Electronic Colloquium on Computational Complexity, Report No. 40 (2001)

On the Languages Recognized by Nilpotent Groups

Pierre Péladeau Denis Thérien

May 16, 2001

Abstract

We study a model of computation where executing a program on an input corresponds to calculating a product in a finite monoid. We show that in this model, the subsets of $\{0,1\}^n$ that can be recognized by nilpotent groups have exponential cardinality.

Translator's Note: This is a translation of the article "Sur les langages reconnus par des groupes nilpotents," *C. R. Acad. Sci. Paris*, t. 306, Série I, p. 93-95, 1988. It was translated in 1998 with permission from the authors by Alexander and Sarah Russell.

We will consider here a model of computation, recently formalized in [BT87a], that permits the definition of subsets of $\{0,1\}^n$ by performing operations in a finite monoid M.

Let $[n] = \{1,\ldots,n\}$. Elements of $[n] \times M^{\{0,1\}}$ we shall call *instructions*. A *program* (on M) is a finite sequence $P = v_1 \ldots v_l$ of instructions. Such a program defines a function from $\{0,1\}^n$ to M: for all $w_1 \ldots w_n \in \{0,1\}^n$, $P(w) = v_1(w)\cdots v_l(w)$, where $(i,f)(w) = f(w_i)$. We shall say that a subset $L \subseteq \{0,1\}^n$ is *recognizable* by M if there exists a program P and a subset F of M such that $L = P^{-1}(F)$.

This notion of recognition generalizes that of finite automata; it was introduced in connection with the study Boolean circuits and offers a purely algebraic perspective on certain types of circuits of interest to the community. We shall refer the reader to [Coo85] for a detailed description of such circuit problems and to [BT87a] for the relationship between circuits and programs.

In this model there exist monoids which, for all n, can recognize arbitrary subsets of $\{0,1\}^n$. We concern ourselves, then, for a monoid M and a given language $L \subset \{0,1\}^*$, with the optimum length, as a function of n, of a program over M that permits the recognition of $L \cap \{0,1\}$. We know, for example, that the language $\{w : |w|_1 \equiv 0 \bmod p\}$, where $|w|_1$ designates the number of occurrences of 1 in the word w, cannot be recognized by an aperiodic monoid with programs of subexponential length.

One the other hand, there also exist monoids that cannot recognize certain languages at all, regardless of the length of the program. It is shown in [BT87b] that a nilpotent group cannot recognize the subset $\{1^n\}$ for large enough n. We shall sharpen this result, demonstrating the following

Theorem 1. *Let G be a nilpotent group. There exists a constant $c = c(G)$ such that all non-empty subsets of $\{0,1\}^n$ recognized by G are of cardinality at least $2^n/c$.*

It will be convenient to use another description for the languages under study. Let R be a be a commutative, unitary, finite ring and $X = \{x_1,\ldots,x_n\}$ a set of indeterminates: we denote by N the ideal of $R[X]$ generated by the polynomials $x_i - x_i^2$. An element of $R[X]/N$ is therefore a polynomial of the form $r(x_1,\ldots,x_n) = \sum_{I\subset[n]} \lambda_I \left(\prod_{i\in I} x_i\right)$, $\lambda_I \in R$. Any such polynomial determines, in a natural fashion, a function of $\{0,1\}^n$ in R. We will say that $L \subseteq \{0,1\}^n$ is recognizable by r if there exists a subset $S \subset R$ such that $L = r^{-1}(S)$. The theorem follows immediately from the two following lemmata.

Lemma 1. *Let L be a subset of $\{0,1\}^n$ recognized by the nilpotent group G. There exists a finite ring $R = R(G)$ and a polynomial $r \in R[X]/N$ of degree $d = d(G)$ such that L is recognized by r.*

Lemma 2. *Let r be an element of $R[X]/N$ of the degree d. There exists a constant $c = c(R,d)$ such that the cardinality of all nonempty subsets $L \subseteq \{0,1\}^n$ recognized by r is at least $2^n/c$.*

Proof of Lemma 1. Suppose that G is a group of nilpotence class m and exponent q. (That is, the ascending central series of G terminates in m steps.) We consider $P(w)$ as a word in G^*, the free monoid of base G: from [Th´e83], we know that the value of this word in G is determined by the numbers

$$\left\{ \binom{P(w)}{u} \bmod q : u \in G^*, 1 \leq |u| \leq m \right\}$$

where $|u|$ denotes the length of u and $\binom{P(w)}{u}$ represents the number of occurrences of u as a subword of $P(w)$. It is sufficient to establish the existence of a polynomial of degree m, in $(\mathbb{Z}/q\mathbb{Z})[X]/N$, which calculates $\binom{P(w)}{u} \bmod q$, since then the desired parameters can be simultaneously determined by a polynomial of degree m over $(\mathbb{Z}/q\mathbb{Z})^l$, where l is the number of words in G^* of length at most m. Let $|u| = s$: an occurrence of u in $P(w)$ arises from s instructions, thus depends on at most s variables. We denote by F the set of pairs (J,K) of disjoint parts of $[n]$ for which the union has cardinality at most s: let $\lambda_{(J,K)}$ be the number of factorizations of the program P of the form $P = P_0 v_1 P_1 \dots v_s P_s$ such that $v_1 \dots v_s(w) = u$ iff $w_i = 1$ for all $i \in J$ and $w_i = 0$ for all $i \in K$. The desired polynomial is then

$$\sum_{J,K \subset F} \lambda_{J,K} \left(\prod_{j \in J} x_j \right) \left(\prod_{k \in K} (1 - x_k) \right).$$

□

In the proof of the second lemma we shall use the following notations: $\sigma(w)$ will represent $\{i : w_i = 1\}$, and for any subset $J \subset [n]$, $X_J = \{x_j : j \in J\} \subset X$.

Proof of Lemma 2. We suppose that R has cardinality t and characteristic p. The proof proceeds by induction on d.

Base case. Let $r = \lambda_0 + \sum_{i=1}^{n} \lambda_i x_i$ and let a be an element of R in the image of r. We choose w, an element of $r^{-1}(a)$ which minimizes $|w|_1$: we must have $|w|_1 < tp$; otherwise we would have p indices $i_1, \dots, i_p$ in $\sigma(w)$ with $\lambda_{i_1} = \dots = \lambda_{i_p}$, contradicting the choice of w. It remains to be shown that the other variables, of which there can be at most $n - tp$, can be fixed in an exponential number of fashions without changing the value of the polynomial. We are thus brought to study the cardinality of the set $\{w : q(w) = 0\}$ where $q = \sum_{i=0}^{s} \mu_i x_i$ is a polynomial of degree 1 without constant term. For each $a \in R$ we set $I_a = \{i : \mu_i = a\}$, $\psi_a(w) = |\sigma(w) \cap I_a|$ and let n_a be the cardinality of I_a: we can write $q(w) = \sum_{a \in R} a\psi_a(w)$ and we will have $q(w) = 0$ each time $\psi_a(w) = 0 \bmod p$ for all a. The number of solutions to the equation $q(x) = 0$ is therefore at least

$$\prod_{a \in R} \left(\sum_{k=0}^{\frac{n_a}{p}} \binom{n_a}{pk} \right) \geq \prod_{a \in R} \left(\frac{2^{n_a}}{2^p} \right) = \left(\frac{1}{2^p} \right)^t 2^s$$

and we can choose $c(R,1) = 2^{2tp}$.

Inductive case. We now consider $r(x) = \sum \lambda_I \left(\prod_{i \in I} x_i \right)$ where the sum extends over the subsets of $[n]$ of size at most d and we suppose that $r^{-1}(a)$ is nonempty. Then Ramsey's theorem guarantees the existence of a natural number $m = m(p,t,d)$ with the following property: if $n > m$ then there exists a subset $J \subset [n]$ of cardinality $pd!$ such that for $i = 1, \dots, d$ the coefficients associated with the subsets of J of size i all have the same value, which we denote λ_i. It follows that we can find $w \in r^{-1}(a)$ with $|w|_1 \leq m$: in effect, if $|w|_1 > m$, we can find $J \subset \sigma(w)$ with the property defined above. Defining $y \in \{0,1\}^n$ by $y_i \neq w_i$ iff $i \in J$ we have

$$r(y) = r(w) - \sum_{s=1}^{d} \lambda_s \binom{pd!}{s} = r(w).$$

In general, we can therefore find a subset J of size at most tm such that for all a in the image of r there exist w with $\sigma(w) \subset J$ and $r(w) = a$. We rewrite the polynomial r in the form $r(x) = s(x) + u(x) + v(x)$ where $s(x) = \sum_{I \subset J} \lambda_I \left(\prod_{i \in I} x_i \right)$ and $u(x) = \sum_{I \subset [n]-J} \lambda_I \left(\prod_{i \in I} x_i \right)$. The last term $v(x)$ can itself be written as $v(x) = \sum_{I \subset J} \mu_I \left(\prod_{i \in I} x_i \right)$; the coefficients μ_I are then polynomials of degree less than d in the variables $X_{[n]-J}$: this sum consists of $l \leq \sum_{s=1}^{d-1} \binom{tm}{s}$ terms. From the canonical isomorphism $R[X_{[n]-J}]^l \cong R^l[X_{[n]-J}]$ and from the induction hypothesis, we deduce the existence of a constant $c = c(R^l, d-1)$ such that the l polynomials μ_I simultaneously annul themselves for at least $2^{n-tm}/c$ settings of the variables $X_{[n]-J}$. For each of these settings the variables X_J can be fixed in a way to obtain any element of the image of r. Each of these values is thus obtained for at least $2^n/(c2^{tn})$ settings of variables X. □

This restriction on the computational capacity characterizes the nilpotent groups since all others can recognize arbitrary languages.

References

[BT87a] David Barrington and Denis Th´erien. Finite monoids and the fine structure of NC^1. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 101–109, New York City, 25–27 May 1987.

[BT87b] David A. Mix Barrington and Denis Th´erien. Non-uniform automata over groups. In *Proceedings of the Fourteenth Annual International Conference on Automata, Languages, and Programming*, 1987.

[Coo85] Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64(1-3):2–22, 1985.

[Th´e83] Denis Th´erien. Subword counting and nilpotent groups. In *Combinatorics on words (Waterloo, Ont., 1982)*, pages 297–305. Academic Press, Toronto, Ont., 1983.