Discrete Mathematics 16 (1976) 263–270.

ON CERTAIN CONSTRUCTIONS FOR LATIN SQUARES WITH NO LATIN SUBSQUARES OF ORDER TWO

Anton KOTZIG*

Centre de recherches mathématiques, Université de Montréal, Montréal, Québec, Canada

Jean TURGEON**

Département de mathématiques, Université de Montréal, Montréal, Québec, Canada

Received 18 November 1974
Revised 13 January 1976

A latin square is said to be an N_2-latin square (see [1] and [2]) if it contains no latin subsquare of order 2. The existence of N_2-latin squares of all orders except 2^k has been proved in [2]. Trivially, there are no such squares of orders 2 and 4. M. McLeish [3] has shown that there exist N_2-latin squares of all orders 2^k for $k \geqslant 6$. The present paper introduces a construction for N_2-latin squares of all even orders n with $n \not\equiv 0 \pmod 3$ and $n \not\equiv 3 \pmod 5$. The problem is thus solved for the orders 2^4 and 2^5.

For 2^3, the only remaining case, Eric Regener of the Faculty of Music, Université de Montréal, has constructed the following example of an N_2-latin square and kindly granted us the permission to reproduce it here:

$$\begin{matrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
2 & 3 & 1 & 5 & 6 & 7 & 8 & 4 \\
3 & 1 & 4 & 6 & 7 & 8 & 2 & 5 \\
4 & 6 & 8 & 2 & 1 & 3 & 5 & 7 \\
5 & 8 & 2 & 7 & 3 & 4 & 6 & 1 \\
6 & 5 & 7 & 1 & 8 & 2 & 4 & 3 \\
7 & 4 & 5 & 8 & 2 & 1 & 3 & 6 \\
8 & 7 & 6 & 3 & 4 & 5 & 1 & 2
\end{matrix}$$

The existence problem of N_2-latin squares is thus completely solved.

1. Definitions. Introductory remarks

Let n be a positive integer. Unless otherwise stated, all congruences shall be taken modulo n. So we shall write $x \equiv y$ for $x \equiv y \pmod n$.

The $n \times n$ matrix $X = (x_{ij})$ with $x_{ij} \in M = \{1, 2, \ldots, n\}$ and $x_{ij} \equiv i + j$, which is the Cayley table of the cyclic group of order n, shall be called in this paper the

* Research supported by Grant DGES-FCAC-74.
** Research supported by Grant NRCC-A7869.

C_n-*matrix*. A C_n-matrix is obviously an N_2-latin square if and only if n is odd (see [2], Lemma 1).

We shall denote by $D(m, n)$ the greatest common divisor of m and n.

Let $g < n$ be a positive integer with the property that $D(g, n) = D(g+1, n) = 1$. We denote by

$$E_{g,k}(X) = (l_{k,1}, l_{k,2}, \ldots, l_{k,n}), \qquad k = -1, 0, 1$$

the sequence of n entries of the C_n-matrix X defined by

$$l_{k,j} = x_{g(j-k)-k,j}, \qquad j = 1, 2, \ldots, n,$$

the first index being taken modulo n in M. Since X is the C_n-matrix, we have

$$\begin{aligned} l_{k,j} &\equiv [g(j-k)-k]+j \\ &\equiv (g+1)(j-k). \end{aligned} \tag{1.1}$$

Theorem 1.1. *The sequences $E_{g,-1}(X)$, $E_{g,0}(X)$ and $E_{g,1}(X)$ are disjoint transversals of the C_n-matrix X, i.e. each row and each column of X contains exactly one element of $E_{g,k}(X)$ and $E_{g,k}(X)$ is a permutation of M, for each $k = -1, 0, 1$, and $l_{-1,j}$, $l_{0,j}$ and $l_{1,j}$ are distinct for each $j = 1, 2, \ldots, n$.*

Proof. We have

$$l_{k,j+1} - l_{k,j} \equiv g+1; \qquad j = 1, \ldots, n; \qquad k = -1, 0, 1. \tag{1.2}$$

Since $D(g+1, n) = 1$, $E_{g,k}(X)$ is thus a permutation of M for each $K = -1, 0, 1$.

Now the sequence $\{g(j-k)-k\}$ of the first indices is an arithmetic progression of ratio g. Since $D(g, n) = 1$, each row of X contains exactly one element of $E_{g,k}(X)$; $k = -1, 0, 1$. The same is obviously true of the columns of X.

Finally, by (1.1),

$$l_{-1,j} \equiv (g+1)(j+1), \qquad l_{0,j} \equiv (g+1)j, \qquad l_{1,j} \equiv (g+1)(j-1)$$

so that the three are distinct, for each $j = 1, \ldots, n$, since $D(g+1, n) = 1$.

Definition 1.2. Let T_* be the set of the twelve distinct latin squares of order 3. Let $T = (t_{ij}) \in T_*$. Let $g < n$, $D(g, n) = D(g+1, n) = 1$. We shall say that the $(n+3) \times (n+3)$ matrix $Y = t_g(T, X)$ is obtained by a $t_g(T)$-*extension* of the C_n-matrix X if it is obtained from X in the following way.

1.2.1. Each entry of X which belongs to $E_{g,k}(X)$, $k = -1, 0, 1$, is replaced in Y by the number $n+2+k$ (i.e. $y_{g(j-k)-k,j} = n+2+k$, the first index being taken modulo n in M) and the others are left untouched (i.e. $y_{a,b} = x_{a,b}$ if $x_{a,b}$ does not belong to any of the transversals $E_{g,k}(X)$, $k = -1, 0, 1$).

1.2.2. If $x_{a,b}$ of X is replaced in Y by $n+2+k$ according to 1.2.1, then

$$y_{a,n+2+k} = y_{n+2-k,b} = x_{a,b}.$$

1.2.3. $y_{n+i,n+j} = n + t_{ij}$; $i, j \in \{1,2,3\}$.

It is clear from 1.1 that this construction yields a latin square of order $n+3$ with entries in $\{1,2,\dots,n+3\}$.

1.3. If $n = 3$, a $\tau_g(T)$-extension of the C_n-matrix is only possible for $g = 1$. We obtain

$$Y = \tau_1(T, X) = \tau_1\left(T, \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{bmatrix}\right)$$

$$= \left[\begin{array}{ccc|ccc} 5 & 4 & 6 & 3 & 2 & 1 \\ 6 & 5 & 4 & 2 & 1 & 3 \\ 4 & 6 & 5 & 1 & 3 & 2 \\ \hline 3 & 2 & 1 & & & \\ 2 & 1 & 3 & & (3+t_{ij}) & \\ 1 & 3 & 2 & & & \end{array}\right].$$

We shall denote the twelve latin squares of T_* as follows:

$$\begin{matrix} 1\,2\,3 & 2\,3\,1 & 3\,1\,2 & 3\,2\,1 & 2\,1\,3 & 1\,3\,2 \\ 3\,1\,2 & 1\,2\,3 & 2\,3\,1 & 1\,3\,2 & 3\,2\,1 & 2\,1\,3 \\ 2\,3\,1 & 3\,1\,2 & 1\,2\,3 & 2\,1\,3 & 1\,3\,2 & 3\,2\,1 \\ T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \\ 2\,3\,1 & 3\,1\,2 & 1\,2\,3 & 2\,1\,3 & 1\,3\,2 & 3\,2\,1 \\ 3\,1\,2 & 1\,2\,3 & 2\,3\,1 & 1\,3\,2 & 3\,2\,1 & 2\,1\,3 \\ 1\,2\,3 & 2\,3\,1 & 3\,1\,2 & 3\,1\,2 & 2\,1\,3 & 1\,3\,2 \\ T_7 & T_8 & T_9 & T_{10} & T_{11} & T_{12} \end{matrix}$$

For $n = 3$, one can easily show that Y is an N_2-latin square if and only if T is T_4 or T_6. This settles the case $n = 3$.

In general, the conditions $n > 2$, $g > 0$ and $D(g, n) = D(g+1, n) = 1$ imply that n is odd. So we shall assume in the sequel that n is odd and greater than 3.

2. N_2-latin squares obtained by $\tau_g(T)$-extensions

Theorem 2.1. *Let g and n be integers, $1 < g < n$. Suppose*

$$D(g-1, n) = D(g, n) = D(g+1, n) = D(g+2, n) = D(2g+1, n) = 1.$$

Let $T \in \{T_4, T_6\}$ and let X be the C_n-matrix. Then $Y = \tau_g(T, X)$ is an N_2-latin square.

For the proof of Theorem 2.1 we shall need the following lemma.

2.2. *Let g and n be integers such that $0 < g < n$ and $D(g, n) = D(g+1, n) = 1$. Let $T \in \{T_4, T_6\}$ and let X be the C_n-matrix. Let $M = \{1, 2, \ldots, n\}$ and $W = \{n+1, n+2, n+3\}$. Suppose $Y = \tau_g(T, X)$ has a subsquare Z with entries*

$$y_{p,r} = y_{q,s} = u \quad \text{and} \quad y_{p,s} = y_{q,r} = v.$$

Then the following five assertions are true.

(1) *If $p, q, r, s \in M$, then either $g = 1$ or $g > 1$ and $D(g-1, n) > 1$.*
(2) *If $p, q, r, \in M$ and $s \in W$, then $D(2g+1, n) > 1$.*
(3) *If $p, r, s, \in M$ and $q \in W$, then $D(g+2, n) > 1$.*
(4) $|\{p, r\} \cap M| \cdot |\{q, s\} \cap W| < 4$.
(5) $|\{p, q\} \cap M| \cdot |\{r, s\} \cap M| > 0$.

Proof of 2.2(1). Since X is an N_2-latin square, at most one of u and v is in M. Hence at least one of u and v, say $v = n + 2 + k$, is in W. So

$$p \equiv g(s-k) - k \quad \text{and} \quad q \equiv g(r-k) - k. \tag{2.1}$$

Suppose $u \in W$. Then $u = n + 2 + h$ for some $h \neq k$, $h \in \{-1, 0, 1\}$. So

$$p \equiv g(r-h) - h \quad \text{and} \quad q \equiv g(s-h) - h. \tag{2.2}$$

From (2.1) and (2.2) we obtain

$$g(h-k) + h - k \equiv p - q \equiv g(k-h) + k - h$$

or $2(p-q) \equiv 0$. Hence $(p-q) \equiv 0$, since n is odd, and the supposition that $u \in W$ leads to a contradiction. So $u \in M$ and

$$u = y_{p,r} = x_{p,r} = p + r \quad \text{and} \quad u = y_{q,s} = x_{q,s} = q + s$$

so that $p + r \equiv q + s$, i.e. $p - q \equiv s - r$. From (2.1) we obtain

$$(g-1)(s-r) \equiv 0. \tag{2.3}$$

Since $(s-r) \not\equiv 0$, (2.3) is only possible if either $g = 1$ or $g > 1$ and $D(g-1, n) > 1$.

Proof of 2.2(2). Since $s \in W$, both $y_{q,s}$ and $y_{p,s}$ are in M, so that $\{u, v\} \subset M$; cf. 1.2.2. Hence

$$u = y_{p,r} = x_{p,r} \equiv p + r \quad \text{and} \quad v = y_{q,r} = x_{q,r} \equiv q + r \tag{2.4}$$

and there exist indices t and w in M such that

$$q + w \equiv u \quad \text{and} \quad p + t \equiv v \tag{2.5}$$

and such that $x_{p,t}$ and $x_{q,w}$ are replaced in Y by $n + 2 + k$, $k \in \{-1, 0, 1\}$. But then

$$g(t - k) - k \equiv p \quad \text{and} \quad g(w - k) - k \equiv q. \tag{2.6}$$

Replacing w and t in (2.6) according to the congruences

$$w \equiv p - q + r \quad \text{and} \quad t \equiv -p + q + r$$

which follow from (2.4) and (2.5), we obtain

$$g(-p + q + r - k) - k \equiv p \quad \text{and} \quad g(p - q + r - k) - k \equiv q.$$

Hence

$$(2g + 1)(q - p) \equiv 0,$$

which is only possible if $D(2g + 1, n) > 1$.

Proof of 2.2(3). Since $q \in W$, we have $\{y_{q,s}, y_{q,r}\} \subset M$, so that $\{u, v\} \subset M$ and

$$u = y_{p,r} = x_{p,r} \equiv p + r \quad \text{and} \quad v = y_{p,s} = x_{p,s} = p + s. \tag{2.7}$$

Also, $q = n + 2 - k$ for some $k \in \{-1, 0, 1\}$. Suppose $x_{a,r}$ and $x_{b,s}$ are replaced in Y by $n + 2 + k$. Then

$$a \equiv g(r - k) - k \quad \text{and} \quad b \equiv g(s - k) - k. \tag{2.8}$$

Also,

$$u \equiv b + s \quad \text{and} \quad v \equiv a + r. \tag{2.9}$$

From (2.7) and (2.9) we obtain

$$a \equiv p - r + s \quad \text{and} \quad b \equiv p + r - s$$

so that, by (2.8),

$$g(r - k) - k \equiv p - r + s \quad \text{and} \quad g(s - k) - k \equiv p + r - s.$$

Hence $(g + 2)(s - r) \equiv 0$ and $D(g + 2, n) > 1$.

Proof of 2.2(4). Suppose $p, r \in M$ and $q, s \in W$. Then

$$u = y_{q,s} = n + 2 + k \tag{2.10}$$

for some $k \in \{-1, 0, 1\}$ (cf. 1.2.3) and $u \in W$. Since $p \in M$, $s \in W$, we have $v \in M$ (cf. 1.2.2).

It follows from the definition of $l_{k,l}$ that if $x_{a,b}$ is replaced in Y by $n + 2$, then $x_{a+1,b-1}$ is replaced by $n + 1$ and $x_{a-1,b+1}$ is replaced by $n + 3$ (all indices being taken modulo n in M). Then Y contains the entries y_{ij} ordered as follows:

$i =$ \ $j =$	$b-1$	b	$b+1$	$\cdots$	$n+1$	$n+2$	$n+3$
$a-1$	$\cdot$	$\cdot$	$n+3$	$\cdots$	$z-2\eta$	$z-\eta$	z
a	$\cdot$	$n+2$	$\cdot$	$\cdots$	$z-\eta$	z	$z+\eta$
$a+1$	$n+1$	$\cdot$	$\cdot$	$\cdots$	z	$z+\eta$	$z+2\eta$
$\cdot$	$\cdot$	$\cdot$	$\cdot$		$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$		$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$		$\cdot$	$\cdot$	$\cdot$
$n+1$	$z-2\varepsilon$	$z-\varepsilon$	z	$\cdots$	$n+t_{1,1}$	$n+t_{1,2}$	$n+t_{1,3}$
$n+2$	$z-\varepsilon$	z	$z+\varepsilon$	$\cdots$	$n+t_{2,1}$	$n+t_{2,2}$	$n+t_{2,3}$
$n+3$	z	$z+\varepsilon$	$z+2\varepsilon$	$\cdots$	$n+t_{3,1}$	$n+t_{3,2}$	$n+t_{3,3}$

where $z \equiv a+b$ and $\varepsilon \equiv g+1$; cf. (1.2). To determine η, we note that the entry of the line $a+1$ of X which is replaced by $n+2$ is $x_{a+1,b+c}$ where $cg \equiv 1$ (since the sequence $(g(j-k)-k)$ of the first indices of the elements of $E_{g,k}$ is an arithmetic progression, modulo n, of ratio g). The value of this entry is

$$x_{a+1,b+c} \equiv a+b+c+1 \equiv z+\eta$$

where $\eta \equiv c+1$ and $(\eta-1)g \equiv 1$, i.e.

$$\eta g \equiv g+1. \tag{2.11}$$

Clearly, $\varepsilon \not\equiv 0$, $\eta \not\equiv 0$ and $\{\varepsilon, \eta\} \subset M$. Each replaced entry, and hence the entry $y_{p,r}$ belongs to exactly one triple $\{y_{a-1,b+1}, y_{a,b}, y_{a+1,b-1}\}$. Thus

$$z \notin \{z-2\varepsilon, z-\varepsilon, z+\varepsilon, z+2\varepsilon, z-2\eta, z-\eta, z+\eta, z+2\eta\}. \tag{2.12}$$

Since $T \in \{T_4, T_6\}$, we have

$$1 \notin \{t_{1,2}, t_{2,3}, t_{3,1}\} \tag{2.13}$$

$$2 \notin \{t_{1,1}, t_{2,2}, t_{3,3}\} \tag{2.14}$$

and

$$3 \notin \{t_{1,3}, t_{2,1}, t_{3,2}\}. \tag{2.15}$$

If $u = n+1$, then $p = a+1$, $r = b-1$ and, by (2.12) and (2.13), either $q = s = n+2$ or $q = n+1$ and $s = n+3$; in both cases,

$$\varepsilon + \eta \equiv 0. \tag{2.16}$$

If $u = n+2$, then $p = a$, $r = b$ and, by (2.12) and (2.14), either $q = n+3$, $s = n+1$ or $q = n+1$, $s = n+3$ and (2.16) holds again. Finally, if $u = n+3$, then $p = a-1$, $r = b+1$ and, by (2.12) and (2.15), either $q = n+3$, $s = n+1$ or $q = s = n+2$ and we have again (2.16). So, in all cases,

$$\eta \equiv -(g+1) \tag{2.17}$$

By adding the respective sides of (2.11) and (2.17) we obtain $\eta(g+1) \equiv 0$. But this is not possible since $D(g+1, n) = 1$ and $0 < \eta < n$.

Proof of 2.2(5). We have to show that at least one number of $\{p, q\}$ and at least one of $\{r, s\}$ belongs to M. Suppose on the contrary that $\{p, q\} \subset W$. Then

$$m = |\{r, s\} \cap M| \neq 0$$

because T is an N_2-latin square. If $m = 1$, say $r \in M$, $s \in W$, then $\{y_{p,r}, y_{q,r}\} \subset M$ whereas $\{y_{p,s}, y_{q,s}\} \subset W$; so $m \neq 1$. Finally, $m \neq 2$ because the submatrix $Y' = (y_{ij})$ with $i \in W$, $j \in M$ is isomorphic to a submatrix of the C_n-matrix consisting of three of its rows. Therefore $\{p, q\} \cap M \neq \emptyset$. By the same argument, $\{r, s\} \cap M \neq \emptyset$.

Proof of 2.1. Suppose Y has a subsquare Z with entries

$$u = y_{p,r} = y_{q,s} \quad \text{and} \quad v = y_{p,s} = y_{q,r}.$$

Then, by 2.2(5),

$$|\{p, q\} \cap M| \cdot |\{r, s\} \cap M| > 0.$$

The case

$$|\{p, q\} \cap M| = |\{r, s\} \cap M| = 1$$

is not possible, by 2.2(4). The case

$$|\{p, q\} \cap M| = 2, \qquad |\{r, s\} \cap M| = 1$$

is excluded by 2.2(2), since $D(2g+1, n) = 1$, and

$$|\{p, q\} \cap M| = 1, \qquad |\{r, s\} \cap M| = 2$$

is excluded by 2.2(3), since $D(g+2, n) = 1$. Finally, since $D(g-1, n) = 1$ and $g > 1$, 2.2(1) excludes the case

$$|\{p, q\} \cap M| = |\{r, s\} \cap M| = 2.$$

Therefore Y is an N_2-latin square.

2.3. It can be proved that all the conditions stated in 2.1 are necessary for $Y = \tau_g(T, X)$ to be an N_2-latin square, i.e. that if any of g, n or T does not satisfy one of the conditions stated then Y contains a subsquare Z of order 2 (the type of Z depending on the missing property). This assertion is made without proof because it is not necessary for what follows.

3. The effectiveness of the method

Let g be an integer, $g > 1$. Let P_g be the set of all integers $n > 3$ such that the $\tau_g(T_4)$- and $\tau_g(T_6)$-extensions of the C_n-matrix are N_2-latin squares. By 2.1, $n \in P_g$ if $1 < g < n-2$ and

$$D(g-1, n) = D(g, n) = D(g+1, n) = D(g+2, n) = D(2g+1, n) = 1.$$

In particular, $n \in P_g$ must be odd and not divisible by 3 or 5.

Theorem 3.1. *P_2 contains every odd integer $m > 1$ which is not divisible by 3 or 5.*

Proof. By assumption,

$$D(1, m) = D(2, m) = D(3, m) = D(4, m) = D(5, m) = 1.$$

Hence, by 2.1, the $\tau_2(T_4)$- and $\tau_2(T_6)$-extensions of the C_m-matrix are N_2-latin squares and $m \in P_2$.

Theorem 3.2. *$P_g \subset P_2$ for every integer $g > 2$.*

Proof. This follows from 3.1 and the discussion preceding it.

3.3. In spite of 3.2, the study of $\tau_g(T)$-extensions can still be useful for $g > 2$. Such $\tau_g(T)$-extensions cannot give N_2-latin squares of orders that cannot be obtained by $\tau_2(T)$-extensions, but can give new non-isomorphic N_2-latin squares.

Theorem 3.4. *Let h be an integer, $h > 3$, $h \not\equiv 3 \pmod 4$. Let $n = 2^h - 3$. Then the $\tau_2(T_4)$- and $\tau_2(T_6)$-extensions of the C_n-matrix are N_2-latin squares.*

Proof. Clearly, $2^h - 3$ is odd and not divisible by 3. Also, $2^h - 3$ is divisible by 5 if and only if $h \equiv 3 \pmod 4$. Therefore, by 3.1, $2^h - 3 \in P_2$.

3.5. It follows from 3.4 that N_2-latin squares of orders 2^4 and 2^5 can be obtained by $\tau_2(T)$-extensions. Since $2^4 - 3 = 13$ and $2^5 - 3 = 29$ are prime numbers, the conditions of 2.1 are also satisfied by other values of g, and we obtain several non-isomorphic solutions for the orders 2^4 and 2^5. Note that $\tau_g(T)$-extensions also provide a simple method of construction for many other cases.

References

[1] J. Dénes and A.D. Keedwell, Latin Squares and their Applications (Academic Press, New York, 1974).

[2] A. Kotzig, C.C. Lindner and A. Rosa, Latin squares with no latin squares of order two and disjoint Steiner triple systems, Utilitas Mathematica 7 (1975) 287–294.

[3] M. McLeish, On the existence of latin squares with no subsquares of order two (submitted for publication).