Boletin de la Sociedad Matematica Mexicana Vol. 23, No. 2, 1978

ON MAXIMAL SETS OF ANTICOMMUTING MATRICES

BY JOSÉ ADEM

1. Introduction and Main Result

Let $A_1, \cdots, A_r$ be a set of real matrices of order m, satisfying the conditions

$$A_j^2 = \gamma_j I, \tag{1.1}$$

$$A_jA_k + A_kA_j = 0, \qquad (j, k = 1, \cdots, r; j \neq k), \tag{1.2}$$

where I is the identity matrix and each $\gamma_j = 1$ or -1. Matrices fulfilling condition (1.2) are said to anticommute. Let $\mathscr{R}$ and $\mathscr{I}$ denote the number of matrices, respectively, with $\gamma_j = -1$ and $\gamma_j = 1$, in (1.1). We have, $\mathscr{R} + \mathscr{I} = r$.

Given a set of matrices over the real field, as above, we can associate with it an equivalent set $B_1, \cdots, B_r$ of matrices over the complex field, by defining

$$B_j = \begin{cases} A_j & \text{if} \quad \gamma_j = -1, \\ iA_j & \text{if} \quad \gamma_j = 1, \end{cases} \tag{1.3}$$

where $i = \sqrt{-1}$. The new set contains $\mathscr{R}$ real and $\mathscr{I}$ pure imaginary matrices and they satisfy the conditions

$$B_jB_k + B_kB_j = 0 \qquad \text{for } j \neq k, \quad \text{and} \quad B_j^2 = -I. \tag{1.4}$$

Clearly, the conditions (1.1), (1.2) for real matrices, and (1.4), for real and pure imaginary matrices, are equivalent. Also, if we change the place of i in (1.3), and set $B_j = iA_j$ for $\gamma_j = -1$, etc., then, we get, in (1.4), that $B_j^2 = I$, for all j.

Hurwitz determined in [6] maximal sets A_j of anticommuting matrices of order m over the complex field, fulfilling conditions $A_j^2 = I$, for all j[1]. Eddington showed in [4] that any set of anticommuting matrices of order four, such that $A_j^2 = -I$, has at most five matrices; and, if all are real or imaginary, then $\mathscr{R} = 2$ and $\mathscr{I} = 3$ in every set of five. Newman, using a simple argument, generalized in [9] the first part of Eddington's result (when all $A_j^2 = -I$) and explicitly established the following: if $m = p2^q$, with p odd, is the order, then, for r, the number of matrices, we have $r \leq 2q + 1$[2]. The same bound also is obtained

[1]Hurwitz studied composition of quadratic forms (also Radon in [11] with a different setting) and he looked for maximal sets of *skew* matrices. Recently, D. B. Shapiro in [12], got some interesting generalizations of this problem and extended Hurwitz's results to arbitrary fields of characteristic not two. The author in [1] also verified Hurwitz's results for fields of characteristic not two.

[2]This result about the bound for the number of matrices of order m, fulfilling conditions (1.1), (1.2), has also been proved by Littlewood in [9], using representation of groups. Generalizations have been given by Eichhorn in [5], for matrices with elements in an arbitrary field of characteristic not two, and by Dieudonné in [2], for semi-linear transformations of an m-vector space over a skewfield of characteristic not two. Another generalization by Kestelman is given in [7;Th2], for *regular* anticommuting matrices.

from Hurwitz's work, and both, Hurwitz and Newman, showed that this maximum can always be attained with sets where each matrix is either real or pure imaginary.

For the second part of Eddington's result, concerning the values of $\mathscr{R}$ and $\mathscr{I}$ in a maximal set, Newman wrongly stated in general, that $\mathscr{R} - \mathscr{I} = -1$ or 7.

The principal aim of this paper is to establish the correct relation for $\mathscr{R}$ and $\mathscr{I}$ (cf. (1.7)). For this purpose we first consider some definitions.

An *E-set* is a set of matrices satisfying (1.4) and such that, each matrix is either real or imaginary.

Given $m = p2^q$, with p odd, write $q = 4a + b$, where $0 \leq b \leq 3$. Then, set

$$\mathscr{R}(m, t) = 4t + b \quad \text{and} \quad \mathscr{I}(m, t) = 2q + 1 - 4t - b, \tag{1.5}$$

for each $0 \leq t \leq 2a + [b/3]$.

From our previous remarks, it follows that, a maximal E-set of matrices of order m, is an E-set of $2q + 1$ matrices of order m. Hence, for a maximal E-set, the value of $\mathscr{R}(m, t)$, determines the value of $\mathscr{I}(m, t)$.

Our main result is the following

THEOREM 1.6. *There exists a maximal E-set of matrices of order m, if and only if, for some* $t = 0, 1, \cdots, 2a + [b/3]$, *the numbers of real and imaginary matrices are, respectively,* $\mathscr{R}(m, t)$ *and* $\mathscr{I}(m, t)$.

Observe that, from (1.5), we obtain the following relation

$$\mathscr{R}(m, t) - \mathscr{I}(m, t) = 8(t - a) - 1, \tag{1.7}$$

and this, together with (1.6), should correct the statement of [10; Th2].

Using the equivalence between (1.1), (1.2) and (1.4), stated at the beginning, the results of (1.6) can be applied to determine maximal sets of real matrices fulfilling the conditions $A_j^2 = I$ or $-I$.

Perhaps (1.6) should be established using results on Clifford algebras. However, I prefer to present a proof based almost entirely on direct and elementary arguments on matrices. The proof will be given in the next two sections.

2. Some Auxiliary Propositions

Let $\Sigma = \{A_1, \cdots, A_r\}$ be an E-set of order m and suppose it has $\mathscr{R}(m)$ real and $\mathscr{I}(m)$ imaginary matrices.

PROPOSITION 2.1. *The collection*

$$\Sigma_1 = \left\{ \begin{pmatrix} iI & \\ & -iI \end{pmatrix}, \begin{pmatrix} & I \\ -I & \end{pmatrix}, \begin{pmatrix} & A_1 \\ A_1 & \end{pmatrix}, \cdots, \begin{pmatrix} & A_r \\ A_r & \end{pmatrix} \right\},$$

forms an E-set of $r + 2$ *matrices of which we have* $\mathscr{R}(2m) = \mathscr{R}(m) + 1$ *real and* $\mathscr{I}(2m) = \mathscr{I}(m) + 1$ *imaginary.*

Proof. It is immediate to verify the conditions (1.4).

PROPOSITION 2.2. *Given $\sum$ as above, with m even and $r \geq 2$, assume that $\mathscr{I}(m) \neq 0$. Then, there exists an E-set*

$$\textstyle\sum_0 = \{B_3, \cdots, B_r\},$$

of $r-2$ matrices of order $m/2$, such that,

(2.3) *if $\mathscr{R}(m) \neq 0$, then $\mathscr{R}(m/2) = \mathscr{R}(m) - 1$ and $\mathscr{I}(m/2) = \mathscr{I}(m) - 1$,*

(2.4) *if $\mathscr{R}(m) = 0$, then $\mathscr{R}(m/2) = r - 2$ and $\mathscr{I}(m/2) = 0$,*

where $\mathscr{R}(m/2)$ and $\mathscr{I}(m/2)$ denote, respectively, the number of real and imaginary members of $\sum_0$.

Proof. We refer the reader to [10; p94–96] for a complete proof. Here we will only outline the steps, in order to show how (2.3) and (2.4) follow.

Clearly, if the matrices of $\sum$ anticommute and their squares are $-I$, the same holds for the matrices of a similar set

$$Q^{-1}\Sigma Q = \{Q^{-1}A_1Q, \cdots, Q^{-1}A_rQ\}.$$

From the assumptions that m is even, $r \geq 2$ and $\mathscr{I}(m) \neq 0$, it follows that we can start with A_1, an imaginary matrix, and find a *real* nonsingular matrix Q, such that (see loc. cit.)

$$Q^{-1}A_1Q = \begin{pmatrix} iI & \\ & -iI \end{pmatrix}, \quad Q^{-1}A_jQ = \begin{pmatrix} & C_j \\ -C_j^{-1} & \end{pmatrix} \qquad \text{for } j = 2, \cdots, r,$$

where each C_j is a matrix of order $m/2$, real or imaginary, according to the nature of A_j.

Now, if $\mathscr{R}(m) \neq 0$, we can suppose that A_2 is a real matrix, hence, C_2 is also real. It follows that the matrices

$$B_j = C_jC_2^{-1} \quad \text{with} \quad j = 3, \cdots, r, \tag{2.5}$$

form the E-set Σ_0, where (2.3) holds. In the case $\mathscr{R}(m) = 0$, all the matrices C_j are imaginary, consequently, all the B_j's turn out to be real, and (2.4) follows.

To complete the picture we give the reciprocal statement of (2.1). Let

$$R = \begin{pmatrix} I & \\ & C_2^{-1} \end{pmatrix}.$$

Then, if $P = QR$, we get

$$P^{-1}A_1P = \begin{pmatrix} iI & \\ & -iI \end{pmatrix}, \quad P^{-1}A_2P = \begin{pmatrix} & I \\ -I & \end{pmatrix}, P^{-1}A_jP = \begin{pmatrix} & B_j \\ B_j & \end{pmatrix},$$
$$\text{for } j = 3, \cdots, r,$$

where B_j is as in (2.5).

This is, essentially, the type of reduction used by Hurwitz in [6; p11–14].

Proposition 2.6. *If $m = p2^{4a+3}$, with p an odd number, then, there exists a maximal E-set of real matrices of order m.*

Proof. Given m we always have an E-set of real matrices, with $\rho(m) - 1$ elements, where $\rho(m)$ is the Hurwitz-Radon function ([3]). In our case, $\rho(m) = 8a + 8$ and, if $q = 4a + 3$, we have $\rho(m) - 1 = 2q + 1$, so we get a maximal E-set of real matrices, and (2.6) follows.

Proposition 2.7. *Given $A_1, \cdots, A_{2N}$, an E-set with $2N$ elements, we can always add to it the matrix*

$$A_{2N+1}{}^* = i^{N+1} A_1 \cdots A_{2N},$$

to obtain an E-set with $2N + 1$ members.

Proof. This proposition is easily verified and it already appears in [4] and [10].

Proposition 2.8. *Let $A_1, \cdots, A^{2N}$ be an E-set of real matrices. Define*

$$\begin{aligned} A_j{}^* &= i^{N+1} A_3 A_4 \cdots A_{2N} A_j && (j = 1, 2), \\ A_k{}^* &= i A_1 A_2 A_k && (k = 3, 4, \cdots, 2N), \\ A_{2N+1}{}^* &= i^{N+1} A_1 A_2 \cdots A_{2N}. \end{aligned}$$

Then, the matrices $A_1{}^*, \cdots, A_{2N+1}{}^*$ are all distinct and they form an E-set. For this new set we have

$$\mathscr{R} = 0 \quad \text{and} \quad \mathscr{I} = 2N + 1 \qquad \text{if } N \text{ is even},$$

$$\mathscr{R} = 3 \quad \text{and} \quad \mathscr{I} = 2N - 2 \qquad \text{if } N \text{ is odd}.$$

Proof. This proposition, due to Newman [10], is established by a direct verification.

Corollary 2.9. *Let $A_1, \cdots A_{2N}, A_{2N+1}$ be an E-set of real matrices and suppose that N is even. Then, the matrices $A_1{}^*, \cdots, A_{2N}{}^*, A_{2N+1}$, where each A_j^* is as in (2.8), form an E-set where $\mathscr{R} = 1$ and $\mathscr{I} = 2N$.*

Proof. It follows that A_{2N+1} anticommutes with $A_j{}^*$, and this is enough for the proof.

3. Proof of Theorem 1.6

The proof of (1.6) is an involved four-step induction based on the auxiliary propositions of the preceding section. As in (1.5), let $m = p2^q$, with p odd and $q = 4a + b$. The induction is on a and we leave the initial steps, $a = 0$ with $0 \leq b \leq 3$, to the end.

In general, assuming that (1.6) is true for $m = p2^{4a}$, we will show that it is true for $2^k m = p2^{4a+k}$, with $k = 1, 2, 3, 4$, and the case $k = 4$ completes the induction step.

Let $E(m, t)$ denote a maximal E-set of order m, where the number of real matrices is $\mathscr{R}(m, t)$. Given $\mathscr{R}(m, t) = 4t + b$, the "*if*" part of (1.6) is equivalent to establish the existence of $E(m, t)$, and this will first be considered.

Begin with $m = p2^{4a}$. By the induction hypothesis, for each $0 \leq t \leq 2a$, we have $E(m, t)$. Recall that, given an E-set of order m, proposition (2.1) allows us to construct a new E-set of order $2m$, where the numbers of real and imaginary matrices are increased by one. Hence, from $E(m, t)$ and (2.1), we get, first $E(2m, t)$ and then $E(4m, t)$. Continuing in this form, we obtain $E(8m, t)$, where the range of t is as above. Here, the missing case $t = 2a + 1$ is gotten from the Hurwitz-Radon matrices, as it is presented in (2.6). Again, using the matrices $E(8m, t)$ in (2.1), we get the E-sets $E(16m, t + 1)$, where $16m = p2^{4(a+1)}$, and $0 \leq t \leq 2a + 1$. Relabeling with $s = t + 1$, this becomes $E(16m, s)$, for $1 \leq s \leq 2(a + 1)$. To complete the construction for $s = 0$, consider $E(16m, 2a + 2)$. It has $2N = 8a + 8$ real matrices, with N even. Then, from (2.8), it follows the existence of a maximal E-set, say $E(16m, 0)$ with $\mathscr{R}(16m, 0) = 0$. This completes the induction step of the "*if*" part of (1.6).

Now, we will consider the "*only if*" part of (1.6). Given $n = p2^{4a+b}$, suppose the existence of maximal E-sets of order n, with a number of real matrices different from $4t + b$. Represent anyone of these sets by $E^*(n, t)$ and by $\mathscr{R}^*(n, t)$, its number of real matrices. Then, $\mathscr{R}^*(n, t) = 4t + k$, for some $0 \leq k \leq 3$ with $k \neq b$. Let $q = 4a + b$. Since $2q + 1$ is the total number of matrices in $E^*(n, t)$, we have

$$\mathscr{R}^*(n, t) = 4t + k \leq 8a + 2b + 1. \tag{3.1}$$

As before, begin with $m = p2^{4a}$. Here, the induction hypothesis assures us that not any of the sets $E^*(m, t)$ exists. That is, since $b = 0$, we can not have $\mathscr{R}^*(m, t) = 4t + k$ for $k = 1, 2$ or 3.

Take $2m = p2^{4a+1}$, and then, $b = 1$. Suppose there exists $E^*(2m, t)$, with $\mathscr{R}^*(2m, t) = 4t + v$, for some $v = 0, 2$ or 3. We will show that this implies a contradiction.

For shortness, write $E^*(n)$, $\mathscr{R}^*(n)$, etc., instead of $E^*(n, t)$, $\mathscr{R}^*(n, t)$, etc., when the value of t is understood.

Let $v = 0$. From (3.1), it follows that $4t \leq 8a + 3$. There are two cases to be considered: $t = 0$ and $t \neq 0$. If $t = 0$, then $\mathscr{R}^*(2m) = 0$ and $\mathscr{I}^*(2m) = 8a + 3$, and (2.4) implies $\mathscr{R}^*(m) = 8a + 1$. If $t \neq 0$, then, $\mathscr{R}^*(2m) = 4t \neq 0$, and from (3.1), we get $\mathscr{I}^*(2m) \neq 0$. Then, from (2.3), it follows that $\mathscr{R}^*(m) = 4(t - 1) + 3$. Therefore, in both cases we have a contradiction and this excludes $v = 0$.

If $v = 2$, (3.1) implies that $\mathscr{R}^*(2m) \neq 0$ and $\mathscr{I}^*(2m) \neq 0$ and, from (2.3), it follows that $\mathscr{R}^*(m) = 4t + 1$. This is a contradiction.

For $v = 3$, there are two cases: $t = 2a$ and $t \neq 2a$. If $t \neq 2a$, then, $\mathscr{R}^*(2m) \neq 0$ and $\mathscr{I}^*(2m) \neq 0$, and (2.3), implies that $\mathscr{R}^*(m) = 4t + 1$. As before, this is a contradiction. If $t = 2a$, then, $\mathscr{R}^*(2m) = 8a + 3$ and $\mathscr{I}^*(2m) = 0$. Let $2N = 8a + 2$. From (2.8), for N odd, we get a set $E^*(2m)$ with $\mathscr{R}^*(2m) = 3$ and $\mathscr{I}^*(2m) = 8a$. Assuming $a \neq 0$, this is the above case ($t \neq 2a$), hence, $v = 3$ is also excluded. Therefore, we can not have $E^*(2m, t)$.

Now, take $4m = p2^{4a+2}$, and then, $b = 2$. Suppose the existence of $E^*(4m)$ with $\mathscr{R}^*(4m) = 4t + v$, for some $v = 0$, 1 or 3. Here, from (3.1), we get $4t + v \leq 8a + 5$. From now on, the arguments that already have been used, will only be indicated.

For $v = 0$, we have two cases: $t = 0$ and $t \neq 0$. As before, using (2.3) and (2.4), in both cases, it follows the existence of a set $E^*(2m)$, previously excluded.

For $v = 1$, we also have two cases. If $t = 2a + 1$, then, $\mathscr{R}^*(4m) = 8a + 5$ and $\mathscr{I}^*(4m) = 0$. With $2N = 8a + 4$ and $N = 4a + 2$ even, use (2.7), to obtain a set $E^*(4m)$, with $\mathscr{R}^*(4m) = 8a + 4$ and $\mathscr{I}^*(4m) = 1$. Then, from (2.3), get $E^*(2m)$ with $\mathscr{R}^*(2m) = 4a + 3$, and this is not possible. In the other case, $t \neq 2a + 1$, it follows that $\mathscr{R}^*(4m) \neq 0$ and $\mathscr{I}^*(4m) \neq 0$ and, with (2.3), this also is not possible.

The case $v = 3$ implies $\mathscr{R}^*(4m) \neq 0$ and $\mathscr{I}^*(4m) \neq 0$. Again, (2.3) takes care of it.

Next, for $8m = p2^{4a+3}$, we get $b = 3$. Then, assume the existence of $E^*(8m)$ with $\mathscr{R}^*(8m) = 4t + v$, for some $v = 0$, 1 or 2. From (3.1), it follows $4t + v \leq 8a + 7$.

If $v = 0$, again we have here, the cases $t = 0$, $t \neq 0$ and, using (2.3), (2.4), we dispose of them. For the values $v = 1$, 2, it follows that $\mathscr{R}^*(8m) \neq 0$ and $\mathscr{I}^*(8m) \neq 0$ and, using (2.3), these cases are also excluded. Hence, the sets $E^*(8m, t)$ do not exist.

Finally, take $16m = p2^{4(a+1)}$, and then, $b = 0$. Suppose the existence of $E^*(16m)$ with $\mathscr{R}^*(16m) = 4t + v$, for some $v = 1$, 2 or 3. From (3.1), we have $4t + v \leq 8a + 9$.

For $v = 1$, there are two cases: $t = 2a + 2$ and $t \neq 2a + 2$. If $t = 2a + 2$, then $\mathscr{R}^*(16m) = 8a + 9$ and $\mathscr{I}^*(16m) = 0$. Use (2.9), to obtain $E^*(16m)$ with $\mathscr{R}^*(16m) = 1$ and $\mathscr{I}^*(16m) = 8a + 3$. Then, from (2.3), we get $E^*(8m)$ with $\mathscr{R}^*(8m) = 0$, but this is not possible. The case $t \neq 2a + 2$ of $v = 1$, and the other cases $v = 2$, 3 are all settled with (2.3), so that the sets $E^*(16m)$ can not exist. This completes the induction of the "*only if*" part of (1.6).

To finish the proof, we need to establish the first cases of (1.6). Explicitly, when $a = 0$ and $b = 0, 1, 2, 3$. Let $a = 0$ and $b = 0$. Then, $m = p$ and we only have one matrix A_1 of order p, such that $A_1^2 = -I$. This implies that

$$(\det A_1)^2 = (-1)^p = -1.$$

Hence, A_1 can not be real. On the other hand, $A_1 = iI$ proves the existence of an E-set, with $\mathscr{R} = 0$ and $\mathscr{I} = 1$.

From here, the construction of the sets $E(p2^k, t)$, for $k = 1, 2, 3, 4$, is achieved, with the same arguments used for the "*if*" part of (1.6).

We already proved the nonexistence of $E^*(p, t)$, when p is an odd number. With the exception of $E^*(p2, 3)$, the nonexistence of all the other sets $E^*(p2^k, t)$, for $k = 1, 2, 3, 4$, also follows from the same arguments used for the "*only if*" part of (1.6), hence, their proof is omitted.

The special case appears because (2.8) can not be applied if $2N = 2$. Recall that the existence of $E^*(p2, 3)$, where $\mathscr{R}^*(p2) = 3$ and $\mathscr{I}^*(p2) = 0$, is equivalent to the existence of three real matrices A_1, A_2, A_3, of order $p2$, fulfilling conditions (1.4). From (2.7), we may assume that $A_3 = A_1A_2$.

Let R denote the real field, R^n the space of n-tuples with the usual R-vector space structure, and $R(n)$ the R-algebra of real matrices of order n. Let Q be the quaternion algebra over R, and let $\{1, i, j, k\}$ be the usual basis. Setting

$$1 \to I,\ i \to A_1, j \to A_2,\ k \to A_3$$

we get a map of Q into $R(p2)$ as R-algebras. Then, through this map, R^{p2} becomes a Q-module, but R^n is a Q-module if and only if 4 divides n [8; p131]. Therefore, $E^*(p2, 3)$ can not exist. This ends the proof of (1.6).

CENTRO DE INVESTIGACIÓN DEL IPN, MÉXICO 14, D. F.

REFERENCES

[1] J. ADEM, Algebra lineal, campos vectoriales e inmersiones, III ELAM, IMPA, Rio de Janeiro, 1978.

[2] J. DIEUDONNÉ, *A problem of Hurwitz and Newman*. Duke Math. J. **20**(1953), 381–389.

[3] B. ECKMANN, *Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen*. Comment. Math. Helv. **15**(1943), 358–366.

[4] A. S. EDDINGTON, *On sets of anticommuting matrices*. J. London Math. Soc. **7**(1932), 58–68.

[5] W. EICHHORN, *Funktionalgleichungen in Vektorräumen Kompositionsalgebren und Systeme partieller Differentialgleichungen*. Aequations Math. **2**(1969), 287–303.

[6] A. HURWITZ, *Über die Komposition der quadratische Formen*. Math. Ann. **88**(1923), 1–25.

[7] H. KESTELMAN, *Anticommuting linear transformations*. Canadian J. Math. **13**(1961), 614–624.

[8] T. Y. LAM, The Algebraic Theory of Quadratic Forms. Benjamin, New York, 1973.

[9] D. E. LITTLEWOOD, *Note on the anticommuting matrices of Eddington*, J. London Math. Soc. **9**(1934), 41–50.

[10] M. H. A. NEWMAN, *Note on an algebraic theorem of Eddington*, J. London Math. Soc. **7**(1932), 93–99.

[11] J. RADON, *Lineare Scharen orthogonalen Matrizen*, Abh. Math. Sem. Univ. Hamburg, **1**(1922), 1–14.

[12] D. B. SHAPIRO, *Spaces of Similarities* I. *The Hurwitz Problem*. J. Algebra **46**(1977), 148–170.