The number of mates of latin squares of sizes 7 and 8*

Megan Bryant James Figler Roger Garcia
Carl Mummert† Yudhishthir Singh

Preprint: March 3, 2013

Abstract

We study the number of mates that a latin square may possess as a function of the size of the square. An exhaustive computer search of all squares of sizes 7 and 8 was performed, giving the exact value for the maximum number of mates for squares of these sizes. The squares of size 8 with the maximum number of mates are exactly the Cayley tables of $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and each such square has $70,272 \cdot 8!$ mates. We obtain a combinatorial proof that, for every $k \geq 2$, the square obtained from a Cayley table of $\mathbb{Z}_2^k$ has a mate.

1 Introduction

Orthogonal latin squares are well established in the literature, with significant previous research focusing on sets of mutually orthogonal latin squares (MOLS) [1] and on latin squares with few mates [2, 5]. To our knowledge, no attempt has been made to count the total number of mates that a latin square may possess, in terms of its size, or to calculate the frequency distribution of latin squares of a fixed size by the number of mates they possess. We begin to address these questions via computational data and theoretical results.

We conducted an exhaustive computational search of all reduced squares of sizes 7 and 8 in which we counted the number of mates for each square. The software used to perform this search, and the results, are described in

*This research was partially supported by NSF grants OCI-1005117 and EPS-0918949.

†*Address:* Department of Mathematics, Marshall University, One John Marshall Drive, Huntington, WV 25755. *Email:* mummertc@marshall.edu

Section 3. A result of particular interest is that the squares of size 8 with the most mates are product squares of the form $C_2^3 = C_2 \otimes C_2 \otimes C_2$, where C_2 is a cyclic square of size 2. In Section 4, we present a combinatorial construction that produces a mate of C_2^n for each $n \geq 2$.

The research presented here was conducted during two summers in the Marshall University Computational Science Research Experience for Undergraduates (REU). The second and fifth authors were student participants during summer 2011. They wrote software and conducted several computational experiments including the survey of squares of size 7. The first and third authors were student participants during summer 2012. They extended the software to conduct the survey of squares of size 8 and developed the construction presented in Section 4. The third author served as the faculty advisor for this project during both summers. We would like to thank Michael Schroeder for careful proofreading of a preprint of this paper.

2 Background

In this section, we summarize the definitions and notation needed for the remainder of the paper. Dénes and Keedwell [1], Laywine and Mullen [3], and Mullen and Mummert [4] provide more detailed introductions to the subject.

A *latin square* of size n is an array of size $n \times n$ with n symbols each of which appears exactly once in each row and each column. By convention, we take the symbols to be $1, 2, \ldots, n$. A *cyclic latin square* of size n is formed by filling the first row with symbols in any order. The next row is filled by shifting all of the symbols right one place and moving the first symbol to the end. The subsequent rows are filled by continuing in this way, with each row shifted one place to the left of the previous row. For example, the following square, C_4, is a cyclic square of size 4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

C_4

Latin squares A and B of the same size are *orthogonal*, and are called *mates*, if every possible ordered pair of their symbols is present when the squares are superimposed. By definition, the superimposed square $A \wr B$ has at location (i, j) the ordered pair consisting of $A_{i,j}$ and $B_{i,j}$. For example,

the latin squares P and Q shown below are orthogonal, because the square $P \wr Q$ obtained by superimposing them has all nine ordered pairs from the set $\{1, 2, 3\}$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}$$

$$P \qquad\qquad Q \qquad\qquad P \wr Q$$

A latin square with symbols $1, 2, \ldots n$ is said to be *reduced* if the first row and the first column are in the natural order $1, \ldots, n$. In the remainder of this paper, we will let C_n denote the unique reduced cyclic square of size n.

An arbitrary latin square may be put in reduced form by permuting the columns, to put the first row in order, and then permuting the rows to put the first column in order. If the rows and columns of two orthogonal latin squares are permuted in the same way, the resulting squares are also orthogonal. Thus each reduced latin square of size n represents $n!(n-1)!$ distinct latin squares, which all have the same number of mates as the reduced square.

We define a latin square to be *semireduced* if the first row is in the natural order, with no restriction on the first column. If squares A and B are orthogonal, and A is kept fixed while the symbols of B are permuted, each such permutation gives another mate of A, and exactly one of these mates is semireduced. Thus a latin square of size n with s semireduced mates will have $s \cdot n!$ mates overall.

The *Kronecker product* produces a latin square from two smaller latin squares. Suppose that A is an $n \times n$ latin square and B is an $m \times m$ latin square. The *product square* $A \otimes B$ is formed in the following way. The columns and rows of $A \times B$ are labeled with ordered pairs (i, j) in dictionary order, where $1 \leq i \leq n$ and $1 \leq j \leq m$. Then the content of a cell $((i, j), (k, l))$ of $A \otimes B$ is defined to be the pair consisting of $A_{i,k}$ and $B_{j,l}$. For example, the product of the squares C_2 and C_3 is is the 6×6 latin square $C_2 \otimes C_3$:

$$\left(\begin{array}{ccc|ccc} (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) \\ (1,2) & (1,3) & (1,1) & (2,2) & (2,3) & (2,1) \\ (1,3) & (1,1) & (1,2) & (2,3) & (2,1) & (2,2) \\ \hline (2,1) & (2,2) & (2,3) & (1,1) & (1,2) & (1,3) \\ (2,2) & (2,3) & (2,1) & (1,2) & (1,3) & (1,1) \\ (2,3) & (2,1) & (2,2) & (1,3) & (1,1) & (1,2) \end{array}\right).$$

We will identify this square with the reduced square obtained by replacing the symbols with $1, 2, \ldots, nm$ based on their position in the first row:

$$C_2 \otimes C_3 = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 6 & 4 & 2 & 3 & 1 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{array}\right).$$

A *power square* is obtained by taking a repeated product of a fixed square A with itself. We let C_n^m denote the product of the cyclic square C_n with itself m times. In particular, $C_n^1 = C_n$ and $C_n^{m+1} = C_n \otimes C_n^m$. Each cyclic square is the Cayley table of a cyclic group; a power square obtained from a cyclic square is also the Cayley table of the group-theoretic product of that group with itself. In particular, C_2^n is also the Cayley table of the group $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ where there are n factors in the product.

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$
C_2

$$\left(\begin{array}{cc|cc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}\right)$$
$C_2^2 = C_2 \otimes C_2$

$$\left(\begin{array}{cc|cc|cc|cc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ \hline 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ \hline 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ \hline 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{array}\right)$$
$C_2^3 = C_2 \otimes C_2^2$

The 2×2 subsquares indicated above show how C_2^{n+1} can be obtained by replacing each entry i of C_2^n, $1 \le i \le 2^n$, with a fixed 2×2 matrix B_i^n. For example, to form C_2^3 from C_2^2, we use the following four matrices.

$$\begin{array}{cccc} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 4 & 2 \end{pmatrix} & \begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix} & \begin{pmatrix} 7 & 8 \\ 8 & 7 \end{pmatrix} \\ B_1^2 & B_2^2 & B_3^2 & B_4^2 \end{array}$$

This method of obtaining the square C_2^{n+1} will be important in Section 4.

3 Experimental data

In this section, we discuss the computational search we performed to compute the frequency distribution of all reduced squares of size 7 and 8 by the

number of mates each one possesses.[1]

The restriction to reduced squares was required to make the computational searches feasible, as there are too many squares overall to perform an exhaustive search. There are $16,942,080$ reduced latin squares of size 7, and approximately 6×10^{13} total squares, and there are $535,281,401,856$ reduced latin squares of size 8, with approximately 10^{21} total squares. There is no loss of generality in limiting the search to reduced latin squares, because an arbitrary latin square has the same number of mates as its corresponding reduced latin square.

Although it is not possible to simultaneously put an arbitrary square A and mate B into reduced form, we may first reduce the square A using row and column permutations, while simultaneously performing the same operations on the mate B to obtain a new mate B'. We may then permute the symbols of B', while keeping A fixed, to yield a semireduced mate for the reduced form of A. Thus we are able to restrict our search to semireduced mates with no loss of generality. As mentioned in the previous section, each semireduced mate represents $n!$ distinct mates of the same square, and each reduced latin square represents $n!(n-1)!$ distinct squares with the same number of mates. The complete frequency distribution of mates of arbitrary squares can therefore be reproduced from the frequency distribution of semireduced mates of reduced squares.

The search space for squares of size 8 is too large for a single computer to perform in a reasonable time, and we thus used parallelization to distribute the work across a cluster of processors. Our particular method for parallelizing the search space is to have a controller process that enumerates partial reduced latin squares, which we call *blocks*; the number of entries in the partial latin square is the *block length*. A complete latin square that extends the partial square is said to be *in the block* of the partial square. The squares below illustrate a block length of 17 for reduced squares of size 7 and a block length of 24 for reduced squares of size 8.

By filling blocks from top to bottom and left to right, we were able to perform an additional optimization. Because each latin square has the same number of mates as its transpose, it is only necessary to count the number of semireduced mates of one of these two squares. If entries $(2,3)$ and $(3,2)$ of a block are different, then no square in the block can be the same as its transpose. We used this fact to obtain a significant reduction of the search space by only searching one of the two blocks in this case, while storing

[1] The software used to perform the search may be downloaded from `http://science.marshall.edu/mummertc/latin2012/`.

the data for both blocks. This optimization can be seen as a special case of the fact that two parastrophic latin squares have the same number of mates. However, we did not find an efficient way to implement the software to enumerate only one reduced square from each parastrophy class.

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

7×7 block of length 17 $\qquad$ 8×8 block of length 24

The software designated one process as a "controller" and the rest as "workers". The controller was responsible for enumerating the blocks, sending them to the workers, and collecting the results returned by the workers. Upon receiving a block, each worker process enumerates the reduced latin squares in the block. For each reduced square that is found, the worker counts the number of semireduced mates for that square. When it exhausts the reduced squares in the block, the worker returns the block and the information it has found about it to the controller, which stores the information and sends another block to the worker for processing.

The workers counted the number of semireduced mates of each reduced latin square by making an exhaustive search for all ways to cover the square in a set of disjoint transversals such that transversal i includes entry $(1, i)$. The requirement for the mates to be semireduced is thus equivalent to ignoring permutations of labels of the transversals.

To run the search on squares of size 8, we utilized the "Big Green" computing cluster at Marshall University. The Big Green cluster consists of approximately 200, 2.67GHz Intel Xeon cores. We also utilized a local *ad hoc* computer bank of approximately 42, 3.00GHz Intel Core2 Duo cores. The search of all reduced squares of size 8 required approximately 5.5 core-years of processor time on this hardware.

The results of the computational search are frequency distributions for reduced squares of sizes 7 and 8 by the number of semi reduced mates, which are shown in Table 1 and Table 2.

Analysis of the experimental data revealed several facts. There were relatively few mate frequencies for size 7, but a surprisingly large number

Mates	*Frequency*
0	16,765,080
1	105,840
2	52,920
8	210
635	120

Table 1: Frequency of reduced Latin squares of size 7 by number of semireduced mates. For example, there are $52,920$ reduced squares that each have exactly 2 semireduced mates.

of frequencies for size 8. In both cases the most common frequency was 0. Wanless and Webb [5] have conjectured that this is only the case for small squares, and that for larger squares a larger percentage will have mates.

In both sizes 7 and 8, the least common frequency corresponded to the maximum number of mates. We analyzed the squares of each size to characterize the squares with the most mates. We verified computationally that the squares of size 8 with the maximum number of mates are exactly the Cayley tables of $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (that is, they are all isotopic with the usual Cayley table). The squares of size 7 with the most mates are the Cayley tables of $\mathbb{Z}_7$.

4 Mates of Binary Power Squares

In this section, we present a construction of mates of latin power squares of size 2^n. Such squares are already known to be part of a complete set of MOLS [4], but our experimental data suggests that products of cyclic squares have many additional mates that could not fit in a complete set of MOLS. In particular, we have verified computationally that product squares of size 8, 10, and 12 have large numbers of mates. It would be interesting to develop a construction that produces all mates of such squares; we hope that our construction is an initial step in that direction. Moreover, our construction is purely combinatorial, unlike the algebraic construction used to generate complete sets of MOLS.

To explain the construction, we first describe the particular case where we wish to generate a mate of the power square C_2^3. To do so, we begin with a the 4×4 power square C_2^2 and a particular mate M_4, shown below, which will will serve as a blueprint to generate an 8×8 square M_8.

$$\underset{C_2^2}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}} \quad \underset{M_4}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}}$$

The construction will use four 2×2 matrices, A_1, A_2, A_3 and A_4, to form the top half of M_8.

$$\underset{A_1}{\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}} \quad \underset{A_2}{\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}} \quad \underset{A_3}{\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}} \quad \underset{A_4}{\begin{pmatrix} 7 & 8 \\ 5 & 6 \end{pmatrix}}$$

Another four 2×2 matrices tA_1, tA_2, tA_3 and tA_4 will be used for the bottom half of the mate. These are transformed versions of the matrices A_1, A_2, A_3 and A_4 obtained by reflecting the original four 2×2 matrices both vertically and horizontally.

$$\underset{tA_1}{\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}} \quad \underset{tA_2}{\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}} \quad \underset{tA_3}{\begin{pmatrix} 8 & 7 \\ 6 & 5 \end{pmatrix}} \quad \underset{tA_4}{\begin{pmatrix} 6 & 5 \\ 8 & 7 \end{pmatrix}}$$

Our construction forms an 8×8 matrix by replacing the entries of the particular mate M_4 with these 2×2 matrices. In the top half of this matrix, the 1s in M_4 are replaced with A_1, the 2s with A_2, the 3s with A_3, and the 4s with A_4. The bottom half of the new matrix is formed similarly, but using the transformed 2×2 matrices $tA_1, \ldots, tA_4$.

$$\underset{M_4}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}} \quad \underset{\text{Pattern for new square}}{\left(\begin{array}{cccc} A_1 & A_2 & A_3 & A_4 \\ A_3 & A_4 & A_1 & A_2 \\ \hline tA_4 & tA_3 & tA_2 & tA_1 \\ tA_2 & tA_1 & tA_4 & tA_3 \end{array}\right)}$$

This process yields the following 8×8 square M_8 shown below, in which the lines indicate where 2×2 subsquares have been substituted for entries of M_4. It can be verified by hand that M_8 is a mate of C_2^3, which is also shown for reference; Theorem 4.2 below explains why this occurs.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \qquad \left(\begin{array}{cc|cc|cc|cc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ \hline 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ \hline 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ \hline 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{array}\right)$$

C_2^3 $\qquad\qquad$ M_8

There is a deeper pattern in the constructed matrix, because A_2 is a reflection of A_1 across a horizontal axis and A_4 is the corresponding reflection of A_3. Thus, writing hA for the matrix obtained by swapping the columns 2×2 matrix A and vA for the matrix obtained by swapping the rows, we have

$$\left(\begin{array}{cc|cc} A_1 & A_2 & A_3 & A_4 \\ A_3 & A_4 & A_1 & A_2 \\ \hline tA_4 & tA_3 & tA_2 & tA_1 \\ tA_2 & tA_1 & tA_4 & tA_3 \end{array}\right) = \left(\begin{array}{cc|cc} A_1 & vA_1 & A_3 & vA_3 \\ A_3 & vA_3 & A_1 & vA_1 \\ \hline hA_3 & hvA_3 & hA_1 & hvA_1 \\ hA_1 & hvA_1 & hA_3 & hvA_3 \end{array}\right).$$

To generate a mate M_{16} of the 16×16 square M_8, we will use eight 2×2 matrices $A_1, \ldots, A_8$ for the top half of M_{16} and transformed versions of these squares for the bottom half.

$$\left(\begin{array}{cccc|cccc} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 & A_7 & A_8 \\ A_3 & A_4 & A_1 & A_2 & A_7 & A_8 & A_5 & A_6 \\ A_5 & A_6 & A_7 & A_8 & A_1 & A_2 & A_3 & A_4 \\ A_7 & A_8 & A_5 & A_6 & A_3 & A_4 & A_1 & A_2 \\ \hline tA_8 & tA_7 & tA_6 & tA_5 & tA_4 & tA_3 & tA_2 & tA_1 \\ tA_6 & tA_5 & tA_8 & tA_7 & tA_2 & tA_1 & tA_4 & tA_3 \\ tA_4 & tA_3 & tA_2 & tA_1 & tA_8 & tA_7 & tA_6 & tA_5 \\ tA_2 & tA_1 & tA_4 & tA_3 & tA_6 & tA_5 & tA_8 & tA_7 \end{array}\right)$$

Pattern used to generate M_{16} from M_8

In general, the construction begins with a $2^n \times 2^n$ square M, where $n \geq 2$, and produces a $2^{n+1} \times 2^{n+1}$ square N. We first define 2^n squares of size 2×2, labeled $A_1, \ldots, A_{2^n}$. To do so, for each k with $0 \leq k \leq 2^{n-1} - 1$ we

let

$$A_{2k+1} = \begin{pmatrix} 4k+1 & 4k+2 \\ 4k+3 & 4k+4 \end{pmatrix},$$
$$A_{2k+2} = vA_{2k+1} = \begin{pmatrix} 4k+3 & 4k+4 \\ 4k+1 & 4k+2 \end{pmatrix}.$$

We then replace each entry i occurring in the top half of M with the matrix A_i, and each entry i occurring in the bottom half of M with tA_i.

To prove that this algorithm is correct we will require the following definition.

Definition 4.1. A latin square of size $2n \times 2n$ is *balanced* if it has the following property. If the numbers $1, \ldots, 2n$ are grouped into pairs $(2k+1, 2k+2)$, where $0 \leq k \leq n-1$, then in each column one number from each pair occurs in the top half of the square and the other number in the pair occurs in the bottom half of the square.

It can be verified by eye that the squares M_4 and M_8 above are balanced.

Theorem 4.2. *Suppose that M is a mate of the power square C_2^n, where $n \geq 2$, and M is balanced. If N denotes the square of size 2^{n+1} obtained from our construction, then N is latin, is a mate of C_2^{n+1}, and is balanced.*

Proof. We will prove that N is a latin square by considering the rows and columns separately, and then prove the remaining claims.

Claim 1: the rows of N are latin. In the construction, symbols in a row of M are replaced with 2×2 matrices to construct N. Thus each row of M corresponds to two rows of N. Each array from $A_1, A_2, \ldots, A_{2^n}$ is used only once per row of M, because M is latin. Moreover, either no matrix in a row of M is transformed (if the row is in the top half) or all entries are transformed under t (if the row is in the bottom half). Thus the only way for the same number to appear twice in a row of N would be for it to appear in the same row of A_{2k+1} and A_{2k+2} for some k, or in the same row of tA_{2k+1} and tA_{2k+2}. But, because the rows of A_{2k+2} are swapped relative to those of A_{2k+1}, no number appears in the same row of both matrices, and the transformation t preserves this property. Thus each row of N is latin.

Claim 2: the columns of N are latin. Consider a fixed column of N. Again, the entries of this column came from replacing entries of M with 2×2 matrices. Because M is latin, no entry appears twice in the corresponding column of M, and thus for each matrix A_i, exactly one of A_i and tA_i is used to form the column of N. Moreover, because M is balanced, if the

construction of this column of N uses A_{2k+1} then it also uses tA_{2k+2}, and if it uses tA_{2k+1} then it uses A_{2k+2}. However, the transformation t includes a column swap. Thus, by considering the definition of the matrices A_{2k+1} and A_{2k+2}, if exactly one of them is transformed under t, no number will appear in the first column of both, nor in the second column of both. Thus each column of N is latin. We have now proved N is a latin square.

Claim 3: C_2^{n+1} and N are mates. Recall that $C_2^{n+1} = C_2 \otimes C_2^n$, and that C_2^{n+1} is obtained from C_2^n by replacing each entry i, with $1 \leq i \leq 2^n$, with the 2×2 square

$$B_i^n = \begin{pmatrix} 2i-1 & 2i \\ 2i & 2i-1 \end{pmatrix}.$$

The entries that appear in one of these 2×2 squares do not appear in any of the other ones. Thus the only way for a pair (x, y) to appear when C_2^{n+1} and N are superimposed is for x to be obtained from B_i, for the unique i such that x appears in B_i, and for y to be obtained from A_j or A_{j+1}, for the unique j such that y appears in these squares. In other words, any occurrence of (x, y) in $C_2^{n+1} \wr N$ must come from an occurrence of (i, j) or $(i, j+1)$ in $C_2^n \wr M$. Now the pair (i, j) occurs exactly once in $C_2^n \wr M$, and the pair $(i, j+1)$ also appears once, because C_2^n and M are mates. It thus suffices to show that, for arbitrary i and j, all 8 ordered pairs of the elements of B_i and the elements of A_j occur when C_2^{n+1} and N are superimposed.

To this end, first note that the pairs seen by superimposing B_i and A_j are the same as those obtained by superimposing B_i and tA_j, because $tB_i = B_i$ and because the pairs obtained from B_i and A_j must be the same as the pairs obtained from tB_i and tA_j. However, the pairs obtained by superimposing B_i and A_j are different than those obtained by superimposing B_i and $A_{j+1} = vA_j$, although they are the same as those obtained from B_i and tA_{j+1}. For example, the following shows the pairs obtained from B_1, A_1, and A_2.

$$\begin{array}{ccc} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} & \begin{pmatrix} (1,1) & (2,2) \\ (2,3) & (1,4) \end{pmatrix} \\ B_1 & A_1 & B_1 \wr A_1 \end{array}$$

$$\begin{array}{ccc} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} & \begin{pmatrix} (1,3) & (2,4) \\ (2,1) & (1,2) \end{pmatrix} \\ B_1 & A_2 = vA_1 & B_1 \wr A_2 \end{array}$$

Thus all eight different pairs made from entries of B_i and entries of A_j are obtained in $C_2^{n+1} \wr N$: four from locations corresponding to the pair (i, j)

in $C_2^n \wr M$ and four more corresponding to the pair $(i, j+1)$. This completes the proof that C_2^{n+1} and N are mates.

Claim 4: N is balanced. Consider a pair $(2k+1, 2k+2)$ and a particular column of N, with $0 \leq k < 2^n$. The only way for $2k+1$ and $2k+2$ to appear in the column is for them to come from a pair A_{2i}, A_{2i+1} of 2×2 matrices, for an appropriate i. Because M is balanced, exactly one of $2i$ and $2i+1$ occurs in the top half of the corresponding column of M, and thus exactly one of the two matrices A_{2i}, A_{2i+1} is used to construct the top half of the corresponding column of N. Each of A_{2i} and A_{2i+1} has $2k+1$ and $2k+2$ in different columns, so only one of these can appear in the top half of the column of N that we are considering. This shows N is balanced. □

The theorem immediately yields the following corollary.

Corollary 4.1. *If our construction is iterated beginning with the square M_4, it will produce a sequence of latin squares $M_4, M_8, M_{16}, \ldots$ such that M_{2^n} is a mate of C_2^n for each $n \geq 2$.*

We conjecture that the method used here can be extended to generate additional mates of squares C_2^n, and more generally to produce mates of squares of the form C_k^n where C_k is the Cayley table of $\mathbb{Z}_k$.

References

[1] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, New York, 1974. MR 0351850 (50 #4338)

[2] Anthony B. Evans, *Latin squares without orthogonal mates*, Des. Codes Cryptogr. **40** (2006), no. 1, 121–130. MR 2226287 (2007b:05031)

[3] Charles F. Laywine and Gary L. Mullen, *Discrete mathematics using Latin squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR 1644242 (99k:05041)

[4] Gary L. Mullen and Carl Mummert, *Finite fields and applications*, Student Mathematical Library, vol. 41, American Mathematical Society, Providence, RI, 2007. MR 2358760 (2009b:05001)

[5] Ian M. Wanless and Bridget S. Webb, *The existence of Latin squares without orthogonal mates*, Des. Codes Cryptogr. **40** (2006), no. 1, 131–135. MR 2226288 (2008e:05024)

Mates	*Freq.*	*Mates*	*Freq.*	*Mates*	*Freq.*	*Mates*	*Freq.*
0	532,807,827,816	27	967,680	92	241,920	198	40,320
1	1,926,259,200	43	967,680	122	241,920	220	30,240
2	246,274,560	64	967,680	152	241,920	384	30,240
4	75,519,360	69	967,680	234	241,920	536	30,240
3	54,270,720	80	846,720	248	241,920	616	30,240
5	28,304,640	52	645,120	288	241,920	832	30,240
8	22,256,640	42	604,800	308	241,920	1,216	30,240
6	18,466,560	72	544,320	324	241,920	1,488	30,240
16	18,063,360	19	483,840	720	241,920	2,592	30,240
9	9,192,960	26	483,840	252	201,600	3,232	30,240
10	8,104,320	29	483,840	48	120,960	4,000	30,240
7	7,499,520	38	483,840	70	120,960	1,356	26,880
15	6,048,000	91	483,840	74	120,960	236	15,120
18	5,080,320	128	483,840	90	120,960	4,928	10,080
20	4,354,560	144	483,840	166	120,960	2,496	7,560
22	3,507,840	496	483,840	184	120,960	2,816	7,560
32	3,265,920	84	403,200	202	120,960	4,096	7,560
12	3,225,600	46	362,880	242	120,960	4,736	7,560
37	2,177,280	100	362,880	304	120,960	4,248	6,720
24	1,935,360	50	322,560	632	120,960	364	5,040
36	1,774,080	76	322,560	78	80,640	4,020	5,040
28	1,451,520	352	302,400	96	80,640	4,536	5,040
13	1,209,600	25	241,920	156	60,480	12,048	5,040
14	1,209,600	34	241,920	328	60,480	23,232	1,260
44	1,209,600	40	241,920	332	60,480	23,040	630
30	1,128,960	45	241,920	392	60,480	33,408	630
68	1,088,640	56	241,920	528	60,480	32,256	210
11	967,680	65	241,920	864	60,480	70,272	30
21	967,680	66	241,920	54	40,320		

Table 2: Frequency of reduced Latin squares of size 8 by number of semireduced mates