*Revista Colombiana de Matemáticas*
*Volumen III ( 1969) , págs. 45 - 50*

# A NOTE ON SYMETRIC MATRICES

by

**Nelo D. ALLAN**

This is an expository note with the purpose of proving some facts which will be used in my next paper. These facts are mentioned in [1] and one of them is a special case of the well known theorem of Meyer.

1. let $Q$ be the field of all rational numbers, and $Z$ be the ring of integers. We shall denote by $M_n(S)$ the set of all $n$ matrices with coeficients in a ring $S$. We shall say that $H \in M_n(Z)$ is unimodular if $H$ is a unit of this ring, i. e., the determinant, $det\ H$, is $\pm 1$. $H$ is symmetric if it coincides with its transpose ${}^tH$. For the sake of convenience we shall write $H = V \perp W$ if written in blocks,

$$H = \begin{bmatrix} V & 0 \\ 0 & W \end{bmatrix}$$

and we set $H_{(m)} = H \perp \ldots \perp H$ $m$ times. We set

$$J(a) = \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}, \quad a \in Z$$

and $J(0) = J$. We say that $H, H' \in M_n(Z)$ are integrally equivalent, shortly $H \sim H'$, if there exists $U \in M_n(Z)$, unimodular, such that $H' = {}^tUHU$. We say that $H$ is even if for all integral $n$ by $1$ matrices $x$, the values of the form $H(x) = {}^txHx$ are always even ; otherwise we say that $H$ is odd. We shall say that $H$ *represents zero* if the equation $H(x) = 0$ has a non trivial integral solution. Over the reals, $R$, $H$ can be diagonalized to a matrix

$$E_r \perp (-E_s),$$

where in general $E_m$ is the $m$ by $m$ identity matrix ; the difference $\mu = r-s$ is called the *index* of $H$, and for our purpose we can always replace $H$ by $-H$ and assume $\mu \geqslant 0$. We say that $H$ is indefinite if $\mu \neq 0$, and that $H$ is definite otherwise. We shall use essentially the following result.

*THEOREM 1. An indefinite unimodular symmetric matrix with 5 or more variables always represents zero. If* $H$ *is definite, unimodular and even, then* $n \equiv 0 \mod 8$ *; if* $H$ *is odd and* $n \leqslant 7$ *, then* $H \sim E_n$ *.*

Our first objetive is to prove (see [3] )

*THEOREM 2 : Let* $H$ *be an unimodular symmetric matrix, with* $n > 5$ *and* $\mu > 4$ *. If* $H$ *is odd then* $H$ *is equivalent to* $J_{(m)} \perp E_\mu$ *or* $J_{(m)} \perp J(1)$ *according to whether* $\mu \neq 0$ *or not ; if* $H$ *is even, then* $H \sim J_{(m)} \perp W$ *where* $W$ *is even ond definite .*

Actually if we apply the theorems 4 and 5 in [3], then theorem 2 can be easily derived as follows :

*THEOREM 3 : Let* $H$ *be unimodular and indefinite. If* $H$ *is odd, then* $H$ *is equivalent, to either* $J_{(m)} \perp E_\mu$ *or* $J_{(m)} \perp J(1)$ *according to whether* $\mu \neq 0$ *or* $\mu = 0$ *. In the even case* $H \sim J_{(m)} \perp (\phi_8)_{(s)}$ *where* $\phi_8$ *is a representative of the only positive even definite class of rank 8.*

2. We shall break the proof in several lemmas ; we shall assume that $H$ is unimodular, indefinite and $n \geqslant 5$, in all these lemmas.

*LEMMA 1 :* $H \sim J(a) \perp H'$ *, and index of* $H'$ *is the same as index of* $H$*.*

*PROOF :* Let $x$ be a solution of $H(x) = 0,\ x \neq 0$, which we may assume to be primitive , i. e. , to have entries relatively prime. Extend $x$ to an unimodular matrix $U$ where $x_1 = x$ is its first column and $x_i$ is its i-th column ; we set $H_1 = {}^tU H U$ . If

$$H_1 = (b_{ij}) ,\ b_{ij} = x_i H x_j = H_1(x_i , x_j)$$

then $H_1(x) = b_{11} = 0.$ Next we can find $c_2 , \dots , c_n \in Z$ such that $c_2 b_{21} + \dots + c_n b_{n1} = 1$; we set $x'_2 = c_2 x_2 + \dots + c_n x_n$ and $x'_j = x_j - b_{1j} x_2$ , $j=3 , \dots n$ , we get $H_1(x'_1 , x'_2) = 1$ and $H_1(x'_1 , x'_j) = 0$ , $j \geqslant 2$ . Now if $U_1$ denotes the unimodular matrix whose i-ith column is $x'_i$, $i=1 , \dots n$ and $x'_{11} = x_1$ , and if $H_2 = {}^tU_1 H_1 U_1$ , then $H_2 = (b_{ij})$ and $b_{1j} = 0$ or 1 according to whether $j \neq 2$ or not. Now symmetry implies that $b_{12} = b_{21}$, and if we replace $x'_j$ by $x''_j = x'_j - b_{2j} x'_1$ , $j > 3$ we get $H_1(x''_2 , x''_j) = 0$ ; denoting by $U_2$ the matrix whose j-th column is $x''_j$, $j = 1 , \dots , n$, $x''_1 = x_1$ , $x''_2 = x'_2$ , we get $H \sim J(a) \perp H'$ . The invariance of the index follows from the fact that the index of $J(a)$ is zero.

q.e.d.

*LEMMA 2 :* 1. $J \perp E_1 \sim J(1) \perp E_1$

2. $J(a) \perp J(b) \sim J_{(2)}$ or $J \perp J(1)$

*according to whether a and b are both even or not.*

*PROOF :* Let $H = J(1) \perp E_1$ and let us denote by $e_j$ the $j$-*th* column of $E_n$. If $U$ has column $e_1, e_2+e_3, e_3-e_1$, we get that ${}^tU\,H\,U = J(2) \perp E_1$.
Now from

$$ {}^tUJ(a)\,U = J(a+2\lambda), \quad U = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} $$

we get $J(a) \sim J(0)$ or $J(1)$ according to whether a is even or odd. Consequently it remains only to study the case where a and $b$ are both odd, i.e.,

$$ J(a) \perp J(b) \sim J(1) \perp J(1) ; $$

here we consider the column of $U$ to be $e_1, e_2, e_2+e_4, e_3-e_1$ to get

$$ {}^tUHU \sim J(2) \perp J(1) \sim J \perp J(1) . $$

q.e.d.

*LEMMA 3 :* $H = J(1) \perp V \sim J \perp E_m$, *if* $V$ *is positive definite* $m$ *by* $m$ *with* $m > 4$.

*PROOF :* In any case $H$ represents 1, i.e., there exists $x$ primitive such that $Q(x) = 1$; extending $x$ to an unimodular matrix $U$ we may assume that $H = (b_{ij})$ and $b_{11} = 1$. Now replacing $x_j$ by $x_j - b_{i1}x_1$ we get

$$ H(x_j, x_1) = 0 \quad , \; j > 1 ; $$

hence by lemmas 1 and 2

$$ H \sim E_1 \perp V' \sim E_1 \perp J(a) \perp V'' \sim E_1 \perp J(1) \perp V'' . $$

We can repeat the process as long as $m > 4$; in the case $m = 4$ we have

$$ H \sim E_1 \perp J(1) \perp V' , $$

$V'$ being 3 by 3, hence $V' \sim E_3$.

q.e.d.

*LEMMA 4 : If* $H = J \perp V$, *$V$ odd and definite, then* $H \sim J \perp E_m$ *provided that* $m \geqslant 4$.

*PROOF :* Clearly $H$ represents 1, and as is the above lemma

$$ H \sim E_1 \perp H' \sim E_1 \perp J(a) \perp V' \sim E_m \perp J $$

q.e.d.

Before procceding we would like to remark that he hypothesis $m \geq 4$ can be easily removed due to a very simple proof [3] theorem, which states that if $n \leq 5$ and $H$ is indefinite, then $H$ represents zero non trivially.

*PROOF OF THEOREM 2 :* By applying lemmas 1 and 2 several times we arrive to $H \sim J_{(q)} \perp J(a) \perp V$, with $H$ and $V$ having the same index $\mu \geq 4$. If $V$ is indefinite, then as $n = 2s+\mu$ we must have $s \neq 0$, hence $n \geq 6$ and the process can be repeated. Hence may assume $V$ to be definite. If $V$ is odd, then lemmas 3 and 4 implies $V \sim E_{\mu}$. If $V$ is even and $a$ even, i.e., $H$ even, we are done. If $a$ is odd we have

$$J(a) \perp V \sim J(1) \perp V \sim J \perp E_m$$

by lemma 3.

q.e.d.

We would like to remark that the even case in theorem 2 is stated as in [3], which after had proved the odd case, its proof becomes simple. In [3], it is proved that $H$ odd implies that $H \sim E_p \perp (-E_q)$. The statement of theorem 2 will clearly follow from $E_1 \perp (-E_1) \sim J(1)$ and from lemma 2.

3. Closing this note we shall prove the following:

*THEOREM 3 : There exist an unimodular matrix $U \in M_n(Z)$ such that*

$$^tU\,U = V = (v_{ij}),\ V \equiv J_{(q)} \perp A \quad modulo\ 2,$$

*where $A = J(1)$ or $E_1$ according to whether $n$ is even or odd. If $n$ is even (resp. odd) we can choose $U$ such that $v_{n-1,\,n-1} = n$ (resp. $v_m = n$) and $V \sim V' \perp J(1)$ modulo $2^a$ where $a = ord_2(n)$.*

*PROOF :* We shall procced by induction on $n$. If $n = 1$, $V = E_1$, and if $n = 2$ we can take.

$$U = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad and \quad V = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Assume the assertion true for all $k < n$. Let us treat the case where $n$ is odd. We write $E_n = E_{n-1} \perp E_1 \sim V' \perp E_1$, $V = (v_{ij}) = {}^tU'U'$, where $U'$ is chosen by induction and $v_{n-2,n-2} = n-1$, $V' \equiv J_{(q)} \perp J(1)\ mod\ 2$. Let us denote by $e_{ij}$ the unit matrices in $M_n(Z)$, and let $W = E_n + e_{n-2,\,n} + e_{n,\,n-1} + e_{n-3,\,n-1}$. We claim that $V={}^tWHW={}^tUU$, $U=(U'\perp E_1)W$ satisfies the first part our assertions. Let $w_j$ be the j-th column of $W$, $w_j=e_j$, $j>n-2$, $w_{n-1}=e_{n-2}+e_{n-1}+e_n$, $w_n=e_{n-2}+e_n$. We have that $v_{ij}=H(w_i, w_j)\equiv 0$ *modulo* 2 for these values of $(i,j)$. Hence $V\equiv J_{(q)}\perp B$, where $B$ is 3 by 3, $B=(b_{ij})$ and

$$b_{ij}=H(w_{n+3-i}, w_{n+3-j}), \quad i,j=1,2,3.$$

Clearly

$$b_{11}=H(w_{n-2}, w_{n-2})=b_{n-2,n-2}=n-1,$$

$$b_{12}=H(w_{n-2}, w_{n-1})=b_{n-2,n-2}+b_{n,n-2}\equiv(n-1)+v_{n-1,n-2}\equiv 1 \quad modulo\ 2$$

$$b_{22}=H(w_{n-1}, w_{n-2})=b_{n-2,n-2}+b_{n-1,n-1}+b_{nn}\equiv 1+v'_{n-1,n-1}\equiv 0 \quad mod\ 2$$

$$b_{33}=H(w_n, w_n)=b_{n-2,n-2}+b_{nn}+2b_{n-2,n}=n-1+1=n$$

$$b_{13}=H(w_{n-2}, w_n)=b_{n-2,n-2}+b_{n,n-2}=n-1$$

$$b_{23}=H(w_n, w_{n-1})=b_{n-2,n-2}+2b_{n-2,n}+b_{nn}+b_{n-1,n-2}$$

$$\equiv 1+v'_{n-1,n-2}\equiv 0 \quad mod\ 2.$$

Therefore $B\equiv J\perp E$, *mod* 2. If $n$ is even we take $W=E_n+e_{n\,n-1}$, then $V={}^tWHW=(v_{ij})$, $H=V'\perp E_1$, $V'=(v'_{ij})$, with $v_{ij}=v'_{ij}$ $1\leqslant i, j\leqslant n-1$, with exception of $v_{n-1,n-1}=v'_{n-1,n-1}+1=n$, $v_{nj}=0$, If $j\leqslant n-2$, $v_{n-1,n}=v_{nn}=1$. Next we observe that if we replace the $j$-th column of $V$ by its sum with a multiple $a\in Z$ of the $i$-th column, $i\neq j$, and repeat the same operation with the respective rows, then this is equivalent to replace $V$ by ${}^t(E+ae_{ij})\,V(E+ae_{ij})$. We now apply those operations to make the entries in the $(n-1)$-th row and column equal to zero, with exception of the two last ones; this is possible because the last column of $V$ is $e_{n-1}+e_n$ and all we do is to use the above operation with $1=1,\ldots,n-2$, $j=n$ and $a=-v_{i,n-1}$. In the new matrix the $(n-1)$-th column is $ne_{n-1}+e_n$ and the $n$-th is $v_{1,n-1}e_1+\ldots+v_{n-2,n-1}+e_{n-2}+e_{n-1}+e_n$. Next we repeat the same operation, but with $j=n-1$ instead; we get for the n-th column of the new matrix $e_{n-1}+e_n$ and for the (n-1)-th column

$$(-nv_{1,n-1})\,e_1+\ldots+(-nv_{n-2,n-1})e_{n-2}+ne_{n-1}+e_n,$$

and this yields the splitting modulo $2^a$.

q.e.d.

*REFERENCES*

1. N. ALLAN, *A note on the Arithmetic of the Orthogonal group*, Anais da Academia Brasileira de Ciencias, Vol. 39, 1969.

2. O. T. O'MEARA, Introduction to Quadratic Forms, Academic Press, 1963.

3. J. P. SERRE, *Formes bilinéaires symetriques entières a discriminant* $\pm 1$, Séminaire Cartan, 61 / 62, exposé 14.

*Departamento de Matemáticas y Estadística*
*Universidad Nacional de Colombia*
*Bogotá, Colombia S. A.*
*(Recibido en febrero de 1969 )*