Mutually Orthogonal Latin Squares

Serge Ballif, February 25, 2008

The main reference for the talk is **Discrete Mathematics Using Latin Squares** by Charles F. Laywine and Gary L. Mullen

1 3 Challenges

1.1 Challenge I

Challenge I
Consider the 16 aces, kings, queens, and jacks from a regular 52 card deck of playing card. Can the 16 cards be arranged in a 4×4 array so that no suit and no single kind of card occurs twice in any row or column? (The suits are spades, diamonds, hearts, and clubs.)

Solution

$$\begin{array}{cccc} A\spadesuit & K\diamondsuit & Q\heartsuit & J\clubsuit \\ K\heartsuit & A\clubsuit & J\spadesuit & Q\diamondsuit \\ Q\clubsuit & J\heartsuit & A\diamondsuit & K\spadesuit \\ J\diamondsuit & Q\spadesuit & K\clubsuit & A\heartsuit \end{array}$$

1.2 Challenge II

Challenge II
In addition to the above requirements, is it possible to color the cards 4 different colors (red, yellow, blue, green) such that

1. No two cards have the same color and suit,
2. No two cards have the same color and value,
3. no row or column has the same color twice?

1.3 Challenge III

Challenge III
If there were n^2 cards consisting n suits and n types of cards, is it possible to arrange an $n \times n$ array such that each suit and each type of card is present in each row and column?

2 Definitions

2.1 Latin Squares

Definition 1. A *latin square of order* n is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column.

Example 2. Here are latin squares of orders 3 and 4 respectively.

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \quad \text{and} \quad \begin{array}{cccc} A & K & Q & J \\ K & A & J & Q \\ Q & J & A & K \\ J & Q & K & A \end{array}$$

Example 3.
1. Sudoku puzzles are latin squares.
2. Group multiplication tables are latin squares.

Facts

1. The problem of determining if a partially filled square can be completed to form a Latin square is NP-complete.
2. Permuting the rows and columns of a latin square results in a latin square.
3. A permutation of the n symbols in a latin square results in a latin square.

2.2 How Many?

Question
How many latin squares of order n are there?

Answer
One heck of a lot!

When $n = 15$, the number of latin squares is believed to exceed the number of atoms in the universe.

2.3 MOLS

Definition 4. Let L_1 and L_2 be latin squares of the same order, say $n \geq 2$. We say that L_1 and L_2 are *mutually orthogonal* if, when superimposed, each of the possible n^2 ordered pairs occur exactly once.

A set $\{L_1, \ldots, L_t\}$ of $t \geq 2$ latin squares of order n is *orthogonal* if any two distinct latin squares are orthogonal. We call this a set of *mututally orthogonal latin squares* (MOLS).

Let $N(n)$ denote the maximum possible number of MOLS of order n.

Example 5. The following MOLS gave us the solution to the challenge problem.

$$\begin{array}{cccc} A & K & Q & J \\ K & A & J & Q \\ Q & J & A & K \\ J & Q & K & A \end{array} \quad \text{and} \quad \begin{array}{cccc} \spadesuit & \diamondsuit & \heartsuit & \clubsuit \\ \heartsuit & \clubsuit & \spadesuit & \diamondsuit \\ \clubsuit & \heartsuit & \diamondsuit & \spadesuit \\ \diamondsuit & \spadesuit & \clubsuit & \heartsuit \end{array}$$

3 MOLS

3.1 Upper Bound on # of MOLS

Theorem 6. *For each $n \geq 2$, $N(n) \leq n - 1$.*

Proof.
- Consider a maximal set of MOLS $L_1, \ldots, L_t$.
- Relabeling the n symbols of L_i will not affect the orthogonality with any other L_j.
- Hence, we may assume that the top row of each L_i is given by $(1, 2, 3, \ldots, n)$.

$$L_1 = \begin{array}{cccc} 1 & 2 & \cdots & n \\ x_1 & - & \cdots & - \\ \vdots & \vdots & & \vdots \\ - & - & \cdots & - \end{array}, L_2 = \begin{array}{cccc} 1 & 2 & \cdots & n \\ x_2 & - & \cdots & - \\ \vdots & \vdots & & \vdots \\ - & - & \cdots & - \end{array}, \ldots, L_t = \begin{array}{cccc} 1 & 2 & \cdots & n \\ x_t & - & \cdots & - \\ \vdots & \vdots & & \vdots \\ - & - & \cdots & - \end{array}$$

- The entries x_1 through x_t cannot be 1, because the first column already has a 1. Also, $x_i \neq x_j$ for $i \neq j$, because the top row terms are already the same.
- Hence $t \leq n - 1$. $\square$

3.2 Constructing MOLS

Question
How do we construct a (maximal) set of MOLS?

Theorem 7. *If q is a power of a prime, Then $N(q) = q-1$. Moreover, a complete set of MOLS can be found by taking the nonzero elements $a \in F_q$ (the field with q elements) and letting the a^{th} square have coordinate in row x and column y given by $f_a(x,y) = ax + y$.*

Example 8. Over $\mathbb{Z}_3 = \{0, 1, 2\}$ we have

$$\begin{array}{lll} f_1(0,0)=0 & f_1(0,1)=1 & f_1(0,2)=2 \\ f_1(1,0)=1 & f_1(1,1)=2 & f_1(1,2)=0 \\ f_1(2,0)=2 & f_1(2,1)=0 & f_1(2,2)=1 \end{array} \quad \leftrightarrow \quad \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array}$$

$$\begin{array}{lll} f_2(0,0)=0 & f_2(0,1)=1 & f_2(0,2)=2 \\ f_2(1,0)=2 & f_2(1,1)=0 & f_2(1,2)=1 \\ f_2(2,0)=1 & f_2(2,1)=2 & f_2(2,2)=0 \end{array} \quad \leftrightarrow \quad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

Proof that $f_a(x,y)$ gives a latin square.

- A column can't have the same symbol twice because
$$f_a(x,y) = f_a(x',y) \Leftrightarrow ax + y = ax' + y \Leftrightarrow x = x'.$$
- A row can't have the same symbol twice because
$$f_a(x,y) = f_a(x,y') \Leftrightarrow ax + y = ax + y' \Leftrightarrow y = y'.$$ □

Proof that $f_a(x,y)$ and $f_b(x,y)$ are orthogonal.

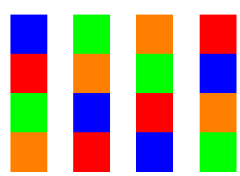
- Suppose the same ordered pair appears in slots (x,y) and (x',y') after superimposition.
- Then $ax + y = ax' + y'$ and $bx + y = bx' + y'$.
- Subtracting one equation from the other gives
$$\begin{aligned} ax - bx = ax' - bx' &\Leftrightarrow (a-b)x = (a-b)x' \\ &\Leftrightarrow x = x' \Leftrightarrow y = y'. \end{aligned}$$ □

3.3 Solution to Challenge II

Solution to Challenge II
Using the procedure in the proof we can get 3 MOLS of order 4.

A	K	Q	J
K	A	J	Q
Q	J	A	K
J	Q	K	A

♠	♢	♡	♣
♡	♣	♠	♢
♣	♡	♢	♠
♢	♠	♣	♡



Together, the MOLS give the affirmative solution to Challenge II.

A♠	K♢	Q♡	J♣
K♡	A♣	J♠	Q♢
Q♣	J♡	A♢	K♠
J♢	Q♠	K♣	A♡

3.4 MOLS Produce More MOLS

Theorem 9. *If there is a pair of MOLS of order m and a pair of MOLS of order n, then there is a pair of MOLS of order mn.*

Proof. If $A = (a_{ij})$ and $B = (b_{kl})$ are latin squares of orders m and n, then the Kronecker product $A \otimes B$ (displayed below) is also a latin square.

$$\begin{array}{ccccccc}
a_{11}b_{11} & a_{11}b_{12} \;\dots\; & a_{11}b_{1n} & & a_{1m}b_{11} & a_{1m}b_{12} \;\dots\; & a_{1m}b_{1n} \\
a_{11}b_{21} & a_{11}b_{22} \;\dots\; & a_{11}b_{2n} & & a_{1m}b_{21} & a_{1m}b_{22} \;\dots\; & a_{1m}b_{2n} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
a_{11}b_{n1} & a_{11}b_{n2} \;\dots\; & a_{11}b_{nn} & & a_{1m}b_{n1} & a_{1m}b_{n2} \;\dots\; & a_{1m}b_{nn} \\
 & \vdots & & & & \vdots & \\
a_{m1}b_{11} & a_{m1}b_{12} \;\dots\; & a_{m1}b_{1n} & & a_{mm}b_{11} & a_{mm}b_{12} \;\dots\; & a_{mm}b_{1n} \\
a_{m1}b_{21} & a_{m1}b_{22} \;\dots\; & a_{m1}b_{2n} & & a_{mm}b_{21} & a_{mm}b_{22} \;\dots\; & a_{mm}b_{2n} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
a_{m1}b_{n1} & a_{m1}b_{n2} \;\dots\; & a_{m1}b_{nn} & & a_{mm}b_{n1} & a_{mm}b_{n2} \;\dots\; & a_{mm}b_{nn}
\end{array}$$

Moreover, if A and B are orthogonal to A' and B', then $A \otimes B$ and $A' \otimes B'$ are orthogonal. □

Example 10. The pairs of MOLS

$$A = \begin{array}{ccc} 1&2&3\\2&3&1\\3&1&2 \end{array}, A' = \begin{array}{ccc} 1&2&3\\3&1&2\\2&3&1 \end{array} \quad \text{and} \quad B = \begin{array}{cccc} 1&2&3&4\\2&1&4&3\\3&4&1&2\\4&3&2&1 \end{array}, B' = \begin{array}{cccc} 1&2&3&4\\3&4&1&2\\4&3&2&1\\2&1&4&3 \end{array}$$

allows us to use the Kronecker product to create the MOLS $A \otimes B =$ and $A' \otimes B'$ displayed below.

$$\begin{array}{cccccccccccc}
11&12&13&14&21&22&23&24&31&32&33&34\\
12&11&14&13&22&21&24&23&32&31&34&33\\
13&14&11&12&23&24&21&22&33&34&31&32\\
14&13&12&11&24&23&22&21&34&33&32&31\\
21&22&23&24&31&32&33&34&11&12&13&14\\
22&21&24&23&32&31&34&33&12&11&14&13\\
23&24&21&22&33&34&31&32&13&14&11&12\\
24&23&22&21&34&33&32&31&14&13&12&11\\
31&32&33&34&11&12&13&14&21&22&23&24\\
32&31&34&33&12&11&14&13&22&21&24&23\\
33&34&31&32&13&14&11&12&23&24&21&22\\
34&33&32&31&14&13&12&11&24&23&22&21
\end{array}
\qquad
\begin{array}{cccccccccccc}
11&12&13&14&21&22&23&24&31&32&33&34\\
13&14&11&12&23&24&21&22&33&34&31&32\\
14&13&12&11&24&23&22&21&34&33&32&31\\
12&11&14&13&22&21&24&23&32&31&34&33\\
31&32&33&34&11&12&13&14&21&22&23&24\\
33&34&31&32&13&14&11&12&23&24&21&22\\
34&33&32&31&14&13&12&11&24&23&22&21\\
32&31&34&33&12&11&14&13&22&21&24&23\\
21&22&23&24&31&32&33&34&11&12&13&14\\
23&24&21&22&33&34&31&32&13&14&11&12\\
24&23&22&21&34&33&32&31&14&13&12&11\\
22&21&24&23&32&31&34&33&12&11&14&13
\end{array}$$

3.5 Solution to Challenge III

Corollary 11. *For $m, n > 1$, $N(mn) \geq \min\{N(m), N(n)\}$*

Euler's Conjecture and Challenge III
Euler had conjectured that no pair of MOLS existed when $n = 2, 6, 10, 14, \ldots$.

Theorem 12 (Bos, Shrikhande, Parker 1960)**.** *For all n except 2 and 6, there is a pair of MOLS of order n (i.e. $N(n) \geq 2$).*

3.6 Concluding Facts

Facts

- The existence of $n-2$ MOLS of order n implies the existence of $n-1$ MOLS of order n ($n \geq 3$).
- The existence of $n-3$ MOLS of order n implies the existence of $n-1$ MOLS of order n ($n \geq 5$).
- Not all latin squares have orthogonal mates; e.g.

$$\begin{array}{cccc} 1&2&3&4\\2&4&1&3\\3&1&4&2\\4&3&2&1 \end{array}$$

- $N(n) \to \infty$ as $n \to \infty$.