Journal of Universal Computer Science, vol. 1, no. 9 (1995), 652-657
submitted: 8/2/95, accepted: 29/8/95, appeared: 28/9/95, ©Springer Pub. Co.

A Decision Method for the Unambiguity of Sets Defined by Number Systems

Juha Honkala
Department of Mathematics
University of Turku
SF-20500 Turku, Finland
juha.honkala@utu.fi

Abstract: We show that it is decidable, given a number system N, whether or not there is an unambiguous number system equivalent to N.

Category: F.4.3

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 digits is arbitrary. These number systems were defined and studied in [Maurer, Salomaa and Wood 83]. The work was continued in [Culik II and Salomaa 83] and [Honkala 82]. These references discuss the connections to the theory of L systems and cryptography. Further results on number systems have been obtained in [Honkala 84, 86, 89, 92]. For closely related work see [Berstel 86], [Frougny 88, 92], [de Luca and Restivo 86] and [Shallit 94].

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 give a decision method for the unambiguity problem of sets defined by number systems. More specifically, given a number system N, it is decidable whether or not there is an unambiguous number system equivalent to N. This problem was posed in [Culik II and Salomaa 83]. A solution is previously known only in the case where the base of N is a prime power or the set $S(N)$ is recognizable, i.e., a finite union of arithmetic progressions [Honkala 92]. Our solution is based on automata-theoretic considerations.

2 Definitions and results

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

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

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

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

The word (1) is said to be a *representation* of the integer (2). The set of all represented integers is denoted by $S(N)$. A set A of positive integers is called *representable by a number system*, shortly RNS, if there exists a number system N such that $A = S(N)$. An integer n is called a *base of an RNS set* A if there is a number system with the base n representing A. By definition, a number system is *unambiguous* if no integer has more than one representation.

Suppose $k \geq 2$ and denote $\mathbf{k} = \{0, 1, \dots, k-1\}$. Define the mapping ν_k from $\mathbf{k}^*$ to the set $\mathbf{N}$ of natural numbers by

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

Note that we use the reversed interpretation; the most significant digit is the rightmost one. The mapping ν_k is extended in the natural way to concern languages $L \subseteq \mathbf{k}^*$. Hence $\nu_k(L) = \{\nu_k(x) \mid x \in L\}$. By definition, a set A of nonnegative integers is *k-recognizable* if there exists a regular language $L \subseteq \mathbf{k}^*$ such that $A = \nu_k(L)$. By definition, a set A of nonnegative integers is *recognizable* if A is a finite union of arithmetic progressions. For the basic properties of k-recognizable sets see [Eilenberg 74] and [Perrin 90]. Culik II and Salomaa showed an important connection between k-recognizable sets and sets defined by number systems: if $N = (n, m_1, \dots, m_v)$ is a number system then $S(N)$ is n-recognizable. For a proof see also [Honkala 84]. By Cobham's well known result (see [Cobham 69] and [Bruyere, Hansel, Michaux and Villemaire 94]) this implies that if N_1 and N_2 are number systems such that $S(N_1) = S(N_2)$ and $S(N_1)$ is not recognizable, then the bases of N_1 and N_2 are powers of the same integer [Honkala 84].

Suppose $A \subseteq \mathbf{N}$. We say that A has *arbitrarily long gaps* if for every $y \in \mathbf{N}$ there exists an $x \in \mathbf{N}$ such that none of the integers $x+1, x+2, \dots, x+y$ belongs to A. Below we need the result that if $N = (n, m_1, \dots, m_v)$ is a number system such that $S(N)$ has arbitrarily long gaps, then $S(N)$ has no bases other than n [Honkala 84].

The purpose of this paper is to prove the following result.

Theorem 1 *It is decidable, given a number system N, whether or not there exists an unambiguous number system N_1 such that $S(N) = S(N_1)$.*

In the proof of Theorem 1 we need a decision method for the recognizability of k-recognizable sets. For two different methods see [Muchnik 91], [Bruyere, Hansel, Michaux and Villemaire 94] and [Honkala 86]. For the notation concerning finite automata used below see [Eilenberg 74] and [Salomaa 85].

3 Proofs

Suppose N is a number system with base n^r where $r \geq 1$ and $n \in \mathbf{N}$ is not a nontrivial power. Denote $A = S(N)$ and $A^0 = A \cup \{0\}$. Define $L \subseteq \mathbf{n}^*$ by $L = \nu_n^{-1}(A)$. By Lemma 3.1 in [Honkala 84] the set A is n^r-recognizable. Hence A is n-recognizable and there exists a finite deterministic automaton $\mathcal{A} = (Q, \mathbf{n}, q_0)$ with state set Q, input alphabet $\mathbf{n}$ and initial state $q_0 \in Q$ such that $L = L(\mathcal{A})$. By definition, the state $q \in Q$ is *additive* if there exist nonnegative integers m and $c_1, \ldots, c_m$ such that

$$\nu_n(L(\mathcal{A}_q)) = c_1 + A^0 \cup \ldots \cup c_m + A^0 \tag{3}$$

where the union is disjoint. Here $\mathcal{A}_q = (Q, \mathbf{n}, q)$ is the automaton obtained from $\mathcal{A}$ by replacing the initial state q_0 by q. Denote the set of the additive states of $\mathcal{A}$ by $Add(\mathcal{A})$. If $q \in Add(\mathcal{A})$, the nonnegative integers m and $c_1, \ldots, c_m$ in (3) are unique.

Denote

$$UB(\mathcal{A}) = \{k \geq 1 \mid \text{ for each } w \in \mathbf{n}^* \text{ of length } k, \text{ the state } q_0 w \text{ is additive } \}.$$

Now we are ready for the key lemma.

Lemma 1. *There is an unambiguous number system N_1 with base n^k such that $S(N_1) = A$ if and only if $k \in UB(\mathcal{A})$ $(k \geq 1)$.*

Proof. First, suppose N_1 is an unambiguous number system with base n^k such that $S(N_1) = A$. Consider a word $w \in \mathbf{n}^*$ of length k. Let $\nu_n(w) + c_1 n^k, \ldots, \nu_n(w) + c_m n^k$ be the digits of N_1 which are congruent to $\nu_n(w)$ modulo n^k. (If there are no such digits, $\nu_n(L(\mathcal{A}_{q_0 w})) = \emptyset$ and $q_0 w$ is trivially additive.) We claim that

$$\nu_n(L(\mathcal{A}_{q_0 w})) = c_1 + A^0 \cup \ldots \cup c_m + A^0$$

where the union is disjoint. First, suppose $w_1 \in L(\mathcal{A}_{q_0 w})$ where $w_1 \in \mathbf{n}^*$. Because then

$$\nu_n(w w_1) = \nu_n(w) + n^k \nu_n(w_1) \in A,$$

there are nonnegative integers $a \in A^0$ and i, $1 \leq i \leq m$, such that

$$\nu_n(w) + n^k \nu_n(w_1) = \nu_n(w) + c_i n^k + n^k a.$$

Hence $\nu_n(w_1) = c_i + a \in c_i + A^0$. Conversely, if $\nu_n(w_1) = c_i + a$ where $w_1 \in \mathbf{n}^*$, $1 \leq i \leq m$ and $a \in A^0$, then

$$\nu_n(w w_1) = \nu_n(w) + n^k \nu_n(w_1) = \nu_n(w) + c_i n^k + n^k a \in A.$$

Therefore $w_1 \in L(\mathcal{A}_{q_0 w})$ and $\nu_n(w_1) \in \nu_n(L(\mathcal{A}_{q_0 w}))$. Finally, suppose that $x = c_i + a = c_j + b$ where $1 \leq i, j \leq m$ and $a, b \in A^0$. Then

$$\nu_n(w) + n^k x = \nu_n(w) + c_i n^k + n^k a = \nu_n(w) + c_j n^k + n^k b.$$

Because the representation of $\nu_n(w) + n^k x$ according to N_1 is unique, we have $i = j$ and $a = b$. Therefore the sets $c_i + A^0$ are pairwise disjoint $(1 \leq i \leq m)$. This proves the claim and shows that $q_0 w$ is additive. Consequently $k \in UB(\mathcal{A})$.

Conversely, suppose that $k \in UB(\mathcal{A})$. Hence, for each word $w \in \mathbf{n}^*$ of length k there exist nonnegative integers $m(w), c(w)_1, \ldots, c(w)_{m(w)}$ such that

$$\nu_n(L(\mathcal{A}_{q_0 w})) = c(w)_1 + A^0 \cup \ldots \cup c(w)_{m(w)} + A^0$$

where the union is disjoint. Define the number system N_1 as follows. The base of N_1 is n^k and the digits are $\nu_n(w) + c(w)_j n^k$ for $w \in \mathbf{n}^k$ and $1 \leq j \leq m(w)$. Clearly, each digit is positive. Indeed, if $w \neq 0^k$ then $\nu_n(w)$ is positive, and if $w = 0^k$ then $c(w)_j \neq 0$ for $1 \leq j \leq m(w)$ because zero does not belong to A. We claim that N_1 is unambiguous and $S(N_1) = A$.

We show first that $S(N_1) \subseteq A$. Suppose $a \in A^0$. Then $c(w)_i + a \in \nu_n(L(\mathcal{A}_{q_0 w}))$ if $w \in \mathbf{n}^k$ and $1 \leq i \leq m(w)$. Therefore there exists $w_1 \in \mathbf{n}^*$ such that $c(w)_i + a = \nu_n(w_1)$ and $\nu_n(ww_1) \in A$. It follows that

$$\nu_n(w) + c(w)_i n^k + n^k a \in A.$$

Therefore, if d is a digit of N_1, then $d + n^k A^0 \subseteq A$. This implies that $S(N_1) \subseteq A$.

Next, we show that $A \subseteq S(N_1)$. Assume on the contrary that this is not true and denote by x the smallest element in $A - S(N_1)$. Choose the word $w \in \mathbf{n}^k$ such that x is congruent to $\nu_n(w)$ modulo n^k and choose a word $w_1 \in \mathbf{n}^*$ such that $x = \nu_n(ww_1)$. Because $x \in A$, we have $w_1 \in L(\mathcal{A}_{q_0 w})$. Hence $\nu_n(w_1) = c(w)_i + a$ for some $1 \leq i \leq m(w)$, $a \in A^0$. By the choice of x, the integer a, if nonzero, belongs to $S(N_1)$. Consequently

$$x = \nu_n(ww_1) = \nu_n(w) + n^k \nu_n(w_1) = \nu_n(w) + c(w)_i n^k + n^k a \in S(N_1).$$

This contradiction shows that indeed $A \subseteq S(N_1)$. Therefore $A = S(N_1)$.

Finally, suppose that

$$b_0 + b_1 n^k + \ldots + b_s n^{ks} = c_0 + c_1 n^k + \ldots + c_t n^{kt}$$

where $s, t \geq 0$ and $b_0, \ldots, b_s, c_0, \ldots, c_t$ are digits of N_1 such that $b_0 \neq c_0$. Choose the word $w \in \mathbf{n}^k$ such that $\nu_n(w)$ is congruent to b_0 (and c_0) modulo n^k. Then there exist $i \neq j$, $1 \leq i, j \leq m(w)$ such that $b_0 = \nu_n(w) + c(w)_i n^k$ and $c_0 = \nu_n(w) + c(w)_j n^k$. Hence

$$c(w)_i + b_1 + b_2 n^k + \ldots + b_s n^{k(s-1)} = c(w)_j + c_1 + c_2 n^k + \ldots + c_t n^{k(t-1)}$$
$$\in c(w)_i + A^0 \cap c(w)_j + A^0.$$

This contradiction shows that N_1 is unambiguous. □

In the next two lemmas we show that the set $UB(\mathcal{A})$ can be computed effectively if A does not have arbitrarily long gaps.

Lemma 2. *Suppose A does not have arbitrarily long gaps. Given a state $q \in Q$ it is decidable whether or not q is additive. If q is additive one can effectively find the numbers $c_1, \ldots, c_m \in \mathbf{N}$ such that*

$$\nu_n(L(\mathcal{A}_q)) = c_1 + A^0 \cup \ldots \cup c_m + A^0.$$

Proof. Denote $y = d(n^r - 1)^{-1}$ where d is the greatest digit of the given number system N. By Lemma 4.6 in [Honkala 84], for any positive integer $x > d$, the set A contains at least one of the integers $x + 1, x + 2, \ldots, x + y$. Hence

$$\liminf_{t \to \infty} t^{-1} N(A, t) \geq y^{-1}$$

where $N(A, t)$ is the number of the elements of A less than or equal to t. This implies that for any nonnegative integers $c_1, \ldots, c_{y+1}$, the sets $c_i + A^0$, $1 \leq i \leq y + 1$, are not pairwise disjoint.

Now, find the smallest element c_1 of $\nu_n(L(\mathcal{A}_q))$ and check whether or not $c_1 + A^0 \subseteq \nu_n(L(\mathcal{A}_q))$. This decision is possible because $c_1 + A^0$ is n-recognizable. If the inclusion does not hold, q is not additive. If the inclusion holds, check whether $\nu_n(L(\mathcal{A}_q)) = c_1 + A^0$. If not, find the smallest element c_2 in $\nu_n(L(\mathcal{A}_q)) - (c_1 + A^0)$ and check whether $c_2 + A^0$ and $c_1 + A^0$ are disjoint and whether $c_2 + A^0 \subseteq \nu_n(L(\mathcal{A}_q))$. If not, q is not additive. Otherwise, check whether $\nu_n(L(\mathcal{A}_q)) = c_1 + A^0 \cup c_2 + A^0$. If not, find the smallest element in $\nu_n(L(\mathcal{A}_q)) - (c_1 + A^0 \cup c_2 + A^0)$ and proceed similarly.

By the first paragraph of the proof, the procedure stops after at most y steps. This proves the lemma. □

Lemma 3. *Suppose A does not have arbitrarily long gaps. Then the set $UB(\mathcal{A})$ can be computed effectively.*

Proof. Denote $Q_j = q_0 \mathbf{n}^j$ for $j \geq 1$. Because the sequence (Q_j) is effectively ultimately periodic, the claim follows by Lemma 2. □

If $S(N)$ is recognizable, it is possible that $S(N)$ has bases which are not powers of n (see [Culik and Salomaa 83]). Therefore, Lemma 1 is not enough to find out the unambiguous bases of $S(N)$. However, the following result has been proved in [Honkala 92].

Lemma 4. *Suppose $S(N)$ is recognizable. Then it is decidable whether or not there exists an unambiguous number system N_1 such that $S(N) = S(N_1)$.*

Proof of Theorem 1. First, decide whether or not $S(N)$ is recognizable. If it is, Theorem 1 follows from Lemma 4. Suppose it is not. Then every base of N is a power of n.

Next, decide whether or not $S(N)$ has arbitrarily long gaps. If it has, n is the only base of $S(N)$, and it suffices to decide whether or not there is an unambiguous number system N_1 with base n such that $S(N) = S(N_1)$. This decision is possible by Theorem 6.3 in [Culik and Salomaa 83]. Finally, if $S(N)$ does not have arbitrarily long gaps, Theorem 1 follows by Lemmas 1 and 3. □

References

[Berstel 86] Berstel, J.: "Fibonacci words - a survey"; In G. Rozenberg and A. Salomaa, eds., The Book of L (Springer, Berlin, 1986) 13-27.

[Bruyere, Hansel, Michaux and Villemaire 94] Bruyere, V., Hansel, G., Michaux, C. and Villemaire, R.: "Logic and p-recognizable sets of integers"; Bulletin of the Belgian Mathematical Society 1 (1994) 191-238.

[Cobham 69] Cobham, A.: "On the base-dependence of sets of numbers recognizable by finite automata"; Math. Systems Theory 3 (1969) 186-192.

[Culik II and Salomaa 83] Culik II, K. and Salomaa, A.: "Ambiguity and decision problems concerning number systems"; Inform. and Control 56 (1983) 139-153.

[Eilenberg 74] Eilenberg, S.: Automata, Languages and Machines, Vol. A; Academic Press, New York (1974).

[Frougny 88] Frougny, C.: "Linear numeration systems of order two"; Inform. and Computation 77 (1988) 233-259.

[Frougny 92] Frougny, C.: "Representations of numbers and finite automata"; Math. Systems Theory 25 (1992) 37-60.

[Honkala 82] Honkala, J.: "Unique representation in number systems and L codes"; Discrete Appl. Math. 4 (1982) 229-232.

[Honkala 84] Honkala, J.: "Bases and ambiguity of number systems"; Theoret. Comput. Sci. 31 (1984) 61-71.

[Honkala 86] Honkala, J.: "A decision method for the recognizability of sets defined by number systems"; RAIRO, Theoret. Informatics and Appl. 20 (1986) 395-403.

[Honkala 89] Honkala, J.: "On number systems with negative digits"; Annales Academiae Scientiarum Fennicae, Series A.I. Mathematica, Vol. 14 (1989) 149-156.

[Honkala 92] Honkala, J.: "On unambiguous number systems with a prime power base"; Acta Cybern. 10 (1992) 155-163.

[de Luca and Restivo 86] de Luca, A. and Restivo, A.: "Star-free sets of integers"; Theoret. Comput. Sci. 43 (1986) 265-275.

[Maurer, Salomaa and Wood 83] Maurer, H., Salomaa, A. and Wood, D.: "L codes and number systems"; Theoret. Comput. Sci. 22 (1983) 331-346.

[Muchnik 91] Muchnik, A.: "Definable criterion for definability in Presburger Arithmetic and its applications"; (preprint in Russian), Institut of new technologies, 1991.

[Perrin 90] Perrin, D.: "Finite automata"; In: J. van Leeuwen, ed., Handbook of Theoretical Computer Science, Vol. B (Elsevier, Amsterdam, 1990) 1-57.

[Salomaa 85] Salomaa, A.: "Computation and Automata"; Cambridge University Press, Cambridge (1985).

[Shallit 94] Shallit, J.: "Numeration systems, linear recurrences and regular sets"; Inform. and Computation 113 (1994) 331-347.