Digit Set Conversion by On-Line Finite Automata

Athasit Surarerks

Abstract

This paper is about numbers represented in positional notation, in integral or complex bases. We first give an abstract scheme of an on-line algorithm for digit set conversion in fixed base. Then we prove that in positive or negative integral base the digit set conversion is computable by an on-line finite state automaton. We also show similar results for complex numbers represented in the Penney number system or in the Knuth number system.

Résumé

Ce papier porte sur les nombres en notation positionnelle selon une base qui peut être un nombre entier ou complexe. Nous donnons d'abord un schéma abstrait d'algorithme en-ligne réalisant la conversion en base fixe entre alphabets de chiffres différents. Ensuite nous prouvons qu'en base entière, positive ou négative, la conversion est réalisable par un automate fini en-ligne. Enfin nous montrons des résultats similaires pour les nombres complexes représentés dans le système de numération de Penney et le système de numération de Knuth.

1 Introduction

Number representation has a long and fascinating history : some of its developments can be found in the work of Knuth [12]. Usually a number is represented by using a finite or infinite string of digits belonging to some finite digit set. In computer arithmetic, the choice of the number system can have a profound influence on the execution time and on the size of implementation of arithmetic algorithms. A redundant number system where a number can be represented by several strings can be used to reduce the complexity of addition. The signed digit number representation of Avizienis [1] is a classical example. By using positive and negative digits, a

Bull. Belg. Math. Soc. -1993 (0), 337–358

redundant system is obtained. Generalized signed digit number systems have been studied by Parhami [17].

When performed digit serially, elementary arithmetic operations, like addition, subtraction and multiplication are classically computed in the Least Significant Digit First (LSDF) mode, but division is performed in the Most Significant Digit First (MSDF) mode. In order to be able to pipeline the operations (*i.e.*, each operation can be started without waiting for the end of the previous operation), all the operations should be processed in the same direction. Since the usual representation of the real numbers is a right infinite string of digits, the MSDF mode is more suited for operations on real numbers. For that purpose, on-line arithmetic was first introduced by Ercegovac and Trivedi [6, 20], using the Avizienis number representation. On-line arithmetic is used for special circuits, such as signal processing, and for very long precision arithmetic. During on-line computations, the operands as well as the results flow serially through arithmetic units, digit by digit, starting from the most significant digit. On-line systems are characterized by their delay (*i.e.*, the number δ such that the first n digits of the result are deduced from the first $n + \delta$ digits of the input values).

Digit set conversion plays an important role in computing particularly in many implementations of elementary arithmetic operations. Addition and multiplication by a fixed integer are particular cases of digit set conversion. We shall investigate only the on-line conversion into signed digit number systems for a fixed base (*i.e.*, for every given number representation in base β over some contiguous digit set, find the representation of the same number over another signed digit set in the same base). The generalizations and applications of parallel digit set conversion have been studied by Kornerup [13].

The notion of on-line finite automata that we use in this work has been introduced by Muller [15]. By using the algorithm of Avizienis [1] and of Chow and Robertson [3], it is shown in [7, 8] that on-line addition in integer base $|\beta| > 1$ with a balanced digit set $\mathcal{D} = \{d \in \mathbb{Z} \mid -b \leq d \leq b\}$ where $\mathcal{D}$ is symmetric, can be realized by an on-line finite automaton with $4b^2 + 1$ states if $\mathcal{D}$ is a minimally redundant digit set, and with $4b^2$ states if $\mathcal{D}$ is not a minimally redundant digit set. Nielsen and Muller in [16] show how to build circuits for redundant complex addition with $\{-1, 0, 1\}$ as digit set.

In this paper, we consider a digit set conversion where the alphabets of signed digits are not supposed to be balanced. We construct an on-line finite automaton, which has less states than the one of [8] for addition in the classical case of balanced alphabets.

The paper develops as follows. In Section 2, some definitions and basic notations are recalled. In Section 3, we present an abstract scheme for an on-line conversion algorithm in base β, where β can be an integer or a complex number. From that, the construction of a formal on-line automaton can be derived. We then consider particular instances of the base β. In Section 4, we focus on the positive integer base number system and show that conversion can be done by an on-line finite automaton with delay k and β^k states, where k depends on the digit sets considered. The negative integer base number system is examined in Section 5. In Section 6, we show that addition in the Penney complex number system, defined by base $\beta = -1+i$ and digit set $\{-1, 0, 1\}$, can be computed by an on-line finite automaton. Finally in Section 7, we show that the digit set conversion in the Knuth complex number system where the base is a number of the form $i\sqrt{r}, r$ integer ≥ 2, can be realized by an on-line finite automaton.

2 Some definitions

Let us recall some definitions that we use in this work. We shall start by the notion of number system and representation of numbers. Then we will recall the definition of an on-line finite automaton.

2.1 Number system

A *number system* $(\beta, \mathcal{D})$ is composed of a *base* β, where β can be a real or a complex number such that $|\beta| > 1$, and of a finite *digit set* $\mathcal{D}$ of real or complex numbers.

A *β-representation* X on $\mathcal{D}$ is a sequence of the form

$$X = (x_m x_{m-1} \cdots x_0.x_{-1}x_{-2} \cdots)_\beta$$

with $x_j \in \mathcal{D}$ for $j \leq m$, for some $m \in \mathbb{Z}$. Sometimes, the radix point will not be written down.

The *numerical value* of X in base β, denoted by $||X||$, is equal to

$$||X|| = \sum_{j=m}^{-\infty} x_j \beta^j.$$

The set of all β-representations on $\mathcal{D}$ is denoted by $P[\beta, \mathcal{D}]$. We denote by $P_m^n[\beta, \mathcal{D}]$ the set of finite β-representations which have the maximum degree m and the minimum degree n, and by $P_m[\beta, \mathcal{D}]$ the set of infinite β-representations with the maximum degree m,

$$\begin{aligned} P_m^n[\beta, \mathcal{D}] &= \{X = (x_m x_{m-1} \cdots x_{n+1} x_n)_\beta \mid x_j \in \mathcal{D}, \quad m \geq j \geq n\} \\ P_m[\beta, \mathcal{D}] &= \{X = (x_m x_{m-1} \cdots)_\beta \mid x_j \in \mathcal{D}, \quad j \leq m\}. \end{aligned}$$

In integer base β, the usual digit set is of the form $\{c \in \mathbb{Z} \mid 0 \leq c \leq |\beta| - 1\}$ called the *canonical* digit set, and denoted by $\mathcal{C}$. Clearly, conventional decimal number system is the case that β is equal to 10 and the canonical digit set is $\{c \in \mathbb{Z} \mid 0 \leq c \leq 9\}$.

The number system $(\beta, \mathcal{D})$ is said to be *redundant* if there exist two different finite β-representations X_1, X_2 on $\mathcal{D}$ such that $||X_1|| = ||X_2||$.

In 1961, the signed digit number system was first introduced by Avizienis [1] in order to design an addition without propagation of the carry. This number system has been defined for any integer base $\beta \geq 3$ with a symmetric digit set of the form $\{e \in \mathbb{Z} \mid -d \leq e \leq d\}$ with $\frac{\beta}{2} < d \leq \beta - 1$. When $\beta = 2$, one takes $\mathcal{D} = \{-1, 0, 1\}$. Parhami in [17] has introduced more general signed digit number systems where the alphabet is not necessarily symmetric.

Definition 1. *The signed digit number system $(\beta, \mathcal{D})$ is composed of a base β, where β is a positive integer ≥ 2 and of a digit set $\mathcal{D} = \{d \in \mathbb{Z} \mid a \leq d \leq b\}$ where a and b are integers, $a \leq 0 \leq b$.*

The number of elements of the digit set $|\mathcal{D}| = b - a + 1$ plays a role for the redundancy property.

Remark 1.

1. *If $|\mathcal{D}| < \beta$, some reals cannot be represented in this system.*
2. *If $|\mathcal{D}| = \beta$, every integer has a unique finite representation, and every real number can be represented.*
3. *If $|\mathcal{D}| > \beta$, this system is redundant.*

Definition 2.

1. *If $|\mathcal{D}| = \beta + 1$, then $\mathcal{D}$ is a minimally redundant digit set.*
2. *If $|\mathcal{D}| = 2\beta - 1$, then $\mathcal{D}$ is a maximally redundant digit set.*
3. *If $b = |a|$, the digit set $\mathcal{D}$ is said to be symmetric.*

From now on, we will denote a negative digit $-e$ by $\bar{e}$ for any integer e.

2.2 On-line finite automata

For general definitions on automata the reader may consult [5]. We give here only the definitions we shall be using in this work. Note that the automata we use are not necessarily finite. Let $\mathcal{D}$ be a finite alphabet. The set of words on $\mathcal{D}$ is denoted by $\mathcal{D}^*$, the empty word is denoted by ε. The set of infinite words is denoted by $\mathcal{D}^{\mathbb{N}}$.

The automata that are used in this work are also known as 2-tape automata or transducers, see [2]. Recall that a *sequential automaton* with input alphabet $\mathcal{D}$ and output alphabet $\mathcal{E}$ is a directed labeled graph

$$\mathcal{A} = (Q, \mathcal{D} \times \mathcal{E}^*, i_0, F)$$

such that Q is the denumerable set of states, $i_0 \in Q$ is the initial state, F is the set of edges, labeled by couples of $\mathcal{D} \times \mathcal{E}^*$, and denoted by

$$p \xrightarrow{x/y} q$$

with $(x, y) \in \mathcal{D} \times \mathcal{E}^*$. The automaton must be *input deterministic*, that is to say if $p \xrightarrow{x/y} q$ and $p \xrightarrow{x/y'} q'$, then $q = q'$ and $y = y'$. This automaton is said to be *finite* if Q and F are finite.

On-line automata are a special kind of sequential automata. More precisely, an *on-line automaton with delay* δ [15] is a sequential automaton

$$\mathcal{A} = (Q, \mathcal{D} \times (\mathcal{E} \cup \varepsilon), i_0, F)$$

such that every path of length δ starting in the initial state i_0 is of the form

$$i_0 \xrightarrow{x_1/\varepsilon} q_1 \xrightarrow{x_2/\varepsilon} q_2 \cdots \xrightarrow{x_\delta/\varepsilon} q_\delta,$$

with $x_i \in \mathcal{D}$ for $i \leq \delta$, and each edge arriving in $i_0, q_1, q_2, \ldots, q_\delta$ is of that type. Such edges are called *transient* edges. All the others edges are of the form $p \xrightarrow{x/y} q$ with $x \in \mathcal{D}, y \in \mathcal{E}$ and are called *synchronous* edges.

In practice, by assuming that the δ first digits of the input are equal to 0, we will consider on-line automata where all the edges are of the form

$$p \xrightarrow{x/y} q$$

where $x \in \mathcal{D}$ and $y \in \mathcal{E}$.

A function f from $\mathcal{D}^{\mathbb{N}}$ to $\mathcal{E}^{\mathbb{N}}$ is said to be *computable by an on-line automaton* $\mathcal{A}$ if the set of labels of infinite paths in $\mathcal{A}$ starting in the initial state i_0 is equal to the graph of the function f.

In the case of finite words, a *terminal function* $\omega : Q \longrightarrow \mathcal{E}^*$ is added to the definition of the automaton. A function $f : \mathcal{D}^* \longrightarrow \mathcal{E}^*$ is said to be computable by an on-line automaton $\mathcal{A}$ if the graph of f is the set of couples (x, y) of $\mathcal{D}^* \times \mathcal{E}^*$ such that there exists in $\mathcal{A}$ a finite path of the form $i_0 \xrightarrow{(x,u)} q$ and $y = u\omega(q)$.

2.3 Digit set conversion

Let $\mathcal{D}$ and $\mathcal{E}$ be two finite digit sets and let β the base be an integer or a complex number. A *digit set conversion* in base β from $\mathcal{D}$ to $\mathcal{E}$ is a function $\chi : \mathcal{D}^{\mathbb{N}} \longrightarrow \mathcal{E}^{\mathbb{N}}$ such that for each $X \in \mathcal{D}^{\mathbb{N}}$, $||\chi(X)|| = ||X||$. Our basic requirement on $(\beta, \mathcal{E})$ is that the digit set $\mathcal{E}$ is of the form $\{e \in \mathbb{Z} \mid a \leq e \leq b\}$, such that $a \leq 0$ and $b \geq 0$, and that $(\beta, \mathcal{E})$ is redundant. The digit set $\mathcal{D}$ is of the form $\{d \in \mathbb{Z} \mid A \leq d \leq B\}$, such that $A \leq B$.

For every β-representation X in $P[\beta, \mathcal{D}]$, it is not the case that there always exists a β-representation Y in $P[\beta, \mathcal{E}]$ such that $||X|| = ||Y||$. For example, consider the conversion from $P[2, \{\bar{1}, 0, 1\}]$ to $P[2, \{0, 1, 2\}]$. Negative integers included in the first system cannot be represented in the second.

In this work, we shall investigate only the case where for each X in $\mathcal{D}^{\mathbb{N}}$, there exists an Y in $\mathcal{E}^{\mathbb{N}}$ such that $\chi(X) = Y$. Let n_1 be the smallest integer such that $n_1 a \leq A$ and let n_2 be the smallest integer such that $n_2 b \geq B$. Take $n = \max\{n_1, n_2\}$. The digit set $\mathcal{D}$ is included in the digit set $\{d \in \mathbb{Z} \mid na \leq d \leq nb\}$. So we consider only the problem of converting an X in $P[\beta, \mathcal{D}]$ where $\mathcal{D} = \{d \in \mathbb{Z} \mid na \leq d \leq nb\}$ into an Y in $P[\beta, \mathcal{E}]$ with $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$ such that $||X|| = ||Y||$.

Addition and multiplication by a fixed integer are particular cases of such digit set conversion: addition is the case that $n = 2$ and multiplication by u is the case that $n = u$.

3 On-line conversion algorithm

In an on-line conversion, one must take care of the *overflow* problem. For instance, for addition of two numbers in the Avizienis signed digit binary number system, the result needs one more digit on the maximum degree. It corresponds to the conversion from $P_m[2, \{\bar{2}, \bar{1}, 0, 1, 2\}]$ into $P_{m+1}[2, \{\bar{1}, 0, 1\}]$. The overflow is the smallest integer l such that

$$\forall X \in P_m[\beta, \mathcal{D}], \exists Y \in P_{m+l}[\beta, \mathcal{E}], \quad ||X|| = ||Y||$$

The *on-line delay* δ of the conversion in base β from $\mathcal{D}$ to $\mathcal{E}$ is the smallest integer such that the most significant digit of the output can be computed from the most $\delta + 1$ significant digits of the input.

Let β be an integer, $|\beta| > 1$. In order that $(\beta, \mathcal{E})$ be redundant, we take $a \leq 0$ and $b \geq 0$ such that $|\mathcal{E}| > |\beta|$. Our aim is the construction of an on-line automaton $\mathcal{A}$ depending on two parameters k and Q where k is a fixed non-negative integer, the delay of $\mathcal{A}$, and Q is the set of states of $\mathcal{A}$, and realizing the conversion $\chi : \mathcal{D}^{\mathbb{N}} \longrightarrow \mathcal{E}^{\mathbb{N}}$ for a fixed base β. In general, $\mathcal{A}$ might be infinite, and the output might not be on the legal alphabet $\mathcal{E}$. Our results (Theorem 1, Theorem 2) consist in proving that there is a choice of k and Q such that the on-line automaton $\mathcal{A}$ is finite and the output is written on $\mathcal{E}$.

Let k be a non-negative integer. Let $Q = \{q \in \mathbb{Z} \mid g \leq q \leq h\}$ with $g \leq h$, be a complete residue system modulo $|\beta^k|$. Let m be in $\mathbb{Z}$.

We introduce some notations. Given a real number x,

$\lfloor x \rfloor$	denotes the greatest integer which is less than or equal to x.
$\lceil x \rceil$	denotes the least integer which is greater than or equal to x.
$\lfloor\lfloor x \rfloor\rfloor$	denotes the greatest integer which is less than x.
$\lceil\lceil x \rceil\rceil$	denotes the least integer which is greater than x.

We need to define an extension of the notion of Euclidean division. Let z and p be two integers. Define $\tau(z, p)$ as :

$$\tau(z, p) = z - p \times \lfloor \tfrac{z}{p} \rfloor.$$

Then we have that $|\tau(z,p)| \leq |p|-1$. When z and p are positive, $\tau(z,p)$ is equal to $z \mod p$.

The abstract scheme of the on-line algorithm for digit set conversion is the following one.

Algorithm $A_{\mathbb{R}}$
input : $X = (x_m x_{m-1} \cdots)_\beta, \quad x_j \in \mathcal{D} = \{d \in \mathbb{Z} \mid na \leq d \leq nb\}$
output : $Y = (y_{m+k} y_{m+k-1} \cdots)_\beta, \quad y_j \in \mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$
begin
$q_{m+k} := 0$;
$j := m$;
while $j \leq m$ **do**
$q_{j+k-1} := \tau(x_j + q_{j+k}\beta, \beta^k)$;
if $q_{j+k-1} < g$ **then** $q_{j+k-1} := q_{j+k-1} + |\beta^k|$ **endif;**
if $q_{j+k-1} > h$ **then** $q_{j+k-1} := q_{j+k-1} - |\beta^k|$ **endif;**
$y_{j+k} := (x_j + q_{j+k}\beta - q_{j+k-1})/\beta^k$;
$j := j-1$;
enddo;
end;

Lemma 1. *For every $j \leq m$,*

1. *q_{j+k} is in Q,*
2. *if the digits y_{j+k} are bounded, then $||X|| = ||Y||$, and*
3. *y_{j+k} is in $\mathcal{E}$ if the two following conditions are satisfied*

$$\min\{x_j + q_{j+k}\beta\} \geq \min\{e\beta^k + q_{j+k-1} \mid e \in \mathcal{E}\}, \tag{1}$$

and

$$\max\{x_j + q_{j+k}\beta\} \leq \max\{e\beta^k + q_{j+k-1} \mid e \in \mathcal{E}\}. \tag{2}$$

In that case Algorithm $A_{\mathbb{R}}$ is said to be correct.

Proof.

1. Clearly,

$$\forall j \leq m, \quad x_j + q_{j+k}\beta = y_{j+k}\beta^k + q_{j+k-1} \tag{3}$$

Let us show that for each $j \leq m$, q_{j+k} is in Q. First, $q_{m+k} \in Q$. Let $r = \tau(x_j + q_{j+k}\beta, \beta^k)$, then r is an integer, $-|\beta^k|+1 \leq r \leq |\beta^k|-1$. If $r < g$, then $q_{j+k-1} = r + |\beta^k|$. We have $q_{j+k-1} < g + |\beta^k| = h+1$ because $h-g+1 = |\beta^k|$. We also have $q_{j+k-1} \geq -|\beta^k| + 1 + |\beta^k| = 1 > g$, thus $q_{j+k-1} \in Q$.

Similarly, if $r > h$, then $q_{j+k-1} = r - |\beta^k|$. Then $q_{j+k-1} > h - |\beta^k| = g - 1$, and $q_{j+k-1} \leq |\beta^k| - 1 - |\beta^k| = -1$, thus $q_{j+k-1} \in Q$.

Therefore for every $j \leq m, q_{j+k}$ is always in Q.

2. Now we show that $||X|| = ||Y||$, provided that the output digits y_j are in a finite set. From (3), we get that for all $j \geq 0$,

$$x_m\beta^m + \cdots + x_{m-j}\beta^{m-j} = y_{m+k}\beta^{m+k} + \cdots + y_{m+k-j}\beta^{m+k-j} + q_{m+k-j-1}\beta^{m-j}.$$

Since $|\beta| > 1$ and for each $j \leq m$, $|q_{j+k}|$ and $|y_{j+k}|$ are bounded, then $||X|| = ||Y||$.

3. This algorithm is *correct* if for every $j \leq m$, y_{j+k} is in $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$. Suppose that Conditions (1) and (2) are satisfied. Since the principal conversion equation is $x_j + q_{j+k}\beta = y_{j+k}\beta^k + q_{j+k-1}$ and $q_{j+k-1} = \tau(x_j + q_{j+k}\beta, \beta^k)$, then

$$y_{j+k} = \lfloor \frac{x_j + q_{j+k}\beta}{\beta^k} \rfloor.$$

In the case where β^k is positive, if Conditions (1) and (2) hold true, then

$$a\beta^k + g \leq x_j + q_{j+k}\beta \leq b\beta^k + h.$$

Since for any $j \leq m$, q_{j+k} is in Q and $-1 < \frac{g-h}{\beta^k} < 0$ and $0 < \frac{h-g}{\beta^k} < 1$, we have that $a \leq y_{j+k} \leq b$.

In the case where β^k is negative, if Conditions (1) and (2) hold true, then

$$b\beta^k + g \leq x_j + q_{j+k}\beta \leq a\beta^k + h.$$

Since for any $j \leq m$, q_{j+k} is in Q and $0 < \frac{g-h}{\beta^k} < 1$ and $-1 < \frac{h-g}{\beta^k} < 0$, we have that $a \leq y_{j+k} \leq b$. ■

On-line finite automaton for the conversion.
We construct an on-line automaton $\mathcal{A} = (Q, \mathcal{D} \times \mathcal{E}, 0, F)$ where 0 is the initial state and every edge is of the from

$$q_{j+k} \xrightarrow{x_j/y_{j+k}} q_{j+k-1}$$

according to the computation done in Algorithm $A_{\mathbb{R}}$. Since the set Q is finite, the automaton is finite. Since, given x_j and q_{j+k}, the digit y_{j+k} and the state q_{j+k-1} are uniquely determined, the automaton is input deterministic, and this is an on-line finite automaton.

4 Positive integer base number systems

In this section, we consider the case that β is an integer ≥ 2. Let $Q = \{q \in \mathbb{Z} \mid g \leq q \leq h\}$ be a contiguous set of integers, $g \leq h$.
We give two possible definitions of Q.

Case 1. Take $g = \lceil \frac{a\beta^k}{b-a} \rceil$ and $h = \lfloor\lfloor \frac{b\beta^k}{b-a} \rfloor\rfloor$. The set Q is called the lower remainder set.

Case 2. Take $g = \lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil$ and $h = \lfloor \frac{b\beta^k}{b-a} \rfloor$. The set Q is called the upper remainder set.

Lemma 2. *In both cases, Q is a complete residue system modulo β^k.*

Proof. It is true that a set of β^k contiguous integers is a complete residue system modulo β^k. We show that Q is a finite set with β^k elements. To prove this, it is enough to show that $h - g + 1 = \beta^k$. The proof will be separated in two cases.

Case 1. The lower remainder set.
By the definition of g and h, we have $-g \leq \frac{-a\beta^k}{b-a}$ and $h < \frac{b\beta^k}{b-a}$. Then $h - g < \beta^k$. It implies that $h - g + 1 \leq \beta^k$. We also have $g - 1 < \frac{a\beta^k}{b-a}$ and $h + 1 \geq \frac{b\beta^k}{b-a}$. Then $h - g + 2 > \beta^k$. This means that $h - g + 1 \geq \beta^k$. We can conclude that $h - g + 1 = \beta^k$.

Case 2. The upper remainder set.
By the same way as for the lower remainder set, $g = \lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil$ implies $-g < \frac{-a\beta^k}{b-a}$ and $h = \lfloor \frac{b\beta^k}{b-a} \rfloor$ implies $h \leq \frac{b\beta^k}{b-a}$. Then we have $h - g < \beta^k$. It means $h - g + 1 \leq \beta^k$. We also have $1 - g \geq \frac{-a\beta^k}{b-a}$ and $h + 1 > \frac{b\beta^k}{b-a}$. Then $h - g + 2 > \beta^k$ or $h - g + 1 \geq \beta^k$. ∎

Remark 2. *The lower and the upper remainder sets may be the same if $a\beta^k$ or $b\beta^k$ is not a multiple of $b - a$.*

We first need some technical results.

Lemma 3. *The following equality holds*

$$\max\left\{\frac{\lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil}{a}, \frac{\lfloor \frac{b\beta^k}{b-a} \rfloor}{b}\right\} = \max\left\{\frac{\lceil \frac{a\beta^k}{b-a} \rceil}{a}, \frac{\lfloor\lfloor \frac{b\beta^k}{b-a} \rfloor\rfloor}{b}\right\},$$

where $a, b \neq 0$.

Proof. Since $\frac{b\beta^k}{b-a} - \frac{a\beta^k}{b-a} = \beta^k$ where β^k is an integer, we have that $\frac{b\beta^k}{b-a}$ is an integer if and only if $\frac{a\beta^k}{b-a}$ is an integer. If $\frac{b\beta^k}{b-a}$ and $\frac{a\beta^k}{b-a}$ are not integers, we obtain the result. On the other hand, we have

$$\begin{aligned}
\frac{\lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil}{a} &= \frac{a\beta^k}{a(b-a)} + \frac{1}{a} &&= \frac{\beta^k}{b-a} + \frac{1}{a} &&< \frac{\beta^k}{b-a}, \\
\frac{\lfloor \frac{b\beta^k}{b-a} \rfloor}{b} &= \frac{\beta^k}{b-a}, \\
\frac{\lceil \frac{a\beta^k}{b-a} \rceil}{a} &= \frac{\beta^k}{b-a}, \\
\frac{\lfloor\lfloor \frac{b\beta^k}{b-a} \rfloor\rfloor}{b} &= \frac{b\beta^k}{b(b-a)} - \frac{1}{b} &&= \frac{\beta^k}{b-a} - \frac{1}{b} &&< \frac{\beta^k}{b-a}.
\end{aligned}$$

Then we get $\max\{\frac{\lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil}{a}, \frac{\lfloor \frac{b\beta^k}{b-a} \rfloor}{b}\} = \max\{\frac{\lceil \frac{a\beta^k}{b-a} \rceil}{a}, \frac{\lfloor\lfloor \frac{b\beta^k}{b-a} \rfloor\rfloor}{b}\} = \frac{\beta^k}{b-a}$. ∎

Lemma 4. *If $n \leq \beta^k$, $\mathcal{D} = \{d \in \mathbb{Z} \mid na \leq d \leq nb\}$, and $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$, then for any β-representation X in $P_m[\beta, \mathcal{D}]$ there exists a β-representation Y in $P_{m+k}[\beta, \mathcal{E}]$ such that $||Y|| = ||X||$.*

Proof. It is enough to show that (4) and (5) are true,

$$na\beta^m + na\beta^{m-1} + \cdots \geq a\beta^{m+k} + a\beta^{m+k-1} + \cdots, \tag{4}$$

and

$$nb\beta^m + nb\beta^{m-1} + \cdots \leq b\beta^{m+k} + b\beta^{m+k-1} + \cdots. \tag{5}$$

Since $n \leq \beta^k$, we have $\frac{na\beta^{m+1}}{\beta-1} \geq \frac{a\beta^{m+k+1}}{\beta-1}$, thus (4) is true, and $\frac{nb\beta^{m+1}}{\beta-1} \leq \frac{b\beta^{m+k+1}}{\beta-1}$, thus (5) is true. ∎

Now we prove that with these definitions, Algorithm $A_{\mathbb{R}}$ is correct. This can be expressed as follows.

Theorem 1. *Let β be a positive integer > 1, let a be a negative integer and b be a positive integer, $b - a + 1 > \beta$, $\mathcal{D} = \{d \in \mathbb{Z} \mid na \leq d \leq nb\}$ and $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$. There exists a non-negative integer k such that an on-line conversion from $P_m[\beta, \mathcal{D}]$ into $P_{m+k}[\beta, \mathcal{E}]$ is computable by an on-line finite state automaton with β^k states, and k is the smallest integer satisfying the following condition*

$$n \leq \beta^k + (1-\beta)\rho,$$

where
$$\rho = \max\{\frac{\lceil\lceil\frac{a\beta^k}{b-a}\rceil\rceil}{a}, \frac{\lfloor\frac{b\beta^k}{b-a}\rfloor}{b}\} = \max\{\frac{\lceil\frac{a\beta^k}{b-a}\rceil}{a}, \frac{\lfloor\lfloor\frac{b\beta^k}{b-a}\rfloor\rfloor}{b}\}.$$

Proof. We use the definition of Q given above. We take $g = \lceil\frac{a\beta^k}{b-a}\rceil$, $h = \lfloor\lfloor\frac{b\beta^k}{b-a}\rfloor\rfloor$ in Case 1, and $g = \lceil\lceil\frac{a\beta^k}{b-a}\rceil\rceil$, $h = \lfloor\frac{b\beta^k}{b-a}\rfloor$ in Case 2. Then $\rho = \max\{\frac{g}{a}, \frac{h}{b}\}$. Applying Algorithm $A_{\mathbb{R}}$, for x_j in $\mathcal{D}$, we find y_{j+k} such that

$$y_{j+k} = \frac{x_j + q_{j+k}\beta - q_{j+k-1}}{\beta^k}$$

where q_{j+k-1} and q_{j+k} are in Q. Since β is a positive integer, Conditions (1) and (2) of Lemma 1 become

(C1). $na + g\beta \geq a\beta^k + g$

(C2). $nb + h\beta \leq b\beta^k + h$

Let us show that (C1) and (C2) hold true.

C1. $\mathbf{na + g\beta \geq a\beta^k + g}$

By definition, $\rho \geq \frac{g}{a}$ and $\beta > 1$, then $\rho(1-\beta) \leq \frac{(1-\beta)g}{a}$. Choosing k the smallest integer such that $n \leq \beta^k + (1-\beta)\rho$, we obtain that $na + g\beta \geq a\beta^k + g$.

C2. $\mathbf{nb + h\beta \leq b\beta^k + h}$

By definition, $\rho \geq \frac{h}{b}$ and $\beta > 1$, then $\rho(1-\beta) \leq \frac{(1-\beta)h}{b}$. Taking k the smallest integer such that $n \leq \beta^k + (1-\beta)\rho$, we have $nb + h\beta \leq b\beta^k + h$.

Then for all $j \le m$, $\quad y_{j+k} \in \mathcal{E}$. By Lemma 1, Algorithm $A_{\mathbb{R}}$ is correct.

In the case where the input sequences are finite, a terminal function $\omega : Q \longrightarrow \mathcal{E}^*$ must be defined. We have to show that all the elements in Q can be written in $P^0_{k-1}[\beta, \mathcal{E}]$, that is to say

$$\forall q \in Q, q = \textstyle\sum_{i=k-1}^{0} e_i\beta^i \text{ where } e_i \in \mathcal{E}.$$

Let $u = \beta^{k-1}+\beta^{k-2}+\cdots+\beta+1$. We only need to prove that $\forall q \in Q, \quad au \le q \le bu$. We have,

$$\lceil \tfrac{a\beta^k}{b-a} \rceil \le \lceil \lceil \tfrac{a\beta^k}{b-a} \rceil \rceil < \lfloor \lfloor \tfrac{b\beta^k}{b-a} \rfloor \rfloor \le \lfloor \tfrac{b\beta^k}{b-a} \rfloor.$$

It is enough to show that $\lceil \frac{a\beta^k}{b-a} \rceil \ge au$ and $\lfloor \frac{b\beta^k}{b-a} \rfloor \le bu$.

1. $\lceil \frac{a\beta^k}{b-a} \rceil \ge au$
   Because $u > 0$, $a < 0$ and $b - a + 1 > \beta$, then $\frac{u(\beta-1-b+a)+a}{b-a} < 0$.
   And then $a(\frac{u(\beta-1-b+a)+a}{b-a}) \ge 0$.
   By the definition of u, we also have $\beta^k = u(\beta - 1) + 1$.
   It means that $\frac{au(\beta-1)}{b-a} + \frac{a}{b-a} - au \ge 0$, which implies $\lceil \frac{a\beta^k}{b-a} \rceil \ge au$.

2. $\lfloor \frac{b\beta^k}{b-a} \rfloor \le bu$
   By the same way, $u > 1$, $b > 0$ and $\beta - 1 - b + a \le -1$.
   We obtain $\frac{u(\beta-1-b+a)+1}{b-a} < 0$.
   Then we have $b(\frac{u(\beta-1-b+a)+1}{b-a}) \le 0$, which implies $\frac{bu(\beta-1)}{b-a} + \frac{b}{b-a} - bu \le 0$.
   It implies that $\lfloor \frac{b\beta^k}{b-a} \rfloor \le bu$.

We conclude that for every q in Q, $q = \sum_{i=k-1}^{0} e_i\beta^i$ with $e_i \in \mathcal{E}$ and we set $\omega(q) = e_{k-1}e_{k-2}\cdots e_0$. ∎

Remark 3. *Note that the integer k given in Theorem 1 is sufficient to take care of the overflow problem, since $n \le \beta^k$ and by Lemma 4.*

Remark 4. *In the case where $a = -b$, the on-line automaton we construct is not symmetric, contrarily to the one deduced from the algorithm of Avizienis or of Chow and Robertson [8, 15].*

Corollary 1. *In the case of $a = 0$ and $b \ge \beta$, an on-line conversion from $P_m[\beta, \mathcal{D}]$ into $P_{m+k}[\beta, \mathcal{E}]$ is computable by an on-line finite state automaton with β^k states, and k is the smallest integer satisfying the condition*

$$n \le \frac{(b+1)\beta^k - \beta^{k+1} + \beta - 1}{b}$$

Proof. As in the proof of Theorem 1, replacing g by 0. It means that we can use only the lower remainder set as the set of states $Q = \{q \in \mathbb{Z} \mid 0 \le q \le \beta^k - 1\}$. ∎

Corollary 2. *In the case where $a \leq -\beta$ and $b = 0$, an on-line conversion from $P_m[\beta, \mathcal{D}]$ into $P_{m+k}[\beta, \mathcal{E}]$ is computable by an on-line finite state automaton with β^k states, and k is the smallest integer satisfying the following condition :*

$$n \leq \frac{(a-1)\beta^k + \beta^{k+1} - \beta + 1}{a}$$

Proof. As the proof of Theorem 1, replacing h by 0. Only the upper remainder set can be used for set of states $Q = \{q \in \mathbb{Z} \mid -\beta^k + 1 \leq q \leq 0\}$. ∎

Remark 5. *In the case of $a = 0$, zero is not included in the upper remainder set, and in the case of $b = 0$, zero is not included in the lower remainder set.*

We also have the following result.

Lemma 5. *The non-negative integer k in Algorithm $A_{\mathbb{R}}$ is the smallest integer such that the on-line automaton constructed in Theorem 1 is finite.*

Proof. Let k' be a non-negative integer such that $k' < k$. Then we have

$$n > \beta^{k'} + (1-\beta)\max\{\frac{g}{a}, \frac{h}{b}\}$$

This gives $n > \beta^{k'} + \frac{(1-\beta)g}{a}$ and $n > \beta^{k'} + \frac{(1-\beta)h}{b}$. And we can see that

1. $na + g\beta < a\beta^{k'} + g$ and
2. $nb + h\beta > b\beta^{k'} + h$.

This implies that the set of states Q could increase in size in that case. ∎

We now consider the case $n = 2$ (*addition*).

Example 1. *Addition in the binary signed digit number system. The base is $\beta = 2$ with $\mathcal{E} = \{\bar{1}, 0, 1\}$, $\mathcal{D} = \{\bar{2}, \bar{1}, 0, 1, 2\}$ and $n = 2$. Then $k = 2$.*

We use the lower remainder set as the set of states $Q = \{-2, -1, 0, 1\}$.
For addition of $(\bar{1}\bar{1}11011.)_2$ and $(\bar{1}\bar{1}111\bar{1}0.)_2$, the result in $P[2, \mathcal{D}]$ is $w = (\bar{2}\bar{2}22101.)_2$.
There is a path

$$0 \xrightarrow{\bar{2}/0} \bar{2} \xrightarrow{\bar{2}/\bar{1}} \bar{2} \xrightarrow{2/0} \bar{2} \xrightarrow{2/0} \bar{2} \xrightarrow{1/\bar{1}} 1 \xrightarrow{0/1} \bar{2} \xrightarrow{1/\bar{1}} 1$$

in the automaton represented on Figure 1. The terminal function $\omega : Q \longrightarrow \mathcal{E}^*$ is defined as $\omega(\bar{2}) = \bar{1}0, \omega(\bar{1}) = 0\bar{1}, \omega(0) = 00$ and $\omega(1) = 01$, so the result of the conversion of w is $v = (0\bar{1}00\bar{1}1\bar{1}01.)_2$. Note that the length of the output is equal to the length of the input +2. Compare with the result given by the algorithm of Chow and Robertson which is $(0\bar{1}\bar{1}110101.)_2$. The automaton given in [8] has 5 states. □

Proposition 1. *The on-line finite state automaton defined in Theorem 1 is minimal in the number of states amongst on-line finite automata realizing the conversion with the same delay k.*

Proof. By Lemma 5, k is the smallest integer such that the automaton $\mathcal{A}$ of Theorem 1 is finite. Suppose that there is another on-line finite automaton $\mathcal{B}$ with delay k realizing the conversion, and such that its set of states S has less than β^k

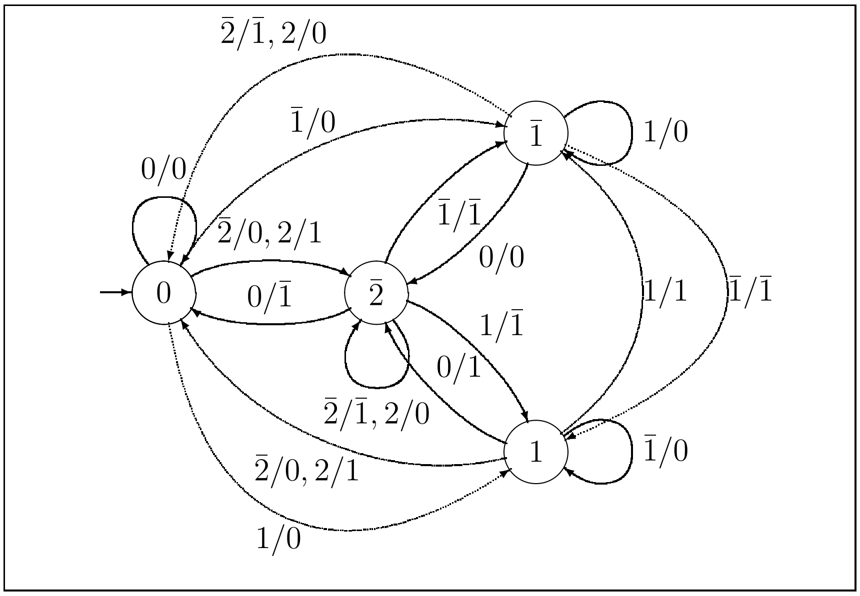

Figure 1: 4-state automaton converting from $P[2, \{\bar{2}, \bar{1}, 0, 1, 2\}]$ to $P[2, \{\bar{1}, 0, 1\}]$ by using the lower remainder set

states. Let $X = (x_m x_{m-1} \cdots)_\beta$ be the input, and $Y = (y_{m+k} y_{m+k-1} \cdots)_\beta$ be the output of a computation in $\mathcal{B}$. Since $\mathcal{B}$ has delay k, this means that for each $j \leq m$, there is a unique path

$$0 = q_{m+k} \xrightarrow{x_m/y_{m+k}} q_{m+k-1} \xrightarrow{x_{m-1}/y_{m+k-1}} q_{m+k-2} \xrightarrow{x_{m-2}/y_{m+k-2}} \cdots$$

$$\cdots \xrightarrow{x_{j+1}/y_{j+k+1}} q_{j+k} \xrightarrow{x_j/y_{j+k}} q_{j+k-1} \xrightarrow{x_{j-1}/y_{j+k-1}} \cdots$$

where all q_j, for $j \leq m+k$, are in S. Since $\sum_{j \leq m} x_j \beta^j = \sum_{j \leq m} y_{j+k} \beta^{j+k}$, we have for any $i \leq m$

$$x_m \beta^{m-i} + \cdots + x_i = y_{m+k} \beta^{m+k-i} + \cdots + y_{i+k} \beta^k + q_{i+k-1}.$$

Let $u_i = x_m \beta^{m-i} + \cdots + x_i$. Then $u_i \sim q_{i+k-1} \mod \beta^k$. Since m and i are arbitrary, and u_i is an integer represented in base β with digits in $\mathcal{D}$, u_i can be in every class modulo β^k. Then S should contain a complete residue system modulo β^k and thus $|S|$ should be greater or equal to β^k. ■

5 Negative integer base number systems

The base is now a negative integer $\beta < -1$. It is known that every real number can be represented in negative base β with digits in $\{c \in \mathbb{Z} \mid 0 \leq c \leq |\beta| - 1\}$ without a sign [12, 14], and that the representation of integers is unique.

By using a signed digit set $\{e \in \mathbb{Z} \mid \bar{d} \leq e \leq d\}$ where $|\frac{\beta}{2}| \leq d \leq |\beta| - 1$, we obtain a redundant number system and it is known [7] that addition is computable by an on-line finite automaton. We show that the on-line conversion can also be done similarly to the positive base, only the condition on k and the definition of Q have to be changed.

The definition of g and h are dependent on the parity of k, because it is no longer true that $\lfloor \frac{a\beta^k}{b-a} \rfloor < 0$ and $\lceil \frac{b\beta^k}{b-a} \rceil > 0$ when k is odd. Then we will modify the definition of g and h, depending on the value of k.

Case 1. The lower remainder set
$g = -\lfloor \frac{a\beta^k}{b-a} \rfloor$ and $h = -\lceil\lceil \frac{b\beta^k}{b-a} \rceil\rceil$ when k is odd,
and
$g = -\lfloor \frac{b\beta^k}{b-a} \rfloor$ and $h = -\lceil\lceil \frac{a\beta^k}{b-a} \rceil\rceil$ when k is even.

Case 2. The upper remainder set
$g = -\lfloor\lfloor \frac{a\beta^k}{b-a} \rfloor\rfloor$ and $h = -\lceil \frac{b\beta^k}{b-a} \rceil$ when k is odd,
and
$g = -\lfloor\lfloor \frac{b\beta^k}{b-a} \rfloor\rfloor$ and $h = -\lceil \frac{a\beta^k}{b-a} \rceil$ when k is even.

Lemma 6. *The finite set Q is a complete residue system modulo $|\beta^k|$.*

Proof. It is similar to the proof of Lemma 2. ■

Theorem 2. *Let β be a negative integer, $\beta < -1$, let a be a negative integer and b be a positive integer such that $b - a + 1 > |\beta|$, and let $\mathcal{D} = \{d \in \mathbb{Z} \mid na \le d \le nb\}$, $\mathcal{E} = \{e \in \mathbb{Z} \mid a \le e \le b\}$. There exists a non-negative integer k such that an on-line conversion from $P_m[\beta, \mathcal{D}]$ to $P_{m+k}[\beta, \mathcal{E}]$ can be done by an on-line finite automaton with $|\beta^k|$ states, where k is the smallest integer satisfying the following condition*

$$n \le \min\{\tfrac{b}{a}\beta^k + \tfrac{g-h\beta}{a}, \tfrac{a}{b}\beta^k + \tfrac{h-g\beta}{b}\} \text{ when } k \text{ is odd,}$$

or

$$n \le \beta^k + \min\{\tfrac{g-h\beta}{a}, \tfrac{h-g\beta}{b}\} \text{ when } k \text{ is even.}$$

Proof. To prove that Algorithm $A_{\mathbb{R}}$ is correct in negative base, it is enough to show that conditions (1) and (2) are satisfied.

Assume that k satisfies the condition above. We first consider the case where k is odd. We have to show that $na + h\beta \ge b\beta^k + g$ and $nb + g\beta \le a\beta^k + h$. Because $n \le \min\{\frac{b}{a}\beta^k + \frac{g-h\beta}{a}, \frac{a}{b}\beta^k + \frac{h-g\beta}{b}\}$, then

$$n \le \tfrac{b}{a}\beta^k + \tfrac{g-h\beta}{a} \quad \Longrightarrow \quad na + h\beta \ge b\beta^k + g,$$

and

$$n \le \tfrac{a}{b}\beta^k + \tfrac{h-g\beta}{b} \quad \Longrightarrow \quad nb + g\beta \le a\beta^k + h.$$

When k is even, we show that $na + h\beta \ge a\beta^k + g$ and $nb + g\beta \le b\beta^k + h$. Because $n \le \beta^k + \min\{\frac{g-h\beta}{a}, \frac{h-g\beta}{b}\}$, then

$$n \le \beta^k + \tfrac{g-h\beta}{a} \quad \Longrightarrow \quad na + h\beta \ge a\beta^k + g$$

and

$$n \le \beta^k + \tfrac{h-g\beta}{b} \quad \Longrightarrow \quad nb + g\beta \le b\beta^k + h.$$

From Lemma 1, the algorithm is correct. ■

6 The Penney complex number system

To represent complex numbers, we may chose a complex radix with a finite real digit set. The Penney number system consists of a base $\beta = -1+i$ and digit set $\mathcal{C} = \{0,1\}$ ([18]). It is known that every complex number has a representation in this system. For instance, $7-2i$ can be written in this system as $(101001.)_{-1+i}$. Gaussian integers have a unique representation, of the form $(x_m x_{m-1}\cdots x_0.)_{-1+i}$. Complex numbers in general may have a right infinite expansion. If we replace the digit set $\mathcal{C} = \{0,1\}$ by the digit set $\mathcal{E} = \{\bar{1},0,1\}$, this system becomes redundant. With digits in $\mathcal{E}$, $7-2i$ can be also written as $(1\bar{1}0\bar{1}0\bar{1}.)_{-1+i}$.

In [4] and [16], it is pointed out that addition in parallel in this system with digit set $\{\bar{1},0,1\}$ is indeed possible but it is not clearly pratical. In [7], it is shown that addition in base $-1+i$ with digit-set $\{d \in \mathbb{Z} \mid \bar{3} \le d \le 3\}$ or $\{d \in \mathbb{Z} \mid \bar{2} \le d \le 2\}$ can be realized by an on-line finite automaton. We show that addition on $\{\bar{1},0,1\}$ can be done by an on-line finite automaton.

Let n be an integer. Since $(-1+i)^4 = -4$, for any $X = (x_{4n}x_{4n-1}\cdots)_{-1+i}$,

$$\begin{aligned} ||X|| &= \textstyle\sum_{j\le 4n} x_j(-1+i)^j \\ &= \textstyle\sum_{j\le n} x_{4j}(-4)^j + (-1+i)^3 \sum_{j\le n} x_{4j-1}(-4)^{j-1} \\ &\quad +(-1+i)^2 \textstyle\sum_{j\le n} x_{4j-2}(-4)^{j-1} + (-1+i)\sum_{j\le n} x_{4j-3}(-4)^{j-1}. \end{aligned}$$

Let

$$\begin{aligned} X_1 &= (x_{4n}x_{4n-4}\cdots)_{-4}, \\ X_2 &= (x_{4n-1}x_{4n-5}\cdots)_{-4}, \\ X_3 &= (x_{4n-2}x_{4n-6}\cdots)_{-4}, \\ X_4 &= (x_{4n-3}x_{4n-7}\cdots)_{-4}, \end{aligned}$$

represented in base -4 with digits in $\mathcal{C}$, we have

$$||X|| = ||X_1|| + (-1+i)^3||X_2|| + (-1+i)^2||X_3|| + (-1+i)||X_4||.$$

Thus the representation X can be obtained by intertwining the representations X_1, X_2, X_3 and X_4. Of course, if the representation is on $\mathcal{E}$, the same remark holds true.

By grouping digits by blocks of length 4 in base $-1+i$, it corresponds to the system with base -4. In the following result, we prove that addition can be done by grouping digits by blocks of length 4.

Theorem 3. *The on-line addition in base $\beta = -1+i$ with digits in $\mathcal{E} = \{\bar{1},0,1\}$ can be performed by one on-line finite automaton with delay 12 with 4096 states, or by the composition of two on-line finite automata with delay $\delta = 12$ with 64 states.*

Proof. We consider addition as a conversion from $P[-1+i,\mathcal{D}]$ where $\mathcal{D} = \{\bar{2},\bar{1},0,1,2\}$ to $P[-1+i,\mathcal{E}]$. By grouping the digits of $\mathcal{D}$ by blocks of length 4, we obtain a number system in base $\gamma = -4$ with digits in $\mathcal{K} = \{\sum_{j=0}^{3} d_j(-1+i)^j \mid d_j \in \mathcal{D}\}$, Remark that $\mathcal{K}$ is a subset of $\mathcal{K}'$ where $\mathcal{K}' = \{u+vi \mid u \in \mathcal{U}$ and $v \in \mathcal{V}\}$, with

$\mathcal{U} = \{u \in \mathbb{Z} \mid \bar{8} \leq u \leq 8\}$ and $\mathcal{V} = \{v \in \mathbb{Z} \mid \bar{10} \leq v \leq 10\}$.

By the same way for $\mathcal{E}$, grouping digits by 4 in $\mathcal{E}$ is equivalent to the system in base $\gamma = -4$ with digits in $\mathcal{G} = \{\sum_{j=0}^{3} d_j(-1+i)^j \mid d_j \in \mathcal{E}\}$. Let $\mathcal{G}' = \{u' + v'i \mid u' \in \mathcal{U}'$ and $v' \in \mathcal{V}'\}$ where $\mathcal{U}' = \mathcal{V}' = \{\bar{1}, 0, 1, 2, 3\}$.

Because $\mathcal{G}' \subset \mathcal{G}$, then our problem is a conversion from $P[-4, \mathcal{K}']$ to $P[-4, \mathcal{G}']$.

We split this conversion into 2 parts, the real and the imaginary part. For the real part, the conversion from $P[-4, \mathcal{U}]$ into $P[-4, \mathcal{U}']$ can be realized by an on-line finite automaton with 64 states ($k = 3$) by Theorem 2. The conversion from $P[-4, \mathcal{V}]$ into $P[-4, \mathcal{V}']$ can also be done by an on-line finite automaton with 64 states ($k = 3$). Combining the two automata together, we obtain an on-line finite automaton with 4096 states for this conversion. Since the conversion runs in base -4 with $k = 3$, the delay is 12 in base $-1 + i$. ∎

7 The Knuth complex number system

Now we consider the Knuth complex number system. Every complex number has a representation in base $\beta = i\sqrt{r}$, where r is an integer, $r \geq 2$, with digits in the canonical digit set $\mathcal{C} = \{c \in \mathbb{Z} \mid 0 \leq c \leq r - 1\}$ [9, 10, 11]. For example, in base $i2$, $-5 + 17i$ can be written with digits in $\{0, 1, 2, 3\}$ as $(102213.2)_{i2}$.

If r is the square of an integer, $r = s^2$, then every Gaussian integer has a unique finite representation in $P^{-1}[is, \mathcal{C}]$, that is, every Gaussian integer has a representation of the form

$$(x_m x_{m-1} \cdots x_0.x_{-1})_{is}, \text{ with } x_j \in \mathcal{C}.$$

Let n be an integer. Since $\beta^2 = -r$, for any β-representation $X = (x_{2n} x_{2n-1} \cdots)_{i\sqrt{r}}$,

$$||X|| = ||X_1|| + (i\sqrt{r})||X_2||$$

where $X_1 = (x_{2n} x_{2n-2} \cdots)_{-r}$ and $X_2 = (x_{2n-1} x_{2n-3} \cdots)_{-r}$. Thus the $i\sqrt{r}$-representation X can be obtained by intertwining the $(-r)$-representations X_1 and X_2.

If we take for digit set $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq e \leq b\}$ where a is a negative integer, b is a positive integer and $|\mathcal{E}| > r$, we obtain a redundant number system.

For instance, in base $i2$, $-5 + 17i$ can also be written with digits in $\mathcal{E} = \{\bar{2}, \bar{1}, 0, 1, 2\}$ as $(10210\bar{1}.2)_{i2}$.

Addition in parallel in base $i\sqrt{2}$ and digit set $\{\bar{1}, 0, 1\}$ has been described in [16]. Addition in base $\beta = i\sqrt{r}$, where r is a positive integer ≥ 2, and with digit set $\mathcal{E} = \{e \in \mathbb{Z} \mid \bar{b} \leq e \leq b\}$, where $b = \lceil \frac{r}{2} \rceil$, has been considered in [7]. In the case where r is even and $b = \frac{r}{2}$, addition is computable by an on-line finite automaton with delay $\delta = 4$. In the case where r is odd and $b = \lceil \frac{r}{2} \rceil$, addition is computable by an on-line finite automaton with delay $\delta = 2$.

Let $\mathcal{E} = \{e \in \mathbb{Z} \mid a \le e \le b\}$ where a and b are integers, $a \le 0$, $b \ge 0$ and $|\mathcal{E}| > r$. Let $\mathcal{D} = \{d \in \mathbb{Z} \mid na \le d \le nb\}$, where n is a positive integer. We show that the on-line conversion from $P[i\sqrt{r}, \mathcal{D}]$ into $P[i\sqrt{r}, \mathcal{E}]$ can be done by an on-line finite automaton.

Algorithm $A_{\mathbb{R}}$ should to be changed for digit set conversion in the Knuth complex number. The new algorithm is the following one.

Algorithm $A_{\mathbb{C}}$
 input : $X = (x_m x_{m-1} \cdots)_\beta, \quad x_j \in \mathcal{D} = \{d \in \mathbb{Z} \mid na \le d \le nb\}$
 output : $Y = (y_{m+k} y_{m+k-1} \cdots)_\beta, \quad y_j \in \mathcal{E} = \{e \in \mathbb{Z} \mid a \le e \le b\}$
 begin
  $q_{m+k} := 0$;
  $j := m$;
  while $j \le m$ **do**
   $\mathrm{Re}(q_{j+k-1}) := \mathrm{Re}(\tau(x_j + q_{j+k}\beta, \beta^k))$;
   $\mathrm{Im}(q_{j+k-1}) := \mathrm{Im}(x_j + q_{j+k}\beta)$;
   if $\mathrm{Re}(q_{j+k-1}) < g$ **then** $\mathrm{Re}(q_{j+k-1}) := \mathrm{Re}(q_{j+k-1}) + |\beta^k|$ **endif;**
   if $\mathrm{Re}(q_{j+k-1}) > h$ **then** $\mathrm{Re}(q_{j+k-1}) := \mathrm{Re}(q_{j+k-1}) - |\beta^k|$ **endif;**
   $y_{j+k} := (x_j + q_{j+k}\beta - q_{j+k-1})/\beta^k$;
   $j := j - 1$;
  enddo;
 end;

The definition of g and h is similar to the negative base and depends on the value of $\frac{k}{2}$ where k is always even.

Case 1. $\frac{k}{2}$ is odd
1. The lower remainder set
$$g = -\lfloor \tfrac{a}{b-a}\beta^k \rfloor - \lceil\lceil \tfrac{b}{b-a}\beta^k \rceil\rceil i\sqrt{r}$$
$$h = -\lceil\lceil \tfrac{b}{b-a}\beta^k \rceil\rceil - \lfloor \tfrac{a}{b-a}\beta^k \rfloor i\sqrt{r}$$
2. The upper remainder set
$$g = -\lfloor\lfloor \tfrac{a}{b-a}\beta^k \rfloor\rfloor - \lceil \tfrac{b}{b-a}\beta^k \rceil i\sqrt{r}$$
$$h = -\lceil \tfrac{b}{b-a}\beta^k \rceil - \lfloor\lfloor \tfrac{a}{b-a}\beta^k \rfloor\rfloor i\sqrt{r}$$

Case 2. $\frac{k}{2}$ is even
1. The lower remainder set
$$g = -\lfloor \tfrac{b}{b-a}\beta^k \rfloor - \lceil\lceil \tfrac{a}{b-a}\beta^k \rceil\rceil i\sqrt{r}$$
$$h = -\lceil\lceil \tfrac{a}{b-a}\beta^k \rceil\rceil - \lfloor \tfrac{b}{b-a}\beta^k \rfloor i\sqrt{r}$$
2. The upper remainder set
$$g = -\lfloor\lfloor \tfrac{b}{b-a}\beta^k \rfloor\rfloor - \lceil \tfrac{a}{b-a}\beta^k \rceil i\sqrt{r}$$
$$h = -\lceil \tfrac{a}{b-a}\beta^k \rceil - \lfloor\lfloor \tfrac{b}{b-a}\beta^k \rfloor\rfloor i\sqrt{r}$$

The set of states Q is defined by

$Q = \{u + v\beta \mid u, v \in \mathbb{Z}$ and $\mathrm{Re}(g) \leq u \leq \mathrm{Re}(h)$ and $\mathrm{Im}(h) \leq v\sqrt{r} \leq \mathrm{Im}(g)\}$.

Lemma 7. *The finite set Q defined above has r^k elements.*

Proof. Let $U = \{u \in \mathbb{Z} \mid \mathrm{Re}(g) \leq u \leq \mathrm{Re}(h)\}$ and let $V = \{v \in \mathbb{Z} \mid \mathrm{Im}(h) \leq v\sqrt{r} \leq \mathrm{Im}(g)\}$. By Lemma 6, U and V are both a complete residue systems modulo $r^{\frac{k}{2}}$. By the definition, Q contains r^k elements. ∎

Theorem 4. *Let β be a complex number of the form $i\sqrt{r}$, where r is a positive integer. Let a be a negative integer, b be a positive integer, $b - a + 1 > r$, $\mathcal{D} = \{d \in \mathbb{Z} \mid na \leq d \leq nb\}$ and $\mathcal{E} = \{e \in \mathbb{Z} \mid a \leq d \leq b\}$. There exist a non-negative integer k such that an on-line conversion from $P_m[\beta, D]$ into $P_{m+k}[\beta, E]$ is computable by an on-line automaton with r^k states, where k is the smallest even integer satisfying the following condition*

$$n \leq \min\{\tfrac{b}{a}\beta^k + \tfrac{Re(g)-Re(h)\beta^2}{a}, \tfrac{a}{b}\beta^k + \tfrac{Re(h)-Re(g)\beta^2}{b}\} \text{ when } \tfrac{k}{2} \text{ is odd,}$$

or

$$n \leq \beta^k + \min\{\tfrac{Re(g)-Re(h)\beta^2}{a}, \tfrac{Re(h)-Re(g)\beta^2}{b}\} \text{ when } \tfrac{k}{2} \text{ is even.}$$

Proof. First let us show that for any $j \leq m$, q_{j+k} is in Q. It is clear that $q_{m+k} = 0$ is in Q. We have to show that if q_u is in Q, then q_{u-1} is also in Q. According to the computation in Algorithm $A_{\mathbb{C}}$,

$$\begin{aligned} \mathrm{Re}(q_{u-1}) &= \mathrm{Re}(\tau(x_{u-k} + q_u\beta, \beta^k)) \quad \text{and} \\ \mathrm{Im}(q_{u-1}) &= \mathrm{Im}(x_{u-k} + q_u\beta). \end{aligned}$$

We have that $-|\beta^k| + 1 \leq \mathrm{Re}(q_{u-1}) \leq |\beta^k| - 1$. Similarly as in the proof of Lemma 1, $\mathrm{Re}(g) \leq \mathrm{Re}(q_{u-1}) \leq \mathrm{Re}(h)$. Since x_u is in $\mathcal{D}$, $\mathrm{Im}(q_{u-1}) = \mathrm{Im}(q_u\beta)$. By the definition of Q and if q_u is in Q, $\mathrm{Im}(h) \leq \mathrm{Im}(q_u\beta) \leq \mathrm{Im}(g)$. Thus q_{u-1} is in Q.

Now, we show that for every $j \leq m$, y_{j+k} is in $\mathcal{E}$ if the two following conditions hold:

$$\min\{\mathrm{Re}(x_j + q_{j+k}\beta)\} \geq \min\{\mathrm{Re}(e\beta^k + q_{j+k-1}) \mid e \in \mathcal{E}\}, \tag{6}$$

$$\max\{\mathrm{Re}(x_j + q_{j+k}\beta)\} \leq \max\{\mathrm{Re}(e\beta^k + q_{j+k-1}) \mid e \in \mathcal{E}\}. \tag{7}$$

Since the conversion equation is $x_j + q_{j+k}\beta = y_{j+k}\beta^k + q_{j+k-1}$ and

$$\mathrm{Re}(q_{j+k-1}) = \mathrm{Re}(\tau(x_j + q_{j+k}\beta, \beta^k)) \quad \text{and}$$

$$\mathrm{Im}(q_{j+k-1}) = \mathrm{Im}(x_j + q_{j+k}\beta).$$

We have that $\mathrm{Re}(y_{j+k}) = \mathrm{Re}(\lfloor \frac{x_j + q_{j+k}\beta}{\beta^k} \rfloor)$ and $\mathrm{Im}(y_{j+k}) = 0$.

In the case where $\frac{k}{2}$ is odd, Conditions (6) and (7) become

$$\begin{aligned} \min\{\mathrm{Re}(x_j + q_{j+k}\beta)\} &\geq b\beta^k + \mathrm{Re}(g), \\ \max\{\mathrm{Re}(x_j + q_{j+k}\beta)\} &\leq a\beta^k + \mathrm{Re}(h). \end{aligned}$$

By definition of Q, $-1 < \frac{\mathrm{Re}(h)-\mathrm{Re}(g)}{\beta^k} < 0$ and $0 < \frac{\mathrm{Re}(g)-\mathrm{Re}(h)}{\beta^k} < 1$, and since for any $j \leq m$, q_{j+k} is in Q, we obtain that $a \leq \mathrm{Re}(y_{j+k}) \leq b$.

In the case where $\frac{k}{2}$ is even, Conditions (6) and (7) become

$$\begin{aligned}\min\{\mathrm{Re}(x_j + q_{j+k}\beta)\} \quad &\geq a\beta^k + \mathrm{Re}(g),\\ \max\{\mathrm{Re}(x_j + q_{j+k}\beta)\} \quad &\leq b\beta^k + \mathrm{Re}(h).\end{aligned}$$

By definition of Q, $0 < \frac{\mathrm{Re}(h)-\mathrm{Re}(g)}{\beta^k} < 1$ and $-1 < \frac{\mathrm{Re}(g)-\mathrm{Re}(h)}{\beta^k} < 0$, and since for any $j \leq m$, q_{j+k} is in Q, we obtain that $a \leq \mathrm{Re}(y_{j+k}) \leq b$.

Since $|\beta| > 1$ and for each $j \leq m$, if $|q_{j+k}|$ and $|y_{j+k}|$ are bounded, and

$$x_m\beta^m + \cdots + x_{m-j}\beta^{m-j} = y_{m+k}\beta^{m+k} + \cdots + y_{m+k-j}\beta^{m+k-j} + q_{m+k-j-1}\beta^{m-j},$$

we get $||X|| = ||Y||$.

We now show that if the conditions of the theorem are satisfied, then Conditions (6) and (7) hold true. It means that we have to show that

Case 1. When $\frac{k}{2}$ is odd, Conditions (6) and (7) become
$na + \mathrm{Re}(g\beta) \geq b\beta^k + \mathrm{Re}(g)$ and $nb + \mathrm{Re}(h\beta) \leq a\beta^k + \mathrm{Re}(h)$.

Case 2. When $\frac{k}{2}$ is even, Conditions (6) and (7) become
$na + \mathrm{Re}(g\beta) \geq a\beta^k + \mathrm{Re}(g)$ and $nb + \mathrm{Re}(h\beta) \leq b\beta^k + \mathrm{Re}(h)$.

In Case 1, by the condition on k, we have

$$\begin{aligned} n &\leq \tfrac{b}{a}\beta^k + \tfrac{\mathrm{Re}(g)-\mathrm{Re}(h)\beta^2}{a}\\ na &\geq b\beta^k + \mathrm{Re}(g) - \mathrm{Re}(h)\beta^2\\ &= b\beta^k + \mathrm{Re}(g) - \mathrm{Re}(g\beta)\\ na + \mathrm{Re}(g\beta) &\geq b\beta^k + \mathrm{Re}(g)\end{aligned}$$

and

$$\begin{aligned} n &\leq \tfrac{a}{b}\beta^k + \tfrac{\mathrm{Re}(h)-\mathrm{Re}(g)\beta^2}{b}\\ nb &\leq a\beta^k + \mathrm{Re}(h) - \mathrm{Re}(g)\beta^2\\ &= a\beta^k + \mathrm{Re}(h) - \mathrm{Re}(h\beta)\\ nb + \mathrm{Re}(h\beta) &\leq a\beta^k + \mathrm{Re}(h)\end{aligned}$$

In Case 2, by the condition on k, we have

$$\begin{aligned} n &\leq \beta^k + \tfrac{\mathrm{Re}(g)-\mathrm{Re}(h)\beta^2}{a}\\ na &\geq a\beta^k + \mathrm{Re}(g) - \mathrm{Re}(h)\beta^2\\ &= a\beta^k + \mathrm{Re}(g) - \mathrm{Re}(g\beta)\\ na + \mathrm{Re}(g\beta) &\geq a\beta^k + \mathrm{Re}(g)\end{aligned}$$

and

$$\begin{aligned} n &\leq \beta^k + \tfrac{\mathrm{Re}(h)-\mathrm{Re}(g)\beta^2}{b}\\ nb &\leq b\beta^k + \mathrm{Re}(h) - \mathrm{Re}(g)\beta^2\\ &= b\beta^k + \mathrm{Re}(h) - \mathrm{Re}(h\beta)\\ nb + \mathrm{Re}(h\beta) &\leq b\beta^k + \mathrm{Re}(h)\end{aligned}$$

In both cases, Conditions (6) and (7) are true. Thus Algorithm $A_{\mathbb{C}}$ is correct. ■

8 Conclusion

In this paper we have presented an on-line finite automaton with delay k for digit set conversion in base β. In the case where β is an integer, the number of states of the automaton is shown on the array below. Note that $|\beta^k|$ is always smaller than or equal to $(b-a)^k$.

	previous results	our algorithm
on-line addition with a minimally redundant digit set	$(b-a)^k+1$	$\|\beta^k\|$
on-line addition with a maximally redundant digit set	$(b-a)^k$	$\|\beta^k\|$

In this work, we have considered digit set conversion from $\mathcal{D}$ to $\mathcal{E}$ where $\mathcal{D}=\{d\in\mathbb{Z}\mid na\le d\le nb\}$ for $n\ge 1$, and $\mathcal{E}=\{e\in\mathbb{Z}\mid a\le e\le b\}, a\le 0, b\ge 0$. More general digit set conversions can be studied. In [19], we give some results for conversion in positive integer base, with a general digit set $\mathcal{D}=\{d\in\mathbb{Z}\mid A\le d\le B\}$, where A and B are integers, $A\le B$, and a redundant digit set $\mathcal{E}=\{e\in\mathbb{Z}\mid a\le e\le b\}$, where a and b are integers, $a\le 0\le b$. Digit set conversion in base 2 from $\{\bar{1},0,1\}$ into $\{0,1,2\}$ falls into this case.

Acknowledgements

We would like to thank the referees for their comments which greatly improved the presentation of this paper.

References

[1] A. Avizienis. Signed-digit number representations for fast parallel arithmetic. *IRE Transactions on Electronic Computers* **10**, 1961, pp. 389-400.

[2] J. Berstel. *Transductions and Context Free Languages*, Teubner Verlag, 1979.

[3] C. Y. Chow and J. E. Robertson. Logical design of a redundant binary adder. *Proc. of the 4th Symposium on Computer Arithmetic*, IEEE Computer Society Press, 1978, pp. 109-115.

[4] J. Duprat and Y. Herreros and S. Kla. New redundant representations of complex numbers and vectors. *Proc. of the 10th Symposium on Computer Arithmetic*, IEEE Computer Society Press, 1991, pp. 2-9.

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

[6] M. D. Ercegovac. On-line Arithmetic: An Overview. SPIE **495**, *Real Time Signal Processing VII*, 1984, pp. 86-93.

[7] Ch. Frougny. On-line finite automata for addition in some numeration systems. *Theoretical Informatics and Applications*, **33**, 1999, pp. 79-101.

[8] Ch. Frougny and J. Sakarovitch. Synchronisation dterministe des automates dlai born. *Theoretical Computer Science*, **191**, 1998, pp. 61-77.

[9] W. Gilbert. Radix representations of quadratic fields. *Journal Math. Anal. Appl.*, **83**, 1981, pp. 264-274.

[10] I. Katai and J. Szabo. Canonical number system. *Acta Sci. Math*, **37**, 1975, pp. 255-280.

[11] D. E. Knuth. An imaginary number system. *CACM*, **3**, 1960, pp. 245-247.

[12] D. E. Knuth. *The Art of Computer Programming, Vol.2: Seminumerical Algorithms.*, 2nd. ed., Addison-Wesley, 1988.

[13] P. Kornerup. Digit-Set Conversions: Generalizations and Applications. *IEEE Transactions on Computers*, **43**, 1994, pp. 622-629.

[14] D. W. Matula. Basic digit sets for radix representation. *JACM*, **29**, 1982, pp. 1131-1143.

[15] J.-M. Muller. Some characterizations of functions computable in on-line arithmetic. *IEEE Transactions on Computers*, **43**, 1994, pp. 752-755.

[16] A. M. Nielsen and J.-M. Muller. Borrow-Save Adders for Real and Complex Number Systems. *Proc. 2nd Real Numbers and Computers*, 1996, pp. 121-137.

[17] B. Parhami. Generalized Signed-Digit Number Systems : A Unifying Framework for Redundant Number Representations. *IEEE Transactions on Computers*, **39**, 1990, pp. 89-98.

[18] W. Penney. A "binary" system for complex numbers. *JACM*, **12**, 1965, pp. 247-248.

[19] A. Surarerks. On-line arithmetics in integer and complex bases. Ph.D. thesis, in preparation.

[20] K. S. Trivedi and M. D. Ercegovac. On-line algorithms for division and multiplication. *IEEE Transactions on Computers*, **26**, 1977, pp. 681-687.

L.I.A.F.A., Université Paris 7
2, Place Jussieu, 75251 Paris Cedex 05, France
athasit@liafa.jussieu.fr