KYBERNETIKA – VOLUME 19 (1983), NUMBER 1

ON REPRESENTABILITY OF P. MARTIN-LÖF TESTS

CRISTIAN CALUDE, ION CHIŢESCU

The tests of P. Martin-Löf [4] constitute themselves as an alternative to the A. N. Kolmogorov theory of complexity [2]. But these theories are not equivalent. In the present paper we investigate the possibility of expressing the P. Martin-Löf tests in terms of Kolmogorov complexity. We show that this can be done by adding an element to the primary alphabet. This "enlarging" procedure generates a series of other problems (for instance, new P. Martin-Löf tests appear, which are not Kolmogorov expressible).

1. BASIC NOTIONS

Throughout the paper N will be the set of all natural numbers, i.e. $N = \{0, 1, 2, \ldots\}$. If A is a finite set, card (A) will be the number of elements in A.

For every non-empty sets A and B and for every function $f : A' \to B$ (where $A' \subset A$) we shall write $f : A \xrightarrow{\circ} B$. We shall say that f is a *partial function* from A to B. We consider that $f(x) = \infty$ in case f is not defined in the point x.

Let $X = \{a_1, a_2, \ldots, a_p\}$, $p \geqq 2$ be a finite alphabet. Denote by X^* the free monoid generated by X under concatenation, i.e. X^* consists of all strings $x = x_1 x_2 \ldots x_m$, where the x_i's belong to X, and also the null string λ belongs to X^*. For every a in X and every natural $n > 0$, $a^n = aa \ldots a$ (n copies of a). For every x in X^*, $l(x)$ is the length of x, i.e. $l(x) = m$ in case $x = x_1 x_2 \ldots x_m$ and $l(\lambda) = 0$. For Recursive Function Theory see [3] and [5]. We shall consider *partial recursive functions* (*p.r. functions* in the sequel)

$$\varphi : X^* \times N \xrightarrow{\circ} X^* \quad \text{or} \quad g : N - \{0\} \xrightarrow{\circ} X^* \times N .$$

For every p.r. function $\varphi : X^* \times N \xrightarrow{\circ} X^*$, the *Kolmogorov complexity* induced by φ is a function $K_\varphi : X^* \times N \to N \cup \{\infty\}$, defined by $K_\varphi(x \mid m) = \min \{l(y) \mid y \in X^*, \varphi(y, m) = x\}$ in case $x = \varphi(y, m)$ for some y in X^* and $K_\varphi(x \mid m) = \infty$, otherwise.

For every $W \subset X^* \times (N - \{0\})$ and for every natural $m \geqq 1$ we shall write $W_m = \{x \in X^* \mid (x, m) \in W\}$. A non-empty recursively enumerable set $V \subset X^* \times (N - \{0\})$ will be called *Martin-Löf test* (*M–L test*) if it possesses the following two properties:

1) For every natural $m \geqq 1$, $V_{m+1} \subset V_m$,
2) For every natural numbers $m, n, m \geqq 1$,

$$\text{card}\,\{x \in X^* \mid l(x) = n,\, x \in V_m\} < p^{n-m}/(p - 1)\,.$$

We agree upon the fact that the *empty set* is a $M-L$ test.

The *critical level induced by a $M-L$ test V* is the function $m_V : X^* \to N$, given by $m_V(x) = \max\{m \geqq 1 \mid x \in V_m\}$ in case such m exists, and $m_V(x) = 0$, in the opposite case.

2. RESULTS

We recall the main example of $M-L$ test used in [1]. Let $\varphi : X^* \times N \xrightarrow{\circ} X^*$ a p.r. function. Then the set

$$V(\varphi) = \{(x, m) \mid x \in X^*, m \in N - \{0\}, K_\varphi(x \mid l(x)) < l(x) - m\}$$

is a $M - L$ test (see Example 10 from [1]). Note that $(x, m) \in V(\varphi)$ iff there exists y in X^* with $l(y) < l(x) - m$ and $\varphi(y, l(x)) = x$. This example suggests the following

Definition 1. Let $V \subset X^* \times N$ be a $M-L$ test. We say that V is *representable* if there exists a p.r. function $\varphi : X^* \times N \xrightarrow{\circ} X^*$ such that $V = V(\varphi)$.

Example 2. (Not all $M - L$ test are representable).

Take $p = 2$, $X = \{0, 1\}$. The set $V = \{(000,1), (010,1), (111,1)\}$ is a $M-L$ test. *We claim that V is not representable.* Indeed, in case there exists a p.r. function $\varphi : X^* \times N \xrightarrow{\circ} X^*$ such that $V = V(\varphi)$ we can infer the existence of three strings y_0, y_1, y_2 in X^* with $l(y_i) \leqq 1$, and $\varphi(y_0, 3) = 000$, $\varphi(y_1, 3) = 010$ and $\varphi(y_2, 3) = 111$. It follows that $\{y_0, y_1, y_2\} = \{\lambda, 0, 1\}$.

For instance, we choose $\varphi(\lambda, 3) = 000$ (and $\varphi(0, 3) = 010$, $\varphi(1, 3) = 111$). For this φ we must have $(000, 2) \in V(\varphi)$, because $l(\lambda) = 0 < l(000) - 2 = 3 - 2 = 1$. This shows that $(000, 2) \in V(\varphi) - V$, which is a contradiction. □

In order to avoid this situation we shall "enlarge" the alphabet X by adding a single new element a_{p+1} (distinct from $a_1, a_2, \ldots, a_p$) obtaining the new alphabet $Y = \{a_1, a_2, \ldots, a_p, a_{p+1}\}$.

In this case, every $M-L$ test $V \subset X^* \times N$ can be viewed as a $M-L$ test $V \subset Y^* \times N$. We shall see that all such $M - L$ tests are representable and in fact the function $\varphi : Y^* \times N \xrightarrow{\circ} Y^*$ which represents V (i.e. $V = V(\varphi)$) takes values in X^*. To be more precise, we have the following

Theorem 3. Let $X = \{a_1, a_2, \ldots, a_p\}$ and $Y = X \cup \{a_{p+1}\}$ as before. For every $M - L$ test $V \subset X^* \times N$ there exists a p.r. function $\varphi : Y^* \times N \xrightarrow{\circ} Y^*$ such that $V = V(\varphi)$ and $(\varphi(Y^* \times N)) - \{\infty\} \subset X^*$.

Proof. First, we order Y as follows: $a_1 < a_2 < \ldots < a_p < a_{p+1}$. This order induces the lexicographical order on Y^* as follows:

$$\lambda < a_1 < a_2 < \ldots < a_p < a_{p+1} < a_1a_1 < a_1a_2 < \ldots$$

$$\ldots < a_1a_{p+1} < a_2a_1 < a_2a_2 < \ldots < a_{p+1}a_{p+1} < a_1a_1a_1 < \ldots$$

Only the non trivial case $V \neq \emptyset$ will be considered.

We shall construct a p.r. function $\varphi : Y^* \times N \xrightarrow{\circ} Y^*$ having the property $K_\varphi(x \mid l(x)) = l(x) - m_V(x) - 1$ for every x in X^*, such that $(x, 1) \in V$.

We distinguish two cases: a) V is *infinite* and in this case there exists an injective recursive function $g : N - \{0\} \to X^* \times N$, such that $g(N - \{0\}) = V$ (see [5]); b) V is *finite* and in this case there exists a (p.r.) injective function $g : \{1, 2, \ldots, q\} \to X^* \times N$, such that $g(\{1, 2, \ldots, q\}) = V$ (we write card $(V) = q$). Namely we write for i in the domain of g the value $g(i) = (x_i, m_i)$.

The action of φ will be described in the sequel by the following procedure. Let $g(1) = (x_1, m_1)$ and

$$\varphi(a_{p+1}^{l(x_1)-m_1-1}, l(x_1)) = x_1 .$$

Let $g(2) = (x_2, m_2)$. Two possibilities can occur: either $(l(x_2), m_2) \neq (l(x_1), m_1)$, or $(l(x_2), m_2) = (l(x_1), m_1)$. In case $(l(x_2), m_2) \neq (l(x_1), m_1)$, put

$$\varphi(a_{p+1}^{l(x_2)-m_2-1}, l(x_2)) = x_2 .$$

In case $(l(x_2), m_2) = (l(x_1), m_1)$, put

$$\varphi(a_{p+1}^{l(x_2)-m_2-2}a_p, l(x_2)) = x_2 .$$

The construction is possible because

$$2 \leqq \text{card}\,\{x \in X^* \mid l(x) = l(x_2), (x, m_2) \in V\} < p^{l(x_2)-m_2}/(p-1) ,$$

which shows that $l(x_2) - m_2 \geqq 2$.

In general, at step i let $g(i) = (x_i, m_i)$. In case $(l(x_i), m_i) \neq (l(x_j), m_j)$ for all $j = 1, 2, \ldots, i - 1$ put

$$\varphi(a_{p+1}^{l(x_i)-m_i-1}, l(x_i)) = x_i .$$

In the opposite case let

$$1 \leqq k = \text{card}\,\{j \in N \mid j < i \text{ and } (l(x_j), m_j) = (l(x_i), m_i)\} \leqq$$
$$\leqq [(p^{l(x_i)-m_i} - 1)/(p-1)] - 1 ,$$

because V is a $M-L$ test. The elements $y \in Y^*$ with $l(y) = l(x_i) - m_i - 1$ are (in lexicographical order):

$$y_1, y_2, \ldots, y_r \quad \text{where} \quad r = (p + 1)^{l(x_i) - m_i - 1} .$$

Put $\varphi(y_{r-k}, l(x_i)) = x_i$. The construction is possible because

$$r = (p + 1)^{l(x_i) - m_i - 1} > [(p^{l(x_i) - m_i} - 1)/(p - 1)] - 1 \geqq k .$$

It is seen that φ acts as a function.

Notice that in case V is finite and card $(V) = q$, then the procedure stops at step q. In case V is infinite, the procedure continues indefinitely.

To be more precise, we shall describe the domain of φ. To this aim, we partition the range of g according to the following rule (equivalence): $g(i) = (x_i, m_i)$ is equivalent to $g(j) = (x_j, m_j)$ iff $(l(x_i), m_i) = (l(x_j), m_j)$. The equivalence class of (x_i, m_i) contains at most h elements, where $h = (p^{n-m} - 1)/(p - 1)$, $n = l(x_i)$ and $m = m_i$. So, the range V of g is the union $\bigcup_{j=1}^{\infty} E_j$ of equivalence classes E_j (in case V is infinite) or is a finite union $\bigcup_{j=1}^{u} E_j$ (in case V is finite). For every equivalence class E_j which contains t elements we consider the set C_j consisting of the last t strings of length $l(x) - m - 1$; here E_j is the class of (x, m). Put then $B_j = \{(y, l(x)) \mid y \in C_j\}$ for the above pair (x, m). The domain of φ is $B = \bigcup_{j=1}^{\infty} B_j$ (in case V is infinite) or $B = \bigcup_{j=1}^{u} B_j$ (in case V is finite). We got the domain of the *function* φ which is now a p.r. function.

Take x in X^* such that $(x, 1) \in V$, so $m_V(x) > 0$. There exists unique $i > 0$ such that $g(i) = (x, m_V(x))$. According to the procedure, there exists y in Y^* with $l(y) = l(x) - m_V(x) - 1$ such that $\varphi(y, l(x)) = x$, which shows that $K_\varphi(x \mid l(x)) \leqq l(x) - m_V(x) - 1$. On the other hand, the equality $\varphi(y', l(x')) = x$ implies $x' = x$ and $l(y') = l(x) - m_j - 1$, where $g(j) = (x, m_j)$. This can be done for some $m_j \leqq m_V(x)$, which implies $l(y') \geqq l(x) - m_V(x) - 1$, showing that $K_\varphi(x \mid l(x)) \geqq l(x) - m_V(x) - 1$. We have proved that $K_\varphi(x \mid l(x)) = l(x) - m_V(x) - 1$.

The last equality proves the inclusion $V \subset V(\varphi)$.

To prove the converse inclusion $V(\varphi) \subset V$ we notice first that $(x, m) \in V(\varphi)$ implies that $(x, 1) \in V$ (see the construction of φ).

Now we take $(x, m) \in V(\varphi)$ and we prove that $m \leqq m_V(x)$ (i.e. $(x, m) \in V$). Supposing that $m > m_V(x)$, we get $(x, m_V(x) + 1) \in V(\varphi)$, which yields the existence of y in Y^* such that $l(y) < l(x) - m_V(x) - 1$ and $\varphi(y, l(x)) = x$. This contradicts the above mentioned property of φ, namely: for $(x, 1) \in V$, we have $K_\varphi(x \mid l(x)) = l(x) - m_V(x) - 1$. □

We conclude with some more examples and a small discussion pertaining the previous facts.

Actually, Example 2 can be generalized:

Example 4. (For every alphabet X with $p \geqq 2$ elements there exists a finite $M-L$ test V and an infinite $M-L$ test W, which are both non-representable).

a) Let $p \geqq 2$ and put $k = (p^p - 1)/(p - 1)$. We can consider k different strings $y_1, y_2, \dots, y_k$ in X^*, with length $l(y_i) = p + 1$. The finite $M-L$ test $V = \{(y_i, 1) \mid i = 1, 2, \dots, k\}$ is not representable.

Indeed, in case V would be representable, we could find the (different) strings $z_1, z_2, \dots, z_k$ in X^* having all length $l(z_i) < p + 1 - 1 = p$ and such that $\varphi(z_i, p + 1) = y_i$, for $i = 1, 2, \dots, k$. Because $p^{p-1} < k$, at least one of the strings z_i, say z_t, must have length $\leqq p - 2$. So $\varphi(z_t, p + 1) = y_t$ and $l(z_t) \leqq p - 2 < < l(y_t) - 2$. This shows that $(y_t, 2) \in V(\varphi)$, contradicting the fact that $(y_t, 2) \notin V$.

b) Put $W = V \cup \{(a_1^i, 1) \mid i = p + 2, p + 3, \dots\}$, where V was defined at a).

The infinite $M-L$ test W is not representable (see the proof of point a)). □

Example 5. (For every alphabet X with p elements and every alphabet $Y \supset X$ with $p + 1$ elements there exists a p.r. function $\varphi : Y^* \times N \xrightarrow{\circ} X^*$ such that the $M-L$ test $V(\varphi)$ over $Y^* \times N$ is not a $M-L$ test over $X^* \times N$).

Let $X = \{a_1, a_2, \dots, a_p\}$ and $Y = \{a_1, a_2, \dots, a_p, a_{p+1}\}$. We order X lexicographically according to the order $a_1 < a_2 < \dots < a_p$ and we order Y lexicographically according to the order $a_1 < a_2 < \dots < a_p < a_{p+1}$ (see the construction in the proof of Theorem 3).

Let $A = \{y \in Y^* \mid l(y) < p\} = \{y_1, y_2, \dots, y_t\}$ in lexicographical order. It is seen that $t = 1 + (p + 1) + (p + 1)^2 + \dots + (p + 1)^{p-1} = ((p + 1)^p - 1)/p$. Let $B = = \{x \in X^* \mid l(x) = p + 1\} = \{z_1, z_2, \dots, z_s\}$ in lexicographical order. It is seen that $s = p^{p+1} > t$.

The domain of φ is the set $D = \{(y_i, p + 1) \mid i = 1, 2, \dots, t\}$. We define $\varphi : D \to \to X^*$ by $\varphi(y_i, p + 1) = z_i$.

It is clear that $V(\varphi)$ is a $M-L$ test over $Y^* \times N$. On the other hand, it is clear that $V(\varphi) \subset X^* \times N$. But, computing card $\{x \in X^* \mid l(x) = p + 1, (x, 1) \in V(\varphi)\}$ we obtain the result $t > (p^p - 1)/(p - 1)$. This shows that $V(\varphi)$ is not a $M-L$ test over $X^* \times N$. □

Remarks.

1. We can interpret the result stated in Theorem 3 as follows:

a) The theories of A. N. Kolmogorov [2] (complexity) and P. Martin - Löf [4] (tests) are not equivalent, according to Examples 2 and 4.

b) Considering the P. Martin - Löf theory over an "enriched" alphabet (Y contains one more element) we can express its notions (tests) as notions in the A. N. Kolmogorov theory (representable tests), according to Theorem 3.

c) For every natural $p \geqq 2$ and for every alphabet X with p elements there exists a $M-L$ test over $X^* \times N$ which is not representable. So, every non representable test $V \subset X^* \times N$ can be done representable in $Y^* \times N$ by adding an element to X, but in $Y^* \times N$ there exist other non representable tests. The "enlargement" process must continue indefinitely.

2. Example 5 goes in a "converse direction". Here, there are "too many" representable tests over the enriched alphabet.

3. We feel we must add the following ideas:

a) We have already seen that there exists a diastic distinction between the binary case ($p = 2$) and the non binary cases ($p > 2$) (see Remark 1, following Corollary 4 in [1]). These ideas of qualitative differences between the cases of alphabets having different numbers of elements (non-representable tests in case p become representable in case $p + 1$) are pursued in the present paper.

b) The theory constructed over non-binary alphabets is therefore legitime, natural and presents an intrinsic importance.

(Received February 9, 1982.)

REFERENCES

[1] C. Calude and I. Chiţescu: Random strings according to A. N. Kolmogorov and P. Martin-Löf — Classical approach. Found. Control Engng. (to appear).

[2] A. N. Kolmogorov: Three approaches to the quantitative definition of information. Problems Inform. Transmission *1* (1965), 1—7.

[3] M. Machtey and P. Young: An Introduction to General Theory of Algorithms. North-Holland, New York 1978.

[4] P. Martin-Löf: The definition of random sequences. Inform. and Control *19* (1966), 602—619.

[5] H. Rogers, Jr.: The Theory of Recursive Functions and Effective Computability. McGraw-Hill, New York 1967.

[6] A. Zvonkin and L. Levin: The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms (in Russian). Uspechi Mat. Nauk *156* (1970), 85—127.

Dr. Cristian Calude, Dr. Ion Chiţescu, Department of Mathematics, University of Bucharest, Str. Academiei 14, R-70109 Bucharest. Romania.