Math 7h | Professor: Padraic Bartlett

Lecture 7: Latin and Magic Squares

Week 7 | *UCSB 2014*

Definition. A **latin square** of order n is a $n \times n$ array filled with n distinct symbols (by convention $\{1, \dots n\}$), such that no symbol is repeated twice in any row or column.

Example. Here are all of the latin squares of order 2:

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

A quick observation we should make is the following:

Proposition. Latin squares exist for all n.

Proof. Behold!

$$\begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ n & 1 & \dots & n-2 & n-1 \end{bmatrix}$$

□

Given this observation, a natural question to ask might be "How many Latin squares exist of a given order n?" And indeed, this is an excellent question! So excellent, in fact, that it turns out that we have no idea what the answer to it is; indeed, we only know the true number of Latin squares of any given order up to 11!

n	reduced Latin squares of size n[1]	all Latin squares of size n
1	1	1
2	1	2
3	1	12
4	4	576
5	56	161280
6	9408	812851200
7	16942080	61479419904000
8	535281401856	108776032459082956800
9	377597570964258816	5524751496156892842531225600
10	7580721483160132811489280	9982437658213039871725064756920320000
11	536393777327737129811967354077184 0	776966836171770144107444346734230682311065600000
12	?	?

[1] (A **reduced** Latin square of size n is a Latin square where the first column and row are both $(1, 2, 3 \dots n)$.)

Asymptotically, the best we know (and you could show, given a lot of linear algebra tools) that

$$L(n) \sim \left(\frac{n}{e^2}\right)^{n^2}.$$

Definition. A **partial latin square** of order n is a $n \times n$ array where each cell is filled with either blanks or symbols $\{1, \ldots n\}$, such that no symbol is repeated twice in any row or column.

Example. Here are a pair of partial 4×4 latin squares:

$$\begin{bmatrix} & & & 4 \\ 2 & & & \\ 3 & 4 & & \\ 4 & 1 & 2 & \end{bmatrix} \qquad \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 2 \end{bmatrix}$$

The most obvious question we can ask about partial latin squares is the following: when can we complete them into filled-in latin squares? There are clearly cases where this is possible: the first array above, for example, can be completed as illustrated below.

$$\begin{bmatrix} & & & 4 \\ 2 & & & \\ 3 & 4 & & \\ 4 & 1 & 2 & \end{bmatrix} \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

However, there are also clearly partial Latin squares that cannot be completed. For example, if we look at the second array

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 2 \end{bmatrix},$$

we can pretty quickly see that there is no way to complete this array to a Latin square: any 4×4 Latin square will have to have a 1 in its last column somewhere, yet it cannot be in any of the three available slots in that last column, because there's already a 1 in those three rows.

Deciding whether a given partial Latin square is completeable to a Latin square is, practically speaking, a useful thing to be able to do. Consider the following simplistic model of a **router**:

- Setup: suppose you have a box with n fiber-optic cables entering it and n fiber-optic cables leaving it. On any of these cables, you have at most n distinct possible wavelengths of light that can be transmitted through that cable simultaneously. As well, you have some sort of magical/electronical device that is capable of "routing" signals from incoming cables to outgoing cables: i.e. it's a list of rules of the form (r, c, s), each of which send mean "send all signals of wavelength s from incoming cable r to outgoing cable s." These rules cannot conflict: i.e. if we're sending wavelength s from incoming cable r to outgoing cable s, we cannot also send s from r to t, for some other outgoing cable t. (Similarly, we cannot have two transmits of the form $\{(r, c, s), (r, t, s)\}$ or $\{(r, c, s), (t, c, s)\}$.)

- Now, suppose that your box currently has some predefined set of rules it would like to keep preserving: i.e. it already has some set of rules $\{(r_1, c_1, s_1), \ldots\}$. We can model this as a **partial Latin square**, by simply interpreting each rule (r, c, s) as "fill entry (r, c) of our partial Latin square with symbol s."

- With this analogy made, adding more symbols to our partial Latin square is equivalent to increasing the amount of traffic being handled by our router.

So: on one hand, Latin squares are incredibly simple to define. On the other hand, very simple questions about Latin squares are still open problems that mathematicians do not know the answer to! On the third hand[2], understanding how Latin squares work is a problem that is relevant to many applications in computer science and engineering!

Let's add another hand, and consider the following concept: **magic squares**!

Definition. A **magic square** is a $n \times n$ grid filled with the integers $\{0, 1, \ldots n^2 - 1\}$, such that

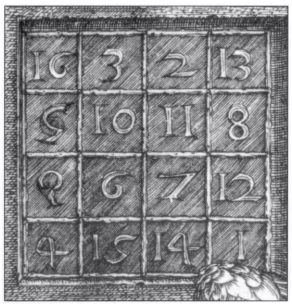
- each number is used exactly once in our entire grid, and

- the sum of all of the entries along any row, column, the main diagonal[3] or the main antidiagonal all come out to the same constant value.

Here's an example for order 3:

1	6	5
8	4	0
3	2	7

Magic squares have been studied for a fairly ridiculously long time. Mathematicians and philosophers were aware of them since about 650 BC; since their discovery, people have used them both as the basis for magic tricks (when your population is largely numerically illiterate, magic squares were a neat way to perform seemingly impossible feats) and religious/spiritual/cultural icons.



(A zoomed-in portion of an engraving by Albrecht Dürer, titled *Melencolia I*. Note how he hid the year of his engraving, 1514, in the last row.)

[2] We have three hands?

[3] The main diagonal of a $n \times n$ grid is simply the set of cells connecting the top-left to the bottom-right cells: i.e. $(1, 1), (2, 2), \ldots (n, n)$. Similarly, the main antidiagonal is just the set of cells connecting the bottom-left to the top-right: i.e. $(n, 1), (n - 1, 2), \ldots (1, n)$.

As mathematicians, our first impulse upon seeing a new definition is to ask "When do these things exist?" By doing some scratchwork, we can show that these don't exist for order 2: this is because every grid we can make will look like either $\begin{array}{|c|c|}\hline 0&2\\\hline 3&1\\\hline\end{array}$ or $\begin{array}{|c|c|}\hline 0&1\\\hline 3&1\\\hline\end{array}$ or $\begin{array}{|c|c|}\hline 0&1\\\hline 2&3\\\hline\end{array}$, by rotating it so that 0 is in the upper-left corner and flipping it so that the entry in the upper-right is greater than the one in the lower-left. None of these are magic: therefore, there is no magic square of order 2.

There is one of order 1 (Behold: $\boxed{0}$!), and we've already shown that ones exist of order 3 and 4. However, we haven't really introduced a method for looking for these yet; we've just sort of given some examples, most of which we made by just picking numbers.

Surprisingly, we can create these objects using Latin squares! We describe the method here:

1 Diagonal Latin Squares

Definition. A **diagonal Latin square** is a Latin square such that its main diagonal contains no repeated symbols, and similarly its main antidiagonal also does not contain any repeated symbols.

We can easily make one of order 1 (Behold: $\boxed{1}$!), and can easily see that we cannot do this for order 2: if we take a 2×2 Latin square with the symbols $1, 2$ on the diagonal, i.e. $\begin{array}{|c|c|}\hline 1&\\\hline &2\\\hline\end{array}$, there's clearly no way to complete this to a Latin square.

Similarly, if we take a 3×3 partial Latin square with $1, 2, 3$ on the diagonal (without any loss of generality, in the order $(1, 2, 3)$), we can see that there is only one way to fill it in:

$$\begin{array}{|c|c|c|}\hline 1&&\\\hline &2&\\\hline &&3\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 1&&\\\hline &2&1\\\hline &1&3\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 1&3&2\\\hline 3&2&1\\\hline 2&1&3\\\hline\end{array}.$$

This square does not contain the symbols $1, 2, 3$ on its antidiagonal; therefore, there is no diagonal Latin square of order 3.

Conversely, using the same method of "just try it" gives us a way to explicitly find a diagonal Latin square of order 4: if we attempt to put the symbols $1 \ldots 4$ on the diagonal, we can try to put 3 in the cells $(1, 2), (2, 1)$,

$$\begin{array}{|c|c|c|c|}\hline 1&&&\\\hline &2&&\\\hline &&3&\\\hline &&&4\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1&3&&\\\hline 3&2&&\\\hline &&3&\\\hline &&&4\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1&3&4&2\\\hline 3&2&?&1\\\hline &&3&\\\hline &&&4\\\hline\end{array}$$

in which case we fail. Alternately, we can try to put 3 in $(1, 2)$ and 4 in $(2, 1)$, in which case we have

$$\begin{array}{|c|c|c|c|}\hline 1&&&\\\hline &2&&\\\hline &&3&\\\hline &&&4\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1&3&&\\\hline 4&2&&\\\hline &&3&\\\hline &&&4\\\hline\end{array} \longrightarrow \begin{array}{|c|c|c|c|}\hline 1&3&4&2\\\hline 4&2&1&3\\\hline 2&4&3&1\\\hline 3&1&2&4\\\hline\end{array},$$

which works! So we've found one for order 4.

However, this ad-hoc approach is unsatisfying: when will it work? How can we do this efficiently; i.e. without having to run into dead ends, or with a guarantee that our process will work?

There are a number of constructions that mathematicians have came up with over time. One of my favorites, b/c of its simplicity, is the following:

Construction. Take any value of n, and any two numbers $a, b \in \{0, \dots n-1\}$. Consider the following square populated with the elements $\{0, 1 \dots n-1\}$:

$$L = \begin{array}{|c|c|c|c|c|c|} \hline 0 & a & 2a & 3a & \dots & (n-1)a \\ \hline b & b+a & b+2a & b+3a & \dots & b+(n-1)a \\ \hline 2b & 2b+a & 2(b+a) & 2b+3a & \dots & 2b+(n-1)a \\ \hline 3b & 3b+a & 3b+2a & 3(b+a) & \dots & 3b+(n-1)a \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline (n-1)b & (n-1)b+a & (n-1)b+2a & (n-1)b+3a & \dots & (n-1)(b+a) \\ \hline \end{array} \mod n.$$

In other words, L's (i, j)-th cell contains the symbol given by taking the quantity $ai + bj \mod n$.

This construction, made by filling in the cells (i, j) of our Latin square using some linear map $ai + bj$, should feel familiar to you: it is the same kind of map we used when we turned finite fields into Latin squares, and it is also the same kind of map we used when we turned affine planes into Latin squares, kinda (i.e. the same idea of parallel lines becoming Latin squares showed up in both of these things.)

Given this construction, a question we'd like to ask is the following: for what values of n is this a diagonal Latin square?

Well: let's start smaller, and just ask that it's a normal Latin square. In order for this to hold, we need to not have any repeats in any given row: in other words, that no two cells $(i, j), (k, j)$ contain the same symbol. But this can happen only if

$$(ai + bj \equiv ak + bj \mod n) \Leftrightarrow (ai \equiv ak \mod n).$$

If a and n have common factors, then this is possible; let $i = 0$ and $k = \frac{n}{\text{GCD}(a,n)}$. However, if a and n are relatively prime, then this can only happen if $i = k$; i.e. if we've picked the same cell! So we have no repeats in any row if and ony if a and n are relatively prime.

Similarly, if we look at any column, we can see that there are no repeats in any column if and only if b and n are relatively prime. Therefore, this construction is a Latin square if and only if a, b are both relatively prime to n.

What about being a diagonal Latin square? Well: to insure this, we also need that the main diagonal and main antidiagonal have no repeats. However, the main diagonal is just

$$\begin{array}{|c|c|c|c|c|} \hline 0 & & & & \\ \hline & b+a & & & \\ \hline & & 2(b+a) & & \\ \hline & & & \ddots & \\ \hline & & & & (n-1)(b+a) \\ \hline \end{array},$$

i.e. the sequence made by looking at multiples of $(a+b)$. This clearly has no repeats if and only if $(a+b)$ is relatively prime to n. Similarly, the main antidiagonal has the form

					$(n-1)(a)$
				$b+(n-2)a$	
			$\iddots$		
		$(n-3)b+2a$			
	$(n-2)b+a$				
$(n-1)b$					

,

which, if we subtract nb from the entire main diagonal (which we can do, because we're just looking at everything mod n, and therefore nb is just 0) we can see is just

					$-b+(n-1)(a-b)$
				$-b+(n-2)(a-b)$	
			$\iddots$		
		$-b+2(a-b)$			
	$-b+(a-b)$				
$-b$					

,

Using the same logic as before, we can again see that this antidiagonal has no repeats if and only if $a-b$ is relatively prime to n.

By combining these observations, we have the following proposition:

Proposition. Suppose that n is an integer such that there are two numbers $a, b \in \{0, \ldots n-1\}$, such that $a, b, a+b, a-b$ are all relatively prime to n. Then the construction above creates a diagonal Latin square.

In particular, we have the following really easy corollary:

Corollary 1. *If n is an odd number that's not divisible by 3, there is a diagonal Latin square of order n.*

Proof. Set $a = 2, b = 1$; then $a, b, a+b = 3, a-b = 1$ are all relatively prime to n. □

As an example, here's the result of our construction for $n = 5$:

0	2	4	1	3
1	3	0	2	4
2	4	1	3	0
3	0	2	4	1
4	1	3	0	2

.

Check: it works! Furthermore, any Latin square produced by this process has the following nice property:

Proposition. Take any $n \times n$ diagonal Latin square L on the symbols $\{1, \ldots n\}$. Form the array M as follows: in entry (i, j) of M, place the sum $L(i, j) + n \cdot L(j, i) - n$. I.e. to fill the square (i, j), add whatever symbol is in $L(i, j)$ to $n \cdot L(j, i)$, and subtract n.

Then M is a magic square!

Proving this is the HW! To illustrate how this works, here's a pair of orthogonal diagonal Latin squares, along with their resulting magic square:

$$L = \begin{array}{|c|c|c|c|c|}\hline 1&3&5&2&4\\\hline 2&4&1&3&5\\\hline 3&5&2&4&1\\\hline 4&1&3&5&2\\\hline 5&2&4&1&3\\\hline\end{array}$$

$$\Rightarrow M = L + n \cdot L^T - 1 = \begin{array}{|c|c|c|c|c|}\hline 1&3&5&2&4\\\hline 2&4&1&3&5\\\hline 3&5&2&4&1\\\hline 4&1&3&5&2\\\hline 5&2&4&1&3\\\hline\end{array} + n \cdot \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 3&4&5&1&2\\\hline 5&1&2&3&4\\\hline 2&3&4&5&1\\\hline 4&5&1&2&3\\\hline\end{array} - n$$

$$= \begin{array}{|c|c|c|c|c|}\hline 1+(n\cdot 1)-n & 3+(n\cdot 2)-n & 5+(n\cdot 3)-n & 2+(n\cdot 4)-n & 4+(n\cdot 5)-n\\\hline 2+(n\cdot 3)-n & 4+(n\cdot 4)-n & 1+(n\cdot 5)-n & 3+(n\cdot 1)-n & 5+(n\cdot 2)-n\\\hline 3+(n\cdot 5)-n & 5+(n\cdot 1)-n & 2+(n\cdot 2)-n & 4+(n\cdot 3)-n & 1+(n\cdot 4)-n\\\hline 4+(n\cdot 2)-n & 1+(n\cdot 3)-n & 3+(n\cdot 4)-n & 5+(n\cdot 5)-n & 2+(n\cdot 1)-n\\\hline 5+(n\cdot 4)-n & 2+(n\cdot 5)-n & 4+(n\cdot 1)-n & 1+(n\cdot 2)-n & 3+(n\cdot 3)-n\\\hline\end{array}$$

$$= \begin{array}{|c|c|c|c|c|}\hline 1&12&23&9&20\\\hline 8&19&5&11&22\\\hline 15&21&8&18&4\\\hline 17&3&14&25&6\\\hline 24&10&16&2&13\\\hline\end{array}.$$