On the Isomorphism Problem for Group Presentations

A Dissertation presented

by

Gary Aviv

to

The Graduate School

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Mathematics

State University of New York

at

Stony Brook

April, 1977

STATE UNIVERSITY OF NEW YORK

AT STONY BROOK

THE GRADUATE SCHOOL

GARY AVIV

We, the dissertation committee for the above candidate for the Ph.D. degree, hereby recommend acceptance of the dissertation.

Bernard Maskit, Professor
Committee Chairman

Elvira R. Strasser, Professor
Thesis Advisor

William Lister, Professor

Irving Gerst, Professor

The dissertation is accepted by the Graduate School.

Herbert Weisinger, Dean
Graduate School

April, 1977

Abstract of the Dissertation

On the Isomorphism Problem for Group Presentations

by

Gary Aviv

Doctor of Philosophy

in

Mathematics

State University of New York at Stony Brook

1977

If F is the free group generated by the n-tuple of symbols $X=(X_1,\ldots,X_n)$, and $W=(W_1,\ldots,W_t)$, $V=(V_1,\ldots,V_t)$ are two t-tuples of elements of F, then $P_1=\langle X;W\rangle$ and $P_2=\langle X;V\rangle$ "present" the groups $F/\{W\}$ respectively $F/\{V\}$ where $\{W\}$ is the normal closure of W in F and similarly for $\{V\}$. If $\{W\}=\{V\}$ then P_1 and P_2 present the same group and we have an instance of a pair of isomorphic presentations. But W need not equal V for this. If $W\neq V$, then one would need an algorithm to prove (or disprove) that P_1 and P_2 are isomorphic.

For technical reasons the first place to look for such an algorithm is among the mappings $Q:\{W\}\longrightarrow\{V\}$ which are reasonable (have an inverse). These are the

"Q-transformations"; they consist of "free isomorphisms" and "conjugations" [1]. In the present work we prove algebraically and give some extensions of a topological result of [7]: Namely, there exist t-tuples W and V with $\{W\}=\{V\}$ such that no Q-transformation can take W into V. An important special case is obtained when $\{W\}=F$ and $V=X$. The question whether in this case W is a Q-transform of V has bearing on the Poincaré Conjecture that the 3-sphere is characterized by its fundamental group [2]. To contribute to the solution of this problem we looked at Q-transforms of W. Since the essence of an algorithm is finiteness, we set out to find and found conditions under which the conjugations in Q-transformations can be restricted to a finite set (to certain permutations). It is possible - some think probable [2]- that the restricted set is all that is ever needed here. However, a decision in this generality is out of reach at present: it could be made only in special situations. While proceeding towards these we extend a theorem of Nielsen and give a new proof of it.

To My Loving Parents

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I wish to express my heartfelt gratitude and sincere appreciation to Professor Elvira Rapaport Strasser for her inspirational guidance and unceasing patience throughout this endeavor.

I would also like to thank my friend through it all Stephen Kronwith, my freshman calculus teacher Jose Andrade, and my dearest Cherie.

CHAPTER 1

INTRODUCTION

BACKGROUND

Many problems of topology manifest themselves as problems in the theory of groups defined in terms of generators and relators. Indeed, the fundamental group of a CW-complex may be computed in terms of its generators and relators. A group that is defined in this way is said to be presented.

Let F_n stand for a free group on n generators. We write $F(a_1,\ldots,a_n)$ when the free generators are to be specified. Let $R=(R_1,\ldots,R_t)$ be a t-tuple of words in F_n. The intersection of all normal subgroups in F_n that contain R (the normal closure of R) will be denoted by $\{R\}$. We say that R normally generates $\{R\}$. A presentation $P=\langle a_1,\ldots,a_n;R_1,\ldots,R_t\rangle$ with a_i generators and R_j relators defines the group $F(a_1,\ldots,a_n)/\{(R_1,\ldots,R_t)\}$. If we allow n and t to be possibly infinite then any group admits a presentation. We will restrict our attention to finite presentations, i.e. $n,t<\infty$.

The presentation of a group is far from unique. In fact, infinitely many presentations define every group. Then when two arbitrary presentations are given how do we decide whether they define isomorphic groups? Indeed, for example, the usefulness of the Fundamental Group as a topological invariant often reduces to this issue. This is Dehn's isomorphism problem which he formulated in 1911.

This problem has proven to be quite difficult and in general unsolvable. Even the more restricted problem of deciding when a presentation defines the trivial group (the group with one element) has been shown to be unsolvable by Rabin [8].

H. Tietze in 1908 defined four basic transformations that could be applied to a presentation to obtain another isomorphic presentation. He showed that given any presentation P of a group G, any other presentation for G can be obtained by repeated applications of these transformations on P. Then the isomorphism problem is reduced to determining whether two presentations are linked by these transformations. This turns out to be of little practical value.

Since the isomorphism problem is so formidable it is necessary to examine well chosen restrictions. Let G and H be defined by $\langle a_1,\ldots,a_n; R_1,\ldots,R_t\rangle$ and $\langle b_1,\ldots,b_n; S_1,\ldots,S_t\rangle$ respectively. The following problem represents one such restriction: If $G \cong H$ then does the map $a_i \rightarrow b_i$ define an isomorphism? This problem is equivalent to the following: Let R, S be t-tuples in F_n. When is $\{R\} = \{S\}$?

In 1921 Nielsen defined transformations on t-tuples of words in a free group and showed that when R, S are two t-tuples that generate the same subgroup of F_n then a repeated application of these transformations on R will yield S. Furthermore he found an "effective" procedure for doing this and therefore solved the problem of deciding when two t-tuples generate the same subgroup of F_n.

With this motivation, Andrews and Curtis in [1] and Rapaport in [9] extended the definition of Nielsen transformation by allowing in addition conjugation. These transformations, which we call Q-transformations adopting the convention of [9], when applied to a t-tuple R in F_n do not change the normal closure of R. Furthermore it is proved in [9] that the set of all invertible transformations of R having this property is precisely the set of Q-transformations.

The following question then remained open: If $\{R\} = \{S\}$ in F_n, does there always exist a Q-transformation taking R to S? Metzler in [7] answered this question in the negative using the topology of the underlying 2-dimensional CW-complexes. We will prove this result algebraically and give some extensions in Chapter 2.

When S is the set of generators of F_n, the above question remains open. Andrews and Curtis in [1] conjectured that in this case a Q would always exist taking R into the generators S. Furthermore they proved that if their conjecture is true and if a counterexample of the 3-dimensional Poincaré conjecture exists then it must exist in 4-space.

Related questions are asked in [2] and [9]. In Chapter 3 we will investigate one of these. In particular we will show that it is possible in some situations to work with a subset of Q-transformations and yet not lose generality.

DEFINITIONS AND NOTATION

We fix the following notation once for all.

$F_n=F(a_1,\ldots,a_n)$ is a free group on the generators $a_1,\ldots,a_n$.

$\bar{X}=X^{-1}$ is the inverse of an element X.

$|X|$ is the length of the element $X\in F(a_1,\ldots,a_n)$ defined to be the sum of the absolute values of all the exponents of the generators a_i appearing in X when X is freely reduced. (i.e. no segment of the form $a_i\bar{a}_i$ or

$\bar{a}_i a_i$ appears in X).

$|(W_1,\dots,W_t)|$ is the length of the t-tuple of elements in F_n defined to be the sum of $|W_i|$, $i=1,\dots,t$.

$\{(W_1,\dots,W_t)\}$ is the normal closure of the t-tuple $(W_1,\dots,W_t)$ in F_n.

$W^X=\bar{X}WX$ is the conjugate of the element W by the element X in F_n.

We make the following common definitions:

A word $X\in F(a_1,\dots,a_n)$ is said to be cyclically reduced if it is freely reduced and it does not begin with a_i^{ε} and end with $a_i^{-\varepsilon}$, $\varepsilon=\pm1$.

W^X is said to be a short conjugate of W when W^X is a cyclic permutation of W.

The exponent sum of X on a_i is the sum of the exponents of a_i appearing in X when X is freely reduced.

Let $W=IT$, $I,T\in F_n$. The product IT is reduced as written when no cancellation occurs between I and T. (i.e. $|W|=|I|+|T|$). I is called an initial segment and T a terminal segment of W.

Finally we define Nielsen and Q-transformations:

Definition Let $\tilde{W}=(W_1,\dots,W_t)$ be a t-tuple of words in F_n. A transformation of W is called an elementary Nielsen transformation if it operates on W in one of the following ways:

1. W is left fixed or any two of the W_i are permuted.

2. W_j is left fixed $\forall j \neq r$, $1 \leq j \leq t$ and W_r is sent to $\overline{W}_r$.

3. W_j is left fixed $\forall j \neq r$, $1 \leq j \leq t$ and for r,s fixed $r \neq s$, $1 \leq r,s \leq t$ either

   a) W_r is sent to $W_r W_s$ or

   b) Wr is sent to $W_s W_r$.

Definition With W as above, a transformation W is called an elementary Q-transformation if it is an elementary Nielsen transformation on W or

2'. W_j is left fixed $\forall j \neq r$, $1 \leq j \leq t$ and W_r is sent to $W_r^{\pm X} = \overline{X} W_r^{\pm 1} X$ for any $X \in F_n$.

The elementary Nielsen and Q-transformations generate the group of Nielsen and Q-transformations respectively. Multiplication of two Nielsen N_1, N_2 is defined so: $(N_1 N_2)(W) = N_1(N_2(W))$, and similarly for two Q-transformations. Then a Nielsen or a Q-tranformation is a finite product of elementary Nielsen or Q-transformations repectively.

A short Q-transformation will be defined exactly as a Q-transformation only in 2', conjugations are limited to short conjugations. Then there are only finitely many elementary short Q-transformations on a fixed t-tuple in F_n since there are at most $|A|$ short conjugates of a word $A \in F_n$. This achieves a substantial simplification.

We say that two t-tuples in F_n are Q-equivalent or belong to the same Q-class if there is a Q-transformation from one to the other. Of course, all t-tuples in a fixed Q-class have the same normal closure in F_n.

SUMMARY OF RESULTS

We prove the following results in the present work:

1. If $\gcd(r,s)=\gcd(t,r)=1$, $0<s<t<r$, and $s+t\neq r$ then $\{(b^r, ab^s\bar{a}\bar{b}^s)\} = \{(b^r, ab^t\bar{a}\bar{b}^t)\}$ in $F(a,b)$ but there is no Q-transformation taking the first pair to the second pair. (Theorems 4 and 5 of Chapter 2) However,
2. If $s=t \mod r$ then in $F(a,b)$ the pair $(b^r, ab^s\bar{a}\bar{b}^s)$ belongs to the Q-class of $(b^r, ab^t\bar{a}\bar{b}^t)$. (Theorem 6 of Chapter 2)
3. Within $F(a,b)$ there exist normal subgroups possessing an arbitrarily large number of Q-classes. (Theorem 7 of Chapter 2)
4. Let W, U be t-tuples in F_n, $f: F_n \longrightarrow F_n$ a homomorphism. If W and U belong to the same Q-class then $f(W)$ and $f(U)$ also belong to the same Q-class. (Theorem 8 of Chapter 2)
5. Let $W=(W_1,\dots,W_t)$, $W'=(\bar{X}_1W_1X_1,\dots,\bar{X}_tW_tX_t)$ with $W_i, X_i \in F_n$, N any Nielsen transformation. Then there

exists a short Q-transformation, Q^s, such that $|Q^s(W)| \leq |N(W')|$. (Theorem 6 of Chapter 3)

We will give several definitions and prove the following technical improvement of a theorem of Nielsen.

6. For every t-tuple W in F_n, there exists a Nielsen transformation $N=N_s \ldots N_1$, with N_i elementary Nielsen such that N(W) is Nielsen reduced and N is semidirect. Moreover, if N_i multiplies one element of W by another then the pair is not isolated. (Theorem 3 of Chapter 3)

We will define "complete" Nielsen transformations and prove:

7. For every t-tuple W in F_n, there exists a complete Nielsen transformation, N^c, such that $N^c(W)$ is Nielsen reduced. (Theorem 4 of Chapter 3)

8. Let N_i be complete Nielsen transformations, C_i conjugating transformations and $Q=C_tN_t \ldots C_1N_1$ a Q-transformation on a t-tuple W in F_n. Then there exists a short Q-transformation, Q^s, such that $|Q^s(W)| \leq |Q(W)|$. (Theorem 7 of Chapter 3)

CHAPTER 2

DISTINCT Q-CLASSES

INTRODUCTION

In this chapter we will show that it is possible for two t-tuples of words in a free group to have the same normal closure and yet not be Q-equivalent. This result has also been obtained by Metzler in [7] by appealing to the underlying 2-dimensional CW-complexes associated with the group presentations with the t-tuples as relators. We give a combinatorial proof. Also we show that there are normal subgroups of a free group possessing arbitrarily (finitely) many pairwise Q-inequivalent normal generating t-tuples. We finally discuss some extensions and conjectures.

FREE DIFFERENTIAL CALCULUS

The following section is due to Fox [5] and will provide the tools by which we will approach the problem of distinguishing Q-inequivalent t-tuples. A good treatment may also be found in Crowell and Fox [4].

Associated with any multiplicative group G generated by the symbols a_i there is a ring $\mathbb{Z}(G)$ called the integral group ring over G. Its elements consist of all formal finite sums of elements in G expressed on the generators a_i with coefficients in $\mathbb{Z}$. The sum of two elements in $\mathbb{Z}(G)$ is defined component-wise. Multiplication is defined to force the distributive law to hold. If $G=\langle a\rangle=\mathbb{Z}$ then $\mathbb{Z}(G)$ consists of polynomials on indeterminate a with integral exponents and coefficients. A typical element would be $n_1 a^{m_1}+\ldots+n_s a^{m_s}$, with $n_i, m_i \in \mathbb{Z}$. Multiplication and addition would be performed exactly as over polynomials.

The ring $\mathbb{Z}(G)$ is generated by the generators of G. The elements of G are also elements of $\mathbb{Z}(G)$ and are among the units. Also $\mathbb{Z}(G)$ is commutative if and only if G is.

If $f: G \longrightarrow H$ is a group homomorphism then f induces a ring homomorphism of $\mathbb{Z}(G)$ to $\mathbb{Z}(H)$. The element $\sum n_i g_i$ ($n_i \in \mathbb{Z}$, $g_i \in G$) of $\mathbb{Z}(G)$ is sent to $\sum n_i f(g_i)$ in $\mathbb{Z}(H)$. In particular for $\Theta: G \longrightarrow 1$, $\Theta(\sum n_i g_i)=\sum n_i$.

A derivation on a group ring is a map D of $\mathbb{Z}(G)$ into itself satisfying for all $u,v \in \mathbb{Z}(G)$:

1) $D(u+v)=Du+Dv$

2) $D(uv)=Du \cdot \Theta(v)+uDv$.

When v is an element of the group, $\Theta(v)=1$ so that for $g,h \in G$ we have

2') $D(gh)=Dg+gDh$.

We derive the following simple consequences of

1) and 2).

3) $Dn=0$ for $n \in \mathbb{Z}$

First we see that $D1=0$ since $D1=D(1\cdot 1)=D1+D1$. Also $D0=0$ from the fact that $D0=D(0+0)=D0+D0$. Then for $n\neq 0$, $n=\underline{+}1\ldots\underline{+}1$ so by 1) the result follows.

4) $D(ng)=nDg$, $g\in G$

By 2) $D(ng)=Dn\cdot\Theta(g)+nDg$, but $Dn=0$ from 3).

5) $D(\bar{g})=-\bar{g}Dg$

By 3) and 2') we have $0=D1=D(\bar{g}g)=D\bar{g}+\bar{g}Dg$.

We will be particularly interested in group rings over free groups. Let $F=F(a_1,\ldots,a_n)$. An element of $\mathbb{Z}(F)$ is sometimes called a free polynomial. To each generator a_i we may define a map on the generators, $\frac{\partial}{\partial a_i}$, having the property that $\frac{\partial a_j}{\partial a_i}=1$ when $j=i$ and 0 otherwise. This map can be extended to a derivation on $\mathbb{Z}(F)$ by using 1) and 2). We need only verify that the map that results is well defined on F. For this it suffices to prove that $\frac{\partial(gh)}{\partial a_i}=\frac{\partial(ga_j\bar{a}_jh)}{\partial a_i}$, for $g,h\in F$. Using 2) repeatedly $\frac{\partial(ga_j\bar{a}_jh)}{\partial a_i}=\frac{\partial g}{\partial a_i}+g\frac{\partial a_j}{\partial a_i}+ga_j\frac{\partial \bar{a}_j}{\partial a_i}+g\frac{\partial h}{\partial a_i}$. By 5) the third term is $-g\frac{\partial a_j}{\partial a_i}$ so the result follows. Similarly it follows for $g\bar{a}_ja_jh$.

Let $g=x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$ where each x_i is a_j for some j, $\varepsilon_i=\underline{+}1$. Define the k'th initial section, $S(k)$, of g to be $x_1^{\varepsilon_1}\ldots x_{k-1}^{\varepsilon_{k-1}}$ if $\varepsilon_k=1$ and $-x_1^{\varepsilon_1}\ldots x_k^{\varepsilon_k}$ if $\varepsilon_k=-1$. Also S(1) is either 1 or $-x_1$ depending on whether ε_1 is 1 or -1 respectively. In all cases $S(k)\in \mathbb{Z}(F)$. Then

$$\frac{\partial g}{\partial a_i}=\sum_{j=1}^{n} S(j)\frac{\partial x_j}{\partial a_i}.$$

This gives a simple method for computing derivatives in $\mathbb{Z}(F)$. Note that only those x's which are a_i contribute terms in the expression of $\frac{\partial g}{\partial a_i}$ and that $\theta(\frac{\partial g}{\partial a_i})$ gives the exponent sum of g on a_i.

For example, consider the free group F(a,b). We have the derivations $\frac{\partial}{\partial a}$ and $\frac{\partial}{\partial b}$.

$\frac{\partial}{\partial a}(a^5)=1+a+a^2+a^3+a^4$, $\frac{\partial}{\partial a}(\bar{a}^5)=-\bar{a}^1-\bar{a}^2-\bar{a}^3-\bar{a}^4-\bar{a}^5$,
$\frac{\partial}{\partial b}(a^5)=0$, $\frac{\partial}{\partial a}(ab\bar{a}\bar{b})=1-ab\bar{a}$, $\frac{\partial}{\partial b}(ab\bar{a}\bar{b})=a-ab\bar{a}\bar{b}$.

Now let $R_1,\ldots,R_m$ be words in F. We have the natural epimorphism $f:F\longrightarrow G=\langle a_1,\ldots,a_n;R_1,\ldots,R_m\rangle$, and the induced ring map $f':\mathbb{Z}(F)\longrightarrow \mathbb{Z}(G)$. The matrix $[f'(\frac{\partial R_i}{\partial a_j})]$ is called the Jacobian matrix for the m-tuple $R=(R_1,\ldots,R_m)$ and is denoted by J[R]. It is a matrix over the group ring $\mathbb{Z}(G)$. For example, for the pair $(a^5,ab\bar{a}\bar{b})$ we get the Jacobian matrix

$$\begin{bmatrix} 1+a+a^2+a^3+a^4 & 0 \\ 1-b & a-1 \end{bmatrix}.$$

<u>ROW EQUIVALENT MATRICES</u>

We now define a notion of equivalence for the set of n x m matrices over $\mathbb{Z}(G)$.

Definition Let M_1 and M_2 be n x m matrices over $\mathbb{Z}(G)$. M_1 is said to be row equivalent to M_2, denoted by $M_1 \sim M_2$, when a finite number of applications of the following operations on M_1 yields M_2:

1) Permute any two rows,
2) Add one row to another,
3) Multiply any row on the left by $\pm g$, $g \in G$.

Note that row equivalence is an equivalence relation on the n x m matrices over $\mathbb{Z}(G)$. The transitive and reflexive properties follow immediately. The property of symmetry holds because each operation can be reversed. Note that the combination of 2) and 3) allows the subtraction of one row from another. Also, 3) may be nullified by multiplying the row by the inverse of the group element.

If $R=(R_1,\ldots,R_m)$ is a Q-transform of $S=(S_1,\ldots,S_m)$ then since $\langle a_1,\ldots,a_n;R\rangle \cong \langle a_1,\ldots,a_n;S\rangle = G$, both $J[R]$ and $J[S]$ are n x m matrices over $\mathbb{Z}(G)$. The relation between them is given in

Theorem 1 Let R and S be m-tuples in F_n with $Q(R)=S$, Q a Q-transformation. Then $J[R] \sim J[S]$.

Proof It suffices to consider the case when Q is simply an elementary Q-transformation for then the theorem follows by induction on the number of elementary components of Q.

If Q permutes R_i with R_j then J[S] is J[R] with row i and j permuted and so J[R]~J[S].

Say Q sends R_i to $\bar{R}_i$. $f'(\frac{\partial}{\partial a_j} \bar{R}_i)=f'(-R_i\frac{\partial}{\partial a_j} R_i)$ by property 5) of derivations. But f' is the ring homomorphism $\mathbb{Z}(F)\longrightarrow\mathbb{Z}(G)$ induced by $f:F\longrightarrow G$, the natural homomorphism under which R_i is sent to 1. So the right side is $-f'(\frac{\partial}{\partial a_j} R_i)$. Then the effect on J[R] is to multiply the i'th row by -1 which preserves its row equivalence class.

Now say Q sends R_i to R_iR_l, $l\neq i$. By property 2') of derivations,

$f'(\frac{\partial}{\partial a_j}(R_iR_l))=f'(\frac{\partial}{\partial a_j}R_i+R_i\cdot\frac{\partial}{\partial a_j}R_l)=f'(\frac{\partial}{\partial a_j}R_i)+f'(\frac{\partial}{\partial a_j}R_l)$. So the effect on J[R] is to add row l to row i. The case where Q sends $R_i\longrightarrow R_lR_i$ is similar.

Finally say Q sends R_i to $\bar{W}R_iW$ for any $W\epsilon F$. $f'(\frac{\partial}{\partial a_j}(\bar{W}R_iW))=f'(-\bar{W}\frac{\partial W}{\partial a_j} + \bar{W}\frac{\partial}{\partial a_j}R_i + \bar{W}R_i\cdot\frac{\partial W}{\partial a_j})$. Applying f' additively we find that the first and third terms cancel leaving $f'(\bar{W})\cdot f'(\frac{\partial}{\partial a_j}R_i)$. Also $f'(\bar{W})$ is an element of G in $\mathbb{Z}(G)$. Therefore, conjugation by W has the effect of multiplying the i'th row of J[R] on the left by an element of G, which again preserves the row equivalence class of J[R]. The proof is now complete.

In order to show that for no Q-transformation is Q(R)=S we may pass to the matrices J[R] and J[S] and prove that $J[R] \not\sim J[S]$. The following two theorems provide tools for distinguishing inequivalent matrices over $\mathbb{Z}(G)$.

Theorem 2 Let M_1 and M_2 be n x m matrices over $\mathbb{Z}(G)$ with G abelian. If $M_1 \sim M_2$ then there exists a n x n matrix L in $\mathbb{Z}(G)$ such that $LM_1 = M_2$ and $\det(L) = \pm g$, $g \in G$.

Proof First we show that it suffices to consider the case when the matrices are linked by a single row operation. Assume this much has been established. Now we have that a finite number of row operations on M_1 yields M_2. Then we may proceed by induction on the number, p, of these steps that are required. If $p>1$, then there exists a matrix M_3 such that $M_1 \sim M_3 \sim M_2$ and the sum of the number of row operations required to go from M_1 to M_3 and from M_3 to M_2 is p. Then by the induction hypothesis, there exist matrices L and L' with $\det(L) = \pm g$, $\det(L') = \pm g'$ and $LM_1 = M_3$, $L'M_3 = M_2$. But then $L'LM_1 = M_2$ and $\det(L'L) = \det(L') \cdot \det(L') = \pm g'g$, so the proof is complete.

Then we are left with proving the theorem when one row operation on M_1 yields M_2. Say this operation is a permutation of rows i and j of M_1. Let I be the n x n identity matrix. If L is I with columns i and j permuted, then $LM_1 = M_2$ and $\det(L) = -1$, $1 \in G$.

Next let the operation on M_1 be adding row j to row i and let L be I but with 1 in position (i,j). Again we have $LM_1=M_2$. Furthermore, L may be obtained from I by adding its j'th row to its i'th row so det(L)=det(I)=1.

Finally, let the operation on M_1 be multiplication of its i'th row by $\pm g$, $g\in G$, and let L be I with $\pm g$ replacing the 1 in its (i,i) position. Then $LM_1=M_2$ and $\det(L)=\pm g$. The proof is now complete.

If $h:G\longrightarrow H$ is a group homomorphism, then h induces a ring homomorphism $\mathbb{Z}(G)\longrightarrow\mathbb{Z}(H)$ and so it also induces a map on the n x m matrices over $\mathbb{Z}(G)$ to the n x m matrices over $\mathbb{Z}(H)$. We show that the induced map preserves row equivalence.

<u>Theorem 3</u> Let $h:G\longrightarrow H$ be a group homomorphism and let M_1 and M_2 be n x m matrices over $\mathbb{Z}(G)$. If $M_1\sim M_2$, then $h(M_1)\sim h(M_2)$ in $\mathbb{Z}(H)$.

<u>Proof</u> Again it will suffice to prove the case where $M_1\sim M_2$ by virtue of a single row operation.

Let $h':\mathbb{Z}(G)\longrightarrow\mathbb{Z}(H)$ be the induced map. Then by $h(M_1)$ we mean h' applied to every entry of M_1. Since h' is additive, if adding one row to another will take M_1 to M_2, the exact same operation will take $h(M_1)$ to $h(M_2)$. Similarly, if M_2 is obtained from M_1 by multiplying one row on the left by $\pm g$, then since h' is multiplicative we need only multiply the same row of $h(M_1)$ by $h'(\pm g)=\pm h'(g)$ with $h'(g)\in H$ to obtain $h(M_2)$. Finally, if the row operation is permutation, the same permutation on $h(M_1)$ yields $h(M_2)$. This completes the proof.

DISTINCT Q-CLASSES

In this section we consider the normal subgroup generated by $(b^r, ab\bar{a}\bar{b})$ in $F(a,b)$ which we denote by N_r. We have $F(a,b)/N_r \cong \mathbb{Z}\oplus\mathbb{Z}_r$. The next theorem gives other normal generators of N_r.

Theorem 4 If $\gcd(r,s)=1$, $r,s>0$ then $(b^r, ab\bar{a}\bar{b})$ and $(b^r, ab^s\bar{a}\bar{b}^s)$ generate the same normal subgroup in $F=F(a,b)$.

Proof Let N_r and N_r^s be the normal subgroups generated by the pairs respectively. To show that $N_r\supset N_r^s$ we need only prove that $ab^s\bar{a}\bar{b}^s=1$ in F/N_r. But in F/N_r $b=ab\bar{a}$, which means $b^s=(ab\bar{a})^s=ab^s\bar{a}$ or $ab^s\bar{a}\bar{b}^s=1$.

Next we show that $N_r^s\supset N_r$. Consider $ab\bar{a}\bar{b}$ in F/N_r^s. Now there are integers p and q with $pr+qs=1$.

$ab^s\bar{a}\bar{b}^s=1 \Rightarrow ab^s\bar{a}=b^s \Rightarrow ab^{qs}\bar{a}=b^{qs}$. Also $b^{pr}=1$ so we have,

$ab^{qs}\bar{a}=b^{qs+pr}=b \Rightarrow b^{qs}=\bar{a}ba \Rightarrow b=\bar{a}ba \Rightarrow ab\bar{a}\bar{b}=1$.

So we have $N_r^s=N_r$ which completes the proof.

The remainder of the section will be devoted to proving that within N_r there are distinct Q-classes. The main result is contained in

Theorem 5 Let $0<s<t<r$ with $\gcd(s,r)=\gcd(t,r)=1$ and

$s+t\neq r$. Then there is no Q-transformation taking $(b^r, ab^s\bar{a}\bar{b}^s)$ to $(b^r, ab^t\bar{a}\bar{b}^t)$ in $F(a,b)$.

Let W_r^s and W_r^t be the respective pairs. The proof will proceed by showing that $J[W_r^s]\not\sim J[W_r^t]$ which yields the result by Theorem 1.

<u>Lemma 1</u>

$$J[W_r^s] = \begin{bmatrix} 0 & 1+b^2+\ldots+b^{r-1} \\ 1-b^s & a+ab+ab^2+\ldots+ab^{s-1}-b^{s-1}-b^{s-2}-\ldots-1 \end{bmatrix}$$

<u>Proof</u> follows by computing the derivatives $\frac{\partial b^r}{\partial a}$, $\frac{\partial b^r}{\partial b}$, $\frac{\partial ab^s\bar{a}\bar{b}^s}{\partial a}$, $\frac{\partial ab^s\bar{a}\bar{b}^s}{\partial b}$ in $\mathbb{Z}(F)$ and then mapping to $\mathbb{Z}(F/\{W_r^s\})$ by the natural map. This amounts to allowing a and b to commute. For example $\frac{\partial}{\partial a}(ab^s\bar{a}\bar{b}^s)=1-ab^s\bar{a}$, but under the ring map $1-ab^s\bar{a}$ is sent to $1-b^s$. Note that for $s=1$, $\frac{\partial}{\partial b}(ab^s\bar{a}\bar{b}^s)=a-ab\bar{a}\bar{b}$ which is sent to $a-1$ under the induced ring map.

Since $F/\{W_s^r\} = \mathbb{Z} \oplus \mathbb{Z}_r$, by factoring out the generator a we get a homomorphism $h: F/\{W_r^s\} \longrightarrow \mathbb{Z}_r$. Using Theorem 3 and the induced map of the rings $\mathbb{Z}(\mathbb{Z}\oplus\mathbb{Z}_r) \longrightarrow \mathbb{Z}(\mathbb{Z}_r)$ it will now suffice to show that $h(J[W_r^s])\not\sim h(J[W_r^t])$. Let $M_s=h(J[W_r^s])$. This yields a substantial simplification:

$$M_s = \begin{bmatrix} 0 & 1+b+b^2+\ldots+b^{r-1} \\ 1-b^s & 0 \end{bmatrix}$$

Furthermore, since $\mathbb{Z}_r$ is abelian, we may apply

Theorem 2. So the problem is reduced to showing that there exists no 2x2 matrix L with $LM_s=M_t$ and $\det(L)=\pm b^i$, for any i; L, M_s, M_t all matrices over $\mathbb{Z}(\mathbb{Z}_r)$.

Let $L=\begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Then the above is shown by proving the following lemmata.

<u>Lemma 2</u> Let $\mathbb{Z}_r$ be generated by b. If $0<s<t<r$, $\gcd(r,s)=\gcd(r,t)=1$ and $s+t\neq r$ then the following system of equations has no solution for $A,B,C,D\in\mathbb{Z}(\mathbb{Z}_r)$ and $0\leq i<r$: $B(1-b^s)=0$, $A(1+b+\ldots+b^{r-1})=1+b+\ldots+b^{r-1}$, $D(1-b^s)=1-b^t$, $C(1+b+\ldots+b^{r-1})=0$, $AD-BC=\pm b^i$.

We first prove Lemma 3 below which will gain us a simplification of Lemma 2.

Note that in $\mathbb{Z}(\mathbb{Z}_r)$ a typical element has the form $q_0+q_1b+\ldots+q_{r-1}b^{r-1}$, with $q_i\in\mathbb{Z}$.

<u>Lemma 3</u> Let $\gcd(r,s)=1$ and $0<s<r$. In $\mathbb{Z}(\mathbb{Z}_r)$, if $B(1-b^s)=C(1+b+\ldots+b^{r-1})=0$ then $BC=0$.

<u>Proof</u> Let $B=q_0+q_1b+\ldots+q_{r-1}b^{r-1}$, $q_i\in\mathbb{Z}$. Then $B(1-b^s)=q_0+q_1b+\ldots+q_{r-1}b^{r-1}-(q_0b^s+q_1b^{s+1}+\ldots+q_{r-1}b^{s+r-1})=0$, where the arithmetic in the superscripts and subscripts is modulo r here and for the rest of the proof.

Collecting like terms we get $q_s-q_0=0$, $q_{s+1}-q_1=0$, $\ldots$, $q_{s+r-1}-q_{r-1}=0$, or $q_{s+j}=q_j$ for all $j\in\mathbb{Z}$. In particular, $q_0=q_s=q_{2s}=\ldots=q_{(r-1)s}$. Now since $\gcd(r,s)=1$, these subscripts modulo r include all integers from 0 to r-1.

So $q_0=q_1=\ldots=q_{r-1}$. Then $B=q(1+b+\ldots+b^{r-1})$ and $BC=CB=Cq(1+b+\ldots+b^{r-1})=qC(1+b+\ldots+b^{r-1})=0$, which completes the proof.

With Lemma 3 the conditions on Lemma 2 can be reduced to equations in only A and D. We state this in

Lemma 4 Let $0<s<t<r$, $\gcd(r,s)=1$ and $s+t\neq r$. The following system of equations has no solutions for $A,D\in\mathbb{Z}(\mathbb{Z}_r)$, $0\leq i<r$: $A(1+b+\ldots+b^{r-1})=1+b+\ldots+b^{r-1}$, $D(1-b^s)=1-b^t$, $AD=\pm b^i$.

Proof Let $g\in\mathbb{Z}_r$, i.e. $g=b^i$ for some $0\leq i<r$. Let us assume that there is a solution to the above system. We have $AD=\pm g$. Multiplying both sides by $1+b+\ldots+b^{r-1}$ yields $AD(1+b+\ldots+b^{r-1})=\pm g(1+b+\ldots+b^{r-1})$. The right side is $\pm(1+b+\ldots+b^{r-1})$ and since $A(1+b+\ldots b^{r-1})=1+b+\ldots+b^{r-1}$, we get $D(1+b+\ldots+b^{r-1})=\pm(1+b+\ldots+b^{r-1})$. Also $D(1-b^s)=1-b^t$. We show that this is impossible.

Let $D=q_0+q_1b+\ldots+q_{r-1}b^{r-1}$ with $q_i\in\mathbb{Z}$. Multiplying by $1+b+\ldots+b^{r-1}$ and collecting like terms we obtain $D(1+b+\ldots+b^{r-1})=p+pb+\ldots+pb^{r-1}$ with $p=q_0+q_1+\ldots+q_{r-1}$. Since the right side must be $\pm(1+b+\ldots+b^{r-1})$, p must be ±1, so $q_0+\ldots+q_{r-1}=\pm1$.

Now consider $D(1-b^s)$. The result is:

$$\begin{aligned} &q_0 + q_1b + \ldots + q_sb^s + \ldots + q_tb^t + \ldots + q_{r-1}b^{r-1} \\ &-q_{r-s}-q_{r-s+1}b^{r-s+1}-\ldots-q_0b^s-\ldots-q_{t-s}b^{t-s}-\ldots-q_{r-1-s}b^{r-1-s}, \end{aligned}$$

where all subscripts and superscripts are taken modulo r. By hypothesis the product above is $1-b^t$. So, the following equations result:

(1) $q_0-q_{r-s}=1$, (2) $q_t-q_{t-s}=-1$, (3) $q_j=q_{r-s+j}$, $j\neq 0,t \bmod r$.

Let u be the smallest non-negative integer such that $us\equiv t \bmod r$. Note that u exists because $\gcd(s,r)=1$ so s is a generator of the additive group $\mathbb{Z}_r$. Also $1<u$, since $s\neq t$, and $t\neq 0,r$ gives $u<r$. So $1<u<r$.

Claim 1: $q_0=q_s=q_{2s}=\dots=q_{(u-1)s}$, which is at least one equality and there is no repetition of subscripts in the list.

Consider q_{ns} for $1\leq n\leq u-1$. If $ns\neq 0,t \bmod r$, we have from (3) with $j=ns$, $q_{ns}=q_{r-s+ns}=q_{(n-1)s}$. Also, $ns\equiv 0 \bmod r \Rightarrow r|ns \Rightarrow r|n$ which is impossible because $n\leq u-1<r$. And, $ns\equiv t \bmod r$ is impossible since $n<u$ violates the definition of u. Therefore, we get $q_{ns}=q_{(n-1)s}$ for $1\leq n\leq u-1$, or $q_0=q_1=\dots q_{(u-1)s}$. Now this represents at least one equality because $u>1$, i.e. $q_0=q_s$. Finally, assume there is repetition in the subscripts of this list. Then for some c and d, $0\leq c,d\leq u-1$ and say $c<d$, $cs\equiv ds \bmod r$. Then $(d-c)s\equiv 0 \bmod r \Rightarrow r|(d-c)$. But this is impossible since $d-c<r$ by assumption, and the claim is proved.

Now let v be the smallest non-negative integer such that $vs \equiv -t \bmod r$. Again v must exist. Furthermore, $v \neq 1$ since otherwise $s \equiv -t \bmod r \Rightarrow s+t=r$ which is contrary to assumption. Finally, $v < r$ because $\gcd(r,s)=1$ and $-t \not\equiv r$. Then $1 < v < r$.

Claim 2: $q_t = q_{t+s} = \dots = q_{t+(v-1)s}$, which is at least one equality and there is no repetition of subscripts in the list.

Consider q_{t+ns} for $1 \le n \le v-1$. If $t+ns \not\equiv 0, t \bmod r$, we have as before using (3) with $j=t+ns$, $q_{t+ns} = q_{r-s+t+ns} = q_{t+(n-1)s}$. Now $t+ns \equiv 0 \bmod r \Rightarrow ns \equiv -t \bmod r$. But since $n < v$ this is a violation of the definition of v. Also, $t+ns \equiv t \bmod r \Rightarrow ns \equiv 0 \bmod r$ which is again impossible since $n < r$ and $\gcd(r,s)=1$. Therefore we have $q_{t+ns} = q_{t+(n-1)s}$ for $1 \le n \le v-1$. This yields $q_t = q_{t+s} = \dots = q_{t+(v-1)s}$. Now at least we have $q_t = q_{t+s}$ because $v > 1$. There is no repetition in the subscripts for otherwise, for some c and d with $1 \le c, d \le v-1$ and say $c < d$ we would have $t+cs \equiv t+ds \bmod r$. Again, this would mean that $(d-c)s \equiv 0 \bmod r$ and $r \mid (d-c)$ which is impossible. This completes claim 2.

In particular from claim 1, $q_0 = q_{(u-1)s} = q_{us-s} = q_{t-s}$. Then $q_0 \neq q_t$ follows from (2). So we see that no q_i can appear on the list of both claim 1 and claim 2. There are u q's in one list and v on the other. Since

$us+vs=t-t=0 \bmod r$, $r|u+v$. From $0<u,v<r$ we have $u+v<2r$ whence $u+v=r$. Then there are r q's on the combined lists so every q is on one of the lists. Let $x=q_0$ and $y=q_t$.

From above $q_0+q_1+\ldots+q_{r-1}=\pm 1$. Collecting those terms equalling q_0 and those equalling q_t yields $nx+my=\pm 1$ for some positive integers n and m. Since at least one equality exists in each claim, $n,m\geq 2$. From (2) and the fact that $q_0=q_{t-s}$ we get $q_t-q_0=-1$. Hence $y-x=-1$, $nx+m(-1+x)=\pm 1$, $(n+m)x=\pm 1+m$ and $x=(\pm 1+m)/(n+m)$. When $n,m\geq 2$ the denominator is bigger than the numerator so $x=q_0$ can not be an integer. This contradicts the existence of D and so completes the proof of Lemma 4.

Now Lemma 2 follows and so Theorem 5 is proven.

For example, for r=11 the following 5 pairs in F(a,b) represent 5 distinct Q-classes, i.e. there is no Q-transformation taking any one to another. If W_r^s is again the pair of words $(b^{11}, ab^s\bar{a}\bar{b}^s)$, then the five pairs are: W_{11}^1, W_{11}^2, W_{11}^3, W_{11}^4, W_{11}^5. The sum of no two superscripts is 11. Notice, however, that W_{11}^5 and W_{11}^6 belong to the same Q-class as follows: $(b^{11}, ab^6\bar{a}\bar{b}^6) \longrightarrow (b^{11}, ab^6\bar{a}b^5) \longrightarrow (b^{11}, b^6\bar{a}b^5a) \longrightarrow (b^{11}, \bar{b}^5\bar{a}b^5a) \longrightarrow (b^{11}, \bar{a}\bar{b}^5ab^5) \longrightarrow (b^{11}, ab^5\bar{a}\bar{b}^5)$.

In general $(b^r, ab^s\bar{a}\bar{b}^s)$ is in the same Q-class as $(b^r, ab^{s+nr}\bar{a}b^{-s-nr})$. So we get

<u>Theorem 6</u> If $s \equiv t \bmod r$ then in $F(a,b)$ $(b^r, ab^s\bar{a}\bar{b}^s)$ belongs to the same Q-class as $(b^r, ab^t\bar{a}\bar{b}^t)$.

<u>Proof</u> Since $s=t+nr$ for some integer n, the result follows easily as in the above example.

Finally, as r grows large we find more and more pairwise distinct Q-classes within the normal subgroup generated by $(b^r, ab\bar{a}\bar{b})$. We state this as

<u>Theorem 7</u> Within $F(a,b)$ there exists normal subgroups possessing an arbitrarily large (finite) number of Q-classes.

<u>Proof</u> Let r be a prime number and u be the largest integer less than r/2. For any pair (s,t) of integers with $0<s<t\leq u$, $W_r^s=(b^r, ab^s\bar{a}\bar{b}^s)$ and W_r^t generate different Q-classes within the normal subgroup generated by W_r^1, since $s+t\neq r$ and $\gcd(s,r)=\gcd(t,r)=1$. There are $u(u-1)/2$ of these pairs so there are at least as many pairwise distinct Q-classes. Allowing r to be sufficiently large and prime results in an arbitrarily large number of distinct Q-classes which completes the proof.

Note that there may be more Q-classes within this normal subgroup generated by pairs not of the form W_r^s. Many possible examples arise from applications of Theorem 8 of the next section.

EXTENSIONS AND CONJECTURES

Examples of distinct Q-classes of normal subgroups of F(a,b) where the factor group is not abelian perhaps may be drawn from the dihedral groups. Let $R_r^s=(a^r,b^2,(a^sb)^2)$. Then $D_r=F(a,b)/\{R_r^1\}$ is the dihedral group of the r-gon where a generates the rotations and b the reflection. When gcd(r,s)=1 then $\{R_r^1\}=\{R_r^s\}$. The proof is much like for Theorem 4. The question then is when R_r^s and R_r^t represent distinct Q-classes.

An investigation of $J[R_r^s]$ leads to the problem of determining whether two 3x2 matrices are row equivalent over $\mathbb{Z}(D_r)$. Since D_r is not abelian, this is a very complicated matter. Factoring by the generator a leads to matrices over $\mathbb{Z}(\mathbb{Z}_2)$. Unfortunately, they are row equivalent so nothing is gained. In the case where r is even, factoring by the generator b leads to matrices over $\mathbb{Z}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$. Here the situation is manageable but tedious. In any case, this leaves the issue open but leads one to believe

Conjecture 1 In F(a,b) if $0<s<t<r$, gcd(s,r)=gcd(t,r)=1 and $s+t\neq r$ then the pairs $(a^r,b^2,(a^sb)^2)$ and $(a^r,b^2,(a^tb)^2)$ belong to different Q-classes.

In the previous section we have shown the existence of arbitrarily large numbers of Q-classes within normal subgroups of F(a,b). The obvious question comes to mind:

Does there exist a normal subgroup of a free group which possesses infinitely many Q-classes?

A related question is:

Given a t-tuple of words in a free group, is it ever the case that the normal subgroup it generates contains only one Q-class?

When the t-tuple happens to be the generators of the free group, this question is exactly the one posed in [1] and [9]. For example, the pairs $T_n=(\bar{a}^{n-1}\bar{b}a^n b, \bar{b}^{n-1}\bar{a}b^n a)$ generate normally the free group F(a,b). For $n>2$, it is unknown whether they are Q-transforms of the pair (a,b). Notice that computing $J[T_n]$ is a futile exercise: Since $F(a,b)/\{T_n\}=1$ the resulting matrix is just minus the identity matrix. The only hope is to map T_n to another pair whose normal closure is not F(a,b) and use the following fact.

Theorem 8 Let $F(a_1,\dots,a_n)$ be a free group, $W=(W_1,\dots,W_s)$ and $U=(U_1,\dots,U_t)$ s and t-tuples in F, and $f:F\longrightarrow F$ a homomorphism. If $\{W\}=\{U\}$ then $\{f(W)\}=\{f(U)\}$. Furthermore, if $Q(W)=U$ for some Q-transformation Q, then there exists a Q-transformation Q' with $Q'(f(W))=f(U)$.

Proof To show that $\{f(W)\}=\{f(U)\}$ it suffices to display for each i, $f(W_i)$ as a product of conjugates of the members of f(U) and similarly $f(U_j)$ as a product of conjugates of members of f(W). But since $\{W\}=\{U\}$, for each i we have W_i expressed as a product of conjugates of elements of U and vice versa. Applying f then yields the result.

Now say Q(W)=U. It will suffice to prove the existence of Q' when Q is an elementary Q-transformation. If Q permutes elements or multiplies one element by another then f(Q(W))=Q(f(W))=f(U) so define Q'=Q. If Q conjugates an element of W by the word X, let Q' conjugate the same indexed element of f(W) by f(X). So in any case we have f(U)=f(Q(W))=Q'(f(W)). Then applying an induction hypothesis on the number of elementary Q's composing Q completes the proof.

As an application, consider $T_3=(\bar{a}^4\bar{b}a^3b,\bar{b}^4\bar{a}b^3a)$; $\{T_3\}=F(a,b)$. Using the endomorphism $a\to ab\bar{a}\bar{b}$ and $b\to b^3$ yields the pair

$T_3'=((ab\bar{a}\bar{b})^{-4}\bar{b}^3(ab\bar{a}\bar{b})^3b^3,\bar{b}^{12}(ab\bar{a}\bar{b})^{-1}b^{12}(ab\bar{a}\bar{b}))$. From Theorem 8 we have that T_3' and $(ab\bar{a}\bar{b},b^3)$ generate the same normal subgroup of F(a,b) and that if these two pairs represent distinct Q-classes then T_3 and (a,b) also belong to distinct Q-classes.

Unfortunately, analysis of $J[T_3']$ yields no useful information. The reason for this becomes obvious when we let $R=ab\bar{a}\bar{b}$, $S=b^3$ and express T_3' as $(\bar{R}^4\bar{S}R^3S, \bar{S}^4\bar{R}S^3R)$ Then $J[T_3']$, which is a 2x2 matrix over $\mathbb{Z}(\mathbb{Z}_5)$ is exactly $-J[(R,S)]$ namely

$$-\begin{bmatrix} \frac{\partial R}{\partial a} & \frac{\partial R}{\partial b} \\ \frac{\partial S}{\partial a} & \frac{\partial S}{\partial b} \end{bmatrix}.$$

It is not difficult to see that in general, the Jacobian will never serve as a useful invariant in situations of this kind.

Nevertheless, we suspect that pairs of the form T_n' are examples of pairs representing different Q-classes from $(b^5, ab^s\bar{a}\bar{b}^s)$ and of a completely different type from those discussed in the previous section.

Perhaps the most promising approach to the problem of finding a Q-class distinct from the generators of a free group (if it exists) is to look into conditions which ensure that a t-tuple can not be reduced in length by a Q-transformation. To this end, we will restrict the action of Q-transformations in certain cases. This is discussed in the next chapter.

CHAPTER 3

SHORT Q-TRANSFORMATIONS

INTRODUCTION

In this chapter we define short Q-transformations on t-tuples of words in a free group and examine the relationships between short Q and Q-transformations and specifically a conjecture of [2] which is also treated in [9]. We will formulate a sufficient condition on Q-transformations for which the conjecture holds. Also, we define extended short Q-transformations and show that the essentially same conjecture holds for them. Along the way, we will prove a variation of a theorem of Nielsen which will yield a restricted set of Nielsen transformations which suffice to reduce t-tuples of words in a free group. We end with some conjectures.

DEFINITIONS

A fundamental complexity that arises when studying Q-transformations is that there are infinitely many elementary Q-transformations which generate the group of Q-transformations. The reason is that a Q-transformation may conjugate an element of a t-tuple and there are infinitely many choices for conjugators. If the free group from which the t-tuple comes is finitely generated, then we may pass to a finite set of generators of the group of Q-transformations by allowing conjugation only by a generator. Clearly we can generate the entire group this way. However, very little insight is gained.

Another approach is to limit conjugation to "short conjugation" in the hope of reducing the problem to a "locally finite" one. We begin with a

Definition Let $W, X \in F_n$. $W^X = \bar{X}WX$ is a short conjugate of W if X or $\bar{X}$ is totally absorbed when reducing $\bar{X}WX$.

This just means that W^X is a cyclic permutation of W. Also $|W^X| \leq |W|$ and if W is cyclically reduced $|W^X| = |W|$. For example $(ab)^a = ba$ is a short conjugate of ab but $(ab)^b = \bar{b}ab^2$ is not. Note also that if W^X is a short conjugate of W then $\bar{W}^X$ is a short conjugate of $\bar{W}$.

Definition Let $W = (W_1, \ldots, W_t)$ be a t-tuple of words in F_n. A transformation of W will be called an elementary short Q-transformation if it operates on W in one of the following ways:

1) W is left fixed or any two of the W_i are permuted.
2) W_j is left fixed $\forall j \neq r$, $1 \leq j \leq t$, and W_r is sent to a short conjugate of W_r or of $\bar{W}_r$.
3) W_j is left fixed $\forall j \neq r$, $1 \leq j \leq t$, and for r, s fixed $r \neq s$ either

   a) W_r is sent to $W_r W_s$ or b) W_r is sent to $W_s W_r$.

Elementary short Q-transformations will be multiplied in exactly the same way as elementary Q-transformations.

Definition Let $Q=q_k\cdots q_1$ be a Q-transformation with q_i elementary Q's. Q will be called a short Q-transformation relative to a t-tuple W when for each j, $k \geq j > 1$, q_j is an elementary short Q-transformation of $q_{j-1}\cdots q_1(W)$, and q_1 is a short Q-transformation of W.

From a fixed t-tuple W, there are only a finite number of short Q-transformations since for a word of length l there are at most l short conjugates. Also note that not all short Q-transformations have inverses. For example if $W=(\bar{a}\bar{b}^2ab^2a,b)$ then (a,b) is a short Q image of W but the inverse transformation is not a short Q-transformation of (a,b).

CONJECTURES

A natural question about short Q-transformations is contained in the following conjecture of [2]:

Conjecture 1 Let W be a n-tuple in $F(a_1,\ldots,a_n)$. If there exists a Q-transformation Q with $Q(W)=(a_1,\ldots,a_n)$ then there exists a short Q-transformation Q^s with $Q^s(W)=(a_1,\ldots,a_n)$.

A stronger statement is

Conjecture 2 Let W be a n-tuple in $F(a_1,\ldots,a_n)$, $n\geq 2$, and Q a Q-transformation. Then there exists a short Q-transformation Q^s with $|Q^s(W)| \leq |Q(W)|$.

These conjectures assert that short Q-transformations have the same "power" to reduce t-tuples of words as do Q-transformations. The truth of Conjecture 1 would open up a new avenue of investigation into the question left open in the previous chapter of whether there exists a n-tuple which normally generates F_n but is not a Q image of the generators of F_n.
Namely, this question seems more manageable when asked about short Q-transformations but it also remains open.

Finally a conjecture which involves only short Q-transformations is

Conjecture 3 Let $W=(W_1,\ldots,W_t)$, $W'=(\bar{x}W_1x,W_2,\ldots,W_t)$ in $F(a_1,\ldots,a_n)$, and $x=a_i^{\pm 1}$, and Q_1^s any short Q-transformation. Then there exists a short Q-transformation Q_2^s such that $|Q_2^s(W)| \leq |Q_1^s(W')|$.

We will discuss conjecture 1 later, but first we prove

Theorem 1 Conjecture 2 $\Longleftrightarrow$ Conjecture 3.

Proof First we show that Conjecture 2 $\Rightarrow$ Conjecture 3.

Let $q: W \longrightarrow W'$, which is an elementary Q-transformation. Now given Q_1^s, any short Q-transformation on W', let $Q(W)=Q_1^s(q(W))=Q_1^s(W')$. We must now show that there exists a short Q-transformation, Q_2^S, with $|Q_2^S(W)| \leq |Q_1^S(W')|$. But Conjecture 2 asserts the existence of a short Q-transformation, Q^S, with $|Q^S(W)| \leq |Q(W)|$. Then we may let $Q_2^S = Q^S$ obtaining $|Q_2^S(W)| \leq |Q(W) = Q_1^S(W')|$.

Now we show that Conjecture 3 $\Rightarrow$ Conjecture 2.

Note that by an induction argument we may replace W' in Conjecture 3 by $(W_1, \ldots, W_{i-1}, \overline{X}W_i^{\pm 1}X, \ldots, W_t)$, where X is any word in F_n.

Now let $W = (W_1, \ldots, W_t)$ and Q any Q-transformation. Say $Q = q_s q_{s-1} \ldots q_1$ with q_i elementary Q-transformations. We must show the existence of Q^S, a short Q-transformation, such that $|Q^S(W)| \leq |Q(W)|$. Let r be the number of q's comprising Q which are not elementary short Q-transformations. Comparing the definitions of elementary Q and short Q-transformations, the only way q_i can fail to be short is when it conjugates an element but strictly increases the length of that element. If $r=0$ then Q is already a short Q-transformation so we can let $Q^S = Q$. Otherwise, we assume the result for any Q-transformation which is a product of elementary Q-transformations of which fewer than r are not short.

Let l be the largest subscript such that q_l is not a short Q-transformation in $Q = q_s \ldots q_l \ldots q_1$, $s \geq l \geq 1$. Let $V = (V_1, \ldots, V_t) = q_{l-1} \ldots q_1(W)$, $l \neq 1$, and $V = W$ when $l = 1$.

Then $q_1: V \longrightarrow (V_1, \ldots, V_i^{\pm X}, \ldots, V_t) = V'$. Now let $Q_1^s = q_s \ldots q_{1+1}$ which is a short Q-transformation on V' by assumption on 1. By Conjecture 3, there exists a short Q-transformation Q_2^s satisfying $|Q_2^s(V)| \leq |Q_1^s(V')|$. Now $Q_2^s q_{1-1} \ldots q_1$ has fewer than r component elementary Q-transformations that are not short, so by the induction hypothesis there exists a short Q-transformation Q^s such that $|Q^s(W)| \leq |Q_2^s q_{1-1} \ldots q_1(W)|$. So finally we have $|Q^s(W)| \leq |Q_2^s q_{1-1} \ldots q_1(W) = Q_2^s(V)| \leq |Q_1^s(V') = q_s \ldots q_1(W) = Q(W)|$ which completes the proof.

Later in this chapter we will give a restricted setting in which Conjecture 2 holds.

EXTENDED SHORT Q-TRANSFORMATIONS

We begin with a definition of another transformation of t-tuples of words in F_n very similar to short Q-transformations.

Definition Let $W=(W_1, \ldots, W_t)$ be a t-tuple of words in F_n. A transformation of W will be called an elementary extended short Q-transformation (hereafter called an elementary P-transformation) if it either is an elementary short Q-transformation on W or it leaves W_j fixed for $j \neq r$, $1 \leq j \leq t$ and for r,s fixed, $r \neq s$ either

a) W_r is sent to $W_r^{\pm X} W_s$ or b) W_r is sent to $W_s W_r^{\pm X}$

where $X \epsilon F_n$ and $W_r^{\pm X}$ is a short conjugate of $W_r^{\pm 1}$.

Once again, we multiply elementary P-transformations in the standard way. A P-transformation relative to a t-tuple W will then be a finite product of elementary P-transformations.

We prove a theorem about P-transformations similar to Conjecture 1. First, however, we need the following

<u>Lemma</u> Let $G=\langle a_1,\ldots,a_n; W_1,\ldots,W_n\rangle$. If $G=1$ then for each generator there exists an i such that the exponent of W_i on this generator is not 0.

<u>Proof</u> Assume this is false. Then there exists a generator, say a_j, whose exponent sum in every W_i is 0. Then G/G' (G mod its commutator subgroup) has a presentation in which a_j does not appear in any relator other than commutators. So in G/G' $a_j \neq 1$ so $G \neq 1$ which is a contradiction and so completes the proof of the lemma.

Before we state the theorem let us give an example for it. Consider the following Q-transformation: $(ab^2, \bar{a}\bar{b}ab^2a) \longrightarrow (\bar{b}ab^3, \bar{a}\bar{b}ab^2a)$, which is just a conjugation of the first element by b. Note that the word ba is a short conjugate of $\bar{a}\bar{b}ab^2a$ and similarly $\bar{a}\bar{b}$ a short conjugate of $\bar{a}\bar{b}^2\bar{a}ba$. So the above Q-transformation can be realized by a P-transformation as follows:

$(ab^2, \bar{a}\bar{b}ab^2a) \longrightarrow (ab^2ba, \bar{a}\bar{b}ab^2a) \longrightarrow (\bar{a}\bar{b}ab^3a, \bar{a}\bar{b}ab^2a) \longrightarrow$
$(\bar{b}ab^3, \bar{a}\bar{b}ab^2a)$.

Theorem 2 Let $G = \langle a_1, \ldots, a_n; W_1, \ldots, W_n \rangle = 1$, $n \geq 2$, and Q any Q-transformation on $W = (W_1, \ldots, W_n)$. Then there exists a P-transformation P such that $P(W) = Q(W)$.

Proof It suffices to prove the theorem in the case that $Q(W) = (W_1, \ldots, W_i^X, W_{i+1}, \ldots, W_n)$ where W_i^X is not a short conjugate of W_i, $X \in F_n$. This is clear since Q is a product of elementary Q-transformations each of which is either a short Q-transformation, and so already a P, or a conjugator of an element but not a short conjugator. And, an induction argument on the number of elementary Q components of Q would yield the result. Furthermore, we can assume $X = x = a_j^{\pm 1}$, a single generator, for we could then proceed by induction on the length of X. Lastly, without loss of generality we assume that $Q(W_1, \ldots, W_n) = (W_1^x, W_2, \ldots, W_n)$.

Now since $G = 1$, by our previous lemma there is some r such that the exponent sum of a_j in W_r is not 0. Let k be the largest such r.

Case 1: $k \neq 1$. Then $W_k^{\pm 1} = \bar{U}AxBU$ with some of A,B,U possibly 1, AxB cyclically reduced and $\bar{U}AxBU$ reduced as written. Then xBA is a short conjugate of $W_k^{\pm 1}$ and the inverse $\bar{A}\bar{B}\bar{x}$ a short conjugate of $W_k^{\mp 1}$, and each is reduced as written. Also, since W_1^x is not a short conjugate of W_1, $\bar{x}W_1x$ is reduced as written and then so is $\bar{A}\bar{B}\bar{x}W_1xBA$. Therefore $\bar{x}W_1x$ is a short conjugate of $\bar{A}\bar{B}\bar{x}W_1xBA$. Then finally the following product of elementary P-transformations on W realize Q(W):

$(W_1,\ldots,W_k,\ldots,W_n) \longrightarrow (W_1xBA,\ldots,W_k,\ldots,W_n) \longrightarrow$
$(\bar{A}\bar{B}\bar{x}W_1xBA,\ldots,W_k,\ldots,W_n) \longrightarrow (\bar{x}W_1x,\ldots,W_k,\ldots,W_n)$.

Case 2: k=1. Then, in particular W_2 has 0 exponent sum on a_j since k was maximal. But then W_1W_2 has non-zero exponent sum on a_j. So, by Case 1:

$(W_1,\ldots,W_n) \longrightarrow (W_1,W_1W_2,\ldots,W_n) \longrightarrow (W_1^x,W_1W_2,\ldots,W_n)$

is realizable by a P-transformation. And, since by assumption $\bar{x}W_1x$ is reduced as written, W_1 is a short conjugate of W_1^x so we may continue with an elementary P-transformation $P:(W_1^x,W_1W_2,\ldots,W_n) \longrightarrow (W_1^x,W_2,\ldots,W_n)$. This completes the proof.

Corollary Let $W=(W_1,\ldots,W_n)$ be in $F(a_1,\ldots,a_n)$, $x=a_j$, and $Q:W \longrightarrow (W_1,\ldots,W_i^x,\ldots,W_n)$ be a Q-transformation with $|W_i^x|>|W_i|$. If there exists a $k\neq i$ such that W_k is both cyclically reduced and has non-zero exponent sum on a_j then Q(W) can be effected by a short Q-transformation.

Proof As before, $W_k^{\pm 1}=AxB$ with possibly A or B 1 but otherwise AxB reduced and cyclically reduced by assumption. Then xBA and AxB are short conjugates of one another and similarly for $\bar{B}\bar{x}\bar{A}$ and $\bar{A}\bar{B}\bar{x}$. Without loss of generality we assume that $Q(W_1,\ldots,W_n)=(W_1^x,\ldots,W_n)$ and $k\neq 1$. So the following short Q-transformations realize Q:

$$(W_1,\ldots,W_n)\longrightarrow(W_1,\ldots,xBA,\ldots,W_n)\longrightarrow(W_1xBA,\ldots,xBA,\ldots,W_n)$$
$$\longrightarrow(W_1xBA,\ldots,\bar{A}\bar{B}\bar{x},\ldots,W_n)\longrightarrow(\bar{A}\bar{B}\bar{x}W_1xBA,\ldots,\bar{A}\bar{B}\bar{x},\ldots,W_n)\xrightarrow{q}$$
$$(\bar{x}W_1x,\ldots,\bar{A}\bar{B}\bar{x},\ldots,W_n)\longrightarrow(\bar{x}W_1x,\ldots,AxB,\ldots,W_n)$$
$$=(W_1^x,\ldots,W_k,\ldots,W_n).$$

In the above, q is a short Q-transformation because $\bar{A}\bar{B}\bar{x}W_1xBA$ is reduced as written by the assumption that $|W_1^x|>|W_1|$. This completes the proof.

Extending this corollary to a proof of Conjecture 2 is sadly beyond reach at this point.

A SUFFICIENT CONDITION

On closer examination, we see that any Q-transformation can be broken down into elementary Nielsen transformations and conjugations. Thus a proof of Conjecture 3 might proceed by induction on the number of conjugations that make up the short Q-transformation, Q_1^s, on $W'=(\bar{x}W_1x,W_2,\ldots,W_t)$. If Q_1^s contains no conjugations then it is simply a Nielsen transformation. One may hope that in this situation the Q_2^s of Conjecture 3 would just turn out to be a Nielsen transformation on $W=(W_1,\ldots,W_t)$ such that $|Q_2^s(W)|\leq|Q_1^s(W')|$. This will be too much to hope for as the following example shows.

Consider the pair $(bab^2abab, abab^2)$ in $F(a,b)$ which will play the role of W. The pair can't be reduced any further by Nielsen transformations since it is Nielsen reduced. However, the pair $(abab^2abab\bar{a}, abab^2)$, which will play the role of W', may be reduced to (a,b) by Nielsen transformations as follows:

$(abab^2abab\bar{a}, abab^2) \longrightarrow (abab\bar{a}, abab^2) \longrightarrow (\bar{b}\bar{a}, abab^2) \longrightarrow$
$(\bar{b}\bar{a}, ab^2) \longrightarrow (\bar{b}\bar{a}, b) \longrightarrow (\bar{a}, b) \longrightarrow (a,b)$.

So even if Q_1^s is only a Nielsen transformation, Q_2^s may need to contain conjugations but, we will show, short conjugations will suffice. Indeed, a short Q-transformation can reduce the original pair to (a,b) as follows: $(bab^2abab, abab^2) \longrightarrow (bab^2abab, bab^2a) \longrightarrow$
$(bab, bab^2a) \longrightarrow (bab, ba) \longrightarrow (b, ba) \longrightarrow (b,a) \longrightarrow (a,b)$.

Later we will be able to generalize this example to the following, which is our

<u>Theorem 6</u> Let $W=(W_1,\ldots,W_t)$, $W'=(\bar{X}_1W_1X_1,\ldots,\bar{X}_tW_tX_t)$, $W_i, X_i \in F(a_1,\ldots,a_n)$, and N any Nielsen transformation. Then there exists a short Q-transformation Q^s such that $|Q^s(W)| \leq |N(W')|$.

Theorem 7, which gives restricting conditions on Q-transformations under which Conjecture 2 holds, will follow as a generalization of Theorem 6.

We will find it necessary to examine a certain subset of the set of Nielsen transformations which turn out to have an especially convenient relationship with short Q-transformations. Fortunately, passing to this subset will yield in some sense no loss of generality (Theorem 4). The following technical observations on Nielsen transformations will be needed to prove this. We begin with a

Definition Let $W \in F_n$ and I an initial segment of W; thus W=IX reduced as written with possibly X=1. If $\frac{1}{2}|W|+1 \geq |I| > \frac{1}{2}|W|$ then I is called a major initial segment, and if $|I|=\frac{1}{2}|W|$ then I is called the left half of W. Similarly if W=YT, T a terminal segment of W with possibly Y=1, then if $\frac{1}{2}|W|+1 \geq |T| > \frac{1}{2}|W|$ then T is called a major terminal segment and if $|T|=\frac{1}{2}|W|$ then T is called the right half of W.

Of course, only words of even length have left and right halves. For example if $W=a^2b\bar{a}^2b$, then the major initial, major terminal, left half and right half of W are $a^2b\bar{a}$, $b\bar{a}^2b$, a^2b, and $\bar{a}^2b$ respectively.

Definition Let $A,B \in F_n$. A will be called isolated from B when the following three conditions hold:

1) The major initial segment of A is not an initial segment of either B or $\bar{B}$.

2) The major terminal segment of A is not a terminal

segment of either B or $\bar{B}$.

3) When A has even length then either

a) The left half of A is not an initial segment of either B or $\bar{B}$, or

b) The right half of A is not a terminal segment of either B or $\bar{B}$.

For example ab is not isolated from a^2b^2 since neither 3a) nor 3b) holds. However, ab is isolated from $a^2b\bar{a}^2$.

Definition A pair (A,B) is called isolated when A is isolated from B and B is isolated from A.

Note that a pair containing the element 1 is isolated in a vacuous sense.

The following lemma simplifies the determination of whether a pair is isolated.

Lemma Let $A,B\neq 1$, $|A|\geq|B|$. If B is isolated from A then A is isolated from B and so the pair (A,B) is isolated.

Proof Assume A is not isolated from B. Say S is a major initial segment of A which is an initial segment of $B^{\pm1}$. Since $|S|>\frac{1}{2}|A|\geq\frac{1}{2}|B|$, an initial segment of S, say R, is the major initial segment of $B^{\pm1}$. But then R is an initial segment of A, which means B is not isolated from A. The above follows similarly for when S is a major terminal segment of A, so if A is of odd length we are done.

Otherwise, $A=LR$ where L is the left half and R the right half, and neither is isolated from B (i.e. L and R are respectively initial and terminal segments of $B^{\pm 1}$). If B has odd length then $|B|<|A|$ and so an initial segment of L is a major initial segment of $B^{\pm 1}$, which is not isolated from A. Then B is not isolated from A.

If B has even length then either B or $\bar{B}$ has initial segment L and terminal segment R. (Note that if L is an initial segment of B and R a terminal segment of $\bar{B}$ then $L=\bar{R}$ so $A=1$ which we don't allow.) Then for $B^{\pm 1}$, its left half is an initial segment of L and its right half is a terminal segment of R. This means that B is not isolated from A, which then completes the proof.

<u>Definition</u> A t-tuple W in F_n is called Nielsen reduced if every pair (W_i, W_j), $i \neq j$, of elements from W is isolated.

Nielsen proved that a Nielsen reduced t-tuple in F_n freely generates a free subgroup of F_n. Also, of all t-tuples generating a particular subgroup of F_n, those that are Nielsen reduced have the smallest total length. For example, all the Nielsen reduced n-tuples generating $F(a_1, \ldots, a_n)$ are permutations of $(a_1^{\pm 1}, \ldots, a_n^{\pm 1})$. Finally, Nielsen proved that given any t-tuple W, there is a "semidirect" Nielsen transformation taking W to a Nielsen reduced t-tuple (which, of course, generates the same subgroup as W). Our next theorem gives a new proof of this last fact (statements 1 and 2 of Theorem 3) and a useful refinement of it (statement 3 of Theorem 3).

Theorem 3 For every t-tuple $W=(W_1,\ldots,W_t)\in F_n$, there exists a Nielsen transformation $N=N_s,\ldots N_1$ with N_i elementary Nielsen transformations such that 1) N(W) is Nielsen reduced and 2) N is semidirect (i.e. no N_i increases the length of the t-tuple it acts on). Moreover, 3) if $W^*=(W_1^*,\ldots,W_t^*)=N_i\ldots N_1(W)$ and $N_{i+1}(W^*)=(W_1^*,\ldots,W_j^*W_k^*,\ldots,W_t^*)$ then the pair (W_j^*,W_k^*) is not isolated.

Proof Consider the set of all t-tuples obtainable as a Nielsen image of W satisfying 2) and 3). Let U be one of minimal length chosen from this set. In other words, no Nielsen transformation satisfying 2) and 3) can further reduce the length of U.

First assume t=2. Then if U is an isolated pair we are done since by definition it is Nielsen reduced and so satisfies 1). Otherwise, the smaller element, say U_1, is not isolated from U_2 (by the previous lemma). Also, U_1 must be of even length: for otherwise it has a non-isolated major segment which means we can reduce the length of U. Therefore, either $(U_1, U_1U_2^{\pm1})$ or $(U_1, U_2^{\pm1}U_1)$ is an isolated pair thus Nielsen reduced, obtained from U by an elementary Nielsen transformation satisfying 2 and 3). So, we are done.

Now assume the result holds for all s-tuples $2 \leq s < t$. Let U be a minimal t-tuple defined as above. By permuting we may obtain $U=(U_1,\ldots,U_t)$ with $|U_1| \leq |U_2| \leq \ldots \leq |U_t|$. Apply the induction hypothesis to $(U_1,\ldots,U_{t-1})$ to obtain $V=(V_1,\ldots,V_{t-1},U_t)$, a t-tuple in which the first t-1 elements are Nielsen reduced. Note that U_t is still the longest element since no Nielsen transformation could have increased length. Permuting if necessary, we can assume that $|V_1| \leq \ldots \leq |V_{t-1}| \leq |U_t|$. If any elements of V are 1 we again apply the induction hypothesis to the remaining ones and we are done. So assume no element is 1. Now, to finish the proof we must isolate the V's from U_t with a Nielsen transformation satisfying 2) and 3) obtaining a Nielsen reduced t-tuple. (The lemma eliminates the need to isolate U_t from the V's.)

Let i be the largest subscript such that V_i is not isolated from U_t. As before, V_i is of even length with major initial and terminal segments isolated from

U_t. Let V_i=LR with R its right half and L its left half. Then $U_t^{\pm 1}$=LXR with X possibly 1. Let $V_t=\bar{V}_i U_t^{\mp 1}=\bar{R}XR$. Then $V=(V_1,\ldots,V_t)$ is a Nielsen image of V' satisfying 2) and 3). Finally, we need to show that for all $j<i$, V_j is still isolated from V_t, and the process may continue so that after at most t-1 steps the t-tuple will be Nielsen reduced.

Assume V_j is not isolated from V_t. Again, V_j is of even length with isolated major segments. But $|V_j|\leq|V_i|$ so its left half must be an initial segment of $\bar{R}$ and its right half a terminal segment of R. But this means V_j=1 which we ruled out before. This completes the proof of Theorem 3.

At this point we would like to restrict our attention to a certain class of Nielsen transformations which we will call complete. The need for these transformations and their connection with short Q-transformations will become evident in Theorem 5. Using Theorem 3 we will show that complete Nielsen transformations suffice to Nielsen reduce any t-tuple.

Before giving the definition we note the following. Any word V in F_n may be expressed as a conjugate of a cyclically reduced word W. That is $V=W^X$. Also, W can be found so that $\bar{X}WX$ is reduced as written. W will then simply be a subword of V. We will illustrate this and the definition by an example below.

<u>Definition</u> The Nielsen transformation N will be called elementary complete with respect to $V=(V_1,\ldots,V_t)\in F_n$ if $|N(V)|\le|V|$ and either

1) N is a permutation of V or takes some V_i to their inverses, or

2) When V is expressed as $W=(W_1^{X_1},\ldots,W_t^{X_t})$ with $V_i=W_i^{X_i}$, W_i cyclically reduced and $\bar{X}_iW_iX_i$ reduced as written then either

   a) $N:(W_1^{X_1},\ldots,W_t^{X_t})\longrightarrow(W_1^{X_1},\ldots,W_l^{X_l}W_k^{X_k},\ldots,W_t^{X_t})$ $k\ne l$, $1\le k,l\le t$ and $\bar{X}_k$ and X_l are absorbed or

   b) $N:(W_1^{X_1},\ldots,W_t^{X_t})\longrightarrow(W_1^{X_1},\ldots,W_{l-1}^{X_{l-1}},\bar{W}_k^{X_k}W_l^{X_l}W_k^{X_k},\ldots,W_t^{X_t})$ $k\ne l$, $1\le k,l\le t$.

The content of this definition is this: When N is a reduction of length then either $\bar{X}_1W_1X_1\longrightarrow\bar{X}_1W_1X_1\bar{X}_kW_kX_k$ and the segment $X_1\bar{X}_k$ is absorbed, or else $\bar{X}_1W_1X_1\longrightarrow\bar{X}_k\bar{W}_kX_k\bar{X}_1W_1X_1\bar{X}_kW_kX_k$. For example, let $V_1=ab\bar{c}\bar{b}\bar{a}=\bar{c}^{\bar{b}\bar{a}}$ and $V_2=abc\bar{b}db\bar{c}\bar{b}\bar{a}=d^{b\bar{c}\bar{b}\bar{a}}$, so $W_1=\bar{c}$, $X_1=\bar{b}\bar{a}$, $W_2=d$, $X_2=b\bar{c}\bar{b}\bar{a}$. Then $(V_1,V_2)\longrightarrow(V_1,V_1V_2)$ is not complete. Even though length is reduced, not all of $b\bar{c}\bar{b}\bar{a}$, the exponent of V_2 is absorbed. However, $(V_1,V_2)\longrightarrow(V_1,V_1V_2\bar{V}_1)$ is complete.

<u>Definition</u> A Nielsen transformation N will be called

complete with respect to $V=(V_1,\dots,V_t)$ when $N=N_s\dots N_1$, N_i complete elementary Nielsen transformations with respect to $N_{i-1}\dots N_1(V)$, $i>1$, and N_1 with respect to V.

Now we show that for our purposes there is no loss in power resulting from passing over to complete Nielsen transformations.

<u>Theorem 4</u> If $V=(V_1,\dots,V_t)\subset F_n$, then there exists a complete Nielsen transformation N with $N(V)$ Nielsen reduced.

First we prove the following

<u>Lemma</u> If $N:(V_1,V_2)\longrightarrow(V_1,V_1V_2)$ does not increase length but is not a complete Nielsen transformation then either (V_1,V_2) is isolated or there exists a complete Nielsen transformation N^c with $|N^c(V_1,V_2)|<|(V_1,V_2)|$.

<u>Proof</u> Let $(W_1^{X_1},W_2^{X_2})=(V_1,V_2)$ with W_i cyclically reduced and $\overline{X}_iW_iX_i$ reduced as written. Then N being not complete means that in the expression $\overline{X}_1W_1X_1\cdot\overline{X}_2W_2X_2$ not all of X_1 and of $\overline{X}_2$ is absorbed. But since $|N(V)|\leq|V|$ all of X_1 and in fact at least half of W_1 must be absorbed. So not all of $\overline{X}_2$ is absorbed.

<u>Case 1</u> More than half of V_1 is absorbed. Then we have $|\overline{X}_1W_1X_1\cdot\overline{X}_2W_2X_2|<|\overline{X}_2W_2X_2|$ and in fact multiplying V_2 by $\overline{V}_1$ on the left reduces length and is a complete Nielsen

transformation.

Case 2 Exactly half of V_1 is absorbed. Then $V_1=LR$ where L is the left and R the right half. Not all of $\bar{X}_2$ is absorbed so $V_2=\bar{R}\bar{Y}W_2YR$. We see that then the left half of V_1 is not an initial segment of V_2 so neither is its major initial segment an initial segment of V_2. The major terminal segment of V_1 is also not a terminal segment of V_2 for otherwise more than half of V_1 would be absorbed in V_1V_2. Then V_1 is isolated from V_2 and since $|V_1|<|V_2|$ we have (V_1,V_2) an isolated pair by the previous lemma. This completes the proof.

Note that the Lemma holds if $N:(V_1,V_2)\longrightarrow(V_1,V_2V_1)$.

Proof of Theorem 4 From Theorem 3 we know that there exists a Nielsen transformation $M=M_s\ldots M_1$ satisfying conditions 1) 2) and 3) for V. We now proceed by induction on $|V|$.

If $|V|=|M(V)|$ then we claim that M is already complete. We need only check that those M_i which multiply one element by another are complete. Now M_i does not increase length and no Nielsen transformation can decrease the length of $M_{i-1}\ldots M_1(V)$ since its length is that of $M(V)$ which is Nielsen reduced. So, by the previous lemma, if M_i multiplies two elements it is either complete or the elements are isolated. But the second case violates 3) of Theorem 3 so in fact M_i must be complete.

If $|V|>|M(V)|$ then let i be the smallest index such that M_i is not complete. Let $U=M_{i-1}\cdots M_1(V)$ or $U=V$ if $i=1$. Then $M_i:(U_1,\ldots,U_t)\to(U_1,\ldots,U_jU_k,\ldots,U_t)$. By assumption, M_i does not increase length and the pair (U_j,U_k) is not isolated. Then by the previous lemma, there exists a complete Nielsen transformation N^c with $|N^c(U)|<|U|\leq|V|$. Applying the induction hypothesis to $N^c(U)$ the reduction can be finished by complete Nielsen transformations. $M_{i-1}\cdots M_1(V)$ is already complete by assumption on i, so the theorem is proven.

The following lemma and Theorem 5 connect short Q-transformations with complete Nielsen transformations.

<u>Lemma</u> Let V and W be t-tuples in F_n with each W_i being V_i cyclically reduced. If N^c is any elementary complete Nielsen transformation on V, then there exists a short Q-transformation Q^s with $|Q^s(W)|\leq|N^c(V)|$ and $Q^s(W)$ conjugate to $N^c(V)$.

<u>Proof</u> There exists $X_1,\ldots,X_t$ with $(W_1^{X_1},\ldots,W_t^{X_t})=W^X=(V_1,\ldots,V_t)$ such that $\bar{X}W_iX$ are reduced as written. Now if N^c is a permutation of V or takes some V_i to their inverses then let Q^s do exactly the same to W. This Q^s will satisfy the conditions of the Lemma.

If N^c is of type 3b) in the definition of complete Nielsen trnasformation it amounts to conjugating an element of V. Then we can let Q^s simply be the identity on W, for $Q^s(W)$ is still conjugate to $N^c(V)$ and since W is cyclically reduced we retain $|Q^s(W)| \leq |N^c(V)|$.

Finally, we consider the case that N^c is of type 3a) in the definition. Then $N^c: (W_j^{X_j}, W_k^{X_k}) \longrightarrow (W_j^{X_j} W_k^{X_k}, W_k^{X_k})$ with X_j and $\overline{X}_k$ absorbed, $j \neq k$ and N^c leaves all other elements fixed. (The case $N^c: (W_j^{X_j}, W_k^{X_k}) \longrightarrow (W_k^{X_k} W_j^{X_j}, W_k^{X_k})$ is similar.)

It suffices to find now a short Q-transformation taking W to a conjugate of $N^c(V)$; having that, we can follow it with the short Q-transformation which cyclically reduces its argument and define Q^s as the product of these. This will ensure that $|Q^s(W)| \leq |N^c(V)|$.

Case 1: $|X_k| \geq |X_j|$. Then $\overline{X}_k W_k X_k = \overline{X}_j \overline{Z} W_k Z X_j$ with possibly $Z=1$. Now all of $\overline{X}_k$ is absorbed so $W_j = TZ$. Then $W_j^{X_j} W_k^{X_k} = \overline{X}_j TZX_j \cdot \overline{X}_j \overline{Z} W_k Z X_j = \overline{X}_j T W_k Z X_j$.

Consider the following transformations on (W_j, W_k): $(TZ, W_k) \xrightarrow{q_1} (ZT, W_k) \xrightarrow{q_2} (ZT \cdot W_k, W_k)$. Since $TZ = W_j$ is cyclically reduced by assumption, ZT is also cyclically reduced and a short conjugate of TZ. So, q_1 is a short Q-transformation, and clearly so is q_2. So, let $Q^s = q_2 q_1$. Then $Q^s(W_j, W_k) = (ZTW_k, W_k)$ which is conjugate to $(W_j^{X_j} W_k^{X_k}, W_k^{X_k}) = (\overline{X}_j T W_k Z X_j, W_k^{X}\ )$.

Case 2: $|X_k|<|X_j|$. Then $\overline{X}_j W_j X_j=\overline{X}_k\overline{Z}W_j Z X_k$. Again X_j is absorbed and also at least half of W_k. Then $W_k=\overline{Z}T$ so $W_j^{X_j}W_k^{X_k}=\overline{X}_k\overline{Z}W_j Z X_k\cdot\overline{X}_k\overline{Z}T X_k=\overline{X}_k\overline{Z}W_j T X_k$.

Consider the following transformations on (W_j,W_k). $(W_j,\overline{Z}T)\xrightarrow{q_1}(W_j,T\overline{Z})\xrightarrow{q_2}(W_j T\overline{Z},T\overline{Z})$. Again since $\overline{Z}T$ is cyclically reduced, $T\overline{Z}$ is also and just a short conjugate of $\overline{Z}T$, so q_1 is a short Q-transformation. Clearly, q_2 is also short. Then let $Q^s=q_2q_1$ giving $Q^s(W_j,W_k)=(W_jT\overline{Z},T\overline{Z})$ which is conjugate to $(W_j^{X_j}W_k^{X_k},W_k^{X_k})$ $=(\overline{X}_k\overline{Z}W_jTX_k,\overline{X}_k\overline{Z}TX_k)$. This completes the proof.

Now we generalize the lemma as

Theorem 5 Let $V=(V_1,\ldots,V_t)$ and $W=(W_1,\ldots,W_t)$ conjugate to V in F_n. If N^c is any complete Nielsen transformation on V then there exists a short Q-transformation Q^s with $|Q^s(W)|\leq|N^c(V)|$ and $Q^s(W)$ conjugate to $N^c(V)$.

Proof Let $N^c=N_r\ldots N_1$ with each N_i an elementary complete Nielsen transformation. Let C be a short Q-transformation such that $C(W)$ is V cyclically reduced. If $r=1$ the previous lemma applied to $C(W)$ yields a short Q-transformation Q_1^s with $|Q_1^sC(W)|\leq|N^c(V)|$. So $Q^s=Q_1^sC$.

Now let $N'=N_{r-1}\ldots N_1$. By the induction hypothesis there exists a short Q-transformation Q_2^s with $Q_2^s(W)$ conjugate to $N'(V)$. Again, let C be a short Q-transformation such that $C(Q_2^s(W))$ is $N'(V)$ cyclically reduced.

We apply the previous lemma to $CQ_2^s(W)$ and $N'(V)$ obtaining a short Q-transformation Q_3^s with $|Q_3^s CQ_2^s(W)| \leq |N_s N'(V)|$ and $Q_3^s CQ_2^s(W)$ conjugate to $N_s N'(V) = N^c(V)$. So $Q^s = Q_3^s C Q_2^s$, which completes the proof.

We can now prove

<u>Theorem 6</u> Let $W=(W_1,\ldots,W_t), W'=(\overline{X}_1 W_1 X_1,\ldots,\overline{X}_t W_t X_t)$ be in F_n and N be any Nielsen transformation. Then there exists a short Q-transformation Q^s such that $|Q^s(W)| \leq |N(W')|$.

<u>Proof</u> By Theorem 4 there exists a complete Nielsen transformation N^c with $N^c(W')$ Nielsen reduced. In particular $|N^c(W')| \leq |N(W')|$. Now W is conjugate to W' so by Theorem 5 there exists a short Q-transformation Q^s with $|Q^s(W)| \leq |N^c(W')|$. So we get $|Q^s(W)| \leq |N(W')|$ and the proof is complete.

A Q-transformation is an alternating product of Nielsen transformations and conjugations. If we demand that the Nielsen transformations comprising Q be complete we can apply Theorem 5 repeatedly to get a restricted case where Conjecture 3 holds.

<u>Theorem 7</u> Let $Q=C_s N_s \ldots C_1 N_1$, N_i complete Nielsen transformations, C_i conjugating transformations and W a t-tuple in F_n. Then there exists a short Q-transformation Q^s with $|Q^s(W)| \leq |Q(W)|$.

SOME QUESTIONS

Theorem 7 leads one to make a conjecture that implies Conjecture 2. To state it call a Q-transformation complete if it satisfies the hypothesis of Theorem 7.

Conjecture 4 Let W be a t-tuple in F_n and Q a Q-transformation. Then there exists a complete Q-transformation Q^c with $|Q^c(W)| \leq |Q(W)|$.

It seems reasonable to make yet another conjecture related to Conjecture 2. Let us call a Q-transformation, $Q=Q_s \ldots Q_1$ with Q_i elementary, quasidirect if the Q_i which are not conjugators do not increase length.

Conjecture 5 Let W be a t-tuple in F_n and Q a quasidirect Q-transformation. Then there exists a short Q-transformation Q^s with $|Q^s(W)| \leq |Q(W)|$.

Though not venturing a conjecture, we raise the following question: when a n-tuple is a Q-transform of the generators of F_n, is it possible to reduce the n-tuple to the generators using a quasidirect Q-transformation? An affirmative answer would further reduce the isomorphism problem of presentations of the trivial group.

REFERENCES

1. Andrews, J.J., Curtis, M.L., "Free groups and handlebodies" Proc. Amer. Math. Soc. 16 (1965), 192-195.

2. ———, "Extended Nielsen operations in free groups" Amer. Math. Monthly 73 (1966), 21-28.

3. Coxeter, H.S.M., Moser, W.O.J., Generators and relations for discrete groups Springer-Verlag, 1957.

4. Crowell, Richard H., Fox, Ralph H., Introduction to knot theory Ginn and Co., 1963.

5. Fox, Ralph H., "Free differential calculus. I. Derivations in the free group ring" Ann. of Math. (2) 57 (1953), 547-560.

6. Magnus, W., Karrass, A. & Solitar, D., Combinatorial group theory Interscience Publ., 1966.

7. Metzler, W., "Über den Homotopietyp zweidimensionaler CW-komplexe und Elementartranformationen bei Darstellungen von Gruppen durch Erzeugende und definierende Relationen" J. Reine Angew. Math. 285 (1976), 7-23.

8. Rabin, M.O., "Recursive unsolvability of group theoretic problems" Ann. of Math. 67 (1958), 172-194.

9. Rapaport, Elvira Strasser, "Groups of order 1: Some properties of presentations" Acta Math. 121 (1968), 127-150.