On orthogonal generalized equitable rectangles

H. Cao*
Department of Mathematics and Computer Science
Nanjing Normal University
Nanjing 210097, Jiangsu, P.R. China
caohaitao@njnu.edu.cn

J. Dinitz
Department of Mathematics and Statistics
University of Vermont
Burlington VT 05405, U.S.A.
Jeff.Dinitz@uvm.edu

D. Kreher
Department of Mathematics
Michigan Technological University
Houghton, MI 49931-1295, USA
kreher@math.mtu.edu

D. R. Stinson†
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, ON, N2L 3G1, Canada
dstinson@uwaterloo.ca

R. Wei‡
Department of Computer Science
Lakehead University
Thunder Bay ON, P7B 5E1, Canada
rwei@lakeheadu.ca

July 31, 2008

Abstract

In this note, we give a complete solution of the existence of orthogonal generalized equitable rectangles, which was raised as an open problem in [4].

Key words: orthogonal latin squares, orthogonal equitable rectangles,

1 Introduction

A *latin square of order* t is a $t \times t$ array defined on t symbols such that every symbol occurs exactly once in each row and exactly once in each column. Two latin squares of order t, say $A = (a_{i,j})$ and $B = (b_{i,j})$, are *orthogonal* if the t^2 pairs $(a_{i,j}, b_{i,j})$, $1 \le i \le t$, $1 \le j \le t$, are distinct.

Suppose $r \le t$. An $r \times t$ *latin rectangle* is an $r \times t$ array defined on t symbols such that every symbol occurs exactly once in each row and at most once in each column. Two $r \times t$ latin rectangles, say $A = (a_{i,j})$ and $B = (b_{i,j})$, are *orthogonal* if the rt pairs $(a_{i,j}, b_{i,j})$, $1 \le i \le r$, $1 \le j \le t$, are distinct. It is easy to see that orthogonal $t \times t$ rectangles are the same as orthogonal latin squares

*research supported by NSF of China grant 10501023 and 60673070
†research supported by NSERC Discovery grant 203114-06
‡research supported by NSERC Discovery grant 239135-06

of order t. Orthogonal latin squares and orthogonal latin rectangles are well-studied combinatorial objects (see, e.g., [1]).

Stinson introduced orthogonal equitable rectangles in a recent paper [4]. Orthogonal equitable rectangles were motivated by a cryptographic application described in [3]. In fact, orthogonal equitable rectangles are a natural variation of orthogonal latin rectangles. An open question in [4] asked for necessary and sufficient conditions for the existence of a certain generalization of orthogonal equitable rectangles, which we define now.

Suppose r, t, s_1, s_2 are positive integers such that $rt = s_1 s_2$. *Orthogonal generalized equitable rectangles (OGER)* are defined to be two $r \times t$ rectangles, say A and B, satisfying the following properties:

1. $A = (a_{i,j})$ is defined on a set S_1 of s_1 symbols and $B = (b_{i,j})$ is defined on a set S_2 of s_2 symbols, where $s_1 s_2 = rt$.

2. A is equitable on rows and equitable on columns: each of the s_1 symbols in S_1 appears $\lceil \frac{t}{s_1} \rceil$ or $\lfloor \frac{t}{s_1} \rfloor$ times in every row of A, and $\lceil \frac{r}{s_1} \rceil$ or $\lfloor \frac{r}{s_1} \rfloor$ times in every column in A.

3. B is equitable on rows and equitable on columns: each of the s_2 symbols in S_2 appears $\lceil \frac{t}{s_2} \rceil$ or $\lfloor \frac{t}{s_2} \rfloor$ times in every row, and $\lceil \frac{r}{s_2} \rceil$ or $\lfloor \frac{r}{s_2} \rfloor$ times in every column in B.

4. A and B are orthogonal: the rt pairs $(a_{i,j}, b_{i,j}), 1 \le i \le r, 1 \le j \le t$ are all distinct.

We denote A and B as $(r, t; s_1, s_2)$-OGER.

Example 1.1 *A* $(2, 6; 3, 4)$-*OGER:*

1	1	2	2	3	3
2	2	3	3	1	1

1	2	1	2	3	4
3	4	2	1	4	3

□

An $(r, t; s_1, s_2)$-OGER is a generalization of a pair of orthogonal equitable rectangles, which are discussed in [4]. In fact, an $(r, t; r, t)$-OGER is the same thing as a pair of orthogonal equitable $r \times t$ rectangles. Furthermore, an $(r, r; r, r)$-OGER is just a pair of orthogonal latin squares of size r.

Stinson [4] gave an almost complete solution for the existence of orthogonal equitable rectangles. His solution only had a few possible exceptions, which were subsequently removed by Guo and Ge [2]. The following theorem summarizes these existence results.

Theorem 1.2 *There exists an $(r, t; r, t)$-OGER (i.e., a pair of orthogonal equitable $r \times t$ rectangles) if and only if $(r, t) \notin \{(2, 2), (2, 3), (3, 4), (6, 6)\}$.*

When $\{r, t\} \neq \{s_1, s_2\}$, orthogonal generalized equitable rectangles have no obvious cryptographic applications. However, their construction is a natural and interesting new problem in combinatorial designs. This problem at first glance seems difficult due to its generality: r, t, s_1, s_2 can be any positive integers that satisfy the equation $rt = s_1 s_2$. Despite the generality of the problem, we are able to completely solve it, using the result of Theorem 1.2 as a starting point, by applying three recursive constructions and three constructions of OGERs for individual parameter sets. The resulting solution is remarkably short.

2 Main Theorem

In this section, we prove our main theorem. We begin by stating two lemmas that indicate some "symmetric" properties of OGERs.

Lemma 2.1 *The following are equivalent:*

- *an* $(r, t; s_1, s_2)$*-OGER,*
- *an* $(r, t; s_2, s_1)$*-OGER,*
- *a* $(t, r; s_1, s_2)$*-OGER, and*
- *a* $(t, r; s_2, s_1)$*-OGER.*

Lemma 2.2 *There exists an* $(r, t; s_1, s_2)$*-OGER if and only if there exists an* $(s_1, s_2; r, t)$*-OGER.*

Proof. Suppose $A = (a_{i,j})$ and $B = (b_{i,j})$, where $1 \le i \le r, 1 \le j \le t$, form an $(r, t; s_1, s_2)$-OGER. Construct two $s_1 \times s_2$ rectangles $A' = (a'_{m,n})$ and $B' = (b'_{m,n})$, where $a'_{m,n} = i$ and $b'_{m,n} = j$ if and only if $(a_{i,j}, b_{i,j}) = (m, n)$. It is readily verified that A' and B' form an $(s_1, s_2; r, t)$-OGER. ∎

We will make essential use of the Kronecker product. Let $C = (c_{i,j})$ be an $r_1 \times t_1$ array, and let $D = (d_{i,j})$ be an $r_2 \times t_2$ array. Define an $r_1 r_2 \times t_1 t_2$ array $E = C \bigotimes D = (e_{i,j})$, where

$$e_{i,j} = (c_{n,q}, d_{m,p}), \text{ for } i = nr_2 + m, j = qt_2 + p, 0 \le m < r_2, 0 \le p < t_2.$$

E is the Kronecker product of C and D.

We now present the three recursive constructions we use.

Construction 2.3 *If there exists a* $(c, b; c, b)$*-OGER and a* $(d, a; a, d)$*-OGER, then there exists a* $(cd, ab; ac, bd)$*-OGER.*

Proof. We begin with two OGERs. The first is a $(c, b; c, b)$-OGER consisting of rectangles C and D and the second is a $(d, a; a, d)$-OGER consisting of rectangles E and F. Now let $A = C \bigotimes E$ and $B = D \bigotimes F$. We prove that A and B are the desired $(cd, ab; ac, bd)$-OGER.

For the ith row of A, where $i = nd + m$, the elements are $(c_{n,q}, e_{m,p}), 0 \le q < b, 0 \le p < a$. Since each symbol in C appears $\lceil \frac{b}{c} \rceil$ or $\lfloor \frac{b}{c} \rfloor$ times in a row and each symbol appears exactly once in a row of E, each pair of the symbols appears $\lceil \frac{b}{c} \rceil$ or $\lfloor \frac{b}{c} \rfloor$ times in a row of A. In a similar way we can check that conditions 2 and 3 of the definition are satisfied. Finally, it is straightforward to prove that A and B are orthogonal. ∎

Construction 2.4 *If there exists an* $(m, n; n, m)$*-OGER, where* $(m, n) \neq (1, 1)$*, then there exists an* $(2m, 3n; 2n, 3m)$*-OGER.*

Proof. First, suppose that $n \ge 2$. Suppose $A = (a_{i,j})$ and $B = (b_{i,j})$, where $1 \le i \le m, 1 \le j \le n$, are an $(m, n; n, m)$-OGER. Let A_1, A_2 be two copies of A using two different symbol sets and let B_1, B_2, B_3 be three copies of B using three different symbol sets. For an $m \times n$ matrix $X = (x_{i,j})$, let $X^1 = (x_{i,j})$, where $1 \le i \le m, 1 \le j \le \lceil \frac{n}{3} \rceil$, $X^2 = (x_{i,j})$, where $1 \le i \le m, \lceil \frac{n}{3} \rceil + 1 \le j \le 2\lceil \frac{n}{3} \rceil$, and the remainder of X as X^3. Observe that X^1 and X^2 always have the same width. X^3 has the same width as X^1 and X^2 when $n \equiv 0 \bmod 3$; when $n \not\equiv 0 \bmod 3$, X^3 is narrower than both X^1 and X^2.

Construct two $2m \times 3n$ matrices C and D as follows:

$C =$

A_1	A_2	A_1
A_2	A_1^2, A_1^3, A_1^1	A_2

$D =$

B_1^1, B_2^2, B_3^3	B_2^1, B_3^2, B_1^3	B_3^1, B_1^2, B_2^3
B_3^1, B_1^2, B_2^3	B_3^2, B_1^3, B_2^1	B_1^1, B_2^2, B_3^3

In the above diagram, commas indicate matrices that are placed side by side.

It is easy to see that C and D form an $(2m, 3n; 2n, 3m)$-OGER. The only tricky part is to check the alignment of the following subarrays of D (these subarrays will not be perfectly aligned when $n \not\equiv 0 \bmod 3$):

B_3^2, B_1^3
B_1^3, B_2^1

The important point is that there is no overlap of the two occurrences of B_1^3.

When $n = 1$, the construction given above does not work. But this does not cause any difficulties. Note that the hypotheses require that $m > 1$ when $n = 1$. Using the fact that an $(m, 1; 1, m)$-OGER is equivalent to a $(1, m; m, 1)$-OGER (Lemma 2.1), we can construct a $(2, 3m; 2m, 3)$-OGER by the method described above. By Lemma 2.2, this is equivalent to a $(2m, 3; 2, 3m)$-OGER. ∎

Similarly, we have the following construction.

Construction 2.5 *If there exists an $(m, n; n, m)$-OGER, where $(m, n) \neq (1, 1)$, then there exists an $(3m, 4n; 3n, 4m)$-OGER.*

Proof. Suppose $A = (a_{i,j})$ and $B = (b_{i,j})$, where $1 \le i \le m, 1 \le j \le n$, are an $(m, n; n, m)$-OGER. Let A_1, A_2, A_3 be three copies of A using three different symbol sets and let B_1, B_2, B_3, B_4 be four copies of B using four different symbol sets. For an $m \times n$ matrix $X = (x_{i,j})$, denote $X = X^1X^2X^3$ as in the proof of Construction 2.4.

Construct two $3m \times 4n$ rectangles C and D as follows:

$C =$

A_1	A_2	A_3	A_1
A_2^1, A_2^3, A_2^2	A_3	A_1	A_2
A_3^2, A_3^3, A_3^1	A_1	A_2	A_3

$D =$

B_1^1, B_2^2, B_3^3	B_2^1, B_3^2, B_4^3	B_3^1, B_4^2, B_1^3	B_4^1, B_1^2, B_2^3
B_3^1, B_1^3, B_4^2	B_4^1, B_1^2, B_2^3	B_2^1, B_3^2, B_4^3	B_1^1, B_2^2, B_3^3
B_2^2, B_3^3, B_1^1	B_3^1, B_4^2, B_1^3	B_4^1, B_1^2, B_2^3	B_2^1, B_3^2, B_4^3

It is simple to show that C and D form an $(3m, 4n; 3n, 4m)$-OGER. As in the proof of Lemma 2.4, there are certain subarrays of D that are not perfectly aligned when $n \not\equiv 0 \bmod 3$:

B_2^2, B_3^3
B_1^3, B_4^2
B_3^3, B_1^1

It is easy to check that there is no overlap of the two occurrences of B_3^3, nor is there an overlap of B_1^3 and B_1^1.

The case $n = 1$ is handled as in Construction 2.4. ∎

Example 2.6 *We illustrate the application of Construction 2.5 with $m = 1$, $n = 4$. The following arrays A and B form a $(1, 4; 4, 1)$-OGER:*

$$A = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline\end{array} \qquad B = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline\end{array}$$

Then A^1, A^2, B^1 and B^2 have width 2, while A^3 and B^3 are empty.

We construct C and D, which form a $(3, 16; 12, 4)$-OGER;

$$C = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & a & b & c & 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 & 9 & a & b & c & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline b & c & 9 & a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & a & b & c \\ \hline\end{array}$$

$$D = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 1 & 1 \\ \hline 3 & 3 & 4 & 4 & 4 & 4 & 1 & 1 & 2 & 2 & 3 & 3 & 1 & 1 & 2 & 2 \\ \hline 2 & 2 & 1 & 1 & 3 & 3 & 4 & 4 & 4 & 4 & 1 & 1 & 2 & 2 & 3 & 3 \\ \hline\end{array}$$

□

Construction 2.7 *There exist a $(6, 6; 4, 9)$-OGER, a $(6, 12; 8, 9)$-OGER and a $(12, 12; 9, 16)$-OGER.*

Proof. These three OGERs are each constructed using a similar technique. For positive integers r and s, define $c = \mathrm{lcm}(r, s)/r$. Then define an $r \times c$ array $D_{r,s}$ having entries $d_{i,j} = jr + i \bmod s$, $0 \leq j \leq c - 1$, $0 \leq i \leq r - 1$. Suppose that $c|t$, and define $E_{r,t,s}$ to consist of t/c copies of $D_{r,s}$ placed side by side.

Next, suppose that $\pi \in (\mathbb{Z}_r)^t$ and construct $\pi(E_{r,t,s})$ from $E_{r,t,s}$ by rotating column j of $E_{r,t,s}$ upwards cyclically by $\pi(j)$ positions, for $j = 0, \ldots, t - 1$.

It can be verified that the following arrays form the desired OGERs:

- $\pi(E_{6,6,4})$ and $\pi(E_{6,6,9})$, where $\pi = (0, 0, 1, 1, 2, 2)$.
- $\pi(E_{6,12,8})$ and $\pi(E_{6,12,9})$, where $\pi = (0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2)$.
- $\pi(E_{12,12,9})$ and $\pi(E_{12,12,16})$, where $\pi = (0, 0, 0, 1, 1, 1, 2, 2, 2, 3, 3, 3)$.

□

Example 2.8 *We illustrate the construction of a $(6, 6; 4, 9)$-OGER. First, we depict $E_{6,6,4}$ and $E_{6,6,9}$:*

$$\begin{array}{|c|c|c|c|c|c|}\hline 0 & 2 & 0 & 2 & 0 & 2 \\ \hline 1 & 3 & 1 & 3 & 1 & 3 \\ \hline 2 & 0 & 2 & 0 & 2 & 0 \\ \hline 3 & 1 & 3 & 1 & 3 & 1 \\ \hline 0 & 2 & 0 & 2 & 0 & 2 \\ \hline 1 & 3 & 1 & 3 & 1 & 3 \\ \hline\end{array} \qquad \begin{array}{|c|c|c|c|c|c|}\hline 0 & 6 & 3 & 0 & 6 & 3 \\ \hline 1 & 7 & 4 & 1 & 7 & 4 \\ \hline 2 & 8 & 5 & 2 & 8 & 5 \\ \hline 3 & 0 & 6 & 3 & 0 & 6 \\ \hline 4 & 1 & 7 & 4 & 1 & 7 \\ \hline 5 & 2 & 8 & 5 & 2 & 8 \\ \hline\end{array}$$

It is not hard to verify that these arrays are orthogonal, and each of them is equitable on columns. Now apply the column rotations specified by π to these two arrays:

0	2	1	3	2	0
1	3	2	0	3	1
2	0	3	1	0	2
3	1	0	2	1	3
0	2	1	3	0	2
1	3	0	2	1	3

0	6	4	1	8	5
1	7	5	2	0	6
2	8	6	3	1	7
3	0	7	4	2	8
4	1	8	5	6	3
5	2	3	0	7	4

It can be verified that the resulting arrays are now orthogonal, equitable on rows and equitable on columns. Therefore we have a $(6, 6; 4, 9)$-OGER. $\square$

At this point, we are in a position to prove our main result.

Theorem 2.9 *Suppose r, t, s_1 and s_2 are positive integers such that $rt = s_1 s_2$. Then there exists an $(r, t; s_1, s_2)$-OGER if and only if $(r, t; s_1, s_2) \notin \{(2, 2; 2, 2), (2, 3; 2, 3), (3, 4; 3, 4), (6, 6; 6, 6)\}$.*

Proof. Let $b = \gcd(t, s_2)$, $a = t/b$, $d = s_2/b$ and $c = r/d$. Then $\gcd(a, d) = 1$. It is clear that a, b and d are integers; we prove now that c is also an integer. Since $rt = s_1 s_2$, we have

$$c = \frac{r}{d} = \frac{rt}{dt} = \frac{s_1 s_2}{dt} = \frac{s_1 bd}{dba} = \frac{s_1}{a}.$$

On the other hand,

$$\frac{s_1 d}{a} = \frac{s_1 db}{ab} = \frac{s_1 s_2}{ab} = \frac{s_1 s_2}{t} = r$$

is an integer. From the fact that $\gcd(a, d) = 1$, it follows that $c = s_1/a$ is an integer.

Therefore we have that $(r, t; s_1, s_2) = (cd, ab; ac, bd)$, where a, b, c and d are positive integers. By Construction 2.3, if there exist a $(c, b; c, b)$-OGER and a $(d, a; a, d)$-OGER, then there exists an $(r, t; s_1, s_2)$-OGER. So we just need to consider the exceptions from Theorem 1.2.

We consider three cases, as follows.

1. There is a $(c, b; c, b)$-OGER, where c and b are not both equal to one, but a $(d, a; a, d)$-OGER does not exist. For $(d, a; a, d) = (2, 2; 2, 2)$ or $(6, 6; 6, 6)$, the designs are constructed in Theorem 1.2. For $(d, a; a, d) = (2, 3; 3, 2)$ or $(3, 4; 4, 3)$, the designs are constructed in Constructions 2.4 and 2.5.

2. There is a $(d, a; a, d)$-OGER, where d and a are not both equal to one, but a $(c, b; c, b)$-OGER does not exist. This is equivalent to case 1, by Lemma 2.1.

3. Both $(c, b; c, b)$-OGER and $(d, a; a, d)$-OGER do not exist. When one of the missing OGERs is of type $(2, 2; 2, 2)$ or $(6, 6; 6, 6)$, then the designs are constructed in Theorem 1.2. So we just need to consider the exceptions $(2, 3; 2, 3)$ and $(3, 4; 3, 4)$. Using Lemmas 2.2 and 2.1, there are three types of OGERs that we need to construct: $(6, 6; 4, 9), (6, 12; 8, 9)$, and $(12, 12; 9, 16)$. These were handled in Construction 2.7.

$\square$

References

[1] C.J. Colbourn and J. H. Dinitz. *The CRC Handbook of Combinatorial Designs, Second Edition.* Chapman & Hall/CRC Press, 2007.

[2] W. Guo and G. Ge. The existence of generalized mix functions. *Designs Codes and Cryptography*, to appear.

[3] T. Ristenpart and P. Rogaway. How to enrich the message space of a cipher. *Lecture Notes in Computer Science* **4593** (2007), 101–118 (Fast Software Encryption, FSE 2007).

[4] D. R. Stinson. Generalized mix functions and orthogonal equitable rectangles. *Designs Codes and Cryptography*, **45** (2007), 347–357.