# MOLS and the Shrikhande Theorem

# Latin Squares

A Latin square is an $n \times n$ array of $n$ symbols where each symbol occurs exactly once in every row and column.

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

The multiplication table of any group is a Latin square.
For any $n$ there are at least $\prod_{k=1}^{k=n} k!$ Latin squares.

# Orthogonality

A pair of Latin squares is orthogonal if, when placed side by side like so:

$$\begin{bmatrix} 00 & 11 & 22 & 33 & 44 \\ 12 & 23 & 34 & 40 & 01 \\ 24 & 30 & 41 & 02 & 13 \\ 31 & 42 & 03 & 14 & 20 \\ 43 & 04 & 10 & 21 & 32 \end{bmatrix}$$

each combination of symbols occurs exactly once in the array. Except for $n = 6$ there exists at least one pair of orthogonal Latin squares for every $n > 2$ (Bose, Parker and Shrikhande 1958).

# Sets of mutually orthogonal Latin squares

If a set of $n \times n$ Latin squares are pairwise orthogonal, then they are said to *mutually orthogonal*, usually abbreviated to MOLS. The maximum size of a set of $n \times n$ MOLS is $n - 1$ as is shown below. If $n$ is a prime power, a set of $n - 1$ always exists. However that is not necessarily true for other values of $n$.

The $5 \times 5$ examples used here are a convenient cheat to avoid writing out large arrays.

# Maximum size of a set of MOLS is $n - 1$

By permuting the symbols in each Latin square we can always arrange the first row in the following standard way:

$$\begin{bmatrix} 000.. & 111.. & 222.. & ... & ... \\ 123.. & . & . & . & . \\ . & . & . & . & \\ . & . & . & . & . \end{bmatrix}$$

Now considering the first element of the second row, none of the squares can have the same symbol as the one above, so there are only $n - 1$ possible choices of symbol here for each square. But because of orthogonality, considering the rest of the top row, the first element of the second row cannot contain any pairs that have occurred before, so can only have $n - 1$ symbols.

# A graph from a set of MOLS

A graph is constructed from a set of MOLS by taking the positions in the $n \times n$ array as vertices. Two vertices are connected if:

a) they are in the same row or column, or
b) they have the same symbol in one of the squares.

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

This shows in red all the vertices which are connected to the top left vertex.

# A MOLS graph is strongly regular (SR)

A MOLS graph of $q$ MOLS clearly has $n^2$ vertices, and each vertex has valency

$$2(n-1) + q(n-1) = (q+2)(n-1).$$

But it is also strongly regular, each pair of connected vertices having $(q+2)(q-1)+n$ common neighbours, and each non-connected pair $(q+1)(q+2)$ common neighbours. This we try to show in the following slides.

# The MOLS graph is SR (connected vertices)

If the connected vertices (in blue) are in the same row (column), then the common neighbours are: vertices in the same row (column) (red), those in same column (row) as one vertex and sharing a symbol with the other (green), and those sharing a symbol with each (yellow).

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

This totals $n - 2 + 2q + q(q-1) = q^2 + q - 2 + n$

# The MOLS graph is SR (connected)

If the two vertices are connected because they share a symbol in the same square, the common neighbours are: those in the same row as one and column as the other (red), those sharing that same symbol (green), those in the same row or column as one and sharing a symbol with the other (orange), and those sharing a symbol with one and a different symbol with the other. Total:
$2 + n - 2 + 4(q-1) + (q-1)(q-2) = q^2 + q - 2 + n$

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

# The MOLS graph is SR (unconnected)

For two unconnected vertices, sharing neither symbol, row or column, the common neighbours are: those in the same row as one and column of the other (red), sharing a row or column as one and a symbol with the other (green), and (different) symbols with both (yellow)

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

Total: $2 + 4q + q(q-1) = (q+1)(q+2)$

# The complement of an SR graph is SR

If a SR graph has parameters $(n, d, \lambda, \mu)$, then the complement graph has degree $n - d - 1$. A vertex is connected to both of two vertices in the complement graph if it is connected to neither in the original graph. If $u$ and $v$ are connected, then the number of vertices connected to $u$ but not $v$ is $d - 1 - \lambda$, and likewise the number of vertices connected to $v$ but not $u$. Therefore the number of vertices connected to neither $u$ nor $v$ is:

$$n - 2 - \lambda - (d - 1 - \lambda) - (d - 1 - \lambda) = n + \lambda - 2d.$$

# The complement of an SR graph is SR

If $u$ and $v$ are not connected, then the number of vertices connected to $u$ but not $v$ is $d - \mu$, and likewise the number of vertices connected to $v$ but not $u$. Therefore in this case the number of vertices connected to neither $u$ nor $v$ is:

$$n - 2 - \mu - (d - \mu) - (d - \mu) = n - 2 + \mu - 2d.$$

and so the complement of a strongly regular graph with parameters $(n, d, \lambda, \mu)$ is strongly regular with parameters:

$$(n, n - d - 1, n - 2 - 2d + \mu, n - 2d + \lambda).$$

# The complement of a MOLS graph

So the complement of a MOLS graph of $q$ $n \times n$ MOLs, which has parameters

$$n^2, (q+2)(n-1), q^2+q-2+n, (q+1)(q+2)$$

is also SR, with parameters:

$$n^2, (n-1)(n-q-1), (n-q-1)(n-q-4)+n,$$

(n-q-2)(n-q-1)

# The complement of a MOLS graph -discussion

So the complement of a MOLS graph is also SR. Each vertex is connected to those vertices not connected in the MOLS graph, notably not the vertices in the same row or column. So the complement is not a MOLS graph with the same configuration of vertices to rows and columns, because it doesn't have the row and column edges, but nevertheless it may sometimes be a MOLS graph with a different configuration. A MOLS graph without the row and column edges is still SR, with parameters $(n^2, q(n-1), (q-1)(q-2), q(q-1))$. Note that there is only one case to consider for common neighbours of connected vertices.

# Filling in the gaps

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

The *deficit* of a set of MOLS is the difference between the number of MOLS in the set and the maximum possible, $n - 1$. If the deficit is 1, as in this example, the degree of the complement graph is $n - 1$, which splits the graph in $n$ cliques, where no two members of a clique are in the same row or column.

This is because the original MOLS graph connects each vertex to $n - 1$ other vertices in each row and column, leaving only one space in each case.

$$\begin{bmatrix} 000 & 111 & 222 & 333 & 444 \\ 123 & 234 & 340 & 401 & 012 \\ 241 & 302 & 413 & 024 & 130 \\ 314 & 420 & 031 & 142 & 203 \\ 432 & 043 & 104 & 210 & 321 \end{bmatrix}$$

The cliques can be used to define another Latin square:

$$\begin{bmatrix} 0000 & 1111 & 2222 & 3333 & 4444 \\ 1234 & 2340 & 3401 & 4012 & 0123 \\ 2413 & 3024 & 4130 & 0241 & 1302 \\ 3142 & 4203 & 0314 & 1420 & 2031 \\ 4321 & 0432 & 1043 & 2104 & 3210 \end{bmatrix}$$

which is orthogonal to each of the others. Recall that each Latin square divides the vertices into $n$ cliques of size $n$ and for any pair of MOLS, any pair of cliques intersects in exactly one vertex.

To prove that the new Latin square is orthogonal to all the other MOLS select any symbol from any Latin square and a symbol from the new square. Select a vertex which has both symbols.

But, apart from the selected vertex, all the vertices in the clique in the new square were not connected to the selected vertex in the MOLS graph, so the selected vertex is the only common vertex of the two cliques. So the two squares are orthogonal.

# Larger deficits

If the deficit is larger than 1, there is no guarantee that the complement graph can be decomposed into mutually orthogonal Latin squares. This would require that the graph could be divided into disjoint cliques of size $n$ in several different ways. Any clique from one division would intersect any clique from any other division in exactly one vertex.

If however the complement graph will split into a set of MOLS, the previous argument shows that each Latin square in the new set will be orthogonal to each Latin square in the original set.

# Sets of MOLS of deficit 2

If the deficit is 2, Shrikhande's theorem comes to our aid. For deficit 2, the parameters of the complement graph are $(n^2, 2(n-1), n-2, 2)$.
Shrikhande's theorem tells us that, if $n \neq 4$, a graph with these parameters is isomorphic to the line graph of $K_{n,n}$.
This is precisely what we need:

$$\begin{bmatrix} 00 & 01 & 02 & 03 & 04 \\ 10 & 11 & 12 & 13 & 14 \\ 20 & 21 & 22 & 23 & 24 \\ 30 & 31 & 32 & 33 & 34 \\ 40 & 41 & 42 & 43 & 44 \end{bmatrix}$$

So when $n \neq 4$ a set of $n-3$ MOLS can always be made up to a full set.

# When $n = 4$

When $n = 4$, for deficit 2 the number of Latin squares in the MOLS graph is just 1. If that Latin square is:

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$

the complement graph is isomorphic to $L(K_{4,4})$, so the single square can be augmented to a full set of MOLS.

# when $n = 4$ continued

If however the chosen Latin square is:

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}$$

the complement graph is isomorphic to the Shrikande graph, and so cannot be augmented to a full set.