MAXIMAL SETS OF INVOLUTIONS

BY

IRVING REINER

§1. Let U_n denote the unimodular group consisting of all $n \times n$ integral matrices of determinant ± 1. An element $W \in U_n$ is called an *involution* if $W^2 = I^{(n)}$ (the n-rowed identity matrix). We shall consider abelian sets of involutions in U_n of maximal size, and call such a set a *maximal set*. For a given involution $W \in U_n$, define $N(W)$ to be the maximum number of involutions, all conjugate to W in U_n, which can occur in a maximal set. Certainly $N(W)$ depends only on the class of W in U_n. We already know([1]) that as x, y, and z range over all non-negative integers such that $2x+y+z=n$, the matrix

$$(1) \qquad W(x, y, z) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \dotplus \cdots \dotplus \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \dotplus (-I)^{(y)} \dotplus I^{(z)}$$

(where x two-by-two blocks occur in the direct sum) gives a complete set of nonconjugate representatives of the classes of involutions in U_n. We shall obtain a new proof of this result during our investigation of $N(W)$.

§2. The analogous problem for the group R_n of rational nonsingular $n \times n$ matrices has previously been considered([2]). We quote some of the known results:

Let V be the space of rational $n \times 1$ vectors. To each involution $W \in R_n$ we let correspond the plus-space $W^+ = \{x \in V : Wx = x\}$, and the minus-space $W^- = \{x \in V : Wx = -x\}$. Then V is the direct sum of W^+ and W^-. If p is the dimension of W^+, and q that of W^-, then $p+q=n$ and we call W a (p, q) involution. If W is a (p, q) involution, we may choose the coordinate system in such a way that the first p columns of $I^{(n)}$ span W^+, and the last q columns span W^-. This gives at once([3])

$$W = \begin{bmatrix} I^{(p)} & 0 \\ 0 & -I^{(q)} \end{bmatrix}.$$

Therefore, in R_n every (p, q) involution is a conjugate of the above matrix. On the other hand, any decomposition $V = A \dotplus B$ determines a unique involution $W \in R_n$ for which $W^+ = A$, $W^- = B$.

Presented to the Society, October 30, 1954; received by the editors September 25, 1954.

([1]) L. K. Hua and I. Reiner, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331–348.

([2]) J. Dieudonné, Memoirs of the American Mathematical Society, no. 2, 1951; also G. W. Mackey, Ann. of Math. vol. 43 (1942) pp. 244–260.

([3]) Throughout this paper we shall use 0 to denote a null matrix of appropriate size.

Next we have for a pair of involutions $W, Z \in R_n$:
(i) $ZW = WZ$ if and only if $ZW^+ = W^+$, $ZW^- = W^-$.
(ii) $ZW = WZ$ implies

$$W^+ = (W^+ \dotplus Z^+) \dotplus (W^+ \cap Z^-),$$
$$W^- = (W^- \dotplus Z^+) \dotplus (W^- \cap Z^-).$$

From these it follows that a set of m mutually commutative involutions gives rise to a decomposition of V into a direct sum of subspaces $V_1, \cdots, V_h$, each of positive dimension. If we choose the direct sum of some of the V_i as W^+, and the direct sum of the remaining V_i as W^-, a unique involution W is determined. Since the h spaces $V_1, \cdots, V_h$ can be grouped into two disjoint sets in 2^h ways, we can obtain at most 2^h mutually commutative involutions from this decomposition of V; therefore $m \leqq 2^h$. If we now take the V_i all of dimension 1, an abelian set of 2^n involutions is generated, and this set is certainly maximal in size. Thus a maximal set in R_n has 2^n elements, and is gotten by starting with any n linearly independent vectors $v_1, \cdots, v_n$ in V, choosing as basis for W^+ any subset of these vectors, and letting the remaining vectors serve as basis for W^-. We shall say that the matrix with columns $v_1, \cdots, v_n$ *generates* the maximal set. Finally we observe that a maximal set contains exactly $C_{n,p}$ involutions of type (p, q).

§3. Let us call a maximal size abelian set of (p, q) involutions in R_n a *maximal* (p, q) *set*. The above reasoning shows that a maximal (p, q) set contains at least $C_{n,p}$ elements. We show now that there must be exactly $C_{n,p}$ elements in a maximal (p, q) set, and that such a set is embeddable in a uniquely determined maximal set. For, suppose that we have an abelian set of m involutions of type (p, q), and that they give rise to a decomposition $V = V_1 \dotplus \cdots \dotplus V_h$. Let $m_i > 0$ be the dimension of V_i. We obtain (p, q) involutions from this decomposition by choosing for W^+ those direct sums

$$V_{i_1} \dotplus \cdots \dotplus V_{i_s}$$

for which

$$m_{i_1} + \cdots + m_{i_s} = p.$$

Hence m cannot exceed the number of solutions of the above equation, so that

$$m \leqq \text{coefficient of } x^p \text{ in } (1 + x^{m_1}) \cdots (1 + x^{m_h}). \tag{2}$$

On the other hand, the right-hand side of (2) is $\leqq$ coefficient of x^p in

$$(1 + x)^{m_1} \cdots (1 + x)^{m_h} = (1 + x)^n,$$

with equality if and only if each $m_i = 1$ (except when $p = 0$ or $q = 0$). Thus $m \leqq C_{n,p}$, and furthermore $m = C_{n,p}$ implies that each $m_i = 1$. Thus any maximal (p, q) set arises from a decomposition of V into n one-dimensional subspaces by choosing, in $C_{n,p}$ ways, any p of these subspaces to make up W^+,

and using the remaining q of them for W^-. This decomposition of V generates a unique maximal set containing the given maximal (p, q) set.

§4. We now return to the unimodular group U_n, and consider an involution $W \in U_n$. Since also $W \in R_n$, we may associate with W the pair of spaces W^+, W^-. Let G denote the set of all $n \times 1$ vectors with integral elements, and define $W_+ = W^+ \cap G$, $W_- = W^- \cap G$. If W is a (p, q) involution, there exist vectors $v_1, \cdots, v_p \in W_+$ which form an integral basis for W_+, that is, every vector in W_+ is uniquely expressible as a linear combination of $v_1, \cdots, v_p$ with integral coefficients. Likewise there exists an integral basis for W_-.

In practice, these integral bases may be obtained as follows: let $x_1, \cdots, x_p \in V$ be a basis for W^+. Since $x \in W^+$ implies $ax \in W^+$ for rational a, we may take $x_1, \cdots, x_p \in G$, with each x_i primitive(4). As b ranges over all integers, let b_0 be such that the greatest common divisor of the elements in the column vector $x_2 + bx_1$ is maximal, say c_0. Then replace x_2 by $(x_2 + b_0 x_1)/c_0$, and repeat the procedure with $x_3 + b_1 x_1 + b_2 x_2$, etc. The integral $n \times p$ matrix whose columns are the p vectors finally obtained by this procedure will be primitive(4), and its columns will furnish an integral basis for W_+. In fact, a set of p vectors $y_1, \cdots, y_p \in W_+$ is an integral basis for W_+ if and only if the matrix $(y_1 \cdots y_p)$ is primitive(5).

§5. We have thus shown that to each involution $W \in U_n$ there correspond two primitive matrices $P^{n \times p}$ and $Q^{n \times q}$, whose columns give integral bases for W_+ and W_-, respectively. Set $T = (P\ Q)$; then we see that $T = (P\ Q)$ and $T_1 = (P_1\ Q_1)$ arise from the same involution in U_n if and only if there exist matrices $R \in U_p$, $S \in U_q$ such that $P_1 = PR$, $Q_1 = QS$. Furthermore, $T = (P\ Q)$ and $T_1 = (P_1\ Q_1)$ arise from conjugate involutions if and only if there exist matrices $A \in U_n$, $R \in U_p$, $S \in U_q$ such that

$$P_1 = APR, Q_1 = AQS, \text{ that is, } T_1 = AT \begin{pmatrix} R & 0 \\ 0 & S \end{pmatrix}.$$

THEOREM 1. *Using the above notation, let $T = (P\ Q)$ arise from an involution $W \in U_n$. Then the invariant factors of T are* 1, $\cdots$, 1, 2, $\cdots$, 2, *and the number of* 2*'s is at most* min (p, q).

Proof. Let N be the module consisting of all integral linear combinations of the columns of T. The invariant factors $\epsilon_1, \cdots, \epsilon_n$ of T have the property that there exists an integral basis $u_1, \cdots, u_n$ of G for which $\epsilon_1 u_1, \cdots, \epsilon_n u_n$ is an integral basis of N(6). As we shall show in a moment, $u \in G$ implies $2u \in N$. From this we have at once that each ϵ_i is 1 or 2.

(4) An integral matrix is called *primitive* if the greatest common divisor of its maximal size minors is 1.

(5) See H. Weyl, Trans. Amer. Math. Soc. vol. 48 (1940) pp. 126–164; also C. L. Siegel, *Geometry of numbers*, New York University notes, 1946.

(6) van der Waerden, *Modern Algebra* II, 2d ed., Chap. XV.

For any $u \in G$ we write

$$2u = (I + W)u + (I - W)u.$$

Since $(I+W)u \in W_+$, and $(I-W)u \in W_-$, we have $2u \in N$.

Finally, P and Q are both primitive, so the pth and qth determinantal divisors of T are both 1. Therefore $\epsilon_1 = \cdots = \epsilon_p = 1$, $\epsilon_1 = \cdots = \epsilon_q = 1$, so the number of invariant factors which are 2 is at most $\min(n-p, n-q) = \min(p, q)$.

DEFINITION. If there are x 2's occurring as invariant factors of T, we shall say that W is a $(p, q; x)$ *involution.*

We now assert that two involutions are conjugate in U_n if and only if they are of the same type. It is easy to see, using the criterion for conjugacy given at the beginning of this section, that conjugate involutions are of the same type. The converse will follow from:

THEOREM 2. *Let $W \in U_n$ be a $(p, q; x)$ involution. Then in U_n, W is conjugate to $W(x, q-x, p-x)$ (see Equation (1)).*

Proof. We shall give a proof which does not depend on the result stated in §1. Let W be a $(p, q; x)$ involution, and let $T = (P\ Q)$. The matrix T may be replaced by

$$T_1 = AT\begin{pmatrix} R & 0 \\ 0 & S \end{pmatrix}, \quad A \in U_n, R \in U_p, S \in U_q,$$

without changing the class of W. Since P is primitive, we may choose $A \in U_n$ so that T becomes

$$\begin{bmatrix} I^{(p)} & Q_1 \\ 0 & Q_2 \end{bmatrix}.$$

Now replace T by

$$\begin{bmatrix} I^{(p)} & 0 \\ 0 & A_1 \end{bmatrix}\begin{bmatrix} I^{(p)} & Q_1 \\ 0 & Q_2 \end{bmatrix}\begin{bmatrix} I^{(p)} & 0 \\ 0 & B \end{bmatrix}, \qquad A_1 \in U_q, B \in U_q.$$

This replaces Q_2 by $A_1 Q_2 B$, and by proper choice of A_1 and B we may diagonalize Q_2. Since none of these operations affects the invariant factors of T, it follows at once that Q_2 has $(q-x)$ 1's and x 2's along its main diagonal. Hence we may take

$$T = \begin{bmatrix} I^{(p)} & Q_3 & Q_4 \\ 0 & I^{(q-x)} & 0 \\ 0 & 0 & 2I^{(x)} \end{bmatrix}.$$

Replacing T by

$$\begin{bmatrix} I^{(p)} & -Q_3 & C \\ 0 & I^{(q-x)} & 0 \\ 0 & 0 & I^{(x)} \end{bmatrix} T,$$

we may make $Q_3=0$, and reduce the elements of Q_4 (mod 2). Next replace T by XTX^{-1}, where $X=A_2\dotplus I^{(q-x)}\dotplus B^{-1}$ with $A_2\in U_p$, $B\in U_x$. Then Q_4 is replaced by A_2Q_4B, and can be diagonalized. As above, reduce the elements of Q_4 (mod 2), so that Q_4 is now a diagonal matrix with diagonal elements 0's and 1's. None of them can be 0, since under all of these transformations each column of T remains primitive. Therefore T becomes

$$\begin{bmatrix} I^{(p)} & 0 & I^{(x)} \\ & 0 & 0 \\ 0 & I^{(q-x)} & 0 \\ 0 & 0 & 2I^{(x)} \end{bmatrix},$$

and so W is conjugate to

$$\begin{bmatrix} I^{(p)} & 0 & -I^{(x)} \\ & 0 & 0 \\ 0 & -I^{(q-x)} & 0 \\ 0 & 0 & -I^{(x)} \end{bmatrix}.$$

This latter matrix is clearly conjugate in U_n to $W(x, q-x, p-x)$.

§6. We shall now prove a result which is roughly the converse of Theorem 1, and which eliminates a great deal of computation in what follows.

THEOREM 3. *Let M be an integral nonsingular $n\times n$ matrix with invariant factors* $1, \cdots, 1, 2, \cdots, 2$, *where k 1's and $(n-k)$ 2's occur. Let $M_1^{n\times n_1}$ consist of any n_1 columns of M, and let $M_2^{n\times n_2}$ consist of the remaining n_2 columns of M. Then the involution W for which W^+ is spanned by the columns of M_1, and W^- by those of M_2, is an involution in U_n. Furthermore, if $m_i=$*rank (mod 2) *of M_i $(i=1, 2)$, then W is of type $(n_1, n_2; x)$ with $x=m_1+m_2-k$.*

Proof. 1. We show firstly that W is integral. Let e_j be the jth column of $I^{(n)}$. Since the invariant factors of M are 1's and 2's, $2e_j$ is an integral linear combination of the columns of M. Thus

$$2e_j = u_1 + u_2,$$

where u_i is an integral linear combination of the columns of M_i $(i=1, 2)$. But then

$$We_j = \frac{u_1 - u_2}{2} = e_j - u_2.$$

Therefore We_j, the jth column of W, is integral. This holds for each j; hence W itself is integral.

2. By the 2-rank of an integral array, we shall mean the rank (mod 2) of that array, that is, its rank over $GF(2)$. Since the kth determinantal divisor of M is 1, the $(k+1)$st 2, we see that the 2-rank of M is k. Consequently $m_1+m_2 \geqq k$.

3. Suppose now that by elementary operations([7]) on the columns of M, a new matrix N is obtained having a column $2u$, $u \in G$. The matrix N_1 gotten by replacing $2u$ by u then has invariant factors $1, \cdots, 1, 2, \cdots, 2$, where now $(k+1)$ 1's occur.

On the other hand, elementary operations on the columns of M cannot produce a matrix M_1 having a column $4u$, $u \in G$. For in that case, letting $x_1, \cdots, x_n$ be the columns of M, we have

$$4u = a_1x_1 + \cdots + a_nx_n,$$

where $a_1, \cdots, a_n$ are integers whose greatest common divisor is 1. But since M has invariant factors 1's and 2's, we have

$$2u = b_1x_1 + \cdots + b_nx_n$$

for some integers $b_1, \cdots, b_n$. From the linear independence of $x_1, \cdots, x_n$ we obtain $a_i = 2b_i$ $(i = 1, \cdots, n)$, contradiction.

4. Now let M be partitioned into M_1 and M_2 as in the hypothesis of the theorem. In general, M_1 will not be primitive; in fact, we may rearrange the columns of M_1 (thereby leaving unchanged the space spanned by its columns) so that the first m_1 of them are linearly independent (mod 2), and the remaining $n_1 - m_1$ of the columns will then be linearly dependent (mod 2) on the first m_1 columns. By further elementary operations on the columns, we may take the last $n_1 - m_1$ columns in the form $2v_i$, $v_i \in G$ $(i = m_1+1, \cdots, n_1)$. Upon replacing each column $2v_i$ by v_i $(i = m_1+1, \cdots, n_1)$, we obtain a "reduced" matrix $\overline{M}_1$ whose first m_1 columns, $u_1, \cdots, u_{m_1}$, coincide with those of M_1. We now verify that $\overline{M}_1$ is primitive, and for this it suffices to show $\overline{M}_1$ primitive (mod 2). If this were not the case, we would have a relation

$$\sum_{i=1}^{m_1} a_iu_i + \sum_{i=m_1+1}^{n_1} a_iv_i \equiv \text{null vector (mod 2)},$$

where each $a_i = 0$ or 1, and at least one $a_i = 1$. Not all of the last $(n_1 - m_1)$ a_i's vanish, since $u_1, \cdots, u_{m_1}$ are linearly independent (mod 2). Multiplying the above congruence by 2, we obtain

$$2 \sum_{i=1}^{m_1} a_iu_i + \sum_{i=m_1+1}^{n_1} a_iu_i \equiv \text{null vector (mod 4)}.$$

([7]) See C. C. MacDuffee, *The theory of matrices*, Springer, 1933, p. 32.

Hence, elementary operations on the columns of M_1 yield a column of the form $4u$, $u \in G$. This is impossible, since the columns of M_1 are also columns of M. Therefore $\overline{M}_1$ is primitive.

5. In the same manner we get a reduced matrix $\overline{M}_2$ from M_2; set $T=(\overline{M}_1\overline{M}_2)$. The columns of $\overline{M}_1$ furnish an integral basis for W_+, those of $\overline{M}_2$ for W_-. We have made $(n_1-m_1)+(n_2-m_2)$ divisions by 2 in passing from (M_1M_2) to $(\overline{M}_1\overline{M}_2)$, so T has invariant factors $1, \cdots, 1, 2, \cdots, 2$, where the number of 2's is

$$(n-k)-(n_1-m_1)-(n_2-m_2)=m_1+m_2-k.$$

This completes the proof of the theorem.

§7. We now consider maximal size abelian sets of involutions in U_n; every such set is also in R_n, hence cannot contain more than 2^n elements. On the other hand, there certainly exist maximal sets in U_n containing 2^n elements; for example, such a set is the set of diagonal matrices with ± 1's as diagonal elements. Thus, we shall consider abelian sets of 2^n involutions in U_n. From the discussion in §2, every maximal set in U_n arises from a generating matrix M consisting of n linearly independent primitive column vectors $u_1, \cdots, u_n$, by choosing in all possible ways a subset of the u_i's as basis for W^+, and the remaining u_i's as basis for W^-. We shall call M *permissible* if the 2^n involutions which it generates are all integral. Examples easily show that not every integral M is permissible.

Suppose now that the permissible generating matrices M and M_1 give rise to two maximal sets: $W_1, \cdots, W_{2^n}$, and $Z_1, \cdots, Z_{2^n}$, respectively. If there exists a matrix $Y \in U_n$ such that the W_i's are a rearrangement of the matrices YZ_iY^{-1}, we call the two maximal sets *conjugate*, and say that M and M_1 are *equivalent* (denoted by $M \sim M_1$).

THEOREM 4. *Let M and M_1 be permissible generating matrices. Then $M \sim M_1$ if and only if there exist matrices $A \in U_n$, $B \in U_n$ (where B is gotten from $I^{(n)}$ by permuting columns, possibly changing their signs), such that $M_1 = AMB$.*

Proof. The sufficiency of the condition is obvious. To prove necessity, let $W_1, \cdots, W_n$ be the $(n-1, 1)$ involutions in the first maximal set, and suppose them numbered so that u_i, the ith column of M, is basis for W_i^-. Renumber the Z's so that $Z_i = YW_iY^{-1}$; then $Z_1, \cdots, Z_n$ are also $(n-1, 1)$ involutions. Permute the columns of M_1 so that v_i, the ith column of M_1, is basis for Z_i^-. Then $W_iu_i = -u_i$ implies $Y^{-1}Z_iYu_i = -u_i$, so $Z_iYu_i = -Yu_i$. Therefore $v_i = \pm Yu_i$, and so, after changing the signs of some of the v_i if necessary, we have $M_1 = YM$. This completes the proof.

In R_n any two maximal sets are conjugate; simple examples show that this is no longer the case in U_n. We seek a complete system of nonequivalent permissible generating matrices. We may remark at once that $M \sim I^{(n)}$ if and only if M is unimodular. Further, $M \sim M_1$ implies that M and M_1 have

the same invariant factors. This condition is not sufficient, however, as the example

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

shows. The maximal set generated by M contains $\pm I$, two each $\pm(2, 1; 1)$ involutions, one each $\pm(2, 1; 0)$ involutions. That generated by M_1 contains $\pm I$ and three each $\pm(2, 1; 1)$ involutions. Hence the maximal sets are not conjugate.

§8. In order to simplify the statement and proof of the next theorem, we introduce here the following four operations on an integral $r \times s$ array R:

(i) Replace R by T, where $T \equiv R \pmod 2$.

(ii) Permute the rows of R.

(iii) Permute the columns of R.

(iv) If R is of the form

$$\begin{bmatrix} 1 & u \\ v & S \end{bmatrix}$$

replace R by

$$\begin{bmatrix} 1 & u \\ -v & S - vu \end{bmatrix}.$$

Or, more generally, if $R = (a_{ij})$ and some $a_{pq} = 1$, perform the corresponding replacement where now u represents the pth row from which a_{pq} has been deleted, v the qth column from which a_{pq} has been deleted, and S the $(r-1) \times (s-1)$ array obtained by deleting the pth row and qth column from R[8].

We call two $r \times s$ arrays *related* if one can be obtained from the other by a finite number of operations of the four types just described. It is easy to see that being related is an equivalence relation.

THEOREM 5. *Every permissible generating matrix is equivalent to one of the form*

$$\begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix}, \tag{3}$$

where the elements of R are 0's and 1's, and where R has no zero columns. Every matrix of this form is permissible. Furthermore, two such matrices

---

[8] The case first illustrated is that where $p = q = 1$. The more general case could have been reduced to the case $p = q = 1$, by use of operations (ii) and (iii).

$$(4) \qquad \begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix} \text{ and } \begin{bmatrix} I^{(t)} & T \\ 0 & 2I^{(n-t)} \end{bmatrix},$$

are equivalent if and only if $r=t$ *and* R *is related to* T.

Proof. 1. The generators equivalent to the permissible generator M are given by AMB, where $A \in U_n$ and where B permutes the columns of M, possibly changing some of their signs. Let $M_1 = AM$, $A \in U_n$; by suitable choice of A, we may take M_1 in Hermite canonical form:

$$M_1 = \begin{bmatrix} d_1 & d_{12} & \cdots & d_{1n} \\ 0 & d_2 & \cdots & d_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & d_n \end{bmatrix},$$

with each $d_i > 0$ $(i=1, \cdots, n)$, and each d_{ij} reduced (mod d_j) $(i<j;\ i, j = 1, \cdots, n)$. Since the first column of M is primitive, we have $d_1 = 1$. Suppose that exactly r of the diagonal elements $d_1, \cdots, d_n$ are 1; by permuting rows and permuting columns, we obtain from M_1 the equivalent generator

$$M_2 = \begin{bmatrix} I^{(r)} & & R \\ & d_{r+1} & \cdots\ d_{r+1,n} \\ 0 & \cdot & \cdots \\ & 0 & \cdots\ d_n \end{bmatrix}.$$

The matrix M_2 is equivalent to the permissible generator M, hence it too is permissible. In particular, if we choose the first r columns of M_2 as basis for W^+, the remaining $n-r$ columns as basis for W^-, and construct a reduced matrix $\overline{M}_2$ (as in the proof of Theorem 3) whose first r columns form an integral basis for W_+, and whose last $n-r$ columns form such a basis for W_-, then the invariant factors of $\overline{M}_2$ must be 1's and 2's. However, in this reduction of M_2 to $\overline{M}_2$, the first $r+1$ columns are unchanged. Upon subtracting from the $(r+1)$st column of $\overline{M}_2$ suitable multiples of each of the first r columns, a column vector is obtained all of whose elements are multiples of d_{r+1}. On the other hand, $\overline{M}_2$ has as invariant factors only 1's and 2's, and so (as in Part (3) of the proof of Theorem 3) we conclude that $d_{r+1} = 2$. Next choose the first $r+1$ columns of M_2 as basis for W^+, the remaining columns as basis for W^-; then the same type of argument shows that $d_{r+2} = 2$. Continuing in this manner, we obtain finally $d_{r+1} = d_{r+2} = \cdots = d_n = 2$.

Next we show that $d_{ij} = 0$ for $r < i < j$. For fixed $i > r$, let $j > i$ be minimal such that $d_{ij} = 1$. (Certainly each such d_{ij} is 0 or 1, since it is reduced modulo d_j.) Upon interchanging the ith and jth columns of M_2, we obtain the equivalent generator

$$M_3 = \begin{bmatrix} & & i & & j & \\ & & \vdots & & \vdots & \\ I^{(r)} & \cdots & \vdots & & \vdots & \cdots \\ & & 1 & 0 \cdots 0 & 2 & \cdots & i \\ 0 & \cdots & \vdots & & \vdots & \\ & & 2 & \cdots & 0 & \cdots & j. \\ & & \vdots & & \vdots & \\ & & \vdots & & \vdots & \end{bmatrix}$$

By subtracting from the $(i+1)$st, $\cdots$, jth rows suitable multiples of the ith row, a new generator M_4 is found, where

$$M_4 = \begin{bmatrix} & & i & & j & \\ & & \vdots & & \vdots & \\ I^{(r)} & \cdots & \vdots & & \vdots & \\ 1 & & 1 & 0 \cdots 0 & 2 & \cdots & i \\ & & 0 & & \vdots & \\ 0 & \cdots & \vdots & & \vdots & \\ & & 0 & \cdots & -4 & \cdots & j. \\ & & \vdots & & \vdots & \\ & & \vdots & & \vdots & \end{bmatrix}$$

But M_4 is a permissible generator, and is triangular. The above discussion has already shown that the diagonal elements in such a matrix are 1's and 2's. This gives a contradiction; therefore each $d_{ij}=0$, $r<i<j$. Thus we have

$$M_2 = \begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix}$$

where each element of R is reduced (mod 2) and so must be 0 or 1. Furthermore, R has no zero column, since the column vectors of the original matrix M were all primitive. This completes the proof of the first statement in the theorem.

2. The matrix given by (3) has invariant factors 1's and 2's. Therefore, by Theorem 3, it is permissible.

3. Since equivalent generators have the same determinant, the two generators given by (4) cannot be equivalent unless $r=t$. Suppose hereafter that $r=t$. We show now that if R and T are related, the generators are equivalent.

(i) If $R \equiv T$ (mod 2), set $R=T+2S$. Then

$$\begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix} = \begin{bmatrix} I & S \\ 0 & I \end{bmatrix} \begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix}.$$

(ii) If $R=PTQ$, where P permutes the rows of T, Q the columns of T, then

$$\begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix} = \begin{bmatrix} P & 0 \\ 0 & Q^{-1} \end{bmatrix} \begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix} \begin{bmatrix} P^{-1} & 0 \\ 0 & Q \end{bmatrix}.$$

(iii) If T is obtained from R by an operation of type (iv), we may assume, after repeated use of operations (ii) and (iii), that

$$R = \begin{bmatrix} 1 & u \\ v & S \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} 1 & u \\ -v & S - vu \end{bmatrix},$$

and we must show that

$$M = \begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix} \sim \begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix} = N.$$

Let B be the permutation matrix which interchanges the 1st and $(r+1)$st columns of M. Then

$$MB = \begin{bmatrix} 1 & 0 \cdots 0 & 1 & u \\ & & 0 & \\ & & \vdots & \\ v & I^{(r-1)} & \vdots & S \\ & & 0 & \\ 2 & 0 \cdots 0 & 0 & 0 \cdots 0 \\ 0 & 0 \cdots 0 & 0 & 2 \cdots 0 \\ \cdot & \cdots\cdots & \cdot & \cdots\cdots \\ 0 & 0 \cdots 0 & 0 & 0 \cdots 2 \end{bmatrix}.$$

Premultiplication of MB by

$$A_1 = \begin{bmatrix} 1 & 0 \cdots 0 \\ -v & \\ -2 & \\ 0 & I^{(n-1)} \\ \vdots & \\ 0 & \end{bmatrix}$$

gives

$$A_1 MB = \begin{bmatrix} I^{(r)} & & T \\ & -2 & 0 \cdots 0 \\ & 0 & \\ 0 & \vdots & 2I \\ & 0 & \end{bmatrix},$$

so there exists a matrix $A \in U_n$ such that

$$AMB = N. \tag{5}$$

Therefore $M \sim N$. (We shall have occasion to use the above discussion again in the course of this proof.)

4. We must now prove, conversely, that if

$$\begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix} = A \begin{bmatrix} I^{(r)} & T \\ 0 & 2I^{(n-r)} \end{bmatrix} B, \tag{6}$$

where $A \in U_n$, and where B permutes columns (possibly changing their signs), then R and T are related. We think of the columns of

$$N = \begin{bmatrix} I^{(r)} & T \\ 0 & 2I^{(n-r)} \end{bmatrix}$$

as partitioned into two sets, the first set consisting of the first r columns of N, the second of the last $(n-r)$ colunns. We say that B *displaces* a column of N if it moves the column out of its set. We now proceed by induction on the number of columns in the first set which B displaces.

If B does not displace any of the first r columns of N, we may write $B = C_1^{(r)} \dotplus C_2^{(n-r)}$, where each C_i is a permutation (and possibly sign-changing) matrix. We then obtain

$$\begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix} = A \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} C_1^{-1} & 0 \\ 0 & C_2^{-1} \end{bmatrix} \begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix} \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}$$

$$= A_2 \begin{bmatrix} I & C_1^{-1} T C_2 \\ 0 & 2I \end{bmatrix} = A_2 \begin{bmatrix} I & T_1 \\ 0 & 2I \end{bmatrix},$$

where $T_1 = C_1^{-1} T C_2$ is related to T, and $A_2 \in U_n$. From the uniqueness of Hermite canonical form, we see at once that $R \equiv T_1 \pmod 2$, so that R is related to T_1. Hence R and T are related.

Suppose now that B displaces some of the first r columns of N, and (for simplicity in exposition) suppose that the first column of N is displaced by B. Then at least one of the last $(n-r)$ columns which B displaces must have 1 as its first component; for otherwise, the 2-rank of the first r columns of

$$\begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix} B$$

would be less than r, while on the other hand these first r columns are also the first r columns of

$$A^{-1} \begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix},$$

and hence have 2-rank equal to r. Let us suppose that the qth column of N $(q>r)$ has 1 as its first component, and is displaced by B. Let B_1 be the permutation matrix which interchanges the 1st and qth columns of a matrix; by the argument in Part 3, there exists a matrix $A_3 \in U_n$ such that

$$A_3 \begin{bmatrix} I & T \\ 0 & 2I \end{bmatrix} B_1 = \begin{bmatrix} I & T_1 \\ 0 & 2I \end{bmatrix},$$

where T_1 is related to T by an operation of type (iv). Hence (6) becomes

$$\begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix} = AA_3^{-1} \begin{bmatrix} I & T_1 \\ 0 & 2I \end{bmatrix} B_1^{-1}B,$$

that is, we get a new equation in which T_1 is related to T, and where $B_1^{-1}B$ displaces one fewer of the first r columns than B does. This completes the proof of the theorem.

§9. While we are now in a position to find complete sets of nonequivalent generators, it will be more convenient to prove a type of duality theorem first. Let $W_1, \cdots, W_{2^n}$ be a maximal set in U_n. Then the set of their transposes $W_1', \cdots, W_{2^n}'$ is also a maximal set in U_n. Furthermore, if W is an involution of type $(p, q; x)$, so is W'. Thus the two maximal sets contain any given type of involution equally often, so that many times it will be enough to consider only one of the pair of sets.

THEOREM 6. *The permissible generating matrices*

$$M = \begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix} \quad \text{and} \quad M_1 = \begin{bmatrix} 2I^{(r)} & 0 \\ -R' & I^{(n-r)} \end{bmatrix}$$

give rise to two maximal sets; the elements in one set are the transposes of the elements in the other set. Furthermore,

$$M_1 \sim M^* = \begin{bmatrix} I^{(n-r)} & R' \\ 0 & 2I^{(r)} \end{bmatrix}.$$

Proof. As D ranges over all 2^n diagonal matrices with diagonal elements ± 1, the involution W defined by

$$WM = MD \tag{7}$$

ranges over the 2^n elements in the maximal set which M generates. From (7) we obtain

$$W'^{-1}M'^{-1} = M'^{-1}D'^{-1}.$$

However, $W^{-1} = W$ and $D'^{-1} = D$. Thus

$$W'M'^{-1} = M'^{-1}D.$$

But if

$$M = \begin{bmatrix} I & R \\ 0 & 2I \end{bmatrix}, \quad \text{then} \quad M'^{-1} = \frac{1}{2}\begin{bmatrix} 2I & 0 \\ -R' & I \end{bmatrix},$$

so that

$$W'M_1 = M_1D.$$

Hence the elements in the set which M_1 generates are the transposes of those generated by M. The last statement, $M_1 \sim M^*$, is trivial.

We shall say that M and M^* are *dual* generators. It might be well to point out that although R has no zero columns, R' may very well have such. In this case, we merely make each column of M^* primitive. For example,

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad M^* = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix};$$

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad M^* \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

Thus, in the first case M is self-dual (up to equivalence). A consequence of this result is that if the two generators given in (4) are equivalent, then R and T must have the same number of zero rows.

§10. In this section we shall list complete sets of nonequivalent generating matrices, and the types of involutions in the maximal sets they generate, for $n = 2, 3, 4$. Since in a maximal set the elements may be paired as $\pm W$, and since the negative of a $(p, q; x)$ involution is of type $(q, p; x)$, we can list the elements in a maximal set according to type $\pm(p, q; x)$.

For $n = 2$, there are 2 nonequivalent generators.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ generates $1 \pm (2, 0; 0)$ involution, $2\ (1, 1; 0)$ involutions.

$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ generates $1 \pm (2, 0; 0)$ involution, $2\ (1, 1; 1)$ involutions.

For $n = 3$, there are 4 nonequivalent generators, given by

$$M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \quad M_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

The types of involutions they generate are shown in the following table:

	M_1	M_2	M_3	M_4
$\pm(3, 0; 0)$	1	1	1	1
$\pm(2, 1; 0)$	3	1	0	0
$\pm(2, 1; 1)$	0	2	3	3

We may remark that M_1 and M_2 are each self-dual, while M_3 and M_4 are duals of one another.

For $n=4$, there are 8 nonequivalent generators, given by

$$M_1=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\quad M_2=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&2\end{bmatrix},\quad M_3=\begin{bmatrix}1&0&0&0\\0&1&0&1\\0&0&1&1\\0&0&0&2\end{bmatrix},\quad M_4=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\\0&0&0&2\end{bmatrix},$$

$$M_5=\begin{bmatrix}1&0&1&1\\0&1&0&0\\0&0&2&0\\0&0&0&2\end{bmatrix},\quad M_6=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&2&0\\0&0&0&2\end{bmatrix},\quad M_7=\begin{bmatrix}1&0&1&1\\0&1&1&0\\0&0&2&0\\0&0&0&2\end{bmatrix},\quad M_8=\begin{bmatrix}1&1&1&1\\0&2&0&0\\0&0&2&0\\0&0&0&2\end{bmatrix}.$$

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	
$\pm(4, 0; 0)$	1	1	1	1	1	1	1	1	self-dual: M_1, M_2, M_6, M_7
$\pm(3, 1; 0)$	4	2	1	0	1	0	0	0	duals: M_3 and M_5, M_4 and M_8.
$\pm(3, 1; 1)$	0	2	3	4	3	4	4	4	
$(2, 2; 0)$	6	2	0	0	0	2	0	0	
$(2, 2; 1)$	0	4	6	6	6	0	2	6	
$(2, 2; 2)$	0	0	0	0	0	4	4	0	

In order to find a complete set of nonequivalent generators for a given n, we list for each r $(1 \leqq r \leqq n)$ a complete set of $r \times (n-r)$ arrays of 0's and 1's, having no zero columns, such that no two arrays can be gotten from one another by row and column permutations. It is not too difficult to decide whether two listed arrays can be gotten one from the other by use of type

(iv) operations coupled with the other three types. By striking out all but one from each set of related arrays, we obtain a complete set of unrelated $r \times (n-r)$ arrays. As R ranges over all of these arrays, the matrix given by

$$M = \begin{bmatrix} I^{(r)} & R \\ 0 & 2I^{(n-r)} \end{bmatrix} \tag{8}$$

gives nonequivalent generators. The totality of these for all r $(1 \leqq r \leqq n)$ form a complete set of nonequivalent generators.

We let C_n denote the number of nonconjugate abelian sets of involutions in U_n containing 2^n elements; that is, C_n is the number of nonequivalent $n \times n$ generators. The method described above can be used to show that $C_5 = 16$ and $C_6 = 36$. (This last figure dashes one's expectations that $C_n = 2^{n-1}$.) However, to compute C_n by the above procedure is very tedious for large n. It would be of interest to have a simple method for evaluating C_n.

§11. Let $f(p, q; x)$ be the maximum number of involutions of type $(p, q; x)$ which occur in any maximal set; this maximum need be taken only over a complete set of nonconjugate maximal sets. Trivially $f(p, q; x) = f(q, p; x) \leqq C_{n,p}$. We now note some partial results on the evaluation of $f(p, q; x)$. By considering the maximal set generated by $I^{(n)}$, we see that $f(p, q; 0) = C_{n,p}$. Further, this is the only maximal set (up to conjugacy) all of whose involutions have $x = 0$.

Next set

$$M = \begin{bmatrix} 1 & 1 \cdots 1 \\ 0 & \\ \vdots & 2I^{(n-1)} \\ 0 & \end{bmatrix}.$$

In the maximal set which M generates, every involution (except $\pm I$) has $x = 1$. Therefore $f(p, q; 1) = C_{n,p}$ for $1 \leqq p \leqq n-1$. Further, the maximal sets generated by M and its dual M^* are the only sets (up to conjugacy) all of whose elements (except $\pm I$) have $x = 1$.

For $x > 1$, the problem of evaluating $f(p, q; x)$ becomes more difficult. For example, it may be shown that for fixed $x > 1$, and fixed $q > x$, we have $f(n-q, q; x) < C_{n,q}$ for all sufficiently large n. On the other hand, let $V^{(k)}$ denote a square matrix all of whose elements are $+1$, except for 0's along the main diagonal. Set

$$M = \begin{bmatrix} I^{(k)} & V \\ 0 & 2I^{(k)} \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} I^{(k+1)} & 1 \cdots 1 \\ & V \\ 0 & 2I^{(k)} \end{bmatrix}$$

according as $n = 2k$ or $n = 2k+1$. Then the maximal set generated by M con-

tains $C_{n,2}$ involutions of type $(n-2, 2; 2)$ for $n \geqq 6$. In general it is true that $f(n-x, x; x) = C_{n,x}$ for $x < [n/2]$.

§12. We shall now characterize the $\pm(n-1, 1; 0)$ involutions in U_n by inner properties; however, we shall not give any group-theoretic method for distinguishing between the $(n-1, 1; 0)$ and $(1, n-1; 0)$ involutions. For the moment, take $n > 4$. Then we show that $f(p, q; x) > n$ except when $(p, q; x) = \pm(n-1, 1; 0)$, $\pm(n-1, 1; 1)$ or $\pm(n, 0; 0)$. Certainly $f(p, q; 0) = C_{n,p} > n$ when $\min(p, q) > 1$, and also $f(p, q; 1) = C_{n,p} > n$ when $\min(p, q) > 1$. We must therefore prove that $f(p, q; x) > n$ for $1 < x \leqq q \leqq p < n-1$.

Let us write $n = ax + b$, $0 \leqq b < x$. Since $x \leqq n/2$, certainly $a \geqq 2$. Define

$$M = \begin{bmatrix} I^{(x)} & I^{(x)} & I^{(x)} \cdots I^{(x)} & I^{(b)} \\ 0 & & 2I^{(n-x)} & 0 \end{bmatrix}.$$

Case 1. $q \geqq x + b$. If we choose any q consecutive columns of M as basis for W^-, and the remaining p columns as basis for W^+, then W is of type $(p, q; x)$ because the 2-rank of each of the two submatrices is x. Thus, the maximal set generated by M contains at least n involutions of type $(p, q; x)$. We may obtain one extra $(p, q; x)$ involution by choosing the 1st column of M instead of the $(x+1)$st or $(2x+1)$st, etc., in one of the previously considered n partitions of M. (This extra involution does not arise when $n = 4$ and $x = 2$; indeed, $f(2, 2; 2) = 4$.) Hence we have $f(p, q; x) > n$ when $q \geqq x + b$.

The same argument also works for $x = 2$ and $x = 3$ even when $q < x + b$, provided that we change M by replacing

$$\begin{pmatrix} I^{(b)} \\ 0 \end{pmatrix} \text{ by } \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \text{ or } \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix},$$

according as $x = 2$, $b = 1$, or $x = 3$, $b = 1$, or $x = 3$, $b = 2$, respectively.

Case 2. Now let $4 \leqq x \leqq q < x + b$. Choose any x linearly independent columns from the first ax columns of M, then pick $q - x$ other columns from the last b columns of M, and use these as basis for W^-; let the remaining p columns of M serve as basis for W^+. Every such W will be of type $(p, q; x)$, and there will be at least a^x of them. Thus

$$f(p, q; x) \geqq a^x.$$

Since $a \geqq 2$, certainly $f(p, q; x) \geqq 2^x > n$ when $x > \log_2 n$. When $4 \leqq x \leqq \log_2 n$, we have

$$a > \frac{n}{x} - 1 \geqq \frac{n}{\log_2 n} - 1,$$

so that

$$f(p, q; x) \geqq \left(\frac{n}{\log_2 n} - 1\right)^x \geqq \left(\frac{n}{\log_2 n} - 1\right)^4.$$

However, it is easy to verify that

$$\frac{n}{\log_2 n} - 1 > n^{1/4} \qquad \text{for } n \geqq 9.$$

Hence in all cases $f(p, q; x) > n$ for $n > 4$ except when $(p, q; x) = \pm(n-1, 1; 0)$, or $\pm(n-1, 1; 1)$, or $\pm(n, 0; 0)$. On the other hand, when $n = 4$, the table in §10 permits us to characterize the $\pm(3, 1; 0)$ involutions by inner properties.

Now we may further distinguish the $\pm(n-1, 1; 0)$ involutions from the $\pm(n-1, 1; 1)$ involutions by observing that all maximal sets containing n involutions of type $(n-1, 1; 0)$ are conjugate, whereas this is false (for $n > 2$) for involutions of type $(n-1, 1; 1)$. For $n = 2$, other arguments may be used to make this distinction(9).

§13. Define $g(p, q; x)$ to be the maximum number of elements in a maximal $(p, q; x)$ set. The previous discussion shows at once that $f(p, q; x) \leqq g(p, q; x) \leqq C_{n,p}$. We remark that neither equality sign can hold in general. For example, we have already shown that $f(2, 2; 2) = 4$; we prove now that $g(2, 2; 2) = 6$. Let

$$N = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{bmatrix}.$$

The maximal set which N generates contains 16 involutions; of these, the 8 involutions of types $\pm(3, 1)$ are not integral, while the remaining 8 are $\pm I$ and 6 integral involutions of type $(2, 2; 2)$. On the other hand, it is easy to verify that $g(3, 2; 2) < 10$. These remarks show that "maximal" sets in U_n in the sense of embeddability need not be maximal in size. It would be of interest to investigate the structure of abelian sets of involutions in U_n which could not be embedded in larger sets.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.
UNIVERSITY OF ILLINOIS,
URBANA, ILL.

(9) Hua and Reiner, op. cit.