JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 65, No. 1, January–March 1961

Some Computational Problems Involving Integral Matrices[1]

Olga Taussky[2]

(November 28, 1960)

In this mainly expository article dealing particularly with recent problems, a computational problem of G. Pall related to finite projective geometries is discussed in greater detail. Numerical results obtained on SEAC and SWAC are discussed.

1. Introduction

All computation on a machine with a fixed number of digits is arithmetic modulo some integer and therefore can be regarded as number theory. From this fact, in "analytic" problems there arise all the difficulties associated with "round-off," i.e., neglect of insignificant digits. However, there are often considerable difficulties in handling actual number theoretical problems, e.g., because the numbers may grow large rapidly. Codes which permit numbers of arbitrary length have been written, but they have to be monitored carefully.

Matrices with integral elements have been studied for a very long time and an enormous number of problems arise, both theoretical and practical. The whole vast classical theory of quadratic forms comes under the theory of symmetric matrices; many new problems have arisen in recent years. Some of the problems can be divided, perhaps, into four topics:

(1) Inversion (see e.g., J. B. Rosser [1]).

(2) Eigenvalues and eigenvectors. These play a role in the determination of the class number of an algebraic number field F by rational methods. For it can be shown that the number of ideal classes coincides with the number of classes of matrices $S^{-1}AS$, where A is a matrix with integral elements which is a root of the algebraic equation determining F, and S runs through all unimodular matrices with integral elements (see O. Taussky [2, 3]).

(3) Enumeration of matrices with special properties. Here we have the various problems concerning latin squares, the problems concerning matrices with ± 1 as elements and orthogonal rows (see e.g., R.E.A.C. Paley [4] and J. Hadamard [5]). The study of finite projective geometries has led to new problems in this field and some of them will be discussed here later. A generalization of these problems is given by the study of block designs which are of importance in statistical work (see M. Hall [6], H. Ryser [7], R. C. Bose [8], W. S. Connor and W. H. Clatworthy [9]).

(4) Maximization problems. These come actually also under the problems discussed in (3), but have been studied rather extensively, particularly in recent years. A prototype among these is the assignment problem: given an $n \times n$ matrix (a_{ij}), determine the permutation $P(i)$ for which

$$\sum a_{iP(i)}$$

is maximum (see e.g., T. S. Motzkin [11], C. B. Tompkins [12], H. W. Kuhn and A. W. Tucker [13]).

2. Some Problems

However, many other problems arise which cannot easily be brought under these headings. Of these we mention a few. Matrices with rational integral coefficients are a generalization of rational integers and any number theoretical process can be applied to them: e.g., any two $n \times n$ matrices of this type have a greatest common left divisor, a greatest common right divisor, a least common left multiple, a least common right multiple. If D is the greatest common left divisor of A,B, then

$$D=AP+BQ$$

can be solved where P, Q are again $n \times n$ matrices with rational integral coefficients. Diophantine equations can be studied, even the Fermat equation

$$x^n+y^n=z^n$$

can be considered for matrices.

Completely new problems arise as well because of the noncommutativity of matrices. A quite elementary example is to express a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with a, b, c, d rational integers and $ad-bc=1$ in terms of the generators $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. A much more difficult problem is to express (when possible) a positive definite $n \times n$ matrix C of rational integers in the form $C=XX'$ where X is again an $n \times n$ matrix of rational integers and X' is its transpose. If the determinant $|C|=1$ and $n<8$ such a decomposition is known to be possible always. Actually to find X can be a difficult computational problem (see [7]).

---

[1] This paper is based on an invited address to the Società Italiana per il Progresso delle Scienze, in Sicily in 1956; it was prepared with partial support from the Office of Naval Research.

[2] Present address: California Institute of Technology, Pasadena 4, Calif.

3. Hermite Normal Forms

For many of the problems concerning matrices of rational integers the so-called Hermite normal form of a matrix A plays an important role. It is a triangular matrix obtained by multiplying A with a suitable unimodular matrix U of integers and is of the form.

$$UA=\begin{pmatrix} h_{11} & h_{12} & . & . & h_{1n} \\ 0 & h_{22} & . & . & h_{2n} \\ . & . & . & . & . \\ 0 & 0 & . & 0 & h_{nn} \end{pmatrix},$$

where $h_{ii}\geq 0$ and $0\leq h_{ik}<h_{ii}(i<k)$.

Another important normal form associated with A is the Smith normal form which is a diagonal matrix. It is obtained by multiplying A with two unimodular matrices U, V so that

$$UAV=\begin{pmatrix} h_1 & & & & & & \\ & h_2 & & & & & \\ & & . & & & & \\ & & & . & & & \\ & & & & . & & \\ & & & & & h_\rho & \\ & & & & & & 0 \end{pmatrix}$$

and $h_1|h_2|\ .\ .\ .\ |h_\rho$.

4. Application of the Hermite Normal Form to Finite Projective Planes

An important use of the Hermite normal form was made in the study of finite projective plane geometries (FPP). An FPP is a set of k elements called points which are distributed over k lines such that exactly $n+1$ points lie on each line and exactly $n+1$ lines pass through a given point. Two distinct points are contained in one and only one line; two distinct lines contain one and only one point in common. We have $k=n^2+n+1$. The number n is called the order of the geometry. With such a geometry there is associated the so-called $k\times k$ incidence matrix

$$A=(a_{ij})$$

where

$a_{ij}=1$ if the ith point lies on the jth line,
$a_{ij}=0$ if the ith point does not lie on the jth line.

Hence any two rows (columns) have a one in common in exactly one column (row) and there are $n+1$ elements $a_{ij}=1$ in each row (column).

The incidence matrix A is a matrix of integers. If the lines (points) are numbered in a different order then A is replaced by PA (AQ) where P and Q are permutation matrices. The following two properties of A are particularly important:

$$\det A=\pm n^{(n^2+n)/2}(n+1),$$
$$AA'=A'A=nI+J,$$

where I is the unit matrix and J the matrix consisting of 1's only.

G. Pall studied the Smith and Hermite normal forms of A (see [14]). He showed that for square free values of n the diagonal elements in the Smith form are

$$1,\ 1,\ .\ .\ .\ ,\ 1,\ n,\ .\ .\ .\ ,\ n,\ n(n+1)$$

and the diagonal elements of the Hermite normal form are 1, or divisors of n, or $(n+1)$ times a divisor of n.

Two different geometries cannot have the same Hermite matrix. Thus the Hermite matrix of a geometry is rather important. G. Pall further investigated the p-rank of A, i.e., the maximum number of linearly independent rows of A, mod p, where p is a prime factor of n. If p^2 is not a factor of n (e.g., if n is square free) then the p-rank of A is exactly

$$\frac{1}{2}(n^2+n)+1.$$

For all other p

$$p\text{-rank}\leq\frac{1}{2}(n^2+n)+1$$

holds. As special examples the 2-rank for the (unique) geometry corresponding to $n=4$ was computed. It is 10. The 3-rank corresponding to $n=9$ presented a more difficult task. There are two different geometries of order 9. The 91×91 incidence matrices of these geometries have as 3-rank 37 and 41 while $\frac{1}{2}(n^2+n)+1=46$. These values of the 3-rank were computed on SEAC and on SWAC. The computation on SEAC was carried out by M. Newman; it took 20 hr. The Hermite normal forms of the geometries of order $n=5$ and $n=7$ were also computed; it took 3 hr for this task.

5. Further Facts About the Incidence Matrix[3]

Incidence matrices have been used to study the still unsolved problem: For what value of n is there a finite projective plane? So far it is known that for $n=p^r$, p a prime number, there is always a

[3] See also reference [15].

finite projective plane. This plane is uniquely determined for $n=2, 3, 4, 5, 7, 8$. This was established for $n=7$ by M. Hall [16] and for $n=8$ by computations carried out on SWAC by M. Hall, J. D. Swift and R. J. Walker [17].

For $n=6$ there is no FPP whatsoever (see R. H. Bruck and H. J. Ryser [18], S. Chowla and H. J. Ryser [19]). On the other hand for $n=9$ it is known that there exist two different geometries; one of these satisfies the axiom of Desargues, the other does not. For $n=10$ it is not known whether a FPP exists.

A valuable contribution towards the solution of the problem of determining the possible orders of a FPP is given by the following theorem of Ryser [20]:

Let n *be odd and let* $k=n^2+n+1$. *Assume* $nI+J=XX'$ *where* X *is a matrix of integers. Then there exists a* FPP *with* $n+1$ *points on each line.*

However, as pointed out earlier, it is a rather difficult computational problem of deciding whether a given positive definite matrix of high order splits up in the form XX' with X an integral matrix.

6. References

The list of references given below is not intended to be exhaustive, even for the selection of problems noted. In some of the papers cited, there are extensive bibliographies.

[1] J. B. Rosser, A method for computing exact inverses of matrices with integer coefficients, J. Research NBS **49,** 349–358 (1952).

[2] O. Taussky, On a theorem of Latimer and MacDuffee, Canad. J. Math. **1,** 300–302 (1949).

[3] O. Taussky, Some computational problems in algebraic number theory, Numerical analysis, Proc. 6th Symp. Appl. Math, pp. 187–193 (New York, N.Y., 1956).

[4] R. E. A. C. Paley, On orthogonal matrices, J. Math. Phys. **38,** 311–320 (1933).

[5] J. Hadamard, Resolution d'une question relative aux déterminants, Bull. Sc. Math. (**2**) **17,** 136–142 (1893).

[6] M. Hall, Projective planes and related topics (California Institute of Technology, 1954).

[7] H. J. Ryser, Geometries and incidence matrices, Am. Math. Monthly **62,** 25–31 (1955).

[8] R. C. Bose, Mathematical theory of the symmetrical factorial design, Sankhya **8,** 107–166 (1947).

[9] W. S. Connor and W. H. Clatworthy, Some theorems for partially balanced designs, Ann. Math. Stat. **25,** 100–112 (1954).

[10] J. H. Curtiss, editor, Numerical analysis, Proc. 6th Symp. Appl. Math. (New York, N.Y., 1956).

[11] T. S. Motzkin, The assignment problem, Numerical analysis, Proc. 6th Symp. Appl. Math., pp. 109–125 (New York, N.Y., 1956).

[12] C. B. Tompkins, Machine attacks on problems whose variables are permutations, Numerical analysis, Proc. 6th Symp. Appl. Math., pp. 195–211 (New York, N.Y., 1956).

[13] H. W. Kuhn and A. W. Tucker, Annals of Math. Studies 24, 28, 38 (Princeton, N.J., 1950, 1953, 1956).

[14] G. Pall, Some theorems on finite projective planes (unpublished manuscript, 1953).

[15] A. J. Hoffman, M. Newman, E. G. Straus, and O. Taussky, On the number of absolute points of a correlation, Pacific J. Math. **6,** 83–96 (1956).

[16] M. Hall, Uniqueness of the projective plane with 57 points, Proc. Am. Math. Soc. **4,** 912–916 (1953).

[17] M. Hall, J. D. Swift, and R. J. Walker, Uniqueness of the projective plane of order eight, Math. Tables Aids Comput. **10,** 186–199 (1956).

[18] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, Canad. J. Math. **1,** 88–93 (1941).

[19] S. Chowla and H. J. Ryser, Combinatorial problems, Canad. J. Math. **2,** 93–99 (1950).

[20] H. J. Ryser, Matrices with integer elements, Am. J. Math. **84,** 769–773 (1952).

[21] O. Taussky, Matrices of rational integers, Bul. Am. Math. Soc. **66,** 327–345 (1960).

[22] H. J. Ryser, Matrices of zeros and ones, Bul. Am. Math. Soc. **66,** 442–464 (1960).

[23] 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 (contains references to work), Canad. J. Math. **12,** 189–203 (1960).

(Paper 65B1–43)