UDC 004.438
doi:10.31799/1684-8853-2020-4-2-10

Articles

Conference matrices from Legendre C-pairs

N. A. Balonin[a], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
D. Ž. Đoković[b], *Dr. Sc., Distinguished Professor Emeritus, orcid.org/0000-0002-0176-2395, 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*

Introduction: *There are just a few known methods for the construction of symmetric C-matrices, due to the lack of a universal structure for them. This obstruction is fundamental, in addition, the structure of C-matrices with a double border is incompletely described in literature, which makes its study especially relevant.* ***Purpose:*** *To describe the two-border two-circulant construction in detail we introduce the concept of the Legendre C-pairs.* ***Results:*** *The paper deals with C-matrices of order $n = 2v + 2$ with two borders and extends the so called generalized Legendre pairs, v odd, to a wider class of Legendre C-pairs with even and odd v, defined on a finite abelian group G of order v. Such a pair consists of two functions a, b: $G \to Z$, whose values are +1 or −1 except that $a(e) = 0$, where e is the identity element of G and Z is the ring of integers. To characterize the Legendre C-pairs we use the subsets $X = \{x \in G: a(x) = -1\}$ and $Y = \{x \in G: b(x) = -1\}$ of G. We show that $a(x^{-1}) = (-1)^v a(x)$ for all x. For odd v we show that X and Y form a difference family, which is not true for even v. These difference families are precisely the so called Szekeres difference sets, used originally for the construction of skew-Hadamard matrices. We introduce the subclass of the special Legendre C-pairs and prove that they exist whenever $2v + 1$ is a prime power. In the last two sections of the paper we list examples of special cyclic Legendre C-pairs for lengths $v < 70$.* ***Practical relevance:*** *C-matrices are used extensively in the problems of error-free coding, compression and masking of video information. Programs for search of conference matrices and a library of constructed matrices are used in the mathematical network "mathscinet.ru" together with executable on-line algorithms.*

Keywords *— conference matrices, skew-Hadamard matrices, periodic autocorrelation functions, Szekeres difference families, generalized Legendre pairs, constructions, telephony.*

For citation: Balonin N. A., Đoković D. Ž. Conference matrices from Legendre C-pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 4, pp. 2–10. doi:10.31799/1684-8853-2020-4-2-10

Introduction

We introduce the notion of Legendre C-pairs on a finite abelian group G of order v and use it to construct many C-matrices of order $n = 2v + 2$ with two borders and a core made up from two multi-circulants. Such a pair consists of two functions a, b: $G \to Z$, whose values are +1 or −1 except that $a(e) = 0$, where e is the identity element of G. (By Z we denote the ring of integers.) Moreover the sum of the periodic autocorrelation functions (PAF) of a and b must be −2, except at shift 0. These pairs are similar to the so called generalized Legendre (GL) pairs. While for the GL-pairs v must be odd, there is no such restriction for the Legendre C-pairs.

In Proposition 1 we show that $a(x^{-1}) = (-1)^v a(x)$ for all x and determine the cardinalities of the sets $X = \{x \in G: a(x) = -1\}$ and $Y = \{x \in G: b(x) = -1\}$. We introduce special Legendre C-pairs and in Proposition 2 and Corollary 2 we show that they exist whenever $2v + 1$ is a prime power.

In the last two sections of the paper we list examples of special cyclic Legendre C-pairs for lengths $v < 70$. In Proposition 3 we characterize the Legendre C-pairs in terms of the subsets X and Y defined above. For odd v we show that X and Y form a difference family, which is not true for even v. These difference families are precisely the so called Szekeres difference sets (see Corollary 3). Originally they were used for the construction of skew-Hadamard matrices, see [1–4]. A wider class of two-block difference families with parameters $(v; (v - 1)/2, (v - 1)/2; (v - 3)/2)$, v odd, has been investigated recently in [5]. In Fig. 3 we summarize diagramatically the main facts about such families. The existence question remains open in many cases.

Let us now recall some definitions and facts about Hadamard and conference matrices. A *Hadamard matrix* is a matrix $\mathbf{H}$ of order n with entries +1 or −1 and such that $\mathbf{H}\mathbf{H}^{\mathrm{T}} = n\mathbf{I}$ (T is the transposition operator and $\mathbf{I}$ is the identity matrix of some order, here of order n). If such a matrix exists and $n > 2$ then n must be divisible by 4. A Hadamard matrix $\mathbf{H}$ is a *skew-Hadamard matrix* if $\mathbf{H} + \mathbf{H}^{\mathrm{T}} = 2\mathbf{I}$.

A *conference matrix* (*C-matrix*) is a matrix $\mathbf{C}$ of order n whose diagonal entries are zeros, the other entries are +1 or −1, and $\mathbf{C}\mathbf{C}^{\mathrm{T}} = (n - 1)\mathbf{I}$. If such a matrix exists and $n > 1$ then n must be even. Two C-matrices of the same order are *equivalent* if one can be transformed to the other by permuting the rows and columns so that the diagonal zeros are preserved and by multiplying by −1 some

rows and some columns. Every equivalence class of C-matrices of order n contains a symmetric matrix if $n \equiv 2 \pmod 4$ and a skew-symmetric matrix if $n \equiv 0 \pmod 4$. If $\mathbf{C}$ is a skew-symmetric C-matrix of order n then $\mathbf{H} = \mathbf{C} + \mathbf{I}$ is a skew-Hadamard matrix of order n, and the converse holds.

It is well-known (see e. g. [6]) that if a C-matrix of order $n \equiv 2 \pmod 4$ exists then $n - 1$ must be a sum of two squares. Let us list such integers $n < 200$:

$$2, 6, 10, 14, 18, 26, 30, 38, 42, 46, 50, 54, 62, 66, 74, 82, 86, 90, 98, 102, 110, 114, 118, 122, 126, 138, 146, 150, 154, 158, 170, 174, 182, 186, 194, 198. \quad (1)$$

We say that a symmetric or skew-symmetric C-matrix is *normalized* if all entries of its first row are +1, except the first entry which must be 0. In that case, its *core* is the submatrix obtained by dropping the first row and column.

The basic examples of C-matrices are so called *Paley C-matrices* $\mathbf{C}$ of order $n = q + 1$ where q is a power of an odd prime (see e. g. [7] or [8, Chapter 18]). The matrix $\mathbf{C}$ is normalized and its core $\mathbf{Q}$ is a matrix of order q. The rows and columns of $\mathbf{Q}$ are labeled by the elements of the finite field GF(q) of order q. The entries of $\mathbf{Q}$ are given by the formula $\mathbf{Q}_{x,y} = \chi(x - y)$, where χ is the quadratic character of GF(q). We recall that $\chi(x) = 1$ if $x \neq 0$ is a square in GF(q), $\chi(x) = -1$ if x is not a square, and $\chi(0) = 0$. Moreover, χ satisfies the multiplicative property $\chi(xy) = \chi(x)\chi(y)$ for all x, y in GF(q). Both $\mathbf{C}$ and $\mathbf{Q}$ are symmetric if $q \equiv 1 \pmod 4$ and skew-symmetric otherwise.

There are just a few methods of construction of symmetric C-matrices. They are listed in the recent survey paper [9]. We investigate here only one of these methods, namely the *two-border two-circulant* (2b2c) *construction*. In the next section we describe this construction in detail and introduce the concept of Legendre C-pairs.

Legendre C-pairs

For the sake of simplicity, we consider first the case of the cyclic group $Z_v = \{0, 1, ..., v - 1\}$ under addition modulo v. In that case we treat the functions on Z_v as sequences of length v. Let a and b be two sequences of length v

$$a = (a_0, a_1, ..., a_{v-1}); b = (b_0, b_1, ..., b_{v-1}), \quad (2)$$

where $a_0 = 0$ while all other a_i and all the b_i are equal to +1 or −1. Recall that the value of the PAF of a sequence $x = (x_0, x_1, ..., x_{v-1})$ at shift s is

$$\mathrm{PAF}_x(s) = \sum_{i=0}^{v-1} x_i x_{i+s}.$$

Definition 1 (*cyclic case*). We say that the pair (a, b) given by (2) is a (*cyclic*) *Legendre C-pair* if the sum of the PAFs of the sequences a and b has the constant value −2, except at the shift 0 where the sum attains its peak value $2v - 1$.

The first examples of Legendre C-pairs originate from Number Theory. Indeed let $v = p$ be a prime number $\equiv 3 \pmod 4$. Then the sequence a of Legendre symbols

$$a_i = \left(\frac{i}{p}\right),\ i = 0, 1, ..., p - 1$$

has constant PAF values, $\mathrm{PAF}_a(s) = -1$ for all nonzero s. The same is true for the sequence b which is obtained from a by replacing the first term 0 by +1. Hence (a, b) is a Legendre C-pair of length p. This construction does not work when p is a prime number $\equiv 1 \pmod 4$.

The above definition differs from that of "generalised Legendre pairs" given in [10, p. 76] (see also [6]) which requires that all elements of the sequences a and b be +1 or −1. We shall refer to them simply as "Legendre pairs". For the Legendre pairs, the sum of the PAFs of a and b is required to be the constant function −2 except for the value $2v$ at shift 0. Our definition of Legendre C-pairs is designed for the construction of C-matrices and so the condition that $a_0 = 0$ is mandatory. It is mentioned in [10, p. 80] that the length of Legendre pairs must be odd. On the other hand, there exist Legendre C-pairs of even and odd lengths. Those of even length give symmetric C-matrices while the ones of odd length give skew-symmetric C-matrices (and skew-Hadamard matrices).

Now let p be a prime number $\equiv 1 \pmod 4$. Let a and b be the sequences obtained from the sequence of Legendre symbols by replacing the 0 term by +1 and −1 respectively. Then (a, b) is a Legendre pair of length p which cannot be used to produce a Legendre C-pair of the same length.

Next we show how to use a cyclic Legendre C-pair (a, b) of length v to construct a C-matrix $\mathbf{C}$ of order $n = 2v + 2$. Let $\mathbf{A}$ and $\mathbf{B}$ denote the circulant matrices whose first rows are given by a and b, respectively.

In the case when v is even, the matrix $\mathbf{C}$ is obtained by plugging the blocks $\mathbf{A}$ and $\mathbf{B}$ into the next array; the first two rows and columns of $\mathbf{C}$ form its *border* and its *core* is made up from the circulants $\mathbf{A}$ and $\mathbf{B}$ (and their transposes):

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & \mathbf{e}^{\mathrm{T}} & \mathbf{e}^{\mathrm{T}} \\ 1 & 0 & \mathbf{e}^{\mathrm{T}} & -\mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & -\mathbf{e} & \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}. \quad (3)$$

(By $\mathbf{e}$ we denote a column vector of 1's.)

It is easy to verify (see Problem 18B on p. 174 and the hint on p. 490 in [8]) that if the matrix **C** defined by (3) is a C-matrix then **C** must be symmetric. Consequently, if **C** is a C-matrix then **A** must be symmetric, i. e. $a_i = a_{v-i}$ for $i = 1, \ldots, v-1$. For an example of such C-matrix see Fig. 1, *a*.

In the case when v is odd, we use the modified array

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & \mathbf{e}^{\mathrm{T}} & \mathbf{e}^{\mathrm{T}} \\ -1 & 0 & \mathbf{e}^{\mathrm{T}} & -\mathbf{e}^{\mathrm{T}} \\ -\mathbf{e} & -\mathbf{e} & \mathbf{A} & \mathbf{B} \\ -\mathbf{e} & \mathbf{e} & -\mathbf{B}^{\mathrm{T}} & \mathbf{A}^{\mathrm{T}} \end{pmatrix}. \qquad (4)$$

As in the previous case one can show that if **C** is a C-matrix then the block **A** must be skew-symmetric matrix, i. e. $a_i + a_{v-i} = 0$ for $i = 1, \ldots, v-1$. For an example see Fig. 1, *b*.

We shall now extend the definition of Legendre C-pairs to any abelian group G of order v with identity element e. Denote by * the involution of the integral group ring $Z[G]$ sending any element x to its inverse x^{-1}. For any $z \in Z[G]$ we define its *norm* $N(z)$ to be the product zz^*. For a subset X of G we say that it is *symmetric* if $X^* = X$ and that it is *skew* if G is a disjoint union of X, X^* and $\{e\}$. For any function a: $G \to Z$ we define its periodic autocorrelation function, PAF_a: $G \to Z$, by the formula

$$\mathrm{PAF}_a(s) = \sum_{x \in G} a(x)a(x+s).$$

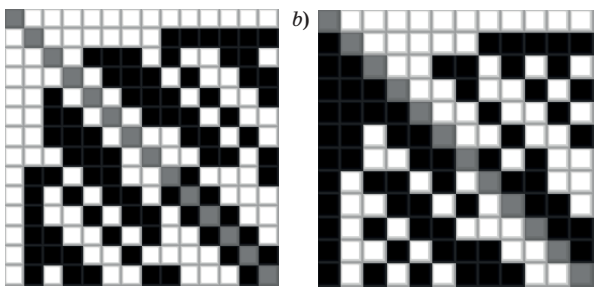
Definition 1 (*general case*). Let a and b be functions $G \to Z$ such that $a(e) = 0$ while all other values of a and all values of b belong to the set $\{+1, -1\}$. We say that the pair (a, b) is a *Legendre C-pair* if the sum of the PAFs of a and b has the constant value -2, except at the shift 0 where the sum attains its peak value $2v - 1$.

To a function a: $G \to Z$ we associate the matrix **A** of order v whose rows and columns are labeled by the elements of G and are given by the formula $\mathbf{A}_{x,y} = a(x^{-1}y)$. Such matrices are known as *G-invariant matrices* because they have the property that $\mathbf{A}_{xz,yz} = \mathbf{A}_{x,y}$ for all x, y, z in G. (By suitably arranging the indices, such matrices can be written as multi-circulants, i. e., circulants of circulants of ...). If (a, b) is a Legendre C-pair of length v and **A** and **B** are their associated matrices, it is easy to show that the matrix **C** given by (3) or (4) is a C-matrix. In that case we say that (a, b) is the *Legendre C-pair of* **C**. It is well known, see [7, Theorem 2.2], that each Paley C-matrix is equivalent to one of the form (3) or (4) with circulant blocks **A** and **B**. Hence, cyclic Legendre C-pairs of length v exist whenever $2v + 1$ is a prime power. The converse is false. For instance there exist a Legendre C-pair of length $v = 7$ while $2v + 1 = 15$ is not a prime power. For a concrete example with multi-circulant blocks **A** and **B** of order 25 see [5] or [6, section 10.3]. Another example is given below.

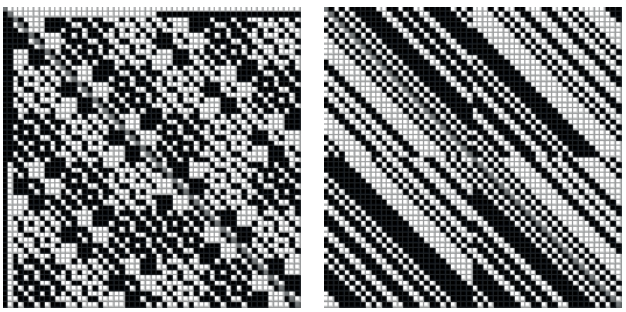
On Fig. 2 we show two skew-symmetric C-matrices. The first one has the form (4) with multi-circulant blocks **A** and **B** of order 27. It is constructed from the difference set X consisting of the nonzero squares in GF(27). To construct this field we used the primitive polynomial $x^3 - x^2 + 1$ over Z_3. The elements of GF(27) are the 27 polynomials $a + bx + cx^2$, with $a, b, c \in \{0, 1, 2\}$. We encode this polynomial by the symbol *abc*, and arrange the symbols in the lexicographic order 000, 001, 002, 010, 011, 012, ..., 222. Explicitly, we have $X = \{1, x^2, 2 + 2x + x^2, 2x + 2x^2, 2 + x + x^2, 1 + 2x + x^2, 2x + x^2, 2x, 1 + 2x^2, 1 + x, 2 + 2x^2, 1 + x + x^2, 1 + 2x\}$.

The corresponding 13 symbols are 100, 001, 221, 022, 211, 121, 021, 020, 102, 110, 202, 111, 120. The matrix **B** associated to X has -1 entries exactly at these 13 positions. It has the block-circulant structure with the first row **[U V W]**. The matrices **U**, **V**, **W** are also multi-circulants but of order 9. Their first block-rows are **[P, J, −J]**, **[−P, −Q, −Q]**, **[Q, P, P]** where **P**, **Q**, **J** are the circulants with the first rows [1, −1, 1], [1, 1, −1], [1, 1, 1], respectively. Further, $\mathbf{A} = \mathbf{B} - \mathbf{I}$.

The second matrix has the form $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ -\mathbf{B}^{\mathrm{T}} & \mathbf{A}^{\mathrm{T}} \end{pmatrix}$ where **A** and **B** are negacyclic blocks of size $v = 28$. We recall that a square matrix of order n is *nega-*



■ ***Fig. 1***. 2b2c conference matrices of orders 14 (*a*) and 12 (*b*), matrix portraits have white and black colors for entries 1, −1 and gray for 0



■ ***Fig. 2***. Two skew-symmetric C-matrices of order 56

cyclic if each row but the first is obtained from the previous one by the negacyclic shift

$$(x_1, x_2, x_3, ..., x_{n-1}, x_n) \to$$
$$\to (-x_n, x_1, x_2, ..., x_{n-2}, x_{n-1}).$$

The first rows of **A** and **B**, respectively, are

$a = [0, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1];$
$b = [1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1].$

Since A is negacyclic and $a_i = a_{v-i}$ for $i = 1, ..., v - 1$ the block **A** is skew-symmetric. Hence the second matrix is also skew-symmetric.

The list (1) gives the feasible sizes $n < 200$ of symmetric C-matrices. It is known that such matrices exist when $n - 1$ is a prime power. By removing such sizes we are left with only seven cases $n = 46$, 66, 86, 118, 146, 154, 186. C-matrices of size 46 have been constructed long time ago, while it is still unknown whether they exist in the remaining six sizes, see [9]. By using a computer search, we have shown that there are no cyclic Legendre C-pairs of length 22 or 32.

The first assertion of the following proposition follows from the properties of the block **A** mentioned earlier in this section.

Proposition 1. Let (a, b) be a Legendre C-pair on an abelian group G of order v and let k_1 and k_2 be the cardinalities of the sets $\{x \in G: a(x) = -1\}$ and $\{x \in G: b(x) = -1\}$, respectively. Then $a(x^{-1}) = (-1)^v a(x)$ for all x. If v is even then $k_1 = k_2 = v/2$. If v is odd then $k_1 = k_2 = (v - 1)/2$.

Proof: Let us prove the second assertion. By the hypothesis, v is even. Let **A** and **B** be the multi-circulant matrices associated to the functions a and b, respectively. Since (a, b) is a Legendre C-pair, the matrix **C** given by (3) is a C-matrix. The first and the second row of **C** are orthogonal to the third row. This gives the two equations

$$1 + (v - 1 - 2k_1) + (v - 2k_2) = 0;$$
$$1 + (v - 1 - 2k_1) - (v - 2k_2) = 0.$$

It follows that $k_1 = k_2 = v/2$. The proof of the third assertion is similar.

Corollary 1. If (a, b) is a Legendre C-pair on an abelian group G of odd order, then after replacing $a(e) = 0$ by $a(e) = 1$ (or $a(e) = -1$) we obtain a Legendre pair. (The converse is not valid.)

Special Legendre C-pairs

We now introduce a subclass of the class of Legendre C-pairs.

Definition 2. Let (a, b) be a Legendre C-pair on G, a group of order v. If v is odd we say that (a, b) is *special* if the subset $\{x \in G: b(x) = -1\}$ is symmetric. If v is even and G is cyclic, say $G = Z_v$, we say that (a, b) is *special* if $b_{v-1-i} = -b_i$, $i = 0, 1, ..., v - 1$.

We shall now prove that cyclic special Legendre C-pairs of length v exist whenever $2v + 1$ is a prime power.

Proposition 2. The equivalence class of any Paley C-matrix **C** contains a C-matrix of the form (3) or (4) whose Legendre C-pair is cyclic and special.

Proof: We follow the proof of [7, Theorem 2.2] and modify it in order to prove our assertion. All Paley C-matrices of the same order are mutually equivalent, see [7]. Hence it suffices to construct for each odd prime power $q = 2v + 1$ a Paley C-matrix **C** of order $q + 1$, having the 2b2c form (3) or (4), whose Legendre C-pair is cyclic and special.

Let V be the 2-dimensional vector space over GF(q) with basis vectors $x = (1, 0)$ and $y = (0, 1)$. Choose a primitive element η of GF(q). Define the vectors $z_k = y - \eta^k x = (-\eta^k, 1)$ for $k = 0, 1, ..., q - 2$. We arrange the vectors x, y and the z_k as follows: $x, y, z_0, z_2, ..., z_{2v-2}, z_1, z_3, ..., z_{2v-1}$. Note that this arrangement is slightly different from the one used in [7]. We use these $q + 1$ vectors to define a Paley C-matrix **C** as usual and let (a, b) be its Legendre C-pair. It follows from [7, Theorem 2.2] that **C** has the 2b2c form.

In more details, the entries of **C** are computed as follows. Let i and j be any indices in the range 1, 2, ..., $q + 1$. Let u and w be the i-th and j-th vectors in the above list, respectively. Then the (i, j)-th entry of **C** is equal to $\chi(\det(u, w))$ where (u, w) denotes the matrix of order two made up from u and w. Moreover, $a_k = \mathbf{C}_{3,3+k}$ and $b_k = \mathbf{C}_{3,v+3+k}$ for $k = 0, 1, ..., v - 1$.

We claim that $\mathbf{C}_{3,q+1-k} = -\chi(-1)\mathbf{C}_{3,v+3+k}$ for $k = 0, 1, ..., v - 1$. Indeed for $i = 3$ and $j = q + 1 - k$ we have $u = z_0 = (-1, 1)$ and $w = z_{q-2-2k} = (-\eta^{-2k-1}, 1)$. Since $\det(u, w) = \eta^{-2k-1} - 1$, we have $\mathbf{C}_{3,q+1-k} = \chi(\eta^{-2k-1} - 1 = -\chi(-1)\chi(\eta^{2k+1} - 1)$. Similarly we have $\mathbf{C}_{3,v+3+k} = \chi(\eta^{2k+1} - 1)$. We conclude that our claim holds.

Hence the sequence b satisfies the equalities $b_{v-k} = -\chi(-1)b_k$ for $k = 0, 1, ..., v - 1$. If $q \equiv 1 \pmod 4$ this means that the Legendre C-pair (a, b) is special. The same is true in the case $q \equiv 3 \pmod 4$ after a suitable cyclic shift of b. This completes the proof.

Corollary 2. Cyclic special Legendre C-pairs of length v exist whenever $2v + 1$ is a prime power.

Many special Legendre C-pairs of odd length v can be constructed from the so called Szekeres difference sets. We recall that the *Szekeres difference sets* are in fact a difference family (DF) in an abelian group G of odd order v consisting of two blocks, X and Y, such that X is skew and $|X| = |Y| = (v - 1)/2$. Hence the parameters of such DF are

$$(v;\ (v-1)/2,\ (v-1)/2;\ (v-3)/2). \qquad (5)$$

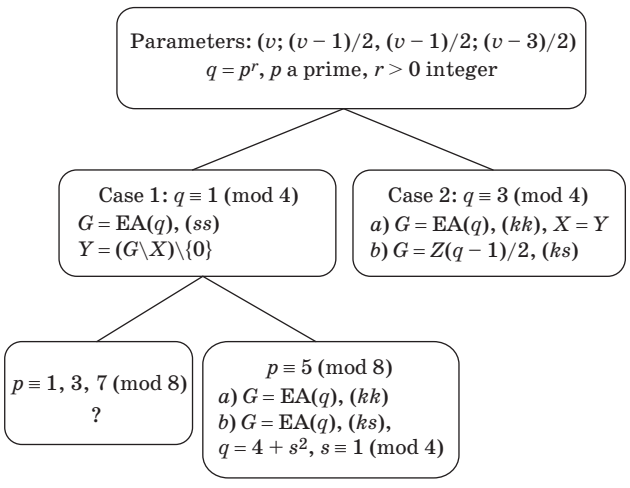
We say that a Szekeres DF (X, Y) is *special* if Y is symmetric. It is well known, see [1, Theorem 5.18] or [2], that the special Szekeres DFs in Z_v exist whenever $2v + 1$ is a prime power $\equiv 3 \pmod 4$. Let us give a simple example.

Example 1. Let $v = 5$ and note that $2v + 1 = 11$ is a prime $\equiv 3 \pmod 4$. The subsets $X = \{g, g^3\} = g + g^3$ and $Y = \{g^2, g^3\} = g^2 + g^3$ of the cyclic group $G = < g >$ of order 5 form a special Szekeres DF. The * operator sends g^i to g^{-i}. Thus $X^* = \{g^2,\ g^4\} = g^2 + g^4$, $Y^* = Y$ and we have $G = X + X^* + e$. To construct the special Legendre C-pair, we form the binary sequence $a = (1, -1, 1, -1, 1)$ by setting $a_i = -1$ if $g^i \in X$ and $a_i = 1$ otherwise, and form $b = (1, 1, -1, -1, 1)$ similarly by using Y. The sum of the PAFs of a and b is the constant function -2 apart from the origin. Thus (a, b) is a Legendre pair. By replacing the first term of a by 0 we obtain a special Legendre C-pair.

Difference families with parameters (5)

In the following diagram (Fig. 3) we summarize the main results on the existence of DFs (X, Y) with parameters (5) and X and Y symmetric or skew. By EA(q) we denote an elementary abelian group of order $q = p^r$, p a prime, r a positive integer. [The additive group of GF(q) is an EA(q).] The symmetry types of X and Y are indicated by the letter s if the block is symmetric, k if it is skew, and the symbol $*$ if no symmetry is required. For instance (ks) means that X is skew and Y is symmetric. While arbitrary Szekeres DFs have the symmetry type ($k*$), the special ones have type (ks).

In Case 1 the block X is the set of nonzero squares in GF(q). The same is true for part a) of Case 2, see [2, Theorem 4]. For part b) of Case 2 see [2, Theorem 3] and [1, Theorem 5.18]. Note that in the first subcase ($p \equiv 1, 3, 7 \pmod 8$) of Case 1 we also require that $q \equiv 1 \pmod 8$. No general result seems to be known about this subcase. In the second subcase ($p \equiv 5 \pmod 8$), part a) was proved in [2, Theorem 5] when $q \equiv 5 \pmod 8$ and in [3, 4] when $q \equiv 1 \pmod 8$. For part b) of the same subcase see [11].



■ ***Fig. 3.*** Existence of DFs (X, Y) with parameters (5)

Let us give two examples of Legendre C-pairs (X, Y) of type (kk) and length v with $2v + 1$ not a prime power. Both examples are obtained from a theorem of Szekeres, see [2, Theorem 6] and [5, Theorem 2]. First example: we start with the Szekeres DF (X, Y) in Z_{37}:

$X = \{3, 4, 5, 6, 8, 11, 13, 17, 19, 21, 22, 23, 25, 27, 28, 30, 35, 36\}$;
$Y = \{2, 3, 4, 11, 14, 15, 18, 20, 21, 24, 25, 27, 28, 29, 30, 31, 32, 36\}$.

The corresponding binary sequences a and b are

$a = (1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1)$;
$b = (1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, -1)$.

Since X is skew, by replacing the first term of a by 0, we obtain a Legendre C-pair of length 37. Second example: (X, Y) in Z_{61}:

$X = \{2, 3, 4, 5, 7, 14, 18, 19, 23, 24, 26, 27, 30, 32, 33, 36, 39, 40, 41, 44, 45, 46, 48, 49, 50, 51, 52, 53, 55, 60\}$;
$Y = \{3, 4, 5, 6, 8, 10, 11, 14, 17, 19, 21, 27, 28, 29, 31, 35, 36, 37, 38, 39, 41, 43, 45, 46, 48, 49, 52, 54, 59, 60\}$.

It gives the Legendre C-pair

$a = (0, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1)$
$b = (1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1)$

of length 61. In general, such pairs of length q exist whenever q is a power of a prime $p \equiv 5 \pmod 8$, see [2–4].

Regarding the Legendre C-pairs of symmetry type (ks) one can ask whether they exist for lengths v when $2v + 1$ is not a prime power? It turns out that they do. The smallest such pair known to us has

length $v = 1373$ in which case $2v + 1 = 2747 = 41 \times 67$. For this see [11, Theorem 3.1].

Characterization of Legendre C-pairs

Let us give an algebraic characterization of Legendre C-pairs over an abelian group G of order v with the identity element e. Let $a, b: G \to Z$ be functions such that $a(e) = 0$ and all other values of a and all the values of b are +1 or −1. Define the subsets $X, Y \subseteq G$ by

$$X = \{x \in G: a(x) = -1\} \text{ and } Y = \{x \in G: b(x) = -1\}. \quad (6)$$

Note that $e \notin X$ because $a(e) = 0$. Also note that the pair (X, Y) determines uniquely the pair (a, b). If (a, b) is a Legendre C-pair, by using Definition 1 and [6, equation (7)], it is straightforward to verify that

$$N(G - e - 2X) + N(G - 2Y) =$$
$$= (2v - 1)e - 2(G - e) = (2v + 1)e - 2G. \quad (7)$$

Proposition 3. Let a, b, X, Y be as above. (We shall view the subsets $X, Y \subseteq G$ also as elements of the group ring $Z[G]$.) If v is even then (a, b) is a Legendre C-pair if and only if

$$XX^* + YY^* = \frac{v}{2}(e + G) - X. \quad (8)$$

If v is odd then (a, b) is a Legendre C-pair if and only if

$$XX^* + YY^* = \frac{v+1}{2}e + \frac{v-3}{2}G. \quad (9)$$

Proof: First, let v be even and assume that (a, b) is a Legendre C-pair. By Proposition 1 we have $X^* = X$ and $k_1 = k_2 = v/2$. Since $GG = vG$, $GX = k_1G$ and $GY = k_2G$, it is easy to verify that $N(G - e - 2X) = 4N(X) + 4X + e - (v + 2)G$ and $N(G - 2Y) = 4N(Y) - vG$. The sum of these two norms is equal to $4(N(X) + N(Y)) + 4X + e - 2(v + 1)G$. By comparing this expression with the right hand side of (7) we obtain (8). For the converse note that (8) implies that $X^* = X$ and so we can reverse the above arguments.

Second, let v be odd and assume that (a, b) is a Legendre C-pair. By Proposition 1 we have $X^* + X = G - e$ and $k_1 = k_2 = (v - 1)/2$. Since $GG = vG$, $GX = k_1G$ and $GY = k_2G$, it is easy to verify that $N(G - e - 2X) = 4N(X) - (v - 2)G - e$ and $N(G - 2Y) = 4N(Y) - (v - 2)G$. The sum of these two norms is equal to $4(N(X) + N(Y)) - (v - 2)G - e - (v - 2)G$. By comparing this expression with the right hand side of (7) we obtain (9).

The following corollary follows immediately from the second claim of Proposition 3.

Corollary 3. In the case when v is odd, the functions (a, b) form a Legendre C-pair if and only if the corresponding subsets X, Y form a Szekeres DF in G.

Note that if (a, b) in this corollary is a special Legendre C-pair then the corresponding Szekeres DF (X, Y) is also special.

Example 2. Let us verify the equation (9) for the sequences $a = (0 - + - +)$, $b = (- + + + -)$. In these sequences, + and − stand for +1 and −1 respectively. They form a special Legendre C-pair of length $v = 5$. By using (6) we find that $X = \{g^1, g^3\} = g + g^3$ and $Y = \{g^0, g^4\} = e + g^4$. Thus $Y^* = e + g$ and so Y is not symmetric. However its translate $Yg^{-2} = g^2 + g^3$ is symmetric. Further, $XX^* = 2e + g^2 + g^3$ and $YY^* = 2e + g + g^4$. Thus $XX^* + YY^* = 4e + g + g^2 + g^3 + g^4 = 3e + G$.

Example 3. Let us verify the equation (8) for the sequences $a = (0 + - - - +)$, $b = (- + + - - +)$. They form a special Legendre C-pair of length $v = 6$. By using (6) we find that $X = \{g^2, g^3, g^4\} = g^2 + g^3 + g^4$ and $Y = \{g^0, g^3, g^4\} = e + g^3 + g^4$. Further, we have $XX^* = 3e + 2g + g^2 + g^4 + 2g^5$ and $YY^* = 3e + g + g^2 + 2g^3 + g^4 + g^5$. Thus $XX^* + YY^* = 6e + 3g + 2(g^2 + g^3 + g^4) + 3g^5 = 3(e + G) - X$.

Algorithm for constructing negacyclic C-matrices

As stated earlier, all Paley C-matrices of the same order $n = 1 + q$ are equivalent to each other. In view of Proposition 2, the equivalence class of any Paley C-matrix contains a C-matrix of 2b2c-type. It is also well known that the same equivalence class also contains a negacyclic C-matrix, see [12, Corollary 7.2].

Let q be any odd prime power. We describe a simple algorithm which for any given q outputs a negacyclic C-matrix $\mathbf{C}$ of order $n = 1 + q$ equivalent to the Paley C-matrix of the same order. This algorithm is based on the proof of [12, Corollary 7.2]. Since $\mathbf{C}$ is negacyclic it suffices to find its first row $[c_0 = 0, c_1, c_2, ..., c_q]$.

By a theorem of Belevitch, see [12, Theorem 4.1], we have $c_{n/2+j} = (-1)^j c_{n/2-j}$ for $j = 1, 2, ..., n/2 - 1$. Thus it suffices to compute only the values of c_i for $i = 1, 2, ..., n/2$.

We assume that a suitable software for computations in finite fields is available. (One of the authors used Maple and its GF package.)

Step 1. Construct the finite field GF(q^2) and select any primitive element ε of that field.

Step 2. Construct the matrix $\mathbf{A}$ of order 2 with first row $[0, -\omega]$ and second row $[1, \tau]$ where $\omega = \varepsilon^{1+q}$ and $\tau = \varepsilon + \varepsilon^q$. Note that ω and τ belong to the subfield GF(q) while ε does not. In fact ω is a primitive element of GF(q).

Step 3. Set $x_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and define the vectors $x_i = \begin{pmatrix} x_i[1] \\ x_i[2] \end{pmatrix}$, $i = 1, 2, ..., n/2$ recursively by the formula $x_{i+1} = \mathbf{A}x_i$.

Step 4. Then we have $c_i = \chi(x_i[2])$ for $i = 1, 2, ..., n/2$ where χ is the quadratic character of GF(q).

This completes the description of the algorithm.

We remark that in the case $q \equiv 1 \pmod 4$ the Paley C-matrix of order $1 + q$ is also equivalent to a C-matrix of 2c-type, i. e., a C-matrix made up from two circulants as in (2) or (3) but without any border.

Example 4. We choose $q = 9$ and for a primitive polynomial $f(x)$ of degree 4 over the field GF(3) = $= Z_3$ we choose $f(x) = x^4 - x - 1$. Then GF(81) = $= Z_3[x]/(x^4 - x - 1)$, a quotient ring of $Z_3[x]$ mod the ideal (f). Denote by ε the image of x in GF(81). Then we have $\varepsilon^4 = 1 + \varepsilon$. Thus $\varepsilon^8 = 1 - \varepsilon + \varepsilon^2$, and we obtain that $\omega = \varepsilon^{10} = 1 + \varepsilon + \varepsilon^2 - \varepsilon^3$. A further computation shows that $\omega^2 = 1 - \omega$ and $\omega^3 = -1 - \omega$. As $\omega^4 = -1$ we have $\omega^5 = -\omega$, $\omega^6 = -\omega^2$ and $\omega^7 = -\omega^3$. The subfield GF(9) is given by GF(9) = $\{0, \pm 1, \pm\omega, \pm 1 \pm \omega\}$. The matrix $\mathbf{A}$ has rows $[0, -\omega]$ and $[1, \omega^2]$. The first row c of $\mathbf{C}$ has the form $c = [0, c_1, c_2, c_3, c_4, c_5, -c_4, c_3, -c_2, c_1]$. The vectors x_i are

$$x_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad x_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad x_2 = \begin{pmatrix} -\omega \\ \omega^2 \end{pmatrix}, \quad x_3 = \begin{pmatrix} -\omega^3 \\ -1-\omega \end{pmatrix},$$

$$x_4 = \begin{pmatrix} \omega + \omega^2 \\ \omega^3 - \omega^2 \end{pmatrix}, \quad x_5 = \begin{pmatrix} 1 - \omega^3 \\ 1 + \omega^2 \end{pmatrix}.$$

Finally, we compute the c_i: $c_1 = \chi(1) = 1$, $c_2 = \chi(\omega^2) = = 1$, $c_3 = \chi(-1 - \omega) = \chi(\omega^3) = -1$, $c_4 = \chi(\omega^3 - \omega^2) = \chi(1) = 1$ and $c_5 = \chi(1 + \omega^2) = \chi(\omega^3) = -1$. Thus $c = [0, 1, 1, -1, 1, -1, -1, -1, -1, 1]$.

Special Legendre C-pairs of even length

We list below the special Legendre C-pairs of even length $v < 70$, which give 2b2c-type symmetric C-matrices of order $2v + 2$. The pairs are specified by the subsets X and Y (see Proposition 3). For $v = 2, 4, 6$ we show the sequences a and b as well. In all cases $2v + 1$ is a power of a prime.

$v = 2$
[1], [0] $a = (0\ -)$, $b = (-\ +)$
$v = 4$
[1, 3], [0, 1] $a = (0\ -\ +\ -)$, $b = (-\ -\ +\ +)$
$v = 6$
[2, 3, 4], [0, 3, 4] $a = (0\ +\ -\ -\ -\ +)$, $b = (-\ +\ +\ -\ -\ +)$
$v = 8$
[2, 3, 5, 6], [0, 4, 5, 6]
$v = 12$
[1, 4, 5, 7, 8, 11], [0, 2, 3, 4, 5, 10]
$v = 14$
[3, 4, 5, 7, 9, 10, 11], [0, 1, 2, 4, 5, 7, 10]
$v = 18$
[1, 2, 4, 5, 9, 13, 14, 16, 17], [0, 1, 2, 3, 6, 8, 10, 12, 13]
$v = 20$
[2, 6, 7, 8, 9, 11, 12, 13, 14, 18], [0, 4, 5, 7, 8, 10, 13, 16, 17, 18]
$v = 24$
[2, 3, 5, 9, 10, 11, 13, 14, 15, 19, 21, 22], [0, 2, 3, 9, 12, 13, 15, 16, 17, 18, 19, 22]
$v = 26$
[1, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 25], [0, 1, 6, 7, 9, 10, 12, 14, 17, 20, 21, 22, 23]
$v = 30$
[1, 3, 8, 9, 11, 12, 14, 15, 16, 18, 19, 21, 22, 27, 29], [0, 6, 7, 11, 12, 14, 16, 19, 20, 21, 24, 25, 26, 27, 28]
$v = 36$
[2, 7, 9, 10, 11, 12, 13, 16, 17, 19, 20, 23, 24, 25, 26, 27, 29, 34], [0, 3, 5, 6, 10, 11, 12, 14, 15, 16, 18, 22, 26, 27, 28, 31, 33, 34]
$v = 40$
[1, 2, 3, 6, 8, 9, 13, 14, 16, 18, 22, 24, 26, 27, 31, 32, 34, 37, 38, 39], [0, 1, 3, 4, 6, 10, 11, 12, 13, 14, 15, 17, 18, 19, 23, 30, 31, 32, 34, 37]
$v = 44$
[1, 2, 3, 8, 11, 12, 13, 16, 18, 19, 20, 24, 25, 26, 28, 31, 32, 33, 36, 41, 42, 43], [0, 3, 5, 6, 9, 10, 12, 13, 14, 15, 16, 17, 19, 21, 23, 25, 32, 35, 36, 39, 41, 42]
$v = 48$
[3, 4, 9, 11, 12, 14, 16, 17, 18, 20, 21, 22, 26, 27, 28, 30, 31, 32, 34, 36, 37, 39, 44, 45], [0, 3, 4, 5, 8, 12, 14, 15, 16, 17, 18, 19, 21, 24, 25, 27, 34, 36, 37, 38, 40, 41, 45, 46]
$v = 50$
[2, 3, 8, 10, 11, 13, 17, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 37, 39, 40, 42, 47, 48], [0, 2, 5, 9, 10, 11, 13, 14, 17, 19, 20, 21, 25, 26, 27, 31, 33, 34, 37, 41, 42, 43, 45, 46, 48]
$v = 54$
[2, 3, 4, 5, 13, 15, 16, 18, 19, 22, 23, 24, 26, 27, 28, 30, 31, 32, 35, 36, 38, 39, 41, 49, 50, 51, 52], [0, 2, 3, 5, 9, 12, 16, 17, 18, 22, 24, 27, 28, 30, 32, 33, 34, 38, 39, 40, 42, 43, 45, 46, 47, 49, 52]
$v = 56$
[3, 4, 5, 7, 9, 15, 16, 18, 20, 21, 23, 24, 25, 26, 30, 31, 32, 33, 35, 36, 38, 40, 41, 47, 49, 51, 52, 53], [0, 1, 4, 5, 6, 7, 9, 13, 19, 20, 23, 26, 28, 30, 31, 33, 34, 37, 38, 39, 40, 41, 43, 44, 45, 47, 52, 53]
$v = 60$
[1, 2, 4, 5, 7, 9, 11, 14, 15, 16, 17, 21, 22, 25, 26, 34, 35, 38, 39, 43, 44, 45, 46, 49, 51, 53, 55, 56, 58, 59], [0, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 17, 22, 24, 25, 26, 28, 29, 32, 36, 38, 39, 40, 41, 43, 44, 49, 51, 57, 58]

$v = 62$
[3, 4, 8, 13, 14, 15, 16, 18, 19, 20, 21, 22, 24, 28, 29, 31, 33, 34, 38, 40, 41, 42, 43, 44, 46, 47, 48, 49, 54, 58, 59], [0, 2, 4, 5, 6, 9, 12, 13, 19, 21, 22, 24, 27, 31, 32, 33, 35, 36, 38, 41, 43, 44, 45, 46, 47, 50, 51, 53, 54, 58, 60]
$v = 68$
[1, 3, 4, 5, 7, 9, 10, 11, 14, 15, 18, 20, 23, 30, 31, 32, 33, 35, 36, 37, 38, 45, 48, 50, 53, 54, 57, 58, 59, 61, 63, 64, 65, 67], [0, 4, 5, 6, 7, 9, 11, 12, 13, 14, 16, 17, 22, 23, 25, 26, 28, 29, 33, 35, 36, 37, 40, 43, 46, 47, 48, 49, 52, 57, 59, 64, 65, 66]

Special Legendre C-pairs of odd length

For the sake of completeness we list here the special Szekeres DFs in cyclic groups Z_v for odd lengths $v < 70$ whenever $2v + 1$ is a prime power. In the first three cases we also give the corresponding special Legendre C-pairs. For odd v in this range, when $2v + 1$ is not a prime power, we were not able to find any special Szekeres DFs. We point out that the diagram in Fig. 2 shows (the case $q = 25 \equiv 1 \pmod 4$ and $p = 5$) that there exist Szekeres DFs in EA(25) of symmetry type (*kk*).

$v = 1$
[], [] $a = (0)$, $b = (+)$
$v = 3$
[1], [0] $a = (0 - +)$, $b = (- + +)$
$v = 5$
[3, 4], [1, 4] $a = (0 + + - -)$, $b = (+ \ - + + -)$
$v = 9$
[1, 2, 3, 5], [1, 4, 5, 8];
$v = 11$
[2, 3, 4, 6, 10], [0, 2, 3, 8, 9]
$v = 13$
[4, 7, 8, 10, 11, 12], [1, 3, 4, 9, 10, 12]
$v = 15$
[3, 5, 8, 9, 11, 13, 14], [0, 1, 2, 6, 9, 13, 14]
$v = 21$
[2, 4, 8, 11, 12, 14, 15, 16, 18, 20], [2, 3, 4, 5, 8, 13, 16, 17, 18, 19]
$v = 23$
[1, 2, 4, 5, 6, 7, 9, 12, 13, 15, 20], [0, 1, 2, 6, 8, 11, 12, 15, 17, 21, 22]
$v = 29$
[1, 7, 8, 10, 12, 15, 16, 18, 20, 23, 24, 25, 26, 27], [2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27]
$v = 33$
[2, 3, 4, 6, 7, 8, 9, 10, 12, 17, 18, 19, 20, 22, 28, 32], [2, 3, 4, 6, 9, 10, 13, 15, 18, 20, 23, 24, 27, 29, 30, 31]
$v = 35$
[1, 3, 7, 8, 9, 10, 11, 13, 14, 15, 18, 19, 23, 29, 30, 31, 33],
[0, 2, 6, 7, 9, 12, 15, 16, 17, 18, 19, 20, 23, 26, 28, 29, 33]
$v = 39$
[1, 3, 4, 5, 6, 10, 13, 14, 16, 20, 21, 22, 24, 27, 28, 30, 31, 32, 37],
[0, 3, 5, 9, 10, 14, 16, 17, 18, 19, 20, 21, 22, 23, 25, 29, 30, 34, 36]
$v = 41$
[2, 3, 4, 5, 6, 8, 9, 11, 12, 16, 17, 19, 21, 23, 26, 27, 28, 31, 34, 40],
[2, 3, 4, 6, 7, 8, 10, 15, 17, 18, 23, 24, 26, 31, 33, 34, 35, 37, 38, 39]
$v = 51$
[5, 9, 11, 12, 13, 16, 17, 19, 21, 22, 26, 27, 28, 31, 33, 36, 37, 41, 43, 44, 45, 47, 48, 49, 50], [0, 1, 2, 3, 4, 7, 10, 11, 13, 15, 20, 22, 23, 28, 29, 31, 36, 38, 40, 41, 44, 47, 48, 49, 50]
$v = 53$
[1, 5, 8, 10, 12, 13, 14, 15, 16, 18, 21, 22, 23, 24, 27, 28, 33, 34, 36, 42, 44, 46, 47, 49, 50, 51], [2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 23, 26, 27, 30, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51]
$v = 63$
[1, 2, 5, 6, 12, 17, 18, 19, 21, 25, 27, 29, 30, 32, 35, 37, 39, 40, 41, 43, 47, 48, 49, 50, 52, 53, 54, 55, 56, 59, 60], [0, 1, 4, 6, 7, 8, 10, 11, 13, 14, 22, 23, 25, 27, 30, 31, 32, 33, 36, 38, 40, 41, 49, 50, 52, 53, 55, 56, 57, 59, 62]
$v = 65$
[2, 5, 6, 7, 9, 10, 13, 14, 15, 16, 17, 19, 20, 22, 28, 29, 31, 33, 35, 38, 39, 40, 41, 42, 44, 47, 53, 54, 57, 61, 62, 64], [4, 5, 7, 10, 12, 14, 18, 19, 20, 22, 23, 24, 25, 26, 30, 31, 34, 35, 39, 40, 41, 42, 43, 45, 46, 47, 51, 53, 55, 58, 60, 61]
$v = 69$
[1, 5, 8, 10, 11, 12, 13, 16, 17, 18, 19, 22, 24, 25, 26, 27, 28, 29, 31, 33, 35, 37, 39, 46, 48, 49, 54, 55, 60, 62, 63, 65, 66, 67], [2, 3, 5, 7, 8, 11, 12, 13, 15, 20, 21, 24, 27, 31, 32, 33, 34, 35, 36, 37, 38, 42, 45, 48, 49, 54, 56, 57, 58, 61, 62, 64, 66, 67]

Acknowledgements

The research of the first author leading to these results has received funding from the Ministry of Education and Science of the Russian Federation according to the project part of the state funding assignment No 2.2200.2017/4.6. The research of the second author was enabled in part by support provided by SHARCNET (http://www.sharcnet.ca) and Compute Canada (http://www.computecanada.ca).

References

1. Seberry J. *Orthogonal Designs: Hadamard Matrices, Quadratic Forms and Algebras*. Chapter 4. Springer, 2017. doi:10.1007/978-3-319-59032-5

2. Szekeres G. Tournaments and Hadamard matrices. *L'Enseignement Math*, 1969, vol. 15, pp. 269–278.
3. Szekeres G. Cyclotomy and complementary difference sets. *Acta Arithmetica*, 1971, vol. 18, pp. 349–353. doi:10.4064/aa-18-1-349-353
4. Whiteman A. L. An infinite family of skew Hadamard matrices. *Pacific Journal of Mathematics*, 1971, vol. 38, no. 3, pp. 817–822.
5. Blat D. and Szekeres G. A skew Hadamard matrix of order 52. *Canad. J. Math*., 1969, vol. 21, pp. 1319–1322.
6. Đoković D. Ž., Kotsireas I. S. Computational methods for difference families in finite abelian groups. *Spec. Matrices*, 2019, vol. 7, pp. 127–141. doi:10.1515/spma-2019-0012
7. Goethals J.-M., Seidel J. J. Orthogonal matrices with zero diagonal. *Canad. J. Math.,* 1967, vol. 19, pp. 1001–1010. doi:10.4153/CJM-1967-091-8
8. van Lint J. H., Wilson R. M. *A Course in Combinatorics*. Cambridge University Press, 1992. 530 p.
9. Balonin N. A., Seberry J. A review and new symmetric conference matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 4, pp. 2–7.
10. Fletcher R. J., Gysin M., Seberry J. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. *Australas. J. Combin*, 2001, vol. 23, pp. 75–86.
11. Ding C. Two constructions of $(v, (v-1)/2, (v-3)/2)$ difference families. *J. Combin. Designs*, 2008, vol. 16, no. 2, pp. 164–171. doi:10.1002/jcd.20159
12. Delsarte P., Goethals J.-M., Seidel J. J. Orthogonal matrices with zero diagonal II. *Canad. J. Math*., 1971, vol. 23, no. 5, pp. 816–832.

УДК 004.438
doi:10.31799/1684-8853-2020-4-2-10

Конференц-матрицы на основе С-пар Лежандра

Н. А. Балонин[a], доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
Д. Ж. Джокович[б], доктор наук, профессор, orcid.org/0000-0002-0176-2395, djokovic@uwaterloo.ca
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ
[б]Университет Ватерлоо, кафедра чистой математики и Институт квантовых вычислений, Ватерлоо, Онтарио, N2L 3G1, Канада

Введение: существует несколько методов построения симметричных С-матриц ввиду отсутствия для них универсальной структуры. Это ограничение принципиально, кроме того, в литературе неполно освещена структура С-матриц с парной каймой, что делает ее изучение особенно актуальным. **Цель:** детально описать бициклическую конструкцию с парной каймой и предложить концепцию С-пар Лежандра. **Результаты:** рассмотрены С-матрицы порядка $n = 2v + 2$ с парной каймой на основе адаптации так называемых обобщенных пар Лежандра нечетной длины v к более широкому случаю четных и нечетных значений v, что позволяет построить новые С-пары Лежандра в конечных абелевых группах G порядка v. Такая пара описывается двумя функциями a, b: $G \to Z$, значения которых равны +1 или −1, за исключением $a(e) = 0$, где e – единичный элемент группы G, через Z обозначено кольцо целых чисел. Для характеристики С-пар Лежандра введены два набора $X = \{x \in G: a(x) = -1\}$ и $Y = \{x \in G: b(x) = -1\}$ группы G. Показано, что $a(x^{-1}) = (-1)^v a(x)$ для всех x. Для нечетных значений v отмечено, что X и Y образуют разностное семейство, что неприменимо к четным порядкам. Это разностное семейство и разностное семейство Секереша — один и тот же класс, первоначально используемый для построения кососимметричных матриц Адамара. Введен подкласс специальных С-пар Лежандра и доказано, что они существуют для случаев, когда $2v + 1$ — степень простого числа. В последних двух разделах статьи приведены примеры специальных циклических С-пар Лежандра для размеров $v < 70$. **Практическая значимость:** С-матрицы широко используются в задачах помехоустойчивого кодирования, сжатия и маскирования видеоинформации. Программы для поиска конференц-матриц и библиотеки построенных матриц применяются в математической сети «mathscinet.ru» вместе с исполняемыми онлайн-алгоритмами.

Ключевые слова — конференц-матрицы, кососимметричные матрицы Адамара, периодические автокорреляционные функции, разностные семейства Секереша, обобщенные пары Лежандра, конструкции, телефония.

Для цитирования: Balonin N. A., Đoković D. Ž. Conference matrices from Legendre C-pairs. *Информационно-управляющие системы*, 2020, № 4, с. 2–10. doi:10.31799/1684-8853-2020-4-2-10
For citation: Balonin N. A., Đoković D. Ž. Conference matrices from Legendre C-pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 4, pp. 2–10. doi:10.31799/1684-8853-2020-4-2-10