Operations Research Perspectives 10 (2023) 100260

Contents lists available at ScienceDirect

Operations Research Perspectives

journal homepage: www.elsevier.com/locate/orp

An integer programming model for obtaining cyclic quasi-difference matrices

Luis Martínez [a,*], María Merino [a,b], Juan Manuel Montoya [a,c]

[a] University of the Basque Country UPV/EHU, Department of Mathematics, 48080 Bilbao, Spain
[b] Basque Center for Applied Mathematics (BCAM), Alameda Mazarredo 14, 48009 Bilbo, Bizkaia, Spain
[c] University of Pamplona, Faculty of Basic Sciences, Pamplona, Colombia

ARTICLE INFO

Keywords:
Integer programming
Bimodal Local Search
Orthogonal arrays
Automorphism groups
Quasi-difference matrices

ABSTRACT

Orthogonal arrays are of great importance in mathematical sciences. This paper analyses a certain practical advantage of quasi-difference matrices over difference matrices to obtain orthogonal arrays with given parameters. We also study the existence of quasi-difference matrices over cyclic groups originating orthogonal arrays with $t = 2$ and $\lambda = 1$, proving their existence for some parameters sets. Moreover, we present an Integer Programming model to find such quasi-difference matrices and also a Bimodal Local Search algorithm to obtain them. We provide a conjecture related to the distributions of differences along rows and columns of arbitrary square matrices with entries in a cyclic group in positions outside the main diagonal which shows an intriguing symmetry, and we prove it when the matrix is a quasi-difference matrix.

1. Introduction

Orthogonal arrays (OAs) are of great importance in pure and applied mathematical sciences. In particular, it is crucial to dilucidate the question of the existence of OAs and to find constructions for them (see [1] and [2, Chapters 6 and 7, III]). Moreover, they have applications in Graph Theory [3], Coding theory [4,5], Cryptography [6], Computer Science [7], Chemistry [8], Engineering [9], and Quantum Information Theory [10,11].

An OA(N, k, s, t) is an $N \times k$ array with entries from an alphabet with s symbols (also called levels) in which every $N \times t$ subarray contains every t-tuple of S^t the same number λ of times as a row. The parameter λ can be deduced from N, s and t, because $N = \lambda s^t$. The number of columns is called also number of factors, and t is known as the strength of the orthogonal array. Following the usual notation, when $t = 2$ and $\lambda = 1$ we will refer to an OA$(n^2, m, n, 2)$ just as an OA(m, n).

Symmetry is useful when trying to solve certain difficult mathematical problems [12,13]. In the case of orthogonal arrays (OAs) their symmetries are permutations of symbols or columns (or more generally combinations of those of the previous types) that preserve their structure, and they constitute their whole automorphism groups (more generally we are interested in subgroups of this whole automorphism groups, which we call automorphism groups).

The study of the groups of automorphisms of different classes of combinatorial structures allows certain properties to be determined, and facilitates the finding of their constructions for certain parameters sets. The cases in which the action of the group of automorphisms is regular or, more generally, semiregular are especially interesting. This is what happens, for example, in the case of combinatorial designs [14–16], undirected strongly regular graphs [17,18], or directed strongly regular graphs [19,20].

In particular, Bose and Bush studied in [21] the OAs admitting an abelian automorphism group of symbols that acts regularly on the set of symbols. These types of OAs are generated by the so-called difference schemes. They are formalized with more generality for arbitrary groups with the concept of difference matrix [2, Chapter 17, VI]. We use both terms interchangeably since we only consider abelian groups in this paper. As described in [1], an $r \times c$ array with entries in an abelian group G of order s is called a difference scheme based on G if for all i and j with $1 \le i, j \le c$ and $i \ne j$ the vector difference between the ith and the jth columns of the array contains every element of G the same number of times. If we use λ to denote this number of times, then $r = \lambda s$, and in this case we say that the difference scheme is a $D(r, c, s)$. Obviously, a $D(r, c, s)$ generates an OA$(rs, c, s, 2)$, by taking the translates of the rows obtained adding the same element x of G to all their coordinates for $x \in G$. When the group on which a difference scheme is based is cyclic the difference scheme is called cyclic. When $\lambda = 1$ we will use just $D(c, s)$ to denote a $D(s, c, s)$ in this work.

OAs admitting an automorphism group of symbols fixing one of the symbols and acting regularly on the other ones have been studied in the literature. They can be determined by special cases of quasi-difference matrices [2,22,23].

* Corresponding author.
E-mail addresses: luis.martinez@ehu.eus (L. Martínez), maria.merino@ehu.eus (M. Merino), jmontoya006@ikasle.ehu.eus (J.M. Montoya).

https://doi.org/10.1016/j.orp.2022.100260
Received 26 September 2022; Received in revised form 3 December 2022; Accepted 4 December 2022
Available online 9 December 2022

Definition 1.1 (*[2, Chapter 17, VI]*). Given an abelian group G of order n, a $(n, k; \lambda, \mu; u)$-quasi difference matrix is a matrix $Q = (q_{ij})$ with k rows and $\lambda(n-1+2u)+\mu$ columns with entry either empty (usually denoted by -) or an element in G, such that each row contains exactly λu empty entries, each column contains at most one empty entry, and for each $1 \le i < j \le k$ the multiset

$$\{q_{il} - q_{jl} : 1 \le l \le \lambda(n-1+2u)+\mu, \text{ with } q_{il} \text{ and } q_{jl} \text{ non empty}\}$$

contains every nonzero element in G exactly λ times and 0 exactly μ times.

The quasi-difference matrices that we are going to analyse in this work are the ones that originate OAs of strength 2 and index unity, which are those that have a direct relationship with strongly regular graphs. We are also interested in the case in which the group G is cyclic, because it is powerful enough to guarantee the existence of OAs for many of the currently known parameters despite the plainness of the group structure. We will refer to such matrices as cyclic quasi-difference matrices.

Definition 1.2. We say that an orthogonal array of strength 2 and index unity is a quasi-cyclic orthogonal array if it admits a cyclic automorphism group fixing one of the symbols and acting regularly on the other symbols.

This type of group actions fixing an element and acting regularly (and, more generally, semiregularly) in the other elements has been considered in the literature for other types of combinatorial structures (they are usually called one-rotational), such as for example in [24] for strongly regular graphs and in [14] for combinatorial designs.

We will next provide a simple example. Following the notation in the aforementioned papers [14,24], we will use ∞ to denote the symbol fixed by the group and the other symbols by $0, \dots, n-2$.

The array

$$\begin{pmatrix} 0,0,\infty,1 \\ 0,1,1,\infty \\ 0,\infty,0,0 \\ 1,0,0,\infty \\ 1,1,\infty,0 \\ 1,\infty,1,1 \\ \infty,0,1,0 \\ \infty,1,0,1 \\ \infty,\infty,\infty,\infty \end{pmatrix}$$

is an OA$(4,3)$ admitting the automorphism that fix the symbol ∞ and permutes cyclically the symbols 0,1. Of course giving a single representative for each orbit of the action of the group in the set of rows is sufficient to determine it, and we can then order the rows lexicographically with respect to the order in which $0 < 1 < \infty$, obtaining the subarray

$$\begin{pmatrix} 0,0,\infty,1 \\ 0,1,1,\infty \\ 0,\infty,0,0 \\ \infty,0,1,0 \\ \infty,\infty,\infty,\infty \end{pmatrix}$$

If we remove the last all-infinity row, then transpose it and after that we replace the infinities with the symbol — we get the following $(2,4;1,1;1)$-quasi difference matrix:

$$\begin{pmatrix} 0,0,0,- \\ 0,1,-,0 \\ -,1,0,1 \\ 1,-,0,0 \end{pmatrix}$$

More generally, the matrices that we are considering are cyclic $(n-1, m; 1, 1; 1)$-quasi difference matrices. We will call such a matrix a CQDM(m,n). When the aforementioned lexicographic ordering is performed we will say that the quasi-difference matrix is in canonical form.

We may wonder if the concept of CQDM has any practical advantage over that of CDS, apart from the theoretical interest that the type of action is different. We will next see that this is indeed the case, and that CQDMs are much more versatile and flexible than CDs when it comes to finding orthogonal arrays.

One of the first upper bounds on the maximal number of factors in an orthogonal array was obtained by Rao [25]. The bounds for the number of factors are given implicitly and, in general, no explicit form is known. The result for $t = 2$ was already known from the work of Plackett and Burman [26].

Theorem 1.3 (***Rao's Inequalities***). *[1, Theorem 2.1] The parameters of an OA(N,k,s,t) satisfy the following inequalities:*

$$N \ge \sum_{i=0}^{u} \binom{k}{i}(s-1)^i, \quad \text{if } t = 2u,$$

$$N \ge \sum_{i=0}^{u} \binom{k}{i}(s-1)^i + \binom{k-1}{u}(s-1)^{u+1}, \quad \text{if } t = 2u+1,$$

for $u \ge 0$.

The following theorem was proven by Jungnickel in [27]:

Theorem 1.4 (*[1, Theorem 6.5]*). *If a $D(r,c,s)$ exists, then $c \le r$.*

A consequence of the previous theorem is that Rao's bound is never attained for the orthogonal arrays derived from difference schemes, because Rao's bound says that $m \le n+1$ for an OA(m,n). The situation is different for CQDMs since, for instance, the example given in the previous section shows that a CQDM$(4,3)$ exists. Thus, in a difference scheme symmetry is gained at the cost of losing factors, that is, the number of factors is less than the maximum value allowed by Rao's bound, but with a CQDM we still have a symmetry group with an action close to be regular and at the same time the number of factors appearing in Rao's bound is attained.

The following Theorem was proven, using another notation, by Ge in [28, Lemma 3.1]:

Theorem 1.5 (*[28, Lemma 3.1]*). *If n is an even number, there is no cyclic difference scheme $A = D(m,n)$ for all integer number $m \ge 3$.*

As a consequence of the theorem, no $D(3,4)$ exists. Nonetheless, the next example shows the existence of a CQDM$(5,4)$.

The array

$$\begin{pmatrix} 0,0,0,-,2 \\ 0,1,2,1,- \\ 0,2,-,0,0 \\ 0,-,1,2,1 \\ -,0,2,2,0 \end{pmatrix}$$

is a CQDM$(5,4)$.

We note that the condition that the associated orthogonal array is of index unity cannot be removed from the theorem. For instance, the orthogonal array obtained from the following difference scheme has 4 symbols, 3 factors and $\lambda = 2$, and admits the cyclic group C_4 as an automorphism group:

$$\begin{pmatrix} 0,0,0 \\ 0,0,3 \\ 0,1,2 \\ 0,1,3 \\ 0,2,1 \\ 0,2,2 \\ 0,3,0 \\ 0,3,1 \end{pmatrix}$$

The rest of the paper is organized as follows. In Section 2 we introduce some constructions of CQDMs, and in particular we provide an Integer Programming model to find CQDMs and a Bimodal Local Search algorithm that allow us to obtain certain CQDMs. Section 3 presents a conjecture on the rows-and-columns distributions of differences in diagonal-disregarded square matrices with entries in a cyclic group, and we prove it when it is a CQDM$(n+1,n)$.

2. Obtaining CQDMs

2.1. Constructions of CQDMs

First, let us prove that CQDMs with $m=3$ exist for any n. In the next two propositions we consider CQDMs in canonical form, that is, if $Q=(q_{i,j})$ is the matrix, then

$$q_{1,j}=\begin{cases}0, & \text{if } 1\le j<n+1\\ -, & \text{if } j=n+1\end{cases}$$

$$q_{2,j}=\begin{cases}j-1, & \text{if } 1\le j<n\\ -, & \text{if } j=n\\ 0, & \text{if } j=n+1\end{cases}$$

(associating, of course, the corresponding coset in the cyclic group $\mathbb{Z}/(n-1)\mathbb{Z}$ to a natural number). Thus, to obtain a $CQDM$ with $m=3$ we need to give only the values $q_{3,j}$. The proof of the following two propositions is immediate and will be omitted.

Proposition 2.1. *If n is even, then the matrix $Q=(q_{i,j})$ with*

$$q_{3,j}=\begin{cases}n-j-2, & \text{if } 1\le j\le n-2\\ -, & \text{if } j=n-1\\ n-2, & \text{if } j=n\\ 0, & \text{if } j=n+1\end{cases}$$

is a CQDM$(3,n)$.

Proposition 2.2. *If n is odd, then the matrix $Q=(q_{i,j})$ with*

$$q_{3,j}=\begin{cases}2j-2, & \text{if } 1\le j\le \frac{n-1}{2}\\ 2(j-\frac{n-1}{2})-1, & \text{if } \frac{n+1}{2}\le j\le n-2\\ -, & \text{if } j=n-1\\ n-2, & \text{if } j=n\\ \frac{n-1}{2}, & \text{if } j=n+1\end{cases}$$

is a CQDM$(3,n)$.

We will next show examples of constructions obtained with the two previous propositions:

Example. For $n=10$ we obtain from Proposition 2.1 the CQDM

$$\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&-\\0&1&2&3&4&5&6&7&8&-&0\\7&6&5&4&3&2&1&0&-&8&0\end{pmatrix},$$

and for $n=11$ we obtain from Proposition 2.2 the CQDM

$$\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0&-\\0&1&2&3&4&5&6&7&8&9&-&0\\0&2&4&6&8&1&3&5&7&-&9&5\end{pmatrix}.$$

We now show that CQDMs with parameters with the form given in the examples of the previous section can be found whenever n is a prime power:

Theorem 2.3. *If $n=p^r$ with p a prime number and $r\in\mathbb{N}$, then a CQDM$(n+1,n)$ exists.*

Proof. Let $\mathbb{F}_n$ be the Galois field of order n, and let $\mathbb{F}_n^\star$ be the set of non-zero elements of $\mathbb{F}_n$. We consider the projective plane $PG(n,2)$ whose point-set is the set X of one-dimensional subspaces of $\mathbb{F}_n^3$ and whose lines are the two-dimensional ones. For any $s\in\mathbb{F}_n^\star$ the mapping $f_s: X\longrightarrow X$ with $f_s(\langle v\rangle)=\langle sv\rangle$ is an automorphism of the plane, and the group of automorphisms $G=\{f_s | s\in\mathbb{F}_n^\star\}$ is isomorphic to the multiplicative group of the non-zero elements of $\mathbb{F}_n$, and is therefore cyclic. Now we have that, under the well-known bijection between projective planes of order n and orthogonal arrays of OA$(n+1,n)$, the OA$(n+1,n)$ associated to $PG(n,2)$ admits a group of automorphisms isomorphic to G that fixes 0 and acts regularly on the non-zero elements of $\mathbb{F}_n$. □

Note that Rao's bound is attained in the orthogonal arrays associated to the CQDMs of the previous theorem, and this is the only case in which this could happen if the Prime Power Conjecture for projective planes was true.

2.2. Integer programming for obtaining CQDMs

This section presents an Integer Programming model (1) that allows arbitrary CQDMs to be obtained, and in particular, we can consider values of n that are not prime powers.

Let us introduce the mathematical modelling whose optimal solution is an OA(m,n) with $N=n^t$ runs, m factors, n levels, strength $t=2$ and index $\lambda=1$ that can be reformulated as a CQDM(m,n). Without loss of generality, let us consider that the array contains the n^t ordered combinations in the first two columns. Now, let us define the following variables, where i denotes the run (or row), $i\in[N]$; $\sigma(i)$, the next row to ith row, related to the automorphism that fix the symbol 1 and permutes cyclically (alphabetically) the symbols $[n]\setminus\{1\}$; s, the level (or symbol), $s\in[n]$; l, the position of $(x_1,\dots,x_t)$ combination, $l\in[|S^t|]$; j, the factor (or column) and (j_1,j_2) a pair of columns, $j,j_1,j_2\in\{3,\dots,m\}: 3\le j_1<j_2\le m$:

$$x_{i,j}^s=\begin{cases}1, & \text{if row } i \text{ and column } j \text{ takes value } s\\ 0, & \text{otherwise}\end{cases}$$

$$z_{i,j_1,j_2}^l=\begin{cases}1, & \text{if row } i \text{ and column pair } (j_1,j_2)\\ & \quad\text{contains the } l\text{th combination}\\ 0, & \text{otherwise}\end{cases}$$

Then, the mathematical modelling for CQDM, with $\mathcal{O}(m^2n^4)$ variables, is as follows:

$$\sum_i x_{i,j}^s=n, \qquad \forall j,\ s \tag{1a}$$

$$\sum_s x_{i,j}^s=1, \qquad \forall i,\ j \tag{1b}$$

$$\sum_{i=(q-1)n+1}^{qn} x_{i,j}^s=1, \qquad \forall q\in[n],\ j,\ s \tag{1c}$$

$$\sum_{i:\,i\equiv q \pmod n} x_{i,j}^s=1, \qquad \forall q\in[n],\ j,\ s \tag{1d}$$

$$x_{i,j}^1=x_{\sigma(i),j}^1, \qquad \forall i,j \tag{1e}$$

$$x_{i,j}^s=x_{\sigma(i),j}^{s+1}, \qquad \forall i,j,\ \forall s\in[n]\setminus\{1,n\} \tag{1f}$$

$$x_{i,j}^n=x_{\sigma(i),j}^2, \qquad \forall i,j \tag{1g}$$

$$\sum_l l\ z_{i,j_1,j_2}^l=n\sum_s s\ x_{i,j_1}^s+\sum_s s\ x_{i,j_2}^s-n, \qquad \forall i,\ j_1,\ j_2 \tag{1h}$$

$$\sum_l z_{i,j_1,j_2}^l=1, \qquad \forall i,\ j_1,\ j_2 \tag{1i}$$

$$\sum_i z_{i,j_1,j_2}^l=1 \qquad \forall l,\ j_1,\ j_2 \tag{1j}$$

$$x_{i,j}^s,\ z_{i,j_2,j_2}^l\in\{0,1\}, \qquad \forall i,\ j,\ j_1,\ j_2,\ l,\ s. \tag{1k}$$

The constraints (1a) guarantee that each level appears once along all the runs for each column. The constraints (1b) ensure that each cell has exactly one level associated. The constraints (1c) and (1d) enforce that the pair of columns $(1, j)$ and $(2, j)$, respectively, contain all the n^t combinations. The constrains (1e)–(1g) ensure the automorphism that fix the symbol 1 and permutes cyclically (alphabetically) the symbols $[n]\setminus\{1\}$, where the symbols $\{1, 2, \dots, n\}$ can be relabelled as $\{-, 0, \dots, n-2\}$. The constraints (1h) determine that for each row, any pair of columns (j_1, j_2) corresponds to one combination from S^t. The constraints (1i) set that for each run, there is exactly one combination associated to each pair of columns (j_1, j_2). The constraints (1j) ensure that for each pair of columns (j_1, j_2), each potential combination appears exactly once. And (1k) are the integrality constraints.

Note that once we solve the Integer Programming (IP) (1), the cell (i, j) of the CQDM contains the symbol determined by the non-null variable of the vector $(x^1_{i,j}, \dots, x^m_{i,j})$, i.e., $a_{i,j} = \sum_s s\ x^s_{i,j}$. Moreover, if objective function is null, the result is a CQDM(m, n); otherwise, there is no CQDM with those parameters.

2.3. ABimodal Local Search algorithm for obtaining CQDMs

We also implemented a Bimodal Local Search algorithm to find a CQDM(m, n) for given values of m and n. We took as the search space the set X of matrices $A = (a_{i,j})$ of order $m \times (n + 1)$ with entries in $C_{n-1} \cup \{-\}$, where C_{n-1} is the cyclic group of order $n - 1$, that satisfy the following conditions:

(i) $a_{i,i} = - \ \forall i \in \{1, \dots, m\}$
(ii) $a_{ij} \in C_{n-1} \forall i \in \{1, \dots, m\}, j \in \{1, \dots, n + 1\}$ with $i \neq j$
(iii) $a_{21} = 0$
(iv) $a_{1j} = 0$ for every $j \in \{2, \dots, n + 1\}$.

We considered the following unfitness function U to minimize: If $A \in X$, then

$$U(A) = \sum_{i=1}^{m} \sum_{j=i+1}^{m} \sum_{a \in C_{n-1}} (|\{k \in \{1, \dots, n+1\}\setminus\{i, j\} \ : \ a_{jk} - a_{ik} = a\}| - 1)^2.$$

We first considered a random matrix in X and performed a first-mode local search, trying all the modifications in one of its non-fixed elements. Whenever the unfitness is strictly reduced, the candidate is replaced by the modified one. Once all the modifications have been tried and no reduction is reached, then a second-mode local search is performed, by trying all the modifications in two non-fixed elements. When a reduction in the unfitness is obtained the algorithm again enters in a first-mode local search. If no reduction happens then a new initial candidate is generated and the whole process is repeated again, until a prefixed threshold time is reached. When we obtain an unbalance of 0 then the candidate is a true CQDM(m, n) and if this happens the algorithm also ends.

After a solution was found, we converted it to canonical form.

Of course, an alternative variation of the algorithm could be to take matrices in which the first two rows are in the canonical form as candidate matrices in the search space, and where the possible positions for the — symbol and the symbols in C_{n-1} are modified during the process. We tried also this variation, but the efficiency of the algorithm was similar, and we obtained no solution for parameters not found with the algorithm in the previous form. Furthermore, the previously described form of the matrices fits better with the statement of the conjecture in the following section.

2.4. Some numerical results

We have obtained certain CQDMs with n not a prime power by using the two computational methods previously described. The Bimodal Local Search algorithm was unable to find solutions for $n > 15$ in less than 48 hours, but the Integer Programming Algorithm did succeed in that task. Nonetheless, we keep the exposition of the former one to offer a comparison between the two algorithms and also because it settles the basis in the statement of the conjecture in the next section. We next show the CQDMs obtained with the Bimodal Local Search algorithm for $n \leq 15$ and using the Integer Programming model for $n \geq 18$. The results have been obtained implementing the model (1) under IBM ILOG CPLEX v20.1 optimization software using up to 8 threads [29]. The computational experiments were conducted in the ARINA computational cluster from SGI/IZO-SGIker at UPV/EHU [30]:

For $n = 10, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & - & 0 \\ 6 & 2 & 0 & 7 & 4 & 8 & 5 & - & 1 & 3 & 5 \\ 4 & 7 & 2 & 8 & - & 3 & 5 & 1 & 0 & 6 & 2 \end{pmatrix}$$

For $n = 12, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & - & 0 \\ 3 & 10 & 6 & 9 & 1 & 4 & 8 & 7 & 2 & 5 & - & 0 & 1 \\ 9 & 6 & 5 & - & 4 & 1 & 8 & 0 & 3 & 10 & 7 & 2 & 10 \end{pmatrix}$$

For $n = 14, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & - & 0 \\ 8 & 11 & 5 & 7 & 0 & 3 & 6 & - & 10 & 2 & 9 & 12 & 4 & 1 & 7 \\ 11 & 8 & - & 9 & 6 & 2 & 7 & 10 & 4 & 0 & 5 & 3 & 12 & 1 & 12 \end{pmatrix}$$

For $n = 15, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & - & 0 \\ 11 & 3 & 0 & 8 & 12 & 5 & 10 & 6 & 1 & 4 & 2 & - & 13 & 9 & 7 & 3 \\ 2 & 1 & 13 & 11 & 7 & 6 & - & 0 & 12 & 4 & 8 & 10 & 3 & 5 & 9 & 10 \end{pmatrix}$$

For $n = 18, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & - & 0 \\ 10 & - & 8 & 0 & 7 & 13 & 1 & 16 & 2 & 5 & 11 & 9 & 12 & 15 & 4 & 14 & 3 & 6 & 5 \\ 10 & 4 & 16 & 7 & 2 & 0 & 15 & 1 & 13 & 11 & 9 & 12 & 8 & 3 & 14 & 6 & - & 5 & 6 \end{pmatrix}$$

For $n = 20, m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & - & 0 \\ 16 & 15 & 4 & 7 & 5 & 13 & 12 & 17 & 6 & - & 2 & 10 & 8 & 1 & 14 & 9 & 0 & 3 & 11 & 18 & 9 \\ 16 & 12 & 5 & 3 & 13 & 0 & 7 & 15 & 18 & 11 & - & 17 & 10 & 6 & 8 & 1 & 4 & 2 & 14 & 9 & 18 \end{pmatrix}$$

We compared the strongly regular graphs corresponding to the orthogonal arrays associated to the CQDMs obtained with the Bimodal Local Search algorithm and the Integer Programming model with the ones corresponding to the orthogonal arrays with the same parameters obtained with the 'Orthogonal arrays' package in the SageMath mathematics software system [31], and we found that they are not isomorphic. In fact, in all the cases even the automorphism groups of the graphs were not isomorphic.

If we call, given $n \geq 3$,

$$\alpha(n) = \max\{m \in \mathbb{N} | \text{ an OA}(m, n) \text{ exists}\}$$

and

$$\beta(n) = \max\{m \in \mathbb{N} | \text{ a CQDM}(m, n) \text{ exists}\},$$

then we can ask ourselves when $\alpha(n) = \beta(n)$. We deduce from Proposition 2.1, Theorem 2.3 and the CQDMs obtained with the bimodal local search algorithm that $\alpha(n) = \beta(n)$ for n up to 9. Although the value $\alpha(10)$ is not known, it is well known that $\alpha(10) \geq 4$. The CQDM$(10, 4)$ obtained in this section opens the possibility, up to the present state of knowledge about bounds of $\alpha(10)$, that $\alpha(10) = \beta(10)$. Furthermore, Theorem 2.3 shows that $\alpha(n) = \beta(n)$ when n is a prime power.

3. Row–column distributions of differences in matrices

Given a square matrix of order n with entries in the cyclic group C_n and defined except in the main diagonal, $U(A)$ will denote the unfitness function defined in the previous section.

Theorem 3.1. *If A is a cyclic quasi-difference matrix, then $U(A) = U(A^t) = 0$.*

Proof. Under the already mentioned bijection between the set of $OA(n+1, n)$ matrices and projective planes, the way of constructing the affine plane from the corresponding set of mutually orthogonal Latin squares is symmetric with respect of the operation of transposing the Latin squares. Therefore, if A is a cyclic quasi-difference matrix, we get the same projective plane when we repeat formally the construction with its transpose A^t. □

Despite the extreme plainness of the previous argumentation, it is striking that the equality $U(A) = U(A^t)$ seems to hold for arbitrary matrices in which we have no combinatorial or algebraic structure, although, of course, this common value is not yet 0.

For instance, if

$$A = \begin{pmatrix} - & 4 & 2 & 4 & 3 & 1 & 2 \\ 0 & - & 0 & 1 & 1 & 1 & 0 \\ 4 & 1 & - & 2 & 3 & 0 & 3 \\ 3 & 1 & 4 & - & 2 & 1 & 4 \\ 2 & 3 & 2 & 1 & - & 0 & 3 \\ 3 & 3 & 4 & 3 & 0 & - & 3 \\ 4 & 4 & 1 & 2 & 3 & 2 & - \end{pmatrix},$$

then the distribution of frequencies of the differences along rows for values 0, 1, 2, 3, 4 and 5 is: 31, 49, 19, 6, 0 and 0, respectively, and therefore $U(A) = 31 \cdot 1^2 + 49 \cdot 0^2 + 19 \cdot 1^2 + 6 \cdot 2^2 + 0 \cdot 3^2 + 0 \cdot 4^2 = 74$.

In a similar way, the distribution of frequencies of the differences along columns for values 0, 1, 2, 3, 4 and 5 is: 32, 46, 22, 5, 0 and 0, respectively, and $U(A^t) = 32 \cdot 1^2 + 46 \cdot 0^2 + 22 \cdot 1^2 + 5 \cdot 2^2 + 0 \cdot 3^2 + 0 \cdot 4^2 = 74$.

We conjecture that the equality $U(A) = U(A^t)$ always holds. There is very strong numeric evidence in favour of the conjecture. We have proven by performing an exhaustive numerical analysis that it is true for all matrices of orders up to 5, and we have randomly generated 10^9 matrices for each order from 6 to 15, and the conjecture held in all cases.

Interestingly, if we change the exponent 2 the result is not longer true. For instance, if we take the exponent 4 in the example given previously, then the value for the matrix A is $31 \cdot 1^4 + 49 \cdot 0^4 + 19 \cdot 1^4 + 6 \cdot 2^4 + 0 \cdot 3^4 + 0 \cdot 4^4 = 146$, and for A^t is $32 \cdot 1^4 + 46 \cdot 0^4 + 22 \cdot 1^4 + 5 \cdot 2^4 + 0 \cdot 3^4 + 0 \cdot 4^4 = 134$.

4. Conclusion

We have explored several constructions to obtain orthogonal arrays with automorphism groups fixing a symbol and acting regularly on the other symbols. Some are general constructions giving infinite families of such OAs, and others provide algorithmic approaches to obtain sporadic OAs with the prescribed symmetry corresponding to parameters that cannot be obtained with the general methods. One of the approaches is a metaheuristic algorithm based on a bi-modal local search, while the other is an integer programming approach.

Although remarkable results were obtained with both algorithms, the integer programming methodology allowed OAs to be obtained that were not obtained by the limiting time with the metaheuristic. This opens up the possibility of delving further into the research on integer programming to find orthogonal arrays with pre-established automorphism groups.

The bi-modal local search algorithm has inspired a conjecture about the distribution of differences in rows and columns of square matrices that goes beyond the kind of combinatorial structures that we have studied in this paper. Although we proven it for quasi-difference matrices, which are the object of study in this work, a vast numerical evidence seems to indicate that it is true for arbitrary matrices.

CRediT authorship contribution statement

Luis Martínez: Conceptualization, Investigation, Software, Writing – original draft. **María Merino:** Conceptualization, Investigation, Software, Writing – original draft. **Juan Manuel Montoya:** Conceptualization, Investigation, Software, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors thank IZO-SGI SGIker of UPV/EHU and European funding (ERDF and ESF) for technical and human support provided.

The authors would like to thank Josué Tonelli for helpful discussions.

Funding

Luis Martínez was supported by the UPV/EHU, Spain and Basque Center of Applied Mathematics, Spain, grant US21/27.

María Merino was supported by the Spanish Ministry of Science and Innovation through project PID2019-104933GB-I00/AEI/10.13039/501100011033 and BCAM Severo Ochoa accreditation, Spain SEV-2017-0718; and by the Basque Government, Spain through the program BERC 2022–2025 and the project IT1494-22; and by UPV/EHU, Spain through the project GIU20/054.

References

[1] Hedayat AS, Sloane NJA, Stufken John. Orthogonal arrays: Theory and applications. In: Springer series in statistics, New York: Springer-Verlag; 1999.
[2] Colbourn Charles J, Dinitz Jeffrey H, editors. Handbook of combinatorial designs, 2nd ed.. Discrete mathematics and its applications (boca raton), Chapman & Hall/CRC, Boca Raton, FL; 2007.
[3] Brouwer Andries E, Haemers Willem H. Spectra of graphs. Universitext, New York: Springer; 2012.
[4] Bose RC. On some connections between the design of experiments and information theory. Bull Inst Internat Statist 1961;38:257–71.
[5] Delsarte P. An algebraic approach to the association schemes of coding theory. Philips Res Rep Suppl 1973;(10):vi+97.
[6] Xu Ming, Tian Zihong. A flexible image cipher based on orthogonal arrays. Inform Sci 2021;551:39–53.
[7] Gopalakrishnan K, Stinson Douglas R. Applications of orthogonal arrays to computer science. In: Proc. of ICDM. Citeseer; 2006, p. 149–64.
[8] Wang Shau-Chun, Liao Hui-Ju, Lee Wan-Chia, Huang Chih-Min, Tsai Tung-Hu. Using orthogonal array to obtain gradient liquid chromatography conditions of enhanced peak intensity to determine geniposide and genipin with electrospray tandem mass spectrometry. J Chromatogr A 2008;1212(1–2):68–75.
[9] Taguchi G. System of experimental design: Engineering methods to optimize quality and minimize costs. Technical report, UNIPUB/Kraus International Publications; 1987.
[10] Goyeneche Dardo, Życzkowski Karol. Genuinely multipartite entangled states and orthogonal arrays. Phys Rev A 2014;90(2):022316.
[11] Pang Shan-Qi, Zhang Xiao, Lin Xiao, Zhang Qing-Juan. Two and three-uniform states from irredundant orthogonal arrays. Npj Quant Inf 2019;5(1):1–10.
[12] Dukanovic I, Rendl F. Semidefinite programming relaxations for graph coloring and maximal clique problems. Math Program 2007;(109):345–65.
[13] Seeger A, Torki M. Centers of sets with symmetry or cyclicity properties. TOP 2014;22:716–38.
[14] Buratti Marco. Old and new designs via difference multisets and strong difference families. J Combin Des 1999;7(6):406–25.
[15] Davis James A, Martínez Luis, Sodupe Maria José. Bi-cayley normal uniform multiplicative designs. Discrete Math 2016;339(9):2224–30.
[16] Wilson Richard M. Cyclotomy and difference families in elementary abelian groups. J Number Theory 1972;4:17–47.

[17] Kutnar Klavdija, Marušič Dragan, Miklavič Štefko, Šparl Primož. Strongly regular tri-Cayley graphs. European J Combin 2009;30(4):822–32.
[18] Leung Ka Hin, Ma Siu Lun. Partial difference triples. J Algebraic Combin 1993;2(4):397–409.
[19] Araluze Alexander, Kovács István, Kutnar Klavdija, Martínez Luis, Marušič Dragan. Partial sum quadruples and bi-Abelian digraphs. J Combin Theory Ser A 2012;119(8):1811–31.
[20] Araluze Alexander, Kutnar Klavdija, Martínez Luis, Marušič Dragan. Edge connectivity in difference graphs and some new constructions of partial sum families. European J Combin 2011;32(3):352–60.
[21] Bose RC, Bush KA. Orthogonal arrays of strength two and three. Ann Math Statist 1952;23:508–24.
[22] Abel RJR. Some $V(12,t)$ vectors and designs from difference and quasi-difference matrices. Australas J Combin 2008;40:69–85.
[23] Wang Kun, Chen Kejun. A short disproof of Euler's conjecture based on quasi-difference matrices and difference matrices. Discrete Math 2018;341(4):1114–9.
[24] Kutnar Klavdija, Malnič Aleksander, Martínez Luis, Marušič Dragan. Quasi m-Cayley strongly regular graphs. J Korean Math Soc 2013;50(6):1199–211.
[25] Radhakrishna Rao C. Factorial experiments derivable from combinatorial arrangements of arrays. Suppl J R Statist Soc 1947;9:128–39.
[26] Plackett RL, Burman JP. The design of optimum multifactorial experiments. Biometrika 1946;33:305–25.
[27] Jungnickel Dieter. On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Math Z 1979;167(1):49–60.
[28] Ge Gennian. On $(g,4;1)$-difference matrices. Discrete Math 2005;301(2–3):164–74.
[29] IBM ILOG Cplex. V12. 1: User's manual for CPLEX. Int Bus Mach Corp 2009;46(53):157.
[30] ARINA. Computational cluster from IZO-SGI, SGIker, UPV/EHU. 2021, http://www.ehu.eus/sgi/recursos/cluster-arina.
[31] The Sage Developers, Stein William, Joyner David, Kohel David, Cremona John, Eröcal Burçin. SageMath, version 9.0. 2020, http://www.sagemath.org.