COMBINATORIAL PROBLEMS

S. CHOWLA AND H. J. RYSER

1. Introduction. Let it be required to arrange v elements into v sets such that every set contains exactly k distinct elements and such that every pair of sets has exactly $\lambda = k(k-1)/(v-1)$ elements in common $(0 < \lambda < k < v)$. This combinatorial problem is studied in conjunction with several similar problems, and these problems are proved impossible for an infinitude of v and k. An incidence matrix is associated with each of the combinatorial problems, and the problems are then studied almost entirely in terms of their incidence matrices. The techniques used are similar to those developed by Bruck and Ryser for finite projective planes [3]. The results obtained are of significance in the study of Hadamard matrices [6; 8], finite projective planes [9], symmetrical balanced incomplete block designs [2; 5], and difference sets [7].

2. Combinatorial problems. Let $x_1, x_2, \ldots, x_v$ denote v elements and let $s_1, s_2, \ldots, s_v$ denote v sets formed from these elements. Let the elements $x_1, x_2, \ldots, x_v$ be listed in a row and let the sets $s_1, s_2, \ldots, s_v$ be listed in a column. Let 1 be inserted in row i and column j if the element x_j belongs to the set s_i, and 0 in the contrary case. The matrix A of order v formed from this square array of zeros and ones is called the *incidence matrix* of the arrangement of v elements into v sets. Clearly the incidence matrix serves to characterize this arrangement completely. We proceed now to consider a series of combinatorial problems, and to study these problems in terms of their incidence matrices.

PROBLEM I. *Arrange v elements into v sets such that*

(I_1) *every set contains exactly k distinct elements,*

(I_2) *every pair of sets has exactly $\lambda = k(k-1)/(v-1)$ elements in common $(0 < \lambda < k < v)$.*

PROBLEM II. *Arrange v elements into v sets such that*

(II_1) *each element occurs in exactly k distinct sets,*

(II_2) *every pair of elements occurs in the v sets exactly $\lambda = k(k-1)/(v-1)$ times $(0 < \lambda < k < v)$.*

PROBLEM II′. *Arrange v elements into v sets fulfilling* (II_1) (II_2), *and* (I_1).

PROBLEM III. *Arrange v elements into v sets fulfilling* (I_1), (I_2), (II_1), *and* (II_2).

Received January 6, 1949.

PROBLEM IV. *Arrange v elements into v sets fulfilling* (I_1) *and* (I_2) *in such a way that the incidence matrix of the arrangement is cyclic, i.e.*

$$A = \begin{bmatrix} a_1 & a_2 & \dots & a_v \\ a_2 & a_3 & \dots & a_1 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ a_v & a_1 & \dots & a_{v-1} \end{bmatrix}.$$

Problem I has a solution if and only if there exists a matrix A of order v composed of zeros and ones such that

$$A A^{\mathsf{T}} = B, \tag{I}$$

where A^{T} denotes the transposed matrix of A and B is a symmetric matrix with k in the main diagonal and λ in all other positions. Problem II requires

$$A^{\mathsf{T}}A = B, \tag{II}$$

and Problem III requires

$$AA^{\mathsf{T}} = A^{\mathsf{T}}A = B. \tag{III}$$

The preceding problems arise naturally in certain combinatorial investigations. Problem I for $v = 4n - 1$, $k = 2n - 1$, and $\lambda = n - 1$ was proposed by Todd, and was shown to be equivalent to finding a Hadamard matrix of order $4n$ [6; 8]. Problem II′ was studied by Bose, and the arrangements obtained were called symmetrical balanced incomplete block designs [2;5]. Veblen and Bussey introduced the finite projective plane, and Problem III for $v = N^2+N+1$, $k = N + 1$, $N \geqslant 2$, and $\lambda = 1$ is equivalent to finding a projective plane with $N + 1$ points on a line [3; 9].

Singer defined a difference set of k numbers mod v as a set of integers d_1, $d_2, \dots, d_k$ such that the congruences $d_i - d_j \equiv n \bmod v$ have the same number of solutions $\lambda = k(k - 1)/(v - 1)$ for every $n \not\equiv 0 \bmod v$ [7]. Problem IV is equivalent to finding a difference set of k numbers mod v. For if such a difference set exists, form the array of k rows and v columns

$$\begin{matrix} d_1, d_1 - 1, \dots, d_1 - (v - 1) \\ \cdot \\ \cdot \\ \cdot \\ d_k, d_k - 1, \dots, d_k - (v - 1) \end{matrix}$$

where the integers are reduced mod v so that they lie in the range $1 \leqslant x \leqslant v$. Now form an incidence matrix A of order v by taking column i of the above array and placing in row i of the matrix A ones in columns $d_1 - (i - 1), \dots, d_k - (i - 1)$ and zeros in all other positions. Clearly, A by the nature of its construction is cyclic. Moreover, A has exactly k ones in each row, and since for $r \not\equiv s$, $d_i - r \equiv d_j - s \bmod v$ has exactly λ solutions, any two rows of A have exactly λ ones in common. Thus the matrix A yields a solution of Problem IV. Conversely, suppose that Problem IV has a solution. Then the

first row of the incidence matrix A has ones in the k columns $d_1, \ldots, d_k$, and these k numbers form a difference set mod v. For row $n+1$ of A has ones in the columns $d_1 - n, \ldots, d_k - n$, where the integers are taken mod v, and for $n \not\equiv 0 \bmod v$, the sets $d_1, \ldots, d_k$ and $d_1 - n, \ldots, d_k - n$ have exactly λ elements in common. Hence $d_i - d_j \equiv n \bmod v$ has exactly λ solutions.

3. Identical combinatorial problems. Let P and Q be any two of the preceding combinatorial problems. The problems P and Q are said to be identical, written $P \equiv Q$, provided that each solution of P is necessarily a solution of Q, and conversely each solution of Q is necessarily a solution of P.

THEOREM 1. *Problem* I $\equiv$ *Problem* II $\equiv$ *Problem* II′ $\equiv$ *Problem* III.

Suppose that A is a matrix of order v composed of zeros and ones such that $AA^{\mathsf{T}} = B$, where B has k in the main diagonal and $\lambda = k(k-1)/(v-1)$ in all other positions. For this A we prove that $A^{\mathsf{T}}A = B$. Define the matrix O of order $v+1$ by the equation

$$O = \begin{bmatrix} -k & \sqrt{-\lambda} & \cdots & \sqrt{-\lambda} \\ \sqrt{-\lambda} & & & \\ \cdot & & & \\ \cdot & & A & \\ \cdot & & & \\ \sqrt{-\lambda} & & & \end{bmatrix}.$$

Recalling that $\lambda = k(k-1)/(v-1)$, an easy computation shows that $OO^{\mathsf{T}} = (k-\lambda)I$, where I is the identity matrix of order $v+1$. But then $OO^{\mathsf{T}} = O^{\mathsf{T}}O$, and then by the very structure of O, it follows that $AA^{\mathsf{T}} = A^{\mathsf{T}}A$.

Thus a solution of Problem I is necessarily a solution of Problem III, and consequently Problem I $\equiv$ Problem III. Moreover, the matric equation $A^{\mathsf{T}}(A^{\mathsf{T}})^{\mathsf{T}} = A^{\mathsf{T}}A = B$ now implies that $AA^{\mathsf{T}} = B$, and consequently Problem I $\equiv$ Problem II. This proves Theorem I. (For another proof see Bose [2].)

THEOREM 2. *There exist values for v and k for which Problem* III *has a solution and for which Problem* IV *has no solution.*

Evidently every solution of Problem IV is a solution of Problem III. To prove Theorem 2 we utilize the following theorem of Chowla, which establishes the nonexistence of a certain class of difference sets. The recent investigations of Marshall Hall have also been successful in proving the nonexistence of large classes of such sets [4].

Let $v, k,$ and $\lambda = k(k-1)/(v-1)$ be positive integers, $0 < \lambda < k < v$. Let $p \equiv 3 \bmod 4$ be a prime factor of v and let q be an odd prime factor which divides the squarefree part of $k - \lambda$. If the Legendre symbol $(-p|q) = -1$, then there does not exist a difference set of k numbers mod v.

To prove the theorem let $d_1, d_2, \ldots, d_k$ denote such a difference set, and define $S = \sum_{j=1}^{k} \rho^{d_j}$, where $\rho = e^{\frac{2\pi i}{p}}$. Then $S\overline{S} = k + \lambda(\rho + \rho^2 + \ldots + \rho^{v-1})$

https://doi.org/10.4153/CJM-1950-009-8 Published online by Cambridge University Press

$= k - \lambda$, where $\bar{S}$ denotes the complex conjugate of S. Let $t = S\theta^2 S\theta^4 S \ldots \theta^{p-3} S$, where θ denotes a generating automorphism of the cyclic algebraic field $R(\rho)$. If $N(S)$ denotes the algebraic norm of S in $R(\rho)$, then $N(S) = t\theta t$. The algebraic integers t and θt are conjugates in the unique quadratic subfield $R\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$ of $R(\rho)$ [1; 10]. Consequently $N(S) = (x^2 + py^2)/4$, where x and y are integers. But the equation $S\bar{S} = (k - \lambda)$ implies $N(S) = (k - \lambda)^{\frac{p-1}{2}}$. Thus $x^2 + py^2 - 4(k - \lambda)^{\frac{p-1}{2}} = 0$, and this equation may be rewritten in the form $x^2 + py^2 - qtz^2 = 0$, where t is squarefree and prime to q, and where x, y, and z do not have a prime factor in common. It now follows that q does not divide y, and hence $(y^{-1}x)^2 \equiv -p \bmod q$.

Now let $v = 55$ and $k = 27$. Then $\lambda = 13$ and $k - \lambda = 14$. Select $p = 11$ and $q = 7$. Then $(-11|7) = -1$, and consequently there does not exist a difference set of 27 numbers mod 55. Thus for these values of v and k, Problem IV does not have a solution. On the other hand it is well known that a Hadamard matrix of order 56 exists, and by the remarks of Todd, Problem I has a solution for these values of v and k [6; 8]. But Problem I $\equiv$ Problem III.

4. The impossibility of certain combinatorial problems. In this section the impossibility of Problem I is proved for an infinitude of v and k. Clearly the impossibility of Problem I for a given v and k implies the impossibility for the same v and k of Problems II, II′, III, and IV. Interpreted with regard to the results of the previous sections, the theorems which follow offer generalizations of numerous previous investigations. Actually Theorems 4 and 5 are rather straightforward generalizations of a theorem of Bruck and Ryser on the nonexistence of certain finite projective planes, and for projective planes these theorems give no new information [3]. However, their proofs are independent of the difficult Minkowski-Hasse theory of the invariants of a rational quadratic form under rational transformations. (The writers are indebted to Daniel Zelinsky for helpful comments concerning the proof of Theorem 5.)

THEOREM 3. *If v is even and if $k - \lambda$ is not a square, then Problem* I *has no solution.*

A solution of Problem I implies that $AA^T = B$, where B has k in the main diagonal and λ in all other positions. Subtract column one of the matrix B from each of the other columns, and then add to row one each of the other rows. It readily follows that the determinant of B is given by

$$\det B = \det^2 A = (k - \lambda)^{v-1}(k + (v - 1)\lambda) = (k - \lambda)^{v-1} k^2.$$

Thus if v is even and if $k - \lambda$ is not a square, then Problem I has no solution.

THEOREM 4. *If $v \equiv 1 \bmod 4$ and if there exists an odd prime p such that p divides the squarefree part of $k - \lambda$, and, moreover, if $(\lambda|p) = -1$, then Problem* I *has no solution.*

The matric equation $AA^T = B$ implies

$$k\sum_{i=1}^{v} x_i^2 + \lambda \sum_{i \neq j} x_i x_j = (k-\lambda)\sum_{i=1}^{v} x_i^2 + \lambda(\sum x_i)^2 = \sum_{i=1}^{v} u_i^2,$$

where the matrix $C = [c_{ij}]$ of the transformation $x_i = \sum c_{ij}u_j$ is rational and nonsingular. By the four-square theorem of Lagrange, $k - \lambda = a_1^2 + a_2^2 + a_3^2 + a_4^2$, where the a's are integers. If

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & a_4 & -a_3 \\ -a_3 & a_4 & a_1 & -a_2 \\ a_4 & a_3 & -a_2 & -a_1 \end{bmatrix},$$

then $AA^{\mathsf{T}} = (k-\lambda)I$, where I is the identity matrix of order 4. Thus if $[k-\lambda, k-\lambda, \ldots, k-\lambda]$ is a diagonal matrix of order $v \equiv 1 \bmod 4$, then there exists a rational and nonsingular D such that

$$[k-\lambda, k-\lambda, \ldots, k-\lambda] = D^{\mathsf{T}}[1, 1, \ldots, 1, k-\lambda]\, D,$$

whence $(k-\lambda)\sum_{i=1}^{v} x_i^2 = \sum_{i=1}^{v-1} y_i^2 + (k-\lambda)y_v^2$. Thus

$$\sum_{i=1}^{v-1} y_i^2 + (k-\lambda)y_v^2 + \lambda(\sum d_i y_i)^2 = \sum_{i=1}^{v} u_i^2,$$

where the d_i are rational and the matrix $E = [e_{ij}]$ of the transformation $y_i = \sum e_{ij}u_j$ is rational and nonsingular.

Now set $y_1 = \sum e_{1j}u_j = \pm u_1$, where the coefficient is $+1$ if $e_{11} \neq 1$ and -1 if $e_{11} = 1$. Then $y_2 = \sum_{j=2}^{v} f_j u_j$, and set $y_2 = \pm u_2$, where the coefficient is $+1$ if $f_2 \neq 1$ and -1 if $f_2 = 1$. Continue the process inductively until $y_{v-1} = g_{v-1}u_{v-1} + g_v u_v$, where $y_{v-1} = \pm u_{v-1}$. Now let u_v equal a nonzero rational. Then $u_1, \ldots, u_{v-1}$ are uniquely determined, and, moreover, $y_i = \pm u_i$, for $i = 1, 2, \ldots, v-1$. Thus the Diophantine equation

$$x^2 = (k-\lambda)y^2 + \lambda z^2$$

has a solution in integers other than the zero solution. The equation may be rewritten in the form

$$x^2 = pty^2 + \lambda z^2,$$

where t is squarefree and prime to p, and where x, y, and z do not have a prime factor in common. Now p does not divide z, and hence $(z^{-1}x)^2 \equiv \lambda \bmod p$.

THEOREM 5. *If $v \equiv 3 \bmod 4$ and if there exists an odd prime p such that p divides the squarefree part of $k - \lambda$, and, moreover, if $(-\lambda|p) = -1$, then Problem* I *has no solution.*

https://doi.org/10.4153/CJM-1950-009-8 Published online by Cambridge University Press

Suppose that $v \equiv 3 \bmod 4$ and that $B = AA^{\mathsf{T}}$. Then

$$\begin{bmatrix} & & 0 \\ & & 0 \\ & B & . \\ & & . \\ & & . \\ & & 0 \\ 0\,0\,\ldots\,0 & & k-\lambda \end{bmatrix} = \begin{bmatrix} & & 0 \\ & & 0 \\ & A & . \\ & & . \\ & & . \\ & & 0 \\ 0\,0\,\ldots\,0 & & 1 \end{bmatrix} [1, 1, \ldots, 1, k-\lambda] \begin{bmatrix} & & 0 \\ & & 0 \\ & A^{\mathsf{T}} & . \\ & & . \\ & & . \\ & & 0 \\ 0\,0\,\ldots\,0 & & 1 \end{bmatrix},$$

and

$$k\sum_{i=1}^{v} x_i^2 + (k-\lambda)x_{v+1}^2 + \lambda \sum_{\substack{i,j=1 \\ i \neq j}}^{v} x_i x_j = (k-\lambda)\sum_{i=1}^{v+1} x_i^2 + \lambda\Big(\sum_{i=1}^{v} x_i\Big)^2$$

$$= \sum_{i=1}^{v} u_i^2 + (k-\lambda)\,u_{v+1}^2,$$

where the matrix $C = [c_{ij}]$ of the transformation $x_i = \sum c_{ij}u_j$ is rational and nonsingular. If $[k-\lambda, k-\lambda, \ldots, k-\lambda]$ is a diagonal matrix of order $v+1 \equiv 0 \bmod 4$, then there exists a rational and nonsingular D such that

$$[k-\lambda, k-\lambda, \ldots, k-\lambda] = D^{\mathsf{T}}[1, 1, \ldots, 1]D,$$

whence $(k-\lambda)\sum_{i=1}^{v+1} x_i^2 = \sum_{i=1}^{v+1} y_i^2$. Thus

$$\sum_{i=1}^{v+1} y_i^2 + \lambda(\sum d_i y_i)^2 = \sum_{i=1}^{v} u_i^2 + (k-\lambda)\,u_{v+1}^2,$$

where the d_i are rational and the matrix $E = [e_{ij}]$ of the transformation $y_i = \sum e_{ij}u_j$ is rational and nonsingular.

Now set $y_1 = \sum_{v+1} e_{1j}u_j = \pm u_1$, where the coefficient is $+1$ if $e_{11} \neq 1$ and -1 if $e_{11} = 1$. Then $y_2 = \sum_{j=2} f_j u_j$, and set $y_2 = \pm u_2$. Continue inductively until $y_v = g_v u_v + g_{v+1}u_{v+1}$, where $y_v = \pm u_v$. Now let u_{v+1} equal a nonzero rational. Then $u_1, \ldots, u_v$ are uniquely determined and $u_i = \pm y_i$ for $i = 1, 2, \ldots, v$. Thus

$$x^2 + \lambda y^2 = (k-\lambda)z^2$$

has a solution in integers other than the zero solution. It follows that $-\lambda$ is a quadratic residue of p. This completes the proof of Theorem 5.

Theorems 4 and 5 may also be derived by the methods employed in [3]. Only minor modifications in the proof given for projective planes are required. It can be shown that for v odd, the matric equation $AA^{\mathsf{T}} = B$ is possible for a rational and nonsingular A if and only if

$$(k-\lambda, -1)_p^{\frac{(v-1)v}{2}}(k-\lambda, v)_p = +1$$

https://doi.org/10.4153/CJM-1950-009-8 Published online by Cambridge University Press

for every odd prime p. The notation $(m, n)_p$ designates the norm-residue symbol of Hilbert. It is easy to verify that this condition excludes precisely those values of v and k covered by Theorems 4 and 5.

References

[1] Bachmann, Paul, *Die Lehre von der Kreistheilung* (Leipzig, 1872), 204.
[2] Bose, R. C., "On the Construction of Balanced Incomplete Block Designs," *Annals of Eugenics*, vol. 9 (1939), 353-399.
[3] Bruck, R. H. and Ryser, H. J., "The Nonexistence of Certain Finite Projective Planes," *Can. J. Math.*, vol. 1 (1949), 88-93.
[4] Hall, Marshall, "Cyclic Projective Planes," *Duke Math. J.* (1947), 1079-1090.
[5] Levi, F. W., *Finite Geometrical Systems* (University of Calcutta, 1942).
[6] Paley, R. E. A. C., "On Orthogonal Matrices," *J. of Math. and Physics*, vol. 12 (1933), 311-320.
[7] Singer, James, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *Trans. Amer. Math. Soc.*, vol. 43 (1938) 377-385.
[8] Todd, J. A., "A Combinatorial Problem," *J. of Math. and Physics*, vol. 12 (1933), 321-333.
[9] Veblen, O. and Bussey, W. H., "Finite Projective Geometries," *Trans. Amer. Math. Soc.*, vol. 7 (1906), 241-259.
[10] van der Waerden, B. L., *Moderne Algebra*, I (Berlin, 1937), 165.

University of Kansas
and
Ohio State University