CCS Discrete Math I	Professor: Padraic Bartlett

Lecture 8: Latin Squares and Finite Fields

Week 8	*UCSB 2014*

> Ayant vu que toutes [les] méthodes que nous avons exposées jusqu'ici ne sauroient fournir aucun quarré magique pour le cas de $n = 6$ et que la même conclusion semble s'étendre à tous les nombres impairement pairs de n, on pourroit croire que, si de tels quarrés sont possibles, les quarreés latins qui leur servent de base, ne suivant aucun des ordes que nous venons de considérer, seroient tout à fait irréguliers. Il faudroit donc examiner tous les cas possibles de tels quarrés latins pour le cas de $n = 6$, dont le nombre est sans doute extrèmement grand.
>
> Euler, *Recherches*

This was a short talk I gave on Wednesday about some applications of finite fields to Latin squares! This isn't something that will show up on any of the required HW; it's mostly here for fun, so that people who were around on Wednesday got to see some fun stuff and eat pie! (Also because Latin squares are the best things ever.)

We start with some definitions:

1 Latin Squares: Definitions

Definition. A **Latin square** of order n is a $n \times n$ array filled with n distinct symbols (by convention $\{1, \ldots n\}$), 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!

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

□

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 exact 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	5363937773277371298119673540771840	776966836171770144107444346734230682311065600000
12	?	?

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

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

2 Mutually Orthogonal Latin Squares

To understand how finite fields apply to Latin squares, try solving the following problem:

Question. Take a deck of playing cards, and remove the 16 aces, kings, queens, and jacks from the deck. Can you arrange these cards into a 4×4 array, so that in each column and row, no two cards share the same suit or same face value?

This question should feel similar to the problem of constructing a Latin square: we have an array, and we want to fill it with symbols that are not repeated in any row or column. However, we have the additional constraint that we're actually putting **two** symbols in every cell: one corresponding to a suit, and another corresponding to a face value.

So: if we just look at the face values, we should get a 4×4 Latin square. Similarly, if we ignore the face values and look only at the suits, we should have a different 4×4 Latin square; as well, these two Latin squares ought to have the property that when we superimpose them (i.e. place one on top of the other), each of the resulting possible 16 pairs of symbols occurs exactly once (because we started with 16 distinct cards.)

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

You can do this! Here is one possible solution:

$A\heartsuit$	$K\diamondsuit$	$Q\spadesuit$	$J\clubsuit$
$K\spadesuit$	$A\clubsuit$	$J\heartsuit$	$Q\diamondsuit$
$Q\clubsuit$	$J\spadesuit$	$A\diamondsuit$	$K\heartsuit$
$J\heartsuit$	$Q\heartsuit$	$K\clubsuit$	$A\spadesuit$

The generalization of this idea is to the concept of **orthogonality**[2] for Latin squares, which we define here:

Definition. A pair of $n \times n$ Latin squares are called **orthogonal** if when we superimpose them (i.e. place one on top of the other), each of the possible n^2 ordered pairs of symbols occur exactly once.

A collection of k $n \times n$ Latin squares is called **mutually orthogonal** if every pair of Latin squares in our collection is orthogonal.

Example. The grid of playing cards weou constructed earlier if you answered our first question is a pair of 4×4 squares, for the reasons we discussed earlier. To further illustrate the idea, we present a pair of orthogonal 3×3 Latin squares:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

Like always, whenever we introduce a mathematical concept in combinatorics, our first instinct should be to attempt to count it! In other words: given an order n, what is the largest collection of mutually orthogonal Latin squares we can find? An upper bound is not too hard to find:

Proposition. For any n, the maximum size of a set of $n \times n$ mutually orthogonal Latin squares is $n - 1$.

Proof. Take any collection $T_1, \dots T_k$ of mutually orthogonal Latin squares. Then notice the following property: if we take any of our Latin squares and permute its symbols (i.e. switch all the 1 and 2's), the new square is still mutually orthogonal to all of the other squares. (Think about this for a bit if you are unpersuaded.)

Using the above observation, notice that we can without any loss of generality assume that the first row of each of our Latin squares is $(1, 2, 3 \dots n)$. Now, take any pair of mutually orthogonal Latin squares from our collection, and look at the symbol in the cell in the first column/second row (i.e. the symbol at $(2, 1)$):

$$\begin{bmatrix} 1 & 2 & \dots & n \\ x & - & \dots & \\ \vdots & & & \\ - & - & \dots & - \end{bmatrix}, \begin{bmatrix} 1 & 2 & \dots & n \\ y & - & \dots & \\ \vdots & & & \\ - & - & \dots & - \end{bmatrix}.$$

[2]This idea has no obvious corresponding geometric context; just think of it as a name for now.

We know that neither x nor y can be 1, because both of these squares are Latin squares. As well, we know that they cannot agree, as the first row of the superimposition of these two squares contains the pairs (k, k) , for every $1 \leq k \leq n$. This means that there are at most $n-1$ squares in our collection $T_1, \ldots T_k$, because there are $n-1$ distinct choices for the cell $(2,1)$ that are not 1. $\square$

We already know that sometimes $n-1$ is attainable: in our example above, we found 2 orthogonal Latin squares of order 3. When can we attain this bound?

Perhaps surprisingly, the answer to this question is intimately related to the concept of finite fields! Specifically, we have the following theorem

Proposition. Let F be a finite field that contains n elements. Then there is a collection of $n-1$ mutually orthogonal Latin squares.

Proof. For simplicity's sake, enumerate the elements F as $\{f_0, f_1 \ldots f_{n-1}\}$, such that $f_0 = 0$ and $f_1 = 1$. Now, notice the following fact: if $a \in F$ is nonzero, then the grid

$$\begin{bmatrix} af_0 + f_0 & af_1 + f_0 & \ldots & af_{n-1} + f_0 \\ af_0 + f_1 & af_1 + f_1 & \ldots & af_{n-1} + f_1 \\ \vdots & \vdots & \ddots & \vdots \\ af_0 + f_{n-1} & af_1 + f_{n-1} & \ldots & af_{n-1} + f_{n-1} \end{bmatrix},$$

where we fill the cell (i, j) with $af_i + f_j$, is in fact a Latin square! To see why, suppose that there is some row i along which two cells (i, j) and (i, k) of this grid are the same: i.e. that

$$\begin{aligned} af_i + f_j &= af_i + f_k \\ \Rightarrow a(f_i - f_i) &= (f_k - f_j) \\ \Rightarrow 0 &= (f_k - f_j) \\ \Rightarrow f_j &= f_k, \end{aligned}$$

and therefore that $j = k$ and that these two cells are the same. Similarly, if we pick any column j along which two cells (i, j) and (k, j) of this grid are the same, we get

$$\begin{aligned} af_i + f_j &= af_k + f_j \\ \Rightarrow a(f_i - f_k) &= (f_j - f_j) \\ \Rightarrow a(f_i - f_k) &= 0 \\ \Rightarrow f_i - f_k &= 0 \\ \Rightarrow f_j &= f_k, \end{aligned}$$

and can again conclude that these two cells were the same.

This generates $n-1$ distinct Latin squares: label them T_a, for every element $a \in F$. We claim that this is fact a set of mutually orthogonal Latin squares! To see why, take any two squares T_a, T_b, and suppose that there are two cells $(i,j),(k,l)$ at which superimposing our two Latin squares yields the same ordered pair of symbols: i.e. that

$$af_i + f_j = af_k + f_l \text{ and } bf_i + f_j = bf_k + f_l.$$

Taking the difference of these two equations yields

$$\begin{aligned}(a-b)f_i &= (a-b)f_k \\ \Rightarrow f_i &= f_k;\end{aligned}$$

plugging this into our earlier equations yields $f_j = f_l$, and therefore that these two cells are the same. Therefore, this is a set of $n-1$ mutually orthogonal Latin squares! $\square$

We give an example of this construction here:

Construction. Given a finite field F, we can form the **ring of polynomials over** F, $F[x]$, by simply taking all of the polynomials of the form

$$a_0 + a_1x + a_2x^2 + \dots x^n,$$

where the elements a_i are all elements in our field F. (We multiply and add these polynomials as we would normally: i.e $(a+bx)(c+dx) = ac + (bc+ad)\cdot x + bd \cdot x^2$, where we use our field to figure out how the multiplication and addition of these elements actually works.

A polynomial in $F[x]$ is called **irreducible** if there is no way to write it as the product of two polynomials with smaller degrees. For example, if $F = F_2 = \mathbb{Z}/2\mathbb{Z}$, the element x^2+1 of $F[x]$ is not irreducible, because $(x+1)\cdot(x+1) = x^2+2x+1 \equiv x^2+1 \mod 2$. However, the polynomial x^2+x+1 is irreducible in $F[x]$, which you can check by taking all of the polynomials of smaller degrees, taking their products, and checking that you never get x^2+x+1.

Suppose that you take a finite field F, create the ring of polynomials $F[x]$, and then find an irreducible polynomial $g(x)$ in $F[x]$ that's irreducible of degree n. By multiplying by an appropriate constant, make it so that the coefficient of x^n in $g(x)$ is 1.

Now, take $F[x]$, and regard two polynomials as being the "same" if they differ by a multiple of $g(x)$. (This is similar to the way we defined $\mathbb{Z}/n\mathbb{Z}$ by saying that two things are the same if they differ by a multiple of n.) Call this object $F[x]/\langle g(x)\rangle$.

This, rather surprisingly, is a finite field with $|F|^n$-many elements.

Example. To illustrate this, take $F = \mathbb{Z}/2\mathbb{Z}$, and $g(x) = x^2+x+1$. The elements of $F[x]$ look like

$$0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^3, \dots$$

Suppose that we regard two elements in $F[x]$ to be the same up to a multiple of $g(x)$. Then, if we take any element $h(x)$ of $F[x]$ and repeatedly subtract appropriately chosen multiples of $x^kg(x)$ from$h(x)$, we can eventually insure that $h(x)$ is a polynomial of degree at most

1. You can check that none of the remaining four elements of $F[x]$ can be turned into each other via adding/subtracting multiples of x^2+x+1; therefore, we have

$$F[x]/\langle g(x)\rangle = \{0, 1, x, x+1\}.$$

By examining the addition and multiplication tables below, we can easily see that this forms a field:

$$\begin{array}{c|cccc} + & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 1 & x & x+1 \\ 1 & 1 & 0 & x+1 & x \\ x & x & x+1 & 0 & 1 \\ x+1 & x+1 & x & 1 & 0 \end{array}, \quad \begin{array}{c|cccc} \cdot & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & x+1 \\ x & 0 & x & x+1 & 1 \\ x+1 & 0 & x+1 & 1 & x \end{array},$$

(To check the multiplication table above, in particular, we used the observation that $x^2 \equiv x^2+(x^2+x+1) = 2x^2+x+1 \equiv x+1 \mod$ "$2, x^2+x+1$," and similarly that $x(x+1) \equiv 1, (x+1)^2 \equiv x \mod$ "$2, x^2+x+1$.")

A beautiful consequence of this example is that it gives us a way to create three mutually orthogonal Latin squares of order 4, using our construction from earlier:

$$T_1 = \begin{bmatrix} 0 & 1 & x & x+1 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \end{bmatrix}, T_x = \begin{bmatrix} 0 & 1 & x & x+1 \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \\ 1 & 0 & x+1 & x \end{bmatrix}$$

$$T_{x+1} = \begin{bmatrix} 0 & 1 & x & x+1 \\ x+1 & x & 1 & 0 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \end{bmatrix}$$

These are all orthogonal!

So: with this lecture, we've shown (up to a nontrivial result on finite fields!) that whenever n is a prime power, we have sets of mutually orthogonal Latin squares that are as large as we could hope for (i.e. $n-1$.)

Given this, you might hope that we can **always** find sets of $n-1$ mutually orthogonal Latin squares, for any order n. This turns out to be tragically false:

Theorem. There are no pair of mutually orthogonal Latin squares of order 6.

As far as I know, there are no known proofs of this result that boil down to anything much more elegant to just brute-force-checking all of the pairs (which, given that there are $6! \cdot 5! \cdot 9,408$ distinct Latin squares, is not pleasant. Relatedly, this makes the fact that this was proved in 1899-1900 by Tarry, long before the advent of computers, even more impressive.)

In general, we don't know very much about this question: the maximum number of mutually orthogonal latin squares of order 10, I believe, is still not known, as is the value for almost all numbers that are not prime powers (and thus values for which we can make finite fields!)