GRUSHKO'S THEOREM

ROGER C. LYNDON[1]

We give a proof of Grushko's Theorem which seems simpler and more straightforward than any we can find in the literature (see [1], [2], [4]). The method is a simplification of one we have used elsewhere (see [3]); the referee has helped with the simplification.

Let a group G be the free product, without amalgamation, of a family of its subgroups G_j. Each element x of G has a unique representation as a normal product of nontrivial factors from the G_j, with no two adjacent factors from the same G_j. The length $|x|$ of x is the number of factors in this product. Grushko's Theorem may be stated as follows.

THEOREM. *Let G be generated by a finite set X. Assume that, if x is in X and g is in the subgroup generated by all the elements of X other than x, then neither xg nor gx is shorter than x. Then each element of X belongs to one of the groups G_j.*

Our proof rests upon showing that X may be assumed to have a somewhat stronger property.

If an element x of G has normal form $x=a_1 \cdots a_n$, where $n=2k$ or $n=2k+1$, we define the "left half" of x to be $L(x)=a_1 \cdots a_k$. The "right half" of x is $L(x^{-1})^{-1}$. We define a relation $x \sim y$ to hold between elements x and y of G if $xy=1$ or if x and y belong to a common group uG_ju^{-1} conjugate to one of the G_j.

Let the union of the groups G_j be well ordered. The induced lexicographical order on normal products defines a well ordering $x \prec y$ on G. It is clear that we can define a new well ordering, $x<y$, on G, with the following properties:

(1) *if* $|x|<|y|$ *then* $x<y$;

(2) *if* $|x|=|y|$ *and* $L(x)\prec L(y)$, *then* $x<y$;

(3) *if* $|x|=|y|$, $L(x)=L(y)$, *and* $L(x^{-1})\prec L(y^{-1})$, *then* $x<y$;

(4) *all nontrivial elements x of each subgroup uG_ju^{-1} (which have the same length $|x|=2|u|+1$ and the same $L(x)=L(x^{-1})=u$) occur consecutively.*

A subset $X\subseteq G$ is *irreducible* if:

(i) $1\notin X$;

(ii) $x\in X$ *implies* $x\leq x^{-1}$;

Received by the editors January 29, 1964 and, in revised form, May 15, 1964.

[1] This work was supported in part by the National Science Foundation.

(iii) $x \in X$ *and* $g \in \mathrm{gp}\{X-x\}$ *implies* $x \leqq xg, gx$.

Let $X \subseteq G$ be finite. Then it is clear that an irreducible set X', such that $\mathrm{gp}\, X' = \mathrm{gp}\, X$, can be obtained from X by a finite number of steps consisting of omitting 1 from X, replacing some x by x^{-1}, or replacing x by xg where $g \in \mathrm{gp}\{X-x\}$ and $|xg| \leqq |x|$. If X satisfies the hypothesis of Grushko's Theorem, the greatest length of an element of X' is the same as that for X. Therefore, it suffices to show that if X is an irreducible set of generators for G, then each x in X has length $|x| = 1$.

Henceforth we assume X irreducible. Let N be the union of all subgroups $uG_j u^{-1}$ of G, and, for $x \in X \cap N$, let $N(x) = \mathrm{gp}\{y \colon y \in X$ and $y \sim x\}$. Define

$$Y = X \cup X^{-1} \cup \bigcup \{N(x) - 1 \colon \text{all } x \in X \cap N\}.$$

Note that $x \in Y$ iff either $x^{\pm 1} \in X$ or else $x \in N(x') - 1$ for some $x' \in X \cap N$. We shall examine products $y_1 \cdots y_m$ such that $y_1, \cdots, y_m \in Y$ and $y_1 \not\sim y_2, \cdots, y_{m-1} \not\sim y_m$.

Lemma 1. *If $x, y \in Y$ and $x \not\sim y$, then $|x|, |y| \leqq |xy|$.*

Proof. Assume, by symmetry, that $|x| \leqq |y|$; we must show that $|y| \leqq |xy|$. If $x = y$, this is immediate. If $y^{\pm 1} \in X$, then $x \neq y$ and $x \not\sim y$ implies that $x \in \mathrm{gp}\{X - y^{\pm 1}\}$, and, from the irreducibility of X, it follows that $y^{\pm 1} \leqq xy$, whence $|y| \leqq |xy|$. Suppose that $|x| = |y|$. If $x^{\pm 1} \in X$ the same argument shows that $|x| \leqq |xy|$, hence $|y| \leqq |xy|$. If neither $x^{\pm 1} \in X$ nor $y^{\pm 1} \in X$, then $x, y \in N$, and $|x| = |y| \geqq |xy|$ would imply that $L(x) = L(y)$ and $x \sim y$, contrary to hypothesis.

The case remains that $|x| < |y|$ and $y \in N(y')$ for some $y' \in X \cap N$. If $|xy| < |y|$, then more than half of x must cancel into y and, since $|x| < |y|$, more than half of x cancels into $L(y)$. Since $L(y) = L(y')$, more than half of x must cancel into the part $L(y')$ of y' in the product xy', whence $|xy'| < |y'|$. Since $y' \in X$ and $x \neq y'$ with $x \not\sim y'$ implies $x \in \mathrm{gp}\{X - y'\}$, this contradicts the irreducibility of X.

Lemma 2. *If $x, y \in Y$, with $x \not\sim y$ and $|xy| = |x|$, then $L(y) \precsim L(y^{-1})$.*

Proof. If $x \in N(x')$ for some $x' \in X \cap N$, then the hypothesis of the lemma holds with x replaced by x'. Thus we may assume that $x^{\pm 1} \in X$. By Lemma 1, $|y| \leqq |xy|$, whence $|y| \leqq |x|$. From $|xy| \leqq |x|$ it follows that the left half of y must cancel into x and, since $|y| \leqq |x|$, into the right half of x; thus $L(x^{-1})$ begins with $L(y)$. From the exact equality, $|xy| = |x|$, it follows that the left half of x remains in xy, hence that $L(xy) = L(x)$; and that the right half of y remains in xy, hence that $L((xy)^{-1})$ begins with $L(y^{-1})$. Suppose that $L(y^{-1}) \prec L(y)$. Since $L((xy)^{-1})$ begins with $L(y^{-1})$ and $L(x^{-1})$ with $L(y)$, it follows that $L((xy)^{-1}) \prec L(x^{-1})$. Since $L(xy) = L(x)$, it follows from (1), (2), and (3) that $xy < x$ and $(xy)^{-1} < x^{-1}$. Since $x^{\pm 1} \in X$ and $y \neq x$, $y \not\sim x$ implies that $y \in \mathrm{gp}\{X - x^{\pm 1}\}$, this contradicts the irreducibility of X.

LEMMA 3. *If $x, y, z \in Y$ and $|xy| = |x|$, $|yz| = |z|$, then $L(y) = L(y^{-1})$, that is, $y \in N$.*

PROOF. If $x \sim y$ or $y \sim z$, it follows that $y \in N$. Otherwise $|xy| = |x|$ implies $L(y) \preceq L(y^{-1})$ by Lemma 2, while, symmetrically, $|yz| = |z|$ implies $L(y^{-1}) \preceq L(y)$.

LEMMA 4. *If x, y, $z \in Y$ and $|xy| = |x|$, $|yz| = |y| = |z|$, $|zw| = |w|$, then $y \sim z$.*

PROOF. Lemma 3 applied to x, y, and z gives $y \in N$, and, applied to y, z, and w, gives $z \in N$. Now y, $z \in N$ and $|yz| = |y| = |z|$ implies that $y \sim z$.

LEMMA 5. *If $x, y, z \in Y$ and $x \not\sim y$, $y \not\sim z$, then $|xyz| \geqq |x| - |y| + |z|$.*

PROOF. Assume that $|xyz| < |x| - |y| + |z|$. Unless y has normal form either $y = uv$ or $y = ubv$ with $|b| = 1$, where u cancels into x and v into z, there would remain in xyz at least two uncancelled factors from y, and the inequality could not hold. By Lemmas 1 and 3, u and v are the left and right halves of y, and $y \in N$, whence $v = u^{-1}$ and $y = ubu^{-1}$. Moreover, the inequality requires that x and z have normal forms $x = pau^{-1}$ and $z = ucq$ where a, $c \sim b$ and $abc = 1$.

By Lemma 1, the hypothesis that $|xy| = |x|$ implies $|y| \leqq |x|$. If $|y| = |x|$, then $x \in N$ is impossible, since $|x| = |y| = |xy|$ and x, $y \in N$ would imply $x \sim y$, contrary to hypothesis. If $|y| < |x|$ and $x \in N(x')$ for some $x' \in X \cap N$, the same hypotheses hold with x replaced by x'. Thus, in any case, we may suppose $x^{\pm 1} \in X$ and, similarly, $z^{\pm 1} \in X$.

Suppose that $|y| < |x|$, $|z|$. Now $x = pau^{-1}$ and $xy = pabu^{-1} = pc^{-1}u^{-1}$, and $L(x) = L(xy)$. From the irreducibility of X, using (1), (2), and (3), we have $L(x^{-1}) \preceq L((xy)^{-1})$, whence $ua^{-1} \preceq uc$ and $a^{-1} \preceq c$. Similar comparison of $z = ucq$ with $yz = ubcq = ua^{-1}q$ gives $c \preceq a^{-1}$. This implies that $c = a^{-1}$, whence $abc = 1$ implies that $b = 1$ and hence $y = ubu^{-1} = 1$, contrary to $y \in Y$.

If $x = z^{-1}$, then again $c = a^{-1}$, a contradiction. If $x = z$, then x begins with $u = L(y)$ and ends with u^{-1}; then $|x| = |y|$ would imply $x \sim y$, contrary to hypothesis.

The case remains that $x \neq z^{\pm 1}$, while $|y| = |x|$ or $|y| = |z|$, say $|y| = |x| \leqq |z|$. But now the inequality $|xyz| < |x| - |y| + |z| = |z|$, with y, $x \in \mathrm{gp}\{X - z^{\pm 1}\}$, contradicts the irreducibility of X.

LEMMA 6. *If* $y_1, \cdots, y_m \in Y$ *and* $y_i \nsim y_{i+1}$ *for all* i, $1 \leqq i < m$, *then*

$$|y_1 \cdots y_m| = \sum_1^m |y_i| - \sum_1^{m-1} (|y_i| + |y_{i+1}| - |y_i y_{i+1}|).$$

PROOF. The number $d_i = |y_i| + |y_{i+1}| - |y_i y_{i+1}|$ is the number of factors from the normal forms of y_i and y_{i+1} that cancel in the product $y_i y_{i+1}$, with 1 added if the two innermost remaining factors are from the same G_j and so combine to give a single factor in the normal form for $y_i y_{i+1}$. The lemma asserts that the normal form for $y_1 \cdots y_m$ can be obtained from those for the y_i by first cancelling between adjacent y_i and y_{i+1}, and then counting as a single factor the product of every maximal consecutive sequence of the remaining factors that lie in the same G_j.

In view of Lemmas 1 and 3, some factor from each y_i must remain after cancellation. Any consecutive sequence of factors in the same G_j must then arise from consecutive y_i, and we have to show that no product of such a sequence is 1. This follows from the assumptions for a sequence of one or two such factors. If three consecutive factors a, b, and c, all in the same G_j, arise from y_i, y_{i+1}, y_{i+2}, then Lemma 5 ensures that $abc \neq 1$. Finally, as many as four such factors, a, b, c, and d, from y_i, y_{i+1}, y_{i+2} and y_{i+3} is impossible, since then the hypotheses of Lemma 4 would be satisfied, and we should have $y_{i+1} \sim y_{i+2}$, contrary to assumption.

LEMMA 7. *If* $y_1, \cdots, y_m \in Y$ *and* $y_i \nsim y_{i+1}$ *for all* i, $1 \leqq i < m$, *then for each* h, $1 \leqq h \leqq m$,

$$|y_h| \leqq |y_1 \cdots y_m|.$$

PROOF. Regroup the equation of Lemma 6 in the form $|y_1 \cdots y_m| = \sum_1^{h-1} (|y_i| - d_i) + |y_h| + \sum_{h+1}^m (|y_i| - d_{i-1})$, and observe that, by Lemma 1, each $|y_i| - d_i \geqq 0$ and each $|y_i| - d_{i-1} \geqq 0$.

LEMMA 8. *If* X *is irreducible and* $g \in \text{gp } X$, *then* g *is in the group generated by those* $x \in X$ *for which* $|x| \leqq |g|$.

PROOF. By hypothesis, $g = z_1 \cdots z_n$ for some $z_i \in X \cup X^{-1}$, hence $z_i \in Y$. By successively combining adjacent factors $z_i \sim z_{i+1}$ and deleting factors 1, we obtain $g = y_1 \cdots y_m$ for $y_1, \cdots, y_m \in Y$ and no $y_i \sim y_{i+1}$. By Lemma 7, each $|y_i| \leqq |g|$, while clearly each y_i is contained in the group generated by those x in X with $|x| = |y_i|$, hence with $|x| \leqq |g|$. It follows that $g = y_1 \cdots y_m$ is in this group.

LEMMA 9. *If* X *is irreducible and generates* G, *then* $|x| = 1$ *for all* $x \in X$.

PROOF. Let X_1 be the set of all x in X for which $|x| = 1$. Since each $G_j \subseteq G = \mathrm{gp}\, X$, we conclude by Lemma 8 that each $G_j \subseteq \mathrm{gp}\, X_1$, and hence that $G = \mathrm{gp}\, X_1$. It follows from the irreducibility of X that $X = X_1$.

This completes the proof of Grushko's Theorem.

BIBLIOGRAPHY

1. I. A. Grushko, *On the bases of a free product of groups*, Mat. Sb. **8** (1940), 169–182.

2. A. G. Kurosh, *The theory of groups*. II, Chelsea, New York, 1955.

3. R. C. Lyndon, *Length functions in groups*, Math. Scand. 12 (1963), 209–234.

4. B. H. Neumann, *On the number of generators of a free product*, J. London Math. Soc. **18** (1943), 12–20.

UNIVERSITY OF MICHIGAN

GENERALIZED FUNCTIONS OF SYMMETRIC MATRICES

MARVIN MARCUS[1] AND MORRIS NEWMAN

1. Introduction. In an abstract published in 1961 [4] we announced the following result:

Let A be an n-square positive semi-definite matrix and assume that $A \geqq S$ where S is doubly stochastic. Then

$$\operatorname{per}(A) \geqq n!/n^n. \tag{1.1}$$

The notation $A \geqq S$ means $a_{ij} \geqq s_{ij}$, $i, j = 1, \cdots, n$. A doubly stochastic (d.s.) matrix has non-negative entries and every row and column sum is 1. The permanent, per (A), is the function defined by

$$\operatorname{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)} \tag{1.2}$$

where the summation extends over the whole symmetric group of degree n, S_n.

In 1962 [3] we also proved that:

If S is an n-square positive semi-definite symmetric matrix which is doubly stochastic in the extended sense then

$$\operatorname{per}(S) \geqq n!/n^n. \tag{1.3}$$

Received by the editors June 8, 1964.

[1] The work of this author was supported by NSF Grant GP-1085.