PAIRS OF MATRICES OF ORDER TWO WHICH GENERATE FREE GROUPS[1]

BY K. GOLDBERG AND M. NEWMAN

Throughout this paper $A = (a_{ij})$ and $B = (b_{ij})$ will denote rational integral unimodular matrices of order two which are not of finite period.

Let us say that an element of a matrix is *dominant* if it is larger in absolute value than any other element of the matrix.

Our object is to prove the following theorem:

THEOREM. *If a_{12} is dominant in A and b_{21} is dominant in B, then A and B generate a free group.*

The first result in this direction was due to I. N. Sanov [1] who proved that $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and A^T generate a free group. The methods used in this paper are derived from Sanov's proof of his result.

More recently J. L. Brenner [2] has shown that $A = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ and A^T generate a free group for all real $m \geqq 2$.

These results were brought to our attention by Professor Brenner and a generalization was suggested by O. Taussky-Todd.

1. Two lemmas

We find it convenient to separate the proof of the theorem into two parts which are described by the lemmas below.

We define $A^n = (a_{ij}^{(n)})$ and $B^n = (b_{ij}^{(n)})$ where n is an integer.

LEMMA 1. *If $a_{12}^{(n)}$ is dominant in A^n and $b_{21}^{(n)}$ is dominant in B^n for all $n \neq 0$, then A and B generate a free group.*

LEMMA 2. *If a_{12} is dominant in A, then $a_{12}^{(n)}$ is dominant in A^n for all $n \neq 0$.*

If A has trace t and determinant d, then the fact that A is not of finite period is used only to imply that $t \neq 0$ for $d = -1$ and $|t| \geqq 2$ for $d = 1$.

The fact that a_{12} is dominant in A implies $|a_{12}| -2$, $|a_{11}a_{22}| -1$, $|a_{11}| - |a_{21}|$ and $|a_{12} - a_{11}| - |a_{22} - a_{21}|$ are all nonnegative: $|a_{12}|$ is at least 2 because at least one other element is not 0, neither diagonal element vanishes because then $|a_{12}| > 1$ would divide the determinant $d = \pm 1$, a_{21} is the least element because $|a_{11}a_{22} - a_{12}a_{21}| = 1$ and $|a_{12}| - |a_{ii}| \geqq 1$, and

Received October 3, 1956.

[1] The preparation of this paper was supported in part by the Office of Naval Research.

the last inequality follows from $|a_{11}(a_{22} - a_{21}) - a_{21}(a_{12} - a_{11})| = 1$ when $|a_{11}| > 1$, and for $|a_{11}| = 1$ by an enumeration of cases.

2. Proof of Lemma 1

Suppose $|x| \geqq |y|$, $x \neq 0$, and set

$$(x\ y)A = (x'\ y'). \tag{1}$$

We shall show that $|y'| \geqq |x|$ and $|y'| \geqq |x'|$.

First we have

$$|y'| = |a_{12}x + a_{22}y| \geqq |a_{12}x| - |a_{22}y| \geqq (|a_{12}| - |a_{22}|)|x| \geqq |x|.$$

Second we may choose x, a_{11}, and a_{12} positive while retaining the dominance of a_{12}. This may be done constructively by premultiplying equation (1) by $\operatorname{sgn} x = x/|x|$ and postmultiplying by the matrix diag(sgn a_{11}, sgn a_{12}).

Then $x' = a_{11}x + a_{21}y \geqq 0$ since $a_{11} \geqq |a_{21}|$ and $x \geqq |y|$, and $y' = a_{12}x + a_{22}y > 0$ since $a_{12} > |a_{22}|$ and $x \geqq |y|$. Thus

$$\begin{aligned}|y'| - |x'| = y' - x' &= (a_{12} - a_{11})x + (a_{22} - a_{21})y \\ &\geqq (a_{12} - a_{11} - |a_{22} - a_{21}|)|y| \geqq 0.\end{aligned}$$

Similarly, suppose $|y| \geqq |x|$ and set $(x\ y)B = (x'\ y')$. Then $|x'| \geqq |y|$ and $|x'| \geqq |y'|$.

These remarks are based solely on the dominance of a_{12} in A and b_{21} in B. Therefore if we assume that $a_{12}^{(n)}$ is dominant in A^n and $b_{21}^{(n)}$ is dominant in B^n for all $n \neq 0$, the same inequalities will hold when A is replaced by A^n in equation (1) and B is similarly replaced by B^n.

Now consider an arbitrary product of powers of A and B:

$$T = A^{s_0} B^{s_1} A^{s_2} \cdots \qquad \text{with } s_n \neq 0 \text{ for } n = 1, 2, \cdots.$$

We may assume that $s_0 \neq 0$. Write

$$(1\quad 0)A^{s_0} = (x_0\, y_0),\ (x_{2n}\, y_{2n})B^{s_{2n+1}} = (x_{2n+1}\, y_{2n+1})$$

and

$$(x_{2n-1}\, y_{2n-1})A^{s_{2n}} = (x_{2n}\, y_{2n}).$$

By our comments above, if $|x_{2n-1}| \geqq |y_{2n-1}|$, we will have $|y_{2n}| \geqq |x_{2n-1}|$ and $|y_{2n}| \geqq |x_{2n}|$, so that $|x_{2n+1}| \geqq |y_{2n}|$ and $|x_{2n+1}| \geqq |y_{2n+1}|$ and so on. Since we begin with the vector $(1\quad 0)$ we have by induction

$$|y_0| \leqq |x_1| \leqq |y_2| \leqq \cdots \leqq |x_{2n-1}| \leqq |y_{2n}| \leqq |x_{2n+1}| \leqq \cdots.$$

But $|y_0| = |a_{12}^{(s_0)}| \geqq 2$ so that either $|x_n|$ or $|y_n|$ is greater than 1 for every n. It follows that $(x_n\, y_n) \neq (1\quad 0)$ for every n, and therefore $T \neq I$.

Thus no nontrivial product of the powers of A and B can reduce to the identity which proves that A and B generate a free group.

3. Proof of Lemma 2

Let t be the trace and d the determinant of A. We may assume $t \geqq 0$, since otherwise A may be replaced by $-A$. We may assume $a_{12} \geqq 0$, since for $\varepsilon = \pm 1$ the similarity

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}^{-1} A \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & \varepsilon a_{12} \\ \varepsilon a_{21} & a_{22} \end{pmatrix}$$

takes a_{12} into εa_{12} and leaves t unchanged. Suppose that $\mu = \pm 1$ is fixed but arbitrary. Set

$$\Delta_n = a_{12}^{(n)} - \mu a_{11}^{(n)}.$$

(The discussion is the same for the three remaining cases). Then

$$\Delta_0 = a_{12}^{(0)} - \mu a_{11}^{(0)} = -\mu,$$

$$\Delta_1 = a_{12}^{(1)} - \mu a_{11}^{(1)} = a_{12} - \mu a_{11},$$

and

$$\Delta_{n+1} = t\Delta_n - d\Delta_{n-1}, \quad n \geqq 1.$$

We see that always $\Delta_1 \geqq 1$. Assume first that $t \geqq 2$. Then

$$\Delta_2 = t\Delta_1 - d\Delta_0 \geqq 2\Delta_1 + d\,\mu \geqq \Delta_1 .$$

Thus if $\Delta_{n-1} > 0$ and $\Delta_n \geqq \Delta_{n-1}$, then $\Delta_n > 0$ and

$$\Delta_{n+1} = t\Delta_n - d\Delta_{n-1} \geqq 2\Delta_n - \Delta_{n-1} \geqq \Delta_n .$$

Therefore $\Delta_n > 0$ for $n \geqq 1$ and so

$$a_{12}^{(n)} > | a_{11}^{(n)} |, \qquad n \geqq 1. \tag{2}$$

If $t \leqq 1$, so that $t = 1$, then $d = -1$. Here

$$\Delta_2 = t\Delta_1 - d\Delta_0 = \Delta_1 + \Delta_0 = \Delta_1 - \mu.$$

If $\Delta_1 \geqq 2$, then $\Delta_2 \geqq 1$, and Δ_n is clearly positive for $n \geqq 1$. If $\mu = -1$, then $\Delta_2 \geqq 2$, and here also Δ_n is positive for $n \geqq 1$. Thus we need only consider $\mu = 1$ and $\Delta_1 = 1$. This however leads to a contradiction; a_{12} can not be dominant in this case, and so (2) is always true. If we note in addition that $a_{11}^{(-n)} = da_{22}^{(n)}$, $a_{12}^{(-n)} = -da_{12}^{(n)}$, $a_{21}^{(-n)} = -da_{21}^{(n)}$, $a_{22}^{(-n)} = da_{11}^{(n)}$, then the proof of Lemma 2 is complete, and so the theorem is proved.

References

1. I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk SSSR (N.S.), vol. 57 (1947), pp. 657–659 (Russian).
2. J. L. Brenner, *Quelques groupes libres de matrices*, C. R. Acad. Sci. Paris, vol. 241 (1955), pp. 1689–1691.

National Bureau of Standards
Washington, D. C.