THE WORD PROBLEM DISTINGUISHES COUNTER LANGUAGES

SEAN CLEARY, MURRAY ELDER, AND GRETCHEN OSTHEIMER

Abstract. Counter automata are more powerful versions of finite-state automata where addition and subtraction operations are permitted on a set of n integer registers, called counters. We show that the word problem of $\mathbf{Z}^n$ is accepted by a nondeterministic m-counter automaton if and only if $m \geq n$.

1. Introduction

Connections between formal language theory and group theory have been considered by many authors. If H is generated as a group by a finite set X, and if we let $X^{\pm}$ be the set X together with formal inverses, one important language to consider is the *word problem*, which is the set of words over $X^{\pm}$ representing the identity element of H. The formal language classification of the word problem of a group is independent of generating set in the sense that if $\mathcal{F}$ is a family of languages and if X and Y are two finite generating sets for a group H, then the word problem of H with respect to X is in $\mathcal{F}$ if and only if the word problem of H with respect to Y is in $\mathcal{F}$ (see Gilman [3]). Therefore we can refer to the word problem of a group rather than to the word problem of a particular generating set for a group.

It is natural then to ask about the extent to which the algebraic structure of a group H determines the formal language classification of the word problem of H. In 1975 Anisimov and Seifert [1] proved that the word problem of H is a regular language if and only if H is finite, and in 1985 Muller and Schupp [8, 9] proved that the word problem of H is a context-free language if and only if H is virtually free. While the Anisimov and Seifert result can be proven easily from first principles, the Muller and Schupp result relies heavily on a deep result of Stallings concerning one-ended groups [10]. In 1991 Herbst [4] used the Muller and Schupp result to show that the word problem of H is a one-counter language if and only if H is virtually cyclic. Notice

The first author is grateful for the hospitality of the Centre de Recerca Matemàtica.

that it follows from these results that if we restrict our attention to languages which are word problems, nondeterministic automata which are either finite state, pushdown or one-counter are no more powerful than their deterministic counterparts.

In formal language theory there are a variety of ways to generalize the ideas of finite-state, pushdown and one-counter automata. One such way is to consider G-automata, where G is a group. Loosely, if G is a group, a *G-automaton* over a finite alphabet X is an automaton in which each edge is labeled by an ordered pair, the first coordinate of which is an element of G and the second coordinate of which is an element of $X^{\pm}$ or the empty word. A word w over $X^{\pm}$ is *accepted by A* if there is a path from the initial state to a final state for which the second coordinate reads the letters of w and the product of the corresponding first coordinates is the identity element of G. If we take G to be the trivial group, a G-automaton is simply a finite-state automaton, and if we take $G = \mathbf{Z}$, a G-automaton is a one-counter automaton. For $G = \mathbf{Z}^n$, a G-automaton is an n-counter automaton. We show below that the word problem of $\mathbf{Z}^n$ is accepted by a nondeterministic m-counter automaton if and only if $m \geq n$, so larger rank free abelian groups require more counters to accept their word problems. Thus, the natural heirarchy of counter languages coming from the number of counters used does not collapse in the nondeterministic case of word problems of groups.

We note that sometimes counter automata are described as *blind counter automata* (see Mitrana and Stiebe [7]) to emphasize the fact that the counters can not be examined until at an accept state.

A pushdown-automaton is equivalent in power to a G-automaton where G is free [5]. Kambites proved that for groups G and H, $W(H)$ is accepted by a deterministic G automaton if and only if H has a finite index subgroup which embeds in G [6], so in the deterministic case, at least n counters are required to accept the word problem of $\mathbf{Z}^n$. Furthermore, he posed the following question: "For what groups G is it true that deterministic and non-deterministic G-automata accept the same word problems?" Below, Theorem 1 answers that question in the case that G is abelian: deterministic and non-deterministic G-automata accept the same word problems. Our methods are elementary: we rely entirely on basic linear algebra.

2. Notation and definitions

Let G be a group. We define a *G-automaton* over X to be a finite directed graph with a distinguished initial vertex, some distinguished

final vertices, and with edges labeled by $G \times (X^{\pm} \bigcup \{\epsilon\})$ where ϵ is the empty word. We will refer to vertices as *states*. By a *loop* we mean an edge that starts and ends at the same state, and by a *circuit* we mean a path that does so.

A G-automaton over X is said to *accept* a word $w \in X^{\pm *}$ if there is a path p from the initial state to some final state labeled $(1, w)$, where 1 is the identity element of G. In this case p is called an *accepting path*.

If n is a positive integer, a $\mathbf{Z}^n$-automaton is called an *n-counter automaton*. An n-counter language is one that is accepted by an n-counter automaton. If r is a regular expression over $X^{\pm}$, we let $L(r)$ denote the language denoted by r.

3. General Preliminaries

We will need to rely on two general results about languages accepted by G-automata. The first establishes that having an n-counter word problem is a property of a group, rather than of a particular generating set for the group. The proof relies on basic properties of rational transductions as summarized by Gilman [3] and Kambites [5], for example.

Lemma 1. *If G and H are groups, and if X and Y are two finite generating sets for H, then the word problem for H with respect to X is accepted by a G-automaton if and only if the word problem for H with respect to Y is as well.*

Proof. Fix a group G, and let $\mathcal{F}$ be the set of languages which are accepted by some G-automaton. Let W_X be the word problem of H with respect to X, and let W_Y be the word problem of H with respect to Y. Suppose that $W_X \in \mathcal{F}$. Then W_Y is a rational transduction of W_X (see Proposition 2 in [5]). $\mathcal{F}$ forms a family of languages. It follows that $\mathcal{F}$ is closed under rational transduction (see Theorem 6.2 in [3]). Therefore $W_Y \in \mathcal{F}$. □

The second general result establishes that the intersection of a regular language and an n-counter language is itself n-counter. This is Lemma 3 in Elder [2] and an immediate consequence of Theorem 4 in Kambites [5]. Later we will need to refer to specific characteristics of an n-counter automaton that accepts such an intersection. For this reason we include the following lemma and proof:

Lemma 2. *Let X be a finite set. Let L_1 be regular language over X, and let L_2 be a language accepted by a $\mathbf{Z}^n$-automaton over X. Then $L_1 \cap L_2$ is also accepted by a $\mathbf{Z}^n$-automaton over X.*

Proof. Let A_1 be a finite-state automaton accepting L_1. Let A_2 be a $\mathbf{Z}^n$-automaton accepting L_2. We construct a $\mathbf{Z}^n$-automaton B as follows. The set of states of B is $\Sigma_1 \times \Sigma_2$, where Σ_i is the set of states of A_i. A state (σ_1, σ_2) is final if and only if σ_i is final in A_i for $i = 1, 2$. For $x \in X^{\pm}$ and $v \in \mathbf{Z}^n$, there is an edge B from (σ_1, σ_2) to (τ_1, τ_2) labeled (v, x) if and only if there is an edge in A_1 from σ_1 to τ_1 labeled x and there is an edge in A_2 from σ_2 to τ_2 labeled (v, x). Furthermore, there is an edge from (σ_1, σ_2) to (τ_1, τ_2) labeled (v, ϵ) if and only if one of three conditions holds:

- there is an edge in A_1 from σ_1 to τ_1 labeled ϵ, and there is an edge in A_2 from σ_2 to τ_2 labeled (v, ϵ), or
- $v = 0$, $\sigma_2 = \tau_2$ and there is an edge in A_1 from σ_1 to τ_1 labeled ϵ, or
- $\sigma_1 = \tau_1$ and there is an edge in A_2 from σ_2 to τ_2 labeled (v, ϵ).

Words accepted by B are exactly those in $L_1 \cap L_2$: a word w in the intersection can follow a path labeled $(0, w)$ to states (σ_1, σ_2) where σ_i is a final state for A_i; similarly, any word accepted by B can lead to a state (σ_1, σ_2) which is a product of final states via a path labeled $(0, w)$ and would thus be accepted by each of the A_i. □

4. Main Result

To show that we cannot accept the word problem of a free abelian group of rank n with a counter automaton with less than n counters, we proceed via a series of lemmas which allow us to consider automata of a preferred form and to derive later a contradiction from a property somewhat analogous to the ranks of vectorspaces not being less than that of their subspaces.

We let $H = \mathbf{Z}^n$, and suppose that $x_1, x_2, \ldots, x_n$ is a basis for H as a free abelian group. Let $X_1, X_2, \ldots, X_n$ be the formal inverses of the generators. Let $L = W(H) \cap L(x_1^* x_2^* \cdots x_n^* X_1^* X_2^* \cdots X_n^*)$. If $j = (j_1, j_2, \ldots, j_n) \in \mathbf{N}^n$, let $w(j)$ denote the word $x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n}$.

Lemma 3. *Let H and L be as above. Suppose $W(H)$ is m-counter. Then there is an m-counter automaton A accepting L with the following structure:*

- *A has a single final state σ.*
- *A can be described as a collection of $2n$ subautomata $A(x_1), A(x_2), \ldots, A(x_n), A(X_1), A(X_2), \ldots, A(X_n)$ satisfying the following criteria:*
  - *the only edges between the subautomata are labeled (v, ϵ) for some $v \in \mathbf{Z}^m$, and these edges go from $A(x_i)$ to $A(x_{i+1})$*

for $i = 1, 2, \ldots, n-1$, from $A(X_i)$ to $A(X_{i+1})$ for $i = 1, 2, \ldots, n-1$, and from $A(x_n)$ to $A(X_1)$.
- *for all $a = x_i, X_i$, edges in $A(a)$ are labeled (v, ϵ) or (v, a) where $v \in \mathbf{Z}^n$.*

Proof. Let A_1 be a finite-state automaton accepting the regular language $L(x_1^* x_2^* \cdots x_n^* X_1^* X_2^* \cdots X_n^*)$ of the following specific form. There are n states σ_{x_i}, n states σ_{X_i}, and two additional states α, the initial state, and β, the only final state. For $a = x_i, X_i$, the state σ_a has a loop labeled a. For $i = 1, 2, \ldots, n-1$, there are edges labeled ϵ from σ_{x_i} to $\sigma_{x_{i+1}}$ and from σ_{X_i} to $\sigma_{X_{i+1}}$. In addition there are edges labeled ϵ from α to $\sigma_{x_1}$and from σ_{X_n} to β.

Let A_2 be a $\mathbf{Z}^m$-automaton accepting $W(H)$. We may assume without loss of generality that A_2 has a single final state. By Lemma 2, there exists a $\mathbf{Z}^m$-automaton A accepting L. The automaton constructed in the proof of Lemma 2 has all of the desired properties. □

We want to show that $m \geq n$ using linear algebra. The following lemma will allow us to do so. $\mathbf{N}$ denotes the set of positive integers.

Lemma 4. *If $m < n$ then $\mathbf{N}^n$ is not contained in the union of finitely many translates of subspaces of $\mathbf{Q}^n$ each of which has dimension at most m.*

Proof. Suppose that $\mathbf{N}^n$ is contained in the union of $Q_1, Q_2, \ldots, Q_r \subseteq \mathbf{Q}^n$, where each Q_i is a translate of an m-dimensional subspace of $\mathbf{Q}^n$. Let $k = r + 1$. Let $B(k)$ be the set of all points $(x_1, x_2, \ldots, x_n)$ in $\mathbf{N}^n$ such that $x_i \leq k$ for $i = 1, 2, \ldots, n$. There are k^n elements in $B(k)$. Let $B_i = B(k) \cap Q_i$. There are at most k^m elements in B_i. Therefore there at most $rk^m < k^{m+1} \leq k^n$ elements in $B(k)$. We have reached a contradiction. □

Let p and q be accepting paths in an m-counter automaton. We will say that $p < q$ if q can be obtained from p by adding circuits. We will say that p is *minimal* if it is minimal with respect to $<$.

Lemma 5. *Let H and L be as above. Suppose $W(H)$ is m-counter. Let A be an m-counter automaton A accepting L with the structure posited in Lemma 3. There exist accepting paths p, $q_1, q_2, \ldots, q_n$ such that*

- *$p < q_i$ for $i = 1, 2, \ldots, n$;*
- *if $j \in \mathbf{N}^n$ such that $w(j)$ is the word accepted by p, and if $a_i \in \mathbf{N}^n$ such that $w(j + a_i)$ is the word accepted by q_i, then $\{a_1, a_2, \ldots, a_n\}$ is a set of linearly independent vectors in $\mathbf{N}^n$.*

Proof. Let p be an accepting path which is minimal with respect to $<$, and let $w(j)$ be the word that it accepts. Let S_p be the semigroup spanned by all vectors of the form $j' - j$ such that there is a path q accepting $w(j')$ with $q > p$. Consider the subspace V_p of $\mathbf{Q}^n$ spanned S_p. Let $Q_p = j + V_p$.

There are finitely many accepting paths p which are minimal with respect to $<$. Suppose that none of these satisfies the criteria of the lemma. Then each V_p has dimension $n-1$ or smaller. But then $\mathbf{N}^n$ is contained in the union of finitely many translates of subspaces $\mathbf{Q}^n$ which are at most $(n-1)$-dimensional. By Lemma 4 this is not possible. □

Theorem 1. *If the word problem of $\mathbf{Z}^n$ is an m-counter language, then $m \geq n$.*

Proof. Suppose that the word problem of $\mathbf{Z}^n$ with respect to some generating set is an m-counter language, with $m < n$. By Lemma 1 we may assume that our generating set for $\mathbf{Z}^n$ is a free basis $x_1, x_2, \ldots, x_n$. Let $X_1, X_2, \ldots, X_n$ be formal inverses of the generators. Let $L = W(\mathbf{Z}^n) \cap L(x_1^* x_2^* \cdots x_n^* X_1^* X_2^* \cdots X_n^*)$. By Lemma 3 there exists an m-counter automaton A accepting L with the specific structure posited in that lemma.

We can take p, j, q_i, a_i as in Lemma 5. Let s_i be the $\mathbf{Z}^m$ contribution of the loops in q_i that are not in p and which lie in $A(x_1) \cup A(x_2) \cup \cdots \cup A(x_n)$. Let S_i be the $\mathbf{Z}^m$ contribution of the loops in q_i that are not in p and which lie in $A(X_1) \cup A(X_2) \cup \cdots \cup A(X_n)$. Since p and q_i are both accepting, and since q_i is built up from p in the specific way that it is, $s_i + S_i = 0$.

Since any set of n vectors in $\mathbf{Z}^m$ is linearly dependent, then there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{Z}$ not all zero such that $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n = 0$. We construct an accepting path r as follows. We start with p. If α_i is strictly positive, consider those loops of q_i that are not part of p but that do lie in $A(x_1) \cup A(x_2) \cup \cdots \cup A(x_n)$; add α_i times as many traversals of these loops. The $\mathbf{Z}^m$ contribution of these loops is $\alpha_i s_i$. If α_i is strictly negative, do the same thing but this time consider those loops of q_i that are not part of p but that do lie in $A(X_1) \cup A(X_2) \cup \cdots \cup A(X_n)$, and add $-\alpha_i$ times as many traversals of these loops. The $\mathbf{Z}^m$ contribution of these loops is $(-\alpha_i)S_i = \alpha_i s_i$. The path r is accepting since $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n = 0$.

We now reach a contradiction by showing that the word accepted by r does not represent the identity and thus is not in $W(\mathbf{Z}^n)$. Consider the case, for example, when $\alpha_1 < 0$ and $\alpha_2, \alpha_3, \ldots, \alpha_n \geq 0$. Let $u = j + \alpha_2 a_2 + \cdots + \alpha_n a_n$, and let $v = j + (-\alpha_1)a_1$. Then the word w

accepted by r is of the form $x_1^{u_1}x_2^{u_2}\cdots x_n^{u_n}X_1^{v_1}X_2^{v_2}\cdots X_n^{v_n}$, so w is in the word problem only if $u = v$. This is the case if and only if

$$\alpha_2 a_2 + \alpha_3 a_3 + \cdots + \alpha_n a_n \quad = \quad -\alpha_1 a_1$$

This is impossible since $\{a_1, a_2, \ldots, a_n\}$ is linearly independent. All other cases reach a similar contradiction. □

From the classification of finitely-generated abelain groups, we get the immediate corollary, analgous to Kambites Theorem 1 [6] for the group case but in the nondeterministic case:

Corollary 2. *The word problem of finitely-generated abelian group H is recognized by a nondeterministic G-automaton if and only if H has a finite-index subgroup isomorphic to a subgroup of G.*

5. Acknowledgments

We would like to thank Mark Kambites for the relevant background material from semigroup theory and Bob Gilman for suggesting the proof of Lemma 4.

References

[1] A.V. Anisimov and F.D. Seifert. Zur algebraischen charateristik der durch kontext-freie sprachen definierten gruppen. *Elektronische Informationsverarbeitung und Kybernetik*, 11:675–702, 1975.

[2] Murray Elder. A context-free and a 1-counter geodesic language for a Baumslag-Solitar group. *Theoretical Computer Science*, 339:344–371, 2005.

[3] Robert H. Gilman. Formal languages and infinite groups. In Gilbert Baumslag et. al., editor, *Geometric and Computational Perspectives on Infinite Groups*, volume 25 of *DIMACS Series in Discrete Mathematics and Computer Science*, pages 27–51, Providence, RI, 1996. American Mathematical Society.

[4] Thomas Herbst. On subclass of context-free groups. *Theoretical Informatics and Applications*, 25:255–272, 1991.

[5] Mark Kambites. Formal languages and groups as memory.

[6] Mark Kambites. Word problems recognisable by deterministic blind monoid automata.

[7] Victor Mitrana and Ralf Stiebe. The accepting power of finite automata over groups. In *New trends in formal languages*, volume 1218 of *Lecture Notes in Comput. Sci.*, pages 39–48. Springer, Berlin, 1997.

[8] D. Muller and P. Schupp. Groups, the theory of ends and context-free languages. *J. Computer and System Sciences*, 26:295–310, 1983.

[9] D. Muller and P. Schupp. The theory of ends, pushdown automata, and second order logic. *Theoretical Computer Science*, 37:51–75, 1985.

[10] John R. Stallings. On torsion-free groups with infinitely many ends. *Ann. of Math. (2)*, 88:312–334, 1968.

Department of Mathematics, The City College of New York & The CUNY Graduate Center, New York, NY 10031, USA
E-mail address: cleary@sci.ccny.cuny.edu

Department of Mathematics, Stevens Institute of Technology, Hoboken, NJ 07030, USA
E-mail address: murrayelder@gmail.com

Department of Computer Science, Hofstra University, Hempstead NY 11549, USA
E-mail address: gretchen.ostheimer@hofstra.edu