Latin Squares and Their Applications

Jason Tang
Mentor: Wendy Baratta

October 27, 2009

1 Introduction

Despite Latin Squares being a relatively unknown aspect of mathematics, there are many interesting areas that are worth studying, including their transversals, Mutually Orthogonal Latin Squares (MOLS) and Latin subsquares, just to name a few. Latin squares also have a variety of different practical applications, for example they can be used to code messages, design tournaments or generate magic squares. The popular number puzzle Sudoku is actually just an order 9 Latin Square, with the additional constraint that each of the 9 distinct 3x3 squares must also contain the numbers 1 to 9 once and only once.

1.1 Basic Definitions

We begin by introducing some basic knowledge, but which is vital to the investigation of applications later on.

A **Latin Square** is square grid with an entry in each cell so that each of the numbers 1 to n (n being the width/height of the square) occurs only once in each row and column. For example,

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

is a Latin Square of order 4.

If there are two Latin Squares, which when superimposed, give co-ordinates which are all different (i.e. every possible co-ordinate occurs exactly once), they are called **Mutually Orthogonal Latin Squares (MOLS)**. The concept of Mutual Orthogonality can extend to a set of more than two squares, with every square being mutually orthogonal to every other.

The two Latin Squares

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \quad \text{and} \quad \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array}$$

are MOLS because when superimposed, they give nine distinct co-ordinates. We call these squares **orthogonal mates** of each other.

Closely related to the MOLS are **transversals**. If, in an $n \times n$ Latin Square, there are n cells so that every cell occurs once in each row and column, and contain the numbers 1 to n, then this set of cells is called a transversal. In the 3×3 square below, the bold entries form a transversal.

$$\begin{array}{ccc} \mathbf{3} & 1 & 2 \\ 2 & 3 & \mathbf{1} \\ 1 & \mathbf{2} & 3 \end{array}$$

So how are MOLS and transversals related?

Theorem 1 *A Latin Square has an orthogonal mate if and only if it contains n disjoint transversals.*

Proof. If a Latin Square contains n disjoint transversals, then these transversals can be put together to form another Latin Square, simply by giving each of the entries in the same transversal the same symbol. In fact, this new Latin Square is an orthogonal mate, because for any particular symbol in the new Square, there is a set of n different symbols in the corresponding positions of the old square because it's a transversal of the old square.

Conversely, if a Latin Square L has an orthogonal mate M, take any element in M and check the corresponding entries in L. Due to the properties of Mutual Orthogonality, the entries in L must all be different. And since the entries picked were a particular element from M, they must all be from different rows and columns, thus fulfilling the properties of a transversal. Repeat this process with every element of M, and n distinct transversals will be found. ■

An example which shows the relationship (explained in Theorem 1) between transversals and MOLS is given below.

$$\begin{array}{cccc} 1_a & 2_b & 4_c & 3_d \\ 2_c & 1_d & 3_a & 4_b \\ 4_d & 3_c & 1_b & 2_a \\ 3_b & 4_a & 2_d & 1_c \end{array} \qquad \begin{array}{cccc} a & b & c & d \\ c & d & a & b \\ d & c & b & a \\ b & a & d & c \end{array}$$

1.2 Conjugates and Isotopes

Any Latin Square can be written as a set of triples in the form (row, column, symbol). For example, the Latin Square

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \text{ can be written as } \begin{array}{cc} (1,1,1) & (1,2,2) \\ (2,1,2) & (2,2,1) \end{array}.$$

If we take an existing Latin Square and permute the rows, columns and symbols, then this new square is called an **isotope** of the old square. It's easy to see that an isotope of a Latin Square is a Latin Square, maps transversals to transversals, and therefore maintains Mutual Orthogonality properties.

A **conjugate** of a Latin Square is a permutation of an existing Latin Square through reordering the co-ordinates. Taking the original Latin Square where the co-ordinates are (r, c, s), we can create five more, (r, s, c), (c, r, s), (c, s, r), (s, r, c), and (s, c, r), so there are six conjugates of any Latin Square including itself. It may be a little more difficult to see how creating a conjugate maps transversals to transversals, so we will now show this.

Theorem 2 *A conjugate of a Latin Square with a transversal also has transversals.*

Proof. If a Latin Square has a transversal, then in the co-ordinate form, the transversal has one of each r value, one of each c value, and one of each s value. If we create a conjugate of a Latin Square, then this transversal will still exist (since we are just re-ordering the co-ordinates). Thus creating a conjugate also maps transversals to transversals. ■

Remark 1 *In this essay, I will use the following notation: if A is a Latin Square, the entry at row i and column j of the square will be denoted by A_{ij}.*

2 Existence and construction of MOLS

2.1 Upper Bound

The following theorem gives a useful upper bound for the maximum number of MOLS of order n.

Theorem 3 *For any $n > 1$, the maximum number of squares in a set of MOLS is $n - 1$.*

Proof. Take a supposed set of MOLS, and for every square permute the columns so that the first row reads $1, 2, \ldots, n$ (Since this does not change the orthogonality of the square with other squares). Then we have generated the co-ordinates $(1,1)(2,2)\ldots\ (n,n)$ so far. Now, take the first entry in the second row of one Latin Square in this set. Call this entry x. Then, for another Latin Square to be orthogonal, the corresponding entry y must be different to x (otherwise we have generated another co-ordinate (x,x) and this contradicts the orthogonality property). A third Latin Square must have a symbol different to both of these to maintain orthogonality. Since there are $(n-1)$ symbols that can appear at this position, this is the bound for the maximum number of MOLS. ■

1	2	3	4	...	n
x					
...					

1	2	3	4	...	n
y					
...					

Diagram showing that only $n-1$ symbols can appear in this position

2.2 $F_a(x, y)$ construction method

The following construction assumes basic knowledge about group theory and modular arithmetic. If unfamiliar with group theory or modular arithmetic, please see Appendices A and B respectively.

Theorem 4 *The upper bound of n-1 MOLS can be reached when constructing Latin Squares of prime orders.*

Proof. Maximum sets of MOLS of prime orders can be generated quite easily by the following method:

Take the integers $0, 1, \ldots\ , p-1$ (where p is a prime). Put them (order isn't important) above and beside a $p \times p$ grid. Then, for $a = 1$, in each cell put $ax+y$ (mod p) where x is the number to the left of the row and y is the number above the column. In every row there will clearly be the numbers $\{0, 1, \ldots\ , p-1\}$ and the same applies for every column, since p is prime.

After doing this, make a a different value and repeat the process. We then obtain a different square.

Firstly, both squares are Latin Squares: two entries in the same column or row cannot be identical, due to group properties. We also see that the two squares are mutually orthogonal, and this is always the case. The reason for this is that changing the value of a simply permutes (here when I say 'permutes' I mean all permutations excluding the identity) $p-1$ of the rows. All of the $p-1$ will be permuted because p and <row-value> are relatively prime, so every time a changes, the value of [$a\times$ <row-value>] will change. Any Latin Square and a permutation of $n-1$ of its rows are mutually orthogonal. ■

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

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

Example grids for $a = 1$ and $a = 2$ where $p = 5$

Proof.

■

The aforementioned upper bound also holds for Latin Squares of prime power orders, however for prime powers, the reader may notice that the above method fails. For composite values of n, two entries in the same column may well be the same (since the elements no longer comprise a group, the left/right cancellation laws don't hold). To overcome this problem we use polynomials. Polynomials are useful because they can be treated as integers; they can be added and multiplied and therefore 'prime polynomials' exist. We work in a similar way, doing the calculations modulo the 'prime polynomial'. A full explanation of the required theory would digress too much from the purposes of this essay, so instead a simple example is given below.

Say we want to create a maximum set of MOLS of order 2^2. We use four polynomials of order 0 and 1 with binary co-efficients (The polynomials used are 0, 1, x and $x + 1$). Then we use the $F_a(x, y)$ construction method and fill in all the entries. An example is given below, using the prime polynomial $x^2 + x + 1$. Note that $x^2 \equiv -(x + 1) \pmod{x^2 + x + 1}$, and since we're dealing with binary co-efficients, $-(x + 1) = x + 1$.

Repeatedly shifting the value of a will yield three Mutually Orthogonal Latin Squares. (If the sight of polynomials in Latin Squares is unsettling, simply replace every polynomial with a number.)

	0	1	x	$x+1$
0	0	1	x	$x+1$
1	x	$x+1$	0	1
x	$x+1$	x	1	0
$x+1$	1	0	$x+1$	x

Polynomially-generated Latin Square for $a = x$ where $p = 2^2$

2.3 Kronecker Product

The following is another useful method of constructing pairs of MOLS:

Say we have a Latin Square A of order 2 and another one, B of order 3. We can obtain a Latin Square of order 6 simply by taking co-ordinates like so:

$$\begin{array}{cc}(A_{11},B) & (A_{12},B)\\(A_{21},B) & (A_{22},B)\end{array} \quad \text{where } (A_{ij},B) = \begin{array}{ccc}(A_{ij},B_{11}) & (A_{ij},B_{12}) & (A_{ij},B_{13})\\(A_{ij},B_{21}) & (A_{ij},B_{22}) & (A_{ij},B_{23})\\(A_{ij},B_{31}) & (A_{ij},B_{32}) & (A_{ij},B_{33})\end{array}$$

For example, the Kronecker Product of A and B is shown below.

$$A = \begin{array}{cc}1 & 0\\0 & 1\end{array} \qquad B = \begin{array}{ccc}0 & 1 & 2\\2 & 0 & 1\\1 & 2 & 0\end{array}$$

$$\text{gives} \quad \begin{array}{cccccc}(1,0) & (1,1) & (1,2) & (0,0) & (0,1) & (0,2)\\(1,2) & (1,0) & (1,1) & (0,2) & (0,0) & (0,1)\\(1,1) & (1,2) & (1,0) & (0,1) & (0,2) & (0,0)\\(0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2)\\(0,2) & (0,0) & (0,1) & (1,2) & (1,0) & (1,1)\\(0,1) & (0,2) & (0,0) & (1,1) & (1,2) & (1,0)\end{array}$$

This construction generalises: Given a square A of order m and a square B of order n, we can always construct a square of order mn using this method.

Theorem 5 *If there are two pairs of MOLS, of order m and n, then there is a pair of MOLS of order mn.*

Proof. Call the two MOLS of order m M_1 and M_2. Call the two MOLS of order n N_1 and N_2. Take the Kronecker product of M_1 and N_1, and do the same for M_2 and N_2. We now have two squares of order mn, and simply need to show that they are Mutually Orthogonal.

M_1 and M_2 are orthogonal, so every ordered pair (M_{1ij}, M_{2ij}) will occur only once. This means that every $((M_{1ij}, N_1), (M_{2ij}, N_2))$ occurs only once. Similarly, since N_1 and N_2 are orthogonal, every ordered pair (N_{1ij}, N_{2ij}) will occur only once also. This means that every $((M_1, N_{1ij}), (M_2, N_{2ij}))$ will also occur only once. Therefore every entry $((M_{1ij}, N_{1ij}), (M_{2ij}, N_{2ij}))$ is different. ■

3 Applications of Latin Squares

3.1 Error-Correcting Codes

I'm sure you're familiar with a wonderful feature called the spell-checker, inherent in most word-processors nowadays. This program gives the reader a list

of allowed suggestions of words from a big dictionary, and it finds the closest matches by choosing the words in which the letters match most closely with the incorrect word.

Proof-reading of codes works in a similar way. There is a preset list of allowed 'codewords'. If the code-writer mistypes a string of characters, the program will then find the closest match from the list of codewords and correct the mistake automatically. The following section focuses more on the *existance* of such codes rather than how they work.

Definition 6 *An (n, M, d) q-ary code C is a set of M codewords taken from a set of q elements, where each codeword has length n and minimum distance d.*

Example 7 *A binary (2-ary) code $(5, 6, 3)$ is a code with 6 codewords, each 5 letters long, taken from the alphabet $\{0, 1\}$ and with each word differing with each other in at least 3 places.*

Theorem 8 *In a code C, for any q, s, d the largest value of M is at most $q^{(s-d+1)}$.*

Proof. Remove the last $(d-1)$ co-ordinates from each codeword in C. Since each pair of codewords have to differ in at least d places, the remaining $(s-d+1)$-tuples must all be different (if they were the same, then the two codewords would differ in less than d places). There are a maximum of $q^{(s-d+1)}$ different $(s-d+1)$-tuples, so this is the maximum number of codewords. ■

Theorem 9 *There exists a q-ary $(4, q^2, 3)$ code $\iff$ There exists a pair of MOLS of order q.*

Proof. Imagine a code C, with codewords $\{I, J, A_{ij}, B_{ij}\}$, where the values come from two MOLS A and B of order q, where I is the row number, J is the column number, A_{ij} is the entry at row i and column j of square A, and similarly for B_{ij} in square B. For any two codewords, only one co-ordinate is allowed to be the same.

We first prove that the existance of MOLS implies the existance of a code:

Assume there exists a pair of MOLS of order q. Then if two I values are the same, then J is different (otherwise they would form the same codeword). Any two A_{ij} values are different, because it's a Latin square and there can't be two entries in the same row with the same value. The same reasoning applies to B_{ij}.

A symmetrical argument applies to the J value, regarding the columns.

The only thing left to consider is if the A_{ij} and B_{ij} values are both the same in two codewords. If the A_{ij} values are the same, then those two values are two entries of a transversal of B_{ij}, and hence the B_{ij} values are different.

Conversely, we now assume that there exists a code and show that the MOLS exist:

Build two Squares using the code. There will be q^2 entries. The fact that every (I, A_{ij}) and every (J, A_{ij}) co-ordinate is different proves that A is a Latin Square, and similarly with (I, B_{ij}) and (J, B_{ij}) with B. Because every pair of (Aij, Bij) co-ordinates are different, A and B are MOLS. ■

Theorem 10 *There exists a q-ary* $(s, q^2, s-1)$ *code* C *if there exist* $(s-2)$ *MOLS of order q.*

Proof. Assume there are $(s-2)$ MOLS of order q, called $A, B, C, \ldots .Z$. Then, take all pairs of codewords $\{I, J, Aij, Bij, Cij, \ldots Zij\}$. We need to show that all pairs of codewords have the same co-ordinate in at most 1 place. If the I values are the same, then every other value is different, due to the reasoning in the previous theorem (two entries in the same row cannot be identical). Similarly for J. If any A_{ij} values are the same, then all the other Bij, $Cij \ldots Zij$ values are different because the A_{ij} values are again two entries of a transversal. The same argument applies to $B_{ij}, C_{ij}, ..., Z_{ij}$. Thus all codewords differ by at least (exactly, in fact) $s-1$. ■

3.2 Cryptography

The basic aim of crytography is simple. A sender wants to send a message, but first encodes it so that no third party can read it. The reciever, upon recieving the message, decodes it using the same code that was used to encrypt it.

Latin Squares can be used in the creation of codes. One way to do this is as follows:

Take two MOLS of order n and assign each of the co-ordinates a letter or symbol, which the sender and receiver agree on beforehand. Then the sender encrypts the message by substituting each letter/symbol with the corresponding co-ordinates, and sends it. The receiver then decrypts the message by using the MOLS, since every co-ordinate occurs only once. Unless a third party knows the two MOLS used *and* which letters correspond to which co-ordinates, it's impossible to decrypt, making it an effective coding system. For example, one might use the MOLS

1	2	3		3	1	2		D	C	I
2	3	1		2	3	1	and the letters	B	H	A
3	1	2		1	2	3		G	F	E

so that the letter C becomes the ordered pair $(2, 1)$.

Then to send the word 'bag' one could just send the string of co-ordinates $(2, 2)(1, 1)(3, 1)$.

Of course, with larger MOLS more letters and symbols could be encrypted.

There is also more secrecy because the number of pairs of MOLS increases exponentially as the value of n gets higher.

Note: Since it has been proven that no pairs of MOLS of order 2 and 6 exist, codes of these sizes cannot be constructed using this method.

3.3 Affine and Projective Planes

Examples are given at the end of this section.

Definition 11 *An affine plane is a set of points and lines such that:*

1. *There is exactly one line joining any two points.*
2. *Given a point P and a line L, there is a unique line passing through P and parallel to L.*
3. *There exist four points such that no three of them are collinear.*

Note that the Euclidian plane is a good example of such a plane, but in this section we are more concerned with finite affine planes, i.e. planes which have a finite number of points and lines.

A finite affine plane of order n contains $n + 1$ parallel 'classes' of n lines, each containing n points. Therefore it contains n^2 points and $n(n + 1)$ lines.

Definition 12 *A projective plane is a set of points and lines such that:*

1. *There is exactly one line joining any two points.*
2. *Any two lines intersect at a unique point.*
3. *There are four points such that no three of them are collinear.*

The difference between an affine plane and a projective plane is that the second requirement of having parallel lines has been replaced with another axiom which states that all lines intersect. The combination of axiom 1 (a unique line joins two points) and axiom 2 (a unique point joins two lines) means that a projective plane is symmetrical in the sense that if a projective plane was inverted - every point turned into a line and vice versa - then the plane would stay the same.

In any projective plane of order n, every line contains $n+1$ points and every point lies on $n + 1$ lines. Each projective plane therefore contains $n^2 + n + 1$ points and $n^2 + n + 1$ lines.

Theorem 13 *The existance of an affine plane of order $n \Leftrightarrow$ The existance of a projective plane of order n.*

Proof. Any affine plane can be transformed into a projective plane as follows:

Extend the lines on each parallel class to meet at a 'point at infinity', so that $n+1$ new points are made. Then join all of these 'points at infinity' with a line. The result is a plane with $n^2 + n + 1$ points and $n^2 + n + 1$ lines. Furthermore, every pair of lines now intersect at a unique point since the parallel classes now join at the 'point at infinity', and every pair of points is still joined by a unique

line since we've joined every new point that was created. Thus the requirements of a projective plane are fulfilled.

Any projective plane can be transformed into an affine plane by the reverse method, i.e. by removing one line and all of the $n+1$ points on it. This will create the parallel classes, and n^2 points on $n(n+1)$ lines will remain. ■

Theorem 14 *There exists an affine plane of order n iff there exists a complete set of MOLS of order n.*

Proof. A complete set of MOLS can be transformed into an affine plane as follows:

Represent every cell in the Latin Square with a point. Let the rows of the squares represent one class, and let the columns of the squares represent another class. Then let the remaining $n-1$ parallel classes be defined by the $n-1$ MOLS, by letting each square represent a parallel class and connecting all instances of the same element. Then we have an affine plane, where each line of a class intersects every line of every other class once (properties of a transversal).

Alternatively, given an affine plane of order n, take one parallel class, label it i, and take another and label it j. Then label the lines in these classes from 1 to n. These represent the rows and columns of our MOLS. Take a different parallel class and put the points into row i and column j of the first Latin Square (i, j is defined by which line of class i and which line from class j the point belongs to), with every parallel class taking the same element. Repeating this with each of the $n-2$ classes remaining, we obtain $n-1$ MOLS. ■

Therefore Theorem 14, in conjunction with Theorem 13, shows the following relationship:

The existance of a complete set of MOLS ⇔ Existance of an affine plane ⇔ Existance of a projective plane

2×2 Affine Plane 2×2 Projective Plane 3×3 Affine Plane

Can you turn the 3×3 Affine Plane into a Projective Plane?

4 Latin Subsquares

Definition 15 *A Latin Subsquare is a Latin Square contained in a larger Latin Square. (The rows and columns in the subsquare are not necessarily adjacent.)*

In the following Latin Square, the bold entries form a Latin Subsquare.

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

4.1 Tang Upper Bound

Theorem 16 *There is a maximum of four* 3×3 *subsquares in an order* 6 *Latin Square (In fact, there can be only* 4 *or* 0*).*

Proof. Assume there is one subsquare. Then we may take an isotope of the Latin Square so that this 3×3 subsquare is in the top left corner (allowable since an isotope is equivalent to the original square). This forces three other subsquares, and they are in the remaining three corners of the square. Now it suffices to show that no more 3×3 subsquares can be found.

	D	E		F		
A	**1**	**2**	**3**	4	5	6
B	**3**	**1**	**2**	6	4	5
C	**2**	**3**	**1**	5	6	4
	4	5	6	**1**	**2**	**3**
G	6	4	5	**3**	**1**	**2**
	5	6	4	**2**	**3**	**1**

Without loss of generality we break up all possible situations into two cases:

Case 1: We pick 3 rows from the same set and split up the columns (e.g. rows ABC, columns DEF), and try to make a subsquare out of the intersection of these lines. We find that column D already has 3 distinct elements, and since column F belongs to a different subsquare, column F contains different elements. If a subsquare were to exist it must contain only 3 elements. So this is not possible.

Case 2: We split up the rows AND the columns (e.g. rows ABG, columns DEF). This will always create a 2×2 square in some subsquare, and any 2×2 square in a 3×3 Latin Square contains 3 different entries. Any entry from an adjacent subsquare (which we always have) will add a different entry, giving us at least 4 entries, and therefore a subsquare cannot exist. ■

This result may lead us to conjecture the following:

Conjecture 17 *For any Latin Square comprised of distinct* $n/2 \times n/2$ *subsquares, there is a maximum of 4 subsquares.*

It only takes a simple counterexample to disprove this:

1	**2**	3	4	**5**	**6**	7	8
2	**1**	4	3	**6**	**5**	8	7
3	4	1	2	7	8	5	6
4	3	2	1	8	7	6	5
5	**6**	7	8	**1**	**2**	3	4
6	**5**	8	7	**2**	**1**	4	3
7	8	5	6	3	4	1	2
8	7	6	5	4	3	2	1

The lines separate the square into 4 subsquares, and the bold entries form another subsquare.

4.2 Upper Bound for Subsquares

Seeing our conjecture disproved, we will now work out a reliable upper bound for the number of subsquares of order m in a given Latin Square of order n.

Theorem 18 *The maximum number of* 2×2 *subsquares (called intercalates) in a Latin Square is* $n^2(n-1)/4$.

Proof. An intercalate can only occur in a pair of rows, so we begin by counting the number of pairs of rows in any Latin Square, and this is ${}^nC_2 = n(n-1)/2$. In any pair of rows, the maximum number of subsquares is $n/2$ (once a square has been found, these symbols cannot be used again in this pair of rows). Thus the maximum number of intercalates in a Latin Square is $n(n-1)/2 \times n/2 = n^2(n-1)/4$. ■

This upper bound can be improved for the case where n is odd.

Theorem 19 *The maximum number of intercalates in a Latin Square of odd order is* $n(n-1)(n-3)/4$.

Proof. The number of pairs of rows is again $n(n-1)/2$. But this time, if we find $(n-1)/2$ intercalates in a pair of rows, then the last pair of entries would be left the same. Therefore we must loosen this to $(n-3)/2$, and by multiplying the two values together we get the result $n(n-1)(n-3)/4$. ■

Next we will investigate the bound for 3×3 subsquares.

Theorem 20 *The maximum number of* 3×3 *subsquares in a LS is* $n^2(n-1)/18$.

Proof. As before, we begin by counting the number of pairs of rows (we don't need to count triplets, because any two rows define the third), which is equal to $n(n-1)/2$. Then, the maximum number of subsquares which can occur in a set of rows is $n/3$, so we have $n^2(n-1)/6$. But since we counted each set of rows three times at the start, we must divide this by three and this gives us $n^2(n-1)/18$. ■

Using the 3×3 subsquares method as a guide, we can derive a theorem for the general case with subsquares of order m:

Theorem 21 *The maximum number of subsquares of order m in a Latin Square is*

$$ {}^nC_{m-1}\frac{n}{m^2}. $$

Proof. We first count the number of sets of $m-1$ rows, and this is ${}^nC_{m-1}$. The maximum number of subsquares which can occur in a row is n/m. But when counting rows at the start, we counted every set of m rows m times, so we must divide by m, giving the desired result. ■

Note: ${}^nC_r$ is the number of ways that a group of r objects can be chosen from n objects. It is equivalent to

$$ \frac{n!}{r!(n-r)!}. $$

References

[1] Fraleigh, J. *A First Course in Abstract Algebra*, Pearson Education Inc, 2003.

[2] Clarke, L. *Applications of Mutually Orthogonal Latin Squares*, Honours essay, 2007.

[3] Clarke, L. *Transversals in Latin Squares*, Honours Project, 2007.

[4] McBride, T. *Subsquares in Latin Squares*, 3rd Year Maths essay, 2009.

5 Appendix A: Introduction to Group Theory

A group is a nonempty set S together with a binary operation $*$ such that it satisfies the following three axioms:

1. There exists an identity element e such that for all $a \in S$, $a * e = a = e * a$.
2. Every element b has an inverse b^{-1} such that $b * b^{-1} = e = b^{-1} * b$.
3. For any $a, b, c \in S$, $(a * b) * c = a * (b * c)$. This is called the associativity law.

An example of a group is the set $\mathbb{Z}$ together with addition. In this case the identity element is 0, the unique inverse of any number is simply its negative, and clearly the associativity law holds.

Theorem 22 *In any group the left and right cancellation laws apply, i.e.* $a * b = a * c \Longrightarrow b = c$ *and* $b * a = c * a \Longrightarrow b = c$ *for all* $a, b, c \in S$.

Proof. To show the left hand cancellation law we first assume $a * b = a * c$. Multiplying both sides by a^{-1} gives $a^{-1} * (a * b) = a^{-1} * (a * c)$. By the associativity law and the inverse property we have $b = c$, showing that the left cancellation law holds. The right cancellation law is shown similarly. ■

Theorem 23 *The identity element in a group is always unique.*

Proof. Say we have two different identities, e and $e\prime$. Then, by the properties of the identity, we get $e = e' * e = e * e' = e'$, showing $e = e'$, which is a contradiction. ■

Theorem 24 *The inverse of an element is unique.*

Proof. Assume $b \in S$ has two inverses, i^1 and i^2. Then:
$b * i^1 = b * i^2 = e$
By the left cancellation law, $i^1 = i^2$. ■

This is only a brief introduction to group theory, but this knowledge is all that is required for the various proofs in the main essay. If you would like to read more, you may consult the book 'Abstract Algebra' by Fraleigh [1].

6 Appendix B: Modular Arithmetic

If you've ever done division, you will have come across the term 'remainders'. Modular arithmetic is just that – arithmetic where one is only concerned with the remainders. Some examples are given below:

1. Counting from -10 to 10 in $(\mathrm{mod}\, 4)$ would look like this:

$2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2$

2. $6 + 5 \pmod 7$ is equal to 4 because the remainder when 11 is divided by 3 is equal to 2.

3. $0 - 3 \pmod 8$ is equal to 5 because the remainder when -3 is divided by 8 is 5.

4. $4 \times 3 \pmod 5$ is equal to 2 because the remainder when 12 is divided by 5 is equal to 2.

You may already have realised that when working in modulo n, numbers will never be equal to or greater than n. Also, for the purposes of the essay, negative modulos don't exist.

There are many uses of modular arithmetic, and it's very handy in solving many competition problems. Theory on modular arithmetic is deeply investigated, but for the purposes of this essay the above knowledge is all that is needed.