Latin squares: Equivalents and equivalence

1 Introduction

This essay describes some mathematical structures 'equivalent' to Latin squares and some notions of 'equivalence' of such structures.

According to the *Handbook of Combinatorial Design* [2], Theorem II.1.5, a Latin square of order n is equivalent to

- the multiplication table (*Cayley table*) of a quasigroup on n elements;
- a transversal design of index 1;
- a $(3,n)$-net;
- an orthogonal array of strength 2 and index 1;
- a 1-factorisation of the complete bipartite graph $K_{n,n}$;
- an edge-partition of the complete tripartite graph $K_{n,n,n}$ into triangles;
- a set of n^2 mutually non-attacking rooks on an $n \times n \times n$ board;
- a single error detecting code of word length 3, with n^2 words from an n-symbol alphabet.

We add two further items to this list:

- a strongly regular graph of Latin square type;
- a sharply transitive set of permutations.

The statement is true but not sufficiently precise, since it is not explained what 'equivalent' means. The imprecision of which this is just an example has led to a number of inaccuracies in the literature. This essay will explain how to transform Latin squares into structures of each of these types, what notions of equivalence of Latin squares result from the natural definitions of isomorphism of these structures, and how the confusion may be avoided.

2 Latin squares

A *Latin square* of order n is an $n \times n$ array in which each of the n^2 cells contains a symbol from an alphabet of size n, such that each symbol in the alphabet occurs just once in each row and once in each column.

The alphabet is completely arbitrary, but it is often convenient to take it to be the set $\{1,2,\ldots,n\}$. This has the advantage that the same set indexes the rows and columns of the square.

It is clear that, if we permute in any way the rows, or the columns, or the symbols, of a Latin square, the result is still a Latin square. We say that two Latin squares L and L' (using the same symbol set) are *isotopic* if there is a triple (f,g,h), where f is a row permutation, g a column permutation, and h a symbol permutation, carrying L to L': this means that, if the (i,j) entry of L is k, then the $(f(i),g(j))$ entry of L' is $h(k)$. The triple (f,g,h) is called an *isotopy*. The relation of being isotopic is an equivalence on the set of Latin squares with given symbol set; its equivalence classes are called *isotopy classes*.

The notion of isotopy can be extended to Latin squares L,L' with different alphabets by allowing h to be a bijective map from the alphabet of L to that of L'. In this wider sense, any Latin square of order n is isotopic to one with alphabet $\{1,\ldots,n\}$.

A Latin square with symbol set $\{1,\ldots,n\}$ is *normalised* if the $(i,1)$ and $(1,i)$ entries are both equal to i, for all $i \in \{1,\ldots,n\}$. Given any Latin square, we can obtain from it a normalised Latin square by row and column permutations. So, in particular, every Latin square is isotopic to a normalised Latin square.

Despite the fact that the definition of a Latin square gives different roles to the rows, columns, and symbols, there are extra ‘equivalences’ connecting them. To each permutation π of the set $\{r,c,s\}$, there is a function on Latin squares. We give two examples (which suffice to generate all six):

- $L^{(r,c)}$ has (j,i) entry k if and only if L has (i,j) entry k (in other words, $L^{(r,c)}$ is the transpose of L);
- $L^{(r,s)}$ has (k,j) entry i if and only if L has (i,j) entry k.

The six Latin squares obtained from L in this way are the *conjugates* of L.

The *main class* or *species* of a Latin square is the union of the isotopy classes of its conjugates. Two Latin squares L,L' are *main class equivalent* if they belong to the same main class; that is, if L is isotopic to a conjugate of L'. Each main class is the union of 1, 2, 3 or 6 isotopy classes.

One of the important properties of main class equivalence is that it preserves various combinatorial properties. Here are some examples. Let L be a Latin square of order n.

- A *subsquare* of L of order k is a set of k rows and k columns in whose cells just k symbols occur. (These k^2 cells form a Latin square of order k if the remaining cells are removed.) A subsquare of order 2 is called an *intercalate*.
- A *transversal* of L is a set T of n cells, such that each row contains one member of T, each column contains one member of T, and each symbol occurs in one member of T. Now the square L possesses an orthogonal mate if and only if the n^2 cells can be partitioned into n transversals. (Associate one symbol of a new alphabet with each transversal, and let L' have (i,j) entry k if cell (i,j) lies in transversal k.)

Now the following is easily checked:

Proposition 1 *If two Latin squares are main class equivalent, then they have the same number of subsquares of each order, the same number of transversals, and the same number of partitions into transversals.*

For example, the two Latin squares shown below belong to different main classes since they have different numbers of intercalates (12 and 4 respectively) and different numbers of transversals (8 and 0 respectively).

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

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

A Web page giving the isotopy classes and main classes of Latin squares of small orders is maintained by McKay [3]. The numbers of Latin squares, isotopy classes, and main classes are given in sequences numbered A002860, A040082, A003090 in the *On-Line Encyclopedia of Integer Sequences* [4].

3 Quasigroups and loops

A *binary system* is a pair $(Q,*)$, where Q is a set and $*$ a binary operation on Q (a function from $Q \times Q$ to Q). We usually write the image of the operation on the pair (a,b) as $a*b$.

A *quasigroup* is a binary system $(Q,*)$ satisfying the two conditions

- for any $a,b \in Q$, there is a unique $x \in Q$ satisfying $a*x=b$;
- for any $a,b \in Q$, there is a unique $y \in Q$ satisfying $y*a=b$.

We often write the elements x and y above as $a\backslash b$ and b/a; these new operations are called *left division* and *right division* of b by a. These binary operations give new quasigroups on the set Q.

The *dual* of a binary system $(Q,*)$ is the binary system $(Q,\circ)$ whose operation is defined by $a\circ b=b*a$. It is also a quasigroup if $(Q,*)$ is.

An *operation table* or *Cayley table* of a set with a binary operation is the square array, having rows and columns indexed by Q in some order (the same order for rows as for columns), for which the entry in row a and column b is $a*b$. Now we have the following observation:

Proposition 2 *(a) The binary system $(Q,*)$ is a quasigroup if and only if some (and hence any) Cayley table for it is a Latin square.*

(b) If $(Q,*)$ is a quasigroup, then the conjugates of its Cayley table are the Cayley tables of $(Q,*)$, $(Q,\backslash)$ and $(Q,/)$ and their duals.

We note that, for some applications, the orders of the row and column labels are not required to be the same. This doesn't change the concept of "quasigroup" but the correspondence between quasigroups and Latin squares is rather different.)

For algebraic structures such as quasigroups, the appropriate notion of equivalence is *isomorphism*. An isomorphism from $(Q,*)$ to $(R,\circ)$ is a bijective function $f:Q\to R$ such that, for all $a,b\in Q$, we have

$$f(a)\circ f(b)=f(a*b).$$

An *automorphism* of a quasigroup $(Q,*)$ is an isomorphism from $(Q,*)$ to itself.

Two Cayley tables representing the same quasigroup differ only in the order of the elements labelling the rows and columns; thus, one is obtained from the other by applying simultaneously the same permutation to the rows and columns (including their labels). If it happens that the resulting square could alternatively be obtained by applying the given permutation to the row and column labels and to the entries of the square, then it is an automorphism of the quasigroup. For example, in the second quasigroup in the list below, the permutation $(a)(b\,c)$ is an automorphism.

We see that isomorphism of quasigroups is a much finer relation than isotopy of Latin squares; isomorphisms are isotopies (f,f,f) whose row, column and symbol permutations are equal. So, although there is only one isotopy class of Latin squares of order 3, there are five isomorphism classes of quasigroups, as shown below.

$*$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

$*$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

$*$	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

These five quasigroups can be distinguished by algebraic properties. An element a of a quasigroup $(Q,*)$ is an *idempotent* if $a*a=a$; it is a *left identity* if $a*x=x$ for all $x\in Q$; a *right identity* is defined analogously; and a is a *two-sided identity* if it is both a left and a right identity. Any isomorphism must preserve these properties of elements. Now

- in the first quasigroup, every element is an idempotent;
- the second quasigroup has one idempotent, which is a two-sided identity;
- the third quasigroup has one idempotent, which is a left but not a right identity;
- the fourth quasigroup has one idempotent, which is a right but not a left identity;
- the fifth quasigroup has no idempotents.

It is a simple exercise to show that the quasigroup defined by each of the twelve Latin squares with symbol set $\{a,b,c\}$ is isomorphic to one of these five.

A *loop* is a quasigroup which has a two-sided identity. This element is necessarily unique; for, if a is a left identity and b a right identity, then $a=a*b=b$. (More is true: a quasigroup cannot have two different left identities. For, if $a*x=x=b*x$, then $a=b$ by cancellation.)

If we write the Cayley table of a loop so that the first element is the identity, then the elements in the first row are the same as the row labels, and similarly for columns. In particular, if we use the labels $1,\ldots,n$, then the resulting Latin square is normalised. So a loop is a quasigroup which has a normalised Latin square as a Cayley table (when the labels occur in natural order). However, different normalised Latin squares can correspond to isomorphic loops! However, since the identity is unique, any quasigroup-isomorphism of loops is a loop-isomorphism.

Of the five quasigroups of order 3 (up to isomorphism), just one is a loop (the second). It is even a group. (A group can be defined as a loop satisfying the *associative law* $a*(b*c) = (a*b)*c$ for all a,b,c.)

The sequences enumerating quasigroups and loops are numbers A057991 and A057771 in the in the *On-Line Encyclopedia of Integer Sequences* [4].

4 Transversal designs and nets

Let L be a Latin square. Associated with L is an incidence structure called a 3-*net*, defined as follows. The points are the n^2 cells of the square, and there are three types of lines: the n rows; the n columns; and, for each of the n symbols in the alphabet, the set of cells containing that symbol. Nets are also called *square lattice designs*.

The net has the following properties:

(a) There are n^2 points and $3n$ lines.

(b) Each line contains n points, and each point lies on 3 lines.

(c) Two points lie on at most one line.

(d) The design is *resolvable*: the lines can be partitioned into three families of n lines, each of which is a partition of the set of points. Moreover, two lines from different families intersect in a (unique) point.

The three families of lines in the resolution correspond to rows, columns, and symbols. The second sentence of (d) shows that there is a unique resolution: two lines belong to the same family if and only if they are disjoint.

Because of this uniqueness, it is possible to recover the Latin square from a structure satisfying (a)–(d). Label the three resolution classes R, C, and S, and number the lines in each class from 1 to n. Now the Latin square has (i,j) entry k if and only if the (unique) point on the ith line of R and the jth line of C is also on the kth line of S.

An isomorphism of nets is a bijection between their point sets which carries lines to lines. It is clear from the above reconstruction that two nets are isomorphic if and only if the Latin squares used to construct them are main-class equivalent.

The *dual* of an incidence structure is obtained by interchanging the roles of 'point' and 'line' while preserving the relation of incidence. Now the dual of a net is a special type of *transversal design*. The defining conditions are:

(a′) There are $3n$ points and n^2 lines.

(b′) Each line contains 3 points, and each point lies on n lines.

(c′) Two points lie on at most one line.

(d′) The points can be partitioned into three families of n points, such that each line contains one point of each family. Moreover, two points from different families lie on a (unique) line.

The families in (d′) are sometimes called *groups*, though the word does not carry its algebraic sense.

One advantage of this representation is that it translates subsquares, transversals and orthogonal mates of a Latin square into familiar notions of design theory: subdesigns, parallel classes, and resolutions (parallelisms) respectively.

Two such transversal designs are isomorphic if and only if the nets dual to them are isomorphic; so this isomorphism is the same as main-class equivalence of the Latin squares.

The *complete tripartite graph* $K_{n,n,n}$ has $3n$ vertices partitioned into three sets of size n, with any two vertices in different classes being joined by an edge. A collection of triangles in such a graph with the property that every edge is contained in exactly one triangle (a partition of the edge set into triangles) is obviously the same thing as a transversal design of the type just discussed, and the same considerations apply.

5 Strongly regular graphs

Given a Latin square L, we define a graph as follows: the vertices of the graph are the n^2 cells of the Latin square; two vertices are adjacent if they lie in the same row or column or contain the same symbol. In other words, it is the *collinearity graph* of the net associated with the Latin square: the vertices are the points of the net, two vertices adjacent if they are collinear.

Such a graph is called a *Latin square graph*. It is *strongly regular* with parameters $(n^2, 3(n-1), n, 6)$: this means that

- there are n^2 vertices;
- each vertex is joined to $3(n-1)$ others;
- two adjacent vertices have n common neighbours;
- two non-adjacent vertices have 6 common neighbours.

The following result is due to Bruck [1].

Proposition 3 *(a) If $n > 23$, then any strongly regular graph with parameters $(n^2, 3(n-1), n, 6)$ is a Latin square graph.*

(b) If $n > 4$, then any isomorphism of Latin square graphs is induced by a main-class equivalence of the Latin squares.

Here the a graph isomorphism is a bijection between the vertex sets which carries edges to edges and non-edges to non-edges. The proof involves recognising the lines of the net as cliques in the strongly regular graph. Bruck's result is actually more general (it extends to sets of mutually orthogonal Latin squares) and was further generalised by Bose to 'partial geometries'.

A strongly regular graph and its complement form an example of a two-class *association scheme*. The notion of isomorphism of association scheme is more general; in this case, an isomorphism from the graph to its complement is an automorphism of the association scheme. However, counting arguments show that such an isomorphism is possible only if $n = 5$.

6 Orthogonal arrays and codes

A different way to describe a Latin square is to list all n^2 triples (i, j, k), where i, j and k are the row, column and symbol numbers associated with a cell of the square. We can imagine these as written out in an $n^2 \times 3$ array. This array is

- an *orthogonal array* of strength 2 and index 1: given any pair of columns, and any choice of two symbols, there is a unique row where those symbols occur in those columns;
- a 1-error-detecting code: any two rows of the array differ in at least two positions.

It is clear that these two properties of an $n^2 \times 3$ array with entries from an alphabet of size n are equivalent, and an array with these properties arises from a Latin square as described.

Two $v \times k$ arrays over an alphabet A are said to be *equivalent* if one can be obtained from the other by a combination of the following operations:

- applying a permutation f_i of A to the symbols in the ith column, for $i = 1, \ldots, k$;
- applying a permutation to the columns;
- applying a permutation to the rows.

Warning: regarding a Latin square as an $n \times n$ array, the above definition is not the same as any standard equivalence of Latin squares! This notion is particularly appropriate for codes, since column permutations and permutations to the symbols in each column independently generate all the isometries of A^n (where the metric is *Hamming distance*, the distance between two n-tuples being the number of positions where they differ.) It is clear that equivalence in this sense of the orthogonal arrays (or codes) constructed from Latin squares L, L' arises from main-class equivalence of L and L', and only thus.

Finally, the rows of such an array are the positions of n^2 non-attacking rooks on an $n \times n \times n$ board, and conversely. (A rook is allowed to move along a 'line' of the board, keeping two coordinates constant.)

If we allow arbitrary permutations of the board which preserve the $3n$ 'lines', then equivalence of such sets of rooks is the same as main class equivalence of Latin squares. However, we may wish to consider a more restricted version of equivalence (if, say, we are considering other kinds of chess pieces at the same time), in which case the equivalence relation will be finer. The most extreme position is not to allow any non-trivial equivalences at all, in which case each configuration of rooks corresponds to a single Latin square. An intermediate position might, for example, allow Euclidean symmetries of the board: here the equivalence relation on Latin squares would be main class equivalence where each of the three permutations involved in the isotopy is either the identity or the reversal on $\{1, \ldots, n\}$.

7 Edge-colourings

An *edge-colouring* of a graph is an assignment of 'colours' to the edges in such a way that two edges sharing a vertex get different colours. It is clear that the number of colours required cannot be smaller than the maximum valency of a vertex. A consequence of Hall's Marriage Theorem is that, if a graph is bipartite, then this bound is attained. If the graph is regular with valency r, then an edge-colouring with r colours is the same as a 1-factorisation of the graph (provided that the names of the colours are not significant).

The *complete bipartite graph* $K_{n,n}$ has $2n$ vertices partitioned into two sets R and C each of size n, such that every vertex of R is joined to every vertex of C (and these are all the edges). Let $R = \{r_1,\ldots,r_n\}$ and $C = \{c_1,\ldots,c_n\}$. Suppose that the edges are coloured with the set $S = \{s_1,\ldots,s_n\}$ of colours. Then we may form an $n\times n$ array in which the (i, j) entry is k if and only if the colour of the edge $\{r_i,c_j\}$ is s_k. This array is a Latin square. Reversing the construction, any Latin square of order n gives rise to an edge-colouring of $K_{n,n}$ with n colours.

An *isomorphism* of edge-colourings of graphs G,G' is a graph isomorphism from G to G' which maps each colour class in G to a colour class in G'. Now two Latin squares L and L' give rise to isomorphic edge-coloured complete bipartite graphs if and only if L is isotopic to either L' or its transpose $(L')^{(r,c)}$. This is because, in the edge-colouring situation, exchanging rows and columns corresponds to a graph isomorphism, but symbols play a different role. So this relation is coarser than isotopy but finer than main-class equivalence.

8 Sharply transitive permutation sets

A set S of permutations of $\{1,\ldots,n\}$ is *sharply transitive* if, for any $i, j \in \{1,\ldots,n\}$, there is a unique $f \in S$ with $f(i) = j$.

If we identify a permutation f with its *passive form* $(f(1),\ldots, f(n))$, we see that a sharply transitive set is precisely the set of rows of a Latin square.

Two sets S,S' of permutations are isomorphic if S' can be obtained from S by re-labelling the domain: that is, there is a permutation g of $\{1,\ldots,n\}$ such that $S' = \{ghg^{-1} : h \in S\}$. The effect of g on the corresponding Latin square is to apply the permutation g simultaneously to the columns and the symbols: we have

$$h(j) = k \Leftrightarrow (ghg^{-1})(g(j)) = g(k).$$

Note that the order of the rows of the square is unspecified. Thus isomorphism of permutation sets corresponds to a specialisation of isotopy of Latin squares: we are allowed only isotopies of the form (f, g, g) for permutations f and g. This relation is coarser than quasigroup isomorphism (which takes $g = f$) but finer than isotopy.

9 Complete Latin squares

A Latin square is said to be *row-complete* if each ordered pair of distinct symbols occurs exactly once in consecutive positions in the same row. A Latin square is said to be *row-quasi-complete* if each unordered pair of distinct symbols occurs exactly twice in adjacent positions in the same row. Such squares are used in experimental design where there is a spatial or temporal structure on the set of experimental units.

Column-completeness and *column-quasi-completeness* are defined analogously. A Latin square is *complete* if it is both row-complete and column-complete, and is *quasi-complete* if it is both row-quasi-complete and column quasi-complete.

For example, the first square below is complete, while the second is quasi-complete.

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

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

In a row-complete or row-quasi-complete Latin square, row and symbol permutations preserve the completeness property, but column permutations (except for the identity and the left-to-right reversal) do not, in general. So the appropriate concept of equivalence for these squares (regarding the completeness as part of the structure) allows row and symbol permutations but only reversal of columns. Similarly, for a complete or quasi-complete Latin square, we can permute the symbols arbitrarily, but at most reverse rows and/or columns (and we may allow transposition as well). This gives rise to several new notions of equivalence.

10 Conclusion

The most natural equivalence relations associated with Latin squares (equality, isotopy and main class equivalence) are not always the relevant ones for objects 'equivalent' to Latin squares. We have identified three others: isomorphism of quasigroups, of edge-coloured complete bipartite graphs, and of sharply transitive permutation sets (and potentially more, in configurations of non-attacking rooks and in Latin squares with various completeness properties).

We conclude by pointing out that the definition of 'isomorphism' of Latin squares in Chapter II.1 of the *Handbook of Combinatorial Design* [2] agrees with quasigroup isomorphism, but the enumeration of isomorphism classes immediately following is not consistent with this (giving only one class for $n = 3$). The moral is that care is required!

Finally, we remark that much of what is said above extends to sets of mutually orthogonal Latin squares.

References

[1] R. H. Bruck, Finite nets, II: Uniqueness and embedding, *Pacific J. Math* **13** (1963), 421–457.

[2] C. J. Colbourn and J. Dinitz (editors), *CRC Handbook of Combinatorial Design*, CRC Press, Boca Raton, 1996.

[3] B. D. McKay, Latin squares, `http://cs.anu.edu.au/~bdm/data/latin.html`

[4] N. J. A. Sloane (ed.), *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`

R. A. Bailey, Peter J. Cameron

August 1, 2003