THE FREIHEITSSATZ FOR ONE-RELATION MONOIDS

C. SQUIER AND C. WRATHALL

Abstract. We give an elementary proof of the Freiheitssatz for one-relation monoids.

The Freiheitssatz is basic to the study of one-relator groups. It states that for a group $G$ presented by generators $X$ and single (cyclically reduced) defining relator $r$, if $Y \subseteq X$ excludes some generator occurring in $r$ then the subgroup of $G$ generated by $Y$ is freely generated by $Y$. The analogous property is true of one-relation monoids, that is, of Thue systems with a single rule. A proof of this fact by appeal to the Freiheitssatz for groups [4, 5, 3] is possible; it can also be derived from the theorem of Gerstenhaber and Rothaus on solutions of nonsingular sets of equations over residually finite groups [1]. We give here a direct proof, based on a construction used by Levin [2], for which only elementary knowledge of groups and monoids is required.

For an alphabet (set of symbols) $\Sigma$, $\Sigma^*$ denotes the free monoid with generators $\Sigma$, with the identity denoted by $e$.

A Thue system with a single rule is a set $T = \{(u,v)\}$ consisting of a pair of words over an alphabet $\Sigma$. The congruence $\leftrightarrow$ on $\Sigma^*$ associated with such a system $T$ is defined as follows: for any strings $x, y \in \Sigma^*$, define $xuv \leftrightarrow xvy$, and define $\leftrightarrow$ to be the reflexive, symmetric and transitive closure of $\leftrightarrow$. The quotient $\Sigma^*/\leftrightarrow$ of $\Sigma^*$ by the congruence is a monoid, the monoid presented by $(\Sigma|u = v)$.

Theorem. Let $\Sigma$ be an alphabet, $\Gamma$ a subset of $\Sigma$, and $u, v$ strings in $\Sigma^*$. Consider the Thue system $\{(u,v)\}$ with associated congruence $\leftrightarrow$ and monoid $M = \Sigma^*/\leftrightarrow$. If a letter not in $\Gamma$ occurs in $u$ or $v$ then for any $x, y \in \Gamma^*$, $xuv \leftrightarrow xvy$ implies $x = y$. In other words, if $uv \notin \Gamma^*$ then the submonoid of $M$ generated by the congruence classes of $\Gamma$ is freely generated by them.

Proof. If both $u$ and $v$ contain letters not in $\Gamma$, then the rule $u \leftrightarrow v$ does not apply to any word in $\Gamma^*$ and the conclusion of the theorem is clearly true. Suppose, therefore, that $u$, but not $v$, contains letters not in $\Gamma$.

We may assume that $\Gamma$ includes all the letters of $\Sigma$ except one, say $a$. Suppose $u$ has some $n > 0$ occurrences of $a$ and write $u$ as $wau_0 \cdots au_{n-1}$, where $w$ and each $u_i$ are in $\Gamma^*$.

To establish the theorem, it is sufficient to prove that there is a group $G$ and a homomorphism $\phi: M \to G$ that is one-to-one on (the congruence classes of) $\Gamma$ such that $\phi(\Gamma)$ freely generates a free subgroup of $G$. Let $F$ be the free group on $\Gamma$, with...
identity $1_F$. View the rule $u \leftrightarrow v$ as an equation $"a u_0 \cdots u_{n-2} a(u_{n-1} v^{-1} w) = 1"$ to be solved for the variable $a$ over $F$: applying Levin's theorem [2], there is a group $G$ containing $F$ as a subgroup and an element $\bar{a}$ of $G$ such that $\bar{a} u_0 \cdots \bar{a} u_{n-1} v^{-1} w = 1_G$. The homomorphism $\phi$ can then be defined via the inclusion of $\Gamma^*$ in $F$ with $\phi(a) = \bar{a}$, thus completing the proof.

For the Thue system $\{(u, v)\}$, Levin's construction takes the following form. The group $G$ is the wreath product of $F$ with the cyclic group $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$; that is, elements of $G$ are pairs $(k, C)$ with $k \in \mathbb{Z}_n$ and $C: \mathbb{Z}_n \to F$ an arbitrary function; and multiplication is given by $(m, C_1)(k, C_2) = (m + k, C_3)$ where $C_3(i) = C_1(i - k)C_2(i)$, $0 \leq i \leq n - 1$, and the index computation is modulo $n$.

For $x \in \Gamma^*$ define $\hat{x}: \mathbb{Z}_n \to F$ by $\hat{x}(i) = x$, $0 \leq i \leq n - 1$. Let $A(i) = u_i^{-1}$ for $0 \leq i \leq n - 2$ and let $A(n - 1) = w^{-1} v u_{n-1}^{-1}$. Finally, let $h: \Sigma^* \to G$ be the homomorphism determined by defining $h(a) = (-1, A)$ and, for $b \in \Gamma$, $h(b) = (0, \hat{b})$. Note that for $x \in \Gamma^*$, $h(x) = (0, \hat{x})$. (In the case $n = 1$, this reduces to the homomorphism $h: \Sigma^* \to F$ given by $h(a) = w^{-1} v u_0^{-1}$, $h(b) = b$.)

It follows from the definition of $h$ that $h(u) = h(v)$, and therefore for any $x, y \in \Sigma^*$, if $x \leftrightarrow y$ then $h(x) = h(y)$. In particular, if $x, y \in \Gamma^*$ and $x \leftrightarrow y$ then from $h(x) = h(y)$ we conclude that $(0, \hat{x}) = (0, \hat{y})$ and so $x = y$, as desired. □

References


Department of Mathematics, University of California at Santa Barbara, Santa Barbara, California 93106