Sets of Mutually Orthogonal Sudoku Latin Squares

Ryan M. Pedersen and Timothy L. Vis

Ryan Pedersen (Ryan.Pedersen@ucdenver.edu) received his B.S. in mathematics and his B.A. in physics from the University of the Pacific, and his M.S. in applied mathematics from the University of Colorado Denver, where he is currently finishing his Ph.D. His research is in the field of finite projective geometry. He is currently teaching mathematics at Los Medanos College, in Pittsburg California. When not participating in something math related, he enjoys spending time with his wife and 1.5 children, working outdoors with his chickens, and participating as an active member of his local church.

Timothy Vis (Timothy.Vis@ucdenver.edu) has a B.A. in mathematics from Dordt College and an M.S. in applied mathematics from the University of Colorado Denver, where he is currently pursuing a Ph.D. His research interests lie in finite projective geometry, and until recently, he could often be seen hunched over pages covered in zeros and ones. When he isn't doing math, he tends to the technological aspects of his wife's artwork as her photographer and webmaster.

In recent years, the number puzzle Sudoku has gained great popularity. A solution to the puzzle is obtained by filling in a 9×9 grid, tiled by nine 3×3 blocks, so that each of nine symbols appears exactly once in each row, column, and 3×3 block. As a *Latin square of order n* is an $n \times n$ grid filled with n symbols (which we can think of as $\{1, 2, \ldots, n\}$) so that each symbol appears exactly once in each row and column, a solution to a Sudoku puzzle presents an example of a Latin square. Since Latin squares have been extensively studied and have far-reaching applications, it makes sense that Sudoku has aroused interest among mathematicians with a view towards extending results about Latin squares to Sudoku solutions. Some related results were obtained independently from this article and appear in [**1**] and [**4**].

Some of the most basic results concerning Latin squares concern orthogonality of Latin squares. Two Latin squares of the same order are called *orthogonal* if when one of the Latin squares is superimposed onto the other, the n^2 ordered pairs obtained are all distinct.

In [**3**, p. 268], Golomb asked "Is it possible for two Sudoku solutions to form a pair of orthogonal Latin squares?" The answer is 'yes' (as confirmed by [**1**] and [**4**]), but a simple yes only piques our curiosity. We ask: How many mutually orthogonal Sudoku solutions can we *hope* to get? How many mutually orthogonal Sudoku solutions can we *actually* get? What about other orders?

The generalization

The question "What about other orders?" is easiest, so we address it first. There is nothing particularly special about the number nine where Sudoku puzzles are concerned—there is no reason we could not ask for a solution that fills a 4×4 grid tiled by four 2×2 blocks with four symbols so that each appears exactly once in each row, column, and 2×2 block. In fact, the only significant thing that sets a Sudoku puzzle apart from another Latin square is that it is of square order (say k^2), and is tiled by $k \times k$ blocks such that each of the k^2 symbols appears exactly once in each of the $k \times k$ blocks. From this point on, then, we call any Latin square of order k^2 satisfying this condition a *Sudoku Latin square*. For ease of reference, we say that a particular $k \times k$ block tiling a Latin square of order k^2 has *Property S* if and only if it contains each of the k^2 symbols exactly once.

Having generalized the Sudoku concept, we now turn to the question of how many mutually orthogonal Sudoku Latin squares of order k^2 we can hope to get. Since independently relabeling the symbols in each of the Sudoku Latin squares clearly cannot alter the Sudoku property of any of the squares or the orthogonality relation of any pair of squares, we can assume that all squares in a set of mutually orthogonal Sudoku Latin squares (MOSLS) have the first k^2 positive integers in order as the entries in the first row. That is, we may assume that all squares are in *standard form* [**5**, p. 96].

An upper bound

Let us try to form an upper bound on the number of MOSLS of order k^2. Assume all squares are in standard form and consider the possible (2, 1) entries in each (see the $\star$ in Figure 1.)

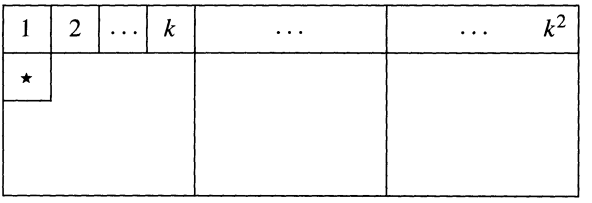

Figure 1. Standard form, top rows.

Notice that this entry is in the upper left block, and the first k positive integers appear in this block in the first row. Notice further that if two Sudoku Latin squares in standard form contain j as this entry, the ordered pairs of $(1, j)$ and $(2, 1)$ entries are both (j, j), so that the squares are not orthogonal. Thus, each square contains a distinct $(2, 1)$ entry and only $k^2 - k$ distinct entries are possible. This gives us an upper bound of $k^2 - k$ on the number of MOSLS of order k^2.

Prime power construction

The simplest example of a set of orthogonal Sudoku Latin squares would be a set of order 2^2 or four. We have seen that we can have at most $2\ (= 2^2 - 2)$ orthogonal 4×4 Sudoku Latin squares. If we play around with some Sudoku Latin squares of order four we might come across the pair of orthogonal squares in Figure 2. We notice that each

of these squares is a row permutation of the Cayley table of the elementary Abelian group of order four, which is also the addition table for the finite field of order four. This small example leads us to the suspicion that as with many other combinatorial structures, the existence of a finite field will allow us to construct a set of Sudoku Latin squares of maximum size.

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

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

Figure 2.

So let k be a prime power; let K be the finite field of order k^2; and let F be the subfield of K of order k. Since the additive group of F is then a subgroup of the additive group of K, K partitions into k additive cosets of F. We label these cosets as P_i, where $0 \leq i \leq k-1$ and choose a representative c_i for each coset. Finally, for each pair (i, j), we let the Latin square $B_{i,j}$ be the addition table of F on the symbols of P_m, where $c_m + F = (c_i + c_j) + F$. Then we can write the addition table for K in such a way that it is tiled with the Latin squares $B_{i,j}$ as shown in Figure 3.

$+$	P_0	P_1	P_2	$\cdots$	P_{k-1}
P_0	$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$\cdots$	$B_{0,k-1}$
P_1	$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$\cdots$	$B_{1,k-1}$
P_2	$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$\cdots$	$B_{2,k-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
P_{k-1}	$B_{k-1,0}$	$B_{k-1,1}$	$B_{k-1,2}$	$\cdots$	$B_{k-1,k-1}$

Figure 3.

Naturally, removing the border from this addition table yields a $k^2 \times k^2$ Latin square, which we call A. This Latin square is tiled by $k \times k$ blocks, each containing symbols from exactly one additive coset of F. Thus, any row of A intersects any $k \times k$ block in precisely one coset P_i. This remains true if we permute the rows of A to obtain another Latin square L with blocks $E_{i,j}$ and $E_{i,l}$. In fact, if two rows of the block $E_{i,j}$ contain the elements of the same coset P_n, those same two rows must intersect $E_{i,l}$ in the elements of the same coset P_m. Thus, we have just proved the following:

Proposition 1. *Suppose L is a Latin square of order k^2 obtained by permuting the rows of A, where A is defined as above. If two blocks $E_{i,j}$ and $E_{i,k}$ are in the same row of blocks of L, then $E_{i,j}$ has property S if and only if $E_{i,k}$ has property S.*

So when does a permutation of the rows of A yield blocks with property S? Well, since each row of a block contains precisely the elements from one coset P_i we simply

require that each row of the block contain the elements from a different coset, and this is easily verified by considering only the elements in the first column of the block. We summarize this by saying:

Proposition 2. *A block of the Latin square L defined as above has property S if and only if the first column contains exactly one element from each of the additive cosets P_i of F.*

Since we now have an easy way of checking whether a block has property S, we have only to determine the appropriate row permutations on A to give orthogonal Sudoku Latin squares. To accomplish this, we use the following notation: r_g denotes the row of A whose entry in the first column is g and (g, h) denote the cell in the Latin square A whose row begins with g and whose column begins with h. This brings us to our first major theorem.

Theorem 1. *For each $x \in K \setminus F$, the Latin square L_x formed by applying the permutation $r_g \to r_{g \cdot x}$ to the rows of A has the Sudoku property. Furthermore for $x_1, x_2 \in K \setminus F$ with $x_1 \neq x_2$, L_{x_1} and L_{x_2} are orthogonal.*

Proof. We begin by verifying that each square L_x is, in fact, Sudoku. The preceding propositions allow us to do this by verifying only that the intersection of each column of L_x with each block contains exactly one element from each coset. So let B be a block intersecting this first column, and let g and h be distinct elements in this intersection. Now from the construction of L_x, both $g \cdot x^{-1}$ and $h \cdot x^{-1}$ lie in the same additive coset. This implies that the difference $g \cdot x^{-1} - h \cdot x^{-1}$ lies in F. But then $g - h \in F$ if and only if $x^{-1} \in F$. Clearly, however, $x^{-1} \notin F$, and thus g and h are in different cosets, so that the intersection of the first column with any block contains exactly one element from each coset and L_x is Sudoku.

Now suppose that $x_1 \neq x_2$ and that cells (g_1, h_1) and (g_2, h_2) contain the same symbol in L_{x_1} and in L_{x_2}. As the entry in the cell (g_i, h_j) in square L_{x_l} is given by $g_i \cdot x_l + h_j$, we obtain the equations $g_1 \cdot x_1 + h_1 = g_2 \cdot x_1 + h_2$ and $g_1 \cdot x_2 + h_1 = g_2 \cdot x_2 + h_2$, which, by a simple subtraction of one from the other yields $g_1 \cdot (x_1 - x_2) = g_2 \cdot (x_1 - x_2)$. With $x_1 \neq x_2$, this implies that $g_1 = g_2$, and thus $h_1 = h_2$. As such, L_{x_1} and L_{x_2} are orthogonal.

Since $K \setminus M$ has order $k^2 - k$, this construction produces a set of MOSLS of maximum size, and we have proved the following corollary. ∎

Corollary. *If k is a prime power, there exists a set of $k^2 - k$ MOSLS.*

Direct product construction

So we can, in fact, obtain a set of MOSLS with the maximum number of elements under certain conditions. But what if k is not a prime power? Certainly intuition would tell us not to expect to find a set of maximum size. On the other hand, intuition might also suggest that we can obtain a set of some size. In fact, being familiar with MacNeish's conjecture and his associated construction (see, for example, [**5**, pp. 97–102]), we might suspect exactly how large a set we can expect to find. Unlike MacNeish, however, we make no conjecture that these sets are the largest possible.

MacNeish's construction proceeds in two steps: constructing sets of MOLS of maximum size where the order is a prime power, and joining these together to create sets

of mutually orthogonal Latin squares (MOLS) where the order is not a prime power. Since we have already constructed sets of MOSLS of maximum size where the order is a prime power, this suggests that we should attempt to join these together to create sets of MOSLS where the order is not a prime power. In fact, we are able to do this by tweaking the direct product technique used to construct MOLS.

In order to ease the necessary notation and maintain intuition, we introduce quasigroups for this purpose. A *quasigroup* is simply some set S together with an operation $\cdot$ such that removing the border from the Cayley table gives us a Latin square on the elements of S. Every Latin square gives rise to a quasigroup (simply by adding a border), and every quasigroup gives rise to a Latin square (by removing the border). Two quasigroups are orthogonal whenever their associated Latin squares are orthogonal.

We first quote the following well known result regarding direct products (see, for example [**2**, p. 427]:

Lemma 1. *Let* $(G, \cdot_1)$ *and* $(G, \cdot_2)$, $(H, \cdot_3)$ *and* $(H, \cdot_4)$ *be pairs of orthogonal quasigroups, and define operations* $\cdot_{1,3}$ *and* $\cdot_{2,4}$ *on the set* $G \times H$ *by* $(a, b) \cdot_{1,3} (c, d) = (a \cdot_1 c, b \cdot_3 d)$ *and* $(a, b) \cdot_{2,4} (c, d) = (a \cdot_2 c, b \cdot_4 d)$. *Then* $(G \times H, \cdot_{1,3})$ *and* $(G \times H, \cdot_{2,4})$ *are orthogonal quasigroups.*

Now if we form the Cayley tables for these quasigroups and remove the border, we obtain a pair of orthogonal Latin squares, a fact that follows directly from the definitions of orthogonality for both quasigroups and Latin squares. As such, if we wish to create MOSLS using a direct product, we need only concern ourselves with the Sudoku property.

So assume we have orthogonal Sudoku Latin squares A and A' using the symbols from the set $G = \{1, 2, \ldots, m^2\}$, and B and B' using the symbols from the set $H = \{1, 2, \ldots, n^2\}$. We define quasigroups $(G, \cdot_A)$, $(G, \cdot_{A'})$, $(H, \cdot_B)$, and $(H, \cdot_{B'})$ by $a \cdot_X b = X_{a,b}$ where $X = A, A', B$, or B'.

If we define quasigroups $(G \times H, \cdot_{A,B})$ and $(G \times H, \cdot_{A',B'})$ by $(a, b) \cdot_{X,Y} (c, d) = (a \cdot_X c, b \cdot_Y d)$, then lemma 1 tells us that in order to obtain a pair of orthogonal Sudoku Latin squares, we need only find an ordering of the elements of $G \times H$ so that the resulting Latin squares are, in fact, Sudoku.

We are able to do this with relative ease. In fact, the blocks of the square C derived from the quasigroups $(G \times H, \cdot_{A,B})$ are obtained as ordered pairs of a block of A and a block of B.

More precisely, the arrangement of blocks sets up a partition $\{P_i\}$ of G into m sets of m elements each, where each set P_i consists of the integers from $(i-1)m+1$ through im. So two elements of G are in the same partition element P_i if and only if the rows (or columns) of A corresponding to x and y intersect the same $m \times m$ blocks of A. In particular, any block of the Sudoku Latin square is determined uniquely by a pair of partition elements and conversely (see Figure 4). Similarly, the arrangement of blocks in B sets up a partition $\{Q_i\}$ of H into n sets of n elements each, where each set Q_i consists of the integers from $(i-1)m+1$ through im.

These partitions on G and H generate a partition $\{P_i\} \times \{Q_i\}$ on the elements of $G \times H$ having mn sets of mn elements each.

Finally, to obtain the most likely candidate for a Sudoku Latin square of order $(mn)^2$, we order the elements of $G \times H$ so that the elements of each partition element $P_i \times Q_j$ are consecutive. We use this ordering in constructing the Cayley table for the quasigroup $(G \times H, \cdot_{A,B})$. When we remove the border, the $mn \times mn$ blocks that tile the resulting Latin square C are again determined by a pair of partition ele-

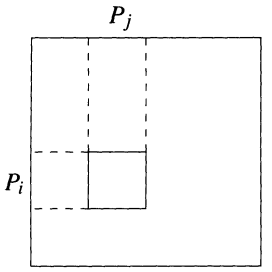

Figure 4.

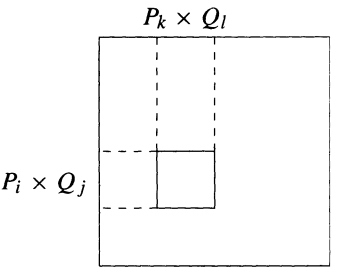

Figure 5.

ments, and vice versa (see Figure 5). Since this ordering is independent of A and B, all that remains is to show that C is Sudoku.

But this can be accomplished by simply showing that an arbitrary block, determined by an arbitrary pair of partition elements ($P_i \times Q_j$ determining the rows and $P_k \times Q_l$ determining the columns) has property S. Now any entry in this block takes the form $(a, b) \cdot_{A,B} (c, d)$, with $a \in P_i$, $b \in Q_j$, $c \in P_k$, and $d \in Q_l$. So let a_1 and a_2 be in P_i, b_1 and b_2 be in Q_j, c_1 and c_2 be in P_k, and d_1 and d_2 be in Q_l and suppose that $(a_1, b_1) \cdot_{A,B} (c_1, d_1) = (a_2, b_2) \cdot_{A,B} (c_2, d_2)$. Then $a_1 \cdot_A c_1 = a_2 \cdot_A c_2$, and since A is Sudoku, $a_1 = a_2$ and $c_1 = c_2$. Similarly, $b_1 \cdot_B d_1 = b_2 \cdot_B d_2$, and since B is Sudoku, $b_1 = b_2$ and $d_1 = d_2$. Thus, all elements in this block are distinct and this block has property S. We have then just proved the following proposition.

Proposition 3. *Any Latin square constructed by this modification of MacNeish's method is Sudoku.*

By extension, and using more than just a pair of MOSLS of each order, we obtain the following:

Corollary. *If there exist r MOSLS of order m^2 and s MOSLS of order n^2, then there are at least* $\min\{r, s\}$ *MOSLS of order $(mn)^2$.*

Proof. To see this let $t = \min\{r, s\}$. Take t MOSLS of order m^2 and t MOSLS of order n^2 and employ the direct product construction just given. A total of t Sudoku Latin squares are created and are pairwise orthogonal. That is, there exists a set of t MOSLS of order $(mn)^2$.

As this construction has given us the tools to construct sets of MOSLS of larger order from sets of MOSLS of smaller order, we are finally able to put everything together and see how many MOSLS of a given order we can obtain.

Theorem 2. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime factorization for n and let $q =$* $\min\{p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}\}$. *Then there exist at least $q^2 - q$ MOSLS of order n^2.*

Proof. This follows inductively from the preceding corollary and the prime power construction. ∎

As a final result, we note that there is no admissible Sudoku order for which there does not exist a pair of MOSLS.

Corollary. *There exist MOSLS of order n^2 for every natural number $n > 1$.*

Proof. In the proof of the preceding theorem, the lowest possible value of q is 2. But $2^2 - 2 = 2$, so that at least two MOSLS exist for every order greater than one.

The only value we haven't addressed is $n = 1$. Up to relabeling, there is clearly only one Latin square of order one. On the other hand, this Latin square is self-orthogonal and has the Sudoku property. So, can we take two copies of this Latin square and claim to have a pair of MOSLS of order one, or do we need distinct squares? You be the judge. ■

Conclusion

While our results provide a nice adaptation of the standard techniques for constructing MOLS to the construction of MOSLS and establish a lower bound on the maximum number of MOSLS of a given order, it seems highly unlikely that these results are sharp (with the exception the case of a prime power). Determining the exact number of MOSLS of a given order remains to be accomplished. Another question worth addressing is when an arbitrary Sudoku Latin square has an orthogonal mate. This question also suggests the possibility of yet another version of the Sudoku puzzle, wherein the participant (presumably one for whom even the most difficult Sudoku puzzles pose little challenge) simultaneously fills in a pair of squares in such a way that they remain orthogonal. This could offer a very challenging, and yet interesting variation of the much-enjoyed puzzle.

References

1. R. A. Bailey, P. J. Cameron, and R. Connelly, Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes, *Amer. Math. Monthly* **115** (2008) 383–404.
2. J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press, New York, 1974.
3. S. Golomb, Proposed problem, *Amer. Math. Monthly* **113** (2006) 268.
4. A. D. Keedwell, On sudoku squares, *Bull. Inst. Combin. Appl.* **50** (2007) 52–60.
5. C. Lindner and C. Rodger, *Design Theory*, CRC Press, Boca Raton, 1997.

Puzzling Mechanisms, Part 1: Misleading Mazes
M. Oskar van Deventer

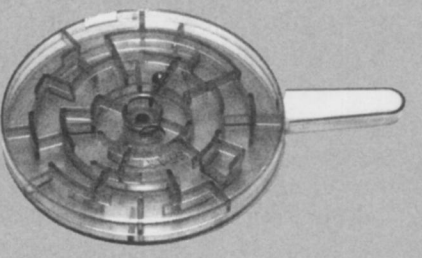

Figure 1. *Frying Pan*, produced by Pentangle.

The inspiration for "Misleading Mazes" is the *Frying Pan* puzzle (see Figure 1). This puzzle looks like an ordinary dexterity maze with a single ball. However, it