Periodic Golay pairs of length 72

Dragomir Ž. Doković and Ilias S. Kotsireas

Abstract We construct supplementary difference sets (SDS) with parameters \((72; 36, 30, 30)\). These SDSs give periodic Golay pairs of length 72. Until now, no periodic Golay pair of length 72 was known. The smallest undecided order for periodic Golay pairs is now 90. The periodic Golay pairs constructed here are the first examples having length divisible by a prime congruent to 3 modulo 4. The basic tool that we use is the compression method which we introduced recently.

1 Introduction

Let \(v\) be any positive integer. We say that a sequence \(A = [a_0, a_1, \ldots, a_{v-1}]\) is a binary sequence if \(a_i \in \{1, -1\}\) for all \(i\). We denote by \(\mathbb{Z}_v = \{0, 1, \ldots, v-1\}\) the ring of integers modulo \(v\). There is a bijection from the set of all binary sequences of length \(v\) to the set of all subsets of \(\mathbb{Z}_v\) which assigns to the sequence \(A\) the subset \(\{i \in \mathbb{Z}_v : a_i = -1\}\). If \(X \subseteq \mathbb{Z}_v\), then the corresponding binary sequence \([x_0, x_1, \ldots, x_{v-1}]\) has \(x_i = -1\) if \(i \in X\) and \(x_i = +1\) otherwise. We associate to \(X\) the cyclic matrix \(C_X\) of order \(v\) having this sequence as its first row.

Periodic Golay pairs are periodic analogs of the well known Golay pairs. Let us give a precise definition. For any complex sequence \(A = [a_0, a_1, \ldots, a_{v-1}]\), its periodic autocorrelation is a complex valued function \(\text{PAF}_A : \mathbb{Z}_v \rightarrow \mathbb{C}\) defined by

\[\text{PAF}_A(x) = \sum_{i=0}^{v-1} a_i a_{i+x}\]
\[
PAF_A(s) = \sum_{j=0}^{v-1} a_{j+s} \bar{a}_j, \tag{1}
\]

where the indexes are computed modulo \(v\) and \(\bar{a}\) is the complex conjugate of \(a\). A pair of binary sequences \((A, B)\) of length \(v\) is a periodic Golay pair if \(PAF_A(j) + PAF_B(j) = 0\) for \(j \neq 0\). For more information on these pairs see [4]. The length \(v\) of a periodic Golay pair must be even except for the trivial case \(v = 1\).

Many periodic Golay pairs of even length \(v\) can be constructed by using supplementary difference sets with suitable parameters \((v; r, s; \lambda)\). We recall that these parameters are nonnegative integers such that \(\lambda(v-1) = r(r-1) + s(s-1)\). (See section 2 below for the formal definition of SDSs over a finite cyclic group.) For convenience, we also introduce the parameter \(n = r + s - \lambda\). Without any loss of generality we may assume that the parameter set is normalized which means that we have \(v/2 \geq r \geq s \geq 0\). The SDSs that we need are those for which \(v = 2n\). We refer to them as periodic Golay SDS.

The feasible parameter sets for the periodic Golay SDSs can be easily generated by using the following proposition.

**Proposition 1.** Let \(P\) be the set of ordered pairs \((x, y)\) of integers \(x, y\) such that \(x \geq y \geq 0\) and \(x > 0\). Let \(Q\) be the set of normalized feasible parameter sets \((v; r, s; \lambda)\), with \(v\) even, for periodic Golay SDSs. Thus, it is required that \(v = 2n\) where \(n = r + s - \lambda\). Then the map \(P \rightarrow Q\) given by the formula

\[
(x, y) \rightarrow (2(x^2 + y^2); x^2 + y^2 - y, x^2 + y^2 - x; x^2 + y^2 - x - y)
\]

is a bijection.

**Proof.** The inverse map \(Q \rightarrow P\) is given by

\[
(v; r, s; \lambda) \rightarrow (\frac{v}{2} - s, \frac{v}{2} - r).
\]

Note that \(n = x^2 + y^2\).

If \((A, B)\) is a periodic Golay pair of length \(v\), then the corresponding pair of subsets \((X, Y)\) of \(\mathbb{Z}_v\) is an SDS. In the nontrivial cases \((v > 1)\), the parameters \((v; r, s; \lambda)\) satisfy the equation \(v = 2n\). Recall that \(n = r + s - \lambda\). The converse is also true, i.e., if \((X, Y)\) is an SDS with parameters \((v; r, s; \lambda)\) then the corresponding binary sequences \((A, B)\) form a periodic Golay pair of length \(v\). Moreover, if \(a = v - 2r\) and \(b = v - 2s\) then \(a^2 + b^2 = 2v\). In particular, \(v\) must be even and a sum of two squares. The associated matrices \(C_X\) and \(C_Y\) satisfy the equation

\[
C_X C_X^T + C_Y C_Y^T = 2vI_v. \tag{2}
\]

Our main result is the construction of periodic Golay pairs of length 72. This is accomplished by constructing the SDSs with parameters \((72; 36, 30; 30)\).
The main tool that we use in our construction is the method of compression of SDSs which we developed in our recent paper [5]. This method uses a nontrivial factorization $v = md$ and so it can be applied only when $v$ is a composite integer. In this case we used the factorization with $m = 3$ and $d = 24$.

In section 2 we recall the definition of SDSs over finite cyclic groups, and in section 3 we establish a relationship between power density functions of a complex sequence of length $v = md$ and its compressed sequence of length $d$. This relationship was used to speed up some of the computations.

In section 5 we list 8 nonequivalent SDSs which give 8 periodic Golay pairs of length 72. This provides the first examples of periodic Golay pairs whose length is divisible by a prime congruent to 3 modulo 4.

2 Supplementary difference sets

We recall the definition of SDSs. Let $k_1, \ldots, k_t$ be positive integers and $\lambda$ an integer such that

$$\lambda(v - 1) = \sum_{i=1}^{t} k_i(k_i - 1).$$

and let $X_1, \ldots, X_t$ be subsets such that

$$\text{(4)}$$

**Definition 1.** We say that the subsets $X_1, \ldots, X_t$ of $\mathbb{Z}_v$ with $|X_i| = k_i$ for $i \in \{1, \ldots, t\}$ are supplementary difference sets (SDS) with parameters $(v; k_1, \ldots, k_t; \lambda)$, if for every nonzero element $c \in \mathbb{Z}_v$ there are exactly $\lambda$ ordered triples $(a, b, i)$ such that $\{a, b\} \subseteq X_i$ and $a - b = c \pmod{v}$.

These SDS are defined over the cyclic group of order $v$, namely the additive group of the ring $\mathbb{Z}_v$. More generally SDS can be defined over any finite abelian group, and there are also further generalizations where the group may be any finite group. However, in this paper we shall consider only the cyclic case.

In the context of an SDS, say $X_1, \ldots, X_t$, with parameters $(v; k_1, \ldots, k_t; \lambda)$, we refer to the subsets $X_i$ as the base blocks and we introduce an additional parameter, $n$, defined by:

$$n = k_1 + \cdots + k_t - \lambda.$$ 

If $x$ is an indeterminate, then the quotient ring $\mathbb{C}[x]/(x^v - 1)$ is isomorphic to the ring of complex circulant matrices of order $v$. Under this isomorphism $x$ corresponds to the cyclic matrix with first row $[0, 1, 0, 0, \ldots, 0]$. By applying this isomorphism to the identity [5] (13), we obtain that the following matrix
Identity holds
\[
\sum_{i=1}^{t} C_i C_i^T = 4nI_v + (tv - 4n)J_v,
\]
where \( C_i = C_{X_i} \) is the cyclic matrix associated to \( X_i \).

In this paper we are mainly interested in SDSs \((X, Y)\) with two base blocks \((t = 2)\) and \(v = 2n\) Then the identity (6) reduces to the identity (2).

3 Compression of SDSs

Let \( A \) be a complex sequence of length \( v \). For the standard definitions of periodic autocorrelation functions (PAF\(_A\)), discrete Fourier transform (DFT\(_A\)), power spectral density (PSD\(_A\)) of \( A \), and the definition of complex complementary sequences, we refer the reader to our paper [5]. If we have a collection of complex complementary sequences of length \( v = dm \), then we can compress them to obtain complementary sequences of length \( d \). We refer to the ratio \( v/d = m \) as the compression factor. Here is the precise definition.

**Definition 2.** Let \( A = [a_0, a_1, \ldots, a_{v-1}] \) be a complex sequence of length \( v = dm \) and set
\[
a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}, \quad j = 0, \ldots, d - 1.
\]
Then we say that the sequence \( A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}] \) is the \( m \)-compression of \( A \).

Let \( X, Y \) be an SDS with parameters \((v; r, s; \lambda)\) with \( v = 2n \) (and \( n = r + s - \lambda \)). Assume that \( v = md \) is a nontrivial factorization. Let \( A, B \) be the binary sequences of length \( v \) associated to \( X \) and \( Y \), respectively. Then the \( m \)-compressed sequences \( A^{(d)}, B^{(d)} \) form a complementary pair. In general they are not binary sequences, their terms belong to the set \( \{m, m-2, \ldots, -m+2, -m\} \). The search for such pairs \( X, Y \) is broken into two stages: first we construct the candidate complementary sequences \( A^{(d)}, B^{(d)} \) of length \( d \), and second we lift each of them and search to find the required pairs \((X, Y)\). Each of the stages requires a lot of computational resources. There are additional theoretical results that can be used to speed up these computations. Some of them are described in [5], namely we use “bracelets” and “charm bracelets” to speed up the first stage. We use our recent new result [6, Theorem 1] to speed up the second stage.
4 Golay numbers and periodic Golay numbers

If there exists a Golay pair resp. a periodic Golay pair of length \( v \) then we say that \( v \) is a Golay number resp. a periodic Golay number. We denote the set of Golay numbers by \( \Gamma \) and the set of periodic Golay numbers by \( \Pi \). By \( \Gamma_0 \) we denote the set of known Golay numbers, i.e., \( \Gamma_0 = \{ 2^n 10^6 26^c : a, b, c \in \mathbb{Z}_+ \} \), where \( \mathbb{Z}_+ \) is the set of nonnegative integers. It is not known whether \( \Gamma_0 = \Gamma \). Since every Golay pair is also a periodic Golay pair, we have \( \Gamma \subseteq \Pi \). Moreover, this inclusion is strict. Indeed, the periodic Golay numbers \( v = 34, 50, 58, 68, 72, 74, 82 \) (see [4]) are not in \( \Gamma \) (see [2]).

If \( X \) and \( Y \) are sets of positive integers, we shall denote by \( XY \) the set of all products \( xy \) with \( x \in X \) and \( y \in Y \). Given a Golay pair of length \( g \) and a periodic Golay pair of length \( v \), then one can “multiply” them to obtain a periodic Golay pair of length \( gv \). This “multiplication” is described in the very recent paper [8]. It is an easy consequence of [9, Theorems 13,16]. Consequently, the set \( \Pi \setminus \Gamma_0 \) is infinite as it contains the set \( \Gamma_0 \cdot \{ 34, 50, 58, 72, 74, 82, 122, 202, 226 \} \).

If \( Z \subseteq \mathbb{Z}_v \) we set \( Z' = \mathbb{Z}_v \setminus Z \). To \( Z \) we associate the binary sequence \( [a_0, a_1, \ldots, a_{v-1}] \), where \( a_i = -1 \) if \( i \in Z \) and \( a_i = +1 \) otherwise. This gives a one-to-one correspondence between subsets \( Z \subseteq \mathbb{Z}_v \) and the set of binary sequences of length \( v \). If \( (X, Y) \) is an SDS with parameters \( (v; r, s; \lambda) \) such that \( v = 2n \), \( (n = r + s - \lambda) \), then the associated binary sequences of \( X \) and \( Y \) form a periodic Golay pair. Conversely, each periodic Golay pair of length \( v > 1 \) arises in this way from an SDS with \( v = 2n \).

The above mentioned “multiplication” has a simple description in terms of the SDS \( (X, Y) \) associated to a periodic Golay pair. Its parameters \( (v; r, s; \lambda) \) satisfy the equation \( v = 2n \).

**Proposition 2.** Let \((U, V)\) be a Golay pair of length \( g \) and \((X, Y)\) the SDS associated to a periodic Golay pair of length \( v = 2n \). Let \( x, y \) be two indeterminates and define the sequence \( A = [a_0, a_1, \ldots, a_{v-1}] \) by setting

\[
    a_i = \begin{cases} 
    x, & \text{if } i \in X \cap Y, \\
    -x, & \text{if } i \in X \cap Y', \\
    y, & \text{if } i \in X \setminus Y, \\
    -y, & \text{if } i \in Y \setminus X.
    \end{cases}
\]

Next, let \( B \) be the sequence obtained from \( A \) by first reversing \( A \) and then simultaneously replacing \( x \) with \( y \) and \( y \) with \( -x \). Finally, by replacing in both \( A \) and \( B \) the indeterminates \( x \) and \( y \) with \( U \) and \( V \), respectively, one obtains a periodic Golay pair of length \( gv \).
5 Computational results for periodic Golay pairs

It is a well known fact [2] that no $v \in \Gamma$ is divisible by a prime congruent to 3 modulo 4. So far, none of the known members of $\Pi$ were divisible by a prime congruent to 3 modulo 4. Hence, the periodic Golay pairs constructed below are the first examples having the length divisible by a prime congruent to 3 modulo 4, namely the prime 3.

We list eight pairwise nonequivalent SDSs with parameters $(72; 36; 30; 30)$. As $n = 36$ we have $v = 2n$, and so these SDSs give periodic Golay pairs of length 72. All solutions are in the canonical form defined in [3] and since they are different, this implies that they are pairwise nonequivalent.

1) $\{0, 1, 2, 3, 4, 5, 6, 7, 10, 12, 13, 15, 17, 18, 20, 22, 24, 26, 27, 29, 30, 31, 35, 37, 39, 40, 43, 44, 47, 51, 52, 53, 55, 56, 58, 59, 62, 63\}$,
   $\{0, 1, 2, 3, 5, 6, 8, 11, 12, 13, 14, 15, 18, 21, 23, 25, 29, 32, 33, 39, 41, 42, 43, 47, 48, 55, 56, 62, 67, 69\}$,
2) $\{0, 1, 2, 3, 4, 5, 6, 7, 10, 12, 13, 15, 18, 20, 22, 24, 26, 27, 29, 30, 31, 35, 37, 39, 40, 43, 44, 47, 51, 52, 53, 56, 58, 59, 62, 63\}$,
   $\{0, 2, 3, 5, 7, 8, 9, 11, 14, 15, 17, 18, 19, 23, 24, 30, 31, 32, 33, 37, 38, 41, 42, 44, 48, 49, 51, 59, 61, 69\}$,
3) $\{0, 1, 2, 3, 5, 7, 10, 11, 12, 13, 15, 17, 19, 20, 26, 27, 28, 29, 30, 32, 34, 35, 38, 39, 40, 42, 43, 46, 49, 51, 54, 56, 59, 60, 63, 64\}$,
   $\{0, 1, 2, 3, 4, 6, 7, 8, 9, 14, 15, 16, 20, 22, 24, 26, 27, 31, 33, 36, 37, 40, 42, 43, 46, 49, 54, 57, 58, 68\}$,
4) $\{0, 1, 2, 3, 5, 7, 10, 11, 12, 13, 15, 17, 19, 20, 26, 27, 28, 29, 30, 32, 34, 35, 38, 39, 40, 42, 43, 46, 49, 51, 54, 56, 59, 60, 63, 64\}$,
   $\{0, 1, 3, 4, 6, 7, 8, 9, 10, 14, 15, 18, 19, 20, 22, 25, 26, 31, 32, 36, 38, 40, 42, 45, 49, 51, 52, 57, 58, 60\}$,
5) $\{0, 1, 2, 4, 5, 6, 7, 9, 10, 11, 14, 15, 16, 17, 22, 23, 25, 26, 29, 30, 33, 35, 37, 38, 43, 45, 46, 48, 50, 51, 52, 54, 55, 60, 62, 63\}$,
   $\{0, 2, 3, 5, 7, 8, 9, 11, 14, 17, 18, 19, 21, 23, 24, 27, 30, 31, 32, 37, 38, 41, 42, 44, 48, 49, 57, 59, 61, 63\}$,
6) $\{0, 1, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 17, 18, 19, 20, 22, 25, 26, 29, 31, 32, 36, 38, 40, 41, 42, 45, 49, 51, 52, 53, 57, 58, 60, 65\}$,
   $\{0, 1, 2, 5, 7, 10, 11, 12, 13, 17, 19, 20, 26, 28, 29, 30, 32, 34, 35, 38, 40, 42, 43, 46, 49, 54, 56, 59, 60, 64\}$,
7) $\{0, 1, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 17, 18, 19, 20, 22, 25, 26, 29, 31, 32, 36, 38, 40, 41, 42, 45, 49, 51, 52, 53, 57, 58, 60, 65\}$,
Periodic Golay pairs of length 72

\{0, 1, 3, 4, 5, 6, 9, 10, 13, 16, 18, 19, 21, 23, 24, 27, 30, 34, 35, 40, 46, 47, 48, 49, 53, 55, 57, 63, 65, 67\},

8) \{0, 2, 3, 4, 5, 7, 8, 9, 11, 14, 15, 16, 17, 18, 23, 24, 28, 30, 31, 32, 33, 37, 40, 41, 42, 44, 48, 49, 51, 52, 59, 61, 64, 69\},

\{0, 1, 2, 4, 5, 6, 7, 10, 12, 13, 18, 20, 22, 24, 26, 29, 30, 31, 35, 37, 40, 43, 44, 47, 52, 53, 56, 58, 59, 62\}.

Let \(v \in \Pi\) and \(v > 1\). Then it is known that \(v\) must be even and \(v/2\) must be a sum of two squares. Moreover there is an SDS with parameters \((v; r, s; \lambda)\) such that \(v = 2n\). The Arasu-Xiang condition \([1\text{ Corollary 3.6}]\) for the existence of such SDS must be satisfied. This gives another restriction on \(v\).

The product \(\Gamma_0 S\), where \(S = \{1, 34, 50, 58, 72, 74, 82, 122, 202, 226\}\), is the set of lengths of the currently known periodic Golay sequences. For reader's convenience we list the integers in the range \(1 < v \leq 300\) which satisfy all necessary conditions mentioned above and do not belong to \(\Gamma_0 S\). There are just sixteen of them:

90, 106, 130, 146, 170, 178, 180, 194, 212, 218, 234, 250, 274, 290, 292, 298.

These are the smallest lengths for which the existence question of periodic Golay sequences remains unsolved.

6 Acknowledgements

The authors wish to acknowledge generous support by NSERC. This research was enabled in part by support provided by WestGrid (www.westgrid.ca) and Compute Canada Calcul Canada (www.computecanada.ca).

References

1. K. T. Arasu, Q. Xiang, On the existence of periodic complementary binary sequences Des. Codes Cryptogr. 2 (1992), 257–262.
2. P. B. Borwein, R. A. Ferguson, A complete description of Golay pairs for lengths up to 100, Math. Comput. 73 (2003), no. 246, 967–985.
3. D. Ž. Doković, Cyclic \((v; r, s; \lambda)\) difference families with two base blocks and \(v \leq 50\), Ann. Comb. 15 (2011), 233–254.
4. D. Ž. Doković, I. S. Kotsireas, Some new periodic Golay pairs, arXiv:1310.577v1 [math.CO] 22 Oct 2013
5. D. Ž. Doković and I. S. Kotsireas, Compression of periodic complementary sequences and applications, Des. Codes Cryptogr. DOI 10.1007/s10623-013-9862-z
6. D. Ž. Doković, I. S. Kotsireas, D-optimal matrices of orders 138, 150, 154 and 174, Numerical Algorithms (to appear), [arXiv:1408.6116v1 [math.CO] 26 Aug 2014]
7. S. Eliahou, M. Kervaire and B. Saffari, A new restriction on the lengths of Golay complementary sequences, J. Combin. Theory A 55 (1990), 49–59.
8. S. D. Georgiou, S. Stylianou, K. Drosou and C. Koukouvinos, Construction of orthogonal and nearly orthogonal designs for computer experiments, Biometrika (2014), pp. 17.
9. C. Koukouvinos and J. Seberry, New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function – a review, Journal of Statistical Planning and Inference 81 (1999) 153–182.