PROBABILISTIC TURING MACHINES AND COMPUTABILITY

EUGENE S. SANTOS

I. **Introduction.** (Deterministic) Turing machines, named after A. M. Turing [5], have been used to characterize a class of numerical functions—(deterministically) computable functions [2]. In the present paper, a more general machine will be defined which corresponds to probabilistic Turing machine. With this will come a mathematical characterization of a class of random functions—computable random functions—and another class of numerical functions—probabilistically computable functions. It turns out that the latter contains the (deterministically) computable functions as proper subclass.

II. **Probabilistic Turing machines.**

DEFINITION. A probabilistic Turing machine (PTM) may be defined through the specification of two finite nonempty sets U and S, $U \cap S = \varnothing$ (empty set), and a function p from $S \times U \times V \times S$ into $[0, 1]$ where $V = U \cup \{R, L, T\}$ and $R \notin U$, $L \notin U$, $T \notin U$. The function p satisfies the following conditions:

(i) $\sum_{v \in V} \sum_{s' \in S} p(s, u, v, s') = 1$ for every $s \in S$ and $u \in U$;

(ii) for every $u \in U$, $p(s, u, T, s') = 0$ if $s \neq s'$.

The set U is the set of symbols which the PTM is capable of printing and the set S is the set of internal states. The symbols R, L and T represent, respectively, a move of one square to the right, a move of one square to the left, and the machine stops (terminates). The function p is the conditional probability of the "next act" of the machine given that the machine is at state s and scanning a square on which appears the symbol u.

A (deterministic) Turing machine is a PTM in which the range of p consists of only two numbers, namely, 0 and 1. Note that in this case, p is completely determined by the set

$$C_p = \{(s, u, v, s') : p(s, u, v, s') = 1 \text{ and } v \neq T\}.$$

DEFINITION. Let $Z = (U, S, p)$ be a PTM. An expression α of Z is a finite sequence (possibly empty) of symbols chosen from $U \cup S$. α is an instantaneous expression of Z iff (if and only if) it contains exactly one $s \in S$ and s is not the rightmost symbol. α is a tape expression iff it consists entirely of symbols from U. If α is an instantaneous ex-

Received by the editors July 25, 1968.

pression of Z which contains $s \in S$ and u is the symbol immediately to the right of s, then we call s the state of Z at α and u the symbol scanned by Z at α. The tape expression obtained by removing s from α is called the expression on the tape of Z at α.

DEFINITION. Let $Z = (U, S, p)$ be a PTM. For every instantaneous expression α and β of Z, define

$$\begin{aligned}
q_Z(\alpha, \beta) &= p(s, u, u', s') && \text{if } \alpha = \gamma s u \delta, && \beta = \gamma s' u' \delta, && u' \in U,\\
&= p(s, u, R, s') && \text{if } \alpha = \gamma s u u' \delta, && \beta = \gamma u s' u' \delta, && u' \in U\\
& && \text{or } \alpha = \gamma s u, && \beta = \gamma u s' u_0,\\
&= p(s, u, L, s') && \text{if } \alpha = \gamma u' s u \delta, && \beta = \gamma s' u' u \delta, && u' \in U\\
& && \text{or } \alpha = s u \delta, && \beta = s' u_0 u \delta,\\
&= 0 && \text{otherwise,}
\end{aligned}$$

where γ and δ are (possibly empty) tape expressions of Z and the symbol $u_0 \in U$ stands for B, i.e., blank.

The $q_Z(\alpha, \beta)$ given above is the probability that the "next" instantaneous expression of Z will be β given that Z "starts" with instantaneous expression α. The function $q_Z(\alpha, \beta)$ may be extended to $q^{(n)}(\alpha, \beta)$, $n = 0, 1, 2, \cdots$, as follows:

$$\begin{aligned}
q_Z^{(0)}(\alpha, \beta) &= 1 && \text{if } \alpha = \beta,\\
&= 0 && \text{if } \alpha \neq \beta,\\
q_Z^{(n)}(\alpha, \beta) &= \sum_{\gamma} q_Z^{(n-1)}(\alpha, \gamma) q_Z(\gamma, \beta),
\end{aligned}$$

where the summation ranges over all instantaneous expression γ. $q_Z^{(n)}(\alpha, \beta)$ may be interpreted as the probability that the instantaneous expression of Z will be β "after n steps" given that Z "starts" with instantaneous expression α.

By induction, it can be shown that for every instantaneous expression α and nonnegative integer n,

$$\sum_{\beta} q_Z^{(n)}(\alpha, \beta) \leqq 1.$$

From the above definitions, it is clear that a PTM behaves like a stochastic sequential machine as defined in [1] or a stochastic sequential-like machine as defined in [4]. Moreover, it is interesting to note that a Markov chain may be associated with each PTM where the states are the instantaneous expressions and an additional absorbing state corresponding to the termination of the machine.

DEFINITION. Let $Z=(U, S, p)$ be a PTM. For every instantaneous expression α and β of Z, and for every $n=1, 2, \cdots$, define

$$t_Z^{(n)}(\alpha, \beta) = p(s, u, T, s)q_Z^{(n-1)}(\alpha, \beta)$$

where s is the state of Z at β and u is the symbol scanned by Z at β. Moreover, define

$$t_Z(\alpha, \beta) = \sum_{n=1}^{\infty} t_Z^{(n)}(\alpha, \beta);$$

$t_Z^{(n)}(\alpha, \beta)$ may be interpreted as the probability that after n steps, Z will terminate with instantaneous expression β, given that Z starts with instantaneous expression α. The interpretation of $t_Z(\alpha, \beta)$ is obvious.

That the series defining $t_Z(\alpha, \beta)$ converges follows from the fact that for every instantaneous expression α and positive integer n,

$$\sum_{\beta}\left[q_Z^{(n)}(\alpha, \beta) + \sum_{k=1}^{n} t_Z^{(k)}(\alpha, \beta)\right] = 1.$$

III. **Computable random functions.** In order to have PTM perform numerical computations, it is necessary that a suitable representation for numbers be introduced. In the present paper, we shall adopt the representation used in [2].

We assume that U always contains the two symbols B and 1. If n is a positive integer, u^n will denote the expression $u\ u \cdots u$ (n times) that consists of n occurrences of u. For completeness sake, we take u^0 to be the null expression. With each nonnegative integer n, we associate the tape expression $\bar{n}$ where $\bar{n}=1^{n+1}$ and with each k-tuple $(n_1, n_2, \cdots, n_k)$ of nonnegative integers, we associate the tape expression

$$\overline{(n_1, n_2, \cdots, n_k)} \quad \text{where} \quad \overline{(n_1, n_2, \cdots, n_k)} = \bar{n}_1 B \bar{n}_2 B \cdots B \bar{n}_k.$$

If α is an expression, then $\langle\alpha\rangle$ will denote the number of occurrences of 1 in α. Note that

$$\langle\overline{m-1}\rangle = m \quad \text{and} \quad \langle\alpha\beta\rangle = \langle\alpha\rangle + \langle\beta\rangle.$$

DEFINITION. A k-ary random function ϕ is a function from E^{k+1}, the collection of all $(k+1)$-tuples of nonnegative integers, into $[0, 1]$ satisfying

$$\sum_{m=0}^{\infty} \phi\ (m_1, m_2, \cdots, m_k, m) \leqq 1$$

for every k-tuple $(m_1, m_2, \cdots, m_k)$.

DEFINITION. Let $Z=(U, S, p)$ be a PTM. Then, for each positive integer k, we associate a k-ary random function $\Phi_Z^{(k)}$ as follows.

$$\Phi_Z^{(k)}(m_1, m_2, \cdots, m_k, m) = \sum_{\langle\beta\rangle=m} t_Z(\alpha, \beta)$$

where

$$\alpha = s_1\overline{(m_1, m_2, \cdots, m_k)}, \qquad s_1 \in S$$

and the summation ranges over all instantaneous expression β of Z such that $\langle\beta\rangle=m$.

The s_1 in the above definition plays the role of the initial state in a stochastic sequential-like machine. If, however, instead of an initial state, the initial distribution h is given, then we define

$$\Phi_Z^{(k)}(m_1, m_2, \cdots, m_k, m) = \sum_{\langle\beta\rangle=m} \sum_{i=1}^{|S|} h(s_i) t_Z(\alpha_i, \beta)$$

where

$$\alpha_i = s_i\overline{(m_1, m_2, \cdots, m_k)}, \qquad s_i \in S$$

and $|S|$ is the cardinality of S.

That $\Phi_Z^{(k)}$ is a k-ary random function follows immediately from the definition of $t_Z(\alpha, \beta)$.

DEFINITION. A k-ary random function ϕ is computable iff $\phi=\Phi_Z^{(k)}$ for some PTM Z.

Given a random function, one may associate numerical functions with it in various ways. A particular way will be introduced below.

DEFINITION. A k-ary function f is a mapping from a subset D_f of E^k into E^1.

DEFINITION. Let f be a k-ary function, ϕ a k-ary random function and $\lambda\in[0, 1)$. f is said to be generated by ϕ with threshold λ iff

(i) for every $(m_1, m_2, \cdots, m_k)\notin D_f$, $\phi(m_1, m_2, \cdots, m_k, m)\leqq\lambda$ for all m, and

(ii) for every $(m_1, m_2, \cdots, m_k)\in D_f$, if $f(m_1, m_2, \cdots, m_k)=m$, then

$$\phi(m_1, m_2, \cdots, m_k, m) = \sup\{\phi(m_1, m_2, \cdots, m_k, m'): m' = 0, 1, 2, \cdots\} > \lambda.$$

Let $C(\phi, \lambda)$ be the collection of all k-ary functions which are generated by ϕ with threshold λ. Since

$$\sum_{m=0}^{\infty} \phi(m_1, m_2, \cdots, m_k, m) \leqq 1,$$

therefore $\sup \{\phi(m_1, m_2, \cdots, m_k, m): m = 0, 1, 2, \cdots\}$ is attained. Thus $C(\phi, \lambda) \neq \varnothing$. Moreover, if $\lambda \geqq \frac{1}{2}$, then $C(\phi, \lambda)$ contains only one element, i.e., the k-ary function generated by ϕ with threshold $\lambda \geqq \frac{1}{2}$ is unique.

DEFINITION. A k-ary function f is a probabilistically computable function (PCF) with threshold λ iff there exists a PTM Z such that f is generated by $\Phi_Z^{(k)}$ with threshold λ.

It follows from the above remark that every PTM gives rise to at least one k-ary function which is a PCF with threshold λ where k and λ are arbitrary.

In the above definition, if Z is a deterministic Turing machine, then we say that f is a deterministically computable function (DCF).

DEFINITION. A k-ary function f is a PCF iff f is a PCF with threshold λ for some $\lambda \in [0, 1]$.

It is apparent that PTM may also be used to characterize a class of random word functions. The procedure is similar to that given in [6].

IV. **PCF versus DCF.** In this section, we shall show that the class of PCF is nondenumerable. Since it is well known that the class of DCF is denumerably infinite, it will follow immediately that the class of DCF is a proper subclass of the class of PCF.

DEFINITION. Let $Z = (U, S, p)$ be a PTM where

$$S = \{s_1, s_2, s_3, \cdots, s_k\}$$

and n a positive integer. By $Z^{(n)}$ we shall mean the PTM obtained from Z by replacing each $s_i \in S$ by s_{n+i}.

DEFINITION. Let $Z_1 = (U_1, S_1, p_1)$ and $Z_2 = (U_2, S_2, p_2)$ be PTM such $S_1 \cap S_2 = \{\bar{s}\}$. By $Z_1 \to Z_2$ we shall mean the PTM (U, S, p) where $U = U_1 \cup U_2$, $S = S_1 \cup S_2$ and

$$\begin{aligned}
p(s, u, v, s') &= p_1(s, u, v, s') && \text{if } s, s' \in S_1, \quad u \in U_1, \quad v \in V_1 \text{ and } s \neq \bar{s},\\
&= p_2(s, u, v, s') && \text{if } s, s' \in S_2, \quad u \in U_2, \quad v \in V_2,\\
&= 1 && \text{if } s = s' \in S_1, \quad u \notin U_1, \quad v = T\\
& && \text{or } s = s' \in S_2, \quad u \notin U_2, \quad v = T,\\
&= 0 && \text{otherwise.}
\end{aligned}$$

In the rest of the section, we shall replace B by 0.

Let $R=(U, S, p)$ be a (deterministic) Turing machine where

$$U = \{0, 1, a, b, c\}, \qquad S = \{s_1, s_2, \cdots, s_{13}\}$$

and C_p consists of

$$\begin{array}{llll}
(s_1, 1, R, s_1), & (s_1, 0, b, s_1), & (s_1, b, L, s_2), & (s_2, 1, 0, s_2), \\
(s_2, 0, L, s_3), & (s_3, 1, c, s_4), & (s_4, c, R, s_5), & (s_5, 0, R, s_5), \\
(s_5, 1, R, s_5), & (s_5, b, L, s_6), & (s_6, 0, 1, s_7), & (s_7, 1, L, s_7), \\
(s_7, 0, L, s_7), & (s_7, c, 0, s_8), & (s_8, 0, L, s_3), & (s_6, 1, 0, s_9), \\
(s_9, 0, L, s_{10}), & (s_{10}, 0, 1, s_7), & (s_{10}, 1, 0, s_9), & (s_3, 0, R, s_{11}), \\
(s_{11}, 0, R, s_{11}), & (s_{11}, 1, L, s_{12}), & (s_{12}, 0, a, s_{13}). &
\end{array}$$

It is easy to verify that for every $\alpha = s_1\bar{m}$, $t_R(\alpha, \beta) = 1$ implies $\beta = as_{13}\gamma b$ where γ is the binary expansion of m.

Let $Q=(U, S, p)$ be a PTM where $U=\{0, 1, a, b\}$, $S=\{s_1, s_2\}$ and

$$\begin{array}{ll}
p(s_1, 0, R, s_1) = 1 & p(s_1, 1, R, s_1) = 1/2 \\
p(s_1, 0, R, s_2) = 0 & p(s_1, 1, R, s_2) = 1/2 \\
p(s_2, 0, R, s_1) = 1/2 & p(s_2, 1, R, s_1) = 0 \\
p(s_2, 0, R, s_2) = 1/2 & p(s_2, 1, R, s_2) = 1 \\
p(s_1, a, R, s_1) = 1 & p(s_2, a, T, s_2) = 1 \\
p(s_1, b, b, s_1) = 1 & p(s_2, b, T, s_2) = 1 \\
p(s, u, v, s') = 0 \quad \text{otherwise.} &
\end{array}$$

LEMMA 1. *For every $\alpha = as_1\gamma b$ where*

$$\gamma = i_1 i_2 \cdots i_n, \qquad i_k \in \{0, 1\}, \qquad k = 1, 2, \cdots, n,$$

$$t_Q(\alpha, \beta) = 0 \quad \text{if } \beta \neq as_2\gamma b \quad \text{and} \quad t_Q(\alpha, \beta) = .i_n \cdots i_2 i_1$$

which is written in binary expansion if $\beta = as_2\gamma b$.

PROOF. Let P_0 and P_1 be the matrices given below:

$$P_0 = \begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \end{pmatrix} \qquad P_1 = \begin{pmatrix} 1/2 & 1/2 \\ 0 & 1 \end{pmatrix}$$

It is well known that if

$$P_{i_1}P_{i_2}\cdots P_{i_n} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, \qquad i_k \in \{0, 1\}, \qquad k = 1, 2, \cdots, n,$$

then $q = .i_n \cdots i_2 i_1$ where q is written in binary expansion. The conclusion follows immediately from this property of P_0 and P_1.

Let $i_1 i_2 \cdots i_n$ be the binary expansion of m, we shall denote by $b(m)$ the number $.i_n \cdots i_2 i_1$ written in binary expansion and by $g(m)$ the number of occurrences of 1 in $i_1 i_2 \cdots i_n$. From the above constructions, it follows that

LEMMA 2. *Let* $Z = R \to Q^{(12)}$ *then*

$$\Phi_Z^{(1)}(m_1, m) = b(m_1) \quad \text{if } m = g(m_1)$$
$$= 0 \quad \text{otherwise.}$$

LEMMA 3. *Let* $Z = R \to Q^{(12)}$ *and* $\lambda \in [0, 1)$. *Then there is a unique* 1*-ary function* f_λ *which is generated by* $\Phi_Z^{(1)}$ *with threshold* λ. *Moreover,*

$$f_\lambda(m) = g(m) \quad \text{if } b(m) > \lambda$$
$$= \text{undefined} \quad \text{if } b(m) \leqq \lambda.$$

THEOREM. $f_{\lambda_1} = f_{\lambda_2}$ *iff* $\lambda_1 = \lambda_2$.

PROOF. Let $D(\lambda)$ be the domain of definition of f_λ. If $\lambda_1 < \lambda_2$, then, by Lemma 3, $D(\lambda_1) \supseteq D(\lambda_2)$. Since $b(m)$ is dense in $[0, 1)$, there exists an m_0 such that $\lambda_1 < b(m_0) < \lambda_2$. Again by Lemma 3, $m_0 \in D(\lambda_1)$ but $m_0 \notin D(\lambda_2)$. Thus $f_{\lambda_1} \neq f_{\lambda_2}$.

COROLLARY. *The class of all PCF is nondenumerable.*

The matrices P_0 and P_1 were used by Rabin [3] to show that the set of tapes acceptable by probabilistic automata is nondenumerable.

REFERENCES

1. J. W. Carlyle, *Reduced forms for stochastic sequential machines*, J. Math. Anal. Appl. **7** (1963), 167–175.

2. M. Davis, *Computability and unsolvability*, McGraw-Hill, New York, 1958.

3. M. O. Rabin, *Probabilistic automata*, Information and Control **6** (1963), 230–245.

4. E. S. Santos, *Maximin sequential-like machines and chains*, Math. Systems Theory (to appear).

5. A. M. Turing, *On computable numbers, with an application to the entscheidungs problem*, Proc. London Math. Soc. Ser. 2 **42** (1936), 230–265.

6. V. Vuckovic, *Basic theorems on Turing algorithms*, Publ. Inst. Math. (NS), 1 (15) (1961), 31–65.

YOUNGSTOWN STATE UNIVERSITY