The Problem of the 36 Officers

Kalei Titcomb

June 12, 2009

Contents

Introduction to the Mathematical Exploration

Ever since I was a little kid, I have enjoyed doing puzzles. While my parents bought the crossword puzzle books, I always wanted the logic books because they had games, and a variety of puzzles including crossword. I never imagined that I would be able to one day explore the idea of a specific type of puzzle and present it through a project for my master's degree in teaching mathematics. The specific puzzle is a square of numbers known as a *Latin Square*

Let n denote a positive integer. A *Latin square* of *order* n is an $n \times n$ array with n symbols arranged in such a way that each symbol occurs once in each row and column. Latin squares are all around us. Specifically, we may find them in operation tables for groups, and in puzzles like Sudoku, or more recently, in the 36 Cube puzzle by Thinkfun. In this project, I wanted to explore a deep combinatorics result that I could nonetheless explain to others.

One man who is famous for such results is Leonhard Euler. His name is everywhere in mathematics, and he is widely regarded as the most prolific mathematician of all time. But while many of Euler's conjectures have been proven true, how many of us can name an instance in which he was wrong?

In around 1780, Euler made a conjecture concerning orthogonal Latin squares. Said briefly, a pair of $n \times n$ Latin squares is *orthogonal* if, when superimposed, the resulting square contains all possible n^2 ordered pairs of entries. Euler conjectured that there does not exist a pair of orthogonal Latin squares of order $n = 4k + 2$ for any non-negative integer k. The relevant terms will be defined more carefully later, but for now, suffice it to say that, although his conjecture was true for $k = 0$ and $k = 1$, it was false for all $k \geq 2$. In this project, our interest lies in the case when $k = 1$. In this case, the question is equivalent to a word problem that Euler dubbed "The problem of the 36 Officers" and can be described as follows. Euler asked "How can a delegation of six regiments, each of which sends a colonel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular 6×6 array such that no row or column duplicates a rank or a regiment?" Such an arrangement would be equivalent to a pair of orthogonal Latin squares of order 6.

Example. A pair of orthogonal Latin squares of order $n = 3$.

$$\begin{array}{|c|c|c|}\hline A & 2 & 3 \\ \hline 3 & A & 2 \\ \hline 2 & 3 & A \\ \hline \end{array} \; : \; \begin{array}{|c|c|c|}\hline \clubsuit & \diamondsuit & \heartsuit \\ \hline \diamondsuit & \heartsuit & \clubsuit \\ \hline \heartsuit & \clubsuit & \diamondsuit \\ \hline \end{array} \; \Rightarrow \; \begin{array}{|c|c|c|}\hline A\clubsuit & 2\diamondsuit & 3\heartsuit \\ \hline 3\diamondsuit & A\heartsuit & 2\clubsuit \\ \hline 2\heartsuit & 3\clubsuit & A\diamondsuit \\ \hline \end{array}$$

What prompted Euler to come up with the conjecture that there does not exist a pair of mutually orthogonal Latin squares of order $n = 4k + 2$? He was researching a related puzzle known as a magic square. A *magic square* of *order* n is an $n \times n$ array whose entries are the numbers $1, 2, \ldots, n^2$ arranged in such a way that each row and column has the same sum (a common variation also requires the diagonals to share this sum). Euler had already established a simple way to construct a magic square from a pair of orthogonal Latin squares. Of course, the reader may wonder why Euler was interested in magic squares as well! Beyond the purely recreational enjoyment of the pursuit of such studies, Euler felt that the "methods" of such problems "would seem to provide a vast field for new and interesting research". And while he concedes that at first glance, such a question may appear to have "little use itself," he concludes that his investigations led him "to some observations just as important for the doctrine of combinations as for the general theory of magic squares."

Although, for the case $k = 1$, Euler correctly conjectured that no solution exists, he never published a proof of this result. Indeed, it was not until around 1900 when a French amateur mathematician by the name of Gaston Tarry, who was originally in the French Financial Administration, proved that there does not exist a pair of mutually orthogonal Latin squares of order 6 by exhausting the $812,851,200$ possibilities. Admittedly, he was able to simplify the number of cases by working with reduced squares, but this simplification still required working out 9408 pairs by hand.

In 1984, D.R. Stinson provided a four-page proof of this nonexistence. His article was titled "A short proof of the nonexistence of a pair of orthogonal Latin squares of order 6" and appeared in the Journal of Combinatorial Theory. Stinson is currently a professor and Univeristy Research Chair in the David R. Cheriton School of Computer Science at the University of Waterloo. Our aim in the mathematical section of this project is to work through his combinatorial proof with the help of a matrix, a few graphs, and a few lemmas.

1 Latin Squares

Suppose n is a positive integer. A *Latin square of order n* is an $n \times n$ array with n different symbols, arranged in such a way that each symbol occurs exactly once in each row and exactly once in each column. For convenience, I will use the first n integers for the symbols.

Example. $n = 2$. There are only 2 possible cases for a 2×2 Latin square.

1	2
2	1

2	1
1	2

Above, we have the only two possible cases for $n = 2$. This is because, once we put our first symbol down, in order to stay true to the definition of a Latin square, the other blank spaces in our array become predetermined. Because there are only two symbols, there are only two possible ways to do this. In general, however, for large n, there is no easy direct way to compute the total number of cases, and only asymptotic bounds are known for the limiting case as n goes to infinity. By contrast, the question of existence is simple, for we will see that it is a rather simple matter to construct a Latin square for any integer $n > 0$.

Example. $n = 3$. (a) There are 12 possible cases for a 3×3 Latin square.

1	2	3
3	1	2
2	3	1

1	3	2
2	1	3
3	2	1

2	3	1
1	2	3
3	1	2

2	1	3
3	2	1
1	3	2

3	1	2
2	3	1
1	2	3

3	2	1
1	3	2
2	1	3

1	2	3
2	3	1
3	1	2

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

3	1	2
1	2	3
2	3	1

3	2	1
2	1	3
1	3	2

Example. $n = 3$. (b) A pair of orthogonal Latin squares.

1	2	3
3	1	2
2	3	1

3	2	1
2	1	3
1	3	2

In part (b) of the example above, we have selected out two of the 12 possible cases listed in part (a) for $n = 3$. Notice how every symbol in each case occurs exactly once in each row or column. Not only this, but if we superimpose one matrix in part (b) on top of the other, we see that each *pair* of symbols occurs only once in the entire array, as follows:

$$\begin{array}{|c|c|c|}\hline 1_3 & 2_2 & 3_1 \\ \hline 3_2 & 1_1 & 2_3 \\ \hline 2_1 & 3_3 & 1_2 \\ \hline \end{array}$$

When this happens, then we say that the two Latin squares are *orthogonal*, or rather that we have a pair of orthogonal Latin squares. This important topic forms the subject of our next section.

2 Orthogonal Latin Squares

Two Latin squares of order n are said to be *orthogonal*, or *mutually orthogonal* if, when superimposed, every ordered pair of symbols occurs exactly once among the n^2 pairs.

Example. $n = 3$. This can be nicely illustrated by using playing cards. We may use our example from the previous page and replace one set of numbers with card values, and the other set of numbers with card suits. Then, using $\{A, 2, 3\}$ and $\{\heartsuit, \diamondsuit, \clubsuit\}$, each of the 9 possible types of cards should occur once in the matrix, and the suits and ranks separately form Latin squares of order 3, as shown below:

$$\begin{array}{|c|c|c|}\hline A & 2 & 3 \\ \hline 3 & A & 2 \\ \hline 2 & 3 & A \\ \hline \end{array} \; : \; \begin{array}{|c|c|c|}\hline \clubsuit & \diamondsuit & \heartsuit \\ \hline \diamondsuit & \heartsuit & \clubsuit \\ \hline \heartsuit & \clubsuit & \diamondsuit \\ \hline \end{array} \; \Rightarrow \; \begin{array}{|c|c|c|}\hline A\clubsuit & 2\diamondsuit & 3\heartsuit \\ \hline 3\diamondsuit & A\heartsuit & 2\clubsuit \\ \hline 2\heartsuit & 3\clubsuit & A\diamondsuit \\ \hline \end{array}$$

We remark that we were unable to give an example of a pair of orthogonal Latin squares for $n = 2$ because there are only two possible Latin squares of order two, and the reader will notice that if we put these together, we get a repetition of the same two pairs, as shown below.

Example. The impossibility of $n = 2$.

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array} \; : \; \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 2 \\ \hline \end{array} \; \Rightarrow \; \begin{array}{|c|c|}\hline 1_2 & 2_1 \\ \hline 2_1 & 1_2 \\ \hline \end{array}$$

Notice above that the pairs 1_2 and 2_1 are repeated, while 1_1 and 2_2 are omitted. If the reader has never tried to construct mutually orthogonal Latin squares, then we suggest to begin with the 3×3 or 4×4 case to get a feel for the task.

Example. $n = 4$. A pair of orthogonal Latin squares of order 4.

$$\begin{array}{|c|c|c|c|}\hline A & 2 & 3 & 4 \\ \hline 2 & A & 4 & 3 \\ \hline 3 & 4 & A & 2 \\ \hline 4 & 3 & 2 & A \\ \hline \end{array} \; : \; \begin{array}{|c|c|c|c|}\hline \heartsuit & \diamondsuit & \clubsuit & \spadesuit \\ \hline \clubsuit & \spadesuit & \heartsuit & \diamondsuit \\ \hline \spadesuit & \clubsuit & \diamondsuit & \heartsuit \\ \hline \diamondsuit & \heartsuit & \spadesuit & \clubsuit \\ \hline \end{array} \; \Rightarrow \; \begin{array}{|c|c|c|c|}\hline A\heartsuit & 2\diamondsuit & 3\clubsuit & 4\spadesuit \\ \hline 2\clubsuit & A\spadesuit & 4\heartsuit & 3\diamondsuit \\ \hline 3\spadesuit & 4\clubsuit & A\diamondsuit & 2\heartsuit \\ \hline 4\diamondsuit & 3\heartsuit & 2\spadesuit & A\clubsuit \\ \hline \end{array}$$

Example. $n = 5$.

A	2	3	4	5
5	A	2	3	4
4	5	A	2	3
3	4	5	A	2
2	3	4	5	A

:

♥	♦	♣	♠	★
♦	♣	♠	★	♥
♣	♠	★	♥	♦
♠	★	♥	♦	♣
★	♥	♦	♣	♠

$\Rightarrow$

A♥	2♦	3♣	4♠	5★
5♦	A♣	2♠	3★	4♥
4♣	5♠	A★	2♥	3♦
3♠	4★	5♥	A♦	2♣
2★	3♥	4♦	5♣	A♠

As it turns out, it is much easier to find a pair of orthogonal Latin squares of odd order than a pair of even order. Notice how, in the case where $n = 5$, we have a pattern of A down one diagonal, and $\star$ down the other diagonal. The other numbers and suits are also organized in a diagonal fashion similar to that of the A or $\star$, respectively.

Example. n odd.

Suppose we have rows $i = \{1, 2, \ldots, n\}$ and columns $j = \{1, 2, \ldots, n\}$ in two $n \times n$ arrays, A and B. For each entry $a_{ij} \in A$, define our entries as $a_{ij} \equiv_n i - j$ and for each entry $b_{ij} \in B$, define our entries as $b_{ij} \equiv_n i + j$. Then both A and B yield Latin squares. More than that, if we superimpose A on B, we will always get a pair of orthogonal Latin squares of order n, when n is odd.

To see why this will yield a pair of orthogonal Latin squares, suppose that, in row i and column j, we have an entry $(i - j, i + j)$ in our square, and an that in row h and column k, we have an entry $(h - k, h + k)$ in the same square, where $i \neq h$ and $j \neq k$. Suppose also that $(i - j, i + j) \equiv_n (h - k, h + k)$. Then, $i - j \equiv_n h - k$ and $i + j \equiv_n h + k$. If we add these equations together, we have $2i \equiv_n 2h$, and since n is odd, we may divide by 2, giving us $i = h$. Similarly, if we had subtracted those equations, we would have $2j \equiv_n 2k \Rightarrow j = k$.

When trying to find a pair of orthogonal Latin squares of odd order, these two trivial Latin squares will always work. The even case is not as easy. We have already seen that the case for $n = 2$ is impossible. One of the main goals of this mathematical exploration is to show why the $n = 6$ case is impossible – a fact that Euler conjectured but apparently never proved.

3 Designs

3.1 Transversal Designs (TDs)

Our proof includes the use of a transversal design, or TD. A TD(g,k) is a triple $(X, \mathscr{G}, \mathscr{A})$, where X is a set of elements (points) such that $|X| = g \cdot k$, $\mathscr{G}$ is a partition of X into g subsets (groups) of X of size k, and $\mathscr{A}$ is a set of k^2 subsets (blocks) of X, each of size g, such that any group meets any block in a point, and any two points from different groups occur in exactly 1 block.

Example. TD(2,3)

$$\begin{aligned} X &= \{1,2,3,4,5,6\} \\ \mathscr{G} &= \{\{1,2,3\},\{4,5,6\}\} \\ \mathscr{A} &= \{\{1,4\},\{1,5\},\{1,6\},\{2,4\},\{2,5\},\{2,6\},\{3,4\},\{3,5\},\{3,6\}\} \end{aligned}$$

Example. TD(3,2)

$$\begin{aligned} X &= \{1,2,3,4,5,6\} \\ \mathscr{G} &= \{\{1,2\},\{3,4\},\{5,6\}\} \\ \mathscr{A} &= \{\{1,3,5\},\{1,4,6\},\{2,3,6\},\{2,4,5\}\} \end{aligned}$$

A TD(4,6) is equivalent to a pair of orthogonal Latin squares of order six. This is not very clear from the above definition, so we offer a bit of an explanation. Suppose we have a TD(4,6)=$(X,\mathscr{G},\mathscr{A})$. It is helpful to think of the 4 groups of $\mathscr{G}$ as:

$$\begin{aligned} \{x_1,\ldots,x_6\} &= \text{The 6 rows of the square} \\ \{x_7,\ldots,x_{12}\} &= \text{The 6 columns of the square} \\ \{x_{13},\ldots,x_{18}\} &= \text{The 6 symbols from one Latin square} \\ \{x_{19},\ldots,x_{24}\} &= \text{The 6 symbols from the other Latin square.} \end{aligned}$$

Remember that a pair of orthogonal Latin squares involves two Latin squares, and it is from this that we get the two sets of symbols. These 4 groups give us our set of 24, or our X. It is also helpful to think of the 36 blocks of $\mathscr{A}$ as corresponding to the 36 locations in the 6×6 square:

$$\{B_5,\ldots,B_{40}\} = \text{The 36 locations in our } 6\times 6 \text{ orthogonal Latin square}$$

In a moment, the fact that the blocks started at B_5 as opposed to B_1 won't be so unclear. We are introduced to these with the use of another design.

3.2 Pairwise balanced Designs (PBDs)

Let $(X,\mathscr{G},\mathscr{A})$ be a TD(4,6). Then $P = (X,\mathscr{G}\cup\mathscr{A})$ is a *pairwise balanced design*, or PBD, with 24 points and 40 blocks. In general, a "PBD" is a set X (of points) and a set of subsets of X (blocks) such that any pair of points are in exactly 1 block, and not all blocks must be of the same size.

These 24 points are our same $\{x_1,\ldots,x_{24}\}$ from the four groups of $\mathscr{G}$. The 40 blocks, $\{B_1,\ldots,B_{40}\}$, consist of 36 blocks of size four, and 4 blocks of size six. Our 36 blocks are our $B_5,\ldots,B_{40}$ blocks from $\mathscr{A}$. Our 4 blocks of size six, B_1, B_2, B_3, B_4 are the groups of $\mathscr{G}$. By this I mean:

$$\begin{aligned} B_1 &= \{x_1,\ldots,x_6\} \\ B_2 &= \{x_7,\ldots,x_{12}\} \\ B_3 &= \{x_{13},\ldots,x_{18}\} \\ B_4 &= \{x_{19},\ldots,x_{24}\} \end{aligned}$$

These definitions are needed in order to form the incidence matrix of M of P, which will be very useful in describing our proof.

4 The incidence matrix M of a PBD

Suppose P is a PBD with p points $x_1, \ldots, x_p$ and b blocks $B_1, \ldots, B_b$. The incidence matrix of P is the $p \times b$ matrix $M = \left(m_{ij}\right)$ defined by

$$\begin{aligned} m_{ij} &= 1 \text{ if } x_i \in B_j, \text{ for } 1 \leq i \leq p, \ 1 \leq j \leq b, \\ &= 0 \text{ if } x_i \notin B_j, \text{ for } 1 \leq i \leq p, \ 1 \leq j \leq b. \end{aligned}$$

We will cleverly denote the ith row of M by ρ_i. If we consider each ρ_i to be a vector in the vector space $V = (GF(2))^b$, then the ρ_i's span a subspace C of V which we call the *code* of P.

So what does this matrix look like if when P corresponds to a pair of orthogonal Latin squares? Since we aim to show the nonexistence of a pair orthogonal Latin squares of order 6, let's begin with a simpler case, when $n = 4$.

Let us recall our orthogonal Latin square example from earlier, along with the two separate Latin squares. This is all shown below.

$$\begin{array}{|c|c|c|c|} \hline A & 2 & 3 & 4 \\ \hline 2 & A & 4 & 3 \\ \hline 3 & 4 & A & 2 \\ \hline 4 & 3 & 2 & A \\ \hline \end{array} \quad : \quad \begin{array}{|c|c|c|c|} \hline \heartsuit & \diamondsuit & \clubsuit & \spadesuit \\ \hline \clubsuit & \spadesuit & \heartsuit & \diamondsuit \\ \hline \spadesuit & \clubsuit & \diamondsuit & \heartsuit \\ \hline \diamondsuit & \heartsuit & \spadesuit & \clubsuit \\ \hline \end{array} \quad \Rightarrow \quad \begin{array}{|c|c|c|c|} \hline A\heartsuit & 2\diamondsuit & 3\clubsuit & 4\spadesuit \\ \hline 2\clubsuit & A\spadesuit & 4\heartsuit & 3\diamondsuit \\ \hline 3\spadesuit & 4\clubsuit & A\diamondsuit & 2\heartsuit \\ \hline 4\diamondsuit & 3\heartsuit & 2\spadesuit & A\clubsuit \\ \hline \end{array}$$

Before we describe the incidence matrix for this 4×4 example, let's first take a look at the TD(4,4) and the PBD. In this case, our points are a set $X = \{x_1, \ldots, x_{16}\}$, where x_1–x_4 correspond to the 4 rows of the square, x_5–x_8 to the 4 columns of the square, x_9–x_{12} to the 4 symbols in one square, and x_{13}–x_{16} to the 4 symbols in the other square. If we encode the corresponding TD(4,4), these would form the 4 groups of $\mathscr{G}$, each of size 4. The 16 locations of the 4×4 square are represented by the 16 blocks B_5–B_{20}, which are also of size 4.

By contrast, in a PBD, the four groups are encoded as four of our blocks, B_1, B_2, B_3, B_4. The remaining 16 blocks $B_5, \ldots, B_{20}$ still each correspond to a unique location in our square.

Now we are ready to consider the incidence matrix M of this PBD with 16 points and 20 blocks. The matrix is given on the next page. Each block of P is a column of our matrix. The first blocks B_1–B_4 correspond to the rows, columns, rank, and suit of the 4×4 square respectively. The locations of 1's in that column say which points belong to that group (row, column, rank, suit). For one of the other blocks, like B_5, we recall that it corresponds to a location in the square. Referring to our example, we see that it contains a 1 at x_1, x_5, x_9, and x_{13}. This tells us that this specific location, B_5, is located in the first row (x_1), and first column (x_5) of the orthogonal matrix, and contains an A (x_9) and a ♥ (x_{13}).

We show the incidence matrix that we will try to fill in for the 6×6 case on the following page. Notice how I could not write out every single block, as it would not fit on one page, but the dots represent the other blocks that would be there.

4.1 Incidence matrix for 4×4 case

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}	B_{16}	B_{17}	B_{18}	B_{19}	B_{20}
x_1 (r_1)	1	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
x_2 (r_2)	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
x_3 (r_3)	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
x_4 (r_4)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
x_5 (c_1)	0	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
x_6 (c_2)	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
x_7 (c_3)	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0
x_8 (c_4)	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
x_9 (A)	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
x_{10} (2)	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	1	0
x_{11} (3)	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0
x_{12} (4)	0	0	1	0	0	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0
x_{13} $(\heartsuit)$	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0
x_{14} $(\diamondsuit)$	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	0	1	0	0	0
x_{15} $(\clubsuit)$	0	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	1
x_{16} $(\spadesuit)$	0	0	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	0	1	0

$x_1, \ldots, x_4 \;=\; r_1, \ldots, r_4,$ The 4 rows of the orthogonal matrix.
$x_5, \ldots, x_8 \;=\; c_1, \ldots, c_4,$ The 4 columns of the orthogonal matrix.
$x_9, \ldots, x_{12} \;=\; A, 2, 3, 4,$ The 4 symbols of one Latin square.
$x_{13}, \ldots, x_{16} \;=\; \heartsuit, \diamondsuit, \clubsuit, \spadesuit,$ The 4 symbols of the other Latin square.

$A\heartsuit$	$2\diamondsuit$	$3\clubsuit$	$4\spadesuit$
$2\clubsuit$	$A\spadesuit$	$4\heartsuit$	$3\diamondsuit$
$3\spadesuit$	$4\clubsuit$	$A\diamondsuit$	$2\heartsuit$
$4\diamondsuit$	$3\heartsuit$	$2\spadesuit$	$A\clubsuit$

4.2 Incidence matrix M for the 6×6 case (assuming such a case exists)

	B_1	B_2	B_3	B_4	B_5 $\cdots$ B_{10}	B_{11} $\cdots$ B_{16}	B_{17} $\cdots$ B_{22}	B_{23} $\cdots$ B_{28}	B_{29} $\cdots$ B_{34}	B_{35} $\cdots$ B_{40}
x_1	1									
x_2	1									
x_3	1									
x_4	1									
x_5	1									
x_6	1									
x_7		1								
x_8		1								
x_9		1								
x_{10}		1								
x_{11}		1								
x_{12}		1								
x_{13}			1							
x_{14}			1							
x_{15}			1							
x_{16}			1							
x_{17}			1							
x_{18}			1							
x_{19}				1						
x_{20}				1						
x_{21}				1						
x_{22}				1						
x_{23}				1						
x_{24}				1						

5 The code C of P and Lemma I

We aim *not* to prove that we *have* a TD(4,6), but rather to show what properties this design *would* have if it existed. In the end we will use these properties to show that it is *not* possible for this design to exist. To this end, suppose P is the PBD for a TD(4,6). We first put an upper bound on the dimension of our code, C, spanned by the rows of the incidence matrix.

Lemma I: $\dim C \leq 20$.

pf: Let $V = (GF(2))^{40}$, and for $u, v \in V$, let $\langle u, v \rangle$ denote the usual inner product (mod 2).
Recall that the rows ρ_i generate C and define

$$C^{\perp} = \{u \in V : \langle u, \rho_i \rangle = 0, 1 \leq i \leq 24\}.$$

Then $\left\langle \rho_i, \rho_j \right\rangle = 1$ for any i, j; so $\left\langle \rho_i, \rho_j + \rho_k \right\rangle = 0$ for any i, j, k.
If $\dim C = t$, let $\rho_{i_1}, \ldots, \rho_{i_t}$ be a basis.
Then the $t-1$ elements $\rho_{i_1} + \rho_{i_2}, \ldots, \rho_{i_1} + \rho_{i_t}$ are all in $C^{\perp}$ and are linearly independent.
So, $\dim C^{\perp} \geq \dim C - 1$. But, $\dim C^{\perp} + \dim C = 40$, so $\dim C \leq 20$.///

Now that we know $\dim C \leq 20$, we are led to conclude that there must be dependencies of the rows of M, since M has 24 rows. We will write a linear dependence as $\sum_{i \in I} \rho_i = 0$ for some $I \subseteq \{1, \ldots, 24\}$. This means that if we add some set of ρ_i's, or rows, then we will get 0 (mod 2).

In regard to P, such a linear dependence means that we have a subset $Y = \{x_i; i \in I\}$ of the points X such that $|B_k \cap Y|$ is even for all k ($1 \leq k \leq 40$). This tells us that the sub-matrix of M consisting of the rows for Y must have an even number of 1s in each column. The subset Y thus gives us a sub-matrix, formed by pulling certain rows from M that have this property.

We may note that the subsets $B_1 \cup B_2$, $B_1 \cup B_3$, and $B_1 \cup B_4$ each give us a dependence relation. When we say $B_1 \cup B_2$, we are referring to the sum:

$$\sum_{i \in B_1 \cup B_2} \rho_i = \sum_{i=1}^{12} \rho_i = 0 \pmod 2.$$

These three dependencies follow from the conditions on our pair of orthogonal Latin squares. The reason we only list these three dependence relations is that the other pairs of blocks among $B_1, \ldots, B_4$ follow trivially from these. For example, $B_2 \cup B_3 = (B_1 \cup B_2) \cup (B_1 \cup B_3)$. So this gives us 3 dependence relations, however since $\dim C \leq 20$, we must have one more dependence relation among the rows of our incidence matrix if there is to exist a TD(4,6). The lack of this dependence relation is where the existence of a TD(4,6) falls apart.

Similarly to the rows of M, the columns of M span a space D, which is its code in $(GF(2))^{24}$, where the 24 indicates that the column vectors have length 24. Saying we have a dependence relation of the rows of M is like saying we have a nonzero codeword in $D^{\perp}$, which is the dual code to D. We may think of Lemma I as saying that $\dim D^{\perp} \geq 4$.

6 Even sub-PBD and Lemma II

To summarize our progress, suppose P is the PBD of our TD(4,6) for a pair of 6×6 orthogonal Latin squares. The rows of the incidence matrix M span a subspace C of $GF(2)^{40}$ called the code of P. These 24 vectors are not linearly independent, and there are 3 basic dependencies formed by $B_1 \cup B_2$, $B_1 \cup B_3$, and $B_1 \cup B_4$. We also learned that there must be a fourth dependency not generated by these three. Let Y denote the subset of points corresponding to this dependence relation. Whenever we have a dependence relation like Y, we will call $\{Y, \{Y \cap B_i : 1 \leq i \leq 40\}\}$ an *even sub*-PBD.

Let us suppose our even sub-PBD given by Y has m points and b_i blocks of size i, where $i = 0, 2, 4, 6$. Our values for i lay in the fact that each column will have at most 6 ones in M, and that we need the blocks to be of even size when intersected with Y. Then, some counting tells us

$$\begin{aligned} b_0 + b_2 + b_4 + b_6 &= 40 && (1) \\ 0b_0 + 2b_2 + 4b_4 + 6b_6 &= 7m && (2) \\ b_2 + 6b_4 + 15b_6 &= \frac{m(m-1)}{2} && (3) \end{aligned}$$

Each of these equations can be described and explained in turn.

Equation 1:

This equation asserts that the rows of the incidence matrix for Y have length 40, and that each column corresponds to a block of length 0, 2, 4, or 6.///

Equation 2:

The right side of this second equation gives us our total number of ones in Y. There are 7 ones per row, and m rows in Y. The seven ones are a result of the fact that there will be six ones in each row from $B_5, \ldots, B_{40}$, with the remaining one in one of the first four blocks, $B_1, \ldots, B_4$. The six ones fall out of the fact that there will be only six blocks in the first row, so there will be six ones that correspond to x_1, six that correspond to x_2, and so forth, up to x_6, because we have a 6×6 orthogonal square, so of course there can only be six elements per row. The same goes with $x_7, \ldots, x_{12}$, in terms of columns as opposed to rows. Only six blocks can be in each column.

Likewise, each symbol of the first Latin square will only appear six times in the entire Latin square and, consequently, in the orthogonal square. If any symbol appeared more than six times, we would not have a Latin square, as each symbol can occur once in each row, and once in each column. This is the reason for there being six one's that correspond with each $x_{13}, \ldots, x_{18}$. The same reasoning goes for $x_{19}, \ldots, x_{24}$, in terms of the symbols of the second Latin square.

So far we have accounted for 6 ones per row, coming from blocks B_5–B_{40}. Let us now consider blocks B_1–B_4. Recall that B_1 corresponds to the rows of the orthogonal square, so there will be six ones in this block, one each corresponding to $x_1, \ldots, x_6$, giving us our seventh one for the rows from this group. Similarly, B_2 represents our columns, so there will be six ones in this block, one each intersecting $x_7, \ldots, x_{12}$, giving our seventh one for the rows from this group. B_3 and B_4 represent the six symbols of each Latin square, and they will both be blocks of size six, giving our seventh one for the rows corresponding to the groups $x_{13}, \ldots, x_{18}$ and $x_{19}, \ldots, x_{24}$.

The left side of equation (2) also gives the total number of 1s in Y, but it separates it into the number of blocks with zero ones, b_0, the number of blocks with two ones, b_2, the number of blocks with four ones, b_4, and the number of blocks with six ones, b_6.

Observe that, from the left side of the equation, we will end up with an even number, telling us that m must be an even number, seeing as how it is being multiplied by 7.///

Equation 3:

Every pair of 1s that share a column of the incidence matrix of Y corresponds to a pair of points that appear in a common block. Recall that every pair of points occurs together in exactly 1 block, so there are $\binom{m}{2}$ such pairs, giving us the right side of equation (3). But there are b_4 blocks of size 4, each with $\binom{4}{2}$ pairs of 1s, b_6 blocks of size 6, each with $\binom{6}{2}$ pairs of 1s, etc. This gives us the left side of equation (3).///

Now, if we combine equations (2) and (3), we have another equation which will tell us more about m.

$$b_4 + 3b_6 = \frac{m(m-8)}{8} \tag{4}$$

The right side of the above equation tells us that $m \geq 8$. This is because we must have $\frac{m(m-8)}{8} \geq 0$, or it would not make sense, as we would be claiming to having a negative amount of blocks of size 4 or 6. Now let

$$\frac{m(m-8)}{8} = k \geq 0$$

Then,

$$m(m-8) = 8k.$$

Since we know from Equation (2) that m is even, we may write m as $m = 2t$. Then,

$$\begin{aligned} m(m-8) &= 8k \\ 2t(2t-8) &= 8k \\ t(t-4) &= 2k \end{aligned}$$

and the last equation above tells us that t is even, so we may set $t = 2i$. Thus, we are left with

$$m = 2t = 2(2i) = 4i \Rightarrow \; m \equiv 0 \pmod{4}.$$

From this we know that m is a multiple of 4 and that $m \geq 8$. However, since m is the number of rows in Y, and since the complement of Y is also an even sub-PBD with 24-$|Y|$ points, we may assume without loss of generality that $m \leq 12$. But since m is also a multiple of 4, this really tells us that $m = 8$ or $m = 12$. This can be summed up in the following lemma.

Lemma II: If a TD(4,6) exists, then it contains an even sub-PBD having 8 or 12 points (rows), which is not the union of two groups of the TD.

7 The mysterious case of $m = 8$ and Lemma III

Using the four equations from the last section, we may cosider the case $m = 8$ and use this to solve for b_0, b_2, b_4, b_6. Therefore with the help of algebra we see that

$$\begin{aligned} b_0 &= 12 \\ b_2 &= 28 \\ b_4 &= 0 \\ b_6 &= 0 \end{aligned}$$

Therefore we know that we only have blocks containing zero ones, or two ones in Y. We also know that no three of our 8 rows are collinear. This means that no three are from one group of $\mathscr{G}$, since otherwise we would have a block (one of $B_1, \ldots, B_4$) with at least three 1s. Thus to get $m = 8$, we must have two rows from each group of $\mathscr{G}$. Let Q be the PBD formed from P by deleting the points in Y. Then Q has 16 points, or rows. We may split P into Y and Y', in our incidence matrix M as well, where Y' is the incidence matrix of Q. But first we will tell a little bit more about Q.

We know that in our original matrix M, that $B_1, \ldots, B_4$ are of size 6 each (contain 6 ones), and that the blocks $B_5, \ldots, B_{40}$ are of size 4. Recall that this is because each of $B_1, \ldots, B_4$ corresponds to the four groups of $\mathscr{G}$, and the blocks $B_5, \ldots, B_{40}$ correspond to one element from each of the four groups, because each block is an entry and therefore has a row, a column, and two symbols, one from each of the original Latin squares from which our orthogonal square was formed.

Because Y has two elements, or rows, from each group of $\mathscr{G}$, then there are still four elements from each group left, and these will go in Y'. Thus if we look at a specific block, B_1, two ones will be found in Y, and the remaining four ones will be found in Y'. This can be better seen on the next page in the revised matrix which we will call M_{jr}. Okay, we'll call it $\widehat{M}$ instead.

Now in Y we also have 12 blocks with zero ones. Since our blocks $B_1, \ldots, B_4$ have two ones in Y, we know these 12 blocks must be found in the blocks $B_5, \ldots, B_{40}$. These same 12 blocks will have 4 ones in Y', because each of these blocks must be of size 4 in P. We may now safely say that Y' has four blocks of size four in $B_1, \ldots, B_4$, and 12 blocks of size 4 in $B_5, \ldots, B_{40}$, for a total of 16 blocks of size 4.

Now remember that Y also had 28 blocks of size 2. But we used up four of these blocks with $B_1, \ldots, B_4$. This means that there are 24 other blocks left in $B_5, \ldots, B_{40}$ that are of size 2. These same blocks of size 2 will also be of size 2 in Y', since every one of these blocks is of size 4 in P. Since Y' has 16 blocks of size 4, and only a total of 40 blocks in all, the remaining 24 will all be of size 2.

For convenience, we renumber blocks B_5–B_{40} if necessary so that B_5–B_{28} have size 2 in Y and B_{29}–B_{40} have size 0 in Y.

7.1 The new incidence matrix: $\widehat{M}$

	B_1	B_2	B_3	B_4	B_5	$\cdots$	B_{10}	B_{11}	$\cdots$	B_{16}	B_{17}	$\cdots$	B_{22}	B_{23}	$\cdots$	B_{28}	B_{29}	$\cdots$	B_{34}	B_{35}	$\cdots$	B_{40}
x_1	1																					
x_2	1																					
x_7		1							6	ones	per	row						0	ones	per	row	
x_8		1																				
x_{13}			1																			
x_{14}			1						2	ones	per	col.						0	ones	per	col.	
x_{19}				1																		
x_{20}				1																		
x_3	1																					
x_4	1																					
x_5	1																					
x_6	1																					
x_9		1																				
x_{10}		1						3	ones	per	row	(Lem.	III)				3	ones	per	row	(Lem.	III)
x_{11}		1																				
x_{12}		1																				
x_{15}			1																			
x_{16}			1																			
x_{17}			1						2	ones	per	col.						4	ones	per	col.	
x_{18}			1																			
x_{21}				1																		
x_{22}				1																		
x_{23}				1																		
x_{24}				1																		

The top portion is the incidence matrix Q' for Y and the bottom portion is the incidence matrix Q for Y'. Together, we have $\widehat{M}$.

7.2 A graph named G

The labeling used to form $\widehat{M}$ was formed without loss of generality. For example, I could have picked x_3 and x_4 to belong in Y and had x_1 and x_2 in Y'. We will now rename our x_i's so that we can separate them into groups corresponding to Y and Y' in a more orderly fashion.

Let $Y = \{a, b, c, d, e, f, g, h\}$ and suppose $Y' = \{1, 2, \ldots, 16\}$. We label our groups of $\mathscr{G}$ as $\{a, b, 1, 2, 3, 4\}$, $\{c, d, 5, 6, 7, 8\}$, $\{e, f, 9, 10, 11, 12\}$, and $\{g, h, 13, 14, 15, 16\}$.

Now define a graph G, with vertex set Y', whose edges are the 24 blocks of size two in the PBD Q. The vertices of the graph would look something like the following. We have drawn no edges as of right now because we are not yet sure as to where they will go. The separate groups are also sectioned off.

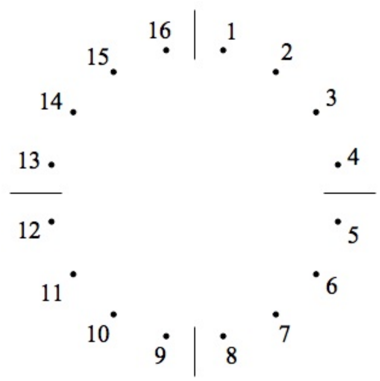


Figure 1: Graph G

Lemma III: (1) G is triangle-free;

(2) G is three-regular, and any point of G is joined to precisely one point from each of the three groups of G not containing that point.

pf: We prove statement (2) first. To see that G is three-regular, choose any point i, $1 \leq i \leq 16$. If i occurs in x blocks of size two and y blocks of size four in Q, then $x + y = 7$ and $x + 3y = 15$. To obtain the second equation, observe that the number of pairs of ones that share a column in Q and contain the point i is 15; one for each pair of rows of Q containing i. Alternately, each of the x blocks of size 2 has one such pair and each of the y blocks of size 4 has three such pairs. So $x = 3$ (and $y = 4$). The three blocks of size two must (in P) contain all six points of Y which are not in the same group as i. Thus statement (2) follows.

	B_5	B_6	B_7	B_8	$\cdots$	B_{16}	B_{17}	$\cdots$	B_{22}	B_{23}	$\cdots$	B_{28}
a			1	1								
b												
c		1										
d												
e	1											
f												
g	1		1									
h		1		1								
1	1	1										
2												
3												
4												
5	1		1	1								
6												
7												
8												
9		1	1	1								
10												
11												
12												
13												
14												
15												
16												

To prove (1), suppose that 1 5 9 is a triangle in G. In the PBD P we have a block 1 5 e g, say, and a block 1 9 c h (without loss of generality). This is shown above with B_5 and B_6. Then the block containing 5 and 9 must be 5 9 x g or 5 9 x h, where x is a or b. Above, the first case corresponds to B_7. If we compare B_7 with B_5, we see that the pair g 5 is repeated. The second case corresponds to B_8, and if we compare this with B_6, we see that the pair h 9 is repeated. This contradiction proves that G is triangle-free.///.

8 Property A and Lemma IV

We now attempt to construct the PBD P. Let us first suppose that there is some point i ($1 \leq i \leq 16$) such that the three neighbors of i in G occur in a block of P. We can suppose that $i = 1$ has neighbors $5, 9$, and 13 in G, and 2 5 9 13 is a block of P. Below we show G displaying the neighbors of 1.

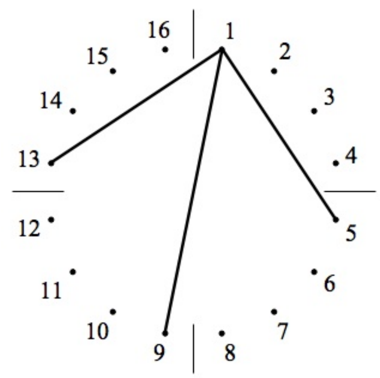


Figure 2: G and the neighbors of 1

Now, without loss of generality, we have blocks 1 6 10 14, 1 7 11 15, and 1 8 12 16; 2 5 9 13, 2 6 11 16, and 2 7 12 14; and six blocks, each of which contains one point from $\{3, 4\}$ and one from $\{5, 9, 13\}$. This is shown in Figure 3. We will call this graph G'. The schematic represented by G' is not taken from Stinson's original paper, but we believe it is helpful in visualizing a few key aspects of the proof. Notice how 5, 9, and 13 are all only of degree 1 at this point. Six more blocks are required.

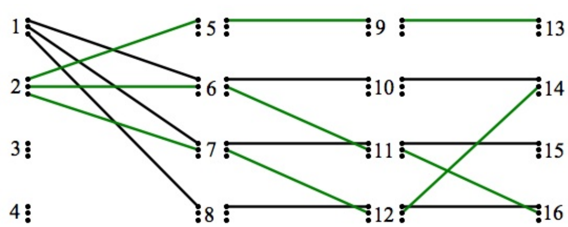


Figure 3: Blocks 1 and 2 of G'

The neighbors of 2 in G are 8, 10, and 15. The above two figures and the matrix interpretation of such actions are all displayed on the following page. Blocks B_5 through B_{28} go with Graph G, and blocks B_{29} to B_{34} go with the graph on the right, our G'.

	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}	B_{16}	$\cdots$	B_{29}	B_{30}	B_{31}	B_{32}	B_{33}	B_{34}	B_{35}	B_{36}	B_{37}	B_{38}	B_{39}	B_{40}
1	1	1	1											1	1	1									
2				1	1	1											1	1	1						
3																									
4																									
5	1																1								
6														1				1							
7															1				1						
8				1												1									
9		1															1								
10					1									1											
11															1			1							
12																1			1						
13			1														1								
14														1					1						
15						1									1										
16																1		1							

Figure 4: Graph G and Blocks of 1 and 2

The three pairs 8 10, 8 15, and 10 15 must occur in three blocks which contain 3 x or 4 y ($x, y \in \{5, 9, 13\}$). This causes a pair to be repeated (one of 3 8, 3 10, 3 15, 4 8, 4 10, or 4 15). Here is how:

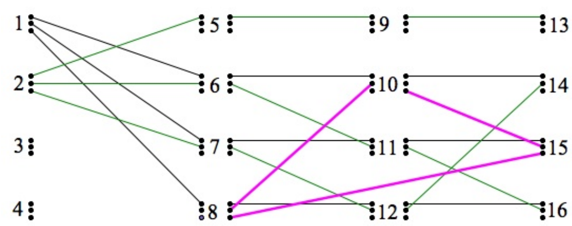


Figure 5: G' showing the three pairs of blocks needed

If we choose {3 5 10 15}, then we still need to use the pairs 8 10 and 8 15, as seen in Figure 6.

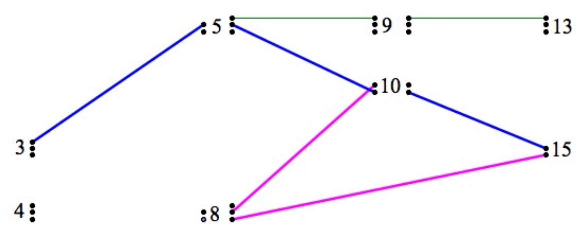


Figure 6: G' showing one scenario

Let us choose 3 8. Then we can either do {3 8 10 13} which would cover the pair 8 15, or we may do {3 8 9 15}, as shown in Figure 7.

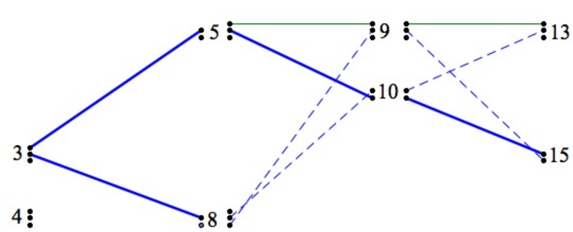


Figure 7: G' in the next step of the same scenario

If we do the first option of {3 8 10 13}, we run into a repeated pair of 3 10, as shown below.

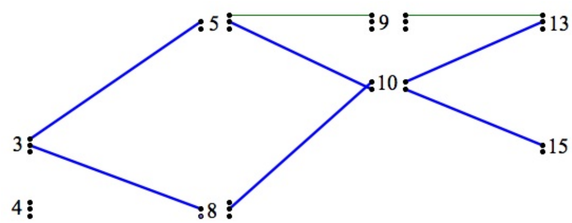


Figure 8: Contradiction 1 of G'

In our second option of {3 8 9 15}, we run into a repeated pair of 3 15, as seen in Figure 9.

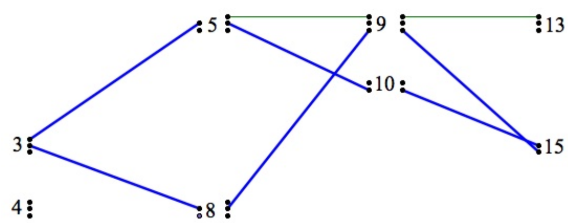


Figure 9: Contradiction 2 of G'

A similar argument follows for the case of {4 x y z}, where $x = 5$ or 8, $y = 9$ or 10, and $z = 13$ or 15. This is a recurring contradiction of repeating pairs.

Thus we may assume the following property holds: (A) For any point i ($1 \leq i \leq 16$) the three pairs formed by the three neighbors of i in G occur in different blocks of P (and G').

Now let us suppose (without loss of generality) that, in G, 1 is adjacent to 5, 9, and 13; 2 is adjacent to 6, 10, and 14; 3 is adjacent to 7, 11, and 15; and 4 is adjacent to 8, 12, and 16. This can all be seen in Figure 10 on the next page.

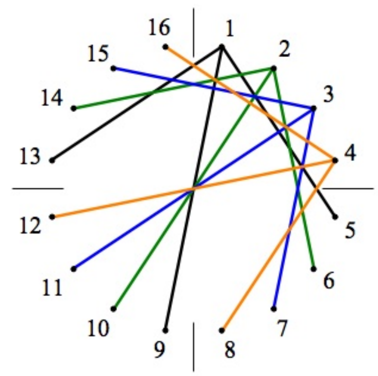


Figure 10: G

By property (A), the point 1 must occur with exactly one pair from each of the three triangles 6 10 14, 7 11 15, and 8 12 16. This means that we must have 1 with 6 10, 6 14, or 10 14. It is a similar concept for the other two triangles. Suppose 1 6 10 15 is a block; then 1 7 11 16 and 1 8 12 14 are forced to be blocks. This is shown through the next few diagrams. Remember by property A that 1 may not be with one of its neighbors, so it may not go with 5, and because it is already with 6 in a block by assumption. We need one element from each group, so the only other two possible points in the group containing $\{5, 6, 7, 8\}$ are 7 and 8. This step is shown in Figure 11.

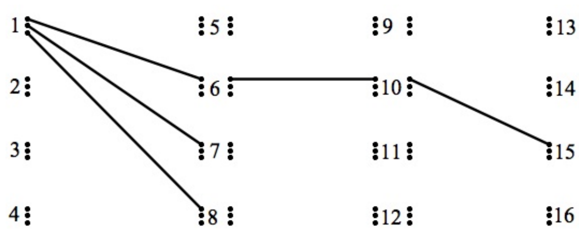


Figure 11: G' blocks of 1

We now have the blocks 1 6 10 15, 1 7 x_1 y_1, 1 8 x_2 y_2. Looking at 1 7 x_1 y_1, we need to end up with the pair 7 11, 7 15, or 11 15, whether it is in the block 1 7 x_1 y_1, or 1 8 x_2 y_2. However, we already have the block 1 6 10 15, so 15 is out. This forces the pair 7 11, and forces 1 7 11 y_1 to be a block, and 1 8 12 y_2 to be a block because 12 is the only other option, since 9 is a neighbor of 1. This step is shown on the next page.

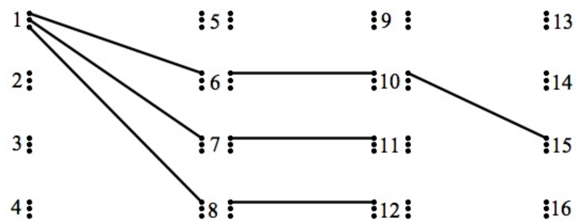


Figure 12: G' blocks of 1

Now because 8 12 is appearing in a block and we don't want triangles, we may not have the block 1 8 12 16, as they are all neighbors of 4, according to G and our assumption. Thus we are forced to have 1 8 12 14, because 15 is already taken and 13 is off limits, being a neighbor of 1. This also forces the block 1 7 11 16. We show this through Figure 13.

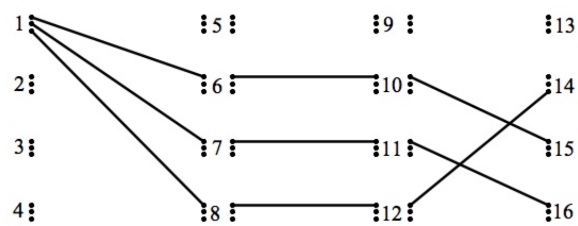


Figure 13: G' blocks of 1

The three pairs 6 10, 7 11, and 8 12 are all from the same two groups, one being $\{5, 6, 7, 8\}$, and the other being $\{9, 10, 11, 12\}$. But, then, where can the pair 5 9 occur? It must occur at some point. If 2 5 9 x is a block, then similar to the case of the blocks of 1, we need to have the blocks 2 7 y_1 z_1, and 2 8 y_2 z_2, as shown below.

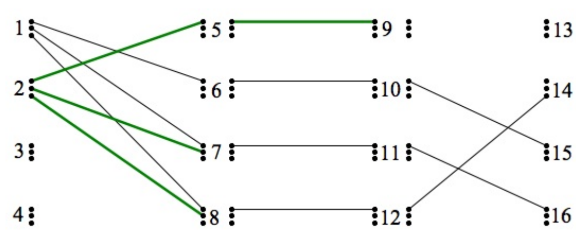


Figure 14: G' blocks of 1 and 2

We have already used the pairs 7 11, and 8 12, so we are forced to switch these this time, yielding 7 12, and 8 11, seeing as how 10 is a neighbor of 2 and is off limits. This forces the block 2 8 11 15 because with 2 8 11 z_2, we need either the pair 8 16, giving us the block 2 8 11 16, or the pair 11 15, giving us the block 2 8 11 15. In forming the blocks of 1, we already used up the pair 11 16, so this results in the block 2 8 11 16. This can be seen here.

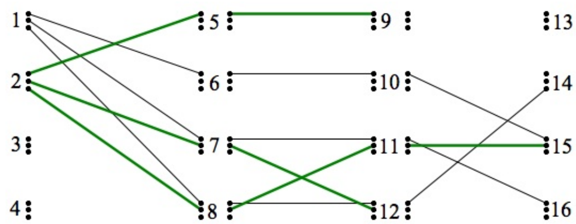


Figure 15: G' blocks 1 and 2

Now because we already have the pair 5 9, and 5 9 13 are neighbors of 1, we are forced to have the block 2 5 9 16, since 15 is taken and both 14 and 13 are not allowed to be in this block. This also forces the block 2 7 12 13, as seen below in Figure 16.

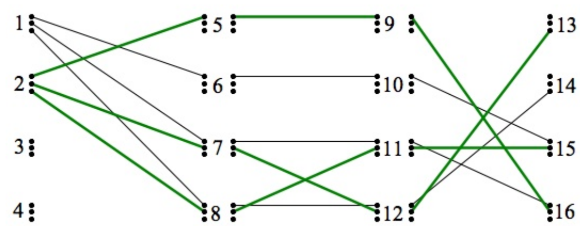


Figure 16: G' blocks 1 and 2

However if we observe the graph above, through the block 2 7 12 13 we accomplished no traditional pairs of any of the original neighbors. This means that we didn't get the pair 7 15 (7 11 was already taken), we didn't get the pair 12 16 (8 12 was already taken), and we didn't get a pair involving 13 either. As this block yielded no traditional pair from the neighbors in G, we have reached a contradiction. A similar argument will also yield contradictions in the case of 3 5 9 x and 2 5 9 x. Therefore, the pair 5 9 does not occur. This contradiction proves Lemma IV.

Lemma IV: No TD(4, 6) contains an even subset with eight points (i.e., $D^{\perp}$ has no codewords of weight eight.)

9 The last hope and Lemma V

We must now consider the possibility $m = 12$. There are several ways the twelve points can be distributed among the four groups:

$$\begin{array}{rl} (i) & 6, 6, 0, 0; \\ (ii) & 6, 4, 2, 0; \\ (iii) & 6, 2, 2, 2; \\ (iv) & 4, 4, 4, 0; \\ (v) & 4, 4, 2, 2. \end{array}$$

Case (i) is the situation of an even subset formed by two groups; we have already noted the existence of these even subsets. For cases (ii)-(v) we use the fact that the sum of two even subsets (mod 2) is again an even subset. (This corresponds to taking the sum of two codewords in $D^{\perp}$.) In each case, add the given even subset to the even subset formed by the first two groups. In each case, an even subset of size eight or size four is produced. But we have already eliminated these cases.

Thus we have

Lemma V: No TD(4, 6) contains an even subset of size twelve, which is not the union of two groups of the TD.

Summarizing, we have our main theorem.

Theorem: There does not exist a pair of orthogonal Latin squares of order six.

pf: Lemata 2-5.

10 Curriculum Activity I

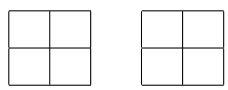
For the curriculum, I designed a worksheet geared toward an early college-level mathematics class, namely Math 105: "Excursions in mathematics", taught by Joe Ediger. I worked through this worksheet with the class by explaining the examples that were on the worksheet, and helping them apply the example to a more difficult question. I spent about 30% of the class time writing on the board, and the rest of the time walking around and helping each group work toward the answer. In each activity, I first provide the worksheet, followed by the answer key, and reflection.

I began with the introduction of Latin squares. I first worked through the $n = 2$ cases with the class before moving on to an example of the $n = 3$ case.

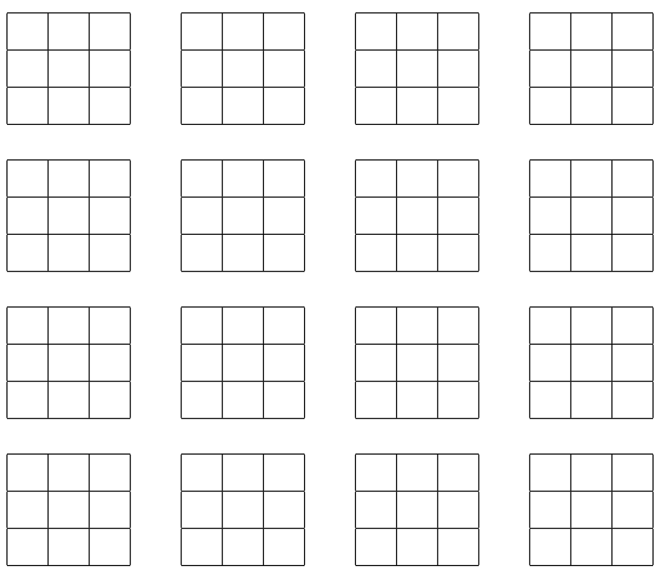
10.1 Latin Squares

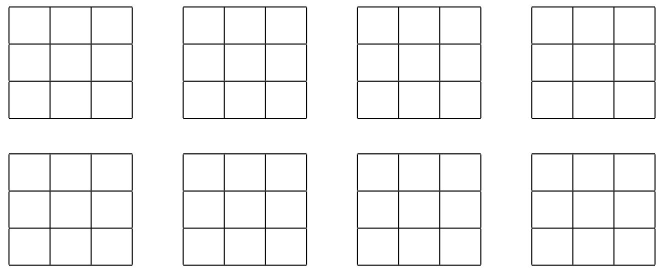
Latin Square: A Latin Square of order n is an $n \times n$ array with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column.

Example. $n = 2$. There are 2 cases.



Example. $n = 3$. There are 12 cases. (Then why so many squares? In case you need a second chance...)





Can you justify that you have all 12?

There is a cool method of finding all 12 by finding where one symbol will go. There will be two of each of the following cases:

1		
	1	
		1

		1
	1	
1		

1		
		1
	1	

		1
1		
	1	

	1	
1		
		1

	1	
		1
1		

Why?

10.2 Latin Squares–key

Latin Square: A Latin Square of order n is an $n \times n$ array with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column.

Example. $n = 2$. There are 2 cases.

1	2
2	1

2	1
1	2

Example. $n = 3$. There are 12 cases.

1	2	3
3	1	2
2	3	1

1	3	2
2	1	3
3	2	1

2	3	1
3	1	2
1	2	3

3	2	1
2	1	3
1	3	2

1	2	3
2	3	1
3	1	2

1	3	2
3	2	1
2	1	3

2	3	1
1	2	3
3	1	2

3	2	1
1	3	2
2	1	3

2	1	3
1	3	2
3	2	1

3	1	2
1	2	3
2	3	1

2	1	3
3	2	1
1	3	2

3	1	2
2	3	1
1	2	3

Can you justify that you have all 12? *See below.*

There is a cool method of finding all 12 by finding where one symbol will go. There will be two of each of the following cases:

1		
	1	
		1

		1
	1	
1		

1		
		1
	1	

		1
1		
	1	

	1	
1		
		1

	1	
		1
1		

Why? *This is because we know that given the placement of one symbol, we have two symbols left to place. This gives us two possibilities for each case because we need only switch the roles of the remaining two symbols for the second case, meaning a 2 becomes a 3, and vice versa. For example, looking at the first square above, we have the following two cases:*

1	2	3
3	1	2
2	3	1

1	3	2
2	1	3
3	2	1

10.3 Reflecting on Activity I

I notice that there are some unexplained portions on the worksheet, but many of these explanations were provided in class.

In introducing the class to Latin squares, I showed the students one of the 2×2 examples, and asked if anyone could tell me what the other square would look like. It took a little convincing, but one student did provide the answer and I then added to the answer an explanation of why there are only 2 cases. This is because we exhaust our possibilities.

I also provided the students with a 3×3 example before I asked them to try and find the other 11 cases. I did not wait for everyone to find all 11, but I made sure that everyone had about 9 and understood the concept before I moved on to justifying how we knew we had found all 12. I then explained to them an option for finding all 12 by finding where one symbol would go (I used 1, as shown on the worksheet), and explaining that because we have two other symbols left, we know that there are two possibilities for each case.

The reason I provide so many blank squares is because I believed that if I left it up to the students to fill in the blanks, they would learn and listen more as opposed to if I provided the answers and then explained. I really wanted the students to feel like we were all doing the worksheet together.

In the future, I would have given an example compare what a Latin square would look like, versus an array that would not qualify as a Latin square. I would have given exercises involving non-Latin squares, and would ask the students which row or column should be switched in order to form a Latin square. I would also have spent more time on justifying how to find all 12 Latin squares of order $n = 3$. More than that, I would arrange the activity so that the students are prompted to discuss how many possible Latin squares there are of orders 2 and 3. I believe that the students could have collectively worked together in a discussion to come to the conclusions that there were 2 Latin squares of order 2, and 12 Latin squares of order 3. In my desire to ensure understanding, I gave away these specific points, however I do believe they could have come to these conclusions on their own.

11 Curriculum Activity II

After the introduction to Latin squares, I showed the class how to construct a pair of orthogonal Latin squares. The class seemed to enjoy this part, as they used playing cards to help them discover and understand this concept.

11.1 Orthogonal Latin Squares

Two Latin Squares of order n are said to be orthogonal if every ordered pair of symbols occurs exactly once among the n^2 pairs.

Example. We may have an easier time looking at them as Card numbers and suits:

A	2	3
3	A	2
2	3	A

♥	◆	♣
◆	♣	♥
♣	♥	◆

A♥	2◆	3♣
3◆	A♣	2♥
2♣	3♥	A◆

Can you find a pair of 4×4 orthogonal Latin Squares?

Note: There is no pair of orthogonal Latin Squares of order 2 and 6.

36 Officers Problem (1780): How can a delegation of six regiments, each of which sends a colonel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular array such that no row or column duplicates a rank or a regiment? The answer is that no such arrangement is possible.

In 1900, Gaston Tarry proved Euler's conjecture by listing out all 812,851,200 cases. He was able to simplify the problem by working with reduced squares to checking only 9408 pairs, all done by hand. Then in 1984 Douglas Stinson provided a short, non-computer proof.

11.2 Orthogonal Latin Squares–key

Two Latin Squares of order n are said to be orthogonal if every ordered pair of symbols occurs exactly once among the n^2 pairs.

Example. We may have an easier time looking at them as Card numbers and suits:

A	2	3
3	A	2
2	3	A

:

♥	◆	♣
◆	♣	♥
♣	♥	◆

⇒

A♥	2◆	3♣
3◆	A♣	2♥
2♣	3♥	A◆

Can you find a pair of 4×4 orthogonal Latin Squares?

A	2	3	4
2	A	4	3
3	4	A	2
4	3	2	A

:

♥	♦	♣	♠
♣	♠	♥	♦
♠	♣	♦	♥
♦	♥	♠	♣

⇒

A♥	2♦	3♣	4♠
2♣	A♠	4♥	3♦
3♠	4♣	A♦	2♥
4♦	3♥	2♠	A♣

Note: There is no pair of orthogonal Latin Squares of order 2 and 6.

36 Officers Problem (1780): How can a delegation of six regiments, each of which sends a colonel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular array such that no row or column duplicates a rank or a regiment? The answer is that no such arrangement is possible.

In 1900, Gaston Tarry proved Euler's conjecture by listing out all 812,851,200 cases. He was able to simplify the problem by working with reduced squares to checking only 9408 pairs, all done by hand. Then in 1984 Douglas Stinson provided a short, non-computer proof.

11.3 Reflecting on Activity II

In section 10.2, I started letting the students use cards to find orthogonal Latin squares. Here they became less skeptical and a little more involved. It felt good to hear different groups calling for my help all at once. Of course I don't want them all to be lost, but I was happy for their enthusiasm and interest. It was great that they cared to understand. There were even a few groups who never wanted my help because they knew that if something was possible that they could do it themselves. I can certainly relate to students like that and gave hints when they would have them.

There was a lot of trouble with the 4×4 case, and some even tried to ask me if they could prove that it was impossible. This made me smile and I assured them that while I was making this worksheet it took me a little while to find a 4×4 case that worked, so although it is difficult it is possible. After a lot of effort every group had found a 4×4 case that worked, some with hints, and some all on their own. Of course, within groups there were a few break away students who were trying to find a case on their own and without the help of the group, and to my knowledge only one young lady had not found a case but I had helped the other member in her group find a case and told her that the option was there if she gave up. I wasn't concerned with giving her the answer because I could tell by my analysis of her work when I stood near her that she knew what she was doing and what she was looking for and wanted nothing more than to find the answer herself.

After the 4×4 scenario, I moved on to explaining that what I was working on was how a 6×6 case did not exist. I explained the history of the problem and how there are over 812,000,000 possible Latin squares. Judging by their reactions, they found it unreasonable that someone had worked through these cases, even though through reduced squares the amount was significantly lessened. I also explained to them that in 1984 someone came up with a four page proof and this is the one through which I am working.

The next time I use this activity, I would love to explain to show them how to always find a Latin square of odd order. As I had many things to cover, I did not want to focus on any one thing if it was unnecessary. Of course, I would like them to know all of the tricks that I have discovered and learned along the way, but the concept must be taught before the shortcut, else the shortcut may never be understood. I also would like to have been more prepared with the knowledge of how many pairs of orthogonal Latin squares there were for certain orders. I was questioned by one student who forced me to think on my feet about something that sounded valid, but without all the proper work already done, I couldn't give him a solid confirmation. I thought about it later and discovered that it was true, yet it was too late.

12 Curriculum Activity III

After the class was comfortable with finding pairs of orthogonal Latin squares, I moved on to Magic squares. In this activity, after some examples, the students were asked and helped to find the constant of a magic square with the help of the formula for the sum of the first k integers.

12.1 Magic Squares

Latin squares have a long history, stretching back at least as far as medieval Islam (c. 1200), when they were used on amulets-“objects that protect a person from trouble”.

A relative of the Latin Square is the Magic Square. The earliest known magic square is Chinese, recorded around 2800 B.C. Fuh-Hi described the ”Loh-Shu”, or ”scroll of the river Loh”. It is a typical 3x3 magic square except that the numbers were represented by patterns not numerals.

Magic Square: A magic square of order n is an arrangement of n^2 numbers, usually distinct integers, in a square, such that the n numbers in all rows, diagonals, and columns sum to the same constant.

Example. $n = 3$. (I don’t know how many cases there are, but the following is not unique)

2	7	6
9	5	1
4	3	8

Example. $n = 4$.

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Can you find the Constant?
Hint: The sum of the first $1, 2, ..., k$ numbers is

$$1 + 2 + \cdot + k = \frac{k(k+1)}{2}$$

12.2 Magic Squares–key

Latin squares have a long history, stretching back at least as far as medieval Islam (c. 1200), when they were used on amulets-“objects that protect a person from trouble”.

A relative of the Latin Square is the Magic Square. The earliest known magic square is Chinese, recorded around 2800 B.C. Fuh-Hi described the ”Loh-Shu”, or ”scroll of the river Loh”. It is a typical 3x3 magic square except that the numbers were represented by patterns not numerals.

Magic Square: A magic square of order n is an arrangement of n^2 numbers, usually distinct integers, in a square, such that the n numbers in all rows, diagonals, and columns sum to the same constant.

Example. $n = 3$. (I don’t know how many cases there are, but the following is not unique)

2	7	6
9	5	1
4	3	8

Example. $n = 4$.

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Can you find the Constant?
Hint: The sum of the first $1, 2, ..., k$ numbers is

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

Now, we are finding the sum of the first k^2 numbers, since our $k = n$ where we have an $n \times n$ array. So we are arranging the first n^2 numbers in this array. Thus, we need to basically multiply our k term in the above equation by another k as follows:

$$1 + 2 + \cdots + k^2 = \frac{k^2\left(k^2+1\right)}{2}$$

Now in order to find our constant c, we must remember that we want our sum to be the same for each row, column, and diagonal. However, we have three rows (three columns), and we distribute all k^2 numbers within these k rows, so we need only divide by k. Therefore,

$$\begin{aligned} c &= \frac{k^2\left(k^2+1\right)}{2k} \\ &= \frac{k\left(k^2+1\right)}{2} \end{aligned}$$

12.3 Reflecting on Activity III

The fun continued when I introduced the class to a relative of Latin squares, called Magic squares. I explained the definition with the help of the $n = 3$ case. I then had the best intention of helping them derive the constant to which the rows, columns, and diagonals summed, but I wrote down the wrong formula. Joe Ediger pointed out my mistake in a very polite way, though I was at first skeptical, not believing that I would mistake the sum of the first $1, 2, \ldots, k$ numbers. I was soon convinced that he was correct by trying out a case myself, and apologized as quickly as possible. I then told the class that if we know the constant, then we at least know what can or cannot be in a row, column, or diagonal together in a magic square.

Due to my mistake, I felt as though I should help them derive the formula for the sum, myself, although I was certainly thrown off and am sure I could have done a much better job. I know that I did not provide a clear explanation on the derivation of the constant from the formula for the sum of the first k numbers. In the end I explained what the formula was to find the constant, and I told them that it worked for all n magic squares. A student asked if I would give an example to show it worked, and I provided the $n = 3$ example, and then Joe suggested that the class try to find the $n = 4$ constant. I thought that the student's question along with Joe's suggestion really helped out my rather poor explanation, and was very thankful.

Next time I use this activity, I will certainly not provide the class with my inaccurate definition for finding the sum of the first k integers. It provided a fair amount of confusion, and there were a few minutes where I lost some composure, as I was worried I would make a mistake through derivation. I would also like to perhaps let them first question and wonder how to find the constant before I tell them that there is a way to find the constant. In my desire to reach the next section, I did not give them enough time to explore the possibility that there is a way to find the constant.

13 Curriculum Activity IV

When the class had an idea of how to find the constant, I showed them an easier way for constructing a magic square, through a pattern of number placement. I started with the odd order case, and would have moved onto the even case for multiples of 4, had I enough time.

13.1 Forming magic squares

We first show a method of finding a magic square of odd order.

Example. $n = 3$. Start with 1 in center square. Then move up one square and to the right one square. If this square is taken by another number, then move straight down one square. We only move down one square if and only if we cannot move up and right. So, in general, this downward movement will only happen once every few moves because, in general, moving up and right will be available. When we run out of squares, we must wrap around to the other side, whether it be row or column. However when we wrap around to the other side, we remain in the same row or column from which we came. The procedure below should help.

	1	

	1	
		2

	1	
3		
		2

	1	
3		
4		2

	1	
3	5	
4		2

	1	6
3	5	
4		2

	1	6
3	5	7
4		2

8	1	6
3	5	7
4	9	2

Can you find a 5×5 magic square?

Magic Squares of Even Order $4k$ (Multiples of 4)

Example. $n = 4$. First list out all numbers:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Then keep corners and middle portion:

1			4
	6	7	
	10	11	
13			16

Then take remaining numbers and reflect twice. Once vertically, and once horizontally, over the center of the square.

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Can you find a magic square of order 8?

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Don't yet know how to find a magic square of even order $4k + 2$. (Even numbers that are non-multiples of 4)

13.2 Finding Magic squares–key

We first show a method of finding a magic square of odd order.

Example. $n = 3$. Start with 1 in center square. Then move up one square and to the right one square. If this square is taken by another number, then move straight down one square. We only move down one square if and only if we cannot move up and right. So, in general, this downward movement will only happen once every few moves because, in general, moving up and right will be available. When we run out of squares, we must wrap around to the other side, whether it be row or column. However when we wrap around to the other side, we remain in the same row or column from which we came. The procedure below should help.

	1	

	1	
		2

	1	
3		
		2

	1	
3		
4		2

	1	
3	5	
4		2

	1	6
3	5	
4		2

	1	6
3	5	7
4		2

8	1	6
3	5	7
4	9	2

Can you find a 5×5 magic square?

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Magic Squares of Even Order $4k$ (Multiples of 4)

Example. $n = 4$. First list out all numbers:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Then keep corners and middle portion:

1			4
	6	7	
	10	11	
13			16

Then take remaining numbers and reflect twice. Once vertically, and once horizontally, over the center of the square.

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

Can you find a magic square of order 8?

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

1	2	62	61	60	59	7	8
9	10	54	53	52	51	15	16
48	47	19	20	21	22	42	41
40	39	27	28	29	30	34	33
32	31	35	36	37	38	26	25
24	23	43	44	45	46	18	17
49	50	14	13	12	11	55	56
57	58	6	5	4	3	63	64

Don't yet know how to find a Magic square of even order $4k + 2$. (Even numbers that are non-multiples of 4)

13.3 Reflecting on Activity IV

This activity was all about showing the class an easier way to find matin squares of certain orders. Starting with odd order Latin squares, I worked through the $n = 3$ case on the board by the method about which I had read, and hadn't realized that there was confusion among the students until I walked around looking at everyone's efforts to find the $n = 5$ case through the same method, which I then decided was not as easy as I thought.

The biggest confusion came from when to move down one square as opposed to up one square and then to the right one square. Of course the $n = 5$ case is much larger so the moments of switching methods happen more frequently. Furthermore, I could have explained the "wrap around" method better, as well as the fact that after we move down one square, then we go back to the original method of going up and to the right one square each. Because there was so much confusion, I ended up showing the class on the board how to form the $n = 5$ magic square right before the end of the class.

It is unfortunate that I was unable to take more time in showing the class how to find a magic square of odd order through a slower step-by-step process. I know that I should have provided a better explanation of the case where $n = 3$, and then should have helped them start the case where $n = 5$.

I also wanted to show the class how to find a magic square of even order $4k$, for multiples of 4. I actually ended up apologizing to one young lady because I had told her to hold on for that because I was going to explain it to the entire class at once. When time ran out, I approached her and tried to give her a quick explanation, but I am sure it was not as detailed as she would have liked. It thrilled me that she was interested because this was the same young lady who, at the beginning of the class, was very skeptical to be in class that day and had asked me if there was any math in what we were doing. That change in her attitude from the beginning of the class to the end really uplifted my confidence as an engaging educator.

The reasoning behind moving from Latin squares to magic squares, as opposed to continuing to the graph theory behind the proof of the nonexistence of a pair of 6×6 orthogonal Latin squares is due to the assumption that the students at this particular level would not be "up to the theory". Also, the lure of magic squares seemed to be a related and useful direction with which to go. In the future, I would include how Euler related Latin squares to magic squares in formulation of this "Problem of the 36 Officers".

The students learned how to form Latin squares, Orthogonal Latin squares, magic squares of odd order, and finally how to find the constant in a magic square of any order. They were given the opportunity to explore something on their own that was mathematical but not so technical that it takes an hour to explain or care about. Furthermore, the next time a sudoku comes their way, they will think about it differently, and that is part of the joy of teaching mathematics...showing students a different way to think about something that is seemingly common and overlooked. The students learned to appreciate the deep mathematics that can be hidden in a simple puzzle.

References

[1] Stinson, D.R.. "A Short Proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six". Journal of Combinatorial Theory, Series A, Volume 36, pg. 373-376, 1984.

[2] Phillips, Tony. "Latin Squares in Practice and in Theory I". AMS Feature Column Archive. July-August 2001. http://www.ams.org/featurecolumn/archive/latinI1.html

[3] Phillips, Tony. "Latin Squares in Practice and in Theory II". AMS Feature Column Archive. September 2001. http://www.ams.org/featurecolumn/archive/latinII1.html

[4] Weisstein, Eric W. "36 Officer Problem." From *MathWorld*–A Wolfram Web Resource. http://mathworld.wolfram.com/36OfficerProblem.html.

[5] L. Euler, Recherches sur une nouvelle esp'ece de quarres magiques. Opera Omnia, Ser. I, Vol 7, 291-392, Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen 9 (1782), 85-239. Also available online at http://www.eulerarchive.org.

[6] http://www.gap-system.org/ history/Biographies/Tarry.html.