing equivalence of negaperiodic Golay pairs in [11].

Define C to be the circulant $v \times v$ matrix

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

and write a $\{\pm 1\}$-sequence as a row vector $a = [a_0, a_1, \ldots, a_{v-1}]$, indexed modulo v. Let X be the set of all pairs of $\{\pm 1\}$-vectors of length v. We define equivalence operations of PGPs of length v in terms of elements of $\mathrm{Sym}(X)$ as follows:

1. $(a, b)\alpha_1 = (b, a)$; Swap a and b.
2. $(a, b)\alpha_2 = (aC, b)$; Replace a with aC.
3. $(a, b)\alpha_3 = ([a_{v-i}]_{1 \le i \le v}, b)$; Reverse a.
4. $(a, b)\alpha_{4,k} = ([a_{ki}]_{0 \le i \le v-1}, [b_{ki}]_{0 \le i \le v-1})$; For any $k < v$ coprime to v replace both a and b with $[a_{ki}]_{0 \le i \le v-1}$ and $[b_{ki}]_{0 \le i \le v-1}$ respectively. This is referred to as a decimation of a and b.

5. $(a,b)\alpha_5 = ([(-1)^i a_i]_{0\le i\le v-1}, [(-1)^i b_i]_{0\le i\le v-1})$; Negate every odd indexed entry of both a and b.

Remark 2.1. It is commonly written that negating one of the sequences is an elementary equivalence operation. We note that $(a,b)\alpha_5\alpha_2\alpha_5\alpha_2^{-1} = (-a,b)$, i.e., negating a sequence is incorporated in these operations.

Let $G \le \mathrm{Sym}(X)$ be the group $\langle \alpha_1, \alpha_2, \alpha_3, \{\alpha_{4,k} : (k,v) = 1\}, \alpha_5\rangle$ of order $32v^2\varphi(v)$ where φ is the Euler-phi function.Then X is a G-set and if any element of a G-orbit is a PGP, each element of the orbit has this property. Thus the action of G on a PGP (a,b) produces its equivalence class.

Let $\mathrm{Mon}(n,X)$ denote the set of $n \times n$ monomial matrices with non-zero entries in a set X. To efficiently calculate equivalence classes we construct a matrix representation $m : G \to \mathrm{Mon}(2v, \langle -1\rangle)$ of G. Let $\delta_x^y = 1$ if $x = y$ and 0 otherwise, and let $f(n)$ be the remainder after division of n by v. We define $K_{(k)} = [\delta_i^{1+f((j-1)k)}]_{1\le i,j\le v}$ where k is coprime to v. Let $T = [\delta_i^j(-1)^{i-1}]_{1\le i,j\le v}$, and let $R = [\delta_i^{v+1-j}]_{1\le i,j\le v}$. We describe the images of the generators of G under m as follows.

$$m(\alpha_1) = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix},\ m(\alpha_2) = \begin{bmatrix} C & 0 \\ 0 & I \end{bmatrix},\ m(\alpha_3) = \begin{bmatrix} R & 0 \\ 0 & I \end{bmatrix},$$

$$m(\alpha_{4,k}) = \begin{bmatrix} K_{(k)} & 0 \\ 0 & K_{(k)} \end{bmatrix},\ m(\alpha_5) = \begin{bmatrix} T & 0 \\ 0 & T \end{bmatrix}.$$

Under this definition we observe that $m : G \to \mathrm{Mon}(2v, \langle -1\rangle)$ is an injective homomorphism and is thus a $2v$-dimensional matrix representation of G. Let $a \circ b$ denote the vector of length $2v$ obtained from the concatenation of a and b. We observe that for any $g \in G$, if $(a,b)g = (c,d)$ then $(a \circ b)m(g) = c \circ d$. Thus given a pair (a,b) we calculate the orbit $(a \circ b)m(G)$, and obtain the equivalence class, in concatenated form. Given a list of PGPs, it is now a manageable task to test equivalence of any distinct pairs. In [11] it was feasible in this manner to complete a classification of all negaperiodic Golay pairs of length up to 20, by allowing the matrix group to act of the set of all $\{\pm 1\}$-vectors, and testing the autocorrelation of representatives of each class. A complete test for longer sequences remains an arduous task, but testing equivalence of a given list is still relatively quick.

2.3 Compression

For any sequence $a = [a_0, \ldots, a_{v-1}]$ of length v and positive integer m dividing v we can construct a compressed sequence $a^{(m)} = [\sum_{i=0}^{\frac{v}{m}-1} a_{im+j}]_{0\le j\le m-1}$ of length m by summing every m^{th} entry in the sequence. This is referred to as m-compression in [10]. For example, a

sequence $[a_0, \ldots, a_9]$ of length 10 can compress to a sequence of length 2, i.e., $[a_0{+}a_2{+}a_4{+}a_6{+}a_8, a_1{+}a_3{+}a_5{+}a_7{+}a_9]$, or a sequence of length 5, i.e., $[a_0{+}a_5, a_1{+}a_6, \ldots, a_4{+}a_9]$. Compression preserves complementarity in sequences. For shorthand we write $(a, b)^{(m)} = (a^{(m)}, b^{(m)})$.

Proposition 2.2. *If $(a, b) \in \mathrm{PGP}(v)$ then for any m dividing v, the pair of sequences $(a, b)^{(m)}$ are complementary.*

Proposition 2.2 is a special case of [10, Theorem 3]. This special case is easily proved by calculating $\mathrm{PAF}_s(a^{(m)}) + \mathrm{PAF}_s(b^{(m)})$ for any $s \leq v/m$. Compression is a useful tool in the construction (or proving non-existence) of PGPs, as we know that if a $\mathrm{PGP}(v)$ exists, then for any m dividing v this $\mathrm{PGP}(v)$ must compress to a pair of complementary sequences of length $\frac{v}{m}$. As an example, suppose we were attempting a complete enumeration of PGPs of length 18 (of which there are none). By compressing to sequences of length 6, each entry is a sum of three terms, giving four possible entries, namely ± 1 and ± 3. To do a complete search (disregarding equivalence), we construct 4^{12} possible pairs of sequences to test for complementarity, rather than 2^{36}, thus reducing computation by a factor of 2^{12}. This does however add the task of rebuilding the sequences of length 18. Fortunately, the entries equal to ± 3 correspond to only one possible set of three terms in the longer sequence, but each ± 1 entry could correspond to one of three.

Helpfully, compression is often compatible with the equivalence operations for PGPs. Namely, we observe that

- $(a, b)^{(m)}\alpha_1 = ((a, b)\alpha_1)^{(m)}$,
- $(a, b)^{(m)}\alpha_2 = ((a, b)\alpha_2)^{(m)}$,
- $(a, b)^{(m)}\alpha_3 = ((a, b)\alpha_3)^{(m)}$, and
- $(a, b)^{(m)}\alpha_{4,k} = ((a, b)\alpha_{4,k})^{(m)}$ for k coprime to v.

Thus we may sort pairs of sequences up to equivalence according to the above operations, and test representatives for complementarity before building larger sequences. For example, this approach was implemented in order to carry out a complete classification of PGP(20), by compressing to sequences of length 4 with entries in $\{\pm 1, \pm 3, \pm 5\}$.

3 Main construction

Adhering to a procedure of [6] we construct PBDs from orbit matrices. We give the necessary definitions and describe the procedure here.

Let $\mathcal{D}$ be a pairwise balanced design $\mathrm{PBD}(v, K, \lambda)$ with a replication number r, and $G \leq \mathrm{Aut}(\mathcal{D})$. We denote the G-orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_m$, G-orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_n$,

and put $|\mathcal{P}_i| = \omega_i$, $|\mathcal{B}_j| = \Omega_j$, $1 \leq i \leq m$, $1 \leq j \leq n$. Further, we denote by γ_{ij} the number of blocks of $\mathcal{B}_j$ incident with a representative of the point orbit $\mathcal{P}_i$. The following equalities hold:

$$0 \leq \gamma_{ij} \leq \Omega_j, \quad 1 \leq i \leq m, 1 \leq j \leq n, \tag{1}$$

$$\sum_{j=1}^{n} \gamma_{ij} = r, \quad 1 \leq i \leq m, \tag{2}$$

$$\sum_{i=1}^{m} \frac{\omega_i}{\Omega_j} \gamma_{ij} \in K, \quad 1 \leq j \leq n, \tag{3}$$

$$\sum_{j=1}^{n} \frac{\omega_t}{\Omega_j} \gamma_{sj} \gamma_{tj} = \lambda \omega_t + \delta_{st} \cdot (r - \lambda), \quad 1 \leq s, t \leq m. \tag{4}$$

Definition 3.1. A $(m \times n)$-matrix $M = (\gamma_{ij})$ with entries satisfying conditions $(1) - (4)$ is called a point orbit matrix of a pairwise balanced design PBD(v, K, λ) with orbit length distributions $(\omega_1, \ldots, \omega_m)$ and $(\Omega_1, \ldots, \Omega_n)$.

Orbit matrices are often used in the construction of designs with a presumed automorphism group. The construction of designs admitting an action of a presumed automorphism group consists of the following two basic steps (see [16]):

1. Construction of orbit matrices for the given automorphism group;

2. Construction of block designs from the obtained orbit matrices. This step is often called an indexing of orbit matrices.

Each orbit structure for the group G decomposes into orbit structures for a normal subgroup $H \lhd G$. Such a decomposition is called a refinement of an orbit structure. In [6] an algorithm for refinement of orbit matrices of a 2-design using a principal series of an abelian automorphism group of that design is described and is generalized using a composition series of a solvable automorphism group in [5]. The construction of PBDs corresponding to PGPs of length v using orbit matrices, consists of the following steps:

1. Find all possible combinations of numbers k_a and k_b of a PBD$(v, \{k_a, k_b\}, \lambda)$ corresponding to PGPs. For a fixed combination of numbers k_a and k_b, we are proceeding with the construction of PBD$(v, \{k_a, k_b\}, \lambda)$. The cyclic group $G \cong C_v$ acts transitively on points and has two orbits on the set of blocks. For the cyclic group G there is exactly one orbit matrix $M = [k_a \;\; k_b]$.

2. Construction of PBD$s(v, \{k_a, k_b\}, \lambda)$ for the orbit matrix M. Since the group G is cyclic, it can be written as direct product of cyclic subgroups as $G \cong C_{v_1} \times \ldots \times C_{v_n}$.

For a construction of PBDs$(v, \{k_a, k_b\}, \lambda)$ we can use a principal series $\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n = G$, $G_i \cong C_{v_1} \times \ldots \times C_{v_i}$, of the group G to construct refinements of the orbit matrix M as presented in [6]. In the ith iteration of the refinements we construct all the orbit matrices for the group G_{n-i}, having in mind the action of the group G. In the last iteration we obtain the orbit matrices for the trivial group *i.e.* incidence matrices of PBDs$(v, \{k_a, k_b\}, \lambda)$.

Remark 3.2. It is well known that a PGP(v) exists only if v is the sum of two squares. Specifically, if $(a, b) \in$ PGP(v), then where r_a and r_b denote the sum of the entries in a and b respectively, it holds that $r_a^2 + r_b^2 = 2v$. It follows that we can limit the possible choices of k_a and k_b so that $2(k_a - \frac{v}{2})^2 + 2(k_b - \frac{v}{2})^2 = v$.

During the construction, elements of the normalizer of the presumed automorphism group, *i.e.* the elements of $N_S(G)$, where $S = S(\mathcal{P}) \times S(\mathcal{B})$, can be used to decrease the number of constructed orbit matrices. This process is known as isomorph rejection. In Section 2.1 we explained the action of the elements of $N_S(G)$ when constructing PBDs corresponding to periodic Golay pairs (a, b) of length v. We have to determine correspondence between the elements of the normalizer $N_S(G)$ of an automorphism group $G \cong C_v$ of a PBD and the equivalence operations of PGPs.

Let $A = \{\alpha_i \mid i = 0, \ldots, n-1\}$, where $\alpha_i(x) = x + i \ (mod\ n)$, for $x = 0, 1, \ldots, n-1$, be the cyclic group of order n. Then the centralizer $C_{S_n}(A)$ equals A, and the normalizer $N_{S_n}(A)$ is the semidirect product $A : M$, where $M = \{\beta_j \mid gcd(j, n) = 1\}$, $\beta_j(x) = jx \ (mod\ n)$, for $x = 0, 1, \ldots, n-1$. Note that the order of M is $\varphi(n)$, where φ is the Euler-phi function.

Let $G \cong C_v$ be an automorphism group of a PBD$(v, \{k_a, k_b\}, \lambda)$ corresponding to PGPs. The elements of the centralizer $C_S(G)$ correspond to the equivalence operation α_2 for the periodic Golay pairs (replace a with aC) when acting on the first orbit of blocks of G (orbit that corresponds to a), or a composition of the equivalence operation 1 (swap a and b) and the equivalence operation 2 when acting on the second orbit of blocks of G (orbit corresponding to b). The elements of the normalizer $N_S(G)$ that are not in the centralizer $C_S(G)$ correspond to the equivalence operation α_4 for the periodic Golay pairs (decimation of a and b), or a composition of the equivalence operations α_2 and α_4, or a composition of the equivalence operations α_1, α_2 and α_4. Hence, with isomorph rejection we eliminate PBDs that lead to periodic Golay pairs (a, b) that are equivalent to some of the already constructed periodic Golay pairs. Consequently, with the above described construction we obtain PBDs that correspond to all equivalence classes of PGPs of length v.

4 Results

In this section we give the results of our computational classifications of isomorphism classes of PBDs and equivalence classes PGPs with various parameters. In general, isomorphism of PBDs is a stronger condition than equivalence of PGPs so there are often several isomorphism types of PBDs corresponding to the same PGP equivalence class. Numerical results from our classifications of equivalence classes of PBDs and PGPs are given in the following subsections. For more detailed information which couldn't be included in this manuscript, representatives of each class of PBD and PGP are hosted here:
`http://www.math.uniri.hr/~ddumicic/results/PGpairs_PBDs.html`.

4.1 PBD classifications

In Table 1 we present the number of isomorphism classes of PBDs with presumed automorphism group C_v corresponding to the existence of PGP(v) up to $v = 34$, constructed as described in Section 3, and more detailed results are given in Table 2 and Table 3. In order to check the correctness of the obtained number of isomorphism classes of PBDs we have used different composition series of the group, as shown in Table 3.

v	4	8	10	16	20	26	32	34
Classes	3	4	8	62	448	816	10208	5856

Table 1: Number of isomorphism classes of PBDs

v	$\{k_a, k_b\}$	r	λ	# nonisomorphic PBDs	Full automorphism group
4	{1,1}	2	0	1	S_4
	{3,1}	4	2	1	S_4
	{3,3}	6	4	1	S_4
8	{4,2}	6	2	2	$C_8,\ C_8 : E_4$
	{6,4}	10	6	2	$C_8,\ C_8 : E_4$
10	{4,3}	7	2	2	C_{10}
	{6,3}	9	4	2	C_{10}
	{7,4}	11	6	2	C_{10}
	{7,6}	13	8	2	C_{10}
16	{6,6}	12	4	16	C_{16}, QD_{32}, $C_{16} : C_2$, $(((C_4.D_8) : C_2) : C_4) : C_2$, $(C_{16} : C_4) : C_2$
	{10,6}	16	8	30	$C_{16},\ C_{16} : C_2$, $(C_2 \times D_{16}) : C_2,\ (C_4.D_8) : C_2$
	{10,10}	20	12	16	$C_{16},\ QD_{32},\ C_{16} : C_2$, $(((C_4.D_8) : C_2) : C_4) : C_2$, $(C_{16} : C_4) : C_2$
20	{9,7}	16	6	112	C_{20}
	{11,7}	18	8	112	C_{20}
	{13,9}	22	12	112	C_{20}
	{13,11}	24	14	112	C_{20}

Table 2: Results using the composition series $\{1\} \lhd C_v$

v	$\{k_a, k_b\}$	r	λ	C_{v_1}	# orbit matrices for C_{v_1}	# nonisomorphic PBDs	Full autom. group
26	{11,10}	21	8	C_2	274	204	C_{26}, $C_2 \times (C_{13} : C_3)$
				C_{13}	1		
	{15,10}	25	12	C_2	458	204	C_{26}, $C_2 \times (C_{13} : C_3)$
				C_{13}	1		
	{16,11}	27	14	C_2	505	204	C_{26}, $C_2 \times (C_{13} : C_3)$
				C_{13}	1		
	{16,15}	31	18	C_2	505	204	C_{26}, $C_2 \times (C_{13} : C_3)$
				C_{13}	1		
32	{16,12}	28	12	C_{16}	2	5104	$C_{32},\ C_{32} : C_2$
	{20,16}	36	20	C_{16}	2	5104	$C_{32},\ C_{32} : C_2$
34	{16,13}	29	12	C_2	5362	1464	C_{34}
	{18,13}	31	14	C_2	6604	1464	C_{34}
	{21,16}	37	20	C_2	7842	1464	C_{34}
	{21,18}	39	22	C_2	7842	1464	C_{34}

Table 3: Results using the composition series $\{1\} \lhd C_{v_1} \lhd C_{v_1} \times C_{v_2} \cong C_v$, for $v \in \{26, 32, 34\}$

For $v = 40$, a lower bound of 565 for the number of isomorphism classes of PBDs is obtained via a partial classification. The obtained PBDs each have automorphism group isomorphic to C_{40}. We use these PBDs to derive the lower bound for |PGP(40)| given in Table 4.

4.2 PGP classifications

Throughout this section, for shorthand we write $\{\pm 1\}$-sequences in the form $[r_i^{n_i}]$ where r_i is the length of a run of consecutive equal entries, n_i is the number of consecutive runs of length r_i. For example the sequence $[1, 1, -, 1, -, -, -, 1, -, 1, -]$ would be written as $[2, 1^2, 3, 1^4]$. Up to length 34 the procedure of Section 3 was completed with no added restrictions, and the equivalence classes of PGPs for length $v \leq 34$ obtainable in this manner are enumerated. At length $v = 40$ a partial classification was obtainable but a complete classification is out of reach with current methods. Following this, we use a refinement of the same procedure to perform targeted searches, and as an example we give a new PGP(74). We further use this approach to rule out the existence of a PGP(90) with automorphism group $H \cong (C_5 : C_2) \times C_2 \times C_9$, with $C_{90} \leq H$.

4.2.1 Classification up to $v = 34$

Table 4 illustrates the number of equivalence classes of PGPs of length v constructed according the procedure of Section 3. The classification is complete for $v \leq 34$, and we give a lower bound due to a partial classification, based on a small proportion of the search space, where $v = 40$.

v	2	4	8	10	16	20	26	32	34	40
Classes	1	1	2	1	11	34	53	838	373	≥ 323

Table 4: Equivalence classes of PGPs

Remark 4.1. A referee brought of a paper of Balonin and Đoković [2] to our attention which we were previously unaware of, where a classification of PGPs of length up to 40 was completed by other means. Up to length 32, our results are identical, however only 256 equivalence classes of length 34 are reported in [2]. We communicated with the authors and have confirmed that 256 of the equivalence classes found in this work coincide with the classes of [2], and the extra 117 equivalence classes we find are new. There are 9301 equivalence classes of length 40 according to [2], which unsurprisingly greatly surpasses the lower bound we find here based on a restricted search.

4.2.2 Periodic Golay pairs of length 74

In [9] the authors constructed two nonequivalent PGP(74)s; the first examples of this length. A search for pairs using the orbit matrix $M = [k_a \ k_b] = [38 \ 43]$ of a PBD$(74, \{38, 43\}, 42)$ with presumed autmorphism group C_{74} returned a third inequivalent class represented by the pair

$$[4, 1^2, 5, 1^5, 2, 3, 1^4, 2, 3, 1, 2, 3, 2, 1^4, 5, 2^3, 1, 2, 1, 2^2, 4, 2, 1^3, 2^2],$$
$$[2^2, 5, 2, 1^2, 3^2, 1, 7, 5, 1, 2, 1^2, 2^2, 1^4, 2^2, 1, 2, 3, 4, 1, 5, 1^3, 4, 1^2].$$

4.2.3 Periodic Golay pairs of length 90

Since the existence of a PGP(90) is still undecided, we implement here the construction given in Section 3 as an attempt to obtain one.

We use the orbit matrices of the corresponding PBD$(90, \{k_a, k_b\}, \lambda)$s under the action of the cyclic automorphism group $G \cong C_{90} \cong C_2 \times C_5 \times C_9$ which acts with the point and block orbit lengths distributions (90) and $(90, 90)$, respectively.

As given in Section 3, the first step is to find all possible combinations of numbers k_a and k_b of a PBD$(v, \{k_a, k_b\}, \lambda)$ corresponding to PGPs. We determine that all possible PBDs with the group G as the presumed automorphism group are PBD$(90, \{39, 42\}, 36)$, PBD$(90, \{39, 48\}, 42)$, PBD$(90, \{42, 51\}, 48)$ and PBD$(90, \{48, 51\}, 54)$, having the replication numbers 81, 87, 93 and 99, respectively. Since there exists exactly one orbit matrix $M = [k_a \ k_b]$ for the cyclic group G, in each case we have that the corresponding orbit matrices are $M_1 = [39, \ 42]$, $M_2 = [39, \ 48]$, $M_3 = [42, \ 51]$ and $M_4 = [48, \ 51]$.

Further, for the construction of the PBDs we use a principal series of the group G, e.g. $\{1\} \lhd C_5 \lhd C_2 \times C_5 \lhd C_2 \times C_5 \times C_9$. In the first iteration of the refinement of the orbit matrices M_1, M_2, M_3 and M_4 we construct all orbit matrices for the group $C_2 \times C_5$ and in the second iteration, all orbit matrices for the group C_5. In Table 5 we present the number of orbit matrices obtained in these iterations.

r	81	87	93	99
# orbit matrices for C_{90}	1	1	1	1
# orbit matrices for $C_2 \times C_5$	362	361	356	363
# orbit matrices for C_5	16232	15331	16536	15330

Table 5: Number of orbit matrices

Due to the large number of possibilities in the last iteration of the refinement of the orbit matrices, we cannot complete the search for the incidence matrices of the PBDs. However, to reduce the number of possibilities and finish the search, we consider the automorphism group $H \cong (C_5 : C_2) \times C_2 \times C_9$, as a presumed automorphism group of the PBDs. In this

approach, we use the composition series $\{1\} \triangleleft C_5 \triangleleft C_5 : C_2 \triangleleft (C_5 : C_2) \times C_2 \triangleleft (C_5 : C_2) \times C_2 \times C_9$ of the solvable automorphism group H (see [5] for more information). We assumed that the group C_2 acts in such a way that the point and block orbits for the group $C_5 : C_2$ are the same as for the group C_5. Hence, the orbit matrices for the group $C_5 : C_2$ are the same as the orbit matrices for the group C_5.

For each of the obtained orbit matrices for the group C_5 (*i.e.* the group $C_5 : C_2$) we try to build all corresponding orbit matrices for the trivial group, which are the incidence matrices of PBDs, having in mind the action of the group H.

As a result, we get that PBD$(90, \{39, 42\}, 36)$, PBD$(90, \{39, 48\}, 42)$, PBD$(90, \{42, 51\}, 48)$ and PBD$(90, \{48, 51\}, 54)$ with the automorphism group $H \cong (C_5 : C_2) \times C_2 \times C_9$, where $C_5 : C_2$ acts in all orbits of length five do not exist.

5 Construction of quasi-cyclic self-orthogonal codes

A linear $[n, k]_q$ code C is a k-dimensional subspace of $V = \mathbb{F}_q^n$ where $\mathbb{F}_q$ denotes the finite field of order q. It has a basis consisting of the rows of a $k \times n$ matrix M called the generator matrix. Its orthogonal complement $C^\perp$ in V is the set $\{v \in V \ : \ v \cdot c = 0 \ \forall \ c \in C\}$. In other words the codewords of $C^\perp$ are the transposes of the column vectors in the kernel of M. We say S is *self-orthogonal* if $C \subseteq C^\perp$. Two codes are *equivalent* if one of the codes can be obtained from the other by permuting the coordinates and permuting the symbols within one or more coordinate positions.

A code is ℓ-quasi-cyclic if for every codeword $c \in C$, the codeword $c^{(\ell)}$ belongs to C where $c^{(\ell)} = [c_{v-\ell}, \ldots, c_{v-1}, c_0, c_1, \ldots, c_{v-\ell-1}]$. Equivalently, C is ℓ-quasicyclic if it is equivalent to a code with generator matrix of the form $[A_1, \ldots, A_\ell]$ where each A_i is circulant. We often just say quasi-cyclic when $\ell = 2$.

Let $\mathcal{D}$ be a PBD$(v, \{k_1, k_2\}, \lambda)$ corresponding to a PGP(v). The incidence matrix of the design $\mathcal{D}$ spans a quasi-cyclic code $\mathcal{C}$ of length $2v$ over a field GF(p^n). Moreover, if p is a prime dividing $k_1 + k_2$ and λ then the code $\mathcal{C}$ is self-orthogonal. In this section we will show how self-orthogonal codes can be constructed using PBDs corresponding to a PGPs.

We will use the following Theorems, that can be found in [5, 6]:

Theorem 5.1. *Let Ω be a finite non-empty set, $G \leq S(\Omega)$ and H a normal subgroup of G. Further, let x and y be elements of the same G-orbit. Then $|xH| = |yH|$.*

Theorem 5.2. *Let Ω be a finite non-empty set, $H \triangleleft G \leq S(\Omega)$, $x \in \Omega$ and $xG = \bigsqcup_{i=1}^{h} x_i H$. Then the group G/H acts transitively on the set $\{x_i H | i = 1, 2, \ldots, h\}$.*

We have the following result, similar to the result given in [15].

Theorem 5.3. *Let $\mathcal{D}$ be a* PBD$(v, \{k_1, k_2\}, \lambda)$ *corresponding to a* PGP(v)*. Then the cyclic group $G \cong C_v$ is a subgroup of* Aut$(\mathcal{D})$*. Let H be a subgroup of G and M be a point orbit matrix with respect to the group H. Then the matrix M spans a quasi-cyclic self-orthogonal code $\mathcal{C}$ of length $\frac{2v}{|H|}$ over the field* GF(p^n)*, where p is a prime dividing $k_1 + k_2$ and λ.*

Proof. The group H acts with $m = \frac{v}{|H|}$ orbits on points and $n = 2m$ orbits on blocks on $\mathcal{D}$ having all orbits of length $|H|$. By Theorems 5.1, and 5.2, each G-orbit of $\mathcal{D}$ decomposes to H-orbits of the same size and the cyclic group G/H acts transitively on H-orbits on points and in two H-orbits on blocks. Hence, the code $\mathcal{C}$ spanned by the matrix M is quasi-cyclic.

From equality (4) it follows that

$$\sum_{j=1}^{n} \gamma_{sj}\gamma_{tj} = \lambda \cdot |H| + \delta_{st} \cdot (k_1 + k_2 - \lambda), \quad 1 \leq s, t \leq m.$$

It follows that when p is a prime dividing $k_1 + k_2$ and λ the code $\mathcal{C}$ is a self-orthogonal code of length $\dfrac{2v}{|H|}$. □

The following result can be proved in a similar way. This result resembles the result given in [17, Theorem 1.113].

Theorem 5.4. *Let $\mathcal{D}$ be a* PBD$(v, \{k_1, k_2\}, \lambda)$ *corresponding to a* PGP(v)*. Then the cyclic group $G \cong C_v$ is a subgroup of* Aut$(\mathcal{D})$*. Let H be a subgroup of G and M be a point orbit matrix with respect to the group H. Then the matrix M spans a quasi-cyclic self-orthogonal code $\mathcal{C}$ of length $\frac{2v}{|H|}$ over the field* GF(p^n)*, where p is a prime dividing $|H|$ and $k_1 + k_2 - \lambda$.*

6 Declarations

6.1 Funding

D. Crnković, D. Dumičić Danilović and A. Švob were supported by Croatian Science Foundation under the project 6732. R. Egan was supported by the Irish Research Council (Government of Ireland Postdoctoral Fellowship, GOIPD/2018/304).

6.2 Conflicts of interest/Competing interests

The authors declare no conflict of interest.

6.3 Availability of data and material

Not applicable.

6.4 Code availability

Not applicable.

6.5 Authors' contributions

This is a joint collaboration with all four authors contributing substantially throughout.

References

[1] K. T. Arasu, Q. Xiang, On the existence of periodic complementary binary sequences, Des. Codes Cryptogr. 2 (1992), 257–262.

[2] N. A. Balonin, D. Ž. Đoković, Symmetry of two-circulant Hadamard matrices and periodic Golay pairs, (in Russian) Inf. Control Syst. 3 (2015), 2–16.

[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, 1994. http://magma.maths.usyd.edu.au/magma.

[4] D. Crnković, Symmetric (70,24,8) designs having $\mathrm{Frob}_{21} \times Z_2$ as an automorphism group, Glas. Mat. Ser. III 34 (54) (1999), 109–121.

[5] D. Crnković, D. Dumičić Danilović, S. Rukavina, On symmetric (78,22,6) designs and related self-orthogonal codes, Util. Math. 109 (2018), 227–253.

[6] D. Crnković, S. Rukavina, Construction of block designs admitting an Abelian automorphism group, Metrika 62 (2005), 175–183.

[7] D. Ž. Đoković, Equivalence classes and representatives of Golay sequences, Discrete Math. 189 (1998), 79–93.

[8] D. Ž. Đoković, I. S. Kotsireas, Periodic Golay Pairs of Length 72, in: C. J. Colbourn, (Ed.), Algebraic Design Theory and Hadamard Matrices, Springer Proceedings in Mathematics and Statistics, vol 133, Springer, Cham, 2015, pp. 83–92.

[9] D. Ž. Đoković, I. S. Kotsireas, Some new periodic Golay pairs, Numer. Algor. 69 (2015), 523–530.

[10] D. Ž. Đoković, I. S. Kotsireas, Compression of periodic complementary sequences and applications, Des. Codes Cryptogr. 74 (2015), 365–377.

[11] R. Egan, On equivalence of negaperiodic Golay pairs, Des. Codes Cryptogr., 85 (2017), 523–532.

[12] S. Eliahou, M. Kervaire, B. Saffari, A new restriction on the lengths of Golay complementary sequences, J Combin Theory (A)., 55 (1990), 49–59.

[13] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.4; 2016. (http://www.gap-system.org)

[14] M. J. E. Golay, Multislit spectrometry, J. Opt. Soc. Am. 39 (1949), 437–444.

[15] M. Harada, V. D. Tonchev, Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, Discrete Math. 264 (2003) 81–90.

[16] Z. Janko, Coset enumeration in groups and constructions of symmetric designs, Combinatorics '90 (Gaeta, 1990), Ann. Discrete Math. 52 (1992), 275–277.

[17] V. D. Tonchev, Codes, in: C. J. Colbourn, J. H. Dinitz (Eds.), Handbook of Combinatorial Designs, second ed., Chapman and Hall, CRC, Boca Raton, 2007, pp. 677–702.

[18] G. Weathers, E. Holiday, Group-complementary array coding for radar clutter rejection, IEEE Trans. Aerosp. Electron. Syst., AES-29 (1983), 369–379.