Latin Squares Instructor: Paddy

Lecture 2: Evans' Conjecture, take 2

Week 1 of 1 *Mathcamp 2010*

Today, we'll finish proving Evans' Conjecture:

Theorem 1 *(Smetianuk, 1981) Any $n \times n$ partial latin square with $\leq n-1$ entries can be completed to a latin square.*

Yesterday, we proved this theorem in the case where we used $\leq n/2$ distinct symbols; tdday, we will handle the case where we have $> n/2$ distinct symbols!

Theorem 2 *Any $n \times n$ partial latin square with $\leq n-1$ entries that uses $> n/2$ distinct symbols can be completed to a latin square.*

Proof. First, note the following useful lemma that describes a form we can insist our latin squares have:

Lemma 3 *If P is a partial latin square with the above properties, we can find an equivalent latin square P' with the following properties:*

- *There is exactly one cell with symbol n; the rest all have symbols $\leq n-1$.*
- *This n-symbol lies on the main diagonal of our matrix: the rest lie strictly beneath the main diagonal.*

			3		7	
5				4		
			5			
						3

$\longrightarrow$

3	7					
5						
	4	5				
			3			

We omit the proof of this lemma here, and encourage the reader to work it out at home; basically, the $> n/2$ distinct symbols insures that there is some symbol that occurs exactly once (and thus it might as well be n,) and the $\leq n-1$ symbols allows us to rearrange all of the rows as desired.

So: what does this give us? Well, suppose we take our partial latin square in the form above, and get rid of the main diagonal:

3	7					
5						
	4	5				
			3			

$\longrightarrow$

●						
3	●					
5		●				
	4	5	●			
				●		
					●	
			3			●

What do we have? Well, if we look at the indicated $n-1 \times n-1$ partial latin subsquare, we have a $n-1 \times n-1$ partial latin square with $\leq n-2$ completed entries, each of which has symbols drawn from the set $\{1, \ldots n-1\}$. This strongly suggests that we proceed by induction! So, let's do so, and use our inductive hypothesis to complete this subsquare:

3	6	1	2	4	5	
5	1	3	4	2	6	
1	4	5	6	3	2	
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

How can we use this mostly-completed latin square to get to a complete latin square? Clearly, we can't just extend this square, as doing so would fill the last column and row with a bunch of n's; so what do we do? Here is where arguably the genius of Smetianuk's proof comes in; the trick we present here, while not difficult to understand, is extremely clever – basically, what he does is creates a way to swap out the main diagonal of our square for the last column of our square, and then bolts back in a main diagonal made entirely out of n's!

Specifically, consider the following algorithm, that inducts on the rows of P:

- For the first step: put a n in the square $(2, n)$, and swap the element in $(2, 2)$ with this n in $(2, n)$.

3	$\boxed{6}$	1	2	4	5	$\boxed{7}$
5	1	3	4	2	6	
1	4	5	6	3	2	
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

⟶

3	$\boxed{7}$	1	2	4	5	$\boxed{6}$
5	1	3	4	2	6	
1	4	5	6	3	2	
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

- For the inductive step: put a n in the square (k, n), and inductively assume that we've filled the rows 2 through $k-1$ of the n-th column with distinct symbols that preserve P as a partial latin square.

  Look at the element in the square (k, k). There are two possibilities:

1. This value hasn't shown up thus far in the n-th column. In this case, just swap (k, k) and (k, n).

3	7	1	2	4	5	6
5	1	$\boxed{3}$	4	2	6	$\boxed{7}$
1	4	5	6	3	2	
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

⟶

3	7	1	2	4	5	6
5	1	$\boxed{7}$	4	2	6	$\boxed{3}$
1	4	5	6	3	2	
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

2. The symbol x_k in (k, k) has shown up earlier in the n-th column! In this situation, swap (k, k) and (k, n), and then perform the following set of moves:

   (a) Let j_1 be the row where this symbol occured earlier: i.e. pick j_1 such that $(j_1, n) = x_k$. Swap the elements (j_1, n) and (j_1, k). Then, there are two possiblities:

   (b) This newly-swapped symbol conflicts again with some other (j_2, n), $j_2 \neq j_1$. In this case, repeat the above process! I.e. go to (a).

   (c) This newly-swapped symbol doesn't conflict with any other elements in our column! Because each time we did a swap we eliminated our old conflict, this means that our column has in fact no conflicts at all in it. Because all of our swaps occured within rows, and all of our swapped elements were above the main diagonal, we've preserved the partial latin square property of P and have made sure that P is still a completion of our original partial latin square.

3	7	1	2	4	5	6
5	1	7	4	2	6	3
1	4	5	$\boxed{6}$	3	2	$\boxed{7}$
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

$\longrightarrow$

3	7	1	$\boxed{2}$	4	5	$\boxed{6}$
5	1	7	4	2	6	3
1	4	5	$\boxed{6}$	3	2	$\boxed{7}$
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

$\longrightarrow$

3	7	1	$\boxed{6}$	4	5	$\boxed{2}$
5	1	7	4	2	6	3
1	4	5	$\boxed{7}$	3	2	$\boxed{6}$
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

How long can the above process go on? Well: think of this switching process as a bipartite graph between the entries $\{(2, k), \ldots (k, k)\}$ in the k-th column and the entries $\{(2, n), \ldots (k, n)\}$ in the n-th column. Connect every (l, k) to (l, n), and connect (l, k) to (m, n) iff they have the same value before our switching process.

Because our graph corresponds to a pair of columns in a partial latin square, we know that the degree of any vertex here is ≤ 2: this is because there can only be one edge arising from $(l, k) \sim (l, n)$-edges, and at most one edge coming from symbols matching up.

So: because our process starts at (k, n) which has symbol n, we know that we're effectively starting at a vertex of degree 1 and taking a walk: because the degrees are all bounded by 2, we know that this cannot be a path and must eventually terminate! Thus, our algorithm above will always terminate; so we can turn P into a $n - 1 \times n$ latin rectangle, which can be completed to a latin square by our earlier work.

3	7	1	6	4	5	2
5	1	7	4	2	6	3
1	4	5	7	3	2	6
6	2	4	5	1	3	
2	3	6	1	5	4	
4	5	2	3	6	1	

$\longrightarrow$

3	7	1	6	4	5	2
5	1	7	4	2	6	3
1	4	5	7	3	2	6
6	2	4	5	7	3	1
2	3	6	1	5	7	4
4	5	2	3	6	1	7

$\longrightarrow$

7	6	3	2	1	4	5
3	7	1	6	4	5	2
5	1	7	4	2	6	3
1	4	5	7	3	2	6
6	2	4	5	7	3	1
2	3	6	1	5	7	4
4	5	2	3	6	1	7

1 Mutually Orthogonal Latin Squares

Now, for something initially very different: mutually orthogonal latin squares! Recall, from day 1, the definition of a pair of mutually orthogonal latin squares:

Definition. Take a pair of $n \times n$ latin squares M_1, M_2, and look at all of the ordered pairs

$$\{\ (x,y)\ | x \text{ is the } (i,j)\text{-th entry in } M_1, \text{ and } y \text{ is the } (i,j)\text{-th entry in } M_2.\}$$

If all of these pairs are distinct, then we say that M_1 and M_2 are **mutually orthogonal**. In general, we say that a set $\{M_1\ ldots M_k\}$ of $n \times n$ latin squares are mutually orthogonal if any pair of elements in the set are mutually orthogonal.

So: from last class, we saw that there were pairs of 4×4 mutually orthogonal latin squares:

$$\begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix} \text{ and } \begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix} \text{ overlaid: } \begin{bmatrix} A\spadesuit & K\heartsuit & Q\diamondsuit & J\clubsuit \\ Q\clubsuit & J\diamondsuit & A\heartsuit & K\spadesuit \\ J\heartsuit & Q\spadesuit & K\clubsuit & A\diamondsuit \\ K\diamondsuit & A\clubsuit & J\spadesuit & Q\heartsuit \end{bmatrix}$$

So: for a given n, how many mutually orthogonal latin squares can there be?

Theorem 4 *If $N(n)$ denotes the maximum size of a set of $n \times n$ mutually orthogonal latin squares, then $N(n) \leq n-1$, for every n.*

Proof. Take any collection of $n \times n$ mutually orthogonal latin squares $M_1, \ldots M_k$.

Note first that if M_1 and M_2 are a pair of mutually orthogonal latin squares, then permuting the symbols of M_1 cannot change whether M_1 and M_2 are mutually orthogonal – in other words, if all of the pairs are distinct, it hardly matters what we've chosen to write down the symbols as (so long as they're all distinct.) Thus, without loss of generality, we can require that the first row of every M_i is of the form $[1, 2, 3\ ldots n]$.

So: look at the $(2,1)$-entry in any pair of squares M_i, M_j. We have that

$$\begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ x & \ldots & & & \\ \vdots & & & & \\ \vdots & & & & \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ y & \ldots & & & \\ \vdots & & & & \\ \vdots & & & & \end{bmatrix}.$$

We know that neither x nor y can be 1, because these are latin squares; as well, we know that $x \neq y$, because the pairs (i,i) exist for every i because the top rows are all lined up. Thus, there can be no more than $n-1$ distinct MOLS in our set.