This is a previous version of the article published in Journal of Combinatorial Optimization. 2018, 35(4): 1061-1085. doi:10.1007/s10878-018-0250-5

A feasibility approach for constructing combinatorial designs of circulant type

Francisco J. Aragón Artacho* Rubén Campoy† Ilias Kotsireas‡
Matthew K. Tam§

November 8, 2017

Dedicated to Jonathan M. Borwein

Abstract

In this work, we propose an optimization approach for constructing various classes of circulant combinatorial designs that can be defined in terms of autocorrelations. The problem is formulated as a so-called feasibility problem having three sets, to which the Douglas–Rachford projection algorithm is applied. The approach is illustrated on three different classes of circulant combinatorial designs: circulant weighing matrices, D-optimal matrices, and Hadamard matrices with two circulant cores. Furthermore, we explicitly construct two new circulant weighing matrices, a $CW(126, 64)$ and a $CW(198, 100)$, whose existence was previously marked as unresolved in the most recent version of Strassler's table.

Keywords. Strassler's table · circulant weighing matrices · circulant combinatorial designs · Douglas–Rachford algorithm

MSC 2010. 05B20 · 90C59 · 47J25 · 47N10

1 Introduction

The notion of *autocorrelation* associated with a finite sequence is a unifying concept that allows several classes of *combinatorial designs of circulant type* to be concisely described. Designs of this type can be represented in terms of circulant matrices formed from finite sequences whose autocorrelation coefficients satisfy certain constancy properties; such sequences are called *complementary sequences*. Examples of these designs include certain *D-optimal matrices*, *Hadamard matrices* and *circulant weighing matrices* amongst many other possibilities. A precise summary describing several of these designs, the associated sequences and their autocorrelation properties, can be found in [29, Table 1]. For an encyclopedic reference on autocorrelation properties and complementary sequences more generally, see [34, 35], and for an authoritative reference on combinatorial designs, see [16].

Many combinatorial designs can be defined as matrices of a given class which attain certain determinantal bounds. For instance, D-optimal and Hadamard matrices of a given order are

*Department of Mathematics, University of Alicante, Spain. Email: francisco.aragon@ua.es
†Department of Mathematics, University of Alicante, Spain. Email: ruben.campoy@ua.es
‡CARGO Lab, Wilfrid Laurier University, Canada. Email: ikotsire@wlu.ca
§Inst. for Num. and Appl. Math., University of Göttingen, Germany. Email: m.tam@math.uni-goettingen.de

precisely the $\{\pm 1\}$-matrices whose determinant is maximal among all other such matrices of the same order [14, 28, 37]. For this reason, combinatorial designs arise in various fields where the determinantal bounds give rise to "best possible" or "optimal" objects. Specific applications include coding theory [2, 33], quantum computing [23, 40], wireless communication, cryptography and radar [24]. In many such applications, precise knowledge of the relevant combinatorial design is required.

In order to explicitly construct combinatorial designs of non-trivial orders, it is necessary to exploit underlying structure. Some possibilities include an appropriate group theoretic structure through which the mathematical analysis can proceed, or an efficient representation which is amenable to search algorithms such as metaheuristics. In this paper, we consider a novel approach closer in spirit to the latter. More precisely, we purpose the *Douglas–Rachford algorithm (DRA)* from continuous (convex) optimization as a search heuristic. In this context, the DRA is a deterministic algorithm which traverses the combinatorial search space and which can be described in terms of a fixed-point iteration built from *nearest point projection operators*. The critical feature of the DRA, which allows for its efficient implementation in this context, is that the autocorrelation function gives rise to a projection operator which can be efficiently computed. Although we will not touch further on it here, we note that there are several other works which consider application of the DRA to combinatorial problems, both from theoretical and experimental perspectives; see [6, 7, 8, 9, 12, 21, 25].

The remainder of this paper is organized as follows. In Section 2, we recall the necessary background regarding the Douglas–Rachford algorithm as well as other key results needed in the sequel. In Section 3, we give our *feasibility problem* model for general combinatorial designs of circulant type before specializing it to *circulant weighing matrices*, *D-optimal designs of circulant-type* and *double circulant core Hadamard matrices*. Finally, in Section 4, we provide computation results to illustrate the potential of the approach. In addition, in Theorem 4.3, we provide two circulant weighing matrices, a $CW(126, 64)$ and a $CW(198, 100)$, whose existence was unresolved in the latest version of *Strassler's table* [38, Appendix A].

2 Preliminaries

2.1 The Douglas–Rachford algorithm

Let $C_1, C_2, \ldots, C_m$ be a collection of closed subsets in $\mathbb{R}^n$ with nonempty intersection. The corresponding *(m-set) feasibility problem* is

$$\text{find } x \in \bigcap_{j=1}^{m} C_j. \tag{1}$$

Any feasibility problem of the form (1) can always be reformulated using Pierra's *product-space reformulation* [31] as an equivalent two set feasibility problem in the product Hilbert space $(\mathbb{R}^n)^m := \mathbb{R}^n \times \overset{(m)}{\cdots} \times \mathbb{R}^n$. More precisely, the equivalence can be stated as

$$x \in \bigcap_{j=1}^{m} C_j \subseteq \mathbb{R}^n \iff (x, x, \ldots, x) \in C \cap D \subseteq (\mathbb{R}^n)^m := \mathbb{R}^n \times \overset{(m)}{\cdots} \times \mathbb{R}^n, \tag{2}$$

where the constraints C and D, both subsets of $(\mathbb{R}^n)^m$, are defined to be

$$\begin{aligned} C &:= \{(c_1, c_2, \ldots, c_m) : c_j \in C_j,\ j = 1, 2, \ldots, m\}, \\ D &:= \{(x, x, \ldots, x) : x \in \mathbb{R}^n\}. \end{aligned} \tag{3}$$

The *Douglas–Rachford algorithm* is an iterative method designed to solve two set feasibility problems (*i.e.,* (1) with $m = 2$) and thus the equivalence in (2) is crucial for its application to finitely many-set problems. Given two subsets A and B of a Hilbert space $\mathcal{H}$, the algorithm can be compactly described as the fixed point iteration corresponding to the set-valued operator $T_{A,B} : \mathcal{H} \rightrightarrows \mathcal{H}$ defined by

$$T_{A,B} := \frac{I + R_B R_A}{2} = I + P_B R_A - P_A,$$

where $P_A : \mathcal{H} \rightrightarrows A$ denotes the (potentially set-valued) *projector* onto A defined by

$$P_A(x) := \left\{ a \in A : \|x - a\| \leq \|x - a'\|, \forall\, a' \in A \right\},$$

and $R_A := 2P_A - I$ denotes the *reflector* with respect to A. In other words, given an initial point $x_0 \in \mathcal{H}$, the algorithm defines a sequence $(x_n)_{n=0}^{\infty}$ according to

$$x_{n+1} \in T_{A,B}(x_n) = \{x_n + b_n - a_n \in \mathcal{H} : a_n \in P_A(x_n),\, b_n \in P_B(2a_n - x_n)\}. \tag{4}$$

We remark that the set-valuedness of $T_{A,B}$ arises from the fact that nearest points to a non-convex set need not be unique. In fact, the *Motzkin–Bunt theorem* states that (in finite dimensions) the class of sets having everywhere unique nearest points are precisely those which are nonempty, closed and convex [13, Theorem 9.2.5].

In order to apply the Douglas–Rachford algorithm it is necessary to have an efficient method for computing the projectors onto the individual sets. For the product-space feasibility problem specified by (3), this is the case whenever the projectors onto the underlying constraint sets in (1) can be efficiently computed. This is summarized in the following proposition.

Proposition 2.1 (Product-space projectors [6, Proposition 3.1])**.** *Suppose that $C_1, \ldots, C_m$ are nonempty and closed subsets of $\mathbb{R}^n$. The projectors onto the sets C and D in (3) are given, respectively, by*

$$P_C((x_j)_{i=1}^m) = P_{C_1}(x_1) \times P_{C_2}(x_2) \times \cdots \times P_{C_m}(x_m) \quad \text{and} \quad P_D((x_j)_{i=1}^m) = \left(\frac{1}{m} \sum_{i=1}^m x_i \right)_{j=1}^m.$$

Having discussed implementability of the DRA, we now turn our attention to its behavior. Our first observation is the following corespondence between *fixed points* of the operator $T_{A,B}$ and points in $A \cap B$.

Fact 2.2 (Fixed points of $T_{A,B}$)**.** *Let A and B be nonempty closed subsets of $\mathcal{H}$. If $x \in \operatorname{Fix} T_{A,B} := \{x \in \mathcal{H} : x \in T_{A,B}(x)\}$, then there is a point $a \in P_A(x)$ such that $a \in A \cap B$.*

Proof. Indeed, if $x \in T_{A,B}x$ then (4) shows that there exist $a \in P_A(x)$ and $b \in P_B(2a - x)$ such that $x = x + b - a$. From the definition of the projectors onto A and B, it follows that $a = b \in P_A(x) \cap P_B(2a - x) \subseteq A \cap B$ which proves the claim. □

Consequently, if under appropriate condition, the DRA can be shown to converge to a fixed point, then it can be used to solve the feasibility problem. Unfortunately, for general combinatorial problems, there is no known unified framework which can be used to guarantee its convergence. Nevertheless, it is instructive to state the standard convergence results in the convex setting. Note that, in this case, both A and B have everywhere single-valued projectors, so the inclusions in (4) can be replaced with equality.

Fact 2.3 (Basic behavior of the Douglas–Rachford algorithm [11, Theorem 3.13])**.** *Let A and B be nonempty closed convex subsets of a finite dimensional Hilbert space $\mathcal{H}$. Let $x_0 \in \mathcal{H}$ and define the sequence $(x_n)_{n=0}^{\infty}$ according to $x_{n+1} = T_{A,B}(x_n)$ for all $n \in \mathbb{N}$. Then either*

(i) $A \cap B \neq \emptyset$ and $x_n \to x \in \operatorname{Fix} T$ with $P_A(x) \in A \cap B$, or

(ii) $A \cap B = \emptyset$ and $\|x_n\| \to +\infty$.

While Fact 2.3 clearly fails to hold when the sets A and B are combinatorial in nature (except in trivial cases), it nevertheless serves as a good template for the expected behavior of the algorithm in non-convex settings. In particular, we see that it is not the sequence $(x_n)_{n=1}^{\infty}$ itself which is of interest but rather its *shadow*; the sequence $(P_A(x_n))_{n=1}^{\infty}$. Implementation of the method is discussed in Algorithm 1. Since it is partly problem specific, we delay the discussion of the precise form of the stopping criteria used in Algorithm 1 until Section 4.

Algorithm 1: Implementation of the Douglas–Rachford algorithm.

Input: $x_0 \in \mathcal{H}$
$n = 0$;
$a_0 \in P_A(x_0)$;
while stopping criteria not satisfied **do**
  $b_n \in P_B(2a_n - x_n)$;
  $x_{n+1} = x_n + b_n - a_n$;
  $a_{n+1} \in P_A(x_{n+1})$;
  $n = n + 1$;
end
Output: $a_n \in \mathcal{H}$

2.2 Correlation and complementary

In this section we recall the definitions of the *periodic correlation operator* and *complementary sequences* before deriving a result which we use to formulate a necessary condition in the sequel. Before this, we start by recalling the *Jacobi–Trudi identity*.

Consider a vector of n variables denoted by $x = (x_1, x_2, \ldots, x_n)$. A polynomial is *symmetric* if it is invariant under every permutation of its variables. The *k-th elementary symmetric polynomial* of x, denoted σ_k, is defined by

$$\sigma_k(x) := \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} \left(\prod_{l=1}^{k} x_{j_l} \right),$$

Every symmetric polynomial can be written uniquely as a polynomial in the elementary symmetric polynomials (see [32, Theorem 1.1.1]). The *k-th power polynomial* of x, denoted p_k, is defined by

$$p_k(x) := \sum_{j=1}^{n} x_j^k. \tag{5}$$

The relationship between the latter two objects is provided by the following identity.

Fact 2.4 (Jacobi–Trudi identity [32, p. 7]). *For each $k = 1, 2, \ldots, n$, it holds that*

$$\sigma_k = \frac{1}{k!} \det \begin{pmatrix} p_1 & 1 & 0 & \ldots & 0 \\ p_2 & p_1 & 2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \ldots & p_1 & k-1 \\ p_k & p_{k-1} & \ldots & \ldots & p_1 \end{pmatrix}. \tag{6}$$

The most important case of this identity for our purposes arises when $k = 2$, in which case it yields

$$2\sigma_2 = \det \begin{pmatrix} p_1 & 1 \\ p_2 & p_1 \end{pmatrix} = p_1^2 - p_2.$$

Let $\star \colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ denote the *periodic correlation operator* whose s-th entry is defined according to

$$(a \star b)_s = \sum_{l=0}^{n-1} a_l b_{l+s}, \quad s = 0, 1, \ldots, n-1; \tag{7}$$

where $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{R}^n$ and $b = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{R}^n$ are n-dimensional real vectors, and the indices in (7) understood modulo n.

Definition 2.5 ((Real) complementary sequences). *Consider vectors $a^0, a^1, \ldots, a^{m-1} \in \mathbb{R}^n$. We say that the collection of sequences $\{a^j\}_{j=0}^{m-1}$ is* (real) complementary *if there exist some constants ν_0 and ν_1 such that*

$$\sum_{j=0}^{m-1} a^j \star a^j = (\nu_0, \nu_1, \ldots, \nu_1). \tag{8}$$

We note that the previous definition appears in [19, Definition 2] for sequences which are potentially complex-valued. Using the Jacobi–Trudi identity, we are able to deduce the following necessary condition for complementary sequences which shall be used in the next section.

Proposition 2.6 (A necessary condition for complementary sequences). *Suppose that the collection of sequences $\{a^j\}_{j=0}^{m-1} \subset \mathbb{R}^n$ is complementary with*

$$\sum_{j=0}^{m-1} a^j \star a^j = (\nu_0, \nu_1, \ldots, \nu_1),$$

for constants ν_0 and ν_1. Then $\{p_1(a^j)\}_{j=0}^{m-1} \subset \mathbb{R}$ satisfy the equation

$$\sum_{j=0}^{m-1} p_1^2(a^j) = \nu_1(n-1) + \nu_0,$$

where p_1 is given by (5).

Proof. Applying the Jacobi–Trudi identity (Fact 2.4), we deduce that

$$\sum_{s=1}^{n-1} (a^j \star a^j)_s = 2\sigma_2(a^j) = \det \begin{pmatrix} p_1(a^j) & 1 \\ p_2(a^j) & p_1(a^j) \end{pmatrix} = p_1^2(a^j) - p_2(a^j),$$

for all $j \in \{0, 1, \ldots, m-1\}$. Consequently,

$$\begin{aligned}\nu_1(n-1) &= \sum_{s=1}^{n-1}\sum_{j=0}^{m-1}(a^j \star a^j)_s = \sum_{j=0}^{m-1}\sum_{s=1}^{n-1}(a^j \star a^j)_s \\ &= \sum_{j=0}^{m-1} p_1^2(a^j) - \sum_{j=0}^{m-1} p_2(a^j) = \sum_{j=0}^{m-1} p_1^2(a^j) - \nu_0.\end{aligned}$$

The claimed result follows by a routine rearrangement, thus completing the proof. □

3 Modelling Framework

In this section we explain how to model a general combinatorial design of circulant type as a three-set feasibility problem. More precisely, we consider designs belonging to the following class.

Definition 3.1 (Design of circulant type)**.** *Consider natural numbers $n, m \in \mathbb{N}$, vectors $\alpha \in \mathbb{R}^m$ and $v \in \mathbb{R}^n$, and let $\mathcal{A} \subset \mathbb{R}$ be finite and nonempty. A* design of circulant type *of order n with parameters $(m, \alpha, v, \mathcal{A})$ is an m-tuple of vectors,*

$$(a^0, a^1, \ldots, a^{m-1}) \in (\mathcal{A}^n)^m := \mathcal{A}^n \times \overset{(m)}{\cdots} \times \mathcal{A}^n,$$

which satisfy the following two conditions:

$$\sum_{s=0}^{n-1} a_s^j = \alpha_j \quad \forall j \in \{0, 1, \ldots, m-1\}, \quad \text{and} \quad \sum_{j=0}^{m-1} a^j \star a^j = v.$$

We remark that the notation "$\mathcal{A}$" will be reserved for a finite subset of $\mathbb{R}$ which we refer to as the *alphabet*. In this work, we will be concerned with the alphabets $\{\pm 1\}$ and $\{0, \pm 1\}$.

Formulation 3.2. *Let $\mathcal{A} \subset \mathbb{R}$ be finite and nonempty, and let $\alpha \in \mathbb{R}^m$ and $v \in \mathbb{R}^n$. Consider the feasibility problem*

$$\text{find } (a^0, a^1, \ldots, a^{m-1}) \in C_1 \cap C_2 \cap C_3 \subseteq (\mathbb{R}^n)^m, \tag{9}$$

where the constraint sets are defined by

$$C_1 := \left\{(a^0, a^1, \ldots, a^{m-1}) \in (\mathbb{R}^n)^m : a^j \in \mathcal{A}^n,\, \forall j = 0, 1, \ldots, m-1\right\}, \tag{10a}$$

$$C_2 := \left\{(a^0, a^1, \ldots, a^{m-1}) \in (\mathbb{R}^n)^m : \sum_{s=0}^{n-1} a_s^j = \alpha_j, \forall j = 0, 1, \ldots, m-1\right\}, \tag{10b}$$

$$C_3 := \left\{(a^0, a^1, \ldots, a^{m-1}) \in (\mathbb{R}^n)^m : \sum_{j=0}^{m-1} a^j \star a^j = v\right\}. \tag{10c}$$

Remark 3.3 (Autocorrelation constraints in bit retrieval). In the special case that $m = 1$, the constraint C_3 appears in the formulation of the *bit retrieval* problem used in [21]. ◊

Remark 3.4 (Variants of C_1). Within our framework, the constraint set C_1 in (10a) can be easily modified so that the alphabet $\mathcal{A}$ set is different for each vector a^j or even for each individual entries of the vectors a^j. In this way, desired entries of a design can be fixed or avoided by choosing the corresponding alphabet sets to be singleton or to exclude certain values, respectively. ◊

For each set of parameters $(m, \alpha, v, \mathcal{A})$, it transpires that an m-tuple of vectors $(a^j)_{j=0}^{m-1}$ satisfies Definition 3.1 precisely when it is a feasible point for Formulation 3.2. This equivalence is justified by the following proposition.

Proposition 3.5. *Let $\mathcal{A} \subset \mathbb{R}$ be nonempty and finite. A collection of real complementary sequences $\{a^j\}_{j=0}^{m-1} \subseteq \mathcal{A}^n$ satisfies (8) with constants ν_0 and ν_1 if and only if $(a^j)_{j=0}^{m-1} \in (\mathbb{R}^n)^m$ solves (9) in Formulation 3.2 with $v = (\nu_0, \nu_1, \ldots, \nu_1)$ and some $\alpha \in \mathbb{R}^m$ which satisfies*

$$\sum_{j=0}^{m-1} \alpha_j^2 = \nu_1(n-1) + \nu_0.$$

Proof. This is an immediate consequence of Proposition 2.6. □

In order for the feasibility problem defined by Formulation 3.2 to be computationally useful, it is necessary that the projectors onto the constraint sets in (10) can be efficiently computed. In what follows, we prove that this is indeed the case.

Proposition 3.6 (Projector onto C_1)**.** *Let $(a^0, a^1, \ldots, a^{m-1}) \in (\mathbb{R}^n)^m$. Then $P_{C_1}\left((a^j)_{j=0}^{m-1}\right)$ is the set of points $(\bar{a}^j)_{j=0}^{m-1} \in (\mathbb{R}^n)^m$ which satisfy, for all $j = 0, 1, \ldots, m-1$ and $s = 0, 1, \ldots, n-1$,*

$$\bar{a}_s^j \in \left\{ l \in \mathcal{A} : \left|l - a_s^j\right| = \min_{\bar{l} \in \mathcal{A}} \left|\bar{l} - a_s^j\right| \right\}. \tag{11}$$

Proof. Let $a \in \mathbb{R}$. We observe that projector onto the set $\mathcal{A}$ is given by

$$P_{\mathcal{A}}(a) = \left\{ l \in \mathcal{A} : |l - a| = \min_{\bar{l} \in \mathcal{A}} \left|\bar{l} - a\right| \right\}.$$

Applying this result pointwise and using definition of the inner-product on $(\mathbb{R}^n)^m$, the result follows. □

Proposition 3.7 (Projector onto C_2)**.** *Let $(a^0, a^1, \ldots, a^{m-1}) \in (\mathbb{R}^n)^m$ and $e = (1, 1, \ldots, 1) \in \mathbb{R}^n$. Then*

$$P_{C_2}\left((a^j)_{j=0}^{m-1}\right) = \left(a^j + \frac{1}{n}\left(\alpha_j - \sum_{s=0}^{n-1} a_s^j\right) e\right)_{j=0}^{m-1}.$$

Proof. The projection of any point $a \in \mathbb{R}^n$ onto the hyperplane $H_j := \left\{a \in \mathbb{R}^n : e^T a = \alpha_j\right\}$ is given by (see, for instance, [10, Example 3.21])

$$P_{H_j}(a) = a + \frac{1}{\|e\|^2}\left(\alpha_j - e^T a\right) e = a + \frac{1}{n}\left(\alpha_j - \sum_{s=0}^{n-1} a_s\right) e.$$

The definition of the inner-product on $(\mathbb{R}^n)^m$ yields $P_{C_2}\left((a^j)_{j=0}^{m-1}\right) = \left(P_{H_j}(a^j)\right)_{j=0}^{m-1}$, from which the result follows. □

Thus, implementation of the projectors given in Proposition 3.6 & 3.7, requires only vector arithmetic and finding the minimum of a finite set. From a computation perspective, the latter poses no problem when the alphabet, $\mathcal{A}$, is small. We now turn our attention to describing the projector onto C_3.

Let $\mathcal{F}:\mathbb{C}^n\to\mathbb{C}^n$ denote the *(unitary) discrete Fourier transform (DFT)*, that is, the linear mapping defined for any $a\in\mathbb{C}^n$ by

$$\mathcal{F}(a):=\frac{1}{\sqrt{n}}\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \omega^{1\cdot 1} & \cdots & \omega^{1\cdot(n-1)}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \omega^{(n-1)\cdot 1} & \cdots & \omega^{(n-1)\cdot(n-1)}\end{pmatrix}a,$$

where $\omega:=e^{2\pi i/n}$ is a primitive n-th root of unity. Let $\mathcal{F}^{-1}$ denote its inverse. In the following facts, both $|\cdot|$ and $(\cdot)^2$ are understood in the pointwise sense, and $(\cdot)^*$ denotes the (complex) conjugate of a complex number.

Fact 3.8 (Properties of the DFT)**.** *Let $a=(a_0,a_1,\dots,a_{n-1})\in\mathbb{C}^n$.*

(i) (Conjugate symmetry) $a\in\mathbb{R}^n$ if and only if $\mathcal{F}(a)$ is conjugate symmetric*, that is,*

$$\mathcal{F}(a)_0\in\mathbb{R}\quad\text{and}\quad\mathcal{F}(a)_s=\left(\mathcal{F}(a)_{n-s}\right)^*,\forall s=1,2,\dots,n-1.$$

(ii) (Correlation theorem) $\mathcal{F}(a\star a)=|\mathcal{F}(a)|^2$.

(iii) $\mathcal{F}$ is a linear isometry on $\mathbb{C}^n$.

Proof. (i): See, e.g., [15, pp. 76–77]. (ii): See, e.g., [15, p. 83]. (iii): This follows from the fact that $\mathcal{F}$ is unitary. □

In the following proposition, we denote the unit sphere in $\mathbb{C}^m$ by

$$\mathbb{S}:=\left\{(z_j)_{j=0}^{m-1}\in\mathbb{C}^m:\sum_{j=0}^{m-1}|z_j|^2=1\right\},$$

and we set $Y:=\mathcal{F}(\mathbb{R}^n)^m=\mathcal{F}(\mathbb{R}^n)\times\overset{(m)}{\cdots}\times\mathcal{F}(\mathbb{R}^n)$ where, due to Fact 3.8, the set $\mathcal{F}(\mathbb{R}^n)$ is precisely the set of conjugate symmetric vectors in $\mathbb{C}^n$, i.e.,

$$\mathcal{F}(\mathbb{R}^n)=\left\{(z_s)_{s=0}^{n-1}\in\mathbb{C}^n:z_0\in\mathbb{R},\,z_s=z_{n-s}^*,\forall s=1,2,\dots,n-1\right\}.$$

Proposition 3.9 (Projector onto C_3)**.** *Let $(\hat{a}^j)_{j=0}^{m-1}\in Y$, $v\in\mathbb{R}^n$ and $\hat{v}:=\mathcal{F}(v)$. Then*

$$P_{C_3}=(\mathcal{F}^{-1},\dots,\mathcal{F}^{-1})\circ P_{\widehat{C_3}}\circ(\mathcal{F},\dots,\mathcal{F}),\tag{12}$$

where the set $\widehat{C_3}$ is given by

$$\widehat{C_3}:=\left\{(\hat{a}^j)_{j=0}^{m-1}\in Y:\sum_{j=0}^{m-1}|\hat{a}^j|^2=\hat{v}\right\}$$

and $P_{\widehat{C_3}}\left((\hat{a}^j)_{j=0}^{m-1}\right)$ is given by the set of all points $(\bar{a}^j)_{j=0}^{m-1}\in Y$ which satisfy, for all $s=0,1,\dots,n-1$:

$$\begin{cases}(\bar{a}_s^j)_{j=0}^{m-1}=\frac{\sqrt{\hat{v}_s}}{\sqrt{\sum_{j=0}^{m-1}|\hat{a}_s^j|^2}}(\hat{a}_s^j)_{j=0}^{m-1}, & \text{if } (\hat{a}_s^j)_{j=0}^{m-1}\neq 0_m,\\ (\bar{a}_s^j)_{j=0}^{m-1}\in\sqrt{\hat{v}_s}\mathbb{S}, & \text{if } (\hat{a}_s^j)_{j=0}^{m-1}=0_m.\end{cases}\tag{13}$$

Proof. We first prove the claimed formula for $P_{\widehat{C_3}}$. To this end, note that

$$\widehat{C_3} = E \cap Y \text{ where } E := \left\{ (\hat{a}^j)_{j=0}^{m-1} \in (\mathbb{C}^n)^m : \sum_{j=0}^{m-1} |\hat{a}^j|^2 = \hat{v} \right\}. \tag{14}$$

As the projector onto $\mathbb{S}$ for a point $z \in \mathbb{C}^m$ is given by

$$P_{\mathbb{S}}(z) = \begin{cases} z/\|z\|, & \text{if } z \neq 0_m, \\ \mathbb{S}, & \text{if } z = 0_m, \end{cases} \tag{15}$$

applying (15) to each m-tuple $(\hat{a}_s^j)_{j=0}^{m-1}$, we deduce that $(\bar{a}^j)_{j=0}^{m-1} \in P_E\left((\hat{a}^j)_{j=0}^{m-1}\right) \subset (\mathbb{C}^n)^m$ precisely when the vector $(\bar{a}_s^j)_{j=0}^{m-1} \in \mathbb{C}^m$ satisfies (13) for all $s = 0, \ldots, n-1$. Due to (14), any vector $(\bar{a}^j)_{j=0}^{m-1}$ which satisfies (13) and is contained in Y is an element of $P_{\widehat{C_3}}\left((\hat{a}^j)_{j=0}^{m-1}\right)$. Thus the claimed formula for $P_{\widehat{C_3}}$ follows.

Next we prove (12). We first note that since the Fourier transform, $\mathcal{F}$, is a linear isometry on $\mathbb{C}^n$ (Fact 3.8(iii)), the operator $(\mathcal{F}, \ldots, \mathcal{F})$ is a linear isometry on $(\mathbb{C}^n)^m$ with inverse given by $(\mathcal{F}, \ldots, \mathcal{F})^{-1} = (\mathcal{F}^{-1}, \ldots, \mathcal{F}^{-1})$. Thanks to [27, Lemma 3.21], we therefore have that

$$P_{C_3} = (\mathcal{F}^{-1}, \ldots, \mathcal{F}^{-1}) \circ P_{\mathcal{F}(C_3)} \circ (\mathcal{F}, \ldots, \mathcal{F}), \tag{16}$$

where $\mathcal{F}(C_3) := \left\{ \left(\mathcal{F}(a^j)\right)_{j=0}^{m-1} : (a^j)_{j=0}^{m-1} \in C_3 \right\}$. To complete the proof, it therefore suffices to show $\mathcal{F}(C_3) = \widehat{C_3}$. To this end, we observe that for a tuple $(a^j)_{j=0}^{m-1} \in (\mathbb{C}^n)^m$, we have

$$\sum_{j=0}^{m-1} a^j \star a^j = v \overset{\text{Fact 3.8(iii)}}{\iff} \sum_{j=0}^{m-1} \mathcal{F}(a^j \star a^j) = \hat{v} \overset{\text{Fact 3.8(ii)}}{\iff} \sum_{j=0}^{m-1} \left|\mathcal{F}(a^j)\right|^2 = \hat{v},$$

which shows that $\mathcal{F}(C_3) \subseteq \widehat{C_3}$. To deduce the reverse inclusion, note that $\mathcal{F}$ is invertible (Fact 3.8(iii)) and use the same argument with $(a^j)_{j=0}^{m-1} := (\mathcal{F}^{-1}(\hat{a}^j))_{j=0}^{m-1}$. □

Remark 3.10 (Equation (13)). We emphasize that it is important to note that the projector onto $\widehat{C_3}$ is given by (13) for tuples $(\bar{a}^j)_{j=0}^{m-1}$ contained in Y but not $(\mathbb{C}^n)^m$. ◊

We now provide three concrete examples of types of combinatorial designs which can be described in terms of the structure proposed in Formulation 3.2.

3.1 Circulant weighing matrices

Recall that a matrix $W \in \mathbb{R}^{n \times n}$ is said to be *circulant* if there is a vector $w \in \mathbb{R}^n$ such that the rows of W are cyclic permutations of w (offset by their row index).

Definition 3.11 (Circulant weighing matrix)**.** *Let $n, k \in \mathbb{N}$. A* circulant weighing matrix *of order n and weight k, denoted* $\mathrm{CW}(n, k^2)$*, is a circulant matrix $W \in \{0, \pm 1\}^{n \times n}$ such that*

$$WW^T = k^2 I, \tag{17}$$

where $I \in \mathbb{R}^{n \times n}$ denotes the identity matrix.

Since the matrix W is circulant, there exists a vector $a \in \{0, \pm 1\}^n$ such that $W = c(a)$ where the mapping $c : \mathbb{R}^n \to \mathbb{R}^{n \times n}$ maps a vector to an associated circulant matrix. For such a vector, the equality (17) is equivalent to

$$a \star a = (k^2, 0, 0, \ldots, 0). \tag{18}$$

Applying Proposition 3.5 (with $m = 1$), we therefore arrive at the following.

Proposition 3.12. *Let $n, k \in \mathbb{N}$. A matrix $W \in \mathbb{R}^{n\times n}$ is $CW(n, k^2)$ if and only if there exists a vector $a \in \{0, \pm 1\}^n$ with $W = c(a)$ such that*

(i) $\sum_{s=0}^{n-1} a_s = \pm k$, *and*

(ii) $a \star a = (k^2, 0, 0, \ldots, 0)$.

Example 3.13 (A CW matrix of small order). The vector $a = (-1, 1, 1, -1, 1, 0, 1, 0, 1, 1, 0, 0, -1)$ defines a $CW(13, 3^2)$. Indeed, it verifies $\sum_{s=0}^{12} a_s = 3$ and $a \star a = (9, 0, 0, 0, 0, 0, 0, 0, 0, 0)$. ♢

The class of circulant weighing matrices are of interest, in part, because they include all *circulant Hadamard matrices* (specially, a $CW(n, k^2)$ is a circulant Hadamard matrix whenever $n = k^2$ and $n = 0 \mod 4$). The existence of a CW matrices for a given order and weight is, in general, not resolved. *Strassler's table*, which originally appeared in 20 years ago in [36], gives the existence status of $CW(n, k^2)$ for $n \leq 200$ and $k \leq 10$. The table has been updated several times, but still contains open cases. The most up-to-date version known to the authors at the time of writing is contained in [38, Appendix A]. For other recent progress regarding CW matrices, see [39]. In Section 4.1 we solve two open cases by presenting two new circulant weighing matrices found with the DRA, namely, a $CW(126, 8^2)$ and a $CW(198, 10^2)$.

3.2 D-optimal designs of circulant type

Let n be an odd positive integer. Ehlich [22] showed that the determinant of a square matrix of order $2n$ having $\{\pm 1\}$ entries satisfies the bound

$$|\det(D)| \leq 2^n (2n-1)(n-1)^{n-1}.$$

Such a matrix is said to be *D-optimal* if it has maximal determinant, that is, the aforementioned determinate bound is attained.

To construct a D-optimal matrix , it suffices to find two commuting square $\{\pm 1\}$-matrices, A and B, of order n such that

$$AA^T + BB^T = (2n-2)I + 2J, \tag{19}$$

where $J \in \mathbb{R}^{n\times n}$ denotes the matrix of all ones. A D-optimal matrix D of order $2n$ can then be constructed from the matrices A and B as follows

$$D = \begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix}. \tag{20}$$

This construction, originally proposed by Ehlich [22] for the case in which A and B are circulant matrices, was later extended by Cohn [17] to the setting in which the matrices commute. The former case constitutes a special type of D-optimal designs known as *D-optimal designs of circulant type*.

Definition 3.14 (D-optimal design of circulant type)**.** *A* D-optimal design of circulant type *is a matrix D of order $2n$ given by (20) for a pair of circulant $\{\pm 1\}$-matrices A and B of order n satisfying (19). When we wish to refer to the underlying matrices A and B explicitly (rather than D), we shall say that (A, B) is a D-optimal design of circulant type.*

Let (A, B) be a D-optimal design of circulant type of order $2n$. As in the previous subsection, since both matrices A and B are circulant, there exist vectors $a, b \in \{\pm 1\}^n$ such that $A = c(a)$ and $B = c(b)$. For such vectors, (19) is equivalent to

$$a \star a + b \star b = (2n, 2, 2, \ldots, 2). \tag{21}$$

By applying Proposition 3.5 as before (now with $m = 2$), we deduce the following characterization.

Proposition 3.15. *Let n be an odd integer. A matrix D is a D-optimal design of circulant type of order $2n$ if and only if there exist constants $\alpha, \beta \in \mathbb{Z}$ with $\alpha^2 + \beta^2 = 4n - 2$ and a pair of vectors $(a, b) \in \{\pm 1\}^n \times \{\pm 1\}^n$ such that D satisfies (20) for $A = c(a)$ and $B = c(b)$, and the following assertions hold:*

(i) $\sum_{s=0}^{n-1} a_s = \alpha$,

(ii) $\sum_{s=0}^{n-1} b_s = \beta$, *and*

(iii) $a \star a + b \star b = (2n, 2, 2, \ldots, 2)$.

Example 3.16 (D-optimal design of circulant type of small order). The vectors

$$a = (-1, 1, -1, 1, 1, 1, 1, 1, -1) \quad \text{and} \quad b = (-1, 1, 1, 1, 1, -1, 1, 1, 1)$$

define a D-optimal design of order 9. Let $\alpha = 3$ and $\beta = 5$. Then we have $\alpha^2 + \beta^2 = 4n - 2$ with $\sum_{s=0}^{8} a_s = \alpha$ and $\sum_{s=0}^{8} b_s = \beta$, and that $a \star a + b \star b = (18, 2, 2, 2, 2, 2, 2, 2, 2)$. ◊

The existence of a D-optimal matrix for values $n < 100$ for which the Diophantine equation $x^2 + y^2 = 4n - 2$ has solutions has been resolved in the affirmative with the exception of $n = 99$; see [20] and [18, Table 1]. In other words, the first unresolved case of existence arises when $n = 99$.

3.3 Double circulant core Hadamard matrices

Let n be an odd positive integer. Recall that a *Hadamard matrix* of order n is a matrix $H \in \{\pm 1\}^{n \times n}$ such that

$$HH^T = H^T H = nI.$$

There are many equivalent characterization of Hadamard matrices. For instance, they are precisely the $\{\pm 1\}$-matrices of maximal determinant [28, Chapter 2].

Definition 3.17 (Double circulant core Hadamard matrix)**.** *Let $n \in \mathbb{N}$. A Hadamard matrix, H, of order $2n + 2$ is said to be a* Hadamard matrix with two circulant cores *if it is of either one of the following two forms*

$$\left(\begin{array}{cc|ccc} - & - & + & \cdots & + \\ - & + & + & \cdots & - \\ \hline + & + & & & \\ \vdots & \vdots & & A & \\ + & + & & & \\ \hline + & - & & & \\ \vdots & \vdots & & B^T & \\ + & - & & & \end{array}\right.\left.\begin{array}{ccc} + & \cdots & + \\ - & \cdots & - \\ \hline & & \\ & B & \\ & & \\ \hline & & \\ & -A^T & \\ & & \end{array}\right), \qquad \left(\begin{array}{cc|ccc} + & + & & & \\ \vdots & \vdots & & A & \\ + & + & & & \\ \hline + & - & & & \\ \vdots & \vdots & & B^T & \\ + & - & & & \\ \hline - & - & + & \cdots & + \\ - & + & + & \cdots & - \end{array}\right.\left.\begin{array}{ccc} & & \\ & B & \\ & & \\ \hline & & \\ & -A^T & \\ & & \\ \hline + & \cdots & + \\ - & \cdots & - \end{array}\right), \tag{22}$$

where A and B are circulant matrices of order n, and $+$ and $-$ are shorthand for $+1$ and -1, respectively.

We note that the two Hadamard matrices in (22) are *equivalent* in the sense that one can be obtained from the other via sequence of row/column negations and row/column permutation [30, §2.1].

Two circulant matrices A and B satisfy Definition 3.17 precisely when [30, p. 3]

$$AA^T + BB^T = (2n + 2)I - 2J. \tag{23}$$

Denote $A = c(a)$ and $B = c(b)$ for vectors $a, b \in \{\pm 1\}^n$. It follows that (23) is equivalent to

$$a \star a + b \star b = (2n, -2, -2, \ldots, -2). \tag{24}$$

Applying Proposition 3.5 as before, we deduce the following characterization.

Proposition 3.18 (Double circulant core Hadamard matrix)**.** *A pair of matrices A and B satisfy (23) and, consequently define a Hadamard matrix with two circulant cores, if and only if there exists vectors $a, b \in \{\pm 1\}^n$ such that $A = c(a), B = c(b)$ with*

(i) $\sum_{s=0}^{n-1} a_s = \pm 1$

(ii) $\sum_{s=0}^{n-1} b_s = \pm 1$, *and*

(iii) $a \star a + b \star b = (2n, -2, -2, \ldots, -2)$.

Proof. We note that as a direct consequence of Proposition 3.5, one has

$$\alpha_1^2 + \alpha_2^2 = \left(\sum_{s=0}^{n-1} a_s\right)^2 + \left(\sum_{s=0}^{n-1} b_s\right)^2 = 2,$$

from which (i)-(ii) follows. Condition (iii) is the same as (24) whose equivalence was already discussed before the statement of the proposition. □

Example 3.19. The vectors $a = (1, -1, -1, 1, -1, 1, 1, 1, -1)$ and $b = (-1, -1, 1, 1, -1, 1, 1, 1, -1)$ define a double core circulant Hadamard matrix design. Note that

$$\sum_{s=0}^{8} a_s = 1, \qquad \sum_{s=0}^{8} b_s = 1,$$

and $a \star a + b \star b = (18, -2, -2, -2, -2, -2, -2, -2, -2)$. ◊

4 Computational Results

In this section, we report the results of numerical experiments which demonstrate the performance of DR feasibility formulation (DRA). In Section 4.1, the formulation is used to construct two circulant weighing matrices, namely, a $CW(126, 8^2)$ and a $CW(198, 10^2)$. Until this work, the existence of these matrices was an open question. We implement the DRA, described in Algorithm 1, in *Python 2.7* with the stopping criteria outlined in the following remark.

Remark 4.1 (stopping criteria). Let $C := C_1 \times C_2 \times C_3$ and D denote the product space sets in (3) and let $\epsilon > 0$ denote a small real number. Further, let (x_n) denote a sequence generated by the DRA operator $T_{D,C}$. Denoting $p_n = (q_n, q_n, q_n) := P_D(x_n)$, we terminate the DRA when either a prespecified time limit is reached or the following condition is satisfied:

$$\|(P_{C_1}, P_{C_1}, P_{C_1})(p_n) - P_C(p_n)\| < \epsilon,$$

where we note that $P_C = (P_{C_1}, P_{C_2}, P_{C_3})$. Notice that, if this condition is satisfied and $\epsilon \approx 0$, then

$$(P_{C_1}, P_{C_1}, P_{C_1})(p_n) \approx (P_{C_1}, P_{C_2}, P_{C_3})(p_n).$$

In other words, we have $P_{C_1}(q_n) \approx P_{C_2}(q_n) \approx P_{C_3}(q_n)$, which implies $P_D(P_C(p_n)) \approx P_C(p_n)$. ◊

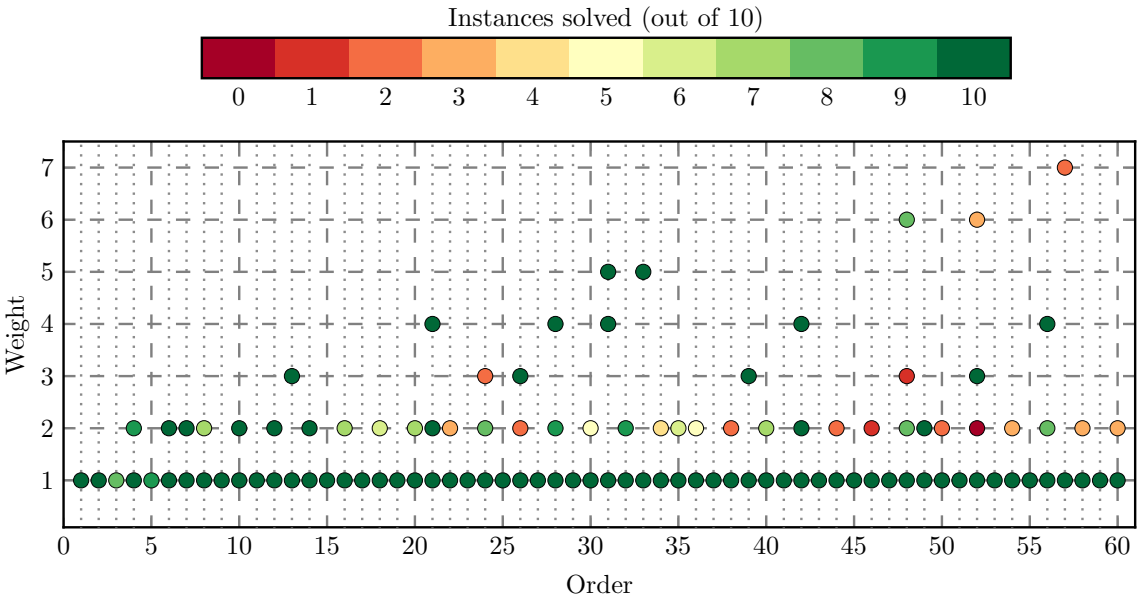

Figure 1: Results for CW matrices (10 random initialization, 3600s time limit).

Once the stopping criteria in Remark 4.1 is satisfied, the resulting solution can be directly checked to see whether is conforms to Definition 3.1. Thus, whilst there may not be theory to guarantee that the DRA will convergence given enough time, if it does converge, then the question of whether or not the output is a circulant design can be easily answered.

Computational results for CW matrices are summarized in Figure 1 and detailed computational results are included in Appendix A. Results for D-optimal designs of circulant-type and Hadamard matrices with two circulant cores, respectively, can be found in Table 1 and Table 2.

4.1 New circulant weighing matrices

In this section, we state and prove our main result regarding the existence of two circulant weighing matrices. Our approach makes use of the following construction which is a consequence of [4, Theorem 2.3]. Since this result appears without a proof in [5, Section 2], we show next how to derive it and give an explicit expression of the components of the constructed matrix in terms of the components of the original matrices.

Theorem 4.2. *Let $n, k \in \mathbb{N}$ with n odd. Let A and B be two $CW(n, k^2)$ whose respective first rows, a and b, have disjoint support*[1]*. Then the circulant matrix $c(w)$ is a $CW(2n, 4k^2)$ where the vector $w = (w_0, w_1, w_2, \ldots, w_{2n-1}) \in \mathbb{R}^{2n}$ is given component-wise by*

$$w_s := \begin{cases} a_{\frac{s}{2}} + b_{\frac{s}{2}}, & \text{if } s \text{ is even,} \\ a_{\frac{s+n}{2}} - b_{\frac{s+n}{2}}, & \text{if } s \text{ is odd and } s \leq n-2, \\ a_{\frac{s-n}{2}} - b_{\frac{s-n}{2}}, & \text{if } s \text{ is odd and } s > n-2. \end{cases} \tag{25}$$

Proof. Let $G = \langle x \rangle = \{1, x, \ldots, x^{2n-1}\}$ be a cyclic group of order $2n$ generated by x, where $x^{2n} = 1$. Clearly, the element x^n of the group G has order 2.

[1]The *support* of $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{R}^n$ is the set $\{i \in \{0, \ldots, n-1\} : c_i \neq 0\}$.

Table 1: Experimental results for D-optimal designs (10 random initialization, 3600s time limit).

Parameters	Solved instances	Average time (s)	Average iterations
(3,1,3)	10	0.00	3.4
(5,3,3)	10	0.00	6.6
(7,1,5)	9	0.01	12.7
(9,3,5)	10	0.19	398.3
(13,1,7)	7	0.13	349.7
(13,5,5)	7	0.16	403.6
(15,3,7)	10	0.24	591.8
(19,5,7)	10	0.81	1999.1
(21,1,9)	8	1.36	3424.9
(23,3,9)	8	2.02	5097.1
(25,7,7)	10	4.64	11 668.6
(27,5,9)	9	116.50	297 617.0
(31,1,11)	10	187.63	460 501.0
(33,3,11)	8	553.44	1 380 160.0
(33,7,9)	8	810.97	2 025 880.0
(37,5,11)	3	1885.47	4 399 507.0
(41,9,9)	1	586.87	1 352 777.0
(43,1,13)	0	–	–
(43,7,11)	1	1207.20	2 737 865.0

Table 2: Experimental results for DHCM designs (10 random initialization, 3600s time limit).

Parameters	Solved instances	Average time (s)	Average iterations
(1,1,1)	10	0.00	1.7
(3,1,1)	10	0.01	33.6
(5,1,1)	10	0.00	5.9
(7,1,1)	8	0.01	35.8
(9,1,1)	10	0.01	35.2
(11,1,1)	10	0.04	89.2
(13,1,1)	9	0.10	222.2
(15,1,1)	10	0.10	241.8
(17,1,1)	10	0.22	549.3
(19,1,1)	10	1.68	4162.5
(21,1,1)	10	1.97	4764.0
(23,1,1)	10	2.26	5533.2
(25,1,1)	9	16.08	40 468.1
(27,1,1)	10	76.10	192 706.0
(29,1,1)	10	91.82	223 875.0
(31,1,1)	10	428.61	1 028 850.0
(33,1,1)	10	849.84	2 070 120.0
(35,1,1)	4	2354.52	5 864 880.0
(37,1,1)	2	1883.67	4 603 068.0
(39,1,1)	1	2536.40	5 916 197.0

Let $a, b \in \mathbb{R}^n$ denote the first rows of A and B, respectively, and consider the generating functions given by

$$\mathbf{A}(x) := \sum_{s=0}^{n-1} a_s x^s \quad \text{and} \quad \mathbf{B}(x) := \sum_{s=0}^{n-1} b_s x^s.$$

Then $\mathbf{A}(x^2), \mathbf{B}(x^2) \in \mathbb{Z}[G]$ where $\mathbb{Z}[G]$ denotes the group ring of G over $\mathbb{Z}$. Let $\widehat{a}, \widehat{b} \in \mathbb{R}^{2n}$ denote the vectors associated with $\mathbf{A}(x^2)$ and $\mathbf{B}(x^2)$, respectively; that is,

$$\widehat{a} := (a_0, 0, a_1, 0, \ldots, a_{n-1}, 0) \quad \text{and} \quad \widehat{b} := (b_0, 0, b_1, 0, \ldots, b_{n-1}, 0). \tag{26}$$

Since A and B are $CW(n, k^2)$, a direct verification using Proposition 3.12 shows that the circulant matrices defined by $\widehat{a}$ and $\widehat{b}$, namely $\widehat{A} := c(\widehat{a})$ and $\widehat{B} := c(\widehat{b})$, are $CW(2n, k^2)$.

Let $\widetilde{a}, \widetilde{b} \in \mathbb{R}^n$ be the vectors associated with the formal sums $x^n\mathbf{A}(x^2)$ and $x^n\mathbf{B}(x^2)$, respectively. Since

$$x^n\mathbf{A}(x^2) = \sum_{s=0}^{n-1} a_s x^{2s+n} = \sum_{s=0}^{\frac{n-1}{2}} a_s x^{2s+n} + \sum_{s=\frac{n+1}{2}}^{n-1} a_s x^{2s-n},$$

it follows that

$$\widetilde{a} = \left(0, a_{\frac{n+1}{2}}, 0, a_{\frac{n+3}{2}}, 0, \ldots, a_{n-1}, 0, a_0, 0, a_1, 0, \ldots, 0, a_{\frac{n-1}{2}}\right). \tag{27}$$

The analogous expression holds for $\widetilde{b}$.

Consider now the circulant matrices $\widetilde{A} = c(\widetilde{a})$ and $\widetilde{B} = c(\widetilde{b})$ associated with the formal sums $x^n\mathbf{A}(x^2)$ and $x^n\mathbf{B}(x^2)$, respectively. Since a and b have disjoint support and n is odd, one can easily check that $\widehat{a}, \widetilde{a}, \widehat{b}, \widetilde{b}$ have pairwise disjoint support. Therefore, all the assumptions of [4, Theorem 2.3] hold, and we deduce that the vector $w \in \mathbb{R}^{2n}$ associated with the formal sum $\mathbf{W}(x)$ given by

$$\mathbf{W}(x) := (1 + x^n)\mathbf{A}(x^2) + (1 - x^n)\mathbf{B}(x^2) \in \mathbb{Z}[G]$$

is such that the circulant matrix $c(w)$ is $CW(2n, 4k^2)$.

To conclude the proof, we just need to check that the components of w are given by (25). Indeed, since

$$w = \widehat{a} + \widetilde{a} + \widehat{b} - \widetilde{b},$$

the expression given by (25) follows from (26) and (27). □

Theorem 4.3. *Both $CW(126, 8^2)$ and $CW(198, 10^2)$ exist.*

Proof. Using the DRA, the following $CW(63, 4^2)$ was found

```
a = [ 1,-1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0,-1, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1,-1, 0, 0, 1, 0,
      0, 0,-1, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1].
```

It has disjoint support with its cyclic permutation, b, given by

```
b = [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1,-1, 0, 0, 0, 0, 0, 1, 1, 0, 1,
      0,-1, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1,-1, 0, 0, 1, 0, 0, 0,-1, 0, 0, 0, 0, 0,-1, 0].
```

The construction in Theorem 4.2 applied to a and b yields

```
w = [ 1, 0,-1, 1, 0,-1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1,-1, 0, 0, 1, 0, 1, 0,-1, 0, 0,-1, 0, 0,-1,-1,
      1, 1, 0, 0, 0, 0, 0,-1, 1, 0, 1, 1,-1, 0, 0, 1, 1, 0, 0, 0, 1, 1,-1, 0, 1, 0, 1, 1, 1, 1, 1, 1,
      0,-1,-1, 0,-1, 0, 0, 0,-1, 0, 0, 0, 0, 1, 0, 1,-1, 0, 0, 1, 0,-1, 0,-1, 0, 0, 1, 0, 0,-1, 1,-1,
     -1, 0, 0, 0, 0, 0, 1,-1, 0,-1, 1, 1, 0, 0,-1, 1, 0, 0, 0, 1, 1,-1, 0,-1, 0,-1,-1, 1, 1,-1],
```

and, consequently, the vector w defines a $CW(126, 8^2)$.

Similarly, using the DRA, the following $CW(99, 5^2)$ was found

```
a = [-1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0,-1, 0, 0, 1, 0, 0, 0, 0, 0,-1, 0, 0, 1, 0, 0, 1, 0, 0,
     -1, 0, 0,-1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,-1, 0, 0,
      1, 0, 0,-1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0,-1, 0, 0]
```

It has disjoint support with its cyclic permutation, b, given by

```
b = [ 0,-1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0,-1, 0, 0, 1, 0, 0, 0, 0, 0,-1, 0, 0, 1, 0, 0, 1, 0,
      0,-1, 0, 0,-1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,-1, 0,
      0, 1, 0, 0,-1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0,-1, 0].
```

The construction in Theorem 4.2 applied to a and b yields

```
w = [-1, 0,-1, 1, 0,-1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0,-1, 1, 0, 1, 1, 0,-1, 0, 0, 0,-1, 0, 1,-1, 0,
     -1, 1, 0,-1, 1, 0, 1,-1, 0, 1, 0, 0, 0, 1, 0,-1,-1, 0,-1, 0, 0, 0, 1, 0, 1, 1, 0,-1, 1, 0, 1,-1,
      0, 1,-1, 0,-1, 0, 0, 0,-1, 0,-1, 0, 0, 0, 0, 0, 0,-1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1,-1, 0, 1,
      1, 0, 1,-1, 0, 1, 1, 0, 1, 1, 0,-1, 0, 0, 0, 1, 0,-1, 1, 0, 1, 1, 0,-1, 1, 0, 1, 0, 0, 0,-1, 0,
     -1,-1, 0, 1, 1, 0, 1, 1, 0,-1,-1, 0,-1, 0, 0, 0, 1, 0, 1,-1, 0, 1, 0, 0, 0, 1, 0,-1, 1, 0, 1, 1,
      0,-1,-1, 0,-1,-1, 0, 1, 0, 0, 0,-1, 0, 1, 0, 0, 0, 0, 0, 0,-1, 0,-1, 1, 0,-1, 0, 0, 0, 1, 0,-1,
     -1, 0,-1, 1, 0,-1],
```

and, consequently, the vector w defines a $CW(198, 10^2)$. □

Remark 4.4. Theorem 4.3 resolves two open cases in the latest update of Strassler's Table appearing in the 2016 work of Tan [38, Appendix A]. We also note that a previous version of Strassler's Table published in 2010 by Arasu & Gutman [3, Table 3] also listed these two cases as open. Despite the fact that these two cases have remained unresolved in multiple updates of Strassler's table, during the preparing of this manuscript (after independently proving Theorem 4.3) we discovered that existence can actually be deduced by combining either of the aforementioned versions of Strassler's table with a much older result of Arasu & Dillon [1, Theorem 2.2] which appeared in 1999. Specifically, the existence of $CW(126, 8^2)$ and $CW(198, 10^2)$ follows by respectively applying this result to $CW(21, 4^2)$ and $CW(33, 5^2)$, with $m = 3$. In fact, the existence of $CW(198, 10^2)$ was already claimed in [1]. This seems to have been missed until now. ♢

Remark 4.5. Although Strassler's original table [36] correctly states that $CW(196, 4^2)$ exist, in both of updates, [38, Appendix A] and [3, Table 3], its status is incorrectly shown as not existing. The same error appears in [26, §5] and [39, p. 144]. Indeed, we obtained the following $CW(28, 4^2)$ with the DRA

```
a = [1, 0, 1, -1, -1, 1, 0, 1, -1, 0, 0, 1, 0, 0, -1, 0, -1, -1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0],
```

from which a $CW(196, 4^2)$ can be deduced by appending 0_6 after each component

```
w = [ 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0,
      0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0,-1, 0, 0, 0, 0, 0, 0, 0, 1, 0,
      0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0],
```

since $196 = 28 \cdot 7$. ♢

Acknowledgments. This work is dedicated to the late Jonathan M. Borwein who suggested this project during his 2016 sabbatical in Canada. FJAA and RC were partially supported by MINECO of Spain and ERDF of EU, grant MTM2014-59179-C2-1-P. FJAA was supported by the Ramón y Cajal program by MINECO of Spain and ERDF of EU (RYC-2013-13327) and RC was supported by MINECO of Spain and ESF of EU (BES-2015-073360) under the program "Ayudas para contratos predoctorales para la formación de doctores 2015". IK is supported by an NSERC grant. MKT was supported by Deutsche Forschungsgemeinschaft RTG2088 and by a Postdoctoral Fellowship from the Alexander von Humboldt Foundation.

References

[1] K.T. Arasu and J.F. Dillon: Perfect ternary arrays, In: A. Pott , P.V. Kumar, T. Helleseth, D. Jungnickel (eds), Difference Sets, Sequences and their Correlation Properties, p. 1–15, 1999.

[2] K.T. Arasu and T.A. Gulliver: Self-dual codes over $\mathbb{F}_p$ and weighing matrices, *IEEE Trans. Inform. Theory* 47(5):2051–2055, 2001.

[3] K.T. Arasu and A.J. Gutman: Circulant weighing matrices, *Cryptogr. Commun.* 2:155–171, 2010.

[4] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, and D.K. Ray-Chaudhuri: Circulant weighing matrices of weight 2^{2t}, *Des. Codes Cryptogr.*, 41(1):111–123, 2006.

[5] K.T. Arasu, I.S. Kotsireas, C. Koukouvinos, and J. Seberry: On circulant and two-circulant weighing matrices, *Australasian Journal of Combinatorics*, 48:43–51, 2010.

[6] F.J. Aragón Artacho, J.M. Borwein and M.K. Tam: Recent results on Douglas–Rachford methods for combinatorial optimization problems, *Journal of Optimization Theory and Applications*, 163(1):1–30, 2014.

[7] F.J. Aragón Artacho, J.M. Borwein and M.K. Tam: Douglas–Rachford feasibility methods for matrix completion problems, *The ANZIAM Journal*, 55(4):299–326, 2014.

[8] F.J. Aragón Artacho, J.M. Borwein and M.K. Tam: Global behavior of the Douglas–Rachford method for a nonconvex feasibility problem, *Journal of Global Optimization*, 65(2):309–327, 2016.

[9] F.J. Aragón Artacho and R. Campoy: Solving graph coloring problems with the Douglas–Rachford algorithm, *Set-Valued Var. Anal.* (accepted for publication in November, 2017). DOI: 10.1007/s11228-017-0461-4

[10] H.H. Bauschke and P.L. Combettes: *Convex Analysis and Monotone Operator Theory in Hilbert Spaces*, Springer, New York, NY, 2011.

[11] H.H. Bauschke, P.L. Combettes and D.R. Luke.: Finding best approximation pairs relative to two closed convex sets in Hilbert space, *J. Approx. Theory* 127(2):178–192, 2004.

[12] H.H. Bauschke and M.N. Dao: On the finite convergence of the Douglas–Rachford algorithm for solving (not necessarily convex) feasibility problems in Euclidean spaces, *SIAM Journal on Optimization* 27:207–537, 2017.

[13] J.M. Borwein and A.S. Lewis: *Convex Analysis and Nonlinear Optimization*, Springer Science+Business Media, Inc., 2006.

[14] R.P. Brent: Finding D-optimal design by randomised decomposition and switching, *Australiasian Journal of Combinatorics*, 55:15–30, 2013.

[15] W.L. Briggs and V.E. Henson: *The DFT. An owner's manual for the discrete Fourier transform*, SIAM, Philadelphia, PA, 1995.

[16] C.J. Colbourn and J.H. Dinitz (Eds): *Handbook of combinatorial designs (2nd ed)*, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[17] J.H.E. Cohn: On determinants with elements ±1. II. *Bull. London Math. Soc.*, 21(1): 36–42, 1989.

[18] D.Ž. Đoković and I.S. Kotsireas: New results on D-pptimal matrices, *Journal of Combinatorial Designs*, 20(6):278–289, 2012.

[19] D.Ž. Đoković and I.S. Kotsireas: Compression of periodic complementary sequences and applications, *Designs, Codes and Cryptography*, 74(2):365–377, 2015.

[20] D.Ž. Đoković and I.S. Kotsireas: D-Optimal Matrices of Orders 118, 138, 150, 154 and 174, *Algebraic design theory and Hadamard matrices*, 71–82, Springer Proc. Math. Stat., 133, Springer, Cham, 2015.

[21] V. Elser, I. Rankenburg and P. Thibault: Searching with iterated maps, *Proceedings of the National Academy of Sciences*, 104(2):418–426, 2007.

[22] H. Ehlich: Determinantenabschätzungen für binäre Matrizen, *Math. Zeitschr.*, 83: 123–132, 1964.

[23] S.T. Flammia and S. Severini: Weighing matrices and optical quantum computing, *J. Phys. A*, 42(6):065302, 2009.

[24] S.W. Golomb and G. Gong: *Signal design for good correlation*, Cambridge University Press New York, 2004.

[25] S. Gravel and V. Elser: Divide and concur: A general approach to constraint satisfaction, *Physical Review E*, 78(3):036706, 2008.

[26] A.J. Gutman: Circulant weighing matrices, Master's Thesis, Wright State University, 2009. http://rave.ohiolink.edu/etdc/view?acc_num=wright1244468669

[27] R. Hesse: *Fixed point algorithms for nonconvex feasibility with applications*, PhD thesis, University of Göttingen, 2014.

[28] K.J. Horadam: *Hadamard matrices and their applications*, Princeton University Press, 2012.

[29] I.S. Kotsireas: *Algorithms and metaheuristics for combinatorial matrices*. In: P.M. Pardalos, D.-Z. Du, and R.L. Graham (eds), Handbook of Combinatorial Optimization, p. 283–309, Springer, 2013.

[30] I.S. Kotsireas, C. Koukouvinos and J. Seberry: Hadamard ideals and Hadamard matrices with two circulant cores. *European Journal of Combinatorics*, 27(5):658–668, 2006.

[31] G. Pierra: Decomposition through formalization in a product space. *Math. Program.*, 28: 96–115, 1984.

[32] B. Sturmfels: *Algorithms in Invariant Theory*, Springer Vienna, 2008.

[33] M. Sala, S. Sakata, T. Mora, C. Traverso and L. Perret (Eds): *Gröbner Bases, Coding, and Cryptography*, Springer Berlin Heidelberg, 2009.

[34] J.R. Seberry: *Orthogonal designs: Hadamard Matrices, Quadratic Forms and Algebras*, in press, 2017.

[35] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, *Contemporary design theory: a collection of surveys* pp. 431-560, 1992.

[36] Y. Strassler, The Classification of Circulant Weighing Matrices of Weight 9, Ph.D. Thesis, Bar-Ilan University, Israel, 1997.

[37] D.R. Stinson: *Combinatorial designs*, Springer-Verlag New York, 2004.

[38] M.M. Tan: Group Invariant Weighing Matrices, arXiv:1610.01914 (2016).

[39] M.M. Tan: Relative difference sets and circulant weighing matrices, PhD Thesis, Nanyang Technological University, 2014. https://repository.ntu.edu.sg/handle/10356/62325

[40] W. van Dam: Quantum Algorithms for Weighing Matrices and Quadratic Residues, *Algorithmica*, 34(4):413–428, 2002.

A Detailed results for CW matrices

Table 3: Results for CW matrices (10 random initialization, 3600s time limit).

(n,k)	No. Solved	Av. time (s)	Av. iterations
(1,1)	10	0.00	1.5
(2,1)	10	0.00	1.4
(3,1)	8	0.00	3.1
(4,1)	10	0.00	5.6
(5,1)	9	0.00	4.0
(6,1)	10	0.00	4.1
(7,1)	10	0.00	3.3
(8,1)	10	0.00	3.5
(9,1)	10	0.00	4.0
(10,1)	10	0.00	4.5
(11,1)	10	0.00	4.0
(12,1)	10	0.00	3.8
(13,1)	10	0.00	4.7
(14,1)	10	0.00	3.8
(15,1)	10	0.00	5.7
(16,1)	10	0.00	6.0
(17,1)	10	0.00	5.7
(18,1)	10	0.00	4.6
(19,1)	10	0.00	7.0
(20,1)	10	0.00	6.2
(21,1)	10	0.00	6.3
(22,1)	10	0.00	8.2
(23,1)	10	0.00	6.9
(24,1)	10	0.00	6.2
(25,1)	10	0.00	4.8
(26,1)	10	0.00	5.2
(27,1)	10	0.00	6.1
(28,1)	10	0.00	6.7
(29,1)	10	0.00	8.7
(30,1)	10	0.00	7.9
(4,2)	9	0.00	5.1
(6,2)	10	0.00	8.1
(7,2)	10	0.09	328.9
(8,2)	7	0.02	81.4
(10,2)	10	0.04	180.5
(12,2)	10	0.05	211.7
(14,2)	10	0.16	649.2
(16,2)	7	0.09	373.0
(18,2)	6	0.03	110.5
(20,2)	7	0.30	1213.9
(21,2)	10	0.32	1165.9
(22,2)	3	0.02	67.7
(24,2)	8	0.13	506.5
(26,2)	2	0.03	101.0
(28,2)	9	0.19	703.3
(30,2)	5	0.07	232.6
(13,3)	10	0.05	172.0
(24,3)	2	10.93	42 967.5
(26,3)	10	1.89	7162.3
(21,4)	10	11.47	45 012.3
(28,4)	10	15.89	60 377.3
(31,1)	10	0.00	9.0
(32,1)	10	0.00	9.8
(33,1)	10	0.00	9.4
(34,1)	10	0.00	9.7
(35,1)	10	0.00	8.5
(36,1)	10	0.00	8.3
(37,1)	10	0.00	11.7
(38,1)	10	0.00	6.2
(39,1)	10	0.00	9.9
(40,1)	10	0.00	10.5
(41,1)	10	0.00	11.8
(42,1)	10	0.00	11.8
(43,1)	10	0.00	9.1
(44,1)	10	0.00	8.7
(45,1)	10	0.00	9.7
(46,1)	10	0.00	14.5
(47,1)	10	0.00	9.3
(48,1)	10	0.00	10.9
(49,1)	10	0.00	11.9
(50,1)	10	0.00	13.4
(51,1)	10	0.00	11.7
(52,1)	10	0.00	16.3
(53,1)	10	0.01	17.8
(54,1)	10	0.00	16.2
(55,1)	10	0.00	14.7
(56,1)	10	0.00	10.4
(57,1)	10	0.00	15.9
(58,1)	10	0.00	11.6
(59,1)	10	0.00	12.4
(60,1)	10	0.00	16.1
(32,2)	9	0.25	984.3
(34,2)	4	0.06	211.8
(35,2)	6	0.14	516.3
(36,2)	5	0.09	359.4
(38,2)	2	0.11	398.0
(40,2)	7	0.34	1287.3
(42,2)	10	0.60	2265.0
(44,2)	2	0.06	241.0
(46,2)	1	0.02	65.0
(48,2)	8	0.21	798.0
(49,2)	10	1.36	5031.0
(50,2)	2	0.05	201.5
(52,2)	0	-	-
(54,2)	3	0.14	491.7
(56,2)	8	0.29	1098.4
(58,2)	3	0.01	44.3
(60,2)	3	0.28	1082.0
(39,3)	10	5.72	22 158.7
(48,3)	1	13.29	52 189.0
(52,3)	10	3.92	14 888.2
(31,4)	10	422.45	1 652 410.0
(42,4)	10	132.12	504 622.0
(56,4)	10	59.63	225 106.0
(31,5)	10	23.10	90 731.5
(33,5)	10	334.83	1 306 620.0
(48,6)	8	607.04	2 365 024.0
(52,6)	3	2314.49	8 309 650.0
(57,7)	2	482.54	1 812 060.0