Reprinted from JOURNAL OF COMBINATORIAL THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 20, No. 3, May 1976
Printed in Belgium

The Number of Distinct Latin Squares as a Group-Theoretical Constant

A.-A.A. JUCYS

Institute of Physics and Mathematics of the Academy of Sciences of Lithuanian SSR, 232600 Vilnius, Lithuanian SSR, USSR

Communicated by the Managing Editors

Received July 8, 1974

It is shown that the number l_n of all distinct Latin squares of the nth order appears as a structure constant of the algebra defined on the Magic squares of the same order. The algebra is isomorphic to the algebra of double cosets of the symmetric group of degree n^2 with respect to the intransitive subgroup of all substitutions in the n sets of transitivity, each set being of cardinality n. The representation theory makes it possible then to express l_n in terms of eigenvalues of a certain element of the algebra.

1. INTRODUCTION

The Latin square of the nth order is usually defined [1] as an arrangement in the square table of n distinct symbols subject to conditions that each symbol appears in each row and in each column exactly once. A more convenient definition used in this paper is in terms of zero–one cubic matrices. Such a matrix $\| a_{ijk} \|$ of the nth order represents a Latin square of the same order if

$$\sum_{i=1}^{n} a_{ijk} = \sum_{j=1}^{n} a_{ijk} = \sum_{k=1}^{n} a_{ijk} = 1. \tag{1}$$

And conversely, each Latin square can be represented by the matrix, obeying (1). The one-to-one correspondence between the two sets can be stated by the rule: $a_{ijk} = 1$ if and only if there is the kth symbol placed in the intersection of the ith row and jth column of the corresponding Latin square, otherwise $a_{ijk} = 0$.

There is a well-known algebraic interpretation of the Latin squares: each of them defines the quasi-group. The object of the present note is to reveal an algebraic significance of the Latin squares of a different origin.

In Section 2 it is shown that to obtain one of the structure constants of the algebra defined herein one must count the Latin squares of the given order. The combinatorial problem of enumeration of the Latin squares survived in all Harary's lists [2] of unsolved enumerational problems of the graph theory. The natural generalization of this problem can be suggested: to find all the structure constants of the algebra under discussion. On the other hand, the more general algebras of the same type could be defined and considered. This is, however, a separate theme and will not be discussed here.

In Section 3 the expression is given for the number of distinct Latin squares (i.e., for the corresponding structure constant) in terms of eigenvalues of a certain element of the algebra. At the present stage the expression cannot be regarded as a counting formula because the author has not succeeded in obtaining compact formulas for the eigenvalues. However, it is not obvious that such formulas do not exist.

References [11–15] are devoted to the obtaining of the numbers of the Latin squares and their equivalence classes up to and including the eight order by direct methods.

2. An Algebra on Magic Squares

Let $m = \| m_{ij} \|$ be a square matrix of the order n whose elements are natural numbers (including zero). If all the row and column sums of the matrix are equal, it is called a Magic square of the nth order. In what follows we shall be concerned with the set M of Magic squares having row and column sums equal to the order of the square. That is, $m \in M$ if and only if

$$\sum_{i=1}^{n} m_{ij} = \sum_{j=1}^{n} m_{ij} = n. \tag{2}$$

Let the algebra A_n over the field C of complex numbers, with the set M as the basis of this algebra, be defined by the following multiplication rule. If $r, s \in M$, then

$$rs = \sum_{t \in M} \gamma_{rst} t, \tag{3}$$

where structure constant γ_{rst} is defined by

$$\gamma_{rst} = \sum \left(\prod_{i,k=1}^{n} t_{ik}! \Big/ \prod_{i,j,k=1}^{n} a_{ijk}! \right). \tag{4}$$

Here the summation is taken with respect to all the cubic matrices $\| a_{ijk} \|$ of the order n whose elements are natural numbers satisfying the equations

$$\sum_{k=1}^{n} a_{ijk} = r_{ij}\,, \tag{4a}$$

$$\sum_{i=1}^{n} a_{ijk} = s_{jk}\,, \tag{4b}$$

$$\sum_{j=1}^{n} a_{ijk} = t_{ik}\,. \tag{4c}$$

There exists the element $e \in M$ such that

$$e_{ij} = 1 \tag{5}$$

for each i and each j. From (1), (4), and (5) it follows immediately that the structure constant γ_{eee} of A_n is equal to the number l_n of distinct Latin squares of the nth order.

To reveal the structure and properties of the algebra A_n as well as those of representations of A_n, we shall show that A_n is isomorphic to the certain subalgebra of the symmetric group algebra. For this let us consider the symmetric group $S(n^2)$ of all permutations of the set S of cardinality $| S | = n^2$. Let $P = \{X_1, X_2, \ldots, X_n\}$ be the partition of S such that

$$\forall_{X_i, X_j} [X_i \subset S, | X_i | = n, X_i \cap X_j = \delta_{ij} X_i] \tag{6}$$

($\delta_{ij} X_i$ equals X_i if $i = j$ and is the empty set if $i \neq j$). Denote by $S^n(n)$ the subgroup of $S(n^2)$:

$$S^n(n) = \left\{ \sigma \in S(n^2) \cdot \forall_{X_i \in P} \forall_{b \in X_i} [\sigma(b) \in X_i] \right\}. \tag{7}$$

Clearly, $S^n(n)$ is the direct product of n symmetric groups of separate permutations of n subsets $X_i \in P$. The set

$$m = \bigcup_{\tau, \tau' \in S^n(n)} \tau \circ \sigma \circ \tau', \qquad \sigma \in S(n^2), \tag{8}$$

is called the double coset [3] of the group $S(n^2)$ with respect to the subgroup $S^n(n)$. From (6)–(8) it follows that the double coset (8) can also be defined by

$$m = \left\{ \rho \in S(n^2) \colon \forall_{X_i, X_j \in P} \left[\left| X_i \cap \left(\bigcup_{b \in X_j} \rho(b) \right) \right| = m_{ij} \right] \right\}, \tag{9}$$

where the matrix $\| m_{ij} \|$ is one of the Magic squares of the nth order. Indeed, because of the left and the right group-multiplication in (8) by permutations from $S^n(n)$, there is no need to indicate which elements of X_i are substituted for the elements of X_j and which are the last ones in order to decide to which double coset a given permutation $\rho \in S(n^2)$ belongs. It is sufficient only to indicate the number m_{ij} of the elements. Thus, the one-to-one correspondence between the two sets (the set M and the set of double cosets) is stated, and so it is reasonable to use the same notation for both the sets.

Let $\sigma_r \in r$, $\sigma_s \in s$, $\sigma_t \in t$ $(r, s, t \in M)$ and

$$\sigma_r \circ \sigma_s = \sigma_t \, ; \tag{10}$$

let

$$S_{ijk} = X_i \cap \Bigl(\bigcup_{b \in Q} \sigma_r(b) \Bigr), \qquad \text{where} \quad Q = X_j \cap \Bigl(\bigcup_{c \in X_k} \sigma_s(c) \Bigr) \tag{11}$$

and

$$a_{ijk} = | S_{ijk} | \tag{12}$$

From (9)–(12) it follows that the matrix $\| a_{ijk} \|$ satisfies equations (4a)–(4c). Now we ask: What is the number of different pairs $\langle \sigma_r , \sigma_s \rangle$ of permutations $\sigma_r \in r$, $\sigma_s \in s$ characterized according to (11) and (12) by the same matrix $\| a_{ijk} \|$ and their product giving the same permutation $\sigma_t \in t$? There are $\prod_{i,k=1}^{n} t_{ik} ! / \prod_{i,j,k=1}^{n} a_{ijk}$! possibilities (depending upon $\langle \sigma_r , \sigma_s \rangle$) for the sets S_{ijk} $(i, j, k = 1, 2,..., n)$ to be. Moreover, there are $(n!)^n$ of pairs of interest $\langle \sigma_r \circ \tau^{-1}, \tau \circ \sigma_s \rangle$ having the same sets S_{ijk} and differing by the permutations $\tau \in S^n(n)$. Thus the number of pairs in question is

$$(n!)^n \Bigl(\prod_{i,k=1}^{n} t_{ik}! \Big/ \prod_{i,j,k=1}^{n} a_{ijk}! \Bigr). \tag{13}$$

From this it follows that the set $\{m^\sigma \colon m \in M\}$ of elements

$$m^\sigma = (1/(n!)^n) \sum_{\sigma \in m} \sigma, \qquad m \in M, \tag{14}$$

of the group algebra $A_{S(n^2)}$ of $S(n^2)$ (over C) is the basis of the subalgebra $A_n{}^\sigma$, isomorphic to A_n. Indeed, from (10)–(14) we obtain

$$r^\sigma \circ s^\sigma = \sum_{t \in M} \gamma_{rst} t^\sigma \tag{15}$$

with γ_{rst} obeying (4)–(4c). In the isomorphism $A_n{}^\sigma \leftrightarrow A_n$:

$$m^\sigma \leftrightarrow m.$$

Thus the number l_n of the Latin squares of the nth order appears naturally in the symmetric group theory. The last one being comparatively well developed [4, 5], one can hope to obtain some results on l_n. Before proceeding to the discussion of this subject, we shall show that there is a subalgebra of A_n in which l_n appears in the same way as in A_n.

For this let us consider the symmetric group $S(n)$ of all the permutations of the set $P = \{X_1, X_2, ..., X_n\}$. We find immediately that for any $\rho \in S(n)$

$$\rho \circ e^{\sigma} = e^{\sigma} \circ \rho = e^{\sigma}. \tag{16}$$

The set of permutations $\rho \circ \tau$, where $\rho \in S(n)$, $\tau \in S^n(n)$ constitutes one of the Kranz groups (so named after Pólya [6]; see also [7, 8, 9]) for which the notation $S(n)[S(n)]$ can be used. Because $S^n(n)$ is the subgroup of $S(n)[S(n)]$, the set M' of double cosets of $S(n^2)$ with respect to the subgroup $S(n)[S(n)]$ gives some partition of the set M. Thus the set $\{(m^{\sigma})' \colon m' \in M'\}$

$$(m^{\sigma})' = (1/(n!)^n) \sum_{\sigma \in m'} \sigma, \qquad m' \in M', \tag{17}$$

is the basis of some subalgebra $(A_n{}^{\sigma})'$ of $A_n{}^{\sigma}$. From (16) it follows that

$$(e^{\sigma})' = e^{\sigma}. \tag{18}$$

Denoting the structure constant of $(A_n{}^{\sigma})'$ by $\gamma'_{s'r't'}$ we have

$$\gamma'_{e'e'e'} = \gamma_{eee} = l_n . \tag{19}$$

3. Expression of l_n in Terms of Eigenvalues of e

If

$$a = \sum_{\sigma \in S(n^2)} a(\sigma)\sigma \qquad \left(\forall_{\sigma \in S(n^2)} [a(\sigma) \in C] \right),$$

then let us denote by $\hat{a}$ the element of $A_{S(n^2)}$:

$$\hat{a} = \sum_{\sigma \in S(n^2)} a(\sigma)\, \sigma^{-1},$$

where σ^{-1} is the inverse of σ. We have

$$\hat{e}^{\sigma} = e^{\sigma}. \tag{20}$$

Indeed, let $X_i = \{x_{i1}, x_{i2}, ..., x_{in}\}$ $(X_i \in P)$. As a representative of double coset e we can choose the permutation

$$\sigma_e = \prod_{i>k=1}^{n}{}^{0} (x_{ik} x_{ki}) = \sigma_e^{-1}, \tag{21}$$

where $(x_{ik}x_{ki})$ is the transposition of the two elements and $\prod^0$ denotes the product with respect to the group composition. Now substituting σ_e for σ in (8) and replacing the permutations by their inverses, we obtain (20).

It is well known [3] that there exists a unitary basis for any irreducible representation λ of a finite group over C. Because of (20), in such a basis e^σ would be represented by the hermitian matrix. Thus the basis $B_\lambda = \{b_1, b_2, ..., b_{f(\lambda)}\}$ of the irreducible representation λ of dimension $f(\lambda)$ of $S(n^2)$ (and thereby of $A_{S(n^2)}$) in which e^σ is represented by the real diagonal matrix $\| E_{ik}^\lambda \delta_{ik} = E_i^\lambda \|$ can be found. Moreover, because of

$$\rho' \circ e^\sigma = e^\sigma \circ \rho' = e^\sigma \tag{22}$$

for any $\rho' \in S(n)[S(n)]$ (see (17), (18)), B_λ can be presumed to be the basis of the representation of $S(n^2)$ reduced with respect to the subgroup $S(n)[S(n)]$. Let

$$O_i^\lambda = (f(\lambda)/n^2!) \sum_{\sigma \in S(n^2)} u_{ii}^\lambda(\sigma)\sigma^{-1} \tag{23}$$

be the primitive idempotents of the group algebra corresponding to the representation ($u_{ii}^\lambda(\sigma)$ are diagonal elements of the matrix representing σ). Now again because of (22), in the expansion

$$e^\sigma = \sum_\lambda \sum_{i=1}^{f(\lambda)} E_i^\lambda O_i^\lambda \tag{24}$$

E_i^λ vanish for all subscripts, except those corresponding to the basic elements $b_i \in B_\lambda$ obeying

$$\rho' b_i = b_i \tag{25}$$

for any $\rho' \in S(n)[S(n)]$. To find the number $p(\lambda)$ of such elements in B_λ one must search for the number of appearances of the trivial representation (25) of $S(n)[S(n)]$ in the irreducible representation λ of $S(n^2)$. By the Frobenius reciprocity law, the numbers $p(\lambda)$ appear as the coefficients in the reduction of the symmetrized outer product of the symmetric group representations [4, p. 66; 8; 9]:

$$[n] \odot [n] = \sum_\lambda p(\lambda)[\lambda], \tag{26}$$

where $[n]$ is the trivial representation of the symmetric group of degree n and $[\lambda]$ is an arbitrary one. Thus, letting the first $p(\lambda)$ subscripts correspond to the trivial representation of $S(n)[S(n)]$, we write

$$e^\sigma = \sum_\lambda \sum_{i=1}^{p(\lambda)} E_i^\lambda O_i^\lambda. \tag{27}$$

Now it follows (i) from the definition of e^σ, (ii) from (20), (iii) from (3), (19) and (20) that the coefficient of the unit element of the group, correspondingly,

$$\begin{aligned} &\text{(i)} \quad \text{in } e^\sigma \text{ is } 0, \\ &\text{(ii)} \quad \text{in } e^\sigma \circ e^\sigma \text{ is } 1, \\ &\text{(iii)} \quad \text{in } e^\sigma \circ e^\sigma \circ e^\sigma \text{ is } l_n. \end{aligned} \tag{28}$$

Because of orthogonality of the idempotents $(O_i^\lambda \circ O_{i'}^{\lambda'} = \delta_{\lambda\lambda'}\delta_{ii'}O_i^\lambda)$, from (23), (27), and (28) by comparing the coefficients of the unit element on both sides of the three corresponding equations we find that

$$(1/n^2!) \sum_\lambda f(\lambda) \sum_{i=1}^{p(\lambda)} E_i^\lambda = 0, \tag{29}$$

$$(1/n^2!) \sum_\lambda f(\lambda) \sum_{i=1}^{p(\lambda)} (E_i^\lambda)^2 = 1, \tag{30}$$

$$(1/n^2!) \sum_\lambda f(\lambda) \sum_{i=1}^{p(\lambda)} (E_i^\lambda)^3 = l_n . \tag{31}$$

To obtain these equations was the aim of this section. The following equation is useful for checking the expansions (26):

$$(1/n^2!) \sum_\lambda f(\lambda)\, p(\lambda) = 1/(n!)^{n+1}, \tag{32}$$

and is obtained by setting $m = n$ and $[\mu] = [\nu] = [n]$ in [4, Eq. (3.511), p. 66]. Formulas for the dimensions $f(\lambda)$ are known [4, 5].

We conclude with some remarks. It seems to us that for obtaining the general formulas for the eigenvalues E_i^λ to be substituted in (31), some further developments of Young's substitutional analysis [5] are needed. For the very special simple cases when $p(\lambda) = 1$, the character theory [4, 10] can be used to obtain the eigenvalues, which in the case of $n = 3$ are (all needed to calculate l_3)

$$E_1^{[9]} = 2^3 \cdot 3^3, \qquad E_1^{[7,2]} = -2^3 \cdot 3^2, \qquad E_1^{[6,3]} = 2^4 \cdot 3,$$
$$E_1^{[5,2,2]} = 2^2 \cdot 3, \qquad E_1^{[4,4,1]} = -2^3 \cdot 3.$$

To see what form the eigenvalues E_i^λ for arbitrary n take, again characters were used and it was found that (in these cases also, $p(\lambda) = 1$)

$$E_1^{[n^2,0]} = (n!)^n, \qquad E_1^{[n^2-2,2]} = -\frac{(n!)^n}{n}, \qquad E_1^{[n^2-3,3]} = 2\frac{(n!)^n}{n^2}.$$

These seem to be sufficiently simple. So we are expressing the hope of further developments on indicated lines or related ones, i.e., of investigations of the algebra A_n with or without an explicit implication of the symmetric group representation theory.

Note added in proof. The author would like to thank the referee for drawing his attention to a recent paper by R. Alter (*Amer. Math. Monthly* **82** (1975), 632). The reader can find there an account of the present stage of actual Latin square enumerations, including the recent result by S. E. Bammel and J. Rothstein (*J. Discrete Math.* **11** (1975), 93) on the enumeration of ninth-order Latin squares. Further references are also found there.

References

1. M. Hall, "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
2. F. Harary, "Graph Theory," Addison–Wesley, Reading, Mass., 1969.
3. Ch. W. Curtis and J. Reiner, "Representation Theory of Finite Groups and Associative Algebras," Wiley, New York, 1962.
4. G. de B. Robinson, "Representation Theory of the Symmetric Group," Edinburgh University Press, Edinburgh, 1961.
5. D. E. Rutherford, "Substitutional Analysis," Hafner, New York, 1968.
6. G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen, *Acta Math.* **68** (1937), 145–254.
7. A. Kerber, Zur Darstellungstheorie von Kranzprodukten, *Canad. J. Math.* **20** (1968), 665–672.
8. D. E. Littlewood, The characters and representations of imprimitive groups, *Proc. London Math. Soc.* (*3*) **6** (1956), 251–266.
9. A. Kerber, Zur Darstellungstheorie von Symmetrien symmetrischer Gruppen, *Mitt. Math. Sem. Giessen* **80** (1969), 1–27.
10. D. E. Littlewood, "The Theory of Group Characters," Clarendon Press, Oxford, 1958.
11. R. A. Fisher and F. Yates, The 6 × 6 Latin squares, *Proc. Cambridge Philos. Soc.* **30** (1933–1934), 492–507.
12. N. W. Norton, The 7 × 7 squares, *Ann. Eug.* **9** (1939), 269–307.
13. A. Sade, An omission in Norton's list of 7 × 7 squares, *Ann. Math. Statist.* **22** (1951), 306–307.
14. M. B. Wells, The number of Latin squares of order eight, *J. Combinatorial Theory* **3** (1967), 98–99.
15. J. W. Brown, Enumeration of Latin squares with application to order eight, *J. Combinatorial Theory* **5** (1968), 177–184.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.