MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

Artificial Intelligence
Memo. No. 73

MAC-M-192-2
November 1964

Unrecognizable Sets of Numbers

Marvin Minsky

and

Seymour Papert

1

Unrecognizable Sets of Numbers

MARVIN MINSKY AND SEYMOUR PAPERT*

Massachusetts Institute of Technology, Cambridge, Massachusetts†

Abstract. When is a set A of positive integers, represented as binary numbers, "regular" in the sense that it is a set of sequences that can be recognized by a finite-state machine? Let $\pi_A(n)$ be the number of members of A less than the integer n. It is shown that the asymptotic behavior of $\pi_A(n)$ is subject to severe restraints if A is regular. These constraints are violated by many important natural numerical sets whose distribution functions can be calculated, at least asymptotically. These include the set P of prime numbers for which $\pi_P(n) \sim n/\log n$ for large n, the set of integers $A(k)$ of the form n^k for which $\pi_{A(k)}(n) \sim n^{1/k}$, and many others. The technique cannot, however, yield a decision procedure for regularity since for every infinite regular set A there is a nonregular set A' for which $|\pi_A(n) - \pi_{A'}(n)| \leq 1$, so that the asymptotic behaviors of the two distribution functions are essentially identical.

1. *Introduction*

Let A be some set of positive integers written in binary notation. It is natural to ask what kind of computing machine could *recognize* [1] the set in the sense of deciding whether a given binary sequence represents a number belonging to A. The technique described in this note enables one to show that certain sets cannot be recognized by finite state automata (i.e., these sets are not "regular" [2]). The essential idea is this: Let $\pi_A(n)$ be the number of members of A less than the integer n. It is shown that the asymptotic behavior of $\pi_A(n)$ is subject to severe restraints if A is regular. These constraints are violated by many important natural numerical sets whose distribution functions can be calculated, at least asymptotically. These include the set P of prime numbers, for which $\pi_P(n) \sim n/\log n$ for large n, the set of integers $A(k)$ of the form n^k, for which $\pi_{A(k)}(n) \sim n^{1/k}$, and many others. The technique cannot, however, yield a decision procedure for regularity, since for every infinite regular set A there is a nonregular set A' for which $|\pi_A(n) - \pi_{A'}(n)| \leq 1$, so that the asymptotic behaviors of the two distribution functions are essentially identical.

We consider here only the binary representation, so as to avoid pompous statements, but the same results can be obtained for any radix by changing all 2's to r's in the sequel. We warn readers not to confuse the statement that the primes written in binary form are not a regular set with the trivial statement that the set of strings of prime length is not regular.

2. *Notation*

(1) Consider the set of strings of 0's and 1's of which the first symbol is a 1, i.e., $N = 1(0 \vee 1)^*$, using Kleene's notation [2].

(2) Such strings are regarded ambiguously as integers to the base 2 or as strings of 0's and 1's. Numbers are presented to the machine high digits first. (This convention is innocuous since the set of reversed strings of a regular set is regular.)

* Added in proof: The authors have learned that Alan Cobham obtained substantially the same results at about the same time.

† Both of Department of Electrical Engineering and Project MAC.

(3) For any integer x, $L(x)$ is the number of digits in x, i.e., $2^{L(x)-1} \leq x < 2^{L(x)}$.

(4) Define $x \cdot y = 2^{L(y)}x + y$; that is, "$\cdot$" is concatenation.

(5) A always denotes a set of positive integers and $\pi_A(n)$ the cardinality of $A \cap \{x \mid 1 \leq x \leq n\}$.

(6) If A is regular, let M_A denote the reduced (i.e., minimal) automaton which recognizes A. In the discussion of any particular automaton M, Q is used for its set of states, q_0 for its initial state, Q_F for its set of "final states" (whose occurrence signifies acceptance of a string), and $\delta(q, x)$ for the state-transition function, i.e., the sequence x drives the automaton from state q to the state $\delta(q, x)$.

(7) A *dead state* is a state q such that $\delta(q, x) \in Q_F$ is satisfied by no x. (If the automaton is reduced this is equivalent to saying $\delta(q, x) = q$ for all x, since there is only dead state in a minimal machine.)

(8) We are interested in subsets of $N = 1(0 \vee 1)^*$ rather than in subsets of $(0 \vee 1)^*$. We consider as trivial the part of the automaton which merely verifies that the input sequence begins with a 1. We shall depart from the assumption of minimality by allowing a special dead state into which the machine is driven by an initial zero. In the sequel, "dead state" means dead state other than this special one.

(9) For convenience the following convention is adopted: For any set A, and any *real* number x, $\pi_A(x) = \pi_A([x])$, where $[x]$ is the integral part of x. Where $\pi_A(n)$ is a "natural" function, such as $n/\log n$, $x/\log x$ will be used as an approximation of $[x]/\log [x]$ for very large values of x.

3. *Theorems*

First, the consequences of M having dead states will be shown.

PROPOSITION 1. *Let $M = M_A$ and suppose:*

(a) *$\delta(q_0 \cdot \alpha)$ is a dead state,*

(b) $\lambda_0 = \dfrac{\alpha + 1}{\alpha}$, *and*

(c) $\lim\limits_{n \to \infty} \dfrac{\pi_A(n)}{\pi_A(\lambda_0 n)} = \theta$.

Then $\theta = 1$.

PROOF. Put $n_m = 2^m\alpha$. Then $\lambda_0 n_m = 2^m(\alpha + 1)$. By assumption (a), there is no β such that $\alpha \cdot \beta \in A$. In other words, no matter what m is chosen, there is no $n \in A$ such that

$$n_m = 2^m\alpha \leq n < 2^m\alpha + 2^m = \lambda_0 n_m ,$$

where $m = L(\beta)$.

Then $\pi_A(n_m)/\pi_A(\lambda_0 n_m) = 1$, because there are no members of A between n_m and $\lambda_0 n_m$. But $\{\pi_A(n_m)/\pi_A(\lambda_0 n_m)\}$ is an infinite subsequence of the sequence, supposed by assumption (c) to be convergent, $\{\pi_A(n)/\pi_A(\lambda_0 n)\}$. It follows that the limit, θ, of this sequence (if the limit exists) is 1.

The underlying fact, then, is that dead states produce large gaps in the sequence of numbers recognized by a machine. Below, it is shown that if there is no dead state, the gaps cannot grow in the same manner.

We immediately deduce the weakened, but easier-to-use:

PROPOSITION 2. *If $(\pi_A(n)/\pi_A(\lambda n)) \to \theta(\lambda)$ for all real λ and if $\theta(\lambda) = 1$ only if $\lambda = 1$, then A cannot be a regular set whose reduced automaton has a dead state.*

In some interesting cases (see below), $\pi(n)/\pi(\lambda n)$ fails to converge. We can still sometimes use a sharper but less elegant criterion:

PROPOSITION 3. *Let a_r be the rth member of A in order of magnitude. Then if*

$$\lim_{r\to\infty} \frac{a_{r+1} - a_r}{a_r} = 0,$$

A cannot be a regular set whose reduced automaton has a dead state.

PROOF. Suppose that A is a regular set whose reduced automaton has a dead state, and let α, λ_0, and n_m be defined as in the proof of Proposition 1. Denote by k_m the number of members of A smaller than n_m, i.e., k_m is the largest integer such that $a_{k_m} < n_m$. Since no member of A can lie between n_m and $\lambda_0 n_m$, we have:

$$a_{k_m+1} \geq \lambda_0 n_m .$$

Thus

$$\frac{a_{k_m+1} - a_{k_m}}{a_{k_m}} \geq \frac{\lambda_0 n_m - n_m}{n_m} = \lambda_0 - 1 = \frac{1}{\alpha} .$$

It follows that $(a_{r+1} - a_r)/a_r$ cannot converge to 0 as $r \to \infty$.

Finally, we look at the other side of the coin; what happens if M has no dead state?

PROPOSITION 4. *If A is regular and M_A has no dead state, then $\pi_A(n)/n \geq 2^{-2N}$, where N is the number of states of M_A. Thus the density of A cannot converge to zero.*

PROOF. For each integer t we shall define a 1-1 into map g:

$$g: \quad [2^{Nt}, 2^{N(t+1)}) \to [2^{Nt}, 2^{N(t+N)}) \cap A,$$

where $[a, b)$ denotes the interval $a \leq x < b$.

For any $\alpha \in [2^{Nt}, 2^{N(t+1)})$, let β be the smallest integer for which $\alpha\cdot\beta \in A$. Such a β must exist because $\delta(q_0, \alpha)$ is not dead. Moreover, $\beta < 2^N$ because the shortest path from $\delta(q_0, \alpha)$ to a member of Q_F cannot be longer than $N-1$. It follows that $\alpha\cdot\beta < 2^{N(t+N)}$ so that $\alpha\cdot\beta \in [2^{Nt}, 2^{N(t+N)}) \cap A$. Thus if we define $g(\alpha) = \alpha\cdot\min[\beta \mid \alpha\cdot\beta \in A]$, g has the required range. To see that it is 1-1, we simply note that α is recoverable as the first Nt digits of $g(\alpha)$.

It follows that $[2^{Nt}, 2^{N(t+N)}) \cap A$ contains at least as many members as $[2^{Nt}, 2^{N(t+1)})$. Therefore, $\pi_A(2^{N(t+N)}) \geq 2^{N(t+1)} - 2^{Nt} = 2^{Nt}$. Now consider an arbitrary number n. For some t, $n \in [2^{Nt}, 2^{N(t+1)})$, and since $\pi_A(x)$ increases monotonically,

$$\frac{\pi_A(n)}{n} \geq \frac{\pi_A(2^{Nt})}{2^{N(t+1)}} \geq \frac{2^{N(t-1)}}{2^{N(t+1)}} = 2^{-2N}.$$

Combining this result with the consequences of Propositions 2 and 3 leads to the following Criterion.

CRITERION. *To prove that a set, A, is not regular, it is sufficient to verify Condition 1 and Condition 2 or 2'.*

Condition 1. $\pi_A(n)/n \to 0$ as $n \to \infty$.

Condition 2. $\pi_A(n)/\pi_A(\lambda n) \to \theta(\lambda)$ as $n \to \infty$, and $\theta(\lambda) \neq 1$ for all $\lambda \neq 1$.

Condition 2'. $(a_{n+1} - a_n)/a_n \to 0$ as $n \to \infty$.

If A is regular, by Proposition 1 it has a dead state but by Proposition 2 or 3 it has none.

4. *Applications*

First, some examples are discussed that can be settled using the Criterion of Section 3.

Example 1. $A = \{m^k \mid k \text{ a fixed integer}\}$. Clearly $\pi_A(n) \approx n^{1/k}$ so that:

(1) $\pi_A(n)/n \to n^{1/k-1} \to 0$ as $n \to \infty$,

(2) $\pi_A(n)/\pi_A(\lambda n) \to \lambda^{-1/k} \neq 1$ for all $\lambda \neq 1$.

Therefore A is not regular.[1]

Example 2. Let P be the set of prime numbers. It is well known that $\pi_P(n) \approx n/\log n$. Thus $\pi_P(n)/n \approx 1/\log n \to 0$ as $n \to \infty$, satisfying Condition 1. On the other hand,

$$\frac{\pi_P(n)}{\pi_P(\lambda n)} \approx \frac{n \log \lambda n}{\lambda n \log n} = \frac{(\log \lambda + \log n)}{\lambda \log n} \to \frac{1}{\lambda} \neq 1 \qquad (\text{for } \lambda \neq 1).$$

Again, Conditions 1 and 2 are satisfied; therefore, P is not regular.

Example 3. Let B be the set of all prime powers, i.e., $B = \{p^m \mid p \text{ prime}, m \text{ an integer}\}$. Write B as:

$$B = B_1 \cup B_2 \cup \cdots \cup B_k \cup \cdots, \quad \text{where } B_k = \{p^k \mid p \text{ prime}\}.$$

Then for each k we have, exactly, $\pi_{B_k}(n) = \pi_P(n^{1/k})$.

To compute $\pi_B(n)$, first note that if $n_0 \in B$, $n_0 < n$; then for exactly one k and p, $n_0 = p^k < n$, so that:

$$k < \log_p, \quad n \leq \log_2 n, \quad \text{i.e.,} \quad n_0 \in B_1 \cup \cdots \cup B_{[\log_2 n]}.$$

It follows that

$$\pi_B(n) = \pi_{B_1}(n) + \cdots + \pi_{B_{[\log_2 n]}}(n) = \pi_P(n) + \pi_P(n^{\frac{1}{2}}) + \cdots + \pi_P{}^{1/[\log_2 n]}.$$

Thus

$$\pi_B(n) \approx \frac{n}{\log_e n} + \frac{2n^{\frac{1}{2}}}{\log_e n} + \cdots + \frac{[\log_2 n]n^{1/[\log_2 n]}}{\log_e n}.$$

Since

$$2n^{\frac{1}{2}} + \cdots + [\log_2 n]n^{1/[\log_2 n]} < 2(\log_2 n)^2 n^{\frac{1}{2}},$$

and

$$\frac{(\log_2 n)^2 n^{\frac{1}{2}}}{\log_e n} \to 0 \quad \text{as} \quad n \to \infty,$$

we have

$$\pi_B(n) \approx n/\log_e n \approx \pi_P(n).$$

Thus the set B has the same asymptotic density as P and is not regular. A similar argument shows that the set $\{n^m \mid n, m \text{ integers}, \quad m \geq 2\}$ is not regular.

Example 4. We now illustrate the use of the Criterion in cases where the ratio $\pi_A(n)/\pi_A(\lambda n)$ fails to converge. Let C be the set of binary palindromes, i.e., sequences invariant under reversal. To show that C is not regular, first verify that Condition 1 is satisfied. This is easy; since the first half of the binary digits of an n-digit palindromic number is determined by the last half, neglecting the small odd-

[1] This application includes the result proved by Ritchie [3] by *ad hoc* arguments on the set of perfect squares in binary.

even effects, then $\pi_C(n)/n \sim (\sqrt{n})/n \to 0$. Then, by Proposition 1, if C is regular it must be recognized by an automaton with a dead state. But this is impossible since every sequence can be completed to produce a palindrome of twice its length. Q.E.D. One could, although it would be foolish to do so in this case, come to the same conclusion by using Condition 2′. To do so, estimate the difference $a_{n+1} - a_n$ between the nth palindrome and the next. If a_n is of even length, $2k$, it can be written $a_n = b_n 2^k + \bar{b}_n$, where $\bar{b}_n$ is the sequence of digits of b_n written in reverse order. If a_n is of odd length, $2k+1$, it has the form $a_n = b_n 2^{k+1} + \delta 2^k + \bar{b}_n$, where δ is 0 or 1. It is easy to see that b_{n+1} is either b_n or b_n+1, so that in each case $a_{n+1} - a_n$ cannot be larger than the order of $\sqrt{a_n}$. It follows that $(a_{n+1} - a_n)/a_n \to 0$ as $n \to \infty$.

It is interesting to compare this with the (regular) set of sequences of doublets, i.e., sequences like 00110011110011. This set has roughly the same sort of global distribution as the palindromes; but the fine structure of its distribution of gaps causes it (rightly) to elude the Criterion.

The following examples show how the Criterion can fail to yield useful information.

Example 5. Let $A(a)$ be the set of all powers of some fixed integer a, i.e., $A(a) = \{a^k \mid a \text{ fixed}\}$. Then $\log_a(n) - 1 \leq \pi_A(n) < \log_a(n)$ so that $\pi_A(n) \sim \log_a(n)$. Condition 1 is satisfied.

However, $\pi_A(n)/\pi_A(\lambda n) \to \log_a n/\log_a \lambda n \to 1$ as $n \to \infty$, so Condition 2 fails, and so does Condition 2′: $(a_{n+1} - a_n)/a_n = a - 1$. The Criterion gives no information in this case. In fact $A(2)$ is regular (for a binary machine), while $A(3)$ is not (and vice versa for a ternary machine).

Example 6. Periodic sequences such as {101, 101101, 101101101, ⋯} have $\pi(n) \sim k \log n$ so that

$$\frac{\pi(n)}{\pi(\lambda n)} \to 1.$$

Condition 1 fails. (All such sets are regular.)

5. *Impossibility of a Converse*

Let A be any infinite regular set with an infinite complement and let $\phi(x)$ be a noncomputable function with values 0 and 1. Let A' be the subset of A defined by $x \in A'$ if $x \in A$ and $(x+1) \notin A$. A' is infinite. Let $g(n)$ be an enumeration of A', without repetitions, and define A'' by the conditions:

(1) If $x \in (A - A')$, $x \in A''$.

(2) If $x = g(n) \in A'$, then put x in A'' if $\phi(n) = 0$; otherwise put $x+1$ in A''.

It is clear that A'' is not computable, and a fortiori not regular; otherwise $\phi(n)$ could be computed by observing a machine that recognizes A'', since $\phi(n) = 0$ if and only if $g(n) \in A''$. But $\pi_A(n)$ and $\pi_{A'}(n)$ differ by, at the most, 1. Thus, while tests based on asymptotic density can give evidence against regularity, they cannot give evidence for regularity.

6. *Upper Bound of Growth Rate of Regular Sets*

For the sake of completeness, the following more superficial result is included.

PROPOSITION 5. *If A is regular and infinite, there is some $K > 0$ such that $\pi_A(n) > K \log n$.*

PROOF. Suppose A is regular and that M_A has N states. Let N_0 be any integer. Then there is some $x \in A$ with $N_0 \leq L(x) \leq N_0 + N$. To see this, note first that if $\delta(q_0, y)$ were dead for every y with $L(y) = N_0$, then A would be finite. So we can choose a y with $L(y) = N_0$ and for which $y \cdot y_1 \infty A$ for some y_1. But if y_1 is chosen to produce the shortest path from $\delta(q_0, y)$ to $\delta(q_0, y \cdot y_1)$, then $L(y_1) < N$. Thus $x = y \cdot y_1$ is in the stated range.

It follows that there is at least one member of A in each of the intervals $(1, 2^N)$, $(2^N, 2^{2N}) \cdots (2^{kN}, 2^{(k+1)N}) \cdots$. Therefore, $\pi_A(2^{tN}) \geq t$, and hence, $\pi_A(n) \geq (\log n)/N = K \log n$.

Example 7. It follows from Proposition 5 that sets such as $A = \{2^{t^2}\}$, which increase "faster than exponentially," cannot be regular.

7. *Discussion*

Many questions remain. To what extent will the same kind of methods work on, say, pushdown machines? The criteria will have to change in detail (for example, the palindromes would be recognizable now), but we are inclined to suppose that the pushdown machines will also fail to recognize the arithmetically interesting examples, and that the gap and density arguments can be refined to show this. We are curious as to whether one can show that $\{w \mid n \text{ is prime}\}$ is not regular by much more elementary means. If not, this might suggest some nontrivial relation between automata theory and number-theoretical areas, such as the theory of rational approximations.

RECEIVED DECEMBER, 1965

REFERENCES

1. RABIN, M., AND SCOTT, D. Finite automata and their decision problems. *IBM J. Res. Develop.* **3** (1959), 114–125.
2. KLEENE, S. C. Representation of events in nerve nets and finite automata. In *Automata Studies*, Shannon, C. E., and McCarthy, J. (Eds.), Princeton U. Press, Princeton, N. J., 1956, pp. 3–41.
3. RITCHIE, R. W. Finite automata and the set of squares. *J. ACM 10*, 4 (Oct. 1963), 528–531.