Morehead Electronic Journal of Applicable Mathematics
Issue 4 — MATH-2005-03

An introduction to SDR's and Latin squares[1]

Jordan Bell[2]

School of Mathematics and Statistics
Carleton University, Ottawa, Ontario, Canada

Abstract

In this paper we study systems of distinct representatives (SDR's) and Latin squares, considering SDR's especially in their application to constructing Latin squares. We give proofs of several important elementary results for SDR's and Latin squares, in particular Hall's marriage theorem and lower bounds for the number of Latin squares of each order, and state several other results, such as necessary and sufficient conditions for having a common SDR for two families. We consider some of the applications of Latin squares both in pure mathematics, for instance as the multiplication table for quasigroups, and in applications, such as analyzing crops for differences in fertility and susceptibility to insect attack. We also present a brief history of the study of Latin squares and SDR's.

1 Introduction and history

We first give a definition of Latin squares:

Definition 1. *A Latin square is a $n \times n$ array with n distinct entries such that each entry appears exactly once in each row and column.*

Clearly at least one Latin square exists of all orders $n \geq 1$, as it could be made trivially with cyclic permutations of $(1, \ldots, n)$. This is called a circulant matrix of $(1, \ldots, n)$, seen in Figure 1. We discuss nontrivial methods for generating more Latin squares in Section 3.

Euler studied Latin squares in his "36 officers problem" in [7], which had six ranks of officers from six different regiments, and which asked whether it is possible that no row or column duplicate a rank or a regiment; Euler was unable to produce such a square and conjectured that it is impossible for $n = 4k + 2$, and indeed the original case $k = 1$ of this claim was proved by G. Tarry in [13]. However, in general this conjecture

[1]Keywords: Latin squares, systems of distinct representatives, quasigroups, n-queens. AMS 2000 subject classification: 05B15 (Primary), 05A05 (Secondary).

[2]This paper was written during an NSERC USRA supervised by Dr. B. Stevens, at the School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada. The author's email address is jbell3@connect.carleton.ca

is false, which was proved by Bose, Shrikhande and Parker in [2]. Two $n \times n$ Latin squares that when superimposed make a square such that no 2-tuple is repeated are called *mutually orthogonal Latin squares*, and are historically known as a Graeco-Latin square (for combining Greek and Latin characters in a method for making magic squares by Euler, which we discuss in a moment), and also as an Euler square. An example of two 3×3 Latin squares that are mutually orthogonal is found in [8] by Euler, which we give as Figure 2. We note that Figure 2 first has the two mutually orthogonal Latin squares, and then their composition, which is a Graco-Latin square. Following Euler's paper on Latin squares, a significant amount of work has been done in this area, both in applied and pure mathematics, although most of this work is beyond the scope of this paper, which only studies the use of Latin squares in applied and pure mathematics in an elementary way. An excellent and comprehensive survey of Latin squares is by Dénes and Keedwell in the monograph [5], which gives many important but more advanced results.

Latin squares are similar to the well known magic squares, which are arrays where the sum of the entries in each row, column and center diagonal are equal. In fact, Euler gives a method to produce magic squares of arbitrary order in [8] that uses one $n \times n$ Latin square made out of the first n Latin letters a, b, c, etc. and one $n \times n$ Latin square made out of the first n Greek letters α, β, γ, etc. The Latin letters take the values 0, 1, 2, etc. and the Greek letters take the values 1, 2, 3, etc., with all Latin letters pairwise distinct and all Greek letters pairwise distinct. The two squares are then superimposed on each other on each other such that no 2-tuples are repeated (i.e. mutually orthogonal Latin square), and each square takes the value $an + \alpha$, where a is the Latin letter on the square, and α is the Greek letter on the square. I have a translation of this paper from the Latin in [9].

The study of magic squares themselves is *very* old, and Figure 3, known as the *Lo Shu*, seems to have been studied in China as far back as 2100

Figure 1: Latin square generated by cyclic permutations of $(1, \ldots, n)$

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ n & 1 & 2 & \ldots & n-1 \\ n-1 & n & 1 & \ldots & n-2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2 & 3 & 4 & \ldots & 1 \end{pmatrix}$$

Figure 2: Two mutually orthogonal Latin squares and their composition

$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}, \begin{pmatrix} \gamma & \beta & \alpha \\ \alpha & \gamma & \beta \\ \beta & \alpha & \gamma \end{pmatrix}, \begin{pmatrix} a\gamma & b\beta & c\alpha \\ b\alpha & c\gamma & a\beta \\ c\beta & a\alpha & b\gamma \end{pmatrix}$$

BCE, according to R. Cooke in [4].

Figure 3: Magic square from China, around 2100 BCE

2	9	4
7	5	3
6	1	8

Latin squares are very interesting from a pure math view (e.g. their relation to quasigroups), but there are several practical applications for them. For example, P. J. Cameron in [3] mentions that they are used in statistical design for analyzing crops of different fertility and susceptibility to insect attack. Using Latin squares allows us to perform analysis of variance: we can isolate one particular variable by having lines of crops that are different in everything except that variable. There is an excellent explanation of this by H. Steinhaus in [12].

In the next section we introduce systems of distinct representatives (SDR's), as they have applications for constructing Latin squares, and are very interesting and useful themselves. The fundamental theorem for systems of distinct representatives is Hall's marriage theorem (which we give as Theorem 3 in this paper), by P. Hall, and we discuss this more in Section 2. Historically this is called Hall's marriage theorem because it relates to matching boys to girls for marriage. Both the study of Latin squares and SDR's have applications to the n-queens problem, and we discuss these relations in Section 4.

2 Systems of distinct representatives

First we give a definition for SDR's.

Definition 2. *Let us have a family $\mathscr{A} = \{A_1, \ldots, A_n\}$ of subsets of a set S. A set $X = \{x_1, \ldots, x_n\}$ is a system of distinct representatives (SDR) for $\mathscr{A}$ if for $i \neq j$ it holds that $x_i \neq x_j$, with each $x_i \in A_i$.*

Clearly if we have a family $\mathscr{A}$ and an SDR X for this family, the union of any k sets in $\mathscr{A}$ must have at least k distinct elements in it, because each set A_i has a distinct $x_i \in X$ that represents it. A useful theorem of Hall shows that the converse of this is also true, that if the union of any k sets of a family $\mathscr{A}$ has at least k distinct elements in it (which is known as Hall's condition (1)), an SDR exists for this family. We give a proof of Hall's marriage theorem from Cameron in [3]. There are many proofs for this theorem, from basic counting arguments to graph theory, and this proof is done by counting. We introduce the notation that for $J \subseteq \{1, \ldots, n\}$, $A(J) = \cup_{j \in J} A_j$.

Theorem 3. *Let us have a family $\mathscr{A} = \{A_1, \ldots, A_n\}$ of subsets of a set S. There exists a system of distinct representatives $X = \{x_1, \ldots, x_n\}$ for $\mathscr{A}$ if and only if (1) holds:*

$$\forall J \subseteq \{1, \ldots, n\}, |A(J)| \geq |J|. \tag{1}$$

Proof. As we have already noted, if there is an SDR X such that $|X| = n$ for a family of n sets, there must be at least n elements in the union of these sets, because for $x_i \in X$ then it also must be that $x_i \in A_i$.

We say that a J is critical if $|A(J)| = |J|$, and this implies that every element in the union of sets that J indexes must be used as a representative for some set. We procede by induction on the size n of the family $\mathscr{A}$ of sets. For $n = 1$, we have $\mathscr{A} = \{A_1\}$, for which if $|J| = 0$, then of course the union of 0 sets in $\mathscr{A}$ has at least 0 elements, and if $|J| = 1$, then by assumption $|A(J)| \geq 1$, so there is at least one element in the "union" of the one set A_1 in $\mathscr{A}$, which can be the $x_i \in X$, so there is an SDR for $\mathscr{A}$. We make the induction assumption assumption that for $|\mathscr{A}| = k$ such that $k < n$, there is an SDR for $\mathscr{A}$ whenever (1) holds.

We procede in two cases. Case 1 is where we have an $\mathscr{A}$ such that no J is critical except for possibly $J = \{1, \ldots, n\}$ and (of course) $J = \emptyset$. Let us choose some $a \in A_n$, and set $A'_i = A_i \backslash a$ for all $1 \leq i < n$. Let us have $J \subseteq \{1, \ldots, n-1\}$. Clearly $|A'(J)| \geq |A(J)| - 1$, because at most one element was taken away from $A'(J)$. Then we have $|A'(J)| > |J| - 1$, as J is not critical, and so $|A'(J)| \geq |J|$, and so by our induction assumption there exists an SDR for $\{A'_1, \ldots, A'_{n-1}\}$. Since a is not in any of these sets, we can have $x_n = a$ as a representative for A_n, and have $X = \{x_1, \ldots, x_n\}$ as an SDR for $\mathscr{A}$.

In Case 2 is where we have an $\mathscr{A}$ such that some $J \subseteq \{1, \ldots, n\}$ such that $J \neq \emptyset$, $J \neq \{1, \ldots, n\}$ is critical, and we assume J minimal. Let us have $K = \{1, \ldots, n\} \backslash J$, and for all $k \in K$, $A'_k = A_k \backslash A(J)$; that is, we remove all the elements in $A(J)$ from each of the remaining sets. Clearly $|A'(K)| = |A(J \cup K)| - |A(J)|$, as each A'_k is disjoint from each A_j. Thus $|A'(K)| \geq |J \cup K| - |A(J)|$ by assumption. Since J is critical, we have $|A'(K)| \geq |J \cup K| - |J|$, and since J and K are disjoint, we have $|A'(K)| \geq |K|$. Thus by assumption there is an SDR for the family of A'_k indexed by K, and since we set this family to be disjoint from $A(J)$, this SDR is disjoint from every SDR for the family of sets indexed by J, because the SDR for the family of sets indexed by J is a subset of $A(J)$, the union of the sets indexed by J. Furthermore, the SDR for the family of sets indexed by J exists by assumption. Thus we can combine these SDR's to be an SDR for $\mathscr{A}$. This completes our induction. □

We find that Corollary 4 can be derived from Theorem 3.

Corollary 4. *Let us have a set S and a family $\mathscr{A} = \{A_1, \ldots, A_n\}$ of subsets of S. If we have an SDR for some $n-1$ sets in $\mathscr{A}$, we can extend (i.e. add an entry to) this SDR to be an SDR for the entire family if (1) holds.*

We now give a theorem from Cameron in [3] on the number of different SDR's for some family. The proof is done with a simple extension of our proof of Theorem 3, and the only difference is that it it includes counting the number of different ways to make SDR's (in fact, Theorem 3 can be seen as a specific case of Theorem 5, for $r = 1$).

Theorem 5. *Let us have that $\mathscr{A} = \{A_1, \ldots, A_n\}$ is a family of subsets of a set S such that for all $J \subseteq \{1, \ldots, n\}$, we have $|A(J)| \geq |J|$. As well,*

let us have that for all $i \in \{1, \ldots, n\}$, $|A_i| \geq r$. The minimum number of different SDR's for $\mathscr{A}$ is $r!$ if $r \leq n$ and $r(r-1)\ldots(r-n+1)$ if $r > n$.

Proof. This proof uses our work from the proof of Theorem 3, with our induction assumption modified from $r = 1$ in the original proof to this theorem's general r. We procede by the two cases from our earlier proof. For Case 1, by assumption $|A_n| \geq r$, so we have at least r choices for x_n of the SDR for $\mathscr{A}$. Now for each $1 \leq 1 \leq n-1$ we set $A_i' = A_i \backslash x_n$. But now by the induction assumption we have that there are $(r-1)!$ SDR's for this family if $r \leq n$ and $(r-1)\ldots(r-n+1)$ if $r > n$. Clearly these SDR's are disjoint from the x_n, and by the multiplication principle we have respectively $r(r-1)\ldots(r-n+1)$ or $r!$ different SDR's for $\mathscr{A}$.

In Case 2, some set of indices J of subsets of $\mathscr{A}$ is critical, which we assume to be minimal. By assumption $J \neq \{1, \ldots, n\}$, and since J criticial it follows that $r \leq n$, and thus by our induction assumption for $|J| \leq n-1$ we have that there are $r!$ SDR's for the family of sets indexed by J. However, Corollary 4 then implies that this SDR for the family of sets indexed by J can be extended to be an SDR for $\mathscr{A}$. □

We often want to form a set that is simultaneously an SDR for more than one family, and we call this a system of common distinct representatives. We give the following definition:

Definition 6. *Let us have a set S and families $\mathscr{A} = \{A_1, \ldots, A_n\}, \mathscr{B} = \{B_1, \ldots, B_n\}$ of subsets of S. We call $X = \{x_1, \ldots, x_n\}$ a system of common distinct representatives for $\mathscr{A}$ and $\mathscr{B}$ if for $i \neq j$ it holds that $x_i \neq x_j$, we have that each $x_i \in A_i$, and for some permutation ϕ of $\{1, \ldots, n\}$, $x_i \in B_{\phi(i)}$.*

We now give a theorem of Ford and Fulkerson, from chapter II, section 10 of their monograph [10]. This theorem gives necessary and sufficient conditions for the existence of a system of common distinct representatives for two families of the same cardinality. Ford and Fulkerson's proof is based on defining a certain network based on the members of the two families, and considering whether it admits a feasible circulation. We use the same notation here as from our proof of Theorem 3.

Theorem 7. *For two families $\mathscr{A} = \{A_1, \ldots, A_n\}$ and $\mathscr{B} = \{B_1, \ldots, B_n\}$ of subsets of a set S, there exists a system of common distinct representatives for them if and only if the following holds for all $I, J \subseteq \{1, \ldots, n\}$:*

$$|A(I) \cap B(J)| \geq |I| + |J| - n$$

I am not aware (and have not been able to find even after much searching!) any results for more than two families, and it has been suggested to me (personal communication) that this may be an NP-complete problem; however, I am not aware of any proof about this either.

3 Latin squares

SDR's can be used to construct Latin squares in the following way, for which we immediately after give a proof. Let us have a family $\mathscr{A} =$

$\{A_1, \ldots, A_n\}$ of subsets of $\{1, \ldots, n\}$ with each $A_i = \{1, \ldots, n\}$. It follows from these assumptions that we can make exactly $n!$ SDR's X for $\mathscr{A}$. Thus we give the following theorem, which uses SDR's to construct a Latin square. We first note though that a Latin rectangle is an $m \times n$ array of entries from $\{1, \ldots, n\}$ such that every entry appears in each row, and each entry appears at most once in each column.

Theorem 8. *Let us have an $m \times n$ Latin rectangle. There are at least $(n-m)!$ ways to add a row to it to form an $(m+1) \times n$ Latin rectangle.*

Proof. Let us represent the complement of the entries in the i-th column of the given Latin rectangle as A_i. Adding a row to this Latin rectangle is equivalent to finding an SDR for $\mathscr{A} = \{A_1, \ldots, A_n\}$. Clearly for all i, $|A_i| = n - m$. Let us have $r = n - m$. As well, it is clear that for some $a \in \{1, \ldots, n\}$ there are precisely r columns that do not contain a. This satisfies (1) and also each each column has r distinct elements in it, so by Theorem 5 (with $r \leq n$) there are $r! = (m-n)!$ ways to add a row to make an $(m+1) \times n$ Latin rectangle. □

3.1 Latin squares and quasigroups

A quasigroup S is a very simple groupoid (algebraic structure) such that for all $a, b \in S$, there exist a unique i and j such that $ai = b$ and $ja = b$. In general, quasigroups do not have any other algebraic properties, such as associativity, commutativity, distributivity, having an identity element etc. We can show that a quasigroup is precisely a groupoid such that its multiplication table is a Latin square; by multiplication table we mean the first row is $(a_1a_1, a_1a_2, \ldots, a_1a_n)$, the second row is $(a_2a_1, a_2a_2, \ldots, a_2a_n)$, etc.

Let us have a quasigroup G, with some operation $*$ defined on a set of size n, i.e. $G = \{g_1, \ldots, g_n\}$. We can show that a groupoid G is a quasigroup if and only if its associated $n \times n$ multiplication table A is a Latin square. In our following discussion, we use ab, ai etc.to denote $a * b$, $a * i$ etc.

Theorem 9. *A groupoid $G = \{g_1, \ldots, g_n\}$ is a quasigroup if and only if its multiplication table A is a Latin square.*

Proof. Let us have an $n \times n$ Latin square $A = (a_ij)$, where we number the rows $1, \ldots, n$ from the top to the bottom, and the columns $1, \ldots, n$ from the left to the right. We define $ij = a_{ij}$. Since A is a Latin square, clearly for each choice of row $\alpha \in \{1, \ldots, n\}$ and entry in that row $\beta \in \{1, \ldots, n\}$, there is a unique column $i \in \{1, \ldots, n\}$ such that $\alpha i = \beta$. Similarly, considering α as column number, there is a unique row j such that $j\alpha = \beta$.

Now let us have a quasigroup G with n elements. For each pair g_i and g_j of elements from G, we have two unique elements in G g_k and g_l such that $g_ig_k = g_j$ and $g_lg_i = g_j$. We note that $i, j, k, l \in \{1, \ldots, n\}$. We have that for each i and j there is a unique k such that $ik = j$, and a unique l such that $li = j$. This is equivalent to saying that for each row and column there exists a unique entry at which they pass through each other. So we can construct a Latin square from G by having $g_ig_k = g_j$ if and only if $a_{ij} = k$. □

4 Applications to n-queens

SDR's and Latin squares have applications to the study of the n-queens problem, that of placing n nonattacking queens on an $n \times n$ chessboard. Also, they can be used for placing n nonattacking rooks on the $n \times n$ board, because it is clear that placing a rook on every α of an $n \times n$ Latin square for $\alpha \in \{1, \ldots, n\}$ gives a nonattacking configuration; in fact, Latin squares can always be used to simultaneously place n sets of n rooks each, such that within each set there are no pairwise attacks. One extension of the n-queens problem is to place n^2 queens on the n cube, which can be represented as forming an $n \times n$ Latin square such that for two entries $(i, j) = a$ and $(k, l) = b$ (with i the number of rows down and j the number of columns to the right), $|i - k| \neq |b - a|$ and $|j - l| \neq |b - a|$.

Clearly a Latin square representation of n^2 nonattacking queens on the n cube must be a *pandiagonal Latin square*, where each extended sum and difference diagonal contains n distinct entries. Atkin, Hay and Larson in a larger work on pandiagonal Latin squares [1], discuss the use of Latin squares to find solutions for the modular board. In particular they give the known result that there are solutions to the $n \times n$ modular board when n is prime and $n \geq 13$ (which is weaker than D.A. Klarner's result in [11] that for all n such that $\gcd(n, 210) = 1$ there exists a solution for the n cube).

We can see that a 4-tuple of a row, column, sum diagonal and difference diagonal that agree with each other (i.e. all share a common point) places a queen on the $n \times n$ board, and n disjoint such 4-tuples is equivalent to a solution for the n-queens problem. Thus if we could establish sufficient conditions for forming a system of common distinct representatives for four families (rows, columns, sum diagonals and difference diagonals), we might be able to apply this as a solution for n-queens, by forming n such SDR's.

Latin squares also apply to the n-queens problem in the use of circulant matrices as a solution. A solution by Erbas and Tanik to the n-queens problem in [6] creates two Latin rectangles from 2-circulants, and combines these to form a Latin square, placing queens on each square holding a 2.

References

[1] A. O. L. Atkin, L. Hay, and R. G. Larson, *Enumeration and construction of pandiagonal Latin squares of prime order*, Comput. Math. Appl. **9** (1983), no. 2, 267–292. MR 85i:05048

[2] R. C. Bose, S. S. Shrikhande, and E. T. Parker, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Canad. J. Math. **12** (1960), 189–203. MR 23 #A69

[3] Peter J. Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, Cambridge, 1994. MR 95j:05002

[4] Roger Cooke, *The history of mathematics: a brief course*, Wiley-Interscience, 1997.

[5] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, New York, 1974. MR 50 #4338

[6] Cengiz Erbas and Murat M. Tanik, *Generating solutions to the N-queens problem using* 2*-circulants*, Math. Mag. **68** (1995), no. 5, 343–356. MR 96m:05050

[7] Leonhard Euler, *Recerches sur une nouvelle espèce de quarrés magiques*, Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen **9** (1782), 85–239.

[8] ———, *De quadratis magicis*, Opera omnia, vol. 7, series 1, Teubner, Leipzig, 1911, pp. 441–457.

[9] ———, *On magic squares*, arXiv math.CO/0408230, October 2004, Translated from the Latin by Jordan Bell.

[10] L. R. Ford, Jr. and D. R. Fulkerson, *Flows in networks*, Princeton University Press, Princeton, N.J., 1962. MR MR0159700 (28 #2917)

[11] David A. Klarner, *Queen squares*, J. Recreational Math. **12** (1979/80), no. 3, 177–178. MR 81m:05035

[12] H. Steinhaus, *Mathematical snapshots*, third american ed., ch. 1, pp. 31–33, Oxford University Press, Oxford, 1969.

[13] Gaston Tarry, *Le probléme de 36 officiers*, Comptes Rendus Assoc. Franc. Avance. Sci. **2** (1901), 170–203.