A result on the Word Problem for free groups

MAT 690 Coxeter Groups Seminar

Let $\mathcal{A}$ be a set, and let $\mathcal{W}_\mathcal{A}$ be the set of all finite-length words from the alphabet $\mathcal{A} \cup \mathcal{A}^{-1}$. We refer to each element of a word in $\mathcal{W}_\mathcal{A}$ as a *factor*. Make $\mathcal{W}_\mathcal{A}$ a monoid using concatenation as the operation and the empty word, denoted ε, as the identity. Let $l(w)$ be the length of any word $w \in \mathcal{W}_\mathcal{A}$, with $l(\varepsilon) = 0$. A *subword* of w is a sequence of consecutive factors of w.

Say a word $v \in \mathcal{W}_\mathcal{A}$ is obtained from $u \in \mathcal{W}_\mathcal{A}$ by an *elementary reduction* (respectively, *elementary expansion* if v is obtained from u by deleting (resp. inserting) a subword of the form aa^{-1} or $a^{-1}a$ for some $a \in \mathcal{A}$. Say $u \sim v$ if we can pass from u to v by a (possibly empty) finite sequence of elementary reductions or expansions. In this case say u and v are *freely equivalent*. Say a word $w \in \mathcal{W}_\mathcal{A}$ is *reduced* if it contains no subwords of the form aa^{-1} or $a^{-1}a$.

Exercise 1 Show $\sim$ is an equivalence relation on $\mathcal{W}_\mathcal{A}$.

For $w \in \mathcal{W}_\mathcal{A}$, denote by $[w]$ the equivalence class of w with respect to the equivalence relation $\sim$ on $\mathcal{W}_\mathcal{A}$. If $u, v \in [w]$, then write $u \to v$ if v is obtained from u by an elementary expansion (or, equivalently, if u is obtained from v by an elementary reduction). So we obtain a directed graph $\mathcal{R}(w)$ whose vertices are the set of words freely equivalent to w and whose directed edges correspond to the application of one elementary expansion. Some observations:

Observation 1 The directed graph $\mathcal{R}(w)$ is connected. This follows from the fact that if $u, v \in \mathcal{R}(w)$, then $u \sim w$ and $v \sim w$ implies that u and v are freely equivalent. Thus there is a sequence of elementary expansions or reductions that move us from u to v.

Observation 2 If $w_1 \to w_2$ in $\mathcal{R}(w)$, then $l(w_1) = l(w_2) - 2$. Thus, for a path in $\mathcal{R}(w)$ of the form $u = u_0 \to u_1 \to \cdots \to u_p = v$, we have $p \leq \lfloor l(v)/2 \rfloor$.

Think of directed edges in $\mathcal{R}(w)$ as pointing "up." We will view $\mathcal{R}(w)$ as a partially ordered set as follows: For $u, v \in \mathcal{R}(w)$, say $u \leq v$ if $u = v$ or there is some sequence $u \to \cdots \to v$ of directed edges from u up to v.

Exercise 2 Show that $(\mathcal{R}(w), \leq)$ is a partially ordered set as follows:

(A) Show that $\leq$ is reflexive: $v \leq v$ for all $v \in \mathcal{R}(w)$.

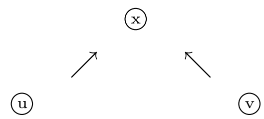
(B) Show that $\leq$ is antisymmetric: If for any $u, v \in \mathcal{R}(w)$ we have $u \leq v$ and $v \leq u$, then $u = v$.

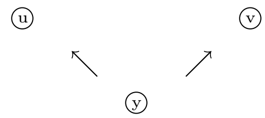
(C) Show that $\leq$ is transitive: If for any $w_1, w_2, w_3 \in \mathcal{R}(w)$ we have $w_1 \leq w_2$ and $w_2 \leq w_3$, then $w_1 \leq w_3$.

We continue with an observation about this partially ordered set $\mathcal{R}(w)$:

Observation 3 For any $v \in \mathcal{R}(w)$, there is a $u \in \mathcal{R}(w)$ for which $u \leq v$ and u is *minimal* in $\mathcal{R}(w)$, i.e. if $u' \leq u$, then $u' = u$. The reason is as follows: Let p be the largest integer such that there is a path in $\mathcal{R}(w)$ from some u up to v of the form $u = u_0 \to u_1 \to \cdots \to u_p = v$.

There is such a largest integer p since for any such path, we have $p \leq \lfloor l(v)/2 \rfloor$ by Observation 2. For any such longest path, u is easily seen to be minimal.

Exercise 3 Show that if $u \to x$ and $v \to x$ for $u, v, x \in \mathcal{R}(w)$, then there exists $y \in \mathcal{R}(w)$ for which $y \to u$ and $y \to v$. That is, whenever 

(a "peak") is part of a path in $\mathcal{R}(w)$, then it can be replaced with some "valley" 

.

We now make the following observations:

Observation 4 For any $u, v \in \mathcal{R}(w)$, there is some $y \in \mathcal{R}(w)$ such that $y \leq u$ and $y \leq v$. The reason is that for any path from u to v, we may adjust any "peak" to become a "valley" as in Exercise 3. Apply this principle again to the resulting path, and again etc, to obtain a path which has only one valley, which therefore occurs at a lower bound y.

Observation 5 A word $u \in \mathcal{R}(w)$ is reduced if and only if it is minimal. Both directions of this equivalence follow immediately from the definitions.

A sequence of elementary reductions applied to a word $w \in \mathcal{W}_{\mathcal{A}}$ is *longest* if, when the sequence is applied to w, no further elementary reductions can be applied. Putting these pieces together, we have the following theorem.

Theorem *For any $w \in \mathcal{W}_{\mathcal{A}}$, the poset $\mathcal{R}(w)$ has a unique minimal element w_0. This word w_0 is the unique reduced word that is freely equivalent to w. Moreover, any longest sequence of elementary reductions applied to w yields w_0.*

Proof. Existence of some minimal element is guaranteed by Observation 3. If u and u' are both minimal, then use Observation 4 to get $y \leq u'$ and $y \leq u$. Since u' and u are minimal, then $u' = y = u$. So, there is a unique minimal element w_0. By Observation 5, w_0 is the unique reduced word freely equivalent to w. Now any longest sequence applied to w corresponds to a longest path of the form $u = u_0 \to u_1 \to \cdots \to u_p = w$, cf. Observation 3. Then u is minimal, and hence $u = w_0$. □

This theorem resolves the Word Problem for free groups, in that it can be used to conclude when a word w is freely equivalent to the empty word ε: $w \sim \varepsilon$ if and only if ε can be obtained by some sequence of elementary reductions of w if and only if every longest sequence of elementary reductions applied to w produces ε.