CYCLIC INCIDENCE MATRICES

MARSHALL HALL AND H. J. RYSER

1. Introduction. Let it be required to arrange v elements into v sets such that each set contains exactly k distinct elements and such that each pair of sets has exactly λ elements in common $(0 < \lambda < k < v)$. This problem we refer to as the v, k, λ combinatorial problem. Listing the elements $x_1, x_2, \ldots, x_v$ in a row and the sets $S_1, S_2, \ldots, S_v$ in a column, one forms the incidence matrix A of the arrangement by inserting 1 in row i and column j if x_j belongs to S_i, and 0 in the contrary case.

It has been shown that $\lambda = k(k-1)/(v-1)$, and consequently the matrix A satisfies

$$AA^{\mathrm{T}} = A^{\mathrm{T}}A = B,$$

where A^{T} denotes the transpose of A and where B has k in the main diagonal and λ in all other positions [7]. In the present paper, we are concerned only with the special case in which the incidence matrix A is cyclic. This problem we analyse in terms of incidence matrices and multipliers of difference sets. Extensive use will be made of certain of the results and techniques developed by Bruck, Chowla, Ryser, and M. Hall in [1], [3], [4].

2. A non-existence theorem. Let us now suppose that the incidence matrix

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

of the v, k, λ problem is cyclic. In this section we derive the following non-existence theorem.

THEOREM 2.1. *Let $0 < \lambda < k < v$, and let v be odd. Let e be an arbitrary positive divisor of v. If there exists a cyclic solution of the v, k, λ problem, then the Diophantine equation*

$$x^2 = (k-\lambda)y^2 + (-1)^{\frac{1}{2}(e-1)}\, ez^2$$

must possess a solution in integers not all zero.

We begin with the following Lemma.

LEMMA. *Let B be a matrix of order v, where v is odd. Let B have the integer k in the main diagonal, and the integer λ in all other positions, where $0 < \lambda < k$. If there exists a matrix A with rational elements such that*

Received July, 14 1950.

(B) $$AA^{\mathrm{T}} = B,$$

then there must exist an integer T such that

(1) $$T^2 = (k - \lambda) + v\lambda.$$

Moreover, the Diophantine equations

(2) $$\bar{x}^2 = (k - \lambda)\bar{y}^2 + (-1)^{\frac{1}{2}(v-1)}\lambda\bar{z}^2$$

and

(3) $$x^2 = (k - \lambda)y^2 + (-1)^{\frac{1}{2}(v-1)}vz^2$$

must each possess solutions in integers not all zero.

Equation (1) follows directly upon observing that the determinant of B is $(k - \lambda)^{v-1}\ (k + (v - 1)\lambda)$, and that this quantity must be a square. The derivation of (2) is contained in [3]. For the sake of completeness, we sketch the proof for the case $v \equiv 1 \pmod 4$.

The matric equation (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 of the transformation $x_i = \sum c_{ij}u_j$ is rational and non-singular. For a diagonal matrix $[k - \lambda, k - \lambda, \ldots, k - \lambda]$ of order $v \equiv 1 \pmod 4$, there exists a rational and non-singular D such that $[k - \lambda, k - \lambda, \ldots, k - \lambda] = D^{\mathrm{T}}[1, 1, \ldots, 1, k - \lambda]D$, whence

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

Hence

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

where the d_i are rational and the matrix of the transformation $y_i = \sum e_{ij}u_j$ is again rational and non-singular. 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 inductively, setting $y_{v-1} = \pm u_{v-1}$. Finally, let u_v equal a non-zero rational. Then $\bar{x}^2 = (k - \lambda)\ \bar{y}^2 + \lambda\bar{z}^2$ possesses a non-zero solution in integers.

To derive (3) from (1) and (2), observe that if $k - \lambda$ is a square, then (3) possesses an obvious non-zero solution. However, if $k - \lambda$ is not a square, then $\bar{z} \neq 0$, and hence (1) and (2) imply

$$(\bar{x}T + (k - \lambda)\bar{y})^2 - (k - \lambda)(\bar{x} + \bar{y}T)^2 = (-1)^{\frac{1}{2}(v-1)}\ v(\lambda\bar{z})^2,$$

so that (3) again possesses a non-zero solution.

Diophantine equations of the form (2) and (3) may be analysed in terms of the classical theory of Legendre, and necessary and sufficient conditions for their solvability are conveniently expressed in terms of the norm-residue symbol. The proof of the Lemma does not require the Minkowski-Hasse theory. However, this theory may be applied directly to the matric equation (B), with the exclusion of the same values of v, k, and λ. This approach has

been developed by Shrikhande in investigations on the non-existence of block designs [8].

To derive Theorem 2.1, we now utilize the techniques developed in [4] for the cyclic projective plane. A cyclic solution of the v, k, λ problem is equivalent to a difference set $d_1, d_2, \ldots, d_k$ of k numbers mod v. Following [4], one defines

$$\theta(x) = x^{d_1} + x^{d_2} + \ldots + x^{d_k},$$

whence $\theta(x)\theta(x^{-1}) = \sum x^{d_i - d_j}$. Now for $n \not\equiv 0 \pmod{v}$, the congruences $d_i - d_j \equiv n \pmod{v}$ have precisely λ solutions. Hence in the notation of polynomial congruences described in [4], it follows that

$$\theta(x)\theta(x^{-1}) \equiv k + \lambda(x + \ldots + x^{v-1}) \qquad \text{mod } x^v - 1.$$

Now let e divide v, where $v = e\mu$. Then

$$\theta(x) \equiv b_0 + b_1 x + \ldots + b_{e-1}x^{e-1} \qquad \text{mod } x^e - 1,$$

where the b_i are by definition the number of d's congruent to i mod e. Then

$$\theta(x)\theta(x^{-1}) \equiv k + \lambda(\mu - 1) + \mu\lambda(x + \ldots + x^{e-1}) \qquad \text{mod } x^e - 1,$$

and upon equating coefficients, it follows that

$$\text{(M)} \qquad \begin{aligned} \textstyle\sum_{i=0}^{e-1} b_i^2 &= k - \lambda + \mu\lambda \\ \textstyle\sum_{i=0}^{e-1} b_i b_{i+j} &= \mu\lambda, \end{aligned}$$

where $j = 1, 2, \ldots, e - 1$, and the subscripts are to be taken modulo e.

Now define the cyclic matrix

$$S = \begin{bmatrix} b_0 & b_1 & \ldots & b_{e-1} \\ b_1 & b_2 & \ldots & b_0 \\ \vdots & \vdots & & \vdots \\ b_{e-1} & b_0 & & b_{e-2} \end{bmatrix}$$

of order e. Then by the equations (M), it follows at once that

$$\text{(N)} \qquad SS^{\mathrm{T}} = D,$$

where D has $k - \lambda + \mu\lambda$ in the main diagonal and $\mu\lambda$ in all other positions. But by the Lemma, the equation $x^2 = (k - \lambda)y^2 + (-1)^{\frac{1}{2}(e-1)} ez^2$ possesses a non-zero solution in integers.

Actually the above theorem for e a prime and $e \equiv 3 \pmod 4$ implies a theorem of Chowla [2], [3]. But the interconnection between equation (N) for the cyclic case and equation (B) for the general case is perhaps of greater interest than the precise range of excluded values.

Singer has established the existence of difference sets for $v = p^{2n} + p^n + 1$, $k = p^n + 1$, and $\lambda = 1$, where p is a prime [9]. Let e be an arbitrary positive divisor of v. By the preceding theorem, the equation

$$x^2 = p^n y^2 + (-1)^{\frac{1}{2}(e-1)} ez^2$$

possesses a non-zero solution in integers.

Recently Bhattacharya [5, p. 122] has exhibited a solution of the v, k, λ problem for $v = 25$, $k = 9$, and $\lambda = 3$. However, cyclic solutions do not exist. For let $e = 5$. Then the equation of the theorem becomes

$$x^2 = 6y^2 + 5z^2,$$

and this does not possess a non-zero solution in integers.

3. The multipliers of a difference set. If $d_1, \ldots, d_k$ are a difference set mod v, following [4] we say that t is a *multiplier* of the set if for some s the residues $td_1, \ldots, td_k \pmod v$ are $d_1 + s, \ldots, d_k + s \pmod v$, apart from order. Clearly, if t is a multiplier, then for some i, j, m, and n, we have $1 \equiv d_i + s - (d_j + s) \equiv t(d_m - d_n) \pmod v$. This implies that $(t, v) = 1$. Moreover, it is clear that the multipliers form a multiplicative group mod v.

Letting $\theta(x) = x^{d_1} + \ldots + x^{d_k}$, it follows that

$$\theta(x)\theta(x^{-1}) \equiv k - \lambda + \lambda T(x) \qquad \text{mod } x^v - 1,$$

where $T(x) = 1 + x + \ldots + x^{v-1}$. The existence of a multiplier t is equivalent to an identity

$$\theta(x^t) \equiv x^s \theta(x) \qquad \text{mod } x^v - 1.$$

THEOREM 3.1. *Let p be a prime divisor of $k - \lambda$ such that $p \nmid v$ and $p > \lambda$. Then p is a multiplier of the difference set $d_1, \ldots, d_k \pmod v$.*

In the notation of [4],

$$\theta(x)\theta(x^{-1}) \equiv 0 \qquad \text{modd } p, T(x).$$

Since $\theta(x^p) \equiv (\theta(x))^p \pmod p$, it follows that

$$\theta(x^p)\theta(x^{-1}) \equiv 0 \qquad \text{modd } p, T(x),$$

whence

$$\theta(x^p)\theta(x^{-1}) \equiv aT(x) + pR_1(x) \qquad \text{mod } x^v - 1.$$

Setting $x = 1$ implies that $k^2 \equiv av \pmod p$. Since $k(k-1) = \lambda(v-1)$, it follows that $k^2 \equiv \lambda v \pmod p$. But $(v, p) = 1$ so that $a \equiv \lambda \pmod p$, and hence

$$\theta(x^p)\theta(x^{-1}) \equiv \lambda T(x) + pR(x) \qquad \text{mod } x^v - 1.$$

Now $\theta(x^p)\theta(x^{-1}) \equiv e_0 + e_1 x + \ldots + e_{v-1}x^{v-1} \bmod x^v - 1$ consists of powers of x with non-negative coefficients. Since $p > \lambda$, it follows that $R(x)$ consists of powers of x with non-negative coefficients, and the sum of these coefficients must be $(k^2 - \lambda v)/p = (k - \lambda)/p$. Similarly,

$$\theta(x)\theta(x^{-p}) \equiv \lambda T(x) + pS(x) \qquad \text{mod } x^v - 1.$$

Now trivially $\theta(x^p)\theta(x^{-p}) \equiv k - \lambda + \lambda T(x) \bmod x^v - 1$. Hence upon noting that $x^i T(x) \equiv T(x) \bmod x^v - 1$ and comparing the two values obtained for $\theta(x^p)\theta(x^{-1})\theta(x)\theta(x^{-p})$, it is clear that

$$p^2R(x)S(x) \equiv (k - \lambda)^2 \qquad \text{mod } x^v - 1.$$

But since both $R(x)$ and $S(x)$ consist of non-negative terms whose coefficients total $(k - \lambda)/p$, this relation can hold only if both $R(x)$ and $S(x)$ consist of a single term with coefficient $(k - \lambda)/p$. Hence $R(x) = (k - \lambda)/p \cdot x^s$ and $S(x) = (k - \lambda)/p \cdot x^{v-s}$, whence

$$\theta(x^p)\theta(x^{-1}) \equiv \lambda T(x) + (k - \lambda)x^s \qquad \text{mod } x^v - 1.$$

Multiplication by $\theta(x)$ implies

$$\theta(x^p)(k - \lambda + \lambda T(x)) \equiv \theta(x)\lambda T(x) + (k - \lambda)x^s\theta(x) \qquad \text{mod } x^v - 1,$$

and since $x^iT(x) \equiv T(x) \bmod x^v - 1$, it is clear that

$$(k - \lambda)\theta(x^p) \equiv (k - \lambda)x^s\theta(x) \qquad \text{mod } x^v - 1.$$

Thus $\theta(x^p) \equiv x^s\theta(x) \bmod x^v - 1$, and the theorem follows.

The existence theorem for multipliers raises an interesting complication which does not arise in the case of the cyclic projective plane. The restriction $p > \lambda$ was used in the derivation of Theorem 3.1. However, the authors have been unable to show by means of an example that this restriction is an essential part of the hypothesis.

THEOREM 3.2. *Let t be a multiplier of a difference set $d_1, \ldots, d_k \pmod v$, and let $(t - 1, v) = 1$. Let q be an odd prime divisor of v, and let t be a primitive root* mod q. *Then the integer $k - \lambda$ is a square.*

Since t is a multiplier, $(t, v) = 1$, and $r \leftrightarrow tr$ constitutes a biunique mapping of the integers mod v upon themselves. The only integer left fixed by this mapping is $r = 0$. Let T_u denote the difference set

$$d_1 + u, d_2 + u, \ldots, d_k + u.$$

Now the multiplier t maps $d_i + u$ into $td_i + tu = d_j + s + tu$, and hence t maps the difference set T_u into the difference set T_{s+tu}. Hence the mapping leaves fixed the unique difference set T_u with $(t - 1)u \equiv -s \pmod v$. Upon applying the multiplier t to the elements of this difference set, it follows that

$$\theta(x^t) \equiv \theta(x) \qquad \text{mod } x^v - 1.$$

Now let ϵ be a primitive qth root of unity. For $n \equiv t^i \pmod q$, it follows that $\theta(\epsilon^n) = \theta(\epsilon)$, and consequently $\theta(\epsilon)$ is rational. Hence $\theta(\epsilon)\theta(\epsilon^{-1}) = k - \lambda$ is a square.

THEOREM 3.3. *Let t be a multiplier belonging to the exponent e* mod v. *Then the mapping $z \to zt - s$ permutes the elements of the difference set $d_1, d_2, \ldots, d_k \pmod v$ in cycles of length dividing e.*

By hypothesis the mapping $z \to zt$ carries the difference set $d_1, \ldots, d_k$ into $td_1, \ldots, td_k$, which is $d_1 + s, \ldots, d_k + s$ in some order. Hence $z \to zt - s$

maps the difference set onto itself. Upon iterating this process e times, we obtain

$$z \to zt^e - s(1 + t + \ldots + t^{e-1}),$$

which maps the difference set onto itself. Since $t^e \equiv 1 \pmod{v}$, this yields $z \to z - A$, with $A = s(1 + t + \ldots + t^{e-1})$. If $A \not\equiv 0 \pmod{v}$, then the difference A occurs at least $k > \lambda$ times. Since this cannot happen, $A \equiv 0 \pmod{v}$, and the period of the permutation must be a divisor of e.

The condition $s(1 + t + \ldots + t^{e-1}) \equiv 0 \pmod{v}$ may often be used to show that s is divisible by common factors of $t - 1$ and v. The condition that s be divisible by $(t - 1, v)$ is of course sufficient to show that an n exists such that $(z + n)t \equiv zt + s + n \pmod{v}$, whence the difference set $d_1 + n, \ldots, d_k + n$ is mapped onto itself by the multiplier t.

The following examples exhibit the various ways in which the use of the multipliers is effective.

Example 1. Let $v = 37$, $k = 9$, and $\lambda = 2$. Here $k - \lambda = 7$ is a multiplier and since $(7 - 1, 37) = 1$, there is a fixed difference set. Multiplying by an appropriate factor, one element of the set may be taken as 1. Hence we have

$$1, 7, 9, 10, 12, 16, 26, 33, 34 \qquad \text{mod } 37,$$

viz., the powers of 7, and these numbers do form the required difference set.

Example 2. For the cyclic plane with $v = 273$, $k = 17$, and $\lambda = 1$, we have $k - \lambda = 16$, and hence 2 is a multiplier. The line through 91 and 182 is necessarily a fixed line. Here $2^{12} \equiv 1 \pmod{273}$, and so the cycles may have lengths 1, 2, 3, 4, 6, or 12. Now $2^4x \equiv x \pmod{273}$ implies $2^2x \equiv x \pmod{273}$, and $x = 0$, 91, or 182. We cannot have 0 with 91 and 182 since 91 cannot occur twice as a difference. Hence besides 91 and 182 we will have elements with cycles of lengths 3, 6, or 12 to make up the remaining 15. Hence there must be at least one cycle of length 3, and $2^3x \equiv x$ means $x \equiv 0 \pmod{39}$. Thus the number of $x \equiv 0 \pmod{39}$ is at least 3, and cannot be greater without repeating differences. The remaining twelve d's cannot all be divisible by 13. Hence there is a d whose common factor with 273 is at most 21. This belongs to a cycle of length 12. But we cannot have $12 \cdot 13 = 132$ differences which are multiples of 3 or 7. Hence the remaining cycle includes numbers prime to 273, of which one may be taken as 1. Thus we have

$$1, 2, 4, 8, 16, 32, 64, 91, 128, 137, 182, 205, 239, 256$$

and either 39, 78, and 156 or 117, 195, and 234. Since $39 - 32 = 8 - 1$, the first alternative is out, and we have only the possibility

$$1, 2, 4, 8, 16, 32, 64, 91, 117, 128, 137, 182, 195, 205, 234, 239, 256 \qquad \text{mod } 273,$$

which is in fact a difference set mod 273.

Example 3. Let $v = 15$, $k = 7$, $\lambda = 3$, and $k - \lambda = 4$. If we assume that 2 which divides $k - \lambda$ is a multiplier, we readily find the difference set 0, 1, 2, 4, 5, 8, 10 (mod 15). Since $2 < 3$, Theorem 3.1 does not apply. But by Todd's enumeration of these designs [**10**], this is in fact the only cyclic solution.

Example 4. Let $v = 41$, $k = 16$, $\lambda = 6$, and $k - \lambda = 10$. Here the prime divisors 2 and 5 of $k - \lambda$ are both less than λ and so Theorem 3.1 does not apply. But $5^3 \equiv 2 \pmod{41}$. Hence

$$\theta(x^2) \equiv \theta(x^{125}) \qquad \text{mod } x^{41} - 1$$

and

$$\theta(x^2)\theta(x^{-1}) \equiv (\theta(x))^{125}\,\theta(x^{-1}) \equiv 0 \qquad \text{modd } 5,\ T(x),$$
$$\theta(x^2)\theta(x^{-1}) \equiv (\theta(x))^{2}\,\theta(x^{-1}) \equiv 0 \qquad \text{modd } 2,\ T(x).$$

Hence $\theta(x^2)\theta(x^{-1}) \equiv 0$ (modd 10, $T(x)$), and $\theta(x^2)\theta(x^{-1}) \equiv aT(x)+10R_1(x)$ mod $x^{41} - 1$. As in Theorem 3.1, we may conclude that 2 is a multiplier. But 2 belongs to the exponent 20 mod 41, and so we readily see that no cyclic solution exists.

The method of this example may be expanded to show that in general if $t \equiv p_1^{e1} \equiv p_2^{e2} \equiv \ldots \equiv p_r^{e_r} \pmod{v}$ is prime to v, where $p_1, \ldots, p_r$ are distinct primes dividing $k - \lambda$ whose product exceeds λ, then t is a multiplier.

Example 5. It has been conjectured by Paley that in the Hadamard case, $v = 4m - 1$, $k = 2m - 1$, and $\lambda = m - 1$, the design always exists [6]. The first case in doubt is $v = 91$, $k = 45$, and $\lambda = 22$. Here $k - \lambda = 23 > \lambda$ is a prime and therefore 23 is a multiplier. Now $(23 - 1, 91) = 1$, and so there is a difference set fixed by the multiplier 23. Of the 45 residues mod 91, let there be a_i congruent to i mod 7, where $i = 0, \ldots, 6$. Since $23 \equiv 2 \pmod{7}$,

$$a_1 = a_2 = a_4 = x,$$
$$a_3 = a_5 = a_6 = y,$$

and

$$a_0 + 3x + 3y = 45.$$

Now $\sum a_i a_{i+1} = 286$, which is the total number of differences congruent to 1 (mod 7). This yields

$$a_0(x + y) + x^2 + 3xy + y^2 = 286.$$

Moreover, the period of 23 mod 91 is 6. Hence a_0 is divisible by 6. Thus in the pair of equations

$$a_0 + 3x + 3y = 45,$$
$$a_0(x + y) + x^2 + 3xy + y^2 = 286$$

we need try only $a_0 = 0, 6, 12$. In no one of these cases do integer values for x and y exist, and hence for $v = 91$ there is no cyclic solution.

References

1. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., vol. 1 (1949), 88-93.

2. S. Chowla, *On difference sets*, Proc. Nat. Acad. Sci., vol. 35 (1949), 92-94.

3. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., vol. 2 (1950), 93-99.

4. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079-1090.

5. H. B. Mann, *Analysis and Design of Experiments* (New York, 1949).

6. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. and Phys., vol. 12 (1933), 311-320.

7. H. J. Ryser, *A note on a combinatorial problem*, Proc. Amer. Math. Soc., vol. 1 (1950), 422-424.

8. S. S. Shrikhande, *The impossiblity of certain symmetrical balanced incomplete block designs*, Ann. Math. Statist., vol. 21 (1950), 106-111.

9. James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377-385.

10. J. A. Todd, *A combinatorial problem*, J. Math. and Phys., vol. 12 (1933), 321-333.

Ohio State University