TWO MEMORY BOUNDS FOR THE RECOGNITION OF PRIMES BY AUTOMATA

J. Hartmanis
H. Shank

Technical Report
No. 68-21

June 1968

Department of Computer Science
Cornell University
Ithaca, New York 14850

I. INTRODUCTION.

It was shown [1] by using the Prime Number Theorem that the set of binary representations of primes, P , cannot be recognized by a finite automaton and the question was raised whether the set of primes could be recognized by a push-down automaton. Shortly afterwards it was shown [2], [3] by elementary means that no infinite set of primes can be recognized by a finite automaton or a push-down automaton. It was shown furthermore [3] that the set of primes can be recognized by an automaton whose memory grows linearly with the length of the input sequence (i.e. a linearly bounded automaton) and it was conjectured that this is the least amount of memory with which the set of primes can be recognized.

In this paper we show that the memory of a two-way automaton which recognizes the set of primes has to grow at least logarithmically with the length of the input sequence. This rate of growth is, unfortunately, still far from that originally conjectured.

The second result of this paper is that for an automaton with a one-way input tape the memory for the recognition of primes has to grow linearly and that this amount is also sufficient. In terms of the states of the automaton, after reading any two different input sequences (not representing even numbers) the automaton has to be in different states and therefore the number of states of any one-way prime recognizer has to grow exponentially with the length of the input sequence.

II. PRELIMINARIES.

We are considering Turing machines with a read-only input tape and read-write working tape [3]. At the start of the computation a binary input string is written (between end markers) on the read-only input tape. We distinguish two models:

a) the one-way automaton can move the reading head on its input tape only in one direction,

b) the two-way automaton can move the reading head on its input tape in either direction.

Thus the one-way automaton can scan the input sequence only once, whereas the two-way automaton can scan it many times. Clearly for any recognition process the two-way automaton cannot require more working tape than the one-way automaton and the two models require the same amount of tape for all recognition processes which use on the two-way automaton at least as much tape as is required to write down the input sequence.

We say that a set A of binary sequences, $A \subseteq (0 + 1)^*$, is accepted or recognized by a one-way (two-way) automaton M if and only if M halts for every input $w \in (0 + 1)^*$ and accepts w if it is in A and rejects w if it is not in A by entering an accepting or rejecting state, respectively. We write

$$\mathcal{T}(M) = A .$$

We say that a one-way (two-way) automaton M accepts the set A with $L(n)$-tape if and only if $\mathcal{T}(M) = A$ and M processes every input of length n using no more than $L(n)$ tape squares of its working tape.

It should be noted that the actual organization of the automaton's memory in the form of a tape is not essential for our results and proofs. The results and proofs can easily be transcribed for any automaton in which we can count the total number of different "states" or "configurations", $S(n)$, entered while processing input sequences of length n. In all our results $L(n)$ and $S(n)$ are logarithmically related.

Finally, some comments about notation. $(0 + 1)^*$ denotes the set of all finite length binary sequences. If $w \in 1(0 + 1)^*$ then $\underline{w}$ denotes the integer represented by w. The length of w, $w \in (0 + 1)^*$, is denoted by $\ell(w)$ and w^k denotes the sequence obtained by concatenating w k-times. For integers p and q $k=(p,q)$ denotes the greatest common divisor of p and q thus $(p,q) = 1$ if and only if p and q are relatively prime. $\pi(n)$ denotes the number of primes not larger than n.

III. MEMORY BOUNDS FOR TWO-WAY AUTOMATA.

In this section we recall two results from [3] and show how these results in conjunction with a result about the distribution of primes yields a lower memory bound for two-way automata which recognize the set of primes.

The following result was derived in [3] using Fermat's theorem.

Lemma 1. If $p = \underline{w_1\ w_2\ w_3}$ is a prime larger than two and

$$2^{\ell(w_2)} \not\equiv 1 \text{ (modulo } \underline{w_1\ w_2\ w_3}\text{)}$$

then

$$\underline{w_1\ w_2^p\ w_3} \equiv 0 \text{ (modulo } \underline{w_1\ w_2\ w_3}\text{)} .$$

Thus when we repeat a subsequence in the representation of a prime p we are guaranteed to obtain the representation of a number divisible by p. This result immediately showed that the set of primes cannot be recognized by a finite automaton and a slight extension of this result showed that it cannot be recognized by a push-down automaton [3]. This result can also be used to show [3] that with slowly growing memory an automaton cannot accept primes which contain sequences of zeros whose length is proportional to the length of their representations. Stated more precisely:

Lemma 2. Let M be a two-way automaton which works on $L(n)$ tape such that

$$\lim_{n\to\infty} \frac{L(n)}{\log n} = 0 .$$

If there exists $\delta > 0$ such that $\mathcal{T}(M)$ contains an infinite subset of the set

$$R_\delta = \{1\ 0^t\ w \mid w \in (0 + 1)^*,\ t > \delta \cdot \ell(w),\ t = 1,2,\ldots\}$$

then $\mathcal{T}(M)$ is not a subset of the set of primes.

Proof. Assume that $\mathcal{T}(M)$ contains an infinite subset of the set R_δ for some $\delta > 0$. Since

$$\lim_{n\to\infty} \frac{L(n)}{\log n} = 0 ,$$

there exists t such that

$$10^t w \in \mathcal{T}(M) , \quad t > \delta \cdot \ell(w) ,$$

and every time M scans the sequence of t-zeros it must repeat its total state (for details see proof of Theorem 4 in [3]). This guarantees that M will also accept certain sequences in which we have inserted additional zeros, namely

$$10^{t+t!k} w \in \mathcal{T}(M) , \quad k = 0,1,2,\ldots .$$

An application of Lemma 1 now implies that if p is a prime larger than two,

$$p = \underline{10^{t+kt!+t!}w} \quad \text{and} \quad 2^{t!} \not\equiv 1 (\text{mod } p)$$

then

$$\underline{10^{t+(k+p)t!}w} \equiv 0 (\text{mod } p) .$$

Thus $\mathcal{T}(M)$ is not a subset of the set of primes, as was to be shown.

Next, using a refinement by Ingham [4] of a result of Hocheisel we show that there exist infinitely many primes with long sequences of zeros in their representations.

Theorem [Ingham]. For small $\varepsilon > 0$ and $\theta = \frac{43}{77}$

$$\pi(n + n^{\theta+\varepsilon}) - \pi(n) \sim \frac{n^{\theta+\varepsilon}}{\log n} .$$

Lemma 3. There are infintely many primes of the form $\underline{10^t w}$, with $w \in (0 + 1)^*$ and $t > \frac{1}{2} \ell(w)$.

Proof. It follows from Ingham's Theorem (since $\frac{43}{77} < \frac{2}{3}$) that for all sufficiently large t there exist primes p_t such that

$$\underline{10^{3t}} < p_t < \underline{10^{3t}} + \underline{10^{2t}}$$

Thus $p_t = \underline{10^t w}$, $t > \frac{1}{2} \ell(w)$, which completes the proof.

Theorem 1. If M works on $L(n)$ tape and recognizes the set of primes then

$$\sup_{n \to \infty} \frac{L(n)}{\log n} > 0 .$$

Proof. By previous lemma we conclude that for $\delta = \frac{1}{2}$ there are infinitely many primes with representations in

$$R_{1/2} = \{1 0^t w \mid 2t > \ell(w) \ , \quad t = 1,2 \ldots\} \ .$$

But then we know that

$$\lim_{n\to\infty} \frac{L(n)}{\log n} \neq 0$$

and therefore

$$\sup_{n\to\infty} \frac{L(n)}{\log n} > 0 \ ,$$

as was to be shown.

It is interesting to recall that $L(n) = \log n$ is the least amount of tape on which the set of primes can be recognized without making several number theoretic conjectures false [3]. Furthermore, it still seems unlikely that $L(n) = \log n$ is sufficient to recognize the set of primes on a two-way device and it would be interesting to find the exact amount of tape required for this recognition. In the next section we find the exact amount of memory required for the recognition of the set of primes on a one-way device.

IV. MEMORY REQUIREMENTS FOR ONE-WAY AUTOMATA.

We consider now one-way automata whose inputs are binary sequences

$$w = x_n x_{n-1} \cdots x_1 x_0$$

and the sequence is read from right to left. Thus

$$\underline{v} = \sum_{0}^{n} 2^i x_i$$

and M is reading the least significant digits first.

We know [3] that with $L(n) = n$ a one-way automaton can recognize the set of primes and we will show that this amount of tape is also necessary.

If A is any set of binary sequences. $A \subseteq (0 + 1)^*$, define an equivalence relation on $(0 + 1)^*$ as follows. $w_1 \equiv w_2$ if and only if for all $\beta \in (0 + 1)^*$

$$\beta w_1 \in A \iff \beta w_2 \in A .$$

Let $E_A(n)$ denote the number of different equivalence classes defined by the above relation on

$$\{w | w \in (0 + 1)^* , \ell(w) \leq n\}$$

Next, by a simple application of Dirichlet's theorem (if $(s,t) = 1$ then there are infinitely many primes of the form $s + kt$, $k = 1,2 \ldots$) we show that for the set of primes $E_p(n) \geq 2^{n-1}$. This yields another proof that P is not a regular set and, since for any $A \subseteq (0 + 1)^*$ $n \leq E_A(n) \leq 2^n$, we see that P is a very complicated set in this measure.

Lemma 4. Let $\alpha \neq \beta$ and α, β in $(0.+1)^* 1$. Then there exists a γ in $1(0+1)^*$ such that $\underline{\gamma\alpha}$ is a prime and $\underline{\gamma\beta}$ is not a prime. Thus for the set of primes $E_p(n) \geq 2^{n-1}$.

Proof. First, we show that for an arbitrary α in $(0+1)^* 1$ the number $\underline{\gamma\alpha}$ is infinitely often a prime, γ in $1(0+1)^*$. Clearly

$$\underline{\gamma\alpha} = \underline{\alpha} + \underline{\gamma}\, 2^{\ell(\alpha)}$$

and $(\underline{\alpha}, 2^{\ell(\alpha)}) = 1$. Therefore by Dirichlet's theorem we conclude that $\underline{\gamma\alpha}$ is infinitely often a prime. Let γ_0 be fixed such that $\underline{\gamma_0\alpha}$ is a prime. If $\underline{\gamma_0\beta}$ is not a prime then the statement is true. Thus we assume that $\underline{\gamma_0\beta} = q$ is a prime.

Consider now γ_n such that

$$\gamma_n = b_{nq}\,\gamma_0 \text{ , with } \underline{b_{nq}} = nq,\ n = 1, 2, \ldots .$$

Then

$$\underline{\gamma_n\alpha} = \underline{b_{nq}\gamma_0\alpha} = \underline{\gamma_0\alpha} + 2^{\ell(\gamma_0\alpha)}\ \underline{b_{nq}} = p + (q\cdot 2^{\ell(\gamma_0\alpha)})n$$

and, since $(p,\ q\cdot 2^{\ell(\gamma_0\alpha)}) = 1$, by Dirichlet's theorem $\underline{\gamma_n\alpha}$ is infinitely often a prime. On the other hand

$$\underline{\gamma_n\beta} = \underline{\gamma_0\beta} + 2^{\ell(\gamma_0\beta)}\ \underline{b_{nq}} = q + (q\cdot 2^{\ell(\gamma_0\beta)})\, n$$

is always a multiple of q and we conclude that there exists a γ_i such that $\underline{\gamma_i \alpha}$ is a prime and $\underline{\gamma_i \beta}$ is not a prime. Thus $E_p(n) \geq 2^{n-1}$, as was to be shown.

From this result we obtain our last theorem.

Theorem 2. If a one-way automaton M recognizes the set of primes with $L(n)$-tape then $L(n) > cn$ for some positive c; and for any $c > 0$ there is an M which recognizes the set of primes with tape bound $L(n) = cn$.

Proof. The above result implies that M must have at least 2^{n-1} different total states and this implies that for large n

$$L(n) > c_1 \cdot \log 2^{n-1} = c_1(n-1) > cn, \quad c > 0.$$

Since P can be recognized with $L(n) = n$ by using more tape symbols per tape square we can recognize P on $L(n) = cn$ for any given $c > 0$.

Acknowledgement

The authors gratefully acknowledge the help of Professor J. B. Rosser who pointed out the applicability of Ingham's result.

1. E. Minsky and S. Papert, Unrecognizable sets of numbers, J. ACM 13 (1966), 281-286.

2. M. P. Schützengerger, A remark on acceptable sets of numbers. J. ACM 15 (1968), 300-303.

3. J. Hartmanis and H. Shank, On the recognition of primes by automata, J. ACM 15 (1968) ____.

4. A. E. Ingham, On the difference between consecutive primes, The Quarterly J. of Math. (Oxford Series) 7 (1936) 255-266.