RATIONAL NORMAL MATRICES SATISFYING THE INCIDENCE EQUATION

A. A. ALBERT

1. Introduction. An incidence matrix A of a finite projective plane of order m is an n-rowed square matrix A with nonnegative integral elements such that

$$B = AA' = mI + N, \tag{1}$$

where $n = m^2 + m + 1$, I is the n-rowed identity matrix, and all elements of N are 1. It can then be shown that every element of A is either 0 or 1, that there are precisely $m+1$ nonzero elements in every row and column of A, and that it follows that

$$A'A = B. \tag{2}$$

Thus an incidence matrix is a *normal* integral matrix satisfying the *incidence equation* (1).

The following result is also known:[1]

Bruck-Ryser Theorem. *Let* $m \equiv 1, 2 \pmod 4$, *and let there exist a rational matrix* P *satisfying the incidence equation* $PP' = mI + N$. *Then* m *is a sum of two squares.*

The converse of this theorem is also true and provides what may be thought of as a rational approximation to an incidence matrix. The purpose of this note is that of giving a constructive proof of the following closer approximation.

Theorem. *Let* m *be a sum of two squares. Then there exists a normal matrix* S *with rational elements such that* $SS' = mI + N$.

2. Algebraic properties. If $PP' = SS' = B$, then $(P^{-1}S)(P^{-1}S)' = I$. Hence, if P and S are any two solutions of the incidence equation, there exists an orthogonal matrix C such that

$$S = PC. \tag{3}$$

When P and S are rational solutions the orthogonal matrix C must also be rational. Conversely if $S = PC$, where C is orthogonal and P satisfies the incidence equation, then S satisfies the incidence equation. We note the following stronger result:

Received by the editors November 17, 1952.

[1] See R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian Journal of Mathematics vol. 1 (1949) pp. 88–93.

LEMMA 1. *The matrix $S=PC$ is normal if and only if $C'P'PC=PP'$. When S is a normal solution of the incidence equation the matrix $T=SG$ is also a normal solution if and only if G is an orthogonal matrix such that the sum of the elements in every row and column of either G or $-G$ is* 1.

For if S is normal we see that $SS'=PP'=S'S=C'(P'P)C$. If $T=SG$ is a second normal solution, then $T'T=G'S'SG=TT'=G'(SS')G$, that is, $G'BG=B$. But $B=mI+N$, and the orthogonal matrix G commutes with B if and only if

$$(4) \qquad GNG' = N, \qquad GN = NG.$$

However

$$(5) \qquad N = u'u, \qquad u = (1, 1, \cdots, 1),$$

and (4) is equivalent to

$$(6) \qquad N = v'v, \qquad v = uG.$$

The ith element of the row vector v is the sum s_i of the elements in the ith column of G, and (6) implies that $s_is_j=1$. Hence $s_i^2=1$ and $s_i=1$ or -1. Since $s_is_j=1$ the sums s_i have the same sign and are equal. The second form of (4) implies that the sum of the elements in the ith row of G is equal to the column sum s_i, and our result is proved.

3. A rational solution and a basic equation.

We shall assume henceforth that

$$(7) \qquad m = a^2 + b^2,$$

for integers a and b. Then the n-rowed square matrix

$$(8) \qquad P = \begin{pmatrix} 0 & c & c & \cdots & c \\ d' & H & 0 & \cdots & 0 \\ d' & 0 & H & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ d' & 0 & 0 & \cdots & H \end{pmatrix}$$

defined by the formulas

$$(9) \qquad c = \left(\frac{a-b}{m}, \frac{a+b}{m}\right), \qquad d = (1, 1), \qquad H = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is a solution of the incidence equation. Indeed the length of the first row of P is $kcc'=km^{-2}[(a-b)^2+(a+b)^2]=2km^{-2}m=m+1$, where we have introduced the notation

$$k = \frac{m^2 + m}{2}. \tag{10}$$

The length of every other row is $1+a^2+b^2=1+m$ and so the diagonal elements of PP' are $m+1$. The inner product of the ith row of P and the jth row is 1 trivially for $i>j>1$. The remaining inner products are $[a(a-b)+b(a+b)]m^{-1}=(a^2+b^2)m^{-1}=1$ and $[-b(a-b)+a(a+b)]m^{-1}=1$, and so we have proved that

$$PP' = B. \tag{11}$$

Let us now compute

$$P'P = mI + M. \tag{12}$$

By direct computation using (8) we see that

$$M = \frac{1}{m^2} w'w, \tag{13}$$

where

$$w = (m^2, a - b, a + b, \cdots, a - b, a + b). \tag{14}$$

Observe that $ww'=m^4+k[(a-b)^2+(a+b)^2]=m^4+m(m^2+m)$, that is,

$$ww' = m^2n. \tag{15}$$

We shall attempt to find a rational orthogonal matrix C such that PC is a normal matrix. Our success will depend on a rational solution of the equation $x^2-my^2=-n$, and we shall write the result as

$$t^2 - ms^2 = - na^2, \tag{16}$$

for *integers* s and t. To compute s and t we note that $(m+1)^2-m(1)^2=m^2+2m+1-m=n$, and that $b^2-m(1)^2=-a^2$. But then $(m+1+m^{1/2})(b+m^{1/2})=t+sm^{1/2}$ where

$$t = b(m + 1) + m, \qquad s = b + (m + 1). \tag{17}$$

It should now be clear that $t^2-ms^2=-na^2$.

4. A rational normal solution. We shall determine C as the product $C_1'C_0$, where C_0 and C_1 are orthogonal matrices such that

$$C_0NC_0' = C_1MC_1' = \begin{pmatrix} 0 & 0 \\ 0 & n \end{pmatrix}. \tag{18}$$

Moreover

$$C_0 = D_0^{-1}E_0, \qquad C_1 = D_1^{-1}E_1, \tag{19}$$

where E_0 and E_1 will be taken to be *integral* matrices, D_0 and D_1 will be taken to be *diagonal* matrices. It will then follow that

$$C = E_1'(D_0D_1)^{-1}E_0 \tag{20}$$

will be rational if and only if D_0D_1 is rational.

Write

$$\begin{aligned} p_1 &= (0, 1, 0, -1, 0, \cdots, 0), \\ p_2 &= (0, 1, 0, 1, 0, -2, \cdots, 0), \\ p_i &= (0, 1, 0, 1, 0, 1, \cdots, 0, 1, 0, -i, 0, \cdots, 0), \cdots, \\ p_{k-1} &= (0, 1, 0, 1, \cdots, 0, 1, 0, 1-k, 0). \end{aligned} \tag{21}$$

Thus p_i has i elements 1, followed by the element $-i$, and these elements are separated by zeros. Since the rows of N are all equal it should be clear that $p_iN=0$. But it is actually evident that

$$p_iN = p_iM = 0. \tag{22}$$

Similarly we write

$$q_j = (0, 0, 1, 0, 1, \cdots, 0, 1, 0, -j, \cdots, 0) \quad (j = 1, \cdots, k-1) \tag{23}$$

and have

$$q_jN = q_jM = 0. \tag{24}$$

Define

$$E_0 = \begin{bmatrix} p_1 \\ \cdot \\ \cdot \\ \cdot \\ p_{k-1} \\ q_1 \\ \cdot \\ \cdot \\ \cdot \\ q_{k-1} \\ x \\ y \\ u \end{bmatrix}, \qquad E_1 = \begin{bmatrix} p_1 \\ \cdot \\ \cdot \\ \cdot \\ p_{k-1} \\ q_1 \\ \cdot \\ \cdot \\ \cdot \\ q_{k-1} \\ z \\ v \\ w \end{bmatrix}, \tag{25}$$

where we have already defined $k=(m^2+m)/2$, $u=(1, 1, \cdots, 1)$, and $w=(m^2, a-b, a+b, \cdots, a-b, a+b)$. Define

(26) $$z = (0, a+b, b-a, a+b, b-a, \cdots, a+b, b-a)$$

and

(27) $$v = (-m-1, a-b, a+b, a-b, a+b, \cdots, a-b, a+b).$$

The first $n-3$ rows of E_0 coincide with those of E_1 and are clearly pairwise orthogonal characteristic vectors of both N and M. The condition that a vector $x=(x_1, \cdots, x_n)$ shall be orthogonal to $p_1, \cdots, p_{k-1}, q_1, \cdots, q_{k-1}$ is that

(28) $$x_2 = x_4 = x_6 = \cdots = x_{n-1}, \qquad x_3 = x_5 = \cdots = x_n,$$

and w, z and v satisfy this condition. By (13) we have

(29) $$zM = \frac{1}{m^2}(zw')w = 0, \qquad vM = \frac{1}{m^2}vw'w = 0,$$
$$wM = \frac{1}{m^2}w(w'w) = nw,$$

where it should be clear that $zw' = k[(a+b)(a-b)+(b-a)(a+b)] = 0 = zv'$ and that $vw' = -m^2(m+1)+k(2m) = -m^2(m+1)+(m^2+m)m = 0$.

It remains to compute the lengths of the rows of E_1. Clearly $p_ip_i' = i+i^2 = i(i+1) = q_iq_i'$. Next we see that $zz' = k[(a+b)^2+(a-b)^2] = 2km = m^2(m+1)$ and that $vv' = (m+1)^2+2km = (m+1)(m+1+m^2) = n(m+1)$. We have proved the following result:

LEMMA 2. *Let E_1 be given by* (25) *and D_1 be the diagonal matrix*

(30) $$D_1 = \operatorname{diag}\{(1\cdot 2)^{1/2}, (2\cdot 3)^{1/2}, \cdots, ((k-1)k)^{1/2}, (1\cdot 2)^{1/2}, (2\cdot 3)^{1/2}, \cdots, ((k-1)k)^{1/2}, m(m+1)^{1/2}; (n(m+1))^{1/2}, mn^{1/2}\}.$$

Then $C_1 = D_1^{-1}E_1$ is an orthogonal matrix such that C_1MC_1' satisfies (18).

We next write $x=(x_1, \cdots, x_n)$ where

(31) $$x_1 = -2ak, \; x_2 = x_4 = \cdots = x_{n-1} = a+t,$$
$$x_3 = x_5 = \cdots = x_n = a-t.$$

Then $xx' = 4a^2k^2+2k(a^2+t^2) = (m^2+m)[(m^2+m+1)a^2+t^2] = (m^2+m)(na^2+t^2)$. By (16) we have the value

(32) $$xx' = m^2s^2(m+1).$$

We similarly write $y=(y_1, \cdots, y_n)$, $y_2=y_4= \cdots =y_{n-1}$, $y_3=y_5 = \cdots = y_n$ where

(33) $$y_1 = -2kt, \qquad y_2 = t-na, \qquad y_3 = t+na.$$

Then $yy'=4k^2t^2+k[(t-na)^2+(t+na)^2]=(m^2+m)[(m^2+m)t^2+t^2+n^2a^2]=(m^2+m)(nt^2+n^2a^2)$. Using (16) we have

$$yy' = m^2s^2n(m+1). \tag{34}$$

The first $n-3$ rows of E_0 are already known to be pairwise orthogonal and orthogonal to x, y, u. It should now be clear that since $xu' = -2ka+k(a+t+a-t)=0$ and $yu'=-2kt+k[t-na+t+na]=0$ the vectors x, y are orthogonal characteristic vectors of $N=u'u$. Moreover

$$\begin{aligned} xy' &= (-2k)^2at + k[(a+t)(t-na)+(a-t)(t+na)] \\ &= 4k^2at + k(t^2+at-na^2-nat+at-t^2+na^2-nat) \\ &= 4k^2at + 2kat(1-n) = 0 \text{ since } 1-n = -(m^2+m) = -2k. \end{aligned}$$

This completes our proof of the fact that the rows of the matrix E_0 form a set of n pairwise orthogonal characteristic vectors of N. Define

$$\begin{aligned} D_0 = \operatorname{diag}\{&(1\cdot 2)^{1/2}, (2\cdot 3)^{1/2}, \cdots, ((k-1)k)^{1/2}, (1\cdot 2)^{1/2}, \\ &(2\cdot 3)^{1/2}, \cdots, ((k-1)k)^{1/2}, ms(m+1)^{1/2}, ms(n(m+1))^{1/2}, n^{1/2}\}, \end{aligned} \tag{35}$$

and see that

$$\begin{aligned} D = D_0D_1 = \operatorname{diag}\{&1\cdot 2, 2\cdot 3, \cdots, k^2-k, 1\cdot 2, 2\cdot 3, \cdots, \\ &k^2-k, m^2s(m+1), msn(m+1), mn\} \end{aligned} \tag{36}$$

is an integral matrix. We have shown that for this D the matrix

$$C = E_1'D^{-1}E_0 \tag{37}$$

is a rational orthogonal matrix, and PC is a rational normal solution of the incidence equation. This completes our constructive proof.

THE UNIVERSITY OF CHICAGO