Des. Codes Cryptogr. (2015) 76:551–569
DOI 10.1007/s10623-014-9977-x

Diagonally cyclic equitable rectangles

Anthony B. Evans · David Fear · Rebecca J. Stones

Received: 4 May 2013 / Revised: 6 May 2014 / Accepted: 9 May 2014 /
Published online: 1 June 2014

Abstract An equitable $(r, c; v)$-rectangle is an $r \times c$ matrix $L = (l_{ij})$ with symbols from $\mathbb{Z}_v$ in which each symbol appears in every row either $\lceil c/v \rceil$ or $\lfloor c/v \rfloor$ times and in every column either $\lceil r/v \rceil$ or $\lfloor r/v \rfloor$ times. We call L diagonally cyclic if $l_{(i+1)(j+1)} = l_{ij} + 1$, where the rows are indexed by $\mathbb{Z}_r$ and columns indexed by $\mathbb{Z}_c$. We give a constructive proof of necessary and sufficient conditions for the existence of a diagonally cyclic equitable $(r, c; v)$-rectangle.

Keywords Equitable rectangle · Latin square · Latin rectangle · Orthogonal array

Mathematical Subclass Classification 05B15

1 Introduction

Definition An *equitable* $(r, c; v)$-*rectangle* is an $r \times c$ matrix L with symbols from $\mathbb{Z}_v$ in which each symbol appears

(a) in every row either $\lceil c/v \rceil$ or $\lfloor c/v \rfloor$ times and
(b) in every column either $\lceil r/v \rceil$ or $\lfloor r/v \rfloor$ times.

For example, an equitable $(r, c; c)$-rectangle with $r \leqslant c$ is commonly known as a *Latin rectangle* and an equitable $(r, r; r)$-rectangle is a *Latin square*.

Communicated by L. Teirlinck.

A. B. Evans
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

D. Fear · R. J. Stones
School of Mathematical Sciences, Monash University, Clayton, VIC 3800, Australia

R. J. Stones
Clayton School of Information Technology, Monash University, Clayton, VIC 3800, Australia

R. J. Stones (✉)
Department of Mathematics and Statistics, Dalhousie University, Halifax, NS B3H 4H8, Canada
e-mail: rebecca.stones82@gmail.com

Suppose $L = (l_{ij})$ is an equitable $(r, c; v)$-rectangle and $L' = (l'_{ij})$ is an equitable $(r, c; v')$-rectangle, such that $rc = vv'$. Then L and L' are said to be *orthogonal* if the rc pairs (l_{ij}, l'_{ij}) are all distinct. Since $rc = vv'$, all possible ordered pairs occur in a pair of orthogonal equitable rectangles. For example

$$\boxed{\begin{matrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{matrix}} \quad \text{and} \quad \boxed{\begin{matrix} 0 & 3 & 2 & 1 \\ 2 & 1 & 0 & 3 \end{matrix}} \tag{1}$$

give an example of an equitable (2, 4; 2)-rectangle that is orthogonal to an equitable (2, 4; 4)-rectangle.

Notation • We will always take r, c and v as positive integers.
- For any $r \times c$ matrix, we will index its rows by $\mathbb{Z}_r$, its columns by $\mathbb{Z}_c$ and the symbols will be taken from $\mathbb{Z}_v$.
- Define the permutations $\alpha = (0\,1 \cdots r-1)$, $\beta = (0\,1 \cdots c-1)$ and $\gamma = (0\,1 \cdots v-1)$ of $\mathbb{Z}_r$, $\mathbb{Z}_c$ and $\mathbb{Z}_v$, respectively.
- Let $g = \gcd(r, c)$ and $m = \gcd(r, c, v)$.

Definition Suppose $L = (l_{ij})$ is an $r \times c$ matrix such that $l_{\alpha(i)\beta(j)} = \gamma(l_{ij})$ for all $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_c$. Then we call L *diagonally cyclic*.

We will be interested in the case of diagonally cyclic equitable $(r, c; v)$-rectangles, or $(r, c; v)$-DCERs for short. For example, the right hand side of (1) is a (2, 4; 4)-DCER.

1.1 History

Equitable rectangles have a short history, although the special case of diagonally cyclic Latin squares goes back to Euler [9] (see also [3,16]). Diagonally cyclic Latin squares have been used for a range of applications (e.g. [4,5,10,17]), sometimes disguised as orthomorphisms or transversals. Equitable rectangles were first defined by Stinson [14], where they were discovered in the course of studying a generalisation of "mix functions" [13].

Theorem 1 *Suppose $r, c \geqslant 1$. There exists an equitable $(r, c; r)$-rectangle that is orthogonal to an equitable $(r, c; c)$-rectangle if and only if $(r, c) \notin \{(2, 2), (2, 3), (3, 4), (6, 6)\}$.*

Stinson proved almost all of the cases in Theorem 1, leaving ten possible exceptions that were later resolved by Guo and Ge [11]. Cao et al. [6] gave the following generalisation of Theorem 1.

Theorem 2 *Suppose $r, c, v, v' \geqslant 1$ and $rc = vv'$. There exists an equitable $(r, c; v)$-rectangle that is orthogonal to an equitable $(r, c; v')$-rectangle if and only if $(r, c; v, v') \notin \{(2, 2; 2, 2), (2, 3; 2, 3), (3, 4; 3, 4), (6, 6; 6, 6)\}$.*

Asplund and Keranen [1] have classified the existence of triples of mutually orthogonal equitable rectangles (barring some classes of exceptions). For equitable rectangles of parameters $(r, c; v)$, $(r, c; w)$ and $(r, c; y)$ to be mutually orthogonal, we need $vw = vy = wy = rc$, and thus $v = w = y = \sqrt{rc}$.

1.2 Basic results

We now observe three basic, but important lemmata concerning diagonally cyclic equitable rectangles.

Definition Suppose $L = (l_{ij})$ is an $(r, c; v)$-DCER. We define an *entry* of L to be one of the rc triplets (i, j, l_{ij}) with $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_c$. Let G be the group generated by (α, β, γ). Then G acts on the set of entries of L. The *orbit* of an entry (i, j, l_{ij}) is the set $\{\theta(i, j, l_{ij}) : \theta \in G\}$.

Lemma 1 *An* $(r, c; v)$*-DCER has exactly* g *orbits, each of size* $\operatorname{lcm}(r, c)$.

Lemma 2 *An* $(r, c; v)$*-DCER is determined by the first* g *entries in the first row.*

Lemma 3 *If an* $(r, c; v)$*-DCER exists,* v *divides* $\operatorname{lcm}(r, c)$.

Proofs of Lemmata 1–3 If $L = (l_{ij})$ is an $(r, c; v)$-DCER, then, for any $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_c$, the entry

$$\left(\alpha^{\operatorname{lcm}(r,c)}(i), \beta^{\operatorname{lcm}(r,c)}(j), \gamma^{\operatorname{lcm}(r,c)}(l_{ij})\right) = \left(i, j, \gamma^{\operatorname{lcm}(r,c)}(l_{ij})\right),$$

since α has order r and β has order c. So we must have $\gamma^{\operatorname{lcm}(r,c)}(l_{ij}) = l_{ij}$. Since γ is a v-cycle without fixed points, $\gamma^{\operatorname{lcm}(r,c)}$ is the identity permutation and so v must divide $\operatorname{lcm}(r, c)$, thereby proving Lemma 3.

Any orbit is thus of the form

$$\left\{\left(\alpha^k(i), \beta^k(j), \gamma^k(l_{ij})\right) : 0 \leqslant k \leqslant \operatorname{lcm}(r, c) - 1\right\}$$

and has size $\operatorname{lcm}(r, c)$. So there are $rc/\operatorname{lcm}(r, c) = g$ orbits. Thus Lemma 1 holds.

To prove Lemma 2, it is sufficient to show that $(0, j, l_{0j})$ and $(0, j', l_{0j'})$ belong to distinct orbits whenever $0 \leqslant j < j' \leqslant g - 1$. If $(0, j, l_{0j})$ and $(0, j', l_{0j'})$ belong to the same orbit, then

$$\left(\alpha^k(0), \beta^k(j), \gamma^k(l_{0j})\right) = (0, j', l_{0j'})$$

for some $k \in \mathbb{Z}$. Since $\alpha^k(0) = 0$, we have that r (and hence g) divides k. Since $\beta^k(j) = j'$, we have that c (and hence g) divides $k - j + j'$. Hence g divides $j - j'$, contradicting that $0 \leqslant j < j' \leqslant g - 1$. □

For example, G induces two orbits on the entries of the $(2, 4; 4)$-DCER on the right hand side of (1), specifically $\{(0, 0, 0), (1, 1, 1), (0, 2, 2), (1, 3, 3)\}$ and $\{(1, 0, 2), (0, 1, 3), (1, 2, 0), (0, 3, 1)\}$, and the $(2, 4; 4)$-DCER is determined by the two entries $(0, 0, 0)$ and $(0, 1, 3)$.

1.3 Motivation

In this paper, we will solve the existence problem for diagonally cyclic equitable rectangles. There are several factors motivating the study of DCERs, for example, they can be described compactly—the first g entries in the first row (or the first column) determine the entire rectangle (Lemma 2). For example, the following $(2, 12; 3)$-DCER is determined by the 0 and the 2 in the top-left corner.

$$\boxed{\begin{matrix} 0 & 2 & 2 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & 2 & 2 \end{matrix}} \qquad (2)$$

Another motivating factor, as we will detail in the following theorem, is that for any $(r, c; v)$-DCER, there always exists an orthogonal equitable $(r, c; v')$-rectangle where $v' = rc/v$.

Theorem 3 *Any* $(r, c; v)$*-DCER is orthogonal to some equitable* $(r, c; rc/v)$*-rectangle.*

Proof Suppose $L = (l_{ij})$ is an $(r, c; v)$-DCER and let $v' = rc/v$. We will construct an equitable $(r, c; v')$-rectangle $M = (m_{ij})$ that is orthogonal to L. We process each of the v' copies of the symbol 0 in L sequentially. If l_{ij} is the t-th copy of 0 in L, we assign $m_{\alpha^a(i)\beta^a(j)} = t$ for all $0 \leqslant a < v$. The diagonally cyclic property of L ensures that $l_{\alpha^a(i)\beta^a(j)} \neq l_{\alpha^s(i)\beta^s(j)}$ whenever $0 \leqslant a < s < v$, while we have assigned $m_{\alpha^a(i)\beta^a(j)} = t = m_{\alpha^s(i)\beta^s(j)}$ for all $0 \leqslant a < s < v$. We can easily check that M is indeed an equitable $(r, c; v')$-rectangle. Hence L and M are orthogonal equitable rectangles. □

So in fact, with knowledge of merely the parameters (2, 12; 3) and the 0 and 2 in the top-left corner of (2), we can quickly construct not only a diagonally cyclic equitable rectangle with those parameters, but also an orthogonal equitable rectangle.

Diagonally cyclic equitable rectangles also have potential applications in constructing generalised Latin squares with non-trivial symmetries, such as frequency squares [7, Sec. 12.5]. For Latin squares, [15] gave a classification of which permutations α, consisting of three or fewer non-trivial cycles, are automorphisms of some Latin square of order n. Within the Latin squares that admit an automorphism consisting of three non-trivial cycles, constructions of $(r, c; v)$-DCERs arise, giving the following result.

Theorem 4 *There exists an* $(r, c; \mathrm{lcm}(r, c))$*-DCER except if* $r = c$ *and* r *is even.*

The exception in Theorem 4 arises due to the non-existence of diagonally cyclic Latin squares of even order [16].

1.4 Main theorem

The aim of this paper is to classify for which parameters r, c, v there can exist an $(r, c; v)$-DCER. More specifically, we will prove the following theorem.

Theorem 5 *An* $(r, c; v)$*-DCER exists if and only if*

- v *divides* $\mathrm{lcm}(r, c)$*,*
- *either* v *is odd or* $g \not\equiv v \pmod{2v}$*,*
- *if* $N_{\mathrm{row}} > 1$ *then* vN_{row} *divides* c*, and*
- *if* $N_{\mathrm{col}} > 1$ *then* vN_{col} *divides* r*,*

where

$$N_{\mathrm{row}} = \frac{c\ \gcd(r, v)}{vg} \quad \textit{and} \quad N_{\mathrm{col}} = \frac{r\ \gcd(c, v)}{vg}.$$

Some elementary number theory reveals that N_{row} and N_{col} are positive integers whenever v divides $\mathrm{lcm}(r, c)$; see Lemma 8 in the Appendix.

The proof we present for Theorem 5 is constructive (where relevant), and a pseudo-code implementation is given in Sect. 5. Note that, in the statement of Theorem 5, both N_{row} and N_{col} are interpreted as numbers, but we will later show that they have a combinatorial interpretation.

In Table 1 we identify which divisors v of $\mathrm{lcm}(r, c)$ admit an $(r, c; v)$-DCER for $1 \leqslant r \leqslant c \leqslant 10$. Note that there exists an $(r, c; v)$-DCER if and only if there exists a $(c, r; v)$-DCER, so we do not include results regarding $(r, c; v)$-DCERs when $r > c$ in Table 1.

2 Necessary conditions

To begin, we will prove the necessity of the conditions in Theorem 5; note we have already shown that v must divide $\mathrm{lcm}(r, c)$ in Lemma 3.

Table 1 The divisors v of $\mathrm{lcm}(r, c)$ for which there exists (or does not exist) an $(r, c; v)$-DCER

r,c	v:∃ DCER	v:∄ DCER
1,1	1	
1,2	1,2	
2,2	1	2
1,3	1,3	
2,3	1,6	2,3
3,3	1,3	
1,4	1,2,4	
2,4	1,4	2
3,4	1,12	2,3,4,6
4,4	1,2	4
1,5	1,5	
2,5	1,10	2,5
3,5	1,15	3,5
4,5	1,20	2,4,5,10
5,5	1,5	
1,6	1,2,3,6	
2,6	1,3,6	2
3,6	1,2,3,6	
4,6	1,12	2,3,4,6
5,6	1,30	2,3,5,6,10,15
6,6	1,3	2,6
1,7	1,7	
2,7	1,14	2,7
3,7	1,21	3,7
4,7	1,28	2,4,7,14
5,7	1,35	5,7
6,7	1,42	2,3,6,7,14,21
7,7	1,7	
1,8	1,2,4,8	
2,8	1,4,8	2
3,8	1,24	2,3,4,6,8,12
4,8	1,2,8	4
5,8	1,40	2,4,5,8,10,20
6,8	1,24	2,3,4,6,8,12
7,8	1,56	2,4,7,8,14,28
8,8	1,2,4	8
1,9	1,3,9	

Euler [9] showed that diagonally cyclic Latin squares of even orders cannot exist, that is, $(r, r; r)$-DCERs cannot exist for even r. The following condition generalises Euler's result; a related generalisation was given in [15], which showed the non-existence of Latin squares with certain automorphisms.

Table 1 continued

2,9	1,18	2,3,6,9
3,9	1,3,9	
4,9	1,36	2,3,4,6,9,12,18
5,9	1,45	3,5,9,15
6,9	1,3,18	2,6,9
7,9	1,63	3,7,9,21
8,9	1,72	2,3,4,6,8,9,12,18,24,36
9,9	1,3,9	
1,10	1,2,5,10	
2,10	1,5,10	2
3,10	1,30	2,3,5,6,10,15
4,10	1,20	2,4,5,10
5,10	1,2,5,10	
6,10	1,15,30	2,3,5,6,10
7,10	1,70	2,5,7,10,14,35
8,10	1,40	2,4,5,8,10,20
9,10	1,90	2,3,5,6,9,10,15,18,30,45
10,10	1,5	2,10

Lemma 4 *If v is even and $g \equiv v \pmod{2v}$ then an $(r, c; v)$-DCER does not exist.*

Proof Suppose L is an $(r, c; v)$-DCER, and let the first g elements of the first row of L be $a_0, a_1, \ldots, a_{g-1}$. By assumption, v divides g and hence v divides both r and c. Hence the first row of L is $a_0, a_1, \ldots, a_{g-1}$ repeated c/g times. Similarly, the first column of L will comprise of the first g entries in that column repeated r/g times. Since L is diagonally cyclic, the first g entries in the first column are $a_0 - 0, a_{g-1} - (g-1), a_{g-2} - (g-2), \ldots, a_1 - 1$. Hence, the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ a_0 & a_1 & \cdots & a_{g-1} \\ 0 & 1 & \cdots & g-1 \end{pmatrix}$$

is a $(v, 3; g/v)$-difference matrix over $\mathbb{Z}_v$; Drake [8, Theorem 1.10] showed that such a difference matrix cannot exist when v is even and g is an odd multiple of v.

The remaining necessary conditions we present are motivated by the following observation. If 0 were in the top-left corner of an (8, 12; 3)-DCER, its orbit would look like the following.

$$\begin{array}{|cccccccccccc|}
\hline
0 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 0 & \cdot & \cdot \\
\cdot & \cdot & 2 & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 2 \\
0 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot & 0 & \cdot & \cdot \\
\cdot & \cdot & 2 & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 2 \\
\hline
\end{array}$$

If we let $2a_i$ be the number of copies of $i \in \mathbb{Z}_3$ in column 0, we must have $2a_0+2a_1+2a_2 = 8$, while at the same time have $|2a_i - 2a_j| \leqslant 1$ for all $i, j \in \mathbb{Z}_3$. It is impossible to satisfy this system of equations and we can conclude that an (8, 12; 3)-DCER cannot exist. (Note that these parameters satisfy the previous necessary conditions, namely Lemmata 3 and 4.)

We will now generalise the above observation.

Definition Let $L = (l_{ij})$ be an $(r, c; v)$-DCER. Let N_{row} be the number of copies of the symbol l_{00} in the first row of L in the orbit of $(0, 0, l_{00})$. Let N_{col} be the number of copies of the symbol l_{00} in the first column of L in the orbit of $(0, 0, l_{00})$.

We will show that

$$N_{\mathrm{row}} = \frac{c\ \gcd(r, v)}{vg} \quad \text{and} \quad N_{\mathrm{col}} = \frac{r\ \gcd(c, v)}{vg}. \tag{3}$$

Let $\mathcal{X}$ be the set of entries of the orbit of $(0, 0, l_{00})$ that appear in row 0 of L. By Lemma 1, there are g orbits in total, so $|\mathcal{X}| = c/g$. Since there are $v/\gcd(r, v)$ symbols congruent to $l_{00} \pmod{\gcd(r, v)}$ in $\mathbb{Z}_v$, each symbol congruent to $l_{00} \pmod{\gcd(r, v)}$ appears in $\mathcal{X}$ exactly N_{row} times. We can similarly show the identity for N_{col}.

To further illustrate, consider the following (2, 8; 4)-DCER:

$$\begin{array}{|cccccccc|}\hline 1&0&3&2&1&0&3&2\\ 3&2&1&0&3&2&1&0\\\hline\end{array}.$$

Here we have $\mathcal{X} = \{(0, 0, 1), (0, 2, 3), (0, 4, 1), (0, 6, 3)\}$, so $|\mathcal{X}| = 4$. Its entries have symbols that are distributed evenly among all symbols congruent to $1 \pmod 2$ (namely 1 and 3), and there are 2 such symbols. Hence we have $N_{\mathrm{row}} = 2$.

Lemma 5 *Suppose an $(r, c; v)$-DCER exists. If $N_{\mathrm{row}} > 1$, then vN_{row} divides c. Similarly, if $N_{\mathrm{col}} > 1$, then vN_{col} divides r.*

Proof We know N_{row} and N_{col} are positive integers because of their combinatorial interpretation (or by Lemma 8, since the existence of a $(r, c; v)$-DCER implies v divides $\mathrm{lcm}(r, c)$).

Assume $N_{\mathrm{row}} > 1$. For $s \in \mathbb{Z}_v$, let k_s be the number of symbols congruent to $s \pmod{\gcd(r, v)}$ in the partial row $(l_{00}, l_{01}, \ldots, l_{0(g-1)})$. Hence $s \in \mathbb{Z}_v$ occurs exactly $k_s N_{\mathrm{row}}$ times in row 0. Since L is an equitable rectangle, we must therefore have $\lfloor c/v \rfloor \leqslant k_s N_{\mathrm{row}} \leqslant \lceil c/v \rceil$ for all $s \in \mathbb{Z}_v$. Since $N_{\mathrm{row}} > 1$, we find $k_0 = k_1 = \cdots = k_{v-1}$. It follows that $k_0 N_{\mathrm{row}} = c/v$. Since k_0 is a positive integer, vN_{row} must divide c.

A symmetric argument implies that if $N_{\mathrm{col}} > 1$, then vN_{col} divides r. □

The main theorem of this paper (Theorem 5) asserts that the necessary conditions for the existence of an $(r, c; v)$-DCER presented thus far are also sufficient.

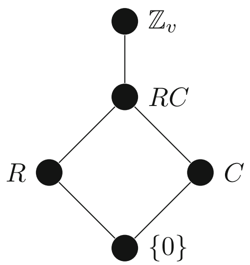
3 Group-theoretical interpretation

If $L = (l_{ij})$ is an $(r, c; v)$-DCER, then Lemma 2 implies the entries $(0, 0, l_{00})$, $(0, 1, l_{01}), \ldots,$ $(0, g-1, l_{0(g-1)})$ determine L. As such, it is natural to rephrase the conditions for the existence of an $(r, c; v)$-DCER as conditions about these entries. We will use $(x_j)_{0 \leqslant j \leqslant g-1}$ to denote an arbitrary element of $(\mathbb{Z}_v)^g$, and if there exists an $(r, c; v)$-DCER $L = (l_{ij})$ with $l_{0j} = x_j$ for all $0 \leqslant j \leqslant g-1$, then we say $(x_j)_{0 \leqslant j \leqslant g-1}$ *generates* an $(r, c; v)$-DCER.

We will frequently use the following subgroups of $\mathbb{Z}_v$:

- R is the subgroup of $\mathbb{Z}_v$ generated by r, so $R = \langle \gcd(r, v) \rangle$, and $|R| = v/\gcd(r, v)$.
- C is the subgroup of $\mathbb{Z}_v$ generated by c, so $C = \langle \gcd(c, v) \rangle$, and $|C| = v/\gcd(c, v)$.
- RC is the subgroup of $\mathbb{Z}_v$ generated by r and c, so $RC = \langle \gcd(r, c, v) \rangle$, and $|RC| = v/\gcd(r, c, v)$.

These groups are depicted by the (partial) subgroup lattice:



Definition Let (a_j) be a sequence of length $n \geqslant 1$. Let Γ be a collection of m disjoint sets. Suppose each a_j belongs to $\cup_{S \in \Gamma} S$.

1. We say that (a_j) is *equitably distributed* among Γ if each $S \in \Gamma$ has either $\lceil n/m \rceil$ or $\lfloor n/m \rfloor$ representatives in (a_j).
2. We say that (a_j) is *equally distributed* among Γ if each $S \in \Gamma$ has exactly n/m representatives in (a_j).

Of course, for (a_j) to be equally distributed among Γ, we need n/m to be a positive integer, or equivalently, that m divides n. If (a_j) is equitably distributed among Γ and m divides n, then it is equally distributed among Γ. Thus, "equally distributed" is simply the special case of "equitably distributed" with the additional condition that m divides n.

Definition Let (a_j) be a sequence of length n, whose elements belong some set S of size v. We will say S is *equitably distributed* in (a_j) if each element in S occurs either $\lceil n/v \rceil$ or $\lfloor n/v \rfloor$ times in (a_j). We will say S is *equally distributed* in (a_j) if each element in S occurs exactly n/v times in (a_j).

Theorem 6 *The sequence* $(x_j)_{0 \leqslant j \leqslant g-1}$ *generates an* $(r, c; v)$*-DCER if and only if* v *divides* $\mathrm{lcm}(r, c)$ *and*

1. $(x_j)_{0 \leqslant j \leqslant g-1}$ *is equitably distributed among* $\mathbb{Z}_v/R$*,*
2. $(x_j - j)_{0 \leqslant j \leqslant g-1}$ *is equitably distributed among* $\mathbb{Z}_v/C$*,*
3. *if* $N_{\mathrm{row}} > 1$ *then* vN_{row} *divides* c*, and*
4. *if* $N_{\mathrm{col}} > 1$ *then* vN_{col} *divides* r*.*

Proof Provided v divides $\mathrm{lcm}(r, c)$, we can use $(x_j)_{0 \leqslant j \leqslant g-1}$ to generate an $r \times c$ matrix $L = (l_{ij})$ in which (a) $l_{0j} = x_j$ for all $0 \leqslant j \leqslant g-1$, and (b) $l_{\alpha(i)\beta(j)} = \gamma(l_{ij})$ for all $i \in \mathbb{Z}_r$ and $j \in \mathbb{Z}_c$ (i.e., L is diagonally cyclic). We wish to determine whether or not L is an $(r, c; v)$-DCER.

We know that L is an $(r, c; v)$-DCER if and only if (a) $\mathbb{Z}_v$ is equitably distributed in row 0 of L and (b) $\mathbb{Z}_v$ is equitably distributed in column 0 of L. (If this holds, the identity $l_{\alpha(i)\beta(j)} = \gamma(l_{ij})$ implies that $\mathbb{Z}_v$ is equitably distributed in the remaining rows and columns.)

The symbols in row 0 of L in the same orbit as entry $(0, j, x_j)$ are $x_j + R$, with each element of this coset occurring N_{row} times.

Case I $N_{\text{row}} = 1$. The elements of $\mathbb{Z}_v$ are equitably distributed in row 0 of L if and only if $(x_j)_{0 \leqslant j \leqslant g-1}$ is equitably distributed among $\mathbb{Z}_v/R$.

Case II $N_{\text{row}} > 1$. The elements of $\mathbb{Z}_v$ are equitably distributed in row 0 of L if and only if $(x_j)_{0 \leqslant j \leqslant g-1}$ is equally distributed among $\mathbb{Z}_v/R$, which occurs if and only if $(x_j)_{0 \leqslant j \leqslant g-1}$ is equitably distributed among $\mathbb{Z}_v/R$ and $[\mathbb{Z}_v : R] = \gcd(r, v)$ divides g. Lemma 10 (in the Appendix) implies that "$\gcd(r, v)$ divides g" and "vN_{row} divides c" are equivalent statements.

A symmetric proof works for columns instead of rows. □

While Theorem 6 indeed gives necessary and sufficient conditions for the existence of an $(r, c; v)$-DCER, we cannot be satisfied just yet—we still need to find sequences $(x_j)_{0 \leqslant j \leqslant g-1}$ that satisfy the conditions of Theorem 6 whenever possible. Largely because of the next lemma, we will find that constructing such sequences $(x_j)_{0 \leqslant j \leqslant g-1}$ is made much easier by studying the "in-between" group RC.

Lemma 6 *Let K be a coset of RC in $\mathbb{Z}_v$.*

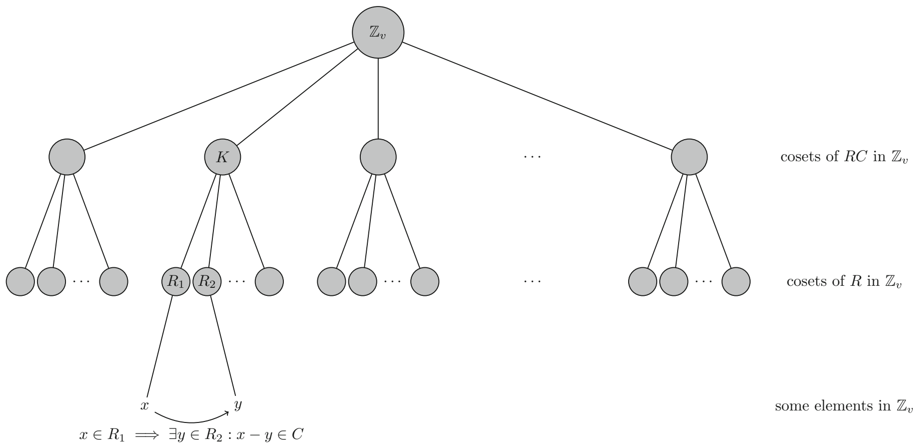
- *Let R_1 and R_2 be cosets of R in $\mathbb{Z}_v$ such that $R_1, R_2 \subseteq K$. If $x \in R_1$, then there exists $y \in R_2$ such that $x - y \in C$. Hence, x and y belong to the same coset of C in $\mathbb{Z}_v$.*
- *Let C_1 and C_2 be cosets of C in $\mathbb{Z}_v$ such that $C_1, C_2 \subseteq K$. If $x \in C_1$, then there exists $y \in C_2$ such that $x - y \in R$. Hence, x and y belong to the same coset of R in $\mathbb{Z}_v$.*

Proof By definition, for some $n \in \mathbb{Z}_v$,

- $K = \{n + a + b : a \in R \text{ and } b \in C\}$,
- $R_1 = \{n + a + b' : a \in R\}$, for some $b' \in C$, and
- $R_2 = \{n + a + b'' : a \in R\}$, for some $b'' \in C$.

Hence, if $x \in R_1$, then $y := x - b' + b'' \in R_2$ and $x - y = b' - b'' \in C$. The second bulleted item is proved symmetrically. □

Underneath the technical detail in Lemma 6 is the essence of how we will construct many sequences $(x_j)_{0 \leqslant j \leqslant g-1}$ that satisfy Theorem 6; the idea is illustrated below:



Suppose an element x_j belongs to a coset R_1 in $\mathbb{Z}_v$, but we want it to instead belong to the coset R_2, then we can try to achieve this by replacing x_j by $x_j + k$, for some $k \in C$. Importantly, this change does not affect which coset of C in $\mathbb{Z}_v$ the element $x_j - j$ belongs to (see Theorem 6). Lemma 6 states that if R_1 and R_2 happen to be subsets of the same coset of RC in $\mathbb{Z}_v$, then there exists a $k \in C$ for which $x_j + k \in R_2$, and we can achieve our objective.

Similarly, we might also have $x_j - j \in C_1$, but want it to instead belong to the coset C_2. This time, we replace x_j by $x_j + k$ for some $k \in R$, which does not affect which coset of R in $\mathbb{Z}_v$ the element x_j belongs to (and, thus, we don't "undo" the changes made in the first step of this process). If C_1 and C_2 are subsets of the same coset of RC in $\mathbb{Z}_v$, then there exists such a k.

In Theorem 7 we will identify some cases when, given some initial sequence $(z_j)_{0 \leqslant j \leqslant g-1}$, we can turn it into a sequence $(x_j)_{0 \leqslant j \leqslant g-1}$ that satisfies the conditions of Theorem 6, using the above procedure.

Definition Let (a_j) be a sequence of length n. Let $\Gamma = \{S_1, S_2, \ldots, S_m\}$ be a collection of m disjoint sets. Suppose each a_j belongs to $\cup_i S_i$. We say (a_j) is *near-equally distributed* among Γ if m divides n and there exists two distinct indices $k, l \in \{1, 2, \ldots, m\}$ such that:

- S_k is represented $n/m - 1$ times in (a_j),
- S_l is represented $n/m + 1$ times in (a_j), and
- S_i is represented n/m times in (a_j) whenever $1 \leqslant i \leqslant m$ except when $i \notin \{k, l\}$.

Definition Let $(z_j)_{0 \leqslant j \leqslant g-1}$ be a sequence of g elements in $\mathbb{Z}_v$.

- If (z_j) and $(z_j - j)$ are both equitably distributed among $\mathbb{Z}_v/RC$, then we call (z_j) a *biequitable sequence*.
- If (z_j) is near-equally distributed among $\mathbb{Z}_v/RC$ and $(z_j - j)$ is equitably distributed among $\mathbb{Z}_v/RC$, then we call (z_j) a *near-biequitable sequence*.
- If (z_j) is equitably distributed among $\mathbb{Z}_v/RC$ and $(z_j - j)$ is near-equally distributed among $\mathbb{Z}_v/RC$, then we call (z_j) a *co-near-biequitable sequence*.

Theorem 7 *Suppose v divides* $\operatorname{lcm}(r, c)$. *Let P be the proposition "there exists $(x_j)_{0 \leqslant j \leqslant g-1}$ such that (x_j) is equitably distributed among $\mathbb{Z}_v/R$ and $(x_j - j)$ is equitably distributed among $\mathbb{Z}_v/C$."*

I. If there exists a biequitable sequence, then P is true.
II. If there exists a near-biequitable sequence, then P is true, except possibly if v divides c.
III. If there exists a co-near-biequitable sequence, then P is true, except possibly if v divides r.

Proof For Cases I–III below, let $(z_j)_{0 \leqslant j \leqslant g-1}$ be the biequitable, near-biequitable or co-near-biequitable sequence, respectively. Let $(X_j)_{0 \leqslant j \leqslant g-1}$ and $(Y_j)_{0 \leqslant j \leqslant g-1}$ be the two sequences of cosets of RC in $\mathbb{Z}_v$ for which $z_j \in X_j$ and $z_j - j \in Y_j$ for all $0 \leqslant j \leqslant g$.

Case I $(z_j)_{0 \leqslant j \leqslant g-1}$ is a biequitable sequence.

Step 1: Let $K \in \mathbb{Z}_v/RC$. There are $|\mathbb{Z}_v/RC| = m$ cosets in $\mathbb{Z}_v/RC$. Since m divides g, we know K occurs in both (X_j) and (Y_j) exactly g/m times. Let $\lambda = [RC : R]$. Let $R_0, R_1, \ldots, R_{\lambda-1}$ be the cosets of R in $\mathbb{Z}_v$ inside K. Define the subsequence $(z_{t_i})_{0 \leqslant i \leqslant g/m-1}$ where t_i is the index of the i-th element of (z_j) that belongs to K.

If $z_{t_i} \notin R_{i \bmod \lambda}$, we replace z_{t_i} by $z_{t_i} + k$ for some $k \in C$ to achieve $z_{t_i} \in R_{i \bmod \lambda}$. Lemma 6 asserts that such a $k \in C$ exists. Since $k \in C$, this operation preserves $z_{t_i} \in X_{t_i}$ and $z_{t_i} - t_i \in Y_{t_i}$. Hence (z_{t_i}) is equitably distributed among $\{R_i\}_{0 \leqslant i \leqslant \lambda-1}$.

Step 2: Repeat Step 1 for every coset $K \in \mathbb{Z}_v/RC$. We conclude that (z_j) is equitably distributed among $\mathbb{Z}_v/R$.

Step 3: Repeat Steps 1 and 2 for C instead of R so that $(z_j - j)$ is equitably distributed among $\mathbb{Z}_v/C$. Importantly, Lemma 6 ensures that these changes do not affect the changes already made in Steps 1 and 2.

Step 4: Once we have completed Steps 1–3, set $(x_j) = (z_j)$, completing the proof of this case.

Case II $(z_j)_{0 \leqslant j \leqslant g-1}$ is a near-biequitable sequence.

First, repeat Steps 1–3 in Case I. However, unlike Case I, we cannot immediately conclude that (z_j) is equitably distributed among $\mathbb{Z}_v/R$. Let $\mu = g/[\mathbb{Z}_v : RC] = g/m$. Since (X_j) is near-equally distributed among $\mathbb{Z}_v/RC$, there exists two cosets $K', K'' \in \mathbb{Z}_v/RC$, which appear $\mu + 1$ times and $\mu - 1$ times in (X_j), respectively, while all other cosets in $\mathbb{Z}_v/RC$ (if any) appear exactly μ times in (X_j).

Since we have performed Steps 1–3 from Case I, we can assume that any coset $\mathbb{Z}_v/R$ has at most $\lceil(\mu + 1)/[RC : R]\rceil$ representatives in (z_j), and has at least $\lfloor(\mu - 1)/[RC : R]\rfloor$ representatives in (z_j). Hence, (z_j) is equitably distributed among $\mathbb{Z}_v/R$ provided

$$\left\lceil \frac{\mu+1}{[RC : R]} \right\rceil - \left\lfloor \frac{\mu-1}{[RC : R]} \right\rfloor \leqslant 1. \tag{4}$$

Equation 4 remains unchanged after replacing μ by its remainder when divided by $[RC : R]$. Hence we will assume $0 \leqslant \mu < [RC : R]$. If $\mu = 0$ (which is when $[RC : R]$ divides μ), then the left hand side of (4) is $1 - (-1)$, so (4) is false. If $\mu > 0$ then

$$\left\lceil \frac{\mu+1}{[RC : R]} \right\rceil - \left\lfloor \frac{\mu-1}{[RC : R]} \right\rfloor = \left\lceil \frac{\mu+1}{[RC : R]} \right\rceil \leqslant \left\lceil \frac{[RC : R]}{[RC : R]} \right\rceil \leqslant 1.$$

Hence (4) is false if and only if $[RC : R]$ divides μ. Note that $[RC : R] = |RC|/|R| = \gcd(r, v)/\gcd(r, c, v)$ and $\mu = g/m$. Hence $[RC : R]$ divides μ if and only if $\gcd(r, v)$ divides g. If $\gcd(r, v)$ divides g, Lemma 11 implies v divides c.

Case III $(z_j)_{0 \leqslant j \leqslant g-1}$ is a co-near-biequitable sequence. This case can be proved similar to Case II. □

The next step in the proof, is to find sequences $(z_j)_{0 \leqslant j \leqslant g-1}$ that satisfy Theorem 7.

Construction 1 *If m is odd, then $(z_j)_{0 \leqslant j \leqslant g-1}$ defined by $z_j = 2j$ is a biequitable sequence.*

Proof We have $(z_j)_{0 \leqslant j \leqslant g-1} = (0, 2, \ldots, 2(g - 1))$. But since m is odd, $\mathbb{Z}_v/RC$ is generated by the coset containing 2. Hence $\mathbb{Z}_v/RC$ is equitably distributed in (z_j). Since $(z_j - j)_{0 \leqslant j \leqslant g-1} = (0, 1, \ldots, g - 1)$, we immediately find that $\mathbb{Z}_v/RC$ is equitably distributed in $(z_j - j)$. □

Construction 2 *Suppose m is even. Define $(z_j)_{0 \leqslant j \leqslant g-1}$ by*

$$z_j = \begin{cases} 2j & \text{for } 0 \leqslant j \leqslant \frac{1}{2}g - 1, \\ 2j + 1 & \text{for } \frac{1}{2}g \leqslant j \leqslant g - 1. \end{cases}$$

Define $(y_j)_{0 \leqslant j \leqslant g-1}$ by $y_j = j - z_j$ for all $0 \leqslant j \leqslant g - 1$.

- *If g/m is even, then (z_j) is a biequitable sequence.*
- *If g/m is odd, then (z_j) is a co-near-biequitable sequence and (y_j) is a near-biequitable sequence.*

Proof We have

$$(z_j) = (0, 2, \ldots, g - 2, g + 1, g + 3, \ldots, 2g - 1).$$

We can reorder (z_j) to obtain the sequence

$$(0, g + 1, 2, g + 3, \ldots, g - 2, 2g - 1) \equiv (0, 1, 2, 3, \ldots, -2, -1) \pmod{m}.$$

(This can be achieved by interlacing the subsequences $(0, 2, \ldots, g-2)$ and $(g+1, g+3, \ldots, 2g-1)$.) Hence $\mathbb{Z}_v/RC$ is equally distributed in (z_j). Further, $\mathbb{Z}_v/RC$ is equally distributed in $(y_j - j)$, since $y_j - j = -z_j$, and $\mathbb{Z}_v/RC$ is equally distributed in (z_j).

We also have

$$(z_j - j) = (0, 1, \ldots, g/2-1, g/2+1, g/2+2, \ldots, g).$$

Case I g/m is even. Since g/m is even, m divides $g/2$. Hence

- the subsequence $(0, 1, \ldots, g/2-1)$ contains $g/(2m)$ representatives from each coset in $\mathbb{Z}_v/RC$, and
- the subsequence $(g/2+1, g/2+2, \ldots, g)$ contains $g/(2m)$ representatives from each coset in $\mathbb{Z}_v/RC$.

Therefore $\mathbb{Z}_v/RC$ is equally distributed in $(z_j - j)$.

Case II g/m is odd. In this case, m does not divide $g/2$, but rather $g/2 \equiv m/2 \pmod{m}$. Thus

- the subsequence $(0, 1, \ldots, g/2-1)$ contains $(g/m+1)/2$ representatives from the cosets in $\mathbb{Z}_v/RC$ containing an element from $\{0, 1, \ldots, m/2-1\}$ and $(g/m-1)/2$ representatives from the cosets in $\mathbb{Z}_v/RC$ containing an element from $\{m/2, m/2+1, \ldots, m-1\}$, and
- the subsequence $(g/2+1, g/2+2, \ldots, g)$ contains $(g/m+1)/2$ representatives from the cosets in $\mathbb{Z}_v/RC$ containing an element from $\{m/2+1, m/2+2, \ldots, m-1\} \cup \{0\}$ and $(g/m-1)/2$ representatives from the cosets in $\mathbb{Z}_v/RC$ containing an element from $\{1, 2, \ldots, m/2\}$.

Therefore, the cosets in $\mathbb{Z}_v/RC$ containing an element from $\{1, 2, \ldots, m/2-1\} \cup \{m/2+1, m/2+2, \ldots, m-1\}$ have $(g/m+1)/2 + (g/m-1)/2 = g/m$ representatives in $(z_j - j)$. The coset containing 0 has $g/m + 1$ representatives in $(z_j - j)$ and the coset containing $m/2$ has $g/m + 1$ representatives in $(z_j - j)$. Hence $\mathbb{Z}_v/RC$ is near-equally distributed in $(z_j - j)$. Further, $\mathbb{Z}_v/RC$ is near-equally distributed in (y_j), since $y_j = -(z_j - j)$, and $\mathbb{Z}_v/RC$ is near-equally distributed in $(z_j - j)$.

Corollary 1 *Suppose (a) v divides $\operatorname{lcm}(r, c)$, (b) if $N_{\text{row}} > 1$ then vN_{row} divides c, and if $N_{\text{col}} > 1$ then vN_{col} divides r. Suppose also that v does not divide g. Then an $(r, c; v)$-DCER exists.*

Proof Apply Theorems 6 and 7 to the sequences in Construction 1 and 2. □

To complete the proof of the main theorem, we need only resolve the case when v divides g, which we will do in the next section.

4 Regular DCERs

An equitable $(r, c; v)$-rectangle is said to be *row-regular* if v divides c, *column-regular* if v divides r and *regular* if it is both row-regular and column-regular, that is, if v divides g. In this section, we will present necessary and sufficient conditions for the existence of a regular $(r, c; v)$-DCER.

Construction 3 *Suppose g is even and v divides $g/2$. An $(r, c; v)$-DCER exists for which $x_j = \lfloor j/2 \rfloor$ for $0 \leqslant j \leqslant g-1$.*

Proof We have

$$(x_j)_{0 \leqslant j \leqslant g-1} = (0, 0, 1, 1, \ldots, g/2 - 1, g/2 - 1)$$

and

$$(x_j - j)_{0 \leqslant j \leqslant g-1} = (0, -1, -1, -2, -2, \ldots, -g/2 + 1, -g/2 + 1, -g/2).$$

Since $g/2 \equiv 0 \pmod{v}$, we know that (x_j) and $(x_j - j)$ are equally distributed in $\mathbb{Z}_v/R$ and $\mathbb{Z}_v/C$, respectively. Since v divides g, Lemma 12 (in the Appendix) implies vN_{row} divides c and vN_{col} divides r. Thus Theorem 6 implies that (x_j) generates an $(r, c; v)$-DCER. □

For example, Construction 3 can be used to generate the following (4, 4; 2)-DCER and (6, 6; 3)-DCER.

$$\boxed{\begin{array}{cccc} 0&0&1&1\\ 0&1&1&0\\ 1&1&0&0\\ 1&0&0&1 \end{array}} \quad \boxed{\begin{array}{cccccc} 0&0&1&1&2&2\\ 0&1&1&2&2&0\\ 1&1&2&2&0&0\\ 1&2&2&0&0&1\\ 2&2&0&0&1&1\\ 2&0&0&1&1&2 \end{array}}$$

In the following construction, we classify when (x_j) defined by $x_j = 2j$ generates an $(r, c; v)$-DCER. For the purpose of proving the main theorem in this paper, we need only need the special case of when v is an odd divisor of g. Nevertheless, we include a complete classification of when the $2j$ construction generates an $(r, c; v)$-DCER since it is of special interest.

Construction 4 *Suppose v divides $\operatorname{lcm}(r, c)$. An $(r, c; v)$-DCER is generated by (x_j) defined by $x_j = 2j$ for $0 \leqslant j \leqslant g - 1$, if and only if*

1. $\gcd(r, v)$ *is odd or* $2g \leqslant \gcd(r, v)$ *(or both),*
2. *if* $N_{\text{row}} > 1$ *then* vN_{row} *divides* c*, and*
3. *if* $N_{\text{col}} > 1$ *then* vN_{col} *divides* r*.*

Proof To begin, observe

$$(x_j - j)_{0 \leqslant j \leqslant g-1} = (0, 1, 2, \ldots, g - 1).$$

We immediately find that $(x_j - j)$ is equitably distributed among $\mathbb{Z}_v/C$. We have

$$\big(x_j\big)_{0 \leqslant j \leqslant g-1} = \big(0, 2, \ldots, 2(g - 1)\big).$$

We immediately find that (x_j) is equitably distributed among $\mathbb{Z}_v/R$ when $2g \leqslant \gcd(r, v)$, since there are no duplicated cosets. When $\gcd(r, v)$ is odd, (x_j) is equitably distributed among $\mathbb{Z}_v/R$ since $\gcd(r, v)$ and 2 are coprime (and thus, the coset containing 2 generates $\mathbb{Z}_v/R$). Theorem 6 thus implies that if conditions *2.* and *3.* hold, then an $(r, c; v)$-DCER exists.

Now suppose $\gcd(r, v)$ is even and $2g > \gcd(r, v)$. Then (x_j) is not equitably distributed among $\mathbb{Z}_v/R$, since the coset containing 0 has at least two representatives whereas the coset containing 1 has no representative. Theorem 6 thus implies (x_j) does not generate an $(r, c; v)$-DCER. □

For Constructions 3 and 4, unlike Constructions 1 and 2, we do not need to apply Theorem 7 to construct an $(r, c; v)$-DCER; they are direct constructions of sequences (x_j) which generate the $(r, c; v)$-DCER.

We are now ready to give necessary and sufficient conditions for the existence of a regular $(r, c; v)$-DCER.

Corollary 2 *There exists a regular* $(r, c; v)$*-DCER whenever* v *divides* g *except if* v *is even and* $g \equiv v \pmod{2v}$.

Proof Construction 3 resolves the case when v is even and $g \equiv 0 \pmod{2v}$. Construction 4 resolves the odd v case (Lemma 10 ensures that vN_{row} divides c and vN_{col} divides r). Lemma 4 resolves the case when v is even and $g \equiv v \pmod{2v}$. □

Corollaries 1 and 2 combine to give a proof of the main theorem in this paper (Theorem 5), thereby resolving the existence problem for $(r, c; v)$-DCERs.

5 Implementation

Algorithm 1 gives a pseudo-code implementation of Theorem 7. We continue using the notation introduced in Sects. 1 and 3.

Algorithm 1 Balancing cosets

```
Require: (x_j)_{0≤j≤g−1} with each x_j ∈ Z_v
for all k ∈ {0, 1, ..., m − 1} do
  T ← R + k
  S ← C + k
  for all j ∈ {0, 1, ..., g − 1} do
    if x_j ≡ k (mod m) then
      T ← T + m
      while not x_j ∈ T do
        x_j ← x_j + gcd(c, v)  mod v
      end while
    end if
    if x_j − j ≡ k (mod m) then
      S ← S + m
      while not x_j − j ∈ S do
        x_j ← x_j + gcd(r, v)  mod v
      end while
    end if
  end for
end for
return (x_j)_{0≤j≤g−1}
```

Algorithm 1 proceeds as follows: for each $k \in \{0, 1, \ldots, m-1\}$, we edit the input sequence (x_j) to ensure that the cosets of R inside $RC + k$ appear in (x_j) in the order

$$R + k + m,\ R + k + 2m,\ \ldots \tag{5}$$

and representatives from the cosets of C in $RC + k$ will appear in the order

$$C + k + m,\ C + k + 2m,\ \ldots. \tag{6}$$

The cosets listed in (5) and (6) respectively include all cosets of R and C inside $RC + k$ an equitable number of times (since m generates RC).

If x_{j^*} is the t-th element of (x_j) that belongs to coset $RC + k$, then we want to ensure it belongs to coset $R + k + tm$. By Lemma 6, there exists an element $s \in C$ for which $x_{j^*} + s \in R + k + tm$. Since C is generated by $\gcd(c, v)$, in Algorithm 1, Line 1, we replace x_{j^*} by $x_{j^*} + \gcd(c, v)$ until we have $x_{j^*} \in R + k + tm$. We perform a similar operation for $(x_j - j)$ in Line 1. Importantly, Lemma 6 ensures that Algorithm 1 will terminate.

If the input sequence for Algorithm 1 satisfies the conditions of Theorem 7 (i.e., (x_j) is either (a) biequitable, (b) near-biequitable and v does not divide c, or (c) co-near-biequitable and v does not divide r), then Algorithm 1 will output a sequence (x_j) which generates and $(r, c; v)$-DCER, as demonstrated in the proof of Theorem 7.

If an $(r, c; v)$-DCER exists, we can construct it either by using either Constructions 1 and/or 2 (with Algorithm 1) or Constructions 3 and/or 4.

6 Concluding remarks

We conclude this paper with some comments about generalising this work. Suppose we have

- a finite group $(G, +)$,
- groups H_1, H_2 and H_3 of cardinalities r, c and v, respectively, and
- three onto homomorphisms $\zeta : G \to H_1$, $\eta : G \to H_2$ and $\theta : G \to H_3$ that satisfy $|\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)| = 1$.

We say an $r \times c$ matrix $M = (m_{ij})$, with rows indexed by H_1 and columns indexed by H_2 and symbols from H_3, is a *generalised diagonally cyclic equitable rectangle* (genDCER) if

$$M_{(i+\zeta(g))(j+\eta(g))} = M_{ij} + \theta(g) \tag{7}$$

for all $i \in H_1$, $j \in H_2$ and $g \in G$.

For example, the cyclic case we have looked at thus far is (up to isomorphism) when:

- $G = \langle(1, 1, 1)\rangle \leqslant \mathbb{Z}_r \times \mathbb{Z}_c \times \mathbb{Z}_v$,
- $H_1 = \mathbb{Z}_r \times \{0\} \times \{0\}$, $H_2 = \{0\} \times \mathbb{Z}_c \times \{0\}$ and $H_3 = \{0\} \times \{0\} \times \mathbb{Z}_v$,
- ζ, η and θ are defined by

$$\begin{aligned}\zeta\big((i, j, k)\big) &= (i, 0, 0)\\ \eta\big((i, j, k)\big) &= (0, j, 0)\\ \theta\big((i, j, k)\big) &= (0, 0, k)\end{aligned}$$

  for all $(i, j, k) \in G$.

If we were to allow $|\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)| > 1$ in our definition of a genDCER, there would be redundancy in (7). This redundancy is unnecessary since we can achieve essentially the same definition by working in $G/(\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta))$ instead of G. Hence we add the condition $|\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)| = 1$.

Lemma 7 *Suppose we have a genDCER with G, H_1, H_2, H_3, ζ, η and θ as defined above. Then* $|\ker(\zeta) \cap \ker(\eta)| = 1$.

Proof If $g \in \ker(\zeta) \cap \ker(\eta)$, then, by definition,

$$M_{ij} = M_{(i+\zeta(g))(j+\eta(g))} = M_{ij} + \theta(g)$$

implying $g \in \ker(\theta)$, and so $g \in \ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)$. Since $|\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)| = 1$, we know $g = \mathrm{id}_G$.

The following theorem generalises the "v divides $\mathrm{lcm}(r, c)$" condition (of Theorem 5) which holds in the cyclic group case; for simplicity, we switch to multiplicative notation.

Theorem 8 *Suppose we have a genDCER with G, H_1, H_2, H_3, r, c, ζ, η and θ as defined above. Then every $h \in H_3$ satisfies $h^{\mathrm{lcm}(r,c)} = \mathrm{id}_{H_3}$ (i.e., H_3 has exponent dividing $\mathrm{lcm}(r, c)$).*

Proof Define the subset $S \subseteq H_1 \times H_2 \times H_3$ by

$$S = \big\{\big(\zeta(g), \eta(g), \theta(g)\big) : g \in G\big\}.$$

Lemma 7 implies $|\ker(\zeta) \cap \ker(\eta)| = 1$, so there is only one element of S of the form $(\mathrm{id}_{H_1}, \mathrm{id}_{H_2}, ?)$, namely $(\mathrm{id}_{H_1}, \mathrm{id}_{H_2}, \mathrm{id}_{H_3})$.

For $g \in G$ define $g^* = \big(\zeta(g^{\mathrm{lcm}(r,c)}), \eta(g^{\mathrm{lcm}(r,c)}), \theta(g^{\mathrm{lcm}(r,c)})\big)$. Thus

$$\begin{aligned} g^* &= \big(\zeta(g)^{\mathrm{lcm}(r,c)}, \eta(g)^{\mathrm{lcm}(r,c)}, \theta(g)^{\mathrm{lcm}(r,c)}\big) && \text{since } \zeta, \eta, \theta \text{ are homomorphisms} \\ &= \big(\mathrm{id}_{H_1}, \mathrm{id}_{H_2}, \theta(g)^{\mathrm{lcm}(r,c)}\big) && \text{since } |H_1| \text{ and } |H_2| \text{ divide } \mathrm{lcm}(r, c) \\ &= \big(\mathrm{id}_{H_1}, \mathrm{id}_{H_2}, \mathrm{id}_{H_3}\big) && \text{since } g^* \in S. \end{aligned}$$

Hence $\theta(g)^{\mathrm{lcm}(r,c)} = \mathrm{id}_{H_3}$ for all $g \in G$. The result follows since θ is an onto homomorphism. □

In the cyclic case, we know $(0, 0, 1)$ generates H_3, so $v = |H_3| = \mathrm{ord}\big((0, 0, 1)\big)$, and Theorem 8 implies v divides $\mathrm{lcm}(r, c)$. However, the property "v divides $\mathrm{lcm}(r, c)$" is not true for all genDCERs, one such example is when:

- $G = \mathbb{Z}_6 \times \mathbb{Z}_{10}$,
- $H_1 = \mathbb{Z}_6 \times \{0\}$, $H_2 = \{0\} \times \mathbb{Z}_{10}$ and $H_3 = G$, and
- ζ, η, θ are defined by

$$\begin{aligned} \zeta\big((i, j)\big) &= (i, 0) \\ \eta\big((i, j)\big) &= (0, j) \\ \theta\big((i, j)\big) &= (i, j) \end{aligned}$$

  for all $(i, j) \in G$.

In this case, we have the following genDCER.

	00	01	02	03	04	05	06	07	08	09
00	00	01	02	03	04	05	06	07	08	09
10	10	11	12	13	14	15	16	17	18	19
20	20	21	22	23	24	25	26	27	28	29
30	30	31	32	33	34	35	36	37	38	39
40	40	41	42	43	44	45	46	47	48	49
50	50	51	52	53	54	55	56	57	58	59

Note that, in this case, $r = 6$, $c = 10$ and $v = 60$, so v does not divide $\mathrm{lcm}(r, c)$.

Another condition that no longer holds when considering genDCERs is Lemma 4, i.e., we may have the situation where $g \equiv v \pmod{2v}$ and v is even. One such example is when

- $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$,

- $H_1 = H_3 = \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $H_2 = G$, and
- ζ, η, θ are defined by

$$\zeta((i, j, k)) = (0, j, k)$$
$$\eta((i, j, k)) = (i, j, k)$$
$$\theta((i, j, k)) = (0, j, k)$$

for all $(i, j, k) \in G$.

Then we have the (4, 8; 4)-genDCER:

	000	001	010	011	100	101	110	111
000	000	011	001	010	000	011	001	010
001	010	001	011	000	010	001	011	000
010	011	000	010	001	011	000	010	001
011	001	010	000	011	001	010	000	011

This is an example of where Lemma 4 doesn't generalise; we have $g = v = 4$, and hence $g \equiv v \pmod{2v}$ and v is even, but a (4, 8; 4)-genDCER exists.

This construction comes from the method used to construct diagonally cyclic Latin squares of size 2^a for $a \geqslant 2$ over the group $(\mathbb{Z}_2)^a$ (historical references [2,12]). We can generalise this construction to give a $(2^a, 2^b; 2^c)$-genDCER for all $a, b, c \geqslant 2$. The parameters are

- $G = (\mathbb{Z}_2)^k$ where $k = \max(a, b, c)$,
- $H_1 = \{0\}^{k-a} \times \mathbb{Z}^a$, $H_2 = \{0\}^{k-b} \times \mathbb{Z}^b$, and $H_3 = \{0\}^{k-c} \times \mathbb{Z}^c$,
- $\zeta : G \to H_1$ sets the first $k - a$ components to 0, $\eta : G \to H_2$ sets the first $k - b$ components to 0, and $\theta : G \to H_3$ sets the first $k - c$ components to 0. (Note that since $k = \max(a, b, c)$, one of these homomorphisms is the identity, and thus has a trivial kernel, and hence $|\ker(\zeta) \cap \ker(\eta) \cap \ker(\theta)| = 1$.)

The entry in cell $(x, y) := (x_1 x_2 \cdots x_{k-1} x_k, y_1 y_2 \cdots y_{k-1} y_k)$ in the $(2^a, 2^b; 2^c)$-genDCER can be generated as follows:

- Let $x + y = z_1 z_2 \cdots z_{k-1} z_k$.
- Define z by replacing $z_{k-1} z_k$ in $x + y$ with $A_{x_{k-1}x_k, y_{k-1}y_k}$ where A is the following $(2^2, 2^2; 2^2)$-genDCER:

	00	01	10	11
00	00	11	01	10
01	10	01	11	00
10	11	00	10	01
11	01	10	00	11

- Set $z_1, z_2, \ldots, z_{k-c}$ equal to 0.

This is a direct product-like construction, essentially gluing together copies of A with the symbol indices suitably edited. We can verify its correctness by verifying that each coordinate satisfies (7) separately. When $a = c$ and $a < b$, we will satisfy $g \equiv v \pmod{2v}$ when v is even, so Lemma 4 would not hold in these cases.

Acknowledgments Stones supported by NSFC grant 61170301. Stones was also partially supported by AARMS.

Appendix: Technical lemmata

In the following lemmata, we say p^k *exactly divides* n if p^k divides n and p^{k+1} does not divide n. For these results, we assume r, c and v are arbitrary positive integers, and, as in the rest of the paper,

$$N_{\text{row}} = \frac{c \ \gcd(r, v)}{v \ \gcd(r, c)} \quad \text{and} \quad N_{\text{col}} = \frac{r \ \gcd(c, v)}{v \ \gcd(r, c)}.$$

Lemma 8 *Suppose v divides $\operatorname{lcm}(r, c)$. Then N_{row} and N_{col} are positive integers.*

Proof Let p be a prime. Suppose p^a exactly divides v, and p^b exactly divides r and p^x exactly divides c. If N_{row} is a positive integer, then it would be exactly divisible by $p^{x+\min(a,b)-a-\min(b,x)}$. Since p is arbitrary, it is sufficient to show that

$$x + \min(a, b) - a - \min(b, x) \geqslant 0 \tag{8}$$

as, if N_{row} were not a positive integer, then (8) would be false for some prime p. Note that $a \leqslant \max(b, x)$ since v divides $\operatorname{lcm}(r, c)$.

Case I $\min(a, b) = a$. Then (8) follows immediately.

Case II $\min(a, b) = b$ and $\min(b, x) = b$. The left hand side of (8) becomes $x - a$, which is non-negative, since $a \leqslant \max(b, x) = x$.

Case III $\min(a, b) = b$ and $\min(b, x) = x$. The left hand side of (8) becomes $b - a$, which is non-negative, since $a \leqslant \max(b, x) = b$.

We can show that N_{col} is a positive integer by switching r and c.

Lemma 9 *Let $\chi = c \ \gcd(r, v)/\gcd(r, c)$. Then χ divides c if and only if $\gcd(r, v)$ divides c.*

Proof If $\gcd(r, v)$ does not divide c, then χ, which is a multiple of $\gcd(r, v)$, also does not divide c.

Conversely, assume $\gcd(r, v)$ divides c. Let p be a prime. Suppose p^a exactly divides $\gcd(r, v)$, and p^b exactly divides $\gcd(r, c)$ and p^x exactly divides c. Hence p^{x+a-b} exactly divides χ. Since p is arbitrary, it is sufficient to show that $b \geqslant a$. Since p^a divides $\gcd(r, v)$, we know p^a divides r, and since $\gcd(r, v)$ divides c, we know p^a also divides c, so p^a divides $\gcd(r, c)$. Hence $b \geqslant a$. □

Lemma 10 *We have:*

- $\gcd(r, v)$ *divides* $\gcd(r, c)$ *if and only if* vN_{row} *divides* c *and*
- $\gcd(c, v)$ *divides* $\gcd(r, c)$ *if and only if* vN_{col} *divides* r.

Proof

$$\begin{aligned} \gcd(r, v) \text{ divides } \gcd(r, c) &\iff \gcd(r, v) \text{ divides } c \\ &\iff c \, \frac{\gcd(r, v)}{\gcd(r, c)} \text{ divides } c \qquad \text{by Lemma 9} \\ &\iff vN_{\text{row}} \text{ divides } c. \end{aligned}$$

The second dot-point is the same as the first with r and c switched. □

Lemma 11 *Suppose v divides $\operatorname{lcm}(r, c)$. Suppose also that $\gcd(r, v)$ divides $\gcd(r, c)$. Then v divides c.*

Proof Let d be a prime power divisor of v. Since v divides $\operatorname{lcm}(r, c)$ and d is a prime power, we know that d divides r or c (or both). Since we want to prove that d divides c, assume d divides r. Since d divides both r and v, we know that d divides $\gcd(r, v)$ and hence d divides $\gcd(r, c)$ by assumption. Therefore d divides c. Since d is an arbitrary prime power divisor of v, we conclude that v divides c. □

Lemma 12 *If v divides $\gcd(r, c)$, then vN_{row} divides c and vN_{col} divides r.*

Proof If v divides $\gcd(r, c)$, then v divides r and hence v divides $\gcd(r, v)$. But since $\gcd(r, v)$ divides v, we must have that $v = \gcd(r, v)$. Hence $N_{\text{row}} = c/\gcd(r, c)$ and

$$vN_{\text{row}} = \frac{c}{\left(\frac{\gcd(r,c)}{v}\right)},$$

which divides c (since v divides $\gcd(r, c)$, and $\gcd(r, c)$ divides c).

The second claim, that vN_{col} divides r, follows from the first claim with r and c switched. □

References

1. Asplund J., Keranen M.S.: Mutually orthogonal equitable latin rectangles. Discret. Math. **311**, 1015–1033 (2011).
2. Bose R.C.: On the application of the properties of Galois fields to the construction of hyper-Graeco-Latin squares. Sankhyā **3**, 323–338 (1938).
3. Bryant D., Buchanan M., Wanless I.M.: The spectrum for quasigroups with cyclic automorphisms and additional symmetries. Discret. Math. **304**, 821–833 (2009).
4. Bryant D., Egan J., Maenhaut B., Wanless I.M.: Indivisible plexes in Latin squares. Des. Codes Cryptogr. **52**, 93–105 (2009).
5. Bryant D., Maenhaut B.M., Wanless I.M.: New families of atomic Latin squares and perfect 1-factorisations. J. Comb. Theory Ser. A **113**, 608–624 (2004).
6. Cao H., Dinitz J., Kreher D., Stinson D., Wei R.: On orthogonal generalized equitable rectangles. Des. Codes Cryptogr. **51**, 225–230 (2009).
7. Dénes J., Keedwell A.D.: Latin Squares and their Applications. Academic Press, New York (1974).
8. Drake D.A.: Partial λ-geometries and generalized hadamard matrices over groups. Can. J. Math. **31**, 617–627 (1979).
9. Euler L.: Recherches sur une nouvelle espéce de quarrés magiques, Verh. Zeeuwsch. Gennot. Weten. Vliss. **9**, 85–239 (1782). Eneström E530, Opera Omnia OI7, pp. 291–392.
10. Evans A.B.: Orthomorphism Graphs of Groups. Springer, Berlin (1992).
11. Guo W., Ge G.: The existence of generalized mix functions. Des. Codes Cryptogr. **50**, 107–113 (2009).
12. Moore E.H.: Tactical memoranda I-III. Am. J. Math. **18**, 264–303 (1896).
13. Ristenpart T., Rogaway P.: How to enrich the message space of a cipher. Lecture Notes in Computer Science. Vol. **4593**, pp. 101–118. Springer, Berlin (2007).
14. Stinson D.R.: Generalized mix functions and orthogonal equitable rectangles. Des. Codes Cryptogr. **45**, 347–357 (2007).
15. Stones D.S., Vojtěchovský P., Wanless I.M.: Cycle structure of autotopisms of quasigroups and latin squares. J. Comb. Des. **20**, 227–263 (2012).
16. Wanless I.M.: Diagonally cyclic Latin squares. Eur. J. Comb. **25**, 393–413 (2004).
17. Wanless I.M.: Atomic Latin squares based on cyclotomic orthomorphisms. Electron. J. Comb. **12**, R22–R23 (2005).