Reprinted from JOURNAL OF MATHEMATICAL ANALYSIS AND APPLICATIONS Vol. 7, No 3, December 1963

On a Formal Product over the Conjugate Classes in a Free Group

M. P. SCHÜTZENBERGER* AND S. SHERMAN†

Harvard University Medical School
Wayne State University

Submitted by Richard Bellman

I. INTRODUCTION

In [1, Eq. (2)] a special case of [2, Theorem 1] (another special case of which was conjectured by Feynman in connection with the Ising model for ferromagnetism) is shown to be an analogue of an identity used by Witt, the special case playing a role relative to free groups analogous to that played by the Witt identity relative to free semigroups. Furthermore, in [1] the question is raised of establishing the special case by methods short of proving [2, Theorem 1]. In the current note a selfcontained proof of a non-commutative generalization of the special case is presented. More explicitly, given a set X_1 and a mapping ρ of X_1 into a certain algebra A we verify the identity of the formal products $\Pi\{(1 - \rho x)^2 \colon x \in X_1\}$ and $\Pi\{(1 - \rho g) \colon g \in C\}$ where the subset C of the free group G generated by X_1 is such that every $g \in G$, $g \neq e_G$ is conjugate of some positive power of one and only one element of C and where $\rho \colon G \to A$ is defined below. Since these definitions are not independent of the choice of X_1 it is convenient to introduce the set X consisting of the elements of X_1 together with their inverses so that A is the algebra over the ring R of the free monoid F generated by X. The anti-automorphism (of period 2) $\alpha \colon F \to F$, the idempotent endomorphism $\beta \colon F \to F$, the epimorphism $\nu \colon F \to G$ are defined by their restriction to X_1, that is

$$\text{for all } x \in X_1,\ x = \beta x = \beta\alpha x;\ (\nu x)^{-1} = \nu\alpha x.$$

The set $\bar{F}$ of the so called *reduced words* is the complement in F of the ideal generated by all words $x\alpha x (x \in X)$ and, as it is well known, the restriction of ν to $\bar{F}$ is a bijection. We abbreviate $\{f \in F \colon f \neq 1\}$ by F^+.

* The research of this author has been supported by the Commonwealth Fund and IBM.

† The research of this author has been supported by the National Science Foundation and the Michigan Institute of Science and Technology.

II. Weight Function

Let there be given a partial order $\lessdot$ (where $\not\lessdot$ means not $\lessdot$) on X_1 and a mapping $r: X_1 \times X_1 \to R$. Writing $s(x, x') = -1$ if $x \lessdot x'$, $= +1$ otherwise, we extend r to a mapping $X \times X \to R$ by the following rules:

For any $x, x' \in X$, $x \neq x'$

1. $r(\alpha x, \alpha x) = r(x, x) = -1$,
2. $r(x, x') = s(x, x')r(x, \alpha x) = -s(x', x)r(\alpha x, x') = -s(x, x')s(x', x)r(\alpha x, \alpha x')$
3. $r(x, \alpha x) = r(\alpha x, x) = 0$.

For any $f \in F^+$, $f = x_{i_1} x_{i_2} \cdots x_{i_m}$ $(x_{i_1}, x_{i_2}, \cdots, x_{i_m} \in X)$ we define

$$\rho' f = r(x_{i_1}, x_{i_2})\, r(x_{i_2}, x_{i_3}) \cdots r(x_{i_{m-1}}, x_{i_m})\, r(x_{i_m}, x_{i_1})$$

and $\rho f = \rho' f \cdot \beta f \in A$. For $g \in G$, $g \neq e_G$, we define $\rho g = \rho f$ where $f (= \nu^{-1} g \cap \bar{F})$ is the reduced word representing g.

In equivalent manner, let μ be any representation of F by $X \times X$ matrices conjugate to the representation μ' defined for all $x \in X$ by $(\mu' x)_{x', x''} = r(x, x'')$ if $x = x'$, $= 0$ otherwise.

Then, it is easily verified that for all $f \in F^+$, $\operatorname{Tr} \mu f = \rho' f$. In the case treated in [1, p. 226], the relation $x' \lessdot x$ corresponds to the relation "$x \neq x'$ and the loop x' is contained in the loop x." See Fig. 2. For each $x, x' \in X$, $r(x, x') = \pm 1$. This can be arranged as follows: By a homeomorphism of the plane onto itself the loops from the origin as center can all be displaced into the first quadrant. Each $x \in X$ corresponds to a counterclockwise loop and $x_i < x_j$ means that the initial tangent vector to x_i at the origin makes a smaller acute angle with the positive x-axis than the acute angle the initial tangent vector to x_j makes with the positive x-axis. Let $r(x_i, x_j) = s(x_j, x_i)$ for all $i < j$, $r(x_i, x_j) = -1$ for all $i > j$, and $r(x_i, x_i) = -1$ for all i. Thus in Fig. 1, $x \not\lessdot x'$ and $x' \not\lessdot x$ while $x < x'$.

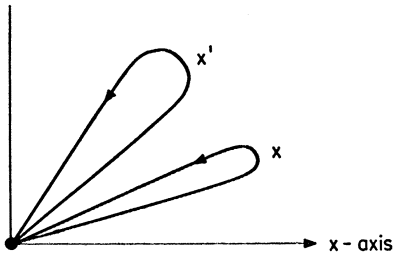

Fig. 1. $x \not\lessdot x'$, $x' \not\lessdot x$, $x < x'$

and $r(x, x')$ is given by Table I. For the case of Fig. 2 we have $x' \circledcirc x$, $x \circledast x'$, and $x < x'$ and r is given by Table II. A geometric interpretation

TABLE I

r	x	αx	x'	$\alpha x'$
x	−1	0	1	1
αx	0	−1	−1	−1
x'	−1	−1	−1	0
$\alpha x'$	1	1	0	−1

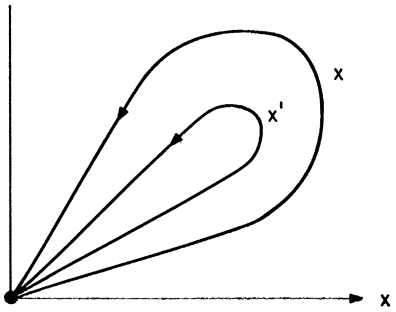

FIG. 2. $x' \circledcirc x$, $x \circledast x'$, $x < x'$

TABLE II

r	x	αx	x'	$\alpha x'$
x	−1	0	−1	−1
αx	0	−1	−1	−1
x'	−1	1	−1	0
$\alpha x'$	1	−1	0	−1

of $r(x, x')$ is that -1 corresponds to an odd number of traversals of the fourth quadrant by the tangent vector as it goes from the initial vector of x to the final vector of x to the initial vector of x' and $+1$ corresponds to an even number of traversals. Thus in the case of Fig. 1, for $r(x, x')$ we have Fig. 3 yielding $r(x, x') = 1$, while in the case of Fig. 1 for $r(x', \alpha x)$ we have Fig. 4 yielding $r(x', \alpha x) = -1$.

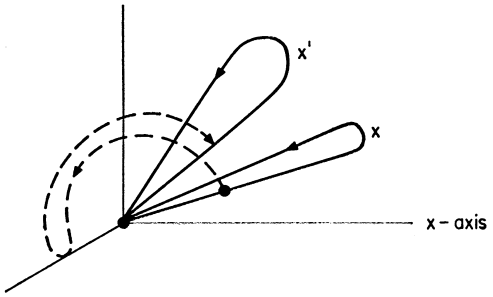

FIG. 3. $r(x, x') = 1$

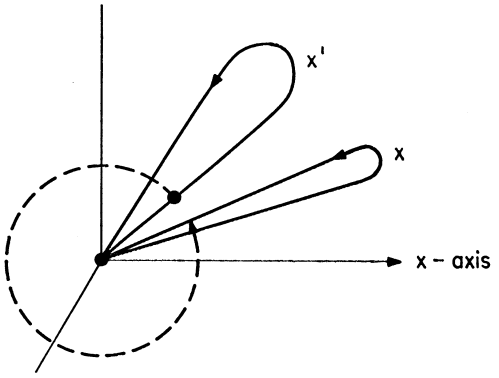

FIG. 4. $r(x', \alpha x) = -1$

III. LEXICOGRAPHIC STANDARD WORDS

Let $<$ be a lexicographic order on the free monoid F and define the subset H of F^+ ($= \{f \in F; f \neq 1\}$) by the condition that $f \in H$ if and only if $f = f'f''$; $f', f'' \in F^+$ implies $f < f''$.

LEMMA 1. [3] *To every $f \in F^+$ there corresponds a unique triple $f' \in F^+$, $f'' \in F$, $m > 0$ such that $f = (f''f')^m$ and $f'f'' \in H$.*

PROOF: Let the subset H' of F^+ be defined by the condition that $f \in H'$ if and only if $f = f'f''$; $f', f'' \in F^+$ implies $f < f''f'$. The verification that H' satisfies the conditions of Lemma 1 and that $H \subset H'$ is immediate. We show $H' \subset H$.

Assume that $f, f_1, f_2, f_3 \in F^+$ are such that $f = f_1f_2 = f_2f_3$ and $f < f_2f_1$. The first condition implies either $f_1 = f_2f_4$ or $f_2 = f_1f_4$ for some $f_4 \in F$. In the first case $f = f_2f_4f_2 < f_2f_1 = f_2f_2f_4$ implies $f_4f_2 < f_2f_4$. Hence $f_4f_2f_2 < f$

and $f \notin H'$. In the second case $f_2 = f_1 f_4 = f_4 f_3$ so that $f = f_1 f_2 < f_2 f_1$, $f_1 f_4 f_3 < f_1 f_4 f_1$ and $f_3 < f_1$. Since the degree of f_3 is equal to the degree of f_1, it follows that $f_3 f_1 f_4 < f$ and $f \notin H'$.

Thus if $f = f'f'' \in H'$; $f', f'' \in F^+$, then f'' is not a left factor of f and $f < f''f'$ implies $f < f''$, that is, $f \in H$ concluding the proof.

LEMMA 2 [4].[1] *Every $f \in F^+$ has one and only one factorization $f = h_{i_1} h_{i_2} \cdots h_{i_m}$ where the elements h_{i_j} belong to H and satisfy $h_{i_m} \leqslant h_{i_{m-1}} \leqslant \cdots \leqslant h_{i_2} \leqslant h_{i_1}$.*

PROOF: Let f and the h_{i_j}'s be as in the Lemma and further $f = f_1 h'$ where $h' \in H$ admits h_{i_m} as a right factor. By definition there exists $m' (1 \leqslant m' \leqslant m)$ and a right factor f' of $h_{i_{m'}}$ such that $h' = f'f''$, and consequently $f' \leqslant h'$. By Lemma 1, $h' \leqslant h_{i_m}$ and $h_{i_{m'}} \leqslant f'$. However, $h_{i_m} \leqslant h_{i_{m'}}$ by hypothesis so that $h_{i_m} = h'$ showing by induction that any f has at most one factorization of the type described.

Reciprocally, let ηf denote for each $f \in F^+$ the right factor $\in F^+$ of f that is minimal with respect to $<$. By Lemma 1, $\eta f \in H$ and, assuming $f \notin H$, $f = f''h'h$ where $h = \eta f$, $h' = \eta(f''h') \in H$, and, by construction, $h < h'h$. Hence the existence of at least one factorization of the prescribed type will follow by induction once it is verified that $h \leqslant h'$. For this, assume $h' \leqslant h$. Cancelling the common left factor of highest degree of h and h' in the two relations $h < h'h$ and $h' \leqslant h$ shows that $h' = h$, and this ends the proof.

IV. MAIN RESULT

Let $a(f)$ denote the coefficient of $f \in F$ in $a \in A$ and $A_u = \{a \in A: a(1) = 1\}$. Let $I = \{i\}$ be totally ordered by $<$ and the mapping $i \to p_i$ of I into A_u be such that for each $f \in F^+$ the subset $P_f = \{i \in I: p_i(f) \neq 0\}$ is finite. For each $f \in F^+$ we define

$$g(f) = \sum p_{i_1}(f_{j_1}) p_{i_2}(f_{j_2}) \cdots p_{i_m}(f_{j_m})$$

where the summation is over all factorizations $f = f_{j_1} f_{j_2} \cdots f_{j_m}$ of f into an arbitrary number of factors $f_{j_k} \in F^+$ and for each such factorization over all $p_{i_1} \in P_{f_{j_1}}$, $p_{i_2} \in P_{f_{j_2}}$, $\cdots$, $p_{i_m} \in P_{f_{j_m}}$ such that $i_1 < i_2 \cdots < i_m$. Thus, $1 + \Sigma\{g(f)f: f \in F^+\}$ is a well defined element of A_u which can be denoted by $\Pi\{p: p \in P; <\}$ where $P = \{p_i: i \in I\}$.

Since A_u is a group (with $a^{-1} = 1 + \Sigma_{n>0}(1 - a)^n$ for each $a \in A_u$) it is easily verified that, setting $p^{-1} > p'^{-1}$ iff $p' < p$, the inverse of

[1] We are indebted to P. M. Cohn for calling our attention to the Širšov paper.

$\Pi\{p: p \in P; <\}$ is precisely $\Pi\{p^{-1}: p \in P; >\}$. In particular (with the notations of Section III) if $(1 - h)^{-1} > (1 - h')^{-1}$ iff $h < h'$, Lemma 2 can be interpreted as the identity

$$\Pi\{(1 - h)^{-1}: h \in H; >\} = \sum\{f: f \in F\}.$$

Since the right member is equal to $(1 - \Sigma\{x: x \in X\})^{-1}$ it follows:

LEMMA 3 [2, Eq. 6].

$$\Pi\{1 - h: h \in H; <\} = 1 - \sum\{x: x \in X\}.$$

Let us assume that the lexicographic order $<$ is now extended from X to $X \cup \alpha X$ such that for all $x, x' \in X$, $x < x'$ implies $x < \alpha x < x' < \alpha x'$ and $x \circledast x'$. On this larger domain the interpretation of $<$ in terms of angular order of initial vectors is no longer valid.

Setting $\bar{H} = \{h \in H: h^2 \in \bar{F}\}$ it is easily verified from Lemma 1 that every $g \in G$, $g \neq e_G$ is conjugate to one and only one element of the form $(\nu h)^m$ with $m > 0$, $h \in \bar{H}$.

THEOREM. [1, Eq. (2).]

$$\Pi\{1 - \rho x)^2: x \in X_1; <\} = \Pi\{1 - \rho h: h \in \bar{H}; <\}.$$

PROOF: Since by definition $1 - \rho x = 1 - \rho\alpha x$ it is sufficient to verify for each $x \in X$

$$1 - \rho x = \Pi\{1 - \rho h: h \in \bar{H} \cap xF; <\}.$$

For this, let K_x be the set of all words of the form $xf \in \bar{F}$ where f has no factor $x' \leqslant x$ and does not belong to $F\alpha x$. By construction $K_x \subset \bar{H}$ and each $h \in \bar{H} \cap xF$ (more generally, each $f \in \bar{F} \cap xF \setminus F\alpha x$) has one and only one factorization as a product of elements of K_x. Also if $h = kf$, $h' = k'f'$, $k, k' \in K_x$, and both f and f' having x as a left factor, then the relation $h < h'$ implies $k \leqslant k'$. Thus one can find a lexicographically ordered free monoid F' and a monomorphism $\zeta: F' \to F$ such that F' is generated by $\zeta^{-1}K_x$ and that $\bar{H} \cap xF = \zeta H'$ where H' is defined for F' as H was defined for F in Section 3.

Using Lemma 3 and the remark that for any $h, h' \in \bar{H} \cap xF$, $\rho hh' = \rho h \rho h'$, it follows:

$\Pi\{1 - \rho h: h \in \bar{H} \cap xF; <\} = 1 - \Sigma\{\rho k: k \in K_x\}$. We verify that the right member reduces to $1 - \rho x$ by constructing an involutory mapping τ of $K_x \setminus \{x\}$ such that, identically, $\rho\tau k + \rho k = 0$.

For this, consider any element $k \neq x$ of K_x. It admits a factorization $k = x\, x_{i_1}^{m_1} x_{i_2}^{m_2} \cdots x_{i_p}^{m_p}$ where $p \geqslant 1$; $m_1, m_2, \cdots, m_p > 0$; $x_{i_1}, x_{i_2}, \cdots, x_{i_p} \in X$; $\beta x \neq \beta x_{i_1}$, $\beta x_{i_1} \neq \beta x_{i_2}$, $\cdots$, $\beta x_{i_{p-1}} \neq \beta x_{i_p}$, $\beta x_{i_p} \neq \beta x$.

Let $j^* = 1$ if $p = 1$ or if $p > 2$ and $\beta x_{i_2} \circledast \beta x_{i_1}$ and $j^* =$ the largest index such that $\beta x_{i_{j^*}} \circledcirc \beta x_{i_{j^*-1}} \cdots \circledcirc \beta x_{i_2} \circledcirc \beta x_{i_1}$ otherwise. Then we define τk as the element obtained when replacing in k, $x_{i_{j^*}}^{m_{j^*}}$ by $(\alpha x_{i_{j^*}})^{m_{j^*}}$.

Since $k \in H$, $\beta x < \beta x_{i_1}$ and because of our choice of $<$ this implies $\beta x \circledast \beta x_{i_1}$. Thus $\beta x_{i_{j^*}} \neq \beta x$ and consequently, $\tau k \in K_x$, $\tau\tau k = k$. For the same reason, $\beta x \circledast \beta x_{i_{j^*}}$ when $j^* = p$. Hence setting $x' = x_{i_{j^*-1}}$ ($= x$ if $j^* = 1$), $\bar{x} = x_{i_{j^*}}$, $x'' = x_{i_{j^*+1}}$ ($= x$ if $j^* = p$) one has always $\beta x' \circledast \beta\bar{x}$ and $\beta x'' \circledast \beta\bar{x}$. From the definition of r it follows that

$$r(x', \bar{x})\,(r(\bar{x}, \bar{x}))^{m_{j^*}}\, r(\bar{x}, x'') \;=\; -r(x', \alpha\bar{x})\;\; (r(\alpha\bar{x}, \alpha\bar{x}))^{m_{j^*}}\, r(\alpha\bar{x}, x'').$$

This shows that $\rho\tau k + \rho k = 0$ and concludes the proof.

References

1. Sherman, S., Combinatorial aspects of the Ising model for ferromagnetism, II. *Bull. Am. Math. Soc.* **68**, 225-229 (1962).
2. Sherman, S., Combinatorial aspects of the Ising model for ferromagnetism, I. *J. Math. Phys.* **1**, 202-207 (1960).
3. Chen, K. T., Fox, R. H., and Lyndon, R. H., Free differential calculus IV. *Ann. Math.* **68**, 81-95 (1958).
4. Širšov, A. I. On free Lie rings. *Mat. Sbornik* **45**, 113-122 (1958)