On Unambiguous Number Systems with a Prime Power Base

Juha Honkala*

Abstract

We study unambiguous number systems with a prime power base. Given a prime p and a p-recognizable set A, it is decidable whether or not A is representable by an unambiguous number system. Given an arbitrary integer n and n-recognizable set A, the unambiguous representation of A is unique if it exists, provided that A is not a finite union of arithmetic progressions.

Keywords: Number system, unambiguity, decidability.

1 Introduction

We study representation of integers in arbitrary number systems. Here "arbitrary" means that the digits may be larger than the base and that completeness is not required, i.e., every integer need not have a representation in the system. Also the number of the digits is arbitrary. These number systems were defined and studied by Maurer, Salomaa and Wood in [14]. The work was continued by Culik II and Salomaa in [5] and Honkala in [8]. These references discuss the connections to the theory of L systems and cryptography. Further results on number systems have been obtained in [9]-[11]. For closely related work see [1,7,13].

The study of number systems is closely connected with the study of sets of integers recognizable by finite automata. By definition, a set A of nonnegative integers is k-recognizable if and only if there exists a finite automaton which recognizes the representations of the integers of A written at base k. Here $k \geq 2$ is a positive integer. Now, if A is represented by a number system N, the representations of the integers of A can be recognized by an automaton with a single state if the digit set $\{0, 1, \ldots, k-1\}$ is replaced by the digit set of N. Thus, representability by a number system implies simplicity of recognition when the choice of the base and the digits is optimal.

In this paper we study unambiguous number systems with a prime power base. By definition, a number system is unambiguous if no integer has more than one representation in the system. The assumption concerning the base makes it possible to apply the theory of finite fields.

Suppose p is a prime. By Christol, [2], a set A of nonnegative integers is p-recognizable if and only if there exists a nonzero polynomial $P(z,t)$ over the finite field $\mathbb{F}_p$ such that $P(z, \sigma_A) = 0$. Here σ_A is the series $\sum_{i \in A} z^i$ of $\mathbb{F}_p[[z]]$. Using

*Department of Mathematics, University of Turku, 20500 Turku 50, Finland

this result we show that it is decidable whether or not a given p-recognizable set is represented by an unambiguous number system. Consequently, given a number system N with a prime power base, it is decidable whether or not there exists an unambiguous number system equivalent to N, i.e., representing the same set of integers as N.

Consider an n-recognizable set A. Here n is an arbitrary integer, not necessarily a prime. It is well known that A is also n^k-recognizable for each positive integer k. We show that, on the contrary, the set A has at most one unambiguous base, provided that A is not a finite union of arithmetic progressions. More specifically, if A is not a finite union of arithmetic progressions, there exists at most one unambiguous number system representing exactly the integers of A.

2 Definitions

By a *number system* we mean a $(v+1)$-tuple $N = (n, m_1, \ldots, m_v)$ of positive integers such that $v \geq 1, n \geq 2$ and $1 \leq m_1 < m_2 < \ldots < m_v$. The number n is referred to as the *base* and the numbers m_i as the *digits* of the number system N. A nonempty word

$$m_{i_k} m_{i_{k-1}} \ldots m_{i_1} m_{i_0}, \; 1 \leq i_j \leq v \tag{1}$$

over the alphabet $\{m_1, \ldots, m_v\}$ is said to *represent* the integer

$$m_{i_k} n^k + m_{i_{k-1}} n^{k-1} + \ldots + m_{i_1} n + m_{i_0}. \tag{2}$$

The word (1) is said to be a *representation* of the integer (2). The set of all represented integers is denoted by $S(N)$. By definition, a number system is *unambiguous* if no integer has more than one representation.

A set A of positive integers is called *representable by a number system*, shortly RNS, if there exists a number system N such that $A = S(N)$.

Suppose $k \geq 2$ and denote $\mathbf{k} = \{0, 1, \ldots, k-1\}$. Define the mapping ν_k from $\mathbf{k}^*$ to $\mathbb{N}$ by

$$\nu_k(a_0 a_1 \ldots a_m) = \sum_{i=0}^{m} a_i k^{m-i} \; (a_i \in \mathbf{k}).$$

The mapping ν_k is extended in the natural way to concern languages $L \subseteq \mathbf{k}^*$. Hence $\nu_k(L) = \{\nu_k(x) | x \in L\}$. By definition, a set A of nonnegative integers is *k-recognizable* if there exists a rational language $L \subseteq \mathbf{k}^*$ such that $A = \nu_k(L)$. For the basic properties of k-recognizable sets see [6] and [15].

The following result is essentially due to Culik II and Salomaa, [5]. For a proof, see [9].

Lemma 2.1 *If $N = (n, m_1, \ldots, m_v)$ is a number system, the set $S(N)$ is n-recognizable.*

If p is a prime, we denote by $\mathbb{F}_p$ the field of integers modulo p. The polynomial ring over $\mathbb{F}_p$ in z is denoted by $\mathbb{F}_p[z]$. The quotient field of $\mathbb{F}_p[z]$ is denoted by $\mathbb{F}_p(z)$. The ring of formal power series over $\mathbb{F}_p$ in z is denoted by $\mathbb{F}_p[[z]]$. An element α belonging to an extension field of $\mathbb{F}_p(z)$ is *algebraic* over $\mathbb{F}_p(z)$ if there exists a nonzero polynomial $P(t) \in \mathbb{F}_p(z)[t]$ such that $P(\alpha) = 0$. If α is algebraic over $\mathbb{F}_p(z)$ there exists a polynomial $R(t) \in \mathbb{F}_p(z)[t]$ of minimal degree such that $R(\alpha) = 0$ and the leading coefficient of $R(t)$ is 1. This polynomial $R(t)$ is called the *minimal polynomial* of α. Notice that $R(t)$ is necessarily irreducible. By definition, the *degree* of α equals the degree of the minimal polynomial of α. The basic facts about minimal polynomials and algebraic extensions of fields which will be needed in the sequel can be found in [12].

Suppose A is a set of nonnegative integers. Then the series σ_A over $\mathbb{F}_p$ is defined by

$$\sigma_A = \sum_{i \in A} z^i.$$

The following theorem is due to Christol, [2], and Christol et al., [3].

Theorem 2.2 *Suppose that p is a prime and A is a set of nonnegative integers. The set A is p-recognizable if and only if the series*

$$\sigma_A = \sum_{i \in A} z^i$$

of $\mathbb{F}_p[[z]]$ is algebraic over the field $\mathbb{F}_p(z)$. If A is p-recognizable there exists a nonzero polynomial P in $\mathbb{F}_p[z,t]$ such that

$$P(z, \sigma_A(z)) = 0$$

and the degree of P in t is at most $p^s - 1$. Here s is the number of states in the minimal deterministic automaton recognizing the set

$$\{a_0 a_1 \ldots a_h | h \geq 0, a_i \in \mathbf{p}, a_0 + a_1 p + \ldots + a_h p^h \in A\}.$$

The bound given above for the degree of P can be deduced from [3, pages 407-408].

In the sequel we need a characterization of the sets A such that σ_A has degree one over $\mathbb{F}_p(z)$. By definition, a set A of nonnegative integers is *recognizable* if A is a finite union of arithmetic progressions.

Lemma 2.3 *A nonempty set $A \subseteq \mathbb{N}$ is recognizable if and only if there exists a nonzero polynomial P in $\mathbb{F}_p[z,t]$ of degree one in t such that $P(z, \sigma_A(z)) = 0$.*

Proof. If A is recognizable, the existence of P is clear. On the contrary, suppose that

$$R(z) + Q(z)\sigma_A = 0,$$

where $R(z), Q(z) \in \mathbb{F}_p[z]$. Without loss of generality we suppose that $Q(0) \neq 0$. Therefore σ_A is an $\mathbb{F}_p$-rational power series. Because $\mathbb{F}_p$ is finite, the set $A = \{i \mid \sigma_A \text{ contains the term } z^i\}$ is recognizable (see [16], Theorem II 5.2). □

3 The Main Results

Suppose p is a prime. In this section we repeatedly use the following fact. If $r = \sum r_i z^i$ belongs to $\mathbb{F}_p[[z]]$ and $q \geq 1$, then

$$r^{p^q} = \sum r_i z^{ip^q}.$$

Lemma 3.1 *Suppose that $N = (n, m_1, \ldots, m_v)$ is an unambiguous number system. Suppose furthermore that $n = p^q$, where p is a prime and $q \geq 1$. Define $a(z) = \sum_{i=1}^{v} z^{m_i}$. Then $\sigma_{S(N)} \in \mathbb{F}_p[[z]]$ satisfies the equation*

$$at^n - t + a = 0$$

in $\mathbb{F}_p[[z]]$.

Proof. Clearly

$$S(N) = \bigcup_{i=1}^{v} (m_i + nS(N)) \bigcup \{m_1, \ldots, m_v\}.$$

Because N is unambiguous,

$$(m_{i_1} + nS(N)) \cap (m_{i_2} + nS(N)) = \emptyset$$

if $i_1 \neq i_2$ and $1 \leq i_1, i_2 \leq v$. Therefore

$$\begin{aligned} \sigma_{S(N)} &= a(z) + \sum_{i=1}^{v} (z^{m_i} \sum_{j \in S(N)} z^{nj}) \\ &= a(z) + a(z) \sum_{j \in S(N)} z^{nj} \\ &= a(z) + a(z)(\sum_{j \in S(N)} z^{j})^n \\ &= a(z) + a(z)\sigma^n_{S(N)}. \end{aligned}$$

□

Lemma 3.2 *Suppose that $R(t) \in \mathbb{F}_p(z)[t]$ has degree $k \geq 2$ in t. Suppose furthermore that $R(t)$ divides*

$$P(t) = at^{p^q} - t + a$$

where $a \in \mathbb{F}_p[z]$, the degree m_1 of the lowest term of a is at least one and $q \geq 1$. Then

$$q \leq \log_p(m_1 k(k-1) + 1).$$

Proof. Because the derivative of $P(t)$ equals -1, the roots of $P(t)$ are simple. At least two of the roots of $P(t)$, say γ_1 and γ_2, are also roots of $R(t)$. Denote $\beta = \gamma_1 - \gamma_2$. Now

$$a\beta^{p^q} - \beta = P(\gamma_1) - P(\gamma_2) = 0. \tag{3}$$

Because β is the difference of two roots of a polynomial of degree k, the degree of the minimal polynomial of β is at most $k(k-1)$. Suppose that the minimal polynomial of β multiplied by an element of $\mathbb{F}_p[z]$ equals

$$S(t) = a_m t^m + \ldots + a_1 t + a_0,$$

where $a_i \in \mathbb{F}_p[z]$ for $0 \le i \le m$, and $a_m \neq 0$. Now

$$\begin{aligned} S(\beta)^{p^q} &= a_m^{p^q}(\beta^{p^q})^m + \ldots + a_1^{p^q}\beta^{p^q} + a_0^{p^q} \\ &= a_m^{p^q}(a^{-1})^m\beta^m + \ldots + a_1^{p^q}(a^{-1})\beta + a_0^{p^q}. \end{aligned}$$

Here the last equation follows by (3). Therefore, β is a root of the polynomial

$$S_1(t) = a_m^{p^q}(a^{-1})^m t^m + \ldots + a_1^{p^q}(a^{-1})t + a_0^{p^q}.$$

Because the degrees of S and S_1 are equal to the degree of the minimal polynomial of β, we have

$$a_m^{p^q-1} = a^m a_0^{p^q-1}. \tag{4}$$

Denote the degrees of the lowest terms of a_m and a_0 by i and j, respectively. Then

$$(i-j)(p^q-1) \le m_1 k(k-1).$$

Because the degree of the lowest term of a is positive, $i > j$, and the claim follows. □

Theorem 3.3 *Suppose p is a prime. Given a p-recognizable set A, it is decidable whether or not there exists an unambiguous number system N such that $A = S(N)$.*

Proof. By Theorem 10 of [10], it is decidable whether or not A is recognizable. Suppose first it is not.

Consider the series $\sigma_A \in \mathbb{F}_p[[z]]$. By Theorem 2.2, σ_A is algebraic over $\mathbb{F}_p(z)$ and the degree of the minimal polynomial $R(t)$ of σ_A is at most $p^s - 1$. Here s is an effectively obtainable positive integer. By Lemma 2.3, the degree of $R(t)$ is at least 2. Suppose now that $A = S(N)$ where $N = (n, m_1, \ldots, m_v)$ is an unambiguous number system. By Lemma 2.1 and Cobham's theorem, [4], there exists a positive integer q such that $n = p^q$. Denote

$$a(z) = z^{m_1} + \ldots + z^{m_v}$$

and

$$P(t) = at^{p^q} - t + a.$$

By Lemma 3.1, we have $P(\sigma_A) = 0$. Therefore, because $R(t)$ is the minimal polynomial of σ_A, the polynomial $R(t)$ divides $P(t)$. By Lemma 3.2,

$$q \le \log_p(m_1(p^s-1)(p^s-2)+1) \le 2s + \log_p m_1.$$

Here m_1 is necessarily the least positive element of A. Therefore, to decide whether or not A is representable by an unambiguous number system, it suffices to decide whether or not $A = S(N)$ for an unambiguous number system N with a base p^i, $i \le 2s + \log_p m_1$. This can be done by Theorem 6.3 of [5].

Suppose then that A is recognizable. The decidability in this case will be shown in the next section of this paper. □

Corollary 3.4 *Given a number system N with a prime power base, it is decidable whether or not there exists an unambiguous number system N_1 such that $S(N) = S(N_1)$.*

The decidability status of the problems considered in Theorem 3.3 and Corollary 3.4 is open in the general case. In the last result of this section, however, no primality assumptions are needed.

Theorem 3.5 *Suppose A is a k-recognizable set for some $k \geq 2$. Furthermore, suppose that A is not recognizable. Then there is at most one unambiguous number system N such that $A = S(N)$.*

Proof. Suppose that $N_1 = (n_1, m_1, \ldots, m_u)$ and $N_2 = (n_2, m_1', \ldots, m_v')$ are distinct unambiguous number systems such that $A = S(N_1) = S(N_2)$. Because A is not recognizable there exist positive integers $n \geq 2$, i and j such that $n_1 = n^i$ and $n_2 = n^j$. Denote

$$a(z) = z^{m_1} + \ldots + z^{m_u}$$

and

$$b(z) = z^{m_1'} + \ldots + z^{m_v'}.$$

Now

$$\sigma_A(z) = a(z) + a(z)\sigma_A(z^{n^i}) \tag{5}$$

and

$$\sigma_A(z) = b(z) + b(z)\sigma_A(z^{n^j}). \tag{6}$$

Here σ_A belongs to $\mathbb{F}_p[[z]]$. The choice of the prime p is free. Replace in (5) z by z^{n^j} and in (6) z by z^{n^i}. Hence

$$\sigma_A(z^{n^j}) = a(z^{n^j}) + a(z^{n^j})\sigma_A(z^{n^{i+j}}) \tag{7}$$

and

$$\sigma_A(z^{n^i}) = b(z^{n^i}) + b(z^{n^i})\sigma_A(z^{n^{i+j}}). \tag{8}$$

Now (5)-(8) imply that

$$\sigma_A(z)[b(z)a(z^{n^j}) - a(z)b(z^{n^i})] = a(z)b(z)[a(z^{n^j}) - b(z^{n^i})]. \tag{9}$$

Because necessarily $m_1 = m_1'$, the lowest terms of $a(z)$ and $b(z)$ have the same degree. Therefore, if $n^j \neq n^i$, the right-hand side of (9) is nonzero. If $n^j = n^i$, necessarily $a(z) \neq b(z)$, and again the right-hand side of (9) is nonzero. By Lemma 2.3 this implies that A is recognizable. This contradiction proves the claim. □

Theorem 3.5 does not hold true for recognizable sets (see e.g. Example 4.4 below).

4 Representation of Recognizable Sets

In this section we give a proof of Theorem 3.3 in the case of a recognizable set.

Suppose $A \subseteq \mathbb{N}$ is recognizable. Given $k \in \mathbb{N}$, it is decidable whether or not $A \subseteq k\mathbb{N}$. Denote by d the greatest common factor of the elements of A. Because d necessarily divides the least nonzero element of A, d can be found out effectively. If $A = S(N)$ where $N = (n, m_1, \ldots, m_t)$ is a number system, d divides all the digits of N. Therefore

$$d^{-1}A = \{x | dx \in A\} = S(N')$$

where $N' = (n, d^{-1}m_1, \ldots, d^{-1}m_t)$. Clearly, N is unambiguous if and only if N' is unambiguous. Hence we suppose without loss of generality in the rest of this section that $d = 1$. Define now the ω-word $\omega(A) = a_1 a_2 a_3 \ldots$ by

$$a_i = \begin{cases} 0 & \text{if } i \notin A \\ 1 & \text{if } i \in A. \end{cases}$$

Because A is recognizable, there exist words $u, v \in \{0,1\}^*$ such that $\omega(A) = uv^\omega$. (Here $v^\omega = vvv\ldots$). The words u and v can be obtained effectively. In the sequel we always assume that v is a primitive word, i.e., that there does not exist a word v_1 and an integer $k \geq 2$ such that $v = v_1^k$. If $i, j \geq 1$, we denote

$$\omega(A)[i,j] = a_i a_{i+1} \ldots a_{i+j-1}.$$

The length of a word w is denoted by $|w|$.

Lemma 4.1 *Suppose A is a recognizable set with $\omega(A) = uv^\omega$. If $N = (n, m_1, \ldots, m_t)$ is an unambiguous number system representing A with $n \geq |u|+|v|$, then the length of v divides n.*

Proof. Suppose that $A = S(N)$ where $N = (n, m_1, \ldots, m_t)$ is an unambiguous number system and $n \geq |u| + |v|$. Suppose m is a digit of N. Denote

$$w_1 = \omega(A)[mn + |u| + 1, |v|]$$

and

$$w_2 = \omega(A)[|u| + 1, |v|].$$

Clearly, if $m_i \in \{|u|+1, \ldots, |u|+|v|\}$, then $mn + m_i \in \{mn + |u| + 1, \ldots, mn + |u|+|v|\}$. On the other hand, any integer in the set $\{|u|+1, \ldots, |u|+|v|\}$ belonging to A is a digit of N. Therefore the word w_1 is obtained from w_2 by replacing some 0's by 1's. However, the number of 1's in w_1 is equal to the number of 1's in w_2. Therefore $w_1 = w_2$. Because a primitive word equals no nontrivial conjugate of itself,

$$mn + |u| + 1 \equiv |u| + 1 (\bmod |v|).$$

Hence $|v|$ divides mn. Because this holds for any digit m and the greatest common factor of the digits is 1, $|v|$ divides n.

□

If $A \subseteq \mathbb{N}$, we denote $A^0 = A \cup \{0\}$. If a set B is a disjoint union of the sets $B_1, \ldots, B_s$, we denote $B = B_1 \dot\cup B_2 \dot\cup \ldots \dot\cup B_s$.

Lemma 4.2 *Suppose that A is a recognizable set of positive integers with $\omega(A) = uv^\omega$. Then there is an unambiguous number system $N = (n, m_1, \ldots, m_t)$ representing A with $n \geq |u|+|v|$ if and only if there exist a positive integer k and nonnegative integers $x_1, x_2, \ldots, x_k$ such that*

$$x_1 + A^0 \dot\cup \ldots \dot\cup x_k + A^0 = \mathbb{N} \tag{10}$$

and, furthermore, for each $x \in A$ there are infinitely many elements of A congruent to x modulo the length of v.

Proof. Suppose first that $A = S(N)$, where $N = (n, m_1, \ldots, m_t)$ is an unambiguous number system such that $n \geq |u| + |v|$. By Lemma 4.1, $|v|$ divides n. Therefore there exists an integer i with $1 \leq i \leq n$ such that

$$\{x | x \equiv i (\bmod n)\} \cap A = i + n\mathbb{N}.$$

Suppose that $y_1, \ldots, y_k$ are the digits of N that are congruent to i modulo n. Because N is unambiguous, we have

$$y_1 + nA^0 \dot{\cup} \ldots \dot{\cup} y_k + nA^0 = i + n\mathbb{N}.$$

Hence

$$\frac{1}{n}(y_1 - i) + A^0 \dot{\cup} \ldots \dot{\cup} \frac{1}{n}(y_k - i) + A^0 = \mathbb{N}.$$

It is clear that if $x \in A$ there are infinitely many elements of A congruent to x modulo the length of v.

Conversely, suppose that there exist $x_1, \ldots, x_k$ such that (10) holds. Fix $n \geq |u| + |v|$ such that $|v|$ divides n. The digits are chosen as follows. Consider an integer i with $1 \leq i \leq n$. If

$$\{x | x \equiv i (\bmod n)\} \cap A = i + n\mathbb{N},$$

then

$$i + nx_1 + nA^0 \dot{\cup} \ldots \dot{\cup} i + nx_k + nA^0 = i + n\mathbb{N} \tag{11}$$

and we take the integers $i + nx_1, \ldots, i + nx_k$ as digits. If

$$\{x | x \equiv i (\bmod n)\} \cap A = i + n + n\mathbb{N},$$

then

$$i + n + nx_1 + nA^0 \dot{\cup} \ldots \dot{\cup} i + n + nx_k + nA^0 = i + n + n\mathbb{N} \tag{12}$$

and we take $i + n + nx_1, \ldots, i + n + nx_k$ as digits. Let N be the number system that has base n and has all the digits chosen above. An inductive argument shows that $A = S(N)$. The unambiguity of N follows because we have disjoint unions in (11) and (12).

□

Notice that there exists at most one sequence $x_1, \ldots, x_k$ of nonnegative integers such that (10) holds. The existence of the sequence is easy to decide.

Suppose A is a recognizable set with $\omega(A) = uv^\omega$. Theorem 6.3 of [5] implies that all unambiguous number systems $N = (n, m_1, \ldots, m_t)$ representing A with $n < |u| + |v|$ can be constructed effectively. Lemmas 4.1 and 4.2 give all unambiguous representations with base greater than or equal to $|u| + |v|$. (This follows because no set has two distinct unambiguous representations with the same base.) In particular, given a recognizable set A, it is decidable whether or not there is an unambiguous number system N such that $A = S(N)$. This concludes the proof of Theorem 3.3.

Example 4.3 Denote $N = (2, 1, 4)$. By [5, Example 2.3], $S(N) = \{x | x \not\equiv 2 (\bmod 3), x \geq 1\}$. Clearly N is unambiguous. This example shows that sometimes a recognizable set has unambiguous bases smaller than the period. By Lemma 4.2, $S(N)$ does not have other unambiguous representations.

Example 4.4 Denote $A = \{x | x \equiv 0, 1 (\bmod 4), x \geq 1\}$. Then

$$A^0 \dot{\cup} 2 + A^0 = \mathbb{N}.$$

Therefore, by the proof of Lemma 4.2, the set A has unambiguous base $4m$ if $m \geq 1$. Hence A has infinitely many unambiguous bases. This shows that Theorem 3.5 does not hold true for recognizable sets.

References

[1] J. Berstel. Fibonacci words - a survey. In G. Rozenberg and A. Salomaa, Editors, *The Book of L*, pages 13-27, Springer-Verlag, 1986.

[2] G. Christol. Ensembles presque periodiques k-reconnaissables. *Theoret. Comput. Sci.* 9:141-145, 1979.

[3] G. Christol, T. Kamae, M. Mendes-France and G. Rauzy. Suites algebriques, automates et substitutions. *Bull. Soc. Math. de France* 108:401-419, 1980.

[4] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory* 3:186-192, 1969.

[5] K. Culik II and A. Salomaa. Ambiguity and decision problems concerning number systems. *Inform. and Control* 56:139-153, 1983.

[6] S. Eilenberg. *Automata, Languages and Machines, Vol. A.* Academic Press, 1974.

[7] C. Frougny. Linear numeration systems of order two. *Inform. and Computation* 77:233-259, 1988.

[8] J. Honkala. Unique representation in number systems and L codes. *Discrete Appl. Math.* 4:229-232, 1982.

[9] J. Honkala. Bases and ambiguity of number systems. *Theoret. Comput. Sci.* 31:61-71, 1984.

[10] J. Honkala. A decision method for the recognizability of sets defined by number systems. *RAIRO Theoretical Informatics* 20:395-403, 1986.

[11] J. Honkala. On number systems with negative digits. *Annales Academiae Scientiarum Fennicae,* Series A.I. Mathematica, Vol. 14:149-156, 1989.

[12] S. Lang. *Algebra.* Addison-Wesley, 1965.

[13] A. de Luca and A. Restivo. Star-free sets of integers. *Theoret. Comput. Sci.* 43:265-275, 1986.

[14] H. Maurer, A. Salomaa and D. Wood. L codes and number systems. *Theoret. Comput. Sci.* 22:331-346, 1983.

[15] D. Perrin. Finite automata. In J. van Leeuwen, Editor, *Handbook of Theoretical Computer Science, Vol.* B, pages 1-57, North-Holland, 1990.

[16] A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series.* Springer-Verlag, 1978.

Received July 1, 1991.