UDC 519.614
doi:10.15217/issn1684-8853.2015.5.2

NEGAPERIODIC GOLAY PAIRS AND HADAMARD MATRICES

N. A. Balonin[a], *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
D. Z. Djokovic[b], *PhD, Distinguished Professor Emeritus, djokovic@uwaterloo.ca*
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[b]University of Waterloo, Department of Pure Mathematics and Institute for Quantum Computing, Waterloo, Ontario, N2L 3G1, Canada

Purpose: *In analogy with the ordinary and the periodic Golay pairs, we introduce also the negaperiodic Golay pairs. (They occurred first, under a different name, in a paper of Ito.)* ***Methods:*** *We investigate the construction of Hadamard (and weighing) matrices from two negacyclic blocks (2N-type). The Hadamard matrices of 2N-type are equivalent to negaperiodic Golay pairs.* ***Results:*** *If a Hadamard matrix is also a Toeplitz matrix, we show that it must be either cyclic or negacyclic. We show that the Turyn multiplication of Golay pairs extends to a more general multiplication: one can multiply Golay pairs of length g and negaperiodic Golay pairs of length v to obtain negaperiodic Golay pairs of length gv. We show that the Ito's conjecture about Hadamard matrices is equivalent to the conjecture that negaperiodic Golay pairs exist for all even lengths.* ***Practical relevance:*** *Hadamard matrices have direct practical applications to the problems of noise-immune coding and compression and masking of video information.*

Keywords *— Hadamard Matrices, Cyclic Matrices, Negacyclic Matrices, Periodic Golay Pairs, Negaperiodic Golay Pairs.*

Introduction

The Golay pairs (abbreviated as G-pairs, and also known as Golay sequences) have been introduced in a note of M. Golay [1] published in 1961. Since then they have been studied by many reseachers and used in various combinatorial constructions, in particular for the construction of Hadamard matrices [2] and [3, Ch. 23].

The periodic Golay pairs (PG-pairs) made their first appearance, under a different name, in a note of the second author [4] published in 1998. They are equivalent to Hadamard matrices built from two circulant blocks (2C-type). It is now known that periodic Golay pairs exist for infinitely many lengths for which no ordinary Golay pairs are known [5].

In this paper we complete the picture by defining the negaperiodic Golay pairs (NG-pairs). These pairs are equivalent to Hadamard matrices built from two negacyclic blocks (2N-type). The NG-pairs were first introduced by N. Ito, under the name of "associated pairs", in his paper [6] published in 2000. An intereseting observation is that the ordinary Golay pairs are precisely the pairs which are both PG and NG-pairs.

In an earlier paper [7] Ito proposed a conjecture which is stronger than the famous Hadamard conjecture. It turns out that his conjecture is equivalent to the assertion that the NG-pairs exist for all even lengths. This is drastically different from the known facts about ordinary and periodic Golay pairs. Examples of NG-pairs of even length ≤92 are listed in [6]. As far as we know, no NG-pairs of length 94 have been constructed.

We now describe the content of each of the remaining sections.

k-Toeplitz matrices: We show that if a Hadamard matrix is also a Toeplitz matrix, then it must be cyclic or negacyclic. As cyclic Hadamard matrices beyond order 4 are not likely to exist, we conjecture that the same holds true for negacyclic Hadamard matrices beyond order 2. We have verified the latter conjecture for orders ≤40. As a substitute for Ito's conjecture we propose the weaker conjecture in which the two negacyclic blocks are replaced by Toeplitz matrices.

Three kind of Golay pairs: We define negaperiodic autocorrelation function (NAF) and NG-pairs. These are binary sequences of the same length v whose NAFs add up to zero. The length v must be an even integer or 1. For the sake of comparisson we recall some facts about ordinary and PG-pairs. We show that the Turyn multiplication of G-pairs extends to give a multiplication of G-pairs and NG-pairs. More precisely, one can multiply G-pairs of length g and NG-pairs of length v to obtain NG-pairs of length gv. In particular, one can double the length of any NG-pair. We also define a natural equivalence relation for NG-pairs.

Cyclic relative difference families: We introduce a natural bijection Φ_v from the set of binary sequences of length v onto the set of v-subsets of $\mathbf{Z}_{2v}$. We recall the definition of the relative difference families in the cyclic group $\mathbf{Z}_{2v}$ with respect to the subgroup of order 2. We show that a pair of binary sequences of length v is an NG-pair if and only if the Φ_v-images of these sequences form a relative difference family in $\mathbf{Z}_{2v}$. We also show that Ito's conjecture, which entails the Hadamard matrix conjecture, is equivalent to the assertion that NG-pairs exist for all even lengths v.

There are only a few known infinite series of NG-pairs. In the subsequent three sections we treat two of them, the first and second Paley series. First we recall the definition of Paley conference matrices (C-matrices). They have order $1 + q$ where q is an odd prime power. Those for $q \equiv 1 \pmod 4$ give rise to the first Paley series of NG-pairs, with lenth $1 + q$. Those for $q \equiv 3 \pmod 4$ give rise to the second Paley series of NG-pairs, with length $(1 + q)/2$. The main facts that we use are that all Paley C-matrices of the same order are equivalent and that each of these equivalence classes contains a negacyclic C-matrix.

Ito series: We recall that Ito constructed in [7] an infinite series of relative difference sets in dicyclic groups. Hence, this gives an infinite series of NG-pairs to which we refer as the Ito series. However, we show that the Ito series is contained in the second Paley series.

Quasi-Williamson matrices: We recall from [8, Theorem 2.2] the fact that the existence of Ito relative difference sets in the dicyclic group of order $8m$, with m odd, is equivalent to the existence of four generalized Williamson matrices of order m. We coined the name "quasi-Williamson matrices" for this type of generalized Williamson matrices. The four quasi-Williamson matrices have to be circulants but not necessarily symmetric. However, it is required that when plugged into the Williamson array they give a Hadamard matrix of order $4m$. The known series of four Williamson matrices of odd order give rise to the series of NG-pairs. As an example, we have computed four quasi-Williamson matrices of order 35. It is not known whether quasi-Williamson matrices of order 47 exist, and we pose this as an open problem.

Weighing matrices of 2N-type: We apply NG-pairs to the construction of weighing matrices of 2N-type. For small lengths v we list in Appendices B, D and E the NG-pairs of the first and second Paley series and the Ito series, respectively.

k-Toeplitz Hadamard Matrices

We say that a square matrix $\mathbf{A} = [a_{ij}]$, $i, j = 0, 1, \ldots, v-1$, is a Toeplitz matrix if $a_{i,j} = a_{i-1,j-1}$ for $i, j > 0$. In particular, we will be interested in two classes of Toeplitz matrices: cyclic (also known as circulant) and negacyclic. The cyclic and negacyclic matrices of order v are polynomials in the cyclic and negacyclic shift matrix $\mathbf{P}$ and $\mathbf{N}$, respectively:

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & & 0 & 1 \\ 1 & 0 & 0 & & 0 & 0 \end{bmatrix};$$

$$\mathbf{N} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & & 0 & 1 \\ -1 & 0 & 0 & & 0 & 0 \end{bmatrix}. \qquad (1)$$

Definition 1. *A* k-Toeplitz matrix *is a square matrix* $\mathbf{A}$ *partitioned into square blocks* $\mathbf{A}_{ij}$, $i, j = 1, 2, \ldots, k$ *such that each block* $\mathbf{A}_{ij}$ *is a Toeplitz matrix. As a special case* ($k = 1$), *a square Toeplitz matrix is 1-Toeplitz. If each block of a k-Toeplitz matrix is cyclic* (*resp. negacyclic*) *we say that it is* k-cyclic (*resp.* k-negacyclic). *We abbreviate "k-Toeplitz", "k-cyclic", "k-negacyclic" with kT, kC, kN, respectively.*

The k-cyclic Hadamard matrices for $k = 1, 2, 4, 8$ have been studied extensively [1, 2, 9–11]. The k-negacyclic ones also have appeared in the literature but to much lesser extent [6, 12]. In this article we are interested mostly in kT-type Hadamard and weighing matrices with $k = 1, 2, 4$.

For $k = 1$ it turns out that Toeplitz Hadamard matrices are necessarily cyclic or negacyclic.

Proposition 1. *If* $\mathbf{H} = [h_{ij}]$ *is a Toeplitz Hadamard matrix of order* $v \equiv 0 \pmod 4$, *then* $\mathbf{H}$ *is cyclic or negacyclic.*

Proof: Let $\mathbf{h}_i$ be the $(i + 1)$th row of $\mathbf{H}$, $\mathbf{h}_i = [h_{i,0}, h_{i,1}, \ldots, h_{i,v-1}]$. As the rows of $\mathbf{H}$ are orthogonal to each other, all dot products of two different rows are 0, $\mathbf{h}_i \cdot \mathbf{h}_j = 0$ for $i < j$. Let $j \in \{2, 3, \ldots, v-1\}$. Then the equality $\mathbf{h}_0 \cdot \mathbf{h}_{j-1} = \mathbf{h}_1 \cdot \mathbf{h}_j$ simplifies and, by using the hypothesis that $\mathbf{H}$ is a Toeplitz matrix, we deduce that

$$h_{0,v-1} h_{0,v-j} = h_{1,0} h_{j,0}, \ \ j = 2, 3, \ldots, v-1. \qquad (2)$$

Since the entries of $\mathbf{H}$ belong to $\{+1, -1\}$, we have two cases: $h_{1,0} = h_{0,v-1}$ and $h_{1,0} = -h_{0,v-1}$.

In the former case, from the equations (2) we deduce that the equality $h_{j,0} = h_{0,v-j}$ holds for all $j = 1, 2, \ldots, v-1$. This means that the matrix $\mathbf{H}$ is cyclic. Similarly, in the latter case one can show that $\mathbf{H}$ is negacyclic.

There is a conjecture, attributed to Ryser [10, p. 134], that there exist no cyclic Hadamard matrices of order >4. We conjecture that the negacyclic analog holds.

Conjecture 1. *There are no negacyclic Hadamard matrices of order* > 2.

By using a computer we have verified this conjecture for orders ≤40.

For $k = 2$ we shall focus on two special classes of kT-Hadamard matrices, namely the 2C- and 2N-Hadamard matrices having the form

$$\mathbf{H} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ -\mathbf{B}^{\mathrm{T}} & \mathbf{A}^{\mathrm{T}} \end{bmatrix}. \qquad (3)$$

($\mathbf{X}^{\mathrm{T}}$ denotes the transpose of a matrix $\mathbf{X}$.)

From now on we refer to 2T-, 2C- and 2N-matrices having the form (3) as *matrices of 2T-type*, *2C-type and 2N-type*, respectively.

We propose the following conjecture.

Conjecture 2. *For each even integer $v > 0$ there exists a Hadamard matrix of 2T-type and order $2v$.*

We shall see later that the stronger conjecture below is equivalent to the Ito's conjecture about Hadamard matrices (see [7, 8, 13, 14]).

Conjecture 3. *For each even integer $v > 0$ there exists a Hadamard matrix of 2N-type and order $2v$.*

Three Kinds of Golay Pairs

Let $\mathbf{a} = (a_0, a_1, ..., a_{v-1})$ be a sequence of integers of length v. If each $a_i \in \{\pm 1\}$ then we say that the sequence is *binary*. If we allow the sequence to have also 0s, then we say that it is *ternary*. One defines similarly the binary and ternary matrices. We shall consider $\mathbf{a}$ also as a row-vector.

There are three kinds of autocorrelation functions that we attach to an arbitrary sequence $\mathbf{a}$: the ordinary or nonperiodic (AF), the periodic (PAF), and negaperiodic (NAF) autocorrelation functions. They are defined by the formulas

$$\mathrm{AF}_{\mathbf{a}}(k) = \sum_{i=0}^{v-k-1} a_i a_{i+k}, \quad k \in \mathbf{Z}; \tag{4}$$

$$\mathrm{PAF}_{\mathbf{a}}(k) = \mathbf{a} \cdot \mathbf{a}\mathbf{P}^k, \quad k \in \mathbf{Z}; \tag{5}$$

$$\mathrm{NAF}_{\mathbf{a}}(k) = \mathbf{a} \cdot \mathbf{a}\mathbf{N}^k, \quad k \in \mathbf{Z}, \tag{6}$$

where "·" is the dot product. In (4) we use the convention that $a_i = 0$ if $i < 0$ or $i \geq v$.

Note that for $0 \leq k < v$ we have

$$\mathrm{PAF}_{\mathbf{a}}(k) = \mathrm{AF}_{\mathbf{a}}(k) + \mathrm{AF}_{\mathbf{a}}(v-k); \tag{7}$$

$$\mathrm{NAF}_{\mathbf{a}}(k) = \mathrm{AF}_{\mathbf{a}}(k) - \mathrm{AF}_{\mathbf{a}}(v-k). \tag{8}$$

The *cyclic shift* and the *negacyclic shift* of $\mathbf{a}$ are given explicitly by $\mathbf{aP} = (a_{v-1}, a_0, a_1, ..., a_{v-2})$ and $\mathbf{aN} = (-a_{v-1}, a_0, a_1, ..., a_{v-2})$, respectively.

Since $\mathbf{N}^v = -\mathbf{I}$, we have $\mathrm{NAF}_{\mathbf{a}}(k+v) = -\mathrm{NAF}_{\mathbf{a}}(k)$ for all k. It follows immediately from (8) that

$$\mathrm{NAF}_{\mathbf{a}}(v-k) = -\mathrm{NAF}_{\mathbf{a}}(k), \quad 0 \leq k < v. \tag{9}$$

In particular, if v is even then $\mathrm{NAF}_{\mathbf{a}}(v/2) = 0$. We also mention that $\mathbf{a}$, its reverse sequence and the negashifted sequence $\mathbf{aN}$ all have the same NAF.

If $\mathbf{A}$ is the negacyclic matrix with first row $\mathbf{a}$, then $\mathbf{A} = \sum_{i=0}^{v-1} a_i \mathbf{N}^i$. Further, $\mathbf{A}^{\mathrm{T}}$ is negacyclic with first row $(a_0, -a_{v-1}, -a_{v-2}, ..., -a_1)$ and we have

$$\mathbf{A}\mathbf{A}^{\mathrm{T}} = \sum_{k=0}^{v-1} \mathrm{NAF}_{\mathbf{a}}(k) \mathbf{N}^k. \tag{10}$$

(Similar properties are valid for cyclic matrices.)

Let us define three kinds of complementarity:

Definition 2. *The integer sequences $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, ..., \mathbf{a}^{(t)}$, each of length v, are*

(i) complementary if $\sum_{i=1}^{t} \mathrm{AF}_{\mathbf{a}^{(i)}}(k) = 0$ for $k \neq 0$;

(ii) P-complementary if $\sum_{i=1}^{t} \mathrm{PAF}_{\mathbf{a}^{(i)}}(k) = 0$ for $0 < k < v$;

(iii) N-complementary if $\sum_{i=1}^{t} \mathrm{NAF}_{\mathbf{a}^{(i)}}(k) = 0$ for $0 < k < v$.

We now define three kinds of Golay pairs.

Definition 3. A Golay pair (G-pair), periodic Golay pair (PG-pair), negaperiodic Golay pair (NG-pair) *of length v is a pair* $(\mathbf{a}, \mathbf{b})$ *of binary sequences of length v which are complementary, P-complementary, N-complementary, respectively. We denote by* GP_v, PGP_v and NGP_v *the set of Golay, periodic Golay and negaperiodic Golay pairs of length v, respectively.*

For instance, the pair $\mathbf{a} = (1, -1, -1, 1, -1, -1)$, $\mathbf{b} = (1, -1, -1, -1, -1, 1)$ is an NG-pair. It is well known that $\mathrm{GP}_v = \mathrm{PGP}_v = \emptyset$ when v is odd and $v > 1$. We shall see later that this is also true for NGP_v.

The equations (7) and (8) imply that for each $v > 0$ we have $\mathrm{GP}_v = \mathrm{PGP}_v \cap \mathrm{NGP}_v$.

For the definition of equivalence of G-pairs and of PG-pairs see e.g. [9] and [15], respectively. To define the equivalence of NG-pairs $(\mathbf{a}, \mathbf{b})$ of even length v, we introduce the elementary transformations which preserve the set of such pairs:

(i) reverse $\mathbf{a}$ or $\mathbf{b}$;

(ii) replace $\mathbf{a}$ with $\mathbf{aN}$ or $\mathbf{b}$ with $\mathbf{bN}$;

(iii) switch $\mathbf{a}$ and $\mathbf{b}$;

(iv) for k relatively prime to v, replace $\mathbf{a}$ and $\mathbf{b}$ with the sequences $\left(z_i a_{ki(\mathrm{mod}\, v)}\right)_{i=0}^{v-1}$ and $\left(z_i b_{ki(\mathrm{mod}\, v)}\right)_{i=0}^{v-1}$ respectively, where $z_i = 1$ if $ki \pmod{2v} < v$ and $z_i = -1$ otherwise;

(v) replace a_i and b_i with $-a_i$ and $-b_i$, respectively, for each odd index i.

We say that two NG-pairs of the same length are *equivalent* if one can be transformed to the other by a finite sequence of elementary transformations.

As an example, we claim that the NG-pairs $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ of length 10:

$$\mathbf{a} = (+, -, -, -, -, +, -, -, -, -),$$

$$\mathbf{b} = (+, -, -, +, -, +, -, +, +, -);$$

$$\mathbf{c} = (+, -, +, -, +, +, +, -, +, -),$$

$$\mathbf{d} = (+, -, -, +, -, +, -, +, +, -);$$

taken from the Appendices C and D, respectively, are equivalent. (We write " + " and "–" for 1 and –1, respectively.) By applying to $(\mathbf{c}, \mathbf{d})$ the elementary transformation (iv) with $k = 9$, we obtain the pair $(\mathbf{a}, \mathbf{d}')$ where $\mathbf{d}' = (+, -, +, -, -, +, +, -, -, +)$.

After reversing $\mathbf{d}'$ and applying the negacyclic shifts, we can transform $\mathbf{d}'$ to $\mathbf{b}$. This proves our claim.

Ito [6] gives a list of NG-pairs of length $v = 2t$ for all odd integers $t \leq 45$. He also points out that no NG-pair of length 94 is known. Apparently this assertion remains still valid.

For lengths $v \leq 40$, the number of equivalence classes in GP_v and their representatives are known (see e.g. [15]). Very recently, such classification has been carried out in [9] for PGP_v with $v \leq 40$.

It is a well-known fact that there is a bijection from PGP_v to the set of 2C-Hadamard matrices of order $2v$. The image of $(\mathbf{a}, \mathbf{b}) \in \mathrm{PGP}_v$ is the matrix (3) in which $\mathbf{a}$ and $\mathbf{b}$ are the first rows of the circulants $\mathbf{A}$ and $\mathbf{B}$. The following is an NG-analog of that result.

Proposition 2. *If* $(\mathbf{a}, \mathbf{b})$ *is an NG-pair of length* v *then the matrix* (3), *where* $\mathbf{A}$ *and* $\mathbf{B}$ *are the negacyclic blocks with the first rows* $\mathbf{a}$ *and* $\mathbf{b}$ *respectively, is a 2N-type Hadamard matrix of order 2v. Moreover, this map is a bijection.*

Proof: The formula (10) implies that if $(\mathbf{a}, \mathbf{b}) \in \mathrm{NGP}_v$, then the matrix (3) is a 2N-type Hadamard matrix. The converse also holds.

In view of this proposition we can restate Conjecture 3 as follows:

Conjecture 4. $\mathrm{NGP}_v \neq \emptyset$ *for all even* $v > 0$.

Let us recall (see [5]) that there are two non-equivalent multiplications

$$\mathrm{GP}_g \times \mathrm{PGP}_v \to \mathrm{PGP}_{gv}. \quad (11)$$

Interestingly, these two multiplications extend (by using the same formulas) to two multiplications

$$\mathrm{GP}_g \times \mathrm{NGP}_v \to \mathrm{NGP}_{gv}. \quad (12)$$

Consequently, in order to prove Conjecture 4, it suffices to consider the case when $v \equiv 2 \pmod 4$.

We can generalize the multiplications (11) and (12) by replacing PG-pairs and NG-pairs with the periodic complementary ternary (PCT) and nega-periodic complementary ternary (NCT) pairs, respectively. We denote by $\mathrm{PCTP}_{v,w}$ and $\mathrm{NCTP}_{v,w}$ the set of PCT-pairs and NCT-pairs of length v and total weight w, respectively. (The weight is the number of nonzero terms.)

Proposition 3. *The Turyn multiplication of Golay pairs* (*see* [11]) *extends to maps*

$$\mathrm{GP}_g \times \mathrm{PCTP}_{v,w} \to \mathrm{PCTP}_{gv,gw}; \quad (13)$$

$$\mathrm{GP}_g \times \mathrm{NCTP}_{v,w} \to \mathrm{NCTP}_{gv,gw}. \quad (14)$$

Proof: The two proofs are essentially the same and we give the proof only for the case of NCT-pairs. (This proof is similar to the proof of [5, Proposition 3].) Given an integer sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$, we shall represent it by the polynomial $a(z) = a_0 + a_1 z + \ldots + a_{v-1} z^{v-1}$ in the variable z. The Turyn multiplication $(\mathbf{a}, \mathbf{b})(\mathbf{c}, \mathbf{d}) = (\mathbf{e}, \mathbf{f})$, where $(\mathbf{a}, \mathbf{b}) \in \mathrm{GP}_g$ and $(\mathbf{c}, \mathbf{d}) \in \mathrm{GP}_v$, is given by the formulas

$$e(z) = \frac{1}{2}\big(a(z)+b(z)\big)c\big(z^g\big) + \frac{1}{2}\big(a(z)-b(z)\big)d\big(z^{-g}\big)z^{gv-g}; \quad (15)$$

$$f(z) = \frac{1}{2}\big(b(z)-a(z)\big)c\big(z^{-g}\big)z^{gv-g} + \frac{1}{2}\big(a(z)+b(z)\big)d\big(z^g\big). \quad (16)$$

The product $(\mathbf{e}, \mathbf{f}) \in \mathrm{GP}_{gv}$.

Now let us assume that $(\mathbf{c}, \mathbf{d}) \in \mathrm{NCTP}_{v,w}$. We define the integer sequences $\mathbf{e}$ and $\mathbf{f}$ of length gv by the same formulas (15) and (16), respectively. It is easy to see that $\mathbf{e}$ and $\mathbf{f}$ are ternary sequences. Since $(\mathbf{a}, \mathbf{b}) \in \mathrm{GP}_g$ we have

$$a(z)a(z^{-1}) + b(z)b(z^{-1}) = 2g. \quad (17)$$

Since $(\mathbf{c}, \mathbf{d}) \in \mathrm{NCTP}_{v,w}$ we have

$$c(z)c(z)^* + d(z)d(z)^* \equiv w \bmod (z^v + 1). \quad (18)$$

This is an identity in the quotient ring $\mathbf{Z}[z]/(z^v + 1)$, which is equipped with the involution "*" sending z to z^{-1}. A computation shows that

$$\begin{aligned}4e(z)e(z^{-1}) &= (a(z) + b(z))(a(z^{-1}) + b(z^{-1}))c(z^g)c(z^{-g}) + \\ &+ (a(z) - b(z))(a(z^{-1}) - b(z^{-1}))d(z^g)d(z^{-g}) + \\ &+ (a(z) + b(z))(a(z^{-1}) - b(z^{-1}))c(z^g)d(z^g)z^{g-gv} + \\ &+ (a(z) - b(z))(a(z^{-1}) + b(z^{-1}))c(z^{-g})d(z^{-g})z^{gv-g};\end{aligned}$$

$$\begin{aligned}4f(z)f(z^{-1}) &= (a(z) - b(z))(a(z^{-1}) - b(z^{-1}))c(z^g)c(z^{-g}) + \\ &+ (a(z) + b(z))(a(z^{-1}) + b(z^{-1}))d(z^g)d(z^{-g}) + \\ &+ (b(z) - a(z))(a(z^{-1}) + b(z^{-1}))c(z^{-g})d(z^{-g})z^{gv-g} + \\ &+ (a(z) + b(z))(b(z^{-1}) - a(z^{-1}))c(z^g)d(z^g)z^{g-gv}.\end{aligned}$$

By using (17) we obtain that

$$e(z)e(z^{-1}) + f(z)f(z^{-1}) = g(c(z^g)c(z^{-g}) + d(z^g)d(z^{-g})).$$

It follows from (18) that

$$c(z^g)c(z^{-g}) + d(z^g)d(z^{-g}) \equiv w \bmod (z^{gv} + 1)$$

and so we have

$$e(z)e(z^{-1}) + f(z)f(z^{-1}) \equiv gw \bmod (z^{gv} + 1).$$

We conclude that $(\mathbf{e}, \mathbf{f}) \in \mathrm{NCTP}_{gv,gw}$.

In the special case when $g = 2$ and $(\mathbf{a}, \mathbf{b}) = ((+, -), (+, +))$ we obtain a map $\mathrm{NCTP}_{v,w} \to \mathrm{NCTP}_{2v,2w}$ to which we refer as "multiplication by 2".

Cyclic Relative Difference Families

Let us define the map, Φ_v, from the set of binary sequences of length v into the set of v-subsets of the finite cyclic group $\mathbf{Z}_{2v}$ of integers modulo $2v$. If $\mathbf{a} = (a_0, a_1, ..., a_{v-1})$ is a binary sequence then

$$\Phi_v(\mathbf{a}) = \{i : a_i = 1\} \cup \{v + i : a_i = -1\}. \qquad (19)$$

Note that Φ_v is injective and that its image consists of all v-subsets $X \subset \mathbf{Z}_{2v}$ such that $i - j \neq v$ for all $i, j \in X$.

We also need the definition of relative difference families in $\mathbf{Z}_{2v}$. They are relative to the subgroup $\{0, v\}$ of order 2.

Definition 4. *The subsets* $X_1, X_2 ..., X_S$ *of* $\mathbf{Z}_{2v}$ *form a* relative difference family *if for each integer* $m \in \mathbf{Z}_{2v}\backslash\{0, v\}$ *the set of triples* $\{(i, j, k):\{i, j\} \subseteq X_k, i - j \equiv m \pmod{2v}\}$ *has fixed cardinality* λ, *independent of* m, *and there is no such triple if* $m = v$.

Note that the parameter λ is uniquely determined by the obvious equation

$$\sum_{i=1}^{s} k_i(k_i - 1) = 2\lambda(v - 1), \qquad (20)$$

where $k_i = |X_i|$ is the cardinality of X_i.

Let us now define the equivalence of relative difference families consisting of two v-subsets X, $Y \subset \mathbf{Z}_{2v}$. First we define five types of elementary transformations which preserve such families:

(i) replace X or Y with its image by the map $i \to v - 1 - i \pmod{2v}$;

(ii) replace X or Y with its image by the map $i \to i + 1 \pmod{2v}$;

(iii) switch X and Y;

(iv) for k relatively prime to $2v$, replace X and Y with their images by the map $i \to ki \pmod{2v}$;

(v) replace X and Y with their images by the map which fixes the even integers and sends $i \to v + i \pmod{2v}$ if i is odd.

Definition 5. *Two relative difference families* (X, Y) *and* (X', Y') *on* $\mathbf{Z}_{2v}$ *are* equivalent *to each other if one can be transformed to the other by a finite sequence of the above elementary transformations.*

Let $(\mathbf{a}, \mathbf{b})$ be a pair of binary sequences of length v and let $X = \Phi_v(\mathbf{a})$ and $Y = \Phi_v(\mathbf{b})$ be the corresponding v-subsets of $\mathbf{Z}_{2v}$. We shall see below that $(\mathbf{a}, \mathbf{b})$ is an NG-pair if and only if (X, Y) is a relative difference family. Moreover, the mapping sending $(\mathbf{a}, \mathbf{b}) \to (\Phi_v(\mathbf{a}), \Phi_v(\mathbf{b}))$ preserves the equivalence classes. This follows from the fact that Φ_v commutes with the elementary operations (i–v) defined for NG-pairs in the previous section and defined above for relative difference families. For instance, if $\mathbf{a}'$ is the binary sequence obtained from $\mathbf{a}$ by applying the elementary transformation (i), then the set $\Phi_v(\mathbf{a}')$ is obtained from $\Phi_v(\mathbf{a})$ by applying the elementary transformation (i) defined above.

As indicated above, the NG-pairs are closely related to relative difference families. The following two propositions make this more precise.

Proposition 4. *Let* $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, ..., \mathbf{a}^{(s)}$ *be binary sequences of length* v *and let* $X_1, X_2, ..., X_s$ *be the subsets of* $\mathbf{Z}_{2v}$ *defined by* $X_i = \Phi_v(\mathbf{a}^{(i)})$. *If* $X_1, X_2, ..., X_s$ *form a relative difference family in* $\mathbf{Z}_{2v}$, *then the sequences* $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, ..., \mathbf{a}^{(s)}$ *are N-complementary.*

Proof: We identify the group ring of $\mathbf{Z}_{2v}$ over the integers with the quotient ring $\mathbf{Z}[x]/(x^{2v} - 1)$ of the polynomial ring $\mathbf{Z}[x]$. The cyclic group $\mathbf{Z}_{2v}$ is identified with the multiplicative group $\langle x\rangle$ by the isomorphism sending $i \to x^i$. The inversion map on $\langle x\rangle$ extends to an involutory automorphism of $\mathbf{Z}[x]/(x^{2v} - 1)$ which we denote by "*". The subsets X_i are now viewed as subsets of $\langle x\rangle$, and will be identified with the sum of their elements in $\mathbf{Z}[x]/(x^{2v} - 1)$.

Since the X_i form a relative difference family, we have

$$\sum_{i=1}^{s} X_i X_i^* = \sum_{i=1}^{s} k_i + \lambda\left(1 + x^v\right)\left(x + x^2 + \ldots + x^{v-1}\right). \qquad (21)$$

The ring of integer negacyclic matrices of order v is isomorphic to the quotient ring $\mathbf{Z}[x]/(x^v + 1)$. It also has an involutory automorphism "*" which sends x to x^{-1}. Let f: $\mathbf{Z}[x]/(x^{2v} - 1) \to \mathbf{Z}[x]/(x^v + 1)$ be the canonical homomorphism and note that $f(x^v) = -1$. By applying f to the identity (21) we obtain that

$$\sum_{i=1}^{s} f(X_i) f(X_i)^* = \sum_{i=1}^{s} k_i.$$

Note that $f(X_i) = \sum_{j=0}^{v-1} a_j^{(i)} x^j$ and

$$f(X_i) f(X_i)^* = \sum_{i=1}^{v-1} \mathrm{NAF}_{\mathbf{a}^{(i)}}(j) x^j.$$

It follows that $\sum_{j=0}^{s} \mathrm{NAF}_{\mathbf{a}^{(i)}}(j) = 0$ for $j = 1, 2, ..., v - 1$, i.e., the sequences $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, ..., \mathbf{a}^{(s)}$ are N-complementary.

The following partial converse holds.

Proposition 5. *Let* $\mathbf{a} = (a_0, a_1, ..., a_{v-1})$ *and* $\mathbf{b} = (b_0, b_1, ..., b_{v-1})$ *be an NG-pair. Then the subsets* $X = \Phi_v(\mathbf{a})$ *and* $Y = \Phi_v(\mathbf{b})$ *form a relative difference family in* $\mathbf{Z}_{2v}$ *with parameter* $\lambda = v$.

Proof: We set $R = \mathbf{Z}[x]/(x^{2v} - 1)$, $R^+ = \mathbf{Z}[x]/(x^v - 1)$ and $R^- = \mathbf{Z}[x]/(x^v + 1)$. Denote the canonical image of $x \in R$ in R^+ and R^- by y and z, respectively. In the proof of Proposition 4 we have defined the involution "*" in R and R^+. There is also one in R^- which sends $z \to z^{-1} = -z^{v-1}$. These involutions commute with the canonical homomorphisms f: $R \to R^-$ and g: $R \to R^+$. Note that R is isomorphic to the direct product $R^+ \times R^-$.

Since $(\mathbf{a}, \mathbf{b})$ is an NG-pair, the elements p, $q \in R^-$ defined by $p = \sum a_i z^i$ and $q = \sum b_i z^i$ satisfy

$pp^* + qq^* = 2v$. For convenience we identify X with the sum of its elements in R, and similarly for Y. Then we have $f(X) = p$ and $f(Y) = q$. It follows that $f(XX^* + YY^* - 2v) = 0$. Thus $XX^* + YY^* - 2v$ belongs to the kernel of f and, by using the fact that $(x^v + 1)x^v = x^v + 1$ in R, we obtain an equality

$$XX^* + YY^* =$$
$$= 2v + (x^v + 1)(c_0 + c_1 x + ... + c_{v-1}x^{v-1}), \quad (22)$$

where the c_i are some integers. Since $X = \Phi_v(\mathbf{a})$ and $y^v = 1$, we have $g(X) = 1 + y + ... + y^{v-1}$. Similarly, $g(Y) = g(X)$. Note that $g(X)^* = g(X)$ and $g(X)^2 = vg(X)$. Hence, by applying g to the equality (22), we obtain that

$$2v(1 + y + ... + y^{v-1}) =$$
$$= 2v + 2(c_0 + c_1 y + ... + c_{v-1}y^{v-1}).$$

We deduce that $c_0 = 0$ and $c_i = v$ for $i \neq 0$. The equality (22) now gives

$$XX^* + YY^* = 2v + v(x^v + 1)(x + x^2 + ... + x^{v-1}).$$

Hence X and Y indeed form a relative difference family in $\mathbf{Z}_{2v}$ with the parameter $\lambda = v$.

It was shown in [13, Conjecture 1] that the Ito's conjecture is equivalent to the assertion that for each $t \geq 1$ there exists a relative difference family X_1, X_2 in the cyclic group $\mathbf{Z}_{4t}$ with $|X_1| = |X_2| = 2t$ and $\lambda = 2t$. By Propositions 4 and 5 this is in turn equivalent to Conjecture 4.

Paley C-matrices

A *conference matrix* (or *C-matrix*) of order v is a matrix $\mathbf{C}$ of order v whose diagonal entries are 0, the other entries are ±1, and such that $\mathbf{CC}^T = (v - 1)\mathbf{I}$, where $\mathbf{I}$ is the identity matrix. There are two well-known necessary conditions for the existence of such matrices. First, v must be even. (We exclude hereafter the trivial case $v = 1$.) Second, if $v \equiv 2 \pmod 4$ then $v-1$ must be the sum of two squares. For the existence of negacyclic C-matrices of order $v \equiv 4 \pmod 8$ there is another necessary condition [12], namely that $v - 1 = a^2 + 2b^2$ for some integers a and b.

Two C-matrices are said to be *equivalent* if they have the same order and one can be obtained from the other by applying a finite sequence of the following elementary transformations: multiplication of a row or a column by –1, and interchanging simultaneously two rows and the corresponding two columns.

If $v = 1 + q$ where q is a power of a prime, then Paley [16] has constructed conference matrices of order v. His construction employs essentially the theory of finite fields. Let us recall a general definition as given in [12]. Denote by V a two-dimensional vector space over the Galois field GF(q). Choose any set X of $1 + q$ pairwise linearly independent vectors of V. Denote by χ the quadratic character of GF(q). In particular, $\chi(0) = 0$. (If q is a prime, then χ is the classical Legendre symbol.) Then the matrix

$$\mathbf{C}_X = [\chi(\det(\xi, \eta))], \quad \xi, \eta \in X \quad (23)$$

associated with X, is a C-matrix of order $1 + q$. If $q \equiv 1 \pmod 4$ then $\chi(-1) = 1$ while when $q \equiv 3 \pmod 4$ we have $\chi(-1) = -1$. Hence, $\mathbf{C}_X$ is symmetric in the former case and skew-symmetric in the latter case. We refer to $\mathbf{C}_X$ as the *Paley* (*conference*) *matrix*. It is known that all Paley conference matrices of the same order are equivalent to each other [17].

In contrast to Conjecture 1, there exist an infinite series of negacyclic C-matrices. Indeed, it is shown in [12, Corollary 7.2] that each Paley C-matrix is equivalent to a negacyclic C-matrix.

Consequently, the following facts hold.

Proposition 6. *Let q be an odd prime power. Then there exist*

(i) *a negacyclic conference matrix* $\mathbf{C}$ *of order* $1 + q$;

(ii) *a 2N-type Hadamard matrix* $\mathbf{H}$ *of order* $2(1 + q)$;

(iii) *an NG-pair of length* $1 + q$.

Proof: In (ii) we can take $\mathbf{H}$ to be the matrix (3) with $\mathbf{A} = \mathbf{C} + \mathbf{I}$ and $\mathbf{B} = \mathbf{C} - \mathbf{I}$. By Proposition 2, (iii) is equivalent to (ii). Explicitly, if $(0, c_1, c_2, ..., c_q)$ is the first row of $\mathbf{C}$, then the sequences $(1, c_1, c_2, ..., c_q)$ and $(-1, c_1, c_2, ..., c_q)$ form an NG-pair of length $1 + q$.

In Appendix A we list the first rows of the negacyclic Paley C-matrices of order $v = 1 + q \leq 128$.

Let $\mathbf{C}$ be a negacyclic conference matrix of order v with first row $(0, c_1, c_2, ..., c_{v-1})$. By a theorem of Belevitch [12, Theorem 4.1] we have

$$c_{v/2+j} = (-1)^j c_{v/2-j}, \quad j = 1, 2, ..., v/2 - 1. \quad (24)$$

One may try to find a counter-example to Conjecture 1 as follows. Let $q \equiv 3 \pmod 4$ be a prime power. There exists a negacyclic Paley C-matrix $\mathbf{C}$ of order $1 + q$. However, the equations (24) imply that $\mathbf{C}$ is not skew-symmetric. Hence $\mathbf{C} + \mathbf{I}$ is not a Hadamard matrix. On the other hand, we know that $\mathbf{C}$ is equivalent to a skew-symmetric conference matrix $\mathbf{C}'$, and so $\mathbf{C}' + \mathbf{I}$ is a Hadamard matrix. However, $\mathbf{C}' + \mathbf{I}$ is not negacyclic. It appears that $\mathbf{C}$ cannot be used to give a negacyclic Hadamard matrix of order $1 + q$.

The two cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ in Proposition 6 should be considered separately. Indeed, we shall show in a later section that in the latter case the assertion (iii) of Proposition 6 can be made stronger, namely we can replace $1 + q$ by $(1 + q)/2$.

The First Paley Series

We say that any NG-pair $(\mathbf{a}, \mathbf{b})$ of length $v = 1 + q$ resulting from Proposition 6, with $q \equiv 1 \pmod 4$, belongs to the *first Paley series*. From the proof of that proposition, we recall that $\mathbf{a}$ and $\mathbf{b}$ are the same sequence except that $b_0 = -a_0$.

In this section we assume that q is a prime power and that $q \equiv 1 \pmod 4$. We recall Theorem 7.3 of [12].

It is easy to verify that if $\mathbf{A}$ is a negacyclic matrix of odd order t and $\mathbf{Z}$ the diagonal matrix of order t with the diagonal elements 1, –1, 1, –1, ..., then the matrix $\mathbf{ZAZ}$ is cyclic (and the converse holds).

Proposition 7. *Any Paley conference matrix of order $v = 1 + q \equiv 2 \pmod 4$, q a prime power, is equivalent to a conference matrix of 2C-type with symmetric circulant blocks.*

Let us give an independent and constructive proof of Proposition 7 in the case of negacyclic conference matrices.

Proof: Let $\mathbf{C}$ be a negacyclic conference matrix of order $v \equiv 2 \pmod 4$. We shall transform it into the 2N-form, and also into the 2C-form with symmetric blocks.

First, we split the first row $\mathbf{c} = (0, c_1, c_2, ..., c_{v-1})$ of $\mathbf{C}$ into two pieces $\mathbf{a} = (0, c_2, c_4, ..., c_{v-2})$ and $\mathbf{b} = (c_1, c_3, ..., c_{v-1})$. One can easily verify that for each integer k we have $\mathrm{NAF}_{\mathbf{c}}(2k) = \mathrm{NAF}_{\mathbf{a}}(k) + \mathrm{NAF}_{\mathbf{b}}(k)$. It follows that $\mathbf{a}$ and $\mathbf{b}$ are N-complementary sequences. Let $\mathbf{A}$ and $\mathbf{B}$ be the negacyclic matrices with first row $\mathbf{a}$ and $\mathbf{b}$, respectively. By plugging the blocks $\mathbf{A}$ and $\mathbf{B}$ into the array (3), we obtain a C-matrix of 2N-type.

Second, we replace $\mathbf{A}$ and $\mathbf{B}$ with the circulants $\mathbf{ZAZ}$ and $\mathbf{ZBZ}$. The equations (24) imply that the block $\mathbf{ZAZ}$ is symmetric and the first row of $\mathbf{ZBZ}$ is symmetric.

Third, we replace the block $\mathbf{ZBZ}$ with $\mathbf{ZBZP}^m$ where $m = (q - 1)/4$. Note that $\mathbf{ZBZP}^m$ is a symmetric circulant. There is no need to change the block $\mathbf{ZAZ}$. By plugging the blocks $\mathbf{ZAZ}$ and $\mathbf{ZBZP}^m$ into the array (3), we obtain a C-matrix of 2C-type with symmetric blocks.

Let us give an example. For $q = 13$ we have $v = 14$ and $m = 3$. From the table in Appendix A, the first row of $\mathbf{C}$ is $\mathbf{c} = (0, +, +, +, +, +, -, -, +, +, -, +, -, +)$. Thus, $\mathbf{a} = (0, +, +, -, +, -, -)$ and $\mathbf{b} = (+, +, +, -, +, +, +)$. The first rows of $\mathbf{ZAZ}$ and $\mathbf{ZBZ}$ are $\mathbf{a}' = (0, -, +, +, +, +, -)$ and $\mathbf{b}' = (+, -, +, +, +, -, +)$. Finally, the first row of the circulant $\mathbf{ZBZP}^m$ is $\mathbf{b}'' = (+, +, -, +, +, -, +)$. Thus, the block $\mathbf{ZBZP}^m$ is also symmetric. By plugging the symmetric circulants $\mathbf{A}$ and $\mathbf{B}$ with first rows $\mathbf{a}'$ and $\mathbf{b}''$ into the array (3), we obtain the desired C-matrix of 2C-type.

In Appendix B, for negacyclic Paley C-matrices listed in Appendix A and of order $v \equiv 2 \pmod 4$, we list the first rows of the symmetric circulant blocks computed by the above procedure.

The Second Paley Series

In this section we denote by $\mathbf{C}$ a negacyclic C-matrix of order $n \equiv 0 \pmod 4$. For convenience we set $v = n/2$. We give a very simple construction for NG-pairs of length v. In particular we can take $n = 1 + q$ where $q \equiv 3 \pmod 4$ is a prime power. Indeed, as mentioned earlier, we know that any Paley C-matrix of order $1 + q$ is equivalent to a negacyclic C-matrix. We point out that we do not have any other examples of matrices $\mathbf{C}$.

Proposition 8. *Let* $\mathbf{C}$ *be a negacyclic C-matrix of order* $n \equiv 0 \pmod 4$. *If* $\mathbf{c} = (0, c_1, c_2, ..., c_{n-1})$ *is the first row of* $\mathbf{C}$, *then the sequences* $\mathbf{a} = (1, c_2, c_4, ..., c_{n-2})$ *and* $\mathbf{b} = (c_1, c_3, ..., c_{n-1})$ *form an NG-pair of length* $v = n/2$.

Proof: For convenience, we set $\mathbf{a}' = (0, c_2, c_4, ..., c_{n-2})$. Then $\mathrm{NAF}_{\mathbf{a}'}(k) + \mathrm{NAF}_{\mathbf{b}}(k) = \mathrm{NAF}_{\mathbf{c}}(2k)$ for $k = 1, 2, ..., v - 1$. Since $\mathbf{C}$ is a conference matrix, it follows from (10) that $\mathrm{NAF}_{\mathbf{c}}(k) = 0$ for $k = 1, 2, ..., n - 1$. Hence, $(\mathbf{a}', \mathbf{b})$ is an N-complementary pair. However, this is not an NG-pair because the first term of $\mathbf{a}'$ is 0.

Let us write $\mathbf{a}'' = (x, a_1, a_2, ..., a_{v-1})$ with $a_i = c_{2i}$ for $i = 1, 2, ..., v–1$ and x an integer variable. We claim that $\mathrm{NAF}_{\mathbf{a}''}(k) = \mathrm{NAF}_{\mathbf{a}'}(k)$ for $0 < k < v$. Indeed, we have $\mathrm{NAF}_{\mathbf{a}''}(k) = \mathrm{AF}_{\mathbf{a}''}(k) - \mathrm{AF}_{\mathbf{a}''}(v - k) = \mathrm{NAF}_{\mathbf{a}'}(k) + x(a_k - a_{v-k})$. By Belevitch's theorem, we have $a_k = a_{v-k}$ for $0 < k < v$ and so $\mathrm{NAF}_{\mathbf{a}'}(k) = \mathrm{NAF}_{\mathbf{a}}(k)$. Thus our claim is proved.

If we now set $x = 1$ then $\mathbf{a}'' = \mathbf{a}$ and we conclude that $\mathrm{NAF}_{\mathbf{a}}(k) = \mathrm{NAF}_{\mathbf{a}'}(k)$ for $0 < k < v$. Consequently, $(\mathbf{a}, \mathbf{b})$ is an NG-pair.

We say that the NG-pairs constructed in this proposition belong to the *second Paley series*. We say that an NG-pair is a *Paley NG-pair* if it belongs to the first or the second Paley series.

Out of the 63 odd positive integers $t \le 125$, there are exactly 18 for which there is no Paley NG-pair of length $v = 2t$. Let us list these integers:

$$23, 29, 39, 43, 47, 59, 65, 67, 73, 81,$$
$$89, 93, 101, 103, 107, 109, 113, 119. \qquad (25)$$

In Appendix C we list the NG-pairs in the second Paley series obtained from the negacyclic C-matrices listed in Appendix A with $q \equiv 3 \pmod 4$.

Ito Series

There is another series, due to Ito [7], of NG-pairs of length $(1 + q)/2$ when $q \equiv 3 \pmod 4$ is a prime power. However, we will show below that the NG-pairs in this series belong to the second Paley series.

For convenience we set $t = (1 + q)/4 = v/2$ and let p be the prime such that $q = p^n$. The Ito series is derived from the relative difference sets constructed by Ito [7]. These relative difference sets R have parameters $(4t, 2, 4t, 2t)$ and lie in the dicyclic group

$$\mathrm{Dic}_{8t} = \langle a^{4t} = 1, b^2 = a^{2t}, bab^{-1} = a^{-1} \rangle \qquad (26)$$

of order $8t$. The forbidden subgroup is $\langle b^2 \rangle$.

For convenience we identify a subset $X \subseteq \mathrm{Dic}_{8t}$ with the sum of its elements in the group-ring (over $\mathbf{Z}$) of Dic_{8t}. Then we can write $R = R_1 + R_2 b$ with $R_1, R_2 \subseteq \langle a \rangle$. The sets R_1 and R_2 form a relative difference family in the cyclic group $\langle a \rangle$ (with the same forbidden subgroup). Let us identify $\langle a \rangle$ with $\mathbf{Z}_{4t}$ by the isomorphism sending $a \to 1$. It is obvious that R_1 and R_2 are $2t$-subsets of $\mathbf{Z}_{4t}$. By Proposition 4, the binary sequences $X_1 = \Phi_v^{-1}(R_1)$ and $X_2 = \Phi_v^{-1}(R_2)$ form an NG-pair.

We shall now describe a procedure which takes as input the integer t and a primitive polynomial f of degree $2n$ over the prime field $\mathrm{GF}(p) = \mathbf{Z}_p$, and gives as output the NG-pair arising from the Ito's difference set R in Dic_{8t}. This procedure is based on the simplification of Ito's construction due to B. Schmidt [8, Theorem 3.3].

We construct the Galois field $\mathrm{GF}(q^2)$ by adjoining a root x of f to $\mathbf{Z}_p$. As $q^2 - 1 = ((q-1)/2)(2(q+1))$ and $(q-1)/2 = 2t - 1$ and $2(q+1) = 8t$ are relatively prime, the multiplicative group $\mathrm{GF}(q^2)^*$ is a direct product of the subgroups U of order $(q-1)/2$ and W of order $2(q+1)$. Note that U is the subgroup of squares in $\mathrm{GF}(q^2)^*$. (Thus we have $Q = U$ for the set Q defined in the proof of [8, Theorem 3.3].)

As f is primitive, x generates $\mathrm{GF}(q^2)^*$ and the elements $u = x^{8t}$ and $w = x^{2t-1}$ generate U and W, respectively. Since $x^{(q^2-1)/2} = -1$, the element $\alpha = x^{2t}$ satisfies the equation $\alpha + \alpha^q = 0$, i.e., $\mathrm{tr}(\alpha) = 0$ where tr: $\mathrm{GF}(q^2) \to \mathrm{GF}(q)$ is the (relative) trace map. We set $v = 2t$ and define two binary sequences $\mathbf{a} = (a_0, a_1, ..., a_{v-1})$ and $\mathbf{b} = (b_0, b_1, ..., b_{v-1})$ of length v. We declare that $a_i = 1$ if and only if $\mathrm{tr}(\alpha w^{2i}) \in U$, and declare that $b_i = 1$ if and only if $\mathrm{tr}(\alpha w^{2i+1}) \in U$. Then $(\mathbf{a}, \mathbf{b}) \in \mathrm{NGP}_v$. Note that $a_0 = -1$.

We say that the NG-pairs obtained by this procedure belong to the *Ito series*. They exist for lengths $v = 2t$ where $q = 4t - 1$ is a prime power.

For a sequence $\mathbf{a} = (a_0, a_1, ..., a_{v-1})$ we say that it is *quasi-symmetric* if $a_i = a_{v-i}$ for $i = 1, 2, ..., v-1$. Note that the negacyclic matrix with first row $\mathbf{a}$ is skew-symmetric if and only if $\mathbf{a}$ is quasi-symmetric and $a_0 = 0$.

The Ito NG-pairs $(\mathbf{a}, \mathbf{b})$ have some additional symmetries. Namely, $\mathbf{a}$ is quasi-symmetric and $\mathbf{b}$ is skew-symmetric. Both assertions follow from the fact that

$$\mathrm{tr}(\alpha w^{8t-i}) = \mathrm{tr}(\alpha w^{-i}) = \alpha(w^{-i} - w^{-iq}) =$$
$$= \alpha w^{-i(q+1)}(w^{iq} - w^i) = (-1)^i \mathrm{tr}(\alpha w^i).$$

These symmetry properties were observed by Ito [7, Proposition 6], as well as the fact that the 2N-type Hadamard matrix constructed from the NG-pair $(-\mathbf{a}, \mathbf{b})$ is skew-Hadamard. (Since the diagonal entries of a skew-Hadamard matrix have to be equal to $+1$, we replaced $\mathbf{a}$ with $-\mathbf{a}$.)

It follows from these symmetry properties that the negacyclic matrix with first row

$$(0, b_0, a_1, b_1 ..., a_{v-1}, b_{v-1})$$

is a conference matrix. This shows that the NG-pair $(-\mathbf{a}, \mathbf{b})$ belongs to the second Paley series.

In Appendix D we list the NG-pairs of length $v = (1+q)/2 \le 154$ in the Ito series, with $q \equiv 3 \pmod 4$ a prime power. We have verified directly that each NG-pair listed in Appendix C is equivalent to the corresponding NG-pair (the one having the same length, v) in the list of Appendix D.

There exist prime powers $q > 1$ such that $q \equiv 1 \pmod 4$ and $1 + 2q$ is also a prime power. For instance, $q = 5, 9, 13, 29, 41$. For such q there exist NG-pairs $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ of length $1 + q$ which belong to the first and the second Paley series, respectively. Then the following question arises: can $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ be equivalent? (We believe that the answer is negative.)

Quasi-Williamson Matrices

We say that four binary matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$ of order t are *quasi-Williamson matrices* if they are circulants and satisfy the equations

$$\mathbf{A}\mathbf{A}^T + \mathbf{B}\mathbf{B}^T + \mathbf{C}\mathbf{C}^T + \mathbf{D}\mathbf{D}^T = 4t\mathbf{I}; \qquad (27)$$

$$\mathbf{A}\mathbf{B}^T + \mathbf{C}\mathbf{D}^T = \mathbf{B}\mathbf{A}^T + \mathbf{D}\mathbf{C}^T. \qquad (28)$$

This is the cyclic case of a more general definition given in [8]. In order to avoid a possible confusion, we have introduced a different name for this type of matrices. Note that the above two equations amount to saying that the matrix

$$\begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C}^T & \mathbf{D}^T & \mathbf{A}^T & -\mathbf{B}^T \\ -\mathbf{D}^T & -\mathbf{C}^T & \mathbf{B}^T & \mathbf{A}^T \end{bmatrix} \qquad (29)$$

is a Hadamard matrix.

The *Williamson matrices* are the special case of quasi-Williamson matrices where we require all four blocks $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}$ to be symmetric, in which case the condition (28) is automatically satisfied. Let us mention the following two infinite series of Williamson matrices of order t. The first, due to Turyn, exists in orders $t = (1+q)/2$, where $q \equiv 1 \pmod 4$ is a prime power. Given a conference matrix of 2C-type, see Proposition 7, with symmetric circulant blocks, say $\mathbf{A}$ and $\mathbf{B}$, then the matrices $\mathbf{A} + \mathbf{I}$, $\mathbf{A} - \mathbf{I}$, $\mathbf{B}$, $\mathbf{B}$ are four Williamson matrices (this is the

Turyn series). The second, due to Whiteman, exists in orders $t = p(1 + p)/2$, where $p \equiv 1 \pmod 4$ is a prime.

In the rest of this section we assume that t is odd. Then quasi-Williamson matrices of order t are equivalent to relative difference sets in Dic_{8t} [8].

Let **a**, **b**, **c**, **d** be the first rows of quasi-Williamson matrices of order t. We set $z = 1$ if $t \equiv 1 \pmod 4$ and $z = -1$ otherwise. We shall describe a procedure which takes as input the quadruple **a**, **b**, **c**, **d** and gives as output an NG-pair of length $v = 2t$. It is based on the proof of [8, Theorem 2.1]. The subgroup $G \times \langle x \rangle$ of the group $G \times Q_8$, in the mentioned proof, is cyclic and is identified with $\mathbf{Z}_{4t}$.

By using the rows **a** and **b**, we construct a binary sequence p of length v as follows. Say, $\mathbf{a} = (a_0, a_1, \ldots, a_{t-1})$. We define two subsets $\mathbf{a}'$, $\mathbf{a}''$ of $\mathbf{Z}_t$ by $\mathbf{a}' = \{i : a_i = 1\}$ and $\mathbf{a}'' = \{i : a_i = -1\}$. We define similarly the subsets $\mathbf{b}', \mathbf{b}'' \subseteq \mathbf{Z}_t$.

For $i = 0, 1, 2, 3$ we define the map $\Psi_i\colon \mathbf{Z}_t \to \mathbf{Z}_{4t}$ by the formula

$$\Psi_i(j) = j + t(z(i - j) \pmod 4). \qquad (30)$$

It is easy to verify that the set

$$X = \Psi_0(\mathbf{a}') \cup \Psi_1(\mathbf{b}') \cup \Psi_2(\mathbf{a}'') \cup \Psi_3(\mathbf{b}'')$$

lies in the image of the map Φ_v [see (19)]. Finally, we set $p = \Phi_v^{-1}(X)$, which is a binary sequence of length v.

Similarly, from **c** and **d** we construct first a v-subset $Y \subseteq \mathbf{Z}_{4t}$ and then the binary sequence $q = \Phi_v^{-1}(Y)$, of length v. Then $(p, q) \in \mathrm{NGP}_v$.

We remark that the v-subsets X and Y form a relative difference family in $\mathbf{Z}_{2v}$ with parameter $\lambda = v$ and the forbidden subgroup $\{0, v\}$.

The converse is also true: given an NG-pair (**a**, **b**) of length $2t$ we can construct quasi-Williamson matrices **A**, **B**, **C**, **D** of order t. As an example, we used the NG-pair of length $v = 70$ given in Appendix D to compute four quasi-Williamson matrices **A**, **B**, **C**, **D** of order 35. The first rows of these matrices (after some cyclic shifts) are:

$$\mathbf{a} = [+, -, +, +, -, +, -, +, +, +, +, +, -, +, +, +, -, -, +, +, -, -, -, +, -, -, -, -, -, +, -, +, -, -, +],$$

$$\mathbf{b} = [+, +, +, +, +, -, -, -, +, -, +, +, -, +, +, +, -, +, +, -, +, +, +, -, +, +, -, +, -, -, -, +, +, +, +];$$

$$\mathbf{c} = [-, +, -, +, +, -, +, -, +, +, +, -, -, -, -, +, +, +, +, +, +, -, -, +, +, -, +, -, +, -, -, -, +, +, -],$$

$$\mathbf{d} = [-, +, +, -, -, -, +, -, +, -, +, +, -, -, +, +, +, +, +, +, -, -, -, -, +, +, +, -, +, -, +, +, -, +, -],$$

respectively. The blocks **A**, **B**, **C**, **D** satisfy the equations (27) and (28), and when plugged into the array (29) we do get a Hadamard matrix. Moreover, **A** is of skew-type, while **B** is symmetric, and **d** is the reverse of **c**. Note also that $\mathbf{AB}^{\mathrm{T}} - \mathbf{BA}^{\mathrm{T}} = (\mathbf{A} - \mathbf{A}^{\mathrm{T}})\mathbf{B} \neq 0$, and so **A**, **B**, **C**, **D** are not matrices of Williamson type according to [2, Definition 3.3].

It is known that Williamson matrices of odd order t exist for $t = 23, 29, 39, 43$, see e.g. [18]. After removing these integers, the list (25) reduces to

$$47, 59, 65, 67, 73, 81, 89, 93, 101, 103, 107, 109, 113, 119. \qquad (31)$$

Let us single out the smallest case.

Open Problem. Do quasi-Williamson matrices of order 47 exist? Equivalently, do NG-pairs of length 94 exist?

The above mentioned facts have been known since 1999 [8, 6] and apparently no progress has been made so far in the search for NG-pairs of order $v = 2t$, for t in the above list. For generalizations where the cyclic group $\mathbf{Z}_{4t}$ is replaced by more general finite abelian groups see [14].

Since the known infinite series of NG-pairs are rather sparse, it is hard to believe that NG-pairs exist for all even lengths. In other words, in our opinion Ito's conjecture is likely to be false.

Weighing Matrices of 2N-type

A *weighing matrix* of order n and *weight* w (abbreviated as $\mathbf{W}(n, w)$) is a matrix $\mathbf{W}$ of order n with entries in $\{0, \pm 1\}$ such that $\mathbf{WW}^{\mathrm{T}} = w\mathbf{I}$. In this section we discuss the existence of weighing matrices of 2N-type.

Note that C-matrices of order v are $\mathbf{W}(v, v-1)$. It is known that there are no cyclic $\mathbf{W}(v, v-1)$ for $v > 2$ [19]. On the other hand there are infinitely many negacyclic $\mathbf{W}(v, v-1)$. Indeed each Paley C-matrix is equivalent to a negacyclic C-matrix. It has been conjectured [12] that there are no negacyclic C-matrices of even order $v \neq 1 + q$, q a prime power. This conjecture has been verified for $v \leq 226$. However, there exist C-matrices of 2N-type whose order v is not of that form. For instance, they exist for

$$v = 16, 40, 52, 56, 64, 88, 96, 120, 136, 144, 160.$$

(See part (iii) of the proposition below.)

We have four infinite series of 2N-type weighing matrices.

Proposition 9. *Let q be an odd prime power. Then there exist weighing matrices of 2N-type*:

(i) $\mathbf{W}(1 + q, q)$;

(ii) $\mathbf{W}(2 + 2q, 2q)$;

(iii) *if* $q \equiv 3 \pmod 4$, $\mathbf{W}(2 + 2q, 1 + 2q)$ *and* $\mathbf{W}(4 + 4q, 2 + 4q)$.

Proof: (i) If $q \equiv 1 \pmod 4$, this was shown in the proof of Proposition 7. Otherwise the claim follows from the fact (proven in the Ito series section), that there exists an NG-pair (**a**, **b**) of length $(1 + q)/2$ with **a** quasi-symmetric. Let **A** and **B** be the negacyclic matrices with first rows **a** and **b**. We may assume that $a_0 = 1$, then the matrix (3) is skew-Hadamard of 2N-type. By replacing the diagonal entries with 0s, we obtain a $\mathbf{W}(1 + q, q)$.

(ii) This follows from (i) because we can "multiply by 2".

(iii) Let (**a**, **b**) be an Ito NG-pair of length $(1 + q)/2$. By multiplying by 2, we obtain an NG-pair ($\mathbf{a}'$, $\mathbf{b}'$) of length $1 + q$ with $\mathbf{a}' = (1, \mathbf{a}'')$ quasi-symmetric. Consequently, the pair ((0, $\mathbf{a}''$), $\mathbf{b}'$) is N-complementary. The corresponding 2N-type matrix (3) is a C-matrix of order $2 + 2q$. Multiplying by 2 we obtain also an $\mathbf{W}(4 + 4q, 2 + 4q)$.

This proposition covers all weighing matrices $\mathbf{W}(4n, 4n - 1)$ and $\mathbf{W}(4n, 4n - 2)$ of 2N-type, for $n \le 50$ except for

$$n = 9, 13, 19, 23, 25, 28, 29, 31, 37, 39, 43, 44, 46, 47, 48, 49$$

and

$$n = 11, 17, 18, 26, 29, 33, 35, 38, 39, 43, 46, 47, 50,$$

respectively. We have constructed five of these matrices:

n	**a & b**
11	[0, –, –, +, –, –, –, –, –, +, +, +, –, +, +, –, +, –, +, +, +, –], [0, +, –, –, –, –, +, –, –, +, –, +, +, +, +, –, –, –, +, –, +, +]
13	[0, +, +, –, +, –, +, +, +, +, –, +, +, –, +, +, –, +, +, +, +, –, +, –, +, +], [+, +, +, –, +, –, –, –, +, –, –, –, +, +, +, –, +, +, –, –, +, +, +, +, –, –]
17	[0, –, –, –, +, –, –, +, –, +, –, –, –, +, –, +, +, +, –, +, +, +, +, –, +, +, +, +, +, –, –, –, +, –], [0, –, +, +, +, +, –, +, –, –, –, +, +, +, +, –, –, +, +, –, –, +, –, +, +, –, +, +, +, +, –, +, –, –]
18	[0, +, +, –, –, –, +, –, –, +, –, –, –, –, –, –, +, +, +, –, +, +, –, +, –, +, –, –, –, +, +, +, –, +, +, –], [0, +, +, –, –, +, +, +, +, –, +, –, –, –, +, –, +, +, +, –, +, +, +, +, –, +, +, +, +, –, +, –, –, +, +, –]
26	[0, +, +, +, +, –, –, –, +, –, –, –, +, +, +, +, +, –, +, –, –, +, +, –, +, –, –, –, +, +, +, +, –, +, +, –, +, +, +, +, +, +, –, –, +, +, –, –, +, –, +, –], [0, +, +, +, +, +, –, –, +, +, –, –, +, –, +, –, +, +, +, –, –, –, +, –, +, +, –, +, +, +, +, –, –, +, +, +, +, –, +, –, +, +, –, +, +, +, –, +, +, –, +, –].

Multiplication by Golay pairs may be used to construct other series of weighing matrices of 2N-type.

In Appendix E we list weighing matrices $\mathbf{W}(4n, 4n - 2)$ of 4C-type for odd $n \le 21$. They can be easily converted to 4N-type by replacing each circulant block **X** of order n with the negacyclic block **ZXZ**.

Acknowledgements: The second author wishes to acknowledge generous support by NSERC. This work was made possible by the facilities of the Shared Hierarchical Academic Research Computing Network (SHARCNET) and Compute/Calcul Canada.

Appendices

Appendix A. For even integers $v = 1 + q \le 128$, with $q = p^n$ a power of a prime p, we give the first row **c** of a negacyclic conference matrix **C** of order v belonging to the equivalence class of Paley conference matrices. The algorithm is described in the section on Paley C-matrices, it is based on [12, Corollary 7.2]. We also record the primitive polynomial $f(x)$ of degree $2n$ over GF(p) used in the computation.

v	$f(x)$; p, q and the first row **c**
4	$x^2 + x + 2$; $p = q = 3$ [0, +, –, –]
6	$x^2 + x + 2$; $p = q = 5$ [0, +, +, +, –, +]
8	$x^2 + x + 3$; $p = q = 7$ [0, +, –, –, –, +, –, –]
10	$x^4 + x^3 + 2$; $p = 3$, $q = 9$ [0, +, –, –, –, –, +, –, +, +]
12	$x^2 + x + 7$; $p = q = 11$ [0, +, –, +, –, –, +, +, –, –, –, –]
14	$x^2 + x + 2$; $p = q = 13$ [0, +, +, +, +, +, –, –, +, +, –, +, –, +]
18	$x^2 + x + 3$; $p = q = 17$ [0, +, +, +, –, +, +, +, +, –, –, +, –, +, +, +, –, +]
20	$x^2 + x + 2$; $p = q = 19$ [0, +, –, –, –, –, –, +, –, –, +, +, –, –, –, +, –, +, –, –]

24 $x^2 + x + 7;\ p = q = 23$
[0, +, –, –, +, +, +, +, +, +, –, +, +, –, –, –, +, –, +, –, +, +, –, –]

26 $x^4 + x^3 + x + 3;\ p = 5,\ q = 25$
[0, +, –, –, –, +, +, +, –, –, –, –, –, –, +, –, +, –, +, +, –, +, +, –, +, +]

28 $x^6 + x^5 + 2;\ p = 3,\ q = 27$
[0, +, +, –, –, +, –, –, +, +, +, +, +, +, +, –, +, –, +, –, +, +, –, –, –, +, +, –]

30 $x^2 + x + 3;\ p = q = 29$
[0, +, +, –, +, +, +, +, +, +, –, –, –, –, +, +, –, –, +, –, +, +, –, +, –, +, –, –, –, +]

32 $x^2 + x + 12;\ p = q = 31$
[0, +, –, +, –, +, +, +, +, –, –, –, +, +, –, –, –, +, –, –, +, +, –, +, +, –, +, –, –, –, –, –]

38 $x^2 + x + 5;\ p = q = 37$
[0, +, +, +, +, +, –, +, –, +, +, –, +, +, +, +, –, –, +, +, –, –, +, +, –, +, –, –, –, +, +, +, +, +, –, +, –, +]

42 $x^2 + x + 12;\ p = q = 41$
[0, +, +, –, +, –, +, +, +, +, –, +, –, –, +, +, +, –, –, –, +, –, –, –, +, –, –, +, –, –, +, +, +, +, –, +, –, –, –, –, –, +]

44 $x^2 + x + 3;\ p = q = 43$
[0, +, –, +, –, +, –, +, +, –, –, +, –, –, +, –, +, +, –, +, +, +, –, –, +, –, –, –, +, +, +, +, –, –, –, +, +, –, –, –, –, –, –, –]

48 $x^2 + x + 13;\ p = q = 47$
[0, +, –, –, +, +, +, –, –, +, +, +, –, +, –, +, –, +, +, +, +, –, +, –, –, +, +, +, +, –, +, –, –, –, –, –, –, –, +, –, –, +, +, –, +, +, –, –]

50 $x^4 + x^3 + x^2 + 3;\ p = 7,\ q = 49$
[0, +, –, –, –, +, +, –, +, –, +, –, –, –, +, –, +, –, –, +, +, +, –, –, –, –, +, –, +, +, –, +, +, –, –, –, –, –, +, –, –, –, –, –, –, +, +, –, +, +]

54 $x^2 + x + 5;\ p = q = 53$
[0, +, +, +, +, +, –, +, –, –, –, +, –, +, +, –, –, +, –, +, –, +, +, –, +, +, –, –, +, +, –, –, –, +, +, +, +, +, +, –, –, +, +, +, +, –, +, +, +, +, –, +, –, +]

60 $x^2 + x + 2;\ p = q = 59$
[0, +, –, –, +, –, –, +, +, –, –, –, –, –, –, +, +, +, –, +, –, +, –, –, –, +, –, +, +, –, +, +, +, –, –, –, –, +, –, –, –, –, –, –, +, –, –, +, –, +, –, +, +, –, –, +, +, +, –, –]

62 $x^2 + x + 2;\ p = q = 61$
[0, +, +, +, +, +, +, –, +, –, –, –, +, +, –, –, –, +, –, –, –, –, +, +, +, –, –, –, +, –, +, +, –, –, –, –, +, –, –, +, –, –, +, –, +, +, +, –, +, +, –, –, +, –, –, –, –, +, –, +, –, +]

68 $x^2 + x + 12;\ p = q = 67$
[0, +, –, +, +, –, +, +, +, +, –, +, +, +, –, +, +, –, –, –, –, –, +, +, –, –, –, –, –, +, –, +, +, –, +, +, +, –, –, –, –, +, –, +, –, –, +, +, –, +, –, +, +, –, –, –, +, –, –, –, +, –, +, +, +, –, –, –]

72 $x^2 + x + 11;\ p = q = 71$
[0, +, –, –, –, +, –, –, –, –, –, +, +, +, +, –, –, –, +, +, –, –, +, –, +, –, +, +, +, +, –, +, +, –, +, +, +, –, +, +, +, –, –, –, +, –, +, +, +, +, +, +, –, –, +, +, –, +, +, –, +, –, –, +, –, +, –, –, –, +, –, –]

74 $x^2 + x + 11;\ p = q = 73$
[0, +, +, –, –, +, –, +, +, +, –, +, –, +, –, +, –, –, +, –, –, –, –, +, –, +, +, +, –, –, +, +, +, –, –, –, –, +, +, –, +, –, –, +, –, –, +, +, –, +, +, +, +, –, +, –, –, –, +, +, +, +, +, +, +, +, –, +, +, +, +, –, –, +]

80 $x^2 + x + 3;\ p = q = 79$
[0, +, –, –, +, +, –, +, –, +, –, +, –, –, +, –, –, –, +, –, –, –, –, +, –, +, +, –, –, –, –, +, –, +, –, –, +, +, +, –, –, +, +, –, +, +, –, –, –, –, –, +, –, +, +, –, –, –, –, +, –, +, +, +, –, +, +, +, –, –, –, –, –, –, –, –, +, +, –, –]

82 $x^8 + x^5 + 2;\ p = 3,\ q = 81$
[0, +, +, –, –, +, –, +, +, +, –, +, +, –, +, –, +, –, +, +, +, –, +, +, –, –, –, –, +, +, +, +, +, –, +, +, –, +, +, +, +, –, –, +, –, +, +, +, –, –, –, +, –, +, –, –, +, –, +, +, –, –, –, +, –, –, –, –, –, –, –, +, +, +, –, +, +, +, +, –, –, +]

84 $x^2 + x + 2;\ p = q = 83$
[0, +, –, –, +, –, +, +, +, –, +, +, +, –, –, +, –, –, +, +, –, +, +, –, +, –, +, –, +, –, –, +, +, –, +, –, –, –, –, –, +, –, +, +, +, +, –, +, –, +, +, +, +, –, –, +, +, +, +, +, +, +, +, –, –, –, +, +, –, –, –, +, +, –, +, +, +, –, +, +, +, +, –, –]

90 $x^2 + x + 6;\ p = q = 89$
[0, +, +, +, +, –, +, –, +, +, +, –, –, –, +, –, –, +, –, +, +, +, –, +, +, +, –, –, +, +, –, +, –, –, –, +, +, –, +, –, +, +, –, +, –, +, +, +, +, +, –, –, –, –, –, +, +, –, +, +, +, +, –, –, +, +, –, +, +, +, –, +, +, +, +, –, –, –, +, –, –, +, –, –, –, –, –, +, –, +]

98 $x^2 + x + 5;\ p = q = 97$
[0, +, +, +, +, +, –, +, +, –, +, +, –, +, –, –, +, +, –, –, –, +, +, –, +, –, +, –, –, +, –, +, +, +, –, +, –, –, –, –, –, +, +, +, –, +, +, +, –, +, +, +, –, +, +, +, –, +, +, –, +, –, +, +, +, +, –, +, +, +, +, –, –, –, –, –, –, +, +, –, +, +, –, –, +, +, +, +, –, –, –, +, +, +, –, +, –, +]

102 $x^2 + x + 3$; $p = q = 101$
[0, +, +, –, +, +, +, +, –, –, +, –, –, –, –, –, +, +, +, +, +, +, +, +, –, +, +, –, +, +, –, +, –, –, –, +, +, +, –, –, –,
–, –, +, –, +, +, +, –, –, +, +, –, –, +, +, –, +, +, +, +, –, +, –, +, +, –, +, +, –, +, +, +, +, –, –, –, +, +, +, –, +,
–, +, –, +, –, –, +, –, +, –, –, –, +, +, –, +, –, –, –, +]
104 $x^2 + x + 5$; $p = q = 103$
[0, +, –, –, +, –, –, +, –, +, –, +, –, –, –, –, +, –, –, –, +, –, +, +, +, –, +, –, –, –, –, –, –, +, +, –, +, +, –, –, +,
+, +, –, +, –, –, +, +, +, +, –, –, +, +, –, +, –, –, +, +, +, +, –, +, +, –, –, +, +, +, –, –, +, –, +, –, +, +, +, +, –,
+, +, +, +, –, +, +, +, –, +, –, –, –, –, –, –, –, +, +, +, –, –]
108 $x^2 + x + 5$; $p = q = 107$
[0, +, –, –, +, +, –, +, –, +, –, –, –, –, –, +, +, +, +, +, –, –, –, –, +, –, +, –, –, –, +, –, –, –, –, +, –, +, –, –, +,
+, –, –, +, –, –, +, +, +, –, –, –, +, –, –, –, +, –, –, +, –, –, +, +, +, –, –, +, +, –, –, –, –, –, +, –, +, +, +, –, +, +,
+, +, +, –, +, –, –, +, –, +, –, –, +, –, +, –, –, –, –, –, –, +, +, –, –]
110 $x^2 + x + 6$; $p = q = 109$
[0, +, +, +, –, –, –, +, –, +, +, +, –, +, –, +, –, +, +, +, –, +, +, –, +, –, –, +, +, –, +, +, –, –, –, +, –, +, –, –, +,
+, –, +, +, +, +, –, –, –, –, –, –, +, +, +, –, +, +, –, +, –, +, –, –, +, –, +, +, +, –, –, +, +, +, +, +, –, +, +, –, –,
–, +, +, –, –, –, –, +, +, +, –, +, +, +, +, +, +, +, –, +, +, +, +, –, +, +, –, +]
114 $x^2 + x + 10$; $p = q = 113$
[0, +, +, +, –, –, –, –, +, –, –, +, +, –, +, +, –, +, –, –, –, +, –, +, –, –, –, –, –, +, +, +, +, +, –, +, +, –, +, –, +,
–, –, –, –, –, +, +, –, –, +, –, –, –, +, –, –, +, +, –, –, –, +, –, –, –, +, +, –, –, +, –, +, –, –, –, –, –, –, +, +, +, –,
+, –, +, +, –, +, –, +, +, +, +, +, –, +, +, +, +, –, –, –, +, +, –, –, –, +, –, +, +, –, +]
122 $x^4 + x^3 + 8$; $p = 11$, $q = 121$
[0, +, –, –, –, –, –, –, –, +, +, –, +, –, –, –, +, –, –, +, +, –, +, –, –, +, +, –, +, –, –, –, –, +, –, +, –, –, –, –, +,
–, –, –, +, +, +, +, –, +, –, –, –, +, +, +, –, –, +, –, –, –, +, –, –, –, +, +, –, +, +, –, +, +, +, +, –, +, –, –, +, –,
–, –, +, –, +, +, +, +, +, –, +, –, –, –, –, +, +, –, –, –, –, +, +, –, –, –, +, –, –, –, –, +, +, –, +, –, +, –, +, +]
128 $x^2 + x + 3$; $p = q = 127$
[0, +, –, –, –, +, –, +, +, –, –, –, +, +, –, –, –, –, +, –, –, –, –, +, –, +, +, +, +, +, –, +, +, –, +, +, –, –, –, +, +,
+, +, –, +, +, +, –, +, +, +, +, +, +, –, –, +, –, +, –, +, +, –, –, –, +, –, –, +, +, +, +, +, +, –, –, +, –, +, –, +, +,
+, –, +, +, +, –, +, –, –, +, –, –, +, +, +, –, –, –, +, –, +, –, –, –, –, +, –, +, +, +, –, +, –, –, +, +, –, +, +, –, –,
–, –, +, –, –]

Appendix B. For even integers $v = 1 + q \leq 128$, with $q \equiv 1 \pmod 4$ a prime power, we give a 2C-type conference matrix of order v with symmetric blocks **A** and **B** which belongs to the equivalence class of Paley conference matrices. The algorithm is described in the section on the first Paley series. Since the blocks **A** and **B** are symmetric circulants of odd order $v/2$, we record only the first $(v + 2)/4$ elements of their first rows **a** and **b**.

We recall that $\mathbf{A} + \mathbf{I}$, $\mathbf{A} - \mathbf{I}$, **B**, **B** are four Williamson matrices of order $v/2$ belonging to the Turyn series.

v	first rows of **a** and **b** (truncated)
6	[0, –], [–, +]
10	[0, +, –], [–, +, +]
14	[0, –, +, +], [+, +, –, +]
18	[0, –, –, –, +], [–, –, +, –, +]
26	[0, +, –, –, –, +, –], [–, +, –, –, +, +, +]
30	[0, –, +, –, +, +, –, –], [–, –, +, +, –, +, +, +]
38	[0, –, +, +, –, –, +, –, –, –], [–, –, –, +, +, +, –, +, –, +]
42	[0, –, +, –, +, +, –, –, +, +, +], [–, +, –, –, –, –, +, –, –, +, +]
50	[0, +, –, –, +, –, –, –, +, +, +, +, –], [–, +, +, –, –, +, –, +, –, +, +, +, +]
54	[0, –, +, +, –, +, –, –, –, +, –, –, +, +], [+, +, +, +, –, +, +, +, –, –, –, +, –, +]
62	[0, –, +, –, +, +, +, +, –, +, –, –, +, +, +, –], [–, –, +, –, –, –, +, +, +, +, +, –, +, +, –, +]
74	[0, –, –, +, +, +, –, +, –, –, –, +, –, –, –, –, +, +, –], [+, +, –, –, –, –, +, –, –, +, –, –, +, –, +, –, +, +, +]
82	[0, –, –, +, +, +, +, –, +, –, +, –, –, +, +, –, +, –, –, –, +], [–, –, +, –, –, –, +, +, –, –, –, –, –, +, –, –, +, –, +, +, +]
90	[0, –, +, –, +, –, –, –, –, +, +, +, +, +, +, +, –, +, +, –, +, +, –], [+, –, +, +, –, –, –, –, +, +, +, –, +, –, +, +, –, +, +, +, –, –, +]
98	[0, –, +, +, +, –, –, +, +, +, –, –, +, –, –, +, +, +, –, +, –, –, –, –, –], [+, –, +, –, +, +, –, –, +, –, +, +, –, +, +, +, +, +, +, –, –, –, +, –, +]
102	[0, –, +, –, –, –, –, +, +, –, +, –, –, –, +, +, –, +, +, +, –, +, –, –, –, –], [–, –, –, +, –, –, +, +, –, –, –, +, +, +, –, +, –, +, +, –, +, –, –, +, +, +]

110	[0, –, –, +, –, –, –, +, –, –, –, –, +, +, +, –, –, +, –, +, +, +, +, –, –, +, –, –], [–, +, +, –, +, +, –, +, +, +, –, –, –, –, –, –, +, +, –, +, –, +, –, +, –, –, –, +]
114	[0, –, –, +, +, +, +, –, –, +, –, +, –, +, –, –, +, +, +, –, +, +, –, –, –, –, –, –, –], [+, +, –, +, –, –, –, +, –, +, –, –, +, –, +, +, –, –, +, +, +, –, –, –, –, +, –, –, +]
122	[0, +, –, +, –, –, +, +, +, +, +, –, –, –, +, +, –, +, –, +, +, +, +, –, –, +, –, –, –, –, –], [–, +, –, –, +, +, +, –, +, +, –, +, –, –, +, +, –, +, +, +, –, –, –, +, –, +, +, +, –, +, +]

Appendix C. For integers $q = 4t - 1$, with $q = p^n \equiv 3 \pmod 4$ a power of a prime p, we give the NG-pairs **(a, b)** of length $v = 2t \le 64$ belonging to the second Paley series. The procedure used to generate this list is described in the section on the second Paley series.

The sequence **a** is quasi-symmetric and **b** is skew-symmetric. We record only the first $t + 1$ terms of **a** and the first t terms of **b**. If **A** and **B** are the negacyclic blocks with first rows **a** and **b**, then the matrix (3) is 2N-type skew-Hadamard.

v	**a** & **b** (truncated)
2	[+, –], [+]
4	[+, –, –], [+, –]
6	[+, –, –, +], [+, +, –]
10	[+, –, –, –, –, +], [+, –, –, +, –]
12	[+, –, +, +, +, –, +], [+, –, +, +, +, +]
14	[+, +, –, –, +, +, +, +], [+, –, +, –, +, +, +]
16	[+, –, –, +, +, –, +, –, –], [+, +, +, +, –, –, +, –]
22	[+, –, –, –, +, –, –, +, +, –, +, –], [+, +, +, +, –, +, –, –, +, +, +]
24	[+, –, +, +, –, +, –, –, –, +, +, +, –], [+, –, +, –, +, +, +, +, +, +, –, –]
30	[+, –, +, –, +, –, –, –, +, –, –, –, –, –, +, +], [+, –, –, +, –, –, –, +, +, +, +, –, +, +, –]
34	[+, –, +, +, +, –, +, –, +, –, –, +, –, –, –, –, +, +], [+, +, –, +, +, +, +, +, –, –, –, +, –, –, +, +, –]
36	[+, –, –, –, –, –, +, +, –, +, –, +, +, +, +, –, +, +, +], [+, –, +, –, –, +, +, –, –, +, –, –, –, +, +, +, –, +]
40	[+, –, +, –, –, –, –, +, –, +, –, –, –, +, –, –, –, –, +, +, –], [+, –, +, +, +, +, –, –, –, –, –, +, +, –, –, +, +, –, +, –]
42	[+, –, +, +, +, +, +, –, –, +, –, +, +, +, +, –, +, +, –, –, +, +], [+, –, –, +, –, +, –, +, –, +, +, –, –, –, –, +, –, –, –, –, –]
52	[+, –, +, –, –, –, –, –, +, –, +, +, +, +, –, –, –, +, +, –, +, +, +, –, +, +, –], [+, –, –, +, +, +, –, –, –, –, –, +, –, –, –, –, +, –, +, –, +, –, –, +, +, –]
54	[+, –, +, –, –, –, –, –, +, +, –, –, +, +, –, +, –, –, –, –, +, –, +, –, +, –, –, –], [+, –, +, +, +, –, –, +, +, +, –, –, –, –, –, –, –, +, +, –, +, –, –, +, +, –, +]
64	[+, –, –, –, +, –, +, –, –, +, –, –, –, +, +, –, +, +, –, –, +, +, +, +, +, +, +, –, +, +, +, –, –], [+, –, +, +, –, –, +, –, –, –, –, +, +, +, +, +, –, +, –, +, +, –, +, –, +, +, +, –, –, –, +,]

Appendix D. For integers $q = 4t - 1$, with $q = p^n \equiv 3 \pmod 4$ a power of a prime p, we give the NG-pairs **(a, b)** of length $v = 2t \le 154$ belonging to the Ito series. The procedure used to generate this list is described in the Ito series section. In the list below, for each length v, we record the primitive polynomial $f(x)$ of degree $2n$ over GF(p) used in the computation, and the NG-pair **(a, b)**.

In all cases we have **a** = (+, **a**′) where the subsequence **a**′ is symmetric while the whole sequence **b** is skew-symmetric. We record only the first $t + 1$ terms of **a** and the first t terms of **b**. If **A** and **B** are the negacyclic blocks with first rows **a** and **b**, then the matrix (3) is skew-Hadamard of 2N-type.

Moreover, by multiplying the NG-pair **(a, b)** by 2, we obtain in the same way a 2N-type skew-Hadamard matrix of order $1 + q$.

v	**a** & **b** (truncated)
2	$x^2 - x - 1$; $p = q = 3$ [+, +], [+]
4	$x^2 - x + 3$; $p = q = 7$ [+, –, +], [+, +]
6	$x^2 + x + 7$; $p = q = 11$ [+, –, +, +], [–, –, +]
10	$x^2 - x + 2$; $p = q = 19$ [+, –, +, –, +, +], [+, +, +, –, –]

12 $x^2 - x + 7;\ p = q = 23$
[+, +, +, –, +, +, +], [+, –, +, –, –, –]
14 $x^6 - x^5 + 2;\ p = 3;\ q = 27$
[+, +, +, –, –, +, –, +], [–, +, –, –, –, –, –]
16 $x^2 - x + 12;\ p = q = 31$
[+, –, +, +, –, –, –, –, +], [+, +, +, –, –, +, –, +]
22 $x^2 + x + 3;\ p = q = 43$
[+, +, –, +, +, +, –, –, +, +, +, +], [–, +, –, –, +, +, +, +, –, +, –]
24 $x^2 + x + 13;\ p = q = 47$
[+, –, –, +, +, +, +, –, +, +, –, +, +], [–, +, +, –, +, –, +, –, –, –, –, –]
30 $x^2 + x + 2;\ p = q = 59$
[+, –, –, –, –, –, +, –, –, –, +, –, +, –, –, +], [–, –, +, +, +, –, +, –, –, +, –, –, –, +, +]
34 $x^2 + x + 12;\ p = q = 67$
[+, –, –, +, –, –, –, –, –, –, +, +, +, –, +, –, –, +], [–, –, +, +, –, –, –, +, –, –, +, –, +, –, –, –, +]
36 $x^2 + x + 11;\ p = q = 71$
[+, +, –, +, –, +, +, –, –, –, –, –, +, –, +, +, +, –, +],
[–, –, –, +, –, –, +, –, –, –, +, +, –, –, +, +, +, +]
40 $x^2 + x + 3;\ p = q = 79$
[+, –, –, –, +, –, +, +, +, +, +, –, +, +, +, –, +, –, –, +, +],
[–, –, –, –, +, +, –, –, +, +, –, +, –, +, +, –, +, –, –, –]
42 $x^2 + x + 2;\ p = q = 83$
[+, –, –, +, –, +, –, –, +, +, +, +, –, +, –, –, –, +, +, –, –, +],
[–, +, –, +, –, –, – , +, –, +, +, –, –, –, –, –, –, –, –, +, +]
52 $x^2 + x + 5;\ p = q = 103$
[+, –, –, –, +, –, +, –, –, –, –, +, –, +, +, –, +, +, –, –, –, +, –, –, –, +, +],
[–, –, +, +, –, –, –, –, –, –, –, +, –, +, +, +, –, +, –, +, +, –, +, +, –, –]
54 $x^2 + x + 5;\ p = q = 107$
[+, +, +, +, –, +, –, +, +, –, –, +, +, –, –, –, –, +, –, +, +, +, +, +, +, +, –, +],
[–, –, –, +, +, –, –, –, –, +, +, –, +, –, +, –, +, +, –, +, +, –, –, +, –, –, –]
64 $x^2 - x + 3;\ p = q = 127$
[+, –, +, –, –, –, –, –, +, +, +, –, +, +, –, –, –, +, +, –, –, +, –, +, –, +, –, –, –, +, –, –, +],
[+, +, +, –, +, +, –, +, +, +, +, +, –, –, –, –, –, +, –, +, –, –, +, –, +, +, +, –, –, +, +, +]
66 $x^2 - x + 14;\ p = q = 131$
[+, –, –, –, –, +, +, –, +, –, +, –, –, +, +, –, –, –, +, +, –, +, –, +, +, +, +, +, –, +, +, –, –, +],
[+, +, +, +, +, +, +, –, –, –, +, –, +, +, –, +, –, –, –, +, +, –, +, –, +, +, +, –, –, –, +, –, –]
70 $x^2 + x + 2;\ p = q = 139$
[+, +, –, +, –, –, –, –, +, –, +, –, +, +, +, –, –, –, +, +, +, –, –, +, –, –, +, +, +, +, +, +, +, –, +, +],
[–, –, –, –, +, +, +, +, –, +, +, –, +, +, –, +, –, +, +, +, –, +, –, –, –, +, +, –, +, –, –, +, +, –, –]
76 $x^2 + x + 12;\ p = q = 151$
[+, –, +, +, +, –, –, +, –, –, +, –, +, +, –, +, –, –, –, +, –, +, +, +, +, +, +, –, –, +, +, –, –, –, –, –, +, –, +],
[–, +, +, +, –, –, –, +, –, +, +, –, –, –, –, –, +, –, –, –, –, +, –, +, –, +, +, –, –, –, –, +, –, –, –, +, –, –]
82 $x^2 + x + 11;\ p = q = 163$
[+, +, +, –, +, –, +, –, –, –, +, +, –, –, –, –, +, +, –, +, –, –, –, +, +, +, +, +, +, +, +, +, –, +, –, +, +, +, +, –, –, +],
[–, +, –, –, +, –, –, +, –, +, –, +, –, +, +, +, +, –, –, –, –, +, –, –, +, +, +, +, –, +, +, +, –, –, +, –, –, +, +, –, –]
106 $x^2 + x + 3;\ p = q = 211$
[+, –, –, –, +, +, –, +, –, –, –, –, –, +, –, –, –, +, +, +, +, –, –, +, +, –, –, –, –, –, –, +, –, –, +, +, –, –, –, –, +,
+, –, +, +, –, +, –, +, +, –, +, –, +], [–, +, +, –, –, –, +, –, +, +, +, –, –, +, –, –, +, –, –, +, –, +, –, –, –, –, –, –,
–, +, +, +, –, –, +, –, –, –, +, –, +, –, –, +, +, +, +, +, +, –, +, –, +]
142 $x^2 + x + 3;\ p = q = 283$
[+, +, –, +, –, –, –, –, +, –, –, –, –, –, +, +, –, –, –, –, +, +, +, –, +, +, +, –, +, –, +, –, +, –, –, +, –, +, –, –, –,
–, +, +, –, +, +, –, +, +, –, +, –, –, –, +, –, –, +, +, +, +, –, +, +, –, –, +, +, –, +, +], [–, +, +, –, –, –, +, +, +, +,
–, +, +, +, +, +, –, +, –, –, +, +, +, +, –, –, +, –, +, +, +, +, +, +, –, –, +, +, –, +, +, +, –, –, –, –, –, –, +, +, –,
+, –, +, +, –, –, –, +, –, –, –, –, +, –, +, +, +, –, +, –]
154 $x^2 + x + 5;\ p = q = 307$
[+, +, +, –, –, +, –, –, +, +, +, –, +, –, +, +, –, +, –, –, +, +, –, –, +, +, –, +, –, –, –, –, –, –, +, +, –, –, –, –, –,
–, –, –, –, –, +, –, –, +, –, +, +, +, +, –, +, +, –, –, –, –, +, +, –, –, –, –, +, +, +, +, –, +, –, +, –, +], [–, +, –, –,
+, +, +, +, –, –, –, –, +, –, +, +, +, –, +, –, –, +, –, –, +, +, –, –, +, –, +, –, +, –, –, –, –, +, –, +, –, –, –, +, –, –,
–, +, +, +, –, +, +, +, +, –, +, +, –, –, –, –, –, –, +, +, –, +, –, +, –, –, +, +, –, –, –]

Appendix E. We list here the weighing matrices **W**($4n$, $4n$–2) of 4C-type for odd $n \leq 21$.

$4n$	**a, b, c, d**
4	[0], [+], [0], [+]
12	[0, +, +], [+, –, –], [0, –, –], [+, –, –]
20	[0, +, +, +, +], [+, +, –, –, +], [0, +, –, –, +], [+, –, +, +, –]
28	[0, –, +, +, +, +, –], [+, +, –, +, +, –, +], [0, –, +, –, –, +, –], [+, +, +, –, –, +, +]
36	[0, +, –, +, –, –, +, –, +], [+, +, –, –, –, –, –, –, +], [0, –, +, +, –, –, +, +, –], [+, +, +, –, +, +, –, +, +]
44	[0, +, –, –, +, –, –, +, –, –, +], [+, +, –, –, –, –, –, –, –, –, +],
	[0, +, –, +, –, +, +, –, +, –, +], [+, +, +, –, –, +, +, –, –, +, +]
52	[0, +, +, –, +, –, –, –, –, +, –, +, +], [+, –, +, –, –, –, +, +, –, –, –, +, –],
	[0, –, –, +, +, +, –, –, +, +, +, –, –], [+, –, –, +, –, –, –, –, –, –, +, –, –]
60	[0, –, –, +, +, +, –, +, +, –, +, +, +, –, –], [+, +, –, –, –, –, +, –, –, +, –, –, –, –, +],
	[0, +, –, +, –, +, +, –, –, +, +, –, +, –, +], [+, –, +, +, –, –, –, –, –, –, –, –, +, +, –]
68	[0, –, +, +, +, –, +, –, –, –, –, +, –, +, +, +, –], [–, +, –, –, +, –, +, +, –, –, +, +, –, +, –, –, +],
	[0, +, +, +, +, +, –, –, +, +, –, –, +, +, +, +, +], [+, +, +, –, +, –, –, –, +, +, –, –, –, +, –, +, +]
76	[0, +, +, +, +, –, +, –, –, +, +, –, –, +, –, +, +, +, +], [–, +, +, +, –, –, –, +, –, +, +, –, +, –, –, –, +, +, +],
	[0, +, +, +, –, +, –, –, +, +, +, +, –, –, +, –, +, +, +], [–, +, –, –, –, +, +, –, +, +, +, +, –, +, +, –, –, –, +]
84	[0, –, –, +, +, –, –, +, –, +, –, –, +, –, +, –, –, +, +, –, –], [–, –, +, +, +, –, +, –, –, –, –, –, –, –, –, +, –, +, +, +, –],
	[0, +, –, +, –, –, +, +, –, –, –, –, –, –, +, +, –, –, +, –, +], [+, –, +, +, +, +, –, +, +, –, –, –, –, +, +, –, +, +, +, +, –]

References

1. **M. J. E. Golay.** Complementary Series. *IRE Trans. Inform. Theory*, 1961, vol. IT-7, pp. 82–87.
2. **J. Seberry and M. Yamada.** Hadamard Matrices, Sequences, and Block Designs. In *Contemporary Design Theory: A Collection of Surveys*. J. H. Dinitz and D. R. Stinson (eds). John Wiley and Sons, 1992, pp. 431–560.
3. **W. de Launey and D. Flannery.** Algebraic Design Theory. *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, R. I., 2011, vol. 175. 298 p.
4. **D. Ž. Đoković.** Note on Periodic Complementary Sets of Binary Sequences. *Designs, Codes and Cryptography*, 1998, no. 13, pp. 251–256.
5. **D. Ž. Đoković, I. S. Kotsireas.** Periodic Golay Pairs of Length 72. In *Algebraic Design Theory and Hadamard Matrices*, ADTHM, Lethbrodge, Alberta, Canada, July 2014. C. J. Colbourn (ed). Springer, 2015, pp. 83–92.
6. **N. Ito.** On Hadamard Groups IV. *Journal of Algebra*, 2000, no. 234, pp. 651–663.
7. **N. Ito.** On Hadamard Groups III. *Kyushu J. Math.*, 1997, no. 51, pp. 369–379.
8. **B. Schmidt.** Williamson Matrices and a Conjecture of Ito's. *Designs, Codes and Cryptography*, 1999, no. 17, pp. 61–68.
9. **Balonin N. A., Đoković D. Ž.** Symmetry of Two Circulant Hadamard Matrices and Periodic Golay Pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3(76), pp. 2–16. doi:10.15217/issn1684-8853.2015.3.2 (In Russian).
10. **H. J. Ryser.** Combinatorial Mathematics. *The Carus Mathematical Monographs*. Published by The Mathematical Association of America, New York, John Wiley and Sons, 1963, no. 14, p. 162.
11. **R. J. Turyn.** Hadamard Matrices, Baumert-Hall Units, four Symbol Sequences, Pulse Compression and Surface Wave Encodings. *J. Combin. Theory*, 1974, no. 16, pp. 313–333.
12. **P. Delsarte, J. M. Goethals, and J. J. Seidel.** Orthogonal Matrices with Zero Diagonal. II. *Can. J. Math.*, 1971, vol. XXIII, no. 5, pp. 816–832.
13. **K. T. Arasu, Y. Q. Chen, and A. Pott.** Hadamard and Conference Matrices. *Journal of Algebraic Combinatorics*, 2001, no. 14, pp. 103–117.
14. **B. Schmidt and M. M. Tan.** Construction of Relative Difference Sets and Hadamard Groups. *Designs, Codes and Cryptography*, 2014, no. 73, pp. 105–119.
15. **D. Ž. Đoković.** Equivalence Classes and Representatives of Golay Sequences. *Discrete Math.*, 1998, no. 189, pp. 79–93.
16. **R. E. A. C. Paley.** On Orthogonal Matrices. *J. Math. and Phys.*, 1933, no. 12, pp. 311–320.
17. **J. M. Goethals and J. J. Seidel.** Orthogonal Matrices with Zero Diagonal. *Can. J. Math.*, 1967, no. 19, pp. 1001–1010.
18. **W. H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie.** Williamson Matrices up to Order 59. *Designs, Codes and Cryptography*, 2008, no. 46, pp. 343–352.
19. **R. G. Stanton and R. C. Mullin.** On the Nonexistence of a Class of Circulant Balanced Weighing Matrices. *SIAM J. Appl. Math.*, 1976, no. 30, pp. 98–102.

УДК 519.614
doi:10.15217/issn1684-8853.2015.5.2

Негапериодические пары Голея и матрицы Адамара

Н. А. Балонин[а], доктор техн. наук, профессор, korbendfs@mail.ru
Д. Ж. Джокович[б], доктор наук, профессор, djokovic@uwaterloo.ca
[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения, 67, Б. Морская ул., 190000, Санкт-Петербург, РФ
[б]Университет Ватерлоо, Ватерлоо, Онтарио, Канада

Цель: показать, что по аналогии с ординарными и периодическими парам Голея существуют и негапериодические пары Голея (впервые они появились под другим именем в трудах Н. Ито). **Методы:** исследуется конструкция адамаровых (и взвешенных) матриц, состоящая из двух негациклических блоков (2N-типа). Матрицы Адамара 2N-типа эквивалентны негапериодическим парам Голея. **Результаты:** показано, что, во-первых, если матрица Адамара имеет форму матрицы Теплица, то она должна быть либо циклической, либо негациклической. Во-вторых, прозведение Тюрина пар Голея расширяемо до более общего произведения: с его помощью можно периодические пары Голея длины g умножать на негапериодические пары Голея длины v, получая негапериодические пары Голея длины gv. В-третьих, гипотеза Ито о матрицах Адамара эквивалентна гипотезе о существовании негапериодических пар Голея для всех возможных четных значений их длины. **Практическая значимость:** матрицы Адамара имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.

Ключевые слова — матрицы Адамара, циклические матрицы, негациклические матрицы, периодические пары Голея, негапериодические пары Голея.