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 $x, y \in \Gamma^*$, $x \leftrightarrow y$ 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 $\phi: M \rightarrow G$ 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

Received by the editors October 4, 1982 and, in revised form, February 3, 1983.
1980 Mathematics Subject Classification. Primary 20M05.
This research was supported in part by the National Science Foundation under Grant No. MCS81-16327. A preliminary version was presented at the First International Conference for Combinatorics on Words, held at the University of Waterloo, August 1982.

© 1983 American Mathematical Society
0002-9939/83 $1.00 + .25 per page
identity 1_F. View the rule u ↔ v as an equation “au_0 \cdots au_{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 ð of G such that ðau_0 \cdots ðau_{n-1}v^{-1}w = 1_G. The homomorphism φ can then be defined via the inclusion of Γ* in F with φ(a) = ð, 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 Z_n = \{0, 1, \ldots, n - 1\}: that is, elements of G are pairs (k, C) with k ∈ Z_n and C: Z_n → F an arbitrary function; and multiplication is given by (m, C_1) \cdot (k, C_2) = (m + k, C_3) where C_3(i) = C_1(i - k)C_2(i), 0 ≤ i ≤ n - 1, and the index computation is modulo n.

For x ∈ Γ* define ixmap: Z_n → F by ixmap(i) = x, 0 ≤ i ≤ n - 1. Let A(i) = u^{-1} for 0 ≤ i ≤ n - 2 and let A(n - 1) = w^{-1}vu^{-1}. Finally, let h: Γ* → G be the homomorphism determined by defining h(a) = (-1, A) and, for b ∈ Γ, h(b) = (0, b). Note that for x ∈ Γ*, h(x) = (0, ixmap). (In the case n = 1, this reduces to the homomorphism h: Σ* → F given by h(a) = w^{-1}vu^{-1}, h(b) = b.)

It follows from the definition of h that h(u) = h(v), and therefore for any x, y ∈ Γ*, if x ↤ y then h(x) = h(y). In particular, if x, y ∈ Γ* and x ↤ y then from h(x) = h(y) we conclude that (0, ixmap) = (0, ixmap) and so x = y, as desired. □

References


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