INTEGRAL p-adic NORMAL MATRICES SATISFYING THE INCIDENCE EQUATION

J. K. GOLDHABER

1. Introduction. The problem of arranging v elements into v sets in such a way that every set contains exactly k distinct elements and that every pair of sets has exactly $\lambda = k(k-1)/(v-1)$ elements in common, where $0 < \lambda < k < v$, is equivalent to finding a normal integral v by v matrix A such that $A^TA = B$, where B is the v by v matrix having k in every position on the main diagonal and λ in all other positions **(10)**. Utilizing the fact that for the existence of a λ, k, v design it is necessary that I (the v by v identity matrix) represent B rationally, **(2)** and **(3)** have proved the non-existence of certain λ, k, v designs. Neither of the proofs utilize the fact that it is necessary that A be normal. However, Albert **(1)** for the projective plane case and Hall and Ryser **(5)** for the general design proved that if there exists a rational A such that $A^TA = B$ then there exists a normal rational matrix satisfying the same equation. Thus the requirement of normality does not exclude any λ, k, v which were not previously excluded.

It is evident that for the existence of a λ, k, v design it is necessary that for every prime p there exist an integral p-adic normal matrix A satisfying $A^TA = B$. Assuming that $(k, k-\lambda) = 1$, we prove in § 2 that if I represents B rationally then this necessary condition is satisfied. Thus, once again, no additional designs are excluded. It does follow, however, that if I represents B rationally then I represents B without essential denominator and, furthermore, that there is a form in the genus of I which represents B integrally.

In § 3 we consider a modified incidence equation which is satisfied by every incidence matrix and which, if I represents B rationally, has integral solutions. Sufficient conditions for the existence of a λ, k v design in terms of these integral solutions are given.

2. The incidence equation examined locally. We assume throughout this paper that $(k, k-\lambda) = 1$. Thus, since $\lambda v = k^2 - (k-\lambda)$ we have $(\lambda, k) = (\lambda, k-\lambda) = (v, k) = (v, k-\lambda) = 1$. The matrices I and B are as above. We prove

THEOREM 1. *If I represents B rationally then for every prime p there exists a matrix A with elements in the ring $R(p)$ of p-adic integers such that $A^TA = AA^T = B$.*

Received November 3, 1958. Research supported in part by the Office of Ordinance Research under Contract DA-23-072-ORD-1051.

We show first that there exists a matrix C (not necessarily normal) with elements in $R(p)$ such that $C^TC = B$. It follows from well-known theorems on quadratic forms **(7)** and the fact that I and B are both positive definite that it is sufficient to show this for all primes $p \in P$, where P is the set of all prime divisors of $2\cdot\det B = 2k^2(k-\lambda)^{v-1}$. Let T be the v by v matrix

$$\begin{bmatrix} 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then

$$T^TT = \begin{bmatrix} v & 0 \\ 0 & I_1 + S_1 \end{bmatrix}$$

where I_1 is the $(v-1)$ by $(v-1)$ identity matrix and S_1 is the $(v-1)$ by $(v-1)$ matrix each of whose entries is 1. Also,

$$T^TBT = \begin{bmatrix} k^2v & 0 \\ 0 & (k-\lambda)(I_1+S_1) \end{bmatrix}.$$

Since $(k, k-\lambda) = 1$, v is a p-adic unit for all odd $p \in P$. v is also a 2-adic unit in the case that v is odd. Hence, for odd p, $X^TX = B$ is solvable in $R(p)$, $p \in P$, if and only if $X^T(T^TT)X = T^TBT$ is solvable in $R(p)$; and for odd v, $X^TX = B$ is solvable in $R(2)$ if and only if $X^T(T^TT)X = T^TBT$ is solvable in $R(2)$.

We first dispose of the case when v is even. Since I represents B rationally, $(k-\lambda)$ is a square **(3)**; whence, obviously T^TT represents T^TBT in $R(p)$ for all odd $p \in P$. Furthermore, since v is even and $(k, k-\lambda) = 1$ it follows that k and $k-\lambda$ are both odd. Thus I and B are properly primitive forms (that is, each has a 2-adic unit element on its main diagonal) with unit 2-adic determinants which, since they are rationally congruent, are congruent over the 2-adic field. Hence **(7**, Theorem 36**)** they are equivalent in $R(2)$. Thus, if v is even I represents B in $R(p)$ all $p \in P$.

Suppose now that v is odd. It is clearly sufficient to show that $I_1 + S_1$ represents $(k-\lambda)(I_1+S_1)$ in $R(p)$ for all $p \in P$.

(i) $I_1 + S_1$ represents $(k-\lambda)(I_1+S_1)$ in $R(2)$.

(a) Suppose $(k-\lambda) = 2^{2b}\, m$ where $b \geqslant 0$ and m is odd. We make use here, and below, of the following known theorem **(6)**:

Two improperly primitive forms (that is, each form has some 2-adic unit element but no 2-adic unit element on its main diagonal) in the same number

https://doi.org/10.4153/CJM-1960-011-9 Published online by Cambridge University Press

of variables and of odd determinants are equivalent in $R(2)$ if and only if their determinants are congruent mod 8.

From this it follows that $I_1 + S_1$ and $m(I_1 + S_1)$ are equivalent in $R(2)$. But then, obviously, $I_1 + S_1$ represents $2^{2b}\, m(I_1 + S_1)$ in $R(2)$.

(b) Suppose $k - \lambda = 2^{2b+1}m$ where m is odd. We shall show below that in this case the assumption that I represents B rationally implies that $v = \pm 1$ mod 8.

If $v \equiv 1$ mod 8 then $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent to the $\frac{1}{2}(v - 1)$ fold direct sum of the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Call the direct sum matrix K. It is thus sufficient to show that K represents $2^{2b+1}\, K$. Since $v \equiv 1$ mod 8, $4|v - 1$. Let L be the $\frac{1}{4}(v - 1)$ fold direct sum of

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}.$$

Then $(2^bL)^T\, K(2^bL) = 2^{b+1}\, K$ as desired.

If $v \equiv -1$ mod 8 then $I_1 + S_1$ and $m\ (I_1 + S_1)$ are both equivalent in $R(2)$ to $K_1 \oplus K_2$. Here $\oplus$ denotes direct sum, K_1 is the $\frac{1}{2}(v - 7)$ fold direct sum of

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

and K_2 is the 6 by 6 matrix having each entry on its main diagonal equal to 2 and all other entries equal to 1. Note that $4|v - 7$. Let L_1 be the $\frac{1}{4}(v - 7)$ fold direct sum of the 4 by 4 matrix given in the preceding paragraph, and let L_2 be the matrix

$$\begin{bmatrix} -1 & 0 & -1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then $[2^b(L_1 \oplus L_2)]^T\ (K_1 \oplus K_2)[2^b(L_1 \oplus L_2)] = 2^{2b+1}(K_1 \oplus K_2)$; whence, $I_1 + S_1$ represents $(k - \lambda)(I_1 + S_1)$ in $R(2)$ as desired.

It remains to show that if I represents B rationally and if $k - \lambda = 2^{2b+1}m$, m odd, then $v \equiv \pm 1$ mod 8. Since $\lambda v = k^2 - (k - \lambda)$ we have

$$\left(\frac{k-\lambda}{\lambda}\right) = \left(\frac{2}{\lambda}\right)\left(\frac{m}{\lambda}\right) = 1,$$

where (a/b) is the Jacobi symbol. (Since $(k, k-\lambda) = 1$, λ is odd.) We thus have

$$\left(\frac{\lambda}{m}\right) = \left(\frac{2}{\lambda}\right)(-1)^{\frac{m-1}{2}\cdot\frac{\lambda-1}{2}}.$$

We consider the cases $b \geqslant 1$, $b = 0$ separately.

If $b \geqslant 1$ then $\lambda \equiv v \bmod 8$. If $v = 3 \bmod 8$ then $(-\lambda/m) = -1$ but this is impossible since I represents B rationally **(3)**. The case $v \equiv 5 \bmod 8$ is disposed of similarly.

If $b = 0$ then $\lambda v \equiv -1$ or $3 \bmod 8$ according as $k - \lambda \equiv 2$ or $6 \bmod 8$. If $k - \lambda \equiv 2 \bmod 8$ and $v \equiv 3 \bmod 8$ then $(-\lambda/m) = -1$ which is impossible. Similar easy computations exclude all possibilities other than $v \equiv \pm 1 \bmod 8$.

(ii) $I_1 + S_1$ represents $(k-\lambda)(I_1 + S_1)$ in $R(p)$ for all odd p such that $p|k$. We make use here, and below, of the following known theorem **(6**, 11**)**. For odd p, two forms, f and g, in the same number of variables and of unit determinants in $R(p)$ are equivalent in $R(p)$ if and only if

$$\left(\frac{\det f}{p}\right) = \left(\frac{\det g}{p}\right).$$

The desired result is an immediate consequence of this theorem. We actually have somewhat more; namely, $I_1 + S_1$ represents $(k - \lambda)$ $(I_1 + S_1)$ in $R(p)$ for all odd p such that $p \nmid (k - \lambda)v$.

(iii) $I_1 + S_1$ represents $(k - \lambda)$ $(I_1 + S_1)$ in $R(p)$ for all odd p such that $p|(k - \lambda)$. Suppose $(k - \lambda) = p^b m$ where $(p, m) = 1$ and $b > 0$. We consider two cases: (a) $v \equiv 1 \bmod 4$, and (b) $v \equiv 3 \bmod 4$.

(a) Since I represents B rationally we must have $(v/p) = (\lambda/p) = 1$, **(2)**. Thus det $(I_1 + S_1) = v$ and det $[m(I_1 + S_1)] = m^{v-1}v$ are both units and perfect squares in $R(p)$. Therefore, $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent in $R(p)$ to I_1. It is thus sufficient to show that I_1 represents $p^b I_1$ in $R(p)$. If b is even, this is obvious. Suppose then that $b = 2c + 1$. We use the device employed in **(3)**. There exist integers a_i, $i = 1, 2, 3, 4$, such that $\sum_1^4 a_i^2 = p$. Let L be the $\frac{1}{4}(v - 1)$ fold direct sum of

$$p^c \cdot \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & -a_4 & a_3 \\ a_3 & a_4 & -a_1 & -a_2 \\ a_4 & -a_3 & a_2 & -a_1 \end{bmatrix}.$$

Then $L^T L = p^{2c+1} I_1$ as desired.

(b) For $v \equiv 3 \bmod 4$ we must have

$$\left(\frac{v}{p}\right) = \left(\frac{\lambda}{p}\right) = (-1)^{\frac{p-1}{2}},$$

(3). Thus $I_1 + S_1$ and $m(I_1 + S_1)$ are both equivalent to the $(v-1)$ $(v-1)$ diagonal matrix $[1, 1, \ldots, 1, (-1)^{\frac{1}{2}p-\frac{1}{2}}] = J$. We must show that J represents $p^b J$. For even b this is obvious and so we may take $b = 2c + 1$. If $p \equiv 3 \bmod 4$ then let L_1 be the $\frac{1}{4}(v-3)$ fold direct sum of the 4 by 4 matrix given in the previous paragraph and let

$$L_2 = p^c \begin{bmatrix} a & 1 \\ 1 & a \end{bmatrix}$$

where a is a p-adic integer such that $a^2 = 1 + p$. Then $[(L_1 \oplus L_2)]^T J[(L_1 \oplus L_2)] = p^b J$. If $p = 1 \bmod 4$ then there exist integers a_1 and a_2 such that $a_1^2 + a_2^2 = p$. Let L be the $\frac{1}{2}(v-1)$ fold direct sum of

$$p^c \begin{bmatrix} a_1 & a_2 \\ a_2 & -a_1 \end{bmatrix}.$$

Then $L^T J L = p^b J$.

It follows from all the above that for every p there exists a matrix C with elements in $R(p)$ such that $C^T C = B$. It remains to show that there exists a normal matrix with the desired properties. If $p \nmid v$ this is clear. In fact, we have seen above that for every $p \nmid v$ there exists a C_1 with elements in $R(p)$ such that $C_1^T\ (I_1 + S_1)\ C_1 = (k - \lambda)(I_1 + S_1)$. Let $A = T(k \oplus C_1)\ T^{-1}$. Then $A^T A = B$ and $AS = kS$, where S is the v by v matrix composed entirely of ones; whence by **(5**, Theorem 3.1**)** A is normal. Since $p \nmid v$, A has its elements in $R(p)$.

Suppose $p|v$. We know that there exists a matrix $C = (c_{ij})$ with elements in $R(p)$ such that $C^T\ C = B$. Let α be the column vector $[r_1, r_2, \ldots, r_v]$ where $r_i = \sum_j c_{ij}$, and let β be the v by 1 column vector each of whose entries is k. We will show that there exists an orthogonal matrix O with elements in $R(p)$ such that $O\alpha = \beta$. It will follow that $A = OC$ is such that $A^T A = B$, $AS = kS$; and again by **(5)**, A is normal as desired.

We use the following theorem **(4**, Satz 10.4**)**. It is stated here more concretely and in a less general form that in **(4)**.

Let V be a v dimensional vector space of column vectors over the p-adic field with a non-degenerate ground form given by the v by v symmetric matrix G. Let $\mathscr{F}$ be a lattice in V and let $\mathscr{D}$ be its different. If α and β are primitive vectors in $\mathscr{F}$ such that $\alpha^T G \alpha = \beta^T G \beta$ and $\alpha - \beta \in \mathscr{D}$ then there exists a v by v matrix O with elements in $R(p)$ such that $O^T G O = G$ and $O\alpha = \beta$.

For our purposes we take G to be the identity matrix, $\mathscr{F}$ as the lattice which has as a basis the column vectors of the identity matrix I, and α and β as above. We note that if p is odd then $\mathscr{D} = \mathscr{F}$, and if $p = 2$ then $\mathscr{D}$ is the lattice which has as a basis the column vectors of $2I$. From the fact that $C^T C = B$ it follows easily **(10)** that $\sum_j c_{ji}\, r_j = k^2$ and $\sum_i r_i^2 = k^2 v$. From the first of the latter equations and the facts that $p|v$, $(k, v) = 1$ it follows that α and β are both primitive. From the second of these equations it follows that $\alpha^T \alpha = \beta^T \beta$. Hence if p is odd the desired O exists.

https://doi.org/10.4153/CJM-1960-011-9 Published online by Cambridge University Press

In order to complete the proof for $p = 2$ it is sufficient to show that $r_i^2 \equiv 1$ mod 2. Let t_{ij} be the inner product of the ith and jth rows of C. Again as in **(10)** we have

$$k^2 t_{ij} = \lambda r_i r_j + k^2(k - \lambda)\,\delta_{ij}.$$

If $r_i^2 \equiv 0$ mod 2 then $t_{ii} \equiv 1$ mod 2 and we would have

$$0 \equiv r_i^2 \equiv \sum_j c_{ij}^2 \equiv t_{ii} \equiv 1 \bmod 2$$

which is clearly absurd.

This completes the proof of Theorem 1.

As immediate consequences we have

COROLLARY 1. *If I represents B over the rational field then I represents B rationally without essential denominator, that is, for every positive integer m there is a matrix D with rational elements whose denominators are prime to m such that $D^TD = B$.*

COROLLARY 2. *If I represents B rationally then there exists a form in the genus of I which represents B integrally.*

3. A modified incidence equation. Since the genus of the identity contains more than one class for $v > 8$ **(8)** Corollary 2 does not yield any new designs. It is natural, therefore, to examine a matric equation, akin to $X^TX = B$, which is still satisfied by every incidence matrix, has integral solutions, and then to examine the relationship of these integral solutions to incidence matrices.

THEOREM 2. *Let $t = a/b$ be a rational number greater than $1/v$ such that $(av - b)b$ is odd. Let S be the v by v matrix composed entirely of ones. If I represents B rationally then $I - tS$ represents $B - tk^2S$ integrally.*

For by Theorem 1, $bI - aS$ represents $bB - ak^2S$ in every $R(p)$. (The normality of A implies that $SA = AS = kS$ and therefore $A^T(bI - aS)\,A = bB - ak^2S$.) Hence there exists a form in the genus of $bI - aS$ which represents $bB - ak^2S$ integrally. Since the genus of an indefinite form of odd determinant in $v > 2$ variables consists of exactly one class **(9)** Theorem 2 follows.

Let $\mathscr{S}$ be the set of all rationals which have the properties stated in Theorem 2. For $t \in \mathscr{S}$ let $A(t) = (a_{ij}(t))$ denote an arbitrary but fixed integral solution of $X^T(I - tS)X = B - tk^2S$. Let $r_i(t) = \sum_j a_{ij}(t)$, and $s_j(t) = \sum_i a_{ij}(t)$.

THEOREM 3: (i) *If $A(t_0)$ is normal and $t_0 \neq (k + (k - \lambda)^{\frac{1}{2}})/kv$ then $A(t_0)$ is an incidence matrix or the negative of one.*

(ii) *If for $t_1, t_2 \in \mathscr{S}$, $t_1 \neq t_2$ we have $r_i(t_1) = r_i(t_2)$ $(s_i(t_1) = s_i(t_2))$ for $i = 1, 2, 3, \ldots, v$, then $A(t_1)$ is an incidence matrix or the negative of one.*

(iii) *If there exists an M and a subset $\mathscr{S}'$ of $\mathscr{S}$ containing sufficiently many distinct elements (see below) such that $|r_i(t)| < M(|s_i(t)| < M)$ for $t \in \mathscr{S}'$ and*

https://doi.org/10.4153/CJM-1960-011-9 Published online by Cambridge University Press

$i = 1, 2, \ldots, v$ *then there exists a* $t_0 \in \mathscr{S}'$ *such that* $A(t_0)$ *is an incidence matrix or the negative of one.*

(iv) *If* $r_i(t_0) > 0$ *for* $i = 1, 2, \ldots, v$ *and for* $t_0 > 1$ *then* $A(t_0)$ *is an incidence matrix.*

(i) As in **(10)** the following relations may be established: For every $t \in \mathscr{S}$,

$$\sum r_i^2(t) - t\Big(\sum r_i(t)\Big)^2 = k^2 v(1 - tv)$$

$$k^2(1 - tv)\Big(\sum s_i^2(t)\Big) + (k^2 t - \lambda)\Big(\sum r_i(t)\Big)^2 = k^2(k - \lambda)v.$$

Now the normality of $A(t_0)$ implies that $\sum r_i^2(t_0) = \sum s_i^2(t_0)$. Since $t_0 \neq (k + (k - \lambda)^{\frac{1}{2}})/kv$, the above equations imply that $\sum r_i^2(t_0) = k^2 v$ and $\sum s_i(t_0) = \sum r_i(t_0) = \pm kv$. Whence $r_i(t_0) = s_i(t_0) = k$ or $r_i(t_0) = s_i(t_0) = -k$ for all i. But then $A^T A = AA^T = B$ and the result follows by **(10**, Theorem 2.1**)**.

(ii) The proof of this result is analogous to the proof of (i).

(iii) The number of lattice points in v dimensional space over the reals with components having absolute value less than M is finite. Hence if $\mathscr{S}'$ contains more elements than the number of such lattice points then there exist $t_1, t_2 \in \mathscr{S}'$, $t_1 \neq t_2$, such that $r_i(t_1) = r_i(t_2)$ for $i = 1, 2, \ldots, v$. The desired result follows from (ii).

(iv) Once again as in **(10)** it may be shown that $r_i(t) \equiv 0 \bmod k$. Since $r_i(t) > 0$ it follows that

$$\Big(\sum r_i(t)\Big)^2 \geqslant \Big(\sum r_i^2(t)\Big) + v(v - 1)k^2.$$

From the first of the equation given in (i) above it follows that

$$k^2 v(1 - t) \leqslant (1 - t) \sum r_i^2(t).$$

Since $t > 1$ we have $\sum r_i^2(t) \leqslant k^2 v$. But also

$$k^2 v^2 \leqslant (\sum r_i(t))^2 \leqslant v(\sum r_i^2(t)).$$

Hence $\sum r_i^2(t) = k^2 v$ and the proof may be completed as was the proof of (i).

We remark that if $v > k + 1$ and $t > 1$ then $r_i(t) \neq 0$ for $i = 1, 2, \ldots, v$.

Theorem 3 gives sufficient conditions for the existence of a λ, k, v design in terms of integral solutions, which by Theorem 2 are known to exist, of the matric equation

$$X^T(I - tS)X = B - tk^2 S.$$

The problem of determining the nature of these solutions appears to be extremely difficult. Also of interest, and possibly a more pliable problem, is the determination of the integral automorphs of $I - tS$ and $B - tk^2 S$.

References

1. A. A. Albert, *Rational normal matrices satisfying the incidence equation*, Proc. Amer. Math. Soc., *4* (1953), 554–9.
2. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., *1* (1949), 88–93.
3. S. Chowla and H. J. Ryser, *Combinational problems*, Can. J. Math., *2* (1950), 93–9.
4. M. Eichler, *Quadratische formen und orthogonale gruppen* (Berlin, 1952).
5. Marshall Hall and H. J. Ryser, *Normal completions of incidence matrices*, Amer. J. Math., *76* (1954), 581–9.
6. B. W. Jones, *A canonical quadratic form for the ring of 2-adic integers*, Duke Math. J., *11* (1944), 715–27.
7. ——— *The arithmetic theory of quadratic forms*, Carus Math. Monographs, *10* (1950).
8. W. Magnus, *Ueber die Anzahl der in einem Geschlecht enthaltenen Klassen von positiv definiten quadratischen Formen*, Math. Ann. *114* (1937), 465–75.
9. A. Mayer, Zürich naturf. Ges., *36* (1891), 241.
10. H. J. Ryser, *Matrices with integer elements in combinational investigations*, Amer. J. Math., *74* (1952), 769–73.
11. C. L. Siegel, *Equivalence of quadratic forms*, Amer. J. Math. *63* (1941), 658–80.

Washington University

https://doi.org/10.4153/CJM-1960-011-9 Published online by Cambridge University Press