Parallel algorithms for addition in non-standard number systems

Christiane Frougny*, Pavel Heller†, Edita Pelantová† and Milena Svobodová†
*LIAFA, UMR 7089 CNRS and Université Paris 7,
Case 7014, 75205 Paris Cedex 13, France
†Doppler Institute for Mathematical Physics and Applied Mathematics,
and Department of Mathematics, FNSPE, Czech Technical University in Prague,
Trojanova 13, 120 00 Praha 2, Czech Republic

***Abstract*—In 1961 Avizienis proposed a parallel algorithm for addition in base 10 with digit set $\mathcal{A} = \{-6, -5, \ldots, 5, 6\}$. Such an algorithm performs addition in constant time, independently of the length of the representation of the summands. In computer arithmetic parallel addition is used for speeding up multiplication and division algorithms. In this work we consider number systems where the base is a complex number β such that $|\beta| > 1$. We show that we can find a set of signed-digits on which addition is realizable by a parallel algorithm if and only if β is an algebraic number with no conjugate of modulus 1. We then address the question of the size of the digit set that permits parallel addition. We also investigate block parallel addition.**

I. Introduction

A positional number system is given by a base and by a set of digits. The base is a real or complex number β such that $|\beta| > 1$, and the digit set $\mathcal{A}$ is a finite alphabet of real or complex digits. The most studied number systems are of course the usual ones, where the base is a positive integer. But there have been also numerous studies where the base is an irrational real number (the so-called β-*expansions*), a complex number, or a non-integer rational number, *etc*. Some surveys can be found in [14, Chapter 7] and [10, Chapter 2].

Since the beginnings of computer science, the fact that addition of two numbers has a worst-case linear-time complexity has been considered as an important drawback (see, in particular, the seminal paper of Burks, Goldstine and von Neumann [2]). Suppose that two numbers x and y are given by their expansion $x = \bullet x_1 x_2 \cdots$ and $y = \bullet y_1 y_2 \cdots$ in a given base β, and the digits x_j's and y_j's are elements of a digit set $\mathcal{A}$. A parallel algorithm to compute their sum $z = x+y = \bullet z_1 z_2 \cdots$ with $z_j \in \mathcal{A}$ exists when the digit z_j can be determined by the examination of a window of fixed length around the digit $(x_j + y_j)$. This avoids carry propagation. Parallel addition has received a lot of attention, because the complexity of the addition of two numbers becomes constant, and so it is used for internal addition in multiplication and division algorithms, see [5] for instance.

In symbolic dynamics, functions computable in parallel are called *sliding block codes* or *local function*, more precisely p-local, which means that to determine the image of a word by a p-local function, it is enough to consider a sliding window of length p of the input.

A parallel algorithm for addition has been given by Avizienis [1] in 1961: numbers are represented in base $\beta = 10$ with digits from the set $\mathcal{A} = \{-6, -5, \ldots, 5, 6\}$. This algorithm has been generalized to any integer base $\beta \geqslant 3$. The case $\beta = 2$ and alphabet $\mathcal{A} = \{-1, 0, 1\}$ has been elaborated by Chow and Robertson [4] in 1978. Notice that Cauchy [3] already considered the representation in base 10 and alphabet $\{-5, \ldots, 5\}$. All these systems are *redundant*, that is to say, some numbers may have several representations. It is known that the cardinality of an alphabet allowing parallel addition in integer base $\beta \geqslant 2$ must be at least equal to $\beta+1$, see [15].

Amongst the non-standard bases, special attention has been paid to the complex ones, which allow to represent any complex number by a single sequence (finite or infinite) of natural digits, without separating the real and the imaginary part. For instance, it is known that every complex number can be expressed with base $-1 + \imath$ and digit set $\{0, 1\}$, [17]. The case of a non-integer positive real number is the most studied one: it is the theory of so-called β-expansions, and it provides strong mathematical tools, that we have extensively used.

In this paper we consider only digit sets that are finite and formed by contiguous integers. The existence of a parallel addition algorithm in base β implies thus that β must be an algebraic number, i.e., satisfies an equation with integer coefficients. First we give a simple algorithm for parallel addition, Algorithm S, which works whenever the base is an algebraic number with no conjugate of modulus 1. We then show that parallel addition is never possible when the base has an algebraic conjugate of modulus 1. The digit set provided by Algorithm S is in general larger than necessary, so we try to find the smallest possible one. We give lower bounds on the minimal size, and we give addition algorithms for popular number systems. We then address the generalization of block parallel addiction, and show that in some cases, it reduces the size of the addition digit set.

This presentation is based on our three papers [8], [9], [7] where the proofs can be found.

II. Preliminaries

A. Number systems

A *positional number system* $(\beta, \mathcal{A})$ within the complex field $\mathbb{C}$ is defined by a *base* β, which is a complex number such that

$|\beta| > 1$, and a *digit set* $\mathcal{A}$ usually called the *alphabet*, which is a subset of $\mathbb{C}$. If a complex number x can be expressed in the form $\sum_{-\infty \leqslant j \leqslant n} x_j \beta^j$ with coefficients x_j in $\mathcal{A}$, we call the sequence $(x_j)_{-\infty \leqslant j \leqslant n}$ a $(\beta, \mathcal{A})$-*representation* of x and note $x = x_n x_{n-1} \cdots x_0 \bullet x_{-1} x_{-2} \cdots$.

In what follows, $\mathcal{A}$ is a finite set of contiguous integers containing 0. If a $(\beta, \mathcal{A})$-*representation* of x has only finitely many non-zero entries, we say that it is *finite* and the trailing zeroes are omitted.

In analogy with the classical algorithms for arithmetical operations, we work only on the set of numbers with *finite* representations, i.e., on the set

$$\mathrm{Fin}_{\mathcal{A}}(\beta) = \Big\{ \sum_{j \in I} x_j \beta^j \mid I \subset \mathbb{Z}, \quad I \quad \text{finite}, \quad x_j \in \mathcal{A} \Big\}.$$

Such a finite sequence $(x_j)_{j \in I}$ of elements of $\mathcal{A}$ is identified with a bi-infinite string $(x_j)_{j \in \mathbb{Z}}$ in $\mathcal{A}^{\mathbb{Z}}$, where only a finite number of digits x_j have non-zero values.

When the base is a positive real number, the domain has been extensively studied. The best-understood case is the one of representations of real numbers in a non-integer base $\beta > 1$, the so-called *greedy expansions*, introduced by Rényi [18]. Every number $x \in [0, 1]$ can be given a β-expansion by the following *greedy algorithm*:

$$r_0 := x; \text{ for } j \geqslant 1 \text{ put } x_j := \lfloor \beta r_{j-1} \rfloor \text{ and } r_j := \beta r_{j-1} - x_j.$$

Then $x = \sum_{j \geqslant 1} x_j \beta^{-j}$, and the digits x_j are elements of the so-called *canonical alphabet* $\mathcal{C}_\beta = \{0, 1, \ldots, \lceil \beta \rceil - 1\}$. For $x \in [0, 1)$, the sequence $(x_j)_{j \geqslant 1}$ is said to be the *Rényi expansion* or the β-*greedy expansion* of x and denoted $\langle x \rangle_\beta$.

The greedy algorithm applied to the number 1 gives the β-expansion of 1, denoted by $d_\beta(1) = (t_j)_{j \geqslant 1}$, and plays a special role in this theory. A number $\beta > 1$ such that $d_\beta(1)$ is eventually periodic, that is to say, of the form $t_1 \cdots t_m (t_{m+1} \cdots t_{m+p})^\omega$ is called a *Parry number*. If $d_\beta(1)$ is finite, $d_\beta(1) = t_1 \cdots t_m$, β is a *simple* Parry number, [16].

B. Parallel addition

Let us first formalize the notion of parallel addition.

Definition 1. A function $\varphi : \mathcal{A}^{\mathbb{Z}} \to \mathcal{B}^{\mathbb{Z}}$ is said to be p-*local* if there exist two non-negative integers r and t satisfying $p = r + t + 1$, and a function $\Phi : \mathcal{A}^p \to \mathcal{B}$ such that, for any $u = (u_j)_{j \in \mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}}$ and its image $v = \varphi(u) = (v_j)_{j \in \mathbb{Z}} \in \mathcal{B}^{\mathbb{Z}}$, we have $v_j = \Phi(u_{j+t} \cdots u_{j-r})$ for every j in $\mathbb{Z}$.

This means that the image of u by φ is obtained through a sliding window of length p. The parameter r is called the *memory* and the parameter t is called the *anticipation* of the function φ. Such functions, restricted to finite sequences, are computable by a parallel algorithm in constant time.

Definition 2. Given a base β with $|\beta| > 1$ and two alphabets $\mathcal{A}$ and $\mathcal{B}$ containing 0, a *digit set conversion* in base β from $\mathcal{A}$ to $\mathcal{B}$ is a function $\varphi : \mathcal{A}^{\mathbb{Z}} \to \mathcal{B}^{\mathbb{Z}}$ such that

1) for any $u = (u_j)_{j \in \mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}}$ with a finite number of non-zero digits, the image $v = (v_j)_{j \in \mathbb{Z}} = \varphi(u) \in \mathcal{B}^{\mathbb{Z}}$ has only a finite number of non-zero digits as well, and
2) $\sum_{j \in \mathbb{Z}} v_j \beta^j = \sum_{j \in \mathbb{Z}} u_j \beta^j$.

Such a conversion is said to be *computable in parallel* if it is a p-local function for some $p \in \mathbb{N}$.

Thus, addition in $\mathrm{Fin}_{\mathcal{A}}(\beta)$ is computable in parallel if there exists a digit set conversion in base β from $\mathcal{A}+\mathcal{A}$ to $\mathcal{A}$ which is computable in parallel.

In [13], Kornerup suggested a more general concept of parallel addition. Instead of manipulating single digits, one works with blocks of digits with fixed block length k. For the precise description of the Kornerup's idea, we introduce the notation

$$\mathcal{A}_{(k)} = \{a_0 + a_1 \beta + \cdots + a_{k-1} \beta^{k-1} \mid a_i \in \mathcal{A}\},$$

where $\mathcal{A}$ is an alphabet and k a positive integer. Clearly, $\mathcal{A}_{(1)} = \mathcal{A}$.

Definition 3. Given a base β with $|\beta| > 1$ and two alphabets $\mathcal{A}$ and $\mathcal{B}$ containing 0, a *digit set conversion* in base β from $\mathcal{A}$ to $\mathcal{B}$ is said to be *block parallel computable* if there exists some $k \in \mathbb{N}$ such that the digit set conversion in base β^k from $\mathcal{A}_{(k)}$ to $\mathcal{B}_{(k)}$ is computable in parallel. When the specification of k is needed, we say k-*block parallel computable*.

In this terminology, the original parallel addition is 1-block parallel addition.

Remark 4. Suppose that the base is an integer β with $|\beta| \geqslant 2$. It is known that parallel addition is possible on an alphabet of cardinality at least $\beta+1$ (see [15] and [9]). But k-block parallel addition on an alphabet $\mathcal{A}$ is just 1-block parallel addition in integer base β^k on $\mathcal{A}_{(k)}$. Thus k-block parallel addition in integer base β is possible on an alphabet $\mathcal{A}$ such that $\#\mathcal{A}_{(k)} \geqslant \beta^k + 1$. This shows that k-block parallel addition with $k \geqslant 2$ does not allow the use of a smaller alphabet than when $k = 1$.

III. Existence of a parallel algorithm for addition

To be self-contained, we recall the classical algorithms for parallel addition of Avizienis [1], and of Chow and Robertson [4].

Algorithm of Avizienis: Base $\beta = b$, $b \geqslant 3$ integer, parallel addition on alphabet $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$, $b/2 < a \leqslant b - 1$.

Input: two words $x_n \cdots x_m$ and $y_n \cdots y_m$ of $\mathcal{A}^*$, with $m \leqslant n$, $x = \sum_{j=m}^{n} x_j \beta^j$ and $y = \sum_{j=m}^{n} y_j \beta^j$.
Output: a word $z_{n+1} \cdots z_m$ of $\mathcal{A}^*$ such that

$$z = x + y = \sum_{j=m}^{n+1} z_j \beta^j.$$

```
for each j in parallel do
    z_j := x_j + y_j
    if z_j ⩾ a then q_j := 1, r_j := z_j − b
    if z_j ⩽ −a then q_j := −1, r_j := z_j + b
```

`if` $-a+1 \leqslant z_j \leqslant a-1$ `then` $q_j := 0$, $r_j := z_j$
$z_j := q_{j-1} + r_j$

Addition realized by the Avizienis algorithm is a 2-local function, with memory 1 and anticipation 0. Notice that the minimally redundant symmetric alphabet is obtained with the value $a = \lceil \frac{b+1}{2} \rceil$.

The Chow and Robertson algorithm works for base 2 and alphabet $\{-1, 0, 1\}$. We give here a generalization to an even base $\beta = b = 2a$, $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$.

Algorithm of Chow and Robertson: Base $\beta = b = 2a$, $a \geqslant 1$ integer, parallel addition on alphabet $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$.

Input: two words $x_n \cdots x_m$ and $y_n \cdots y_m$ of $\mathcal{A}^*$, with $m \leqslant n$, $x = \sum_{j=m}^{n} x_j \beta^j$ and $y = \sum_{j=m}^{n} y_j \beta^j$.
Output: a word $z_{n+1} \cdots z_m$ of $\mathcal{A}^*$ such that

$$z = x + y = \sum_{j=m}^{n+1} z_j \beta^j.$$

`for each` j `in parallel do`
$z_j := x_j + y_j$
`if` $a+1 \leqslant z_j \leqslant b$ `then` $q_j := 1$, $r_j := z_j - b$
`if` $-b \leqslant z_j \leqslant -a-1$ `then` $q_j := -1$, $r_j := z_j + b$
`if` $-a+1 \leqslant z_j \leqslant a-1$ `then` $q_j := 0$, $r_j := z_j$
`if` $z_j = a$ `and` $z_{j-1} > 0$ `then` $q_j := 1$, $r_j := -a$
`if` $z_j = a$ `and` $z_{j-1} \leqslant 0$ `then` $q_j := 0$, $r_j := a$
`if` $z_j = -a$ `and` $z_{j-1} < 0$ `then` $q_j := -1$, $r_j := a$
`if` $z_j = -a$ `and` $z_{j-1} \geqslant 0$ `then` $q_j := 0$, $r_j := -a$
$z_j := q_{j-1} + r_j$

Addition realized by the Chow and Robertson algorithm is a 3-local function, with memory 2 and anticipation 0.

The main difference between the two algorithms is that the Avizienis algorithm is *neighbour-free*, while the Chow and Robertson algorithm is *neighbour-sensitive*, since the decision taken at position j depends also on the digit at position $j-1$.

The alphabets we use are formed by contiguous integers and contain 0. This restriction already forces the base β to be an algebraic number.

Definition 5. Let β be an algebraic number such that $|\beta| > 1$. We say that β satisfies the *strong representation of zero property* (or, for short, that β *is SRZ*) if there exist integers $b_k, \ldots, b_0, \ldots, b_{-h}$, for some non-negative integers h and k, such that β is a root of the polynomial

$$S(X) = b_k X^k + \cdots + b_0 + \cdots + b_{-h} X^{-h}$$

and

$$b_0 > 2 \sum_{i \in \{-h, \ldots, k\} \setminus \{0\}} |b_i| .$$

The polynomial S is a said to be a *strong polynomial* for β.

If β is SRZ, then the word $b_k \cdots b_0 \cdots b_{-h}$ is a β-representation of zero.

Set $B = b_0$ and $M = \sum_{i \in \{-h, \ldots, k\} \setminus \{0\}} |b_i|$. The inequality from Definition 5 now reads

$$B > 2M .$$

Suppose that β is SRZ. We choose the symmetric alphabet

$$\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}, \quad \text{where } a = \left\lceil \tfrac{B-1}{2} \right\rceil + \left\lceil \tfrac{B-1}{2(B-2M)} \right\rceil M .$$

For this fixed alphabet $\mathcal{A}$, we describe a parallel algorithm for addition in base β. Let us denote

$$c = \left\lceil \tfrac{B-1}{2(B-2M)} \right\rceil \quad \text{and} \quad a' = \left\lceil \tfrac{B-1}{2} \right\rceil .$$

Then $a = a' + cM$. The alphabet $\mathcal{A}' = \{-a', \ldots, 0, \ldots, a'\} \subset \mathcal{A}$ is called the *inner* alphabet.

Algorithm S: Parallel addition for base β with the strong representation of zero property (β is SRZ).

Input: two words $x_n \cdots x_m$ and $y_n \cdots y_m$ of $\mathcal{A}^*$, with $m \leqslant n$, $x = \sum_{j=m}^{n} x_j \beta^j$ and $y = \sum_{j=m}^{n} y_j \beta^j$.
Output: a word $z_{n+k} \cdots z_{m-h}$ of $\mathcal{A}^*$ such that

$$z = x + y = \sum_{j=m-h}^{n+k} z_j \beta^j.$$

`for each` j `in parallel do`
$z_j := x_j + y_j$
find $q_j \in \{-c, \ldots, 0, \ldots, c\}$ such that $z_j - q_j B \in \mathcal{A}'$
$z_j := z_j - \sum_{i=-h}^{k} q_{j-i} b_i$

Proposition 6 ([8]). *Suppose that β is SRZ. Then Algorithm S realizes addition in constant time in parallel in* $\mathrm{Fin}_{\mathcal{A}}(\beta)$ *with* $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$, *where* $a = \left\lceil \frac{B-1}{2} \right\rceil + \left\lceil \frac{B-1}{2(B-2M)} \right\rceil M$. *Addition realized by Algorithm S is a $(h+k+1)$-local function with memory k and anticipation h. Algorithm S is neighbour-free.*

Example 7. Consider base $\beta = 10$. It is SRZ for the polynomial $-X + 10$, where $B = 10$ and $M = 1$. In this case

$$c = \left\lceil \tfrac{9}{16} \right\rceil = 1, \quad a' = \left\lceil \tfrac{9}{2} \right\rceil = 5, \quad \text{and} \quad a = 6 .$$

Therefore, Algorithm S provides parallel addition in the decimal number system on alphabet $\mathcal{A} = \{-6, \ldots, 0, \ldots, 6\}$, and in fact it is precisely the algorithm of Avizienis.

Example 8. Consider base $\beta = 2$. For such a base, $-X + 2$ is not a strong polynomial. Nevertheless, this base satisfies also the polynomial $-X^2 + 4 = 0$, which is strong, with $B = 4$ and $M = 1$. Now we have

$$c = \left\lceil \tfrac{3}{4} \right\rceil = 1, \quad a' = \left\lceil \tfrac{3}{2} \right\rceil = 2, \quad \text{and} \quad a = 3 .$$

So Algorithm S works for base 2 with the alphabet $\{-3, \ldots, 0, \ldots, 3\}$, and is 3-local. Remind that the Chow and

Robertson algorithm is 3-local as well, but it works with the smaller alphabet $\{-1, 0, 1\}$.

Example 9. Let us consider the base $\beta = \frac{1+\sqrt{5}}{2}$, the Golden Mean. It is one root of the equation $X^2 = X + 1$, the second root is $\beta' = \frac{1-\sqrt{5}}{2} = -\frac{1}{\beta}$. Since $\beta^4 + (\beta')^4 = 7$, β is a root of the strong polynomial

$$S(X) = -X^4 + 7 - \tfrac{1}{X^4}$$

with $B = 7$ and $M = 2$. This implies $c = 1$, $a' = 3$, and $a = 5$. Thus addition in the Golden Mean base is a 9-local function on $\mathcal{A} = \{-5, \ldots, 0, \ldots, 5\}$.

The alphabet $\mathcal{A}$ provided by Algorithm S is in general larger than necessary, as shown by Example 8. So we introduce another notion.

Definition 10. Let β be an algebraic number such that $|\beta| > 1$. We say that β satisfies the *weak representation of zero property* (or, for short, that β *is WRZ*) if there exist integers $b_k, \ldots, b_0, \ldots, b_{-h}$, for some non-negative integers h and k, such that β is a root of the polynomial

$$W(X) = b_k X^k + \cdots + b_0 + \cdots + b_{-h} X^{-h}$$

and

$$b_0 > \sum_{i \in \{-h,\ldots,k\} \setminus \{0\}} |b_i| \,.$$

The polynomial W is said to be a *weak polynomial* for β.

When β is WRZ, we can describe a parallel algorithm for addition. Let us put as above $B = b_0$ and $M = \sum_{i \in \{-h,\ldots,k\} \setminus \{0\}} |b_i|$, and let

$$\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}, \quad \text{where} \quad a = \left\lceil \tfrac{B-1}{2} \right\rceil + M \,.$$

Similarly to Algorithm S, the inner alphabet is $\mathcal{A}' = \{-a', \ldots, 0, \ldots, a'\}$ with $a' = \lceil \frac{B-1}{2} \rceil$. The algorithm works in

$$s + 1 \quad \text{steps, where} \quad s = \left\lceil \tfrac{a}{B-M} \right\rceil \,.$$

Algorithm W: Parallel addition for base β with the weak representation of zero property (β is WRZ).

Input: two words $x_n \cdots x_m$ and $y_n \cdots y_m$ of $\mathcal{A}^*$, with $m \leqslant n$, $x = \sum_{j=m}^{n} x_j \beta^j$ and $y = \sum_{j=m}^{n} y_j \beta^j$.
Output: a word $z_{n+ks} \cdots z_{m-hs}$ of $\mathcal{A}^*$ such that

$$z = x + y = \sum_{j=m-hs}^{n+ks} z_j \beta^j.$$

```
for each j in parallel do
    z_j := x_j + y_j
    for ℓ := 1 to s do
        if z_j ∈ A' then q_j := 0 else q_j := sgn z_j
        z_j := z_j − Σ_{i=−h}^{k} q_{j−i} b_i
```

Proposition 11 ([8])**.** *Suppose that β is WRZ. Then Algorithm W realizes addition in constant time in parallel in $\mathrm{Fin}_{\mathcal{A}}(\beta)$ with alphabet $\mathcal{A} = \{-a, \ldots, 0, \ldots, a\}$, where $a = \left\lceil \frac{B-1}{2} \right\rceil + M$. Addition realized by Algorithm W is a $(hs + ks + 1)$-local function with memory ks and anticipation hs. Algorithm W is neighbour-free.*

Example 12. The base $\beta = \frac{1+\sqrt{5}}{2}$ is a root of the weak polynomial

$$W(X) = -X^2 + 3 - \frac{1}{X^2}.$$

By Algorithm W addition is a 13-local function on $\mathcal{A} = \{-3, \ldots, 0, \ldots, 3\}$.

In [8] we have proved the following result.

Theorem 13. *Let β with $|\beta| > 1$ be an algebraic number. Then β is SRZ (or WRZ) if and only if it has no conjugate of modulus* 1.

The proof of the previous statement gives a constructive method for finding a suitable strong (or weak) polynomial.

The following proposition shows that the requirement of having no conjugate of modulus 1 is also necessary and, even more, that the generalization of parallelism via working with k-blocks does not change the situation.

Proposition 14 ([7])**.** *Let β with $|\beta| > 1$ be an algebraic number with a conjugate γ of modulus $|\gamma| = 1$ and let $\mathcal{A} \subset \mathbb{Z}$ be a finite alphabet of contiguous integers containing* 0 *and* 1*. Then addition on $\mathcal{A}$ cannot be block parallel computable.*

Corollary 15. *Let β with $|\beta| > 1$. Addition in base β is computable in parallel if and only if β is an algebraic number with no conjugate of modulus* 1.

It is fairly easy to recognize whether an algebraic number does, or does not have a conjugate of modulus 1, by looking at its minimal polynomial. First, if the number is quadratic, it cannot have any conjugate of modulus 1. Suppose now that β is an algebraic number of degree $d > 2$, with a conjugate β' with modulus $|\beta'| = 1$. Let $F(X) = X^d + g_1 X^{d-1} + \cdots + g_{d-1} X + g_d$ be its minimal polynomial, $F(X)$ in $\mathbb{Q}[X]$. Since $F(X)$ is minimal, $\beta' \neq \pm 1$, thus β' is not real. As the minimal polynomial has all its coefficients real, the complex conjugate $\overline{\beta'} = \frac{1}{\beta'}$ is a root of G as well. In general, if the minimal polynomial has two different roots η and $\frac{1}{\eta}$, then the minimal polynomial satisfies

$$F(X) = X^d G\big(\tfrac{1}{X}\big) \,,$$

thus it is reciprocal and its degree is even. This is summarized in the following remark.

Remark 16. Let β with $|\beta| > 1$ be an algebraic number of degree d.

- If d is odd, or
- if $d = 2$, or
- if $d \geqslant 4$ is even and the minimal polynomial of β is not reciprocal,

then β has no conjugate of modulus 1.

IV. Lower bounds on the size of alphabets allowing parallel addition

We now give another parallel algorithm for addition in base the Golden Mean on the smaller alphabet $\{-1, 0, 1\}$, with a method similar to the method of Chow and Robertson. In that case addition is a 21-local function. This alphabet cannot be further reduced, as proved in [6].

We begin by describing two auxiliary algorithms for elimination of digits. Both of them use the weak representation of zero $-\beta^2 + 3 - \frac{1}{\beta^2} = 0$.

The first auxiliary algorithm removes digits -2:

Algorithm A: Base $\beta = \frac{1+\sqrt{5}}{2}$, digit set conversion from $\{-2, \dots, 2\}$ to $\{-1, \dots, 2\}$.

Input: a finite sequence of digits (z_j) of $\{-2, 1, 0, 1, 2\}$, with $z = \sum z_j \beta^j$.
Output: a finite sequence of digits (z_j) of $\{-1, 0, 1, 2\}$, with $z = \sum z_j \beta^j$.

```
for each j in parallel do
    if { z_j = −2
       { z_j = −1
       { z_j = 0  and z_{j+2} < 0  and z_{j−2} < 0
    then q_j := −1
    else q_j := 0
    z_j := z_j − 3q_j + q_{j+2} + q_{j−2}
```

The second auxiliary algorithm removes digits 2:

Algorithm B: Base $\beta = \frac{1+\sqrt{5}}{2}$, digit set conversion from $\{-1, 0, 1, 2\}$ to $\{-1, 0, 1\}$.

Input: a finite sequence of digits (z_j) of $\{-1, 0, 1, 2\}$, with $z = \sum z_j \beta^j$.
Output: a finite sequence of digits (z_j) of $\{-1, 0, 1\}$, with $z = \sum z_j \beta^j$.

```
for each j in parallel do
    if { z_j = 2
       { z_j = 1  and (z_{j+2} ⩾ 1 or z_{j−2} ⩾ 1)
       { z_j = 0  and z_{j+2} = z_{j−2} = 2
       { z_j = 0  and z_{j+2} = z_{j−2} = 1 and z_{j+4} ⩾ 1 and
       { z_{j−4} ⩾ 1
       { z_j = 0  and z_{j+2} = 2 and z_{j−2} = 1  and
       { z_{j−4} ⩾ 1
       { z_j = 0  and z_{j−2} = 2 and z_{j+2} = 1  and
       { z_{j+4} ⩾ 1
    then q_j := 1
    else q_j := 0
    z_j := z_j − 3q_j + q_{j+2} + q_{j−2}
```

Algorithm G realizes parallel addition in base $\beta = \frac{1+\sqrt{5}}{2}$ on alphabet $\{-1, 0, 1\}$:

Algorithm G: Base $\beta = \frac{1+\sqrt{5}}{2}$, parallel addition on alphabet $\mathcal{A} = \{-1, 0, 1\}$.

Input: two finite sequences of digits (x_j) and (y_j) of $\{-1, 0, 1\}$, with $x = \sum x_j \beta^j$ and $y = \sum y_j \beta^j$.
Output: a finite sequence of digits (z_j) of $\{-1, 0, 1\}$ such that

$$z = x + y = \sum z_j \beta^j.$$

```
for each j in parallel do
    v_j := x_j + y_j
    use Algorithm A with input (v_j) and output (w_j)
    use Algorithm B with input (w_j) and output (z_j)
```

This example shows that the question of the size of a minimal digit set allowing parallel addition for a given base β must be taken under consideration. In [9] we have found the following lower bounds.

Theorem 17. *Let β be a positive real algebraic number, $\beta > 1$, and let $\mathcal{A}$ be a finite set of contiguous integers containing 0 and 1. If addition in $\mathrm{Fin}_{\mathcal{A}}(\beta)$ can be performed in parallel then $\#\mathcal{A} \geqslant \lceil \beta \rceil$.*

Remark 18. The inequality $\#\mathcal{A} \geqslant \lceil \beta \rceil$ guarantees that $\mathrm{Fin}_{\mathcal{A}}(\beta)$ is dense in $\mathbb{R}^+$ or in $\mathbb{R}$, depending on the fact whether the digits of $\mathcal{A}$ are non-negative. This property is very important, as it enables us to approximate each positive real number (resp. real number) by an element from $\mathrm{Fin}_{\mathcal{A}}(\beta)$ with arbitrary accuracy.

When β is an algebraic integer, and not only an algebraic number, we can obtain another lower bound on the cardinality of alphabet for parallelism:

Theorem 19. *Let β, with $|\beta| > 1$, be an algebraic integer with minimal polynomial $F(X)$. Let $\mathcal{A}$ be an alphabet of contiguous integers containing 0 and 1. If addition in $\mathrm{Fin}_{\mathcal{A}}(\beta)$ is computable in parallel, then $\#\mathcal{A} \geqslant |F(1)|$. If, moreover, β is a positive real number, $\beta > 1$, then $\#\mathcal{A} \geqslant |F(1)| + 2$.*

We have designed parallel algorithms for addition in well studied number systems in [9], [7]. The results are summarized in the table below. The canonical alphabet is the one which is sufficient to represent all the elements of $\mathbb{R}^+$, $\mathbb{R}$ or $\mathbb{C}$ according to the base.

V. Block parallel addition

In [13] Kornerup has proposed a more general concept of parallel addition. Instead of manipulating single digits, one works with blocks of fixed length k. So the classical parallel addition is just k-block parallel addition with $k = 1$.

We have investigated in [7] how the Kornerup's generalization influences the relationship between the base and the alphabet for parallel addition, in the hope of reducing the size of the alphabet. For instance consider the Penney number system with the complex base $\beta = -1 + \imath$, see [17]. We know that 1-block parallel addition in base $-1 + \imath$ requires an alphabet of cardinality at least 5, whereas Herreros in [12]

Base	Canonical alphabet	Minimal alphabet for parallel addition
$b \in \mathbb{N}$, $b \geqslant 2$	$\{0, \ldots, b-1\}$	All alphabets of size $b+1$
$-b$, $b \in \mathbb{N}$, $b \geqslant 2$	$\{0, \ldots, b-1\}$	All alphabets of size $b+1$
$\sqrt[n]{b}$, $b \in \mathbb{N}$, $b \geqslant 2$		All alphabets of size $b+1$
$-1+\imath$	$\{0,1\}$	All alphabets of size 5
$2\imath$	$\{0, \ldots, 3\}$	All alphabets of size 5
$\imath\sqrt{2}$	$\{0,1\}$	All alphabets of size 3
$\beta^2 = a\beta - 1$, $a \in \mathbb{N}$, $a \geqslant 3$	$\{0, \ldots, a-1\}$	All alphabets of size a
$\beta^2 = a\beta + b$, $a, b \in \mathbb{N}$, $a \geqslant b \geqslant 1$	$\{0, \ldots, a\}$	All alphabets of size $a+b+1$
a/b, $a, b \in \mathbb{N}$, $a > b \geqslant 1$	$\{0, \ldots, a-1\}$	$\{0, \ldots, a+b-1\}$, $\{-a-b+1, \ldots, 0\}$, and all alphabets of size $a+b$ containing $\{-b, \ldots, 0, \ldots, b\}$
$-a/b$, $a, b \in \mathbb{N}$, $a > b \geqslant 1$	$\{0, \ldots, a-1\}$	All alphabets of size $a+b$

gives an algorithm for 4-block parallel addition on the alphabet $\{-1, 0, 1\}$.

In the case where β is a positive real number, we have more results. First we take a base which is a simple Parry number.

Theorem 20. *Let $d_\beta(1) = t_1 t_2 \cdots t_m$ with $1 \leqslant t_m \leqslant t_i$ for $1 \leqslant i < m$ be the Rényi expansion of 1 in base β. If block parallel addition can be performed on alphabet $\mathcal{A} = \{0, 1, \ldots, M\}$, then $M \geqslant t_1 + t_m$.*

The lower bound on the cardinality of the alphabet in Theorem 20 is sharp, i.e. can be attained, as it is the case when β is the positive root of the equation $X^2 = aX + b$ $a \geqslant b \geqslant 1$ (see the table above).

We now consider the case where the base is a non-simple Parry number.

Theorem 21. *Let $d_\beta(1) = t_1 t_2 \cdots t_m (t_{m+1} t_{m+2} \cdots t_{m+p})^\omega$ be the Rényi expansion of 1. Let the coefficients $t_1, \ldots, t_{m+p}$ satisfy one of the following assumptions:*

1) *$m = p = 1$;*
2) *$m = 1$ and $t_2 > t_k$ for all k such that $2 < k \leqslant m+p$;*
3) *$m \geqslant 2$ and $t_2 \geqslant t_k$ for all k such that $2 \leqslant k \leqslant m$ and $t_2 > t_k$ for all k such that $m+1 \leqslant k \leqslant m+p$.*

If block parallel addition can be performed on alphabet $\mathcal{A} = \{0, 1, \ldots, M\}$, then $M \geqslant 2t_1 - t_2 - 1$.

The bound on the cardinality of alphabet in Theorem 21 is sharp, as shown by the quadratic case.

Proposition 22. *Let β be the root > 1 of $X^2 - aX + b$, where $a \geqslant b+2$, $b \geqslant 1$. Then $d_\beta(1) = (a-1)(a-b-1)^\omega$. Parallel addition is possible on $\mathcal{A} = \{0, \ldots, a+b-2\}$.*

A number $\beta > 1$ is said to *satisfy the (PF) Property* if the sum of any two positive numbers with finite greedy β-expansion in base β has its greedy β-expansion finite as well, [11].

Proposition 23. *Let $\beta > 1$ be a number with Property (PF). Then there exists k such that k-block parallel addition is possible on the alphabet $\{0, 1, \ldots, 2\lfloor\beta\rfloor\}$ and on the alphabet $\{-\lfloor\beta\rfloor, \ldots, 0, \ldots, \lfloor\beta\rfloor\}$.*

Using Theorems 20 and 21 and families of numbers satisfying Property (PF), see [11], we obtain the two following results.

Corollary 24. *Let $d_\beta(1) = t_1 t_2 \cdots t_m$ with $t_1 \geqslant t_2 \geqslant \cdots \geqslant t_m \geqslant 1$ be the Rényi expansion of 1. Then there exists $M \in \mathbb{N}$ such that parallel addition by a k-block local function is possible on the alphabet $\{0, 1, \ldots, M\}$ and $t_1 + t_m \leqslant M \leqslant 2t_1$.*

Corollary 25. *Let $d_\beta(1) = t_1 t_2 \cdots t_m t^\omega$ with $t_1 > t_2 \geqslant t_3 \geqslant \cdots \geqslant t_m > t \geqslant 1$ be the Rényi expansion of 1. Then there exists $M \in \mathbb{N}$ such that parallel addition by a k-block local function is possible on the alphabet $\{0, 1, \ldots, M\}$ and $2t_1 - t_2 - 1 \leqslant M \leqslant 2t_1$.*

We end this paper by considering a generalization of the Golden Mean. The root > 1 of the polynomial $X^d - X^{d-1} - X^{d-2} - \cdots - X - 1$ is called a *d-bonacci number*.

Corollary 26. *Let β be a d-bonacci number.*

- *If the alphabet $\mathcal{A}$ allows 1-block parallel addition, then $\#\mathcal{A} \geqslant d+1$.*
- *There exists k such that k-block parallel addition is possible on the alphabets $\{0, 1, 2\}$ and $\{-1, 0, 1\}$ and these alphabets cannot be reduced.*

Unfortunately the parameter k can be quite large: for instance, when $d = 3$ — the so-called Tribonacci number system — k is equal to 14.

VI. Conclusion

The design of a parallel addition in a given base β requires to take into consideration the following parameters of the algorithm:

1) the size of the used alphabet $\mathcal{A}$,

2) the width p of the sliding window, i.e., the number p appearing in the definition of the p-local function Φ,

3) the length k of the blocks in which are grouped the digits of $\mathcal{A}$ for k-block parallel addition.

There are mathematical reasons (for example comparison of numbers) and even more technical reasons to minimize all these three parameters. Intuitively, the smaller is one of the parameters, the bigger have to be the others. The question of the relationship between the values $\#\mathcal{A}$, p and k is far from being answered. The example of the Golden Mean shows that the writing of a parallel addition algorithm working on an alphabet of minimal size is not straightforward, and heavily

depends on the properties of the base, contrarily to Algorithms S and W that are more general.

As said in Remark 4, in integer base k-block parallel addition with $k \geqslant 2$ is not interesting from the point of view of the minimality of the cardinality of the alphabet. However grouping digits in k-blocks can allow a simpler parallel algorithm. For instance, in base 2, 1-block parallel addition is doable on the minimal alphabet $\mathcal{A} = \{-1, 0, 1\}$ by the algorithm of Chow and Robertson, and the associated local function Φ is 3-local. But 2-block addition is just addition base 4 on $\mathcal{A}_{(2)} = \{-3, \ldots, 0, \ldots, 3\}$, and is performable by the simpler algorithm of Avizienis which gives a 2-local function.

The most common reason why to work in number system with an algebraic base β instead of a system with base 2 or 10 consists in the requirement of performing precise computations in the algebraic field $\mathbb{Q}(\beta)$. If the base β is not "nice enough", we can choose another base γ such that $\mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$ and work in the number system with the base γ. The question is which base in $\mathbb{Q}(\beta)$ is "nice enough" and how to find it effectively.

ACKNOWLEDGEMENTS

The second author acknowledges financial support by the Grant Agency of the Czech Technical University in Prague, grant SGS11/162/OHK4/3T/14. The third and fourth authors acknowledge financial support by the Czech Science Foundation grant 13-03538S.

REFERENCES

[1] A. Avizienis, Signed-digit number representations for fast parallel arithmetic, *IRE Trans. Electron. Comput.* **10** (1961) 389–400.
[2] A. Burks, H. H. Goldstine, and J. von Neumann, Preliminary discussion of the logic design of an electronic computing instrument, Institute for Advanced Study, Princeton, NJ, 1946.
[3] A. Cauchy, Sur les moyens d'éviter les erreurs dans les calculs numériques, *C.R. Acad. Sc. Paris* série I **11** (1840) 789–798.
[4] C.Y. Chow, J.E. Robertson, Logical design of a redundant binary adder, in *Proc. 4th IEEE Symposium on Computer Arithmetic* (1978) 109–115.
[5] M. D. Ercegovac and T. Lang, *Digital Arithmetic*, Morgan Kaufmann, 2004.
[6] Ch. Frougny, On-line finite automata for addition in some numeration systems, *RAIRO-Theor. Inf. Appl.* **33** (1999) 79–101.
[7] Ch. Frougny, P. Heller, E. Pelantová, and M. Svobodová, k-block parallel addition versus 1-block parallel addition in non-standard numeration systems, *ArXiv* (2013), Article 1312.4858.
[8] Ch. Frougny, E. Pelantová, and M. Svobodová, Parallel addition in non-standard numeration systems, *Theor. Comput. Sci.* **412** (2011) 5714–5727.
[9] Ch. Frougny, E. Pelantová, and M. Svobodová, Minimal Digit Sets for Parallel Addition in Non-Standard Numeration Systems, *Journal of Integer Sequences* **16** (2013), Article 13.2.17.
[10] Ch. Frougny and J. Sakarovitch, Number representation and finite automata, in V. Berthé, M. Rigo, eds., *Combinatorics, Automata and Number Theory*, Encyclopedia of Mathematics and its Applications, Vol. 135, Cambridge University Press, 2010, Chapter 2, pp. 34–107.
[11] Ch. Frougny and B. Solomyak, Finite beta-expansions, *Ergodic Theory & Dynamical Systems* **12** (1992) 713–723.
[12] Y. Herreros, Contribution à l'arithmétique des ordinateurs, Ph. D. dissertation, Institut National Polytechnique de Grenoble, 1991.
[13] P. Kornerup, Necessary and sufficient conditions for parallel, constant time conversion and addition, in *Proc. 14th IEEE Symposium on Computer Arithmetic*, (1999) 152–155.
[14] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications 90, Cambridge University Press, 2002.
[15] B. Parhami, On the implementation of arithmetic support functions for generalized signed-digit number systems, *IEEE Trans. Computers* **42** (1993), 379–384.
[16] W. Parry, On the β-expansions of real numbers, *Acta Math. Acad. Sci. Hungar.* **11** (1960) 401–416.
[17] W. Penney, A "binary" system for complex numbers, *J. ACM* **12** (1965) 247–248.
[18] A. Rényi, Representations for real numbers and their ergodic properties, *Acta Math. Acad. Sci. Hungar.* **8** (1957) 477–493.