On-line multiplication and division in real and complex bases

Marta Brzicová, Christiane Frougny, Edita Pelantová, Milena Svobodová

FNSPE, CTU Prague, Czech Republic
IRIF, UMR 8243 CNRS & Université Paris-Diderot, France

ARITH 23
July 10-13, 2016
Silicon Valley, USA

Contents

- Positional numeration systems
- Parallel and on-line algorithms
- On-line $\boxtimes$ and $\boxdiv$ by algorithms of Trivedi & Ercegovac
- On-line property
- On-line $\boxtimes$ and $\boxdiv$ for $\mathbb{R}$ and $\mathbb{C}$ numeration systems
- Pre-processing of divisor
- Linear time complexity

Positional Numeration Systems

Positional numeration system $(\beta, \mathcal{A})$

- Base β, $|\beta| > 1$: not just $\beta \in \mathbb{Z}^+, \mathbb{Z}$, but also $\beta \in \mathbb{R}, \mathbb{C}$;
- finite set of digits - Alphabet $\mathcal{A} \ni 0$:
  - not just $\mathcal{A} \subset \mathbb{Z}$ - set of contiguous integers,
  - but also $\mathcal{A} \subset \mathbb{Z}[\beta] = \{\sum_{k=0}^{-n} z_k \beta^{-k} \mid z_k \in \mathbb{Z}\} \subset \mathbb{R}, \mathbb{C}$.

Finite representation of a number $X \in \mathbb{C}$ in the system $(\beta, \mathcal{A})$:

$\mathbf{X = x_{-n} \cdots x_0 \bullet x_1 \cdots x_m}$ stands for $X = \sum_{k=m}^{-n} x_k \beta^{-k}$, with $x_k \in \mathcal{A}$.

Ideal properties of a numeration system $(\beta, \mathcal{A})$

A desired numeration system $(\beta, \mathcal{A})$ has:

- operations of Addition and Subtraction doable in parallel,
- operations of Multiplication and Division doable on-line,
- Divisor Pre-processing algorithm available, and
- all these operations of (at most) linear time complexity.

Parallel and on-line algorithms

For numeration systems $(\beta, \mathcal{A})$ and $(\beta, \mathcal{B})$, mapping $\phi : \mathcal{B}^* \mapsto \mathcal{A}^*$, where the digits of result $\mathbf{V} = \phi(\mathbf{U})$ are obtained:

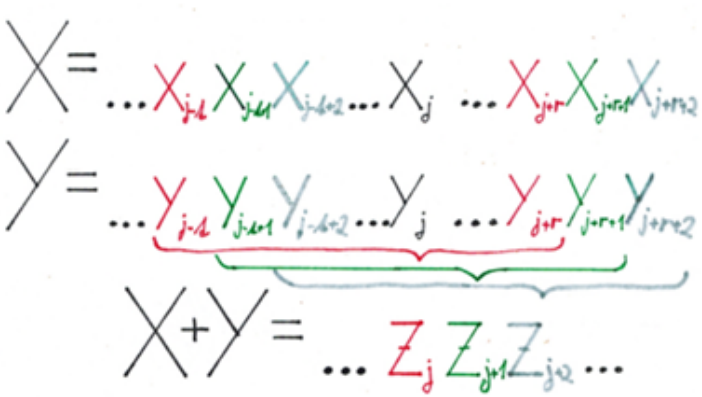
- in parallel: via sliding block code, or p-local function ($p = r + t + 1$)

$$v_j = \varphi(u_{j-t}, \ldots, u_j, \ldots, u_{j+r})$$
$$z_j = \varphi((x_{j-t}, y_{j-t}), \ldots, (x_j, y_j), \ldots, (x_{j+r}, y_{j+r}))$$

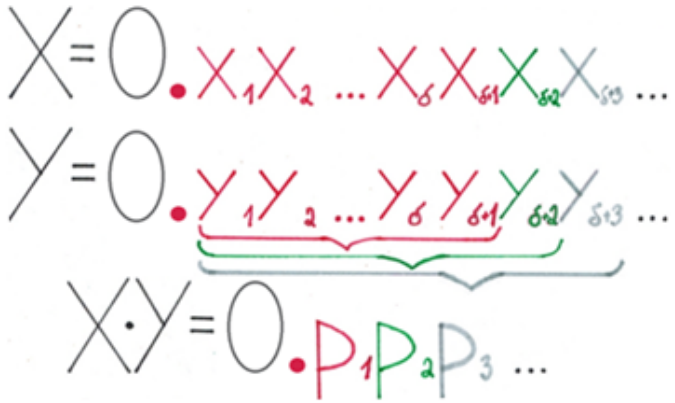
- on-line: with a delay δ

$$v_j = \varphi(u_1, \ldots, u_j, \ldots, u_{j+\delta})$$
$$p_j = \varphi((x_1, y_1), \ldots, (x_j, y_j), \ldots, (x_{j+\delta}, y_{j+\delta}))$$

in parallel



on-line



Both **parallel** and **on-line** algorithms require **redundancy** of $(\beta, \mathcal{A})$.

Algorithms of K.Trivedi & M.Ercegovac

For on-line $\boxtimes$ and $\boxdiv$, denote $Z_k = \bullet z_1 z_2 \dots z_k$ for $Z = \bullet z_1 z_2 \dots$ in $(\beta, \mathcal{A})$:

On-line multiplication $\boxtimes$: $X \cdot Y = P$

- from $X = \bullet x_1 x_2 \cdots$ and $Y = \bullet y_1 y_2 \cdots$, with $x_j, y_j = 0$ for $j = 1, ..., \delta$,
- iterate for $k = 1, 2, \dots$:
  - $W_k := \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$
  - $p_k := \mathrm{Select}_M(W_k) \in \mathcal{A}$
- ensuring $(X_k Y_k - P_{k-1}) = \beta^{-k} W_k$

On-line division $\boxdiv$: $N/D = Q$

- from $N = \bullet n_1 n_2 \cdots$ and $D = \bullet d_1 d_2 \cdots$, with $n_j = 0$ for $j = 1, ..., \delta$
- iterate for $k = 1, 2, \dots$:
  - $W_k := \beta(W_{k-1} - q_{k-1} D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$
  - $q_k := \mathrm{Select}_D(W_k, D_{k+\delta}) \in \mathcal{A}$
- ensuring $N_{k+\delta}/D_{k+\delta} - Q_{k-1} = \beta^{-k} W_k / D_{k+\delta}$

(P_k), (Q_k) converge to $P = XY$ and $Q = N/D$ if:

- the sequences (W_k) are bounded, for both $\boxtimes$ and $\boxdiv$, and
- each divisor D on $\boxdiv$ input fulfils $|D_k| \geq D_{min} > 0$ for any $k \in \mathbb{Z}^+$.

On-line property

- Originally: on-line $\boxtimes$, $\boxdiv$ algo's proposed for integer bases $\beta \in \mathbb{Z}^+$ and symmetric integer alphabets $\mathcal{A} = \{-M, \ldots, 0, \ldots, M\} \subset \mathbb{Z}$.
- Newly: extension to a broader set of numeration systems:

On-line (OL) property of $(\beta, \mathcal{A})$

Numeration system $(\beta, \mathcal{A})$ is said to possess the (OL) property if there exist $\varepsilon > 0$ and a bounded set $I \subset \mathbb{C}$ (or $\mathbb{R}$) satisfying: $0 \in I$, and

$$\forall\ Z \in\ \varepsilon\text{−neighborhood of } (\beta I) \quad \exists\ a \in \mathcal{A} \quad \text{such that } B(Z, \varepsilon) \subset I + a,$$

where $B(Z, \varepsilon)$ is the (real or complex) ball of center Z and radius ε.

(OL) property $\Rightarrow$ sequences (W_k) bounded $\Rightarrow$ on-line algo's converge:

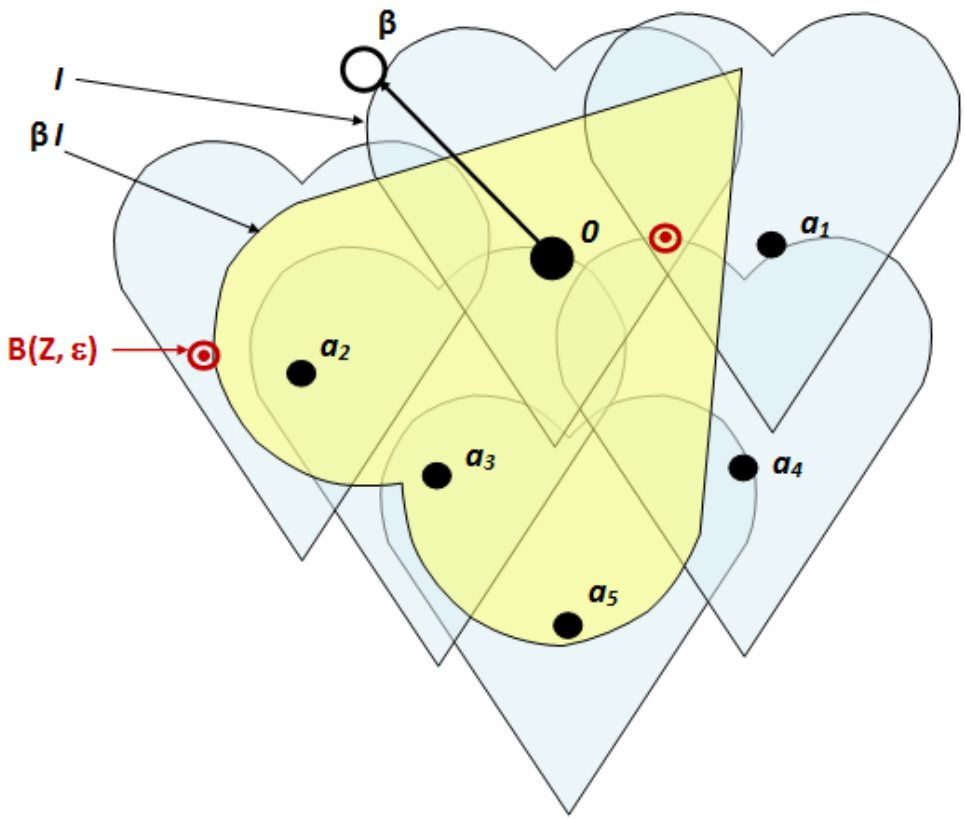
On-line $\boxtimes$, $\boxdiv$ due to (OL) property

Let $(\beta, \mathcal{A})$ possess the (OL) property and the $D_{min} > 0$. $\Rightarrow$ Then $\boxtimes$ and $\boxdiv$ can be performed on-line by the Trivedi-Ercegovac algorithms.

On-line property

? Given $(\beta, \mathcal{A})$: How to assess the (OL) property, and find ε and I fulfilling:

$\forall\ Z \in\ \varepsilon-$neighborhood of $(\beta I)\quad \exists\ a \in \mathcal{A}\quad$ such that $B(Z, \varepsilon) \subset I + a$



Note: The ε-wide overlaps between neighboring copies $(I + a_j)$ and $(I + a_k)$ allow to reach linear time complexity of the algorithms.

(OL) property - results: $\beta \in \mathbb{R}$ and $\mathcal{A} \subset \mathbb{Z}$

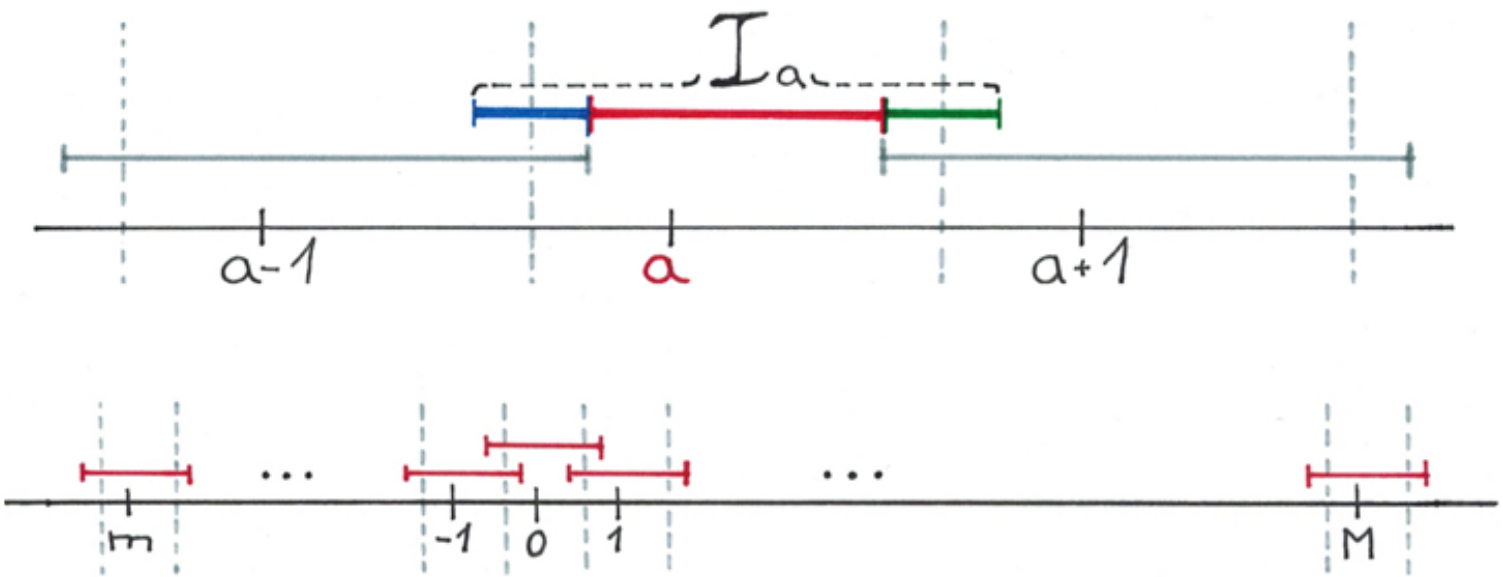
Theorem: (OL) property for real bases

Let $\beta \in \mathbb{R}$ have $|\beta| > 1$, and $\{m, \ldots, 0, \ldots, M\} = \mathcal{A} \subset \mathbb{Z}$.

If $\#\mathcal{A} > |\beta|$, then $(\beta, \mathcal{A})$ has the (OL) property.

Consequently, multiplication and division in $(\beta, \mathcal{A})$ are performable on-line by the Trivedi – Ercegovac algorithms, if $\exists D_{min} > 0$ for division.

(OL) property for a real base with integer alphabet



(OL) property - results: $\beta \in \mathbb{C}$ and $\mathcal{A} \subset \mathbb{Z}$

Theorem: (OL) property for complex bases

Let $\beta \in \mathbb{C} \setminus \mathbb{R}$ have $|\beta| > 1$, and $\{-M, \ldots, 0, \ldots, M\} = \mathcal{A} \subset \mathbb{Z}$.

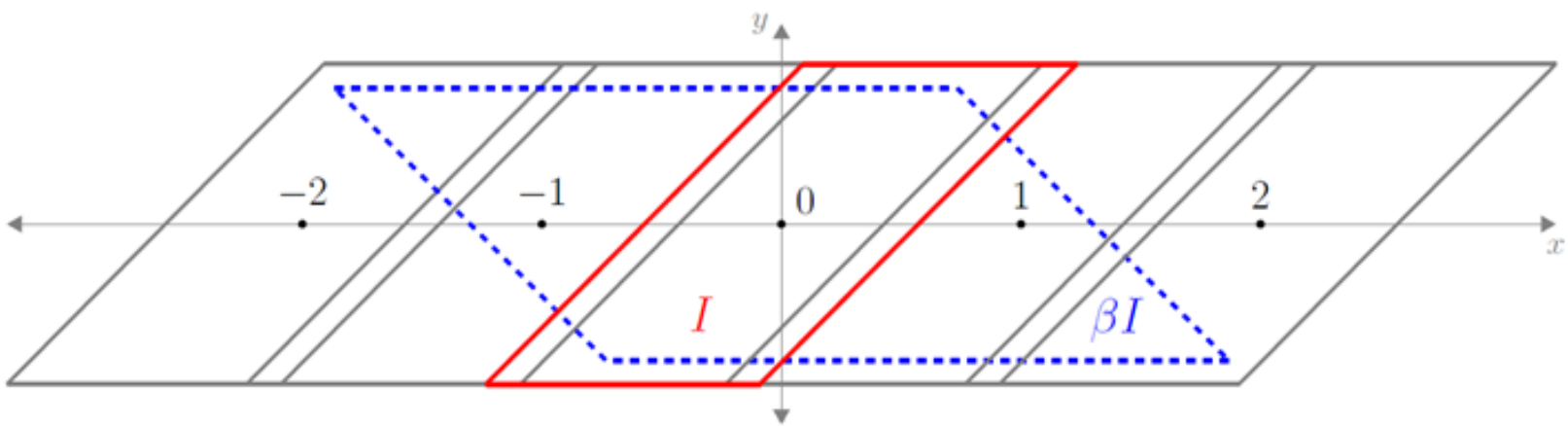
If $\#\mathcal{A} > \beta\overline{\beta} + |\beta + \overline{\beta}|$, then $(\beta, \mathcal{A})$ has the (OL) property.

Consequently, multiplication and division in $(\beta, \mathcal{A})$ are performable on-line by the Trivedi – Ercegovac algorithms, if $\exists D_{min} > 0$ for division.

This way, we find integer alphabets to fulfil the (OL) property for:

- Penney base $\beta = \imath - 1$: $\#\mathcal{A} > \beta\overline{\beta} + |\beta + \overline{\beta}| = 4$
- Eisenstein base $\beta = \omega - 1 = \exp\frac{2\pi\imath}{3} - 1$: $\#\mathcal{A} > \beta\overline{\beta} + |\beta + \overline{\beta}| = 6$

(OL) property for Penney base $\beta = i\text{-}1$ with integer alphabet



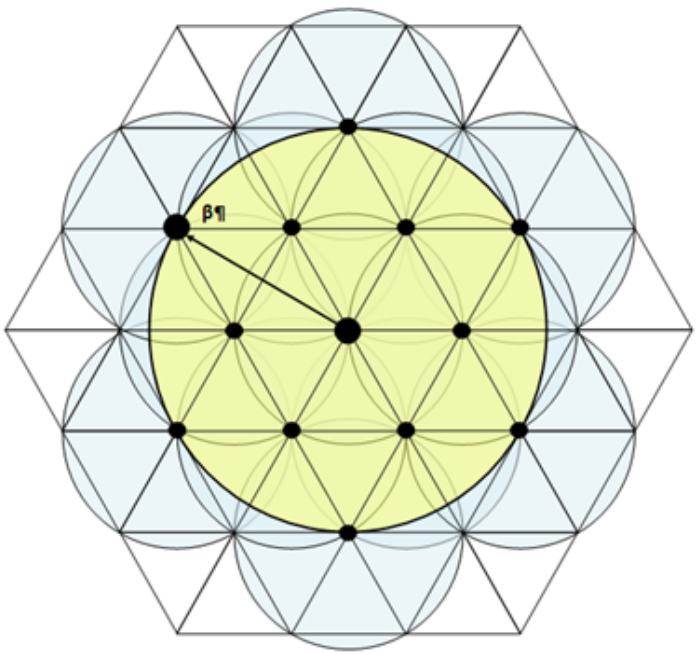
(OL) property - results: $\beta \in \mathbb{C}$ and $\mathcal{A} \subset \mathbb{C}$

For any given base $\beta \in \mathbb{C}$, with $|\beta| > 1$, we can always set an alphabet $\mathcal{A} \subset \mathbb{C}$ allowing on-line $\boxtimes$ and $\boxdiv$, e.g. as follows:

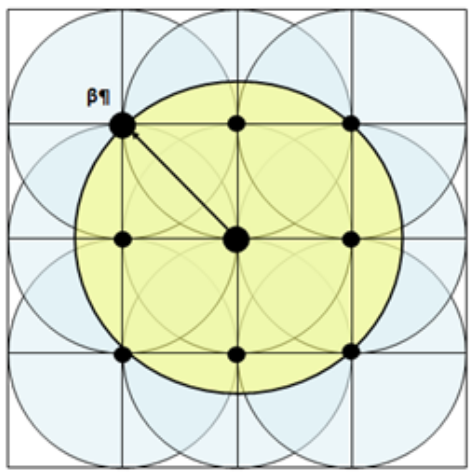
$$\mathcal{A} = \{a \in \mathbb{Z}[i] \,|\, B(a,1) \cap B(0,|\beta|) \neq \emptyset\} \quad \text{with} \quad I = B(0,1)$$

... or with other sets $I = B(0,r)$ and lattices $\mathbb{Z}[\beta] \supset \mathcal{A}$ for specific bases:

Eisenstein base β = ω-1, complex alphabet



Penney base β = i-1, complex alphabet



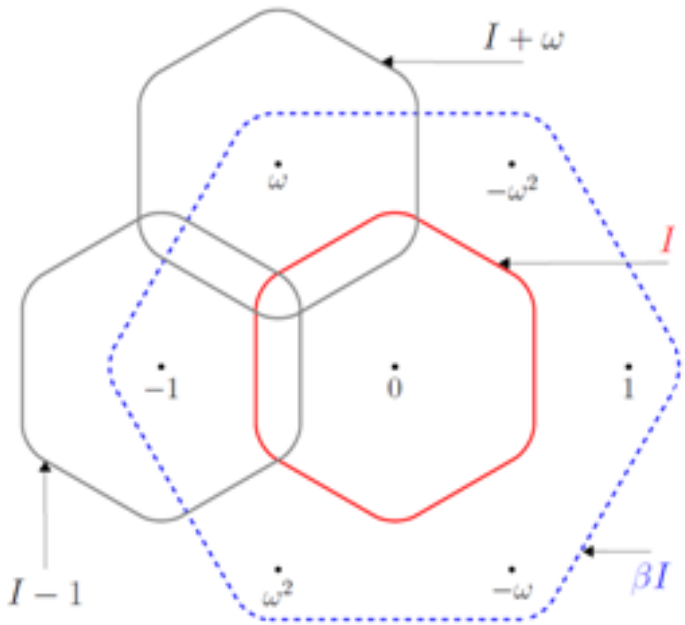
$\Uparrow$ But the alphabets selected in this way are too big !

(OL) property - results: $\beta \in \mathbb{C}$ and $\mathcal{A} \subset \mathbb{C}$

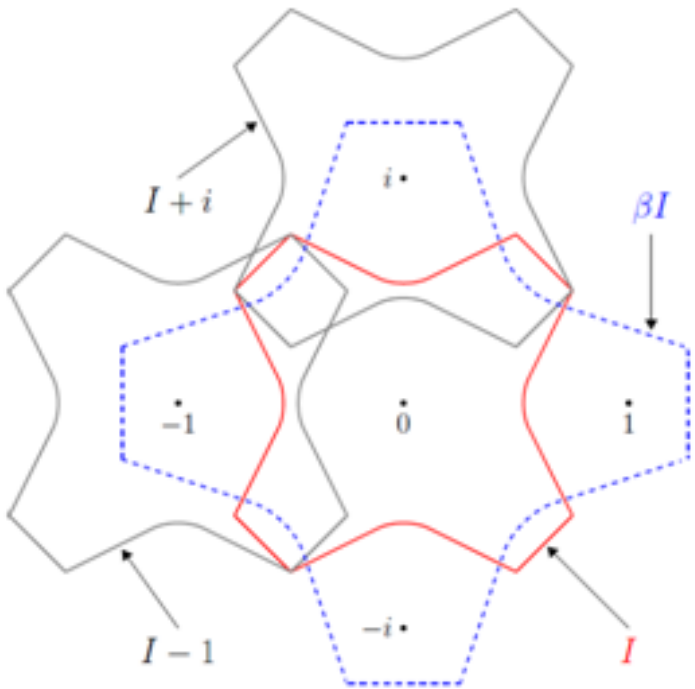
In the specific cases, we find the set $I \subset \mathbb{C}$ for (OL) property with much smaller alphabets, by individual approach:

- Eisenstein base $\beta = \omega - 1$, where $\omega = \exp \frac{2\pi\imath}{3}$,
  with alphabet $\{0, \pm 1, \pm\omega, \pm\omega^2\} = \mathcal{A} \subset \mathbb{Z}[\omega]$ of size $\#\mathcal{A} = 7$;
- Penney base $\beta = \imath - 1$,
  with alphabet $\{0, \pm 1, \pm\imath\} = \mathcal{A} \subset \mathbb{Z}[\imath]$ of size $\#\mathcal{A} = 5$.

Eisenstein base β = ω-1, complex alphabet



Penney base β = *i*-1, complex alphabet



Pre-processing of divisor D in $(\beta, \mathcal{A})$

$(\beta, \mathcal{A})$ must have a constant $D_{min} > 0$ such that each divisor D on $\boxplus$ input fulfils $|D_k| = |\sum_{j=1}^{k} d_j \beta^{-j}| \geq D_{min}$, after **pre-processing** by:

- **shifting the fractional point** to the most significant digit, or
- applying convenient **rewriting rules** from a pre-defined set.

$(\beta, \mathcal{A})$ allows pre-processing if $\exists D_{min} > 0$ such that $\forall \bullet d_1 d_2 d_3 \cdots \in \mathcal{A}^{\mathbb{N}}$:

1. either $|\bullet d_1 d_2 d_3 \cdots d_k| \geq D_{min}$ for all $k \in \mathbb{N}$,
2. or there exists $j \in \mathbb{N}$ such that for some string $\tilde{d}_2 \tilde{d}_3 \cdots \tilde{d}_j \in \mathcal{A}^*$
$$\bullet d_1 d_2 d_3 \cdots d_j = \bullet 0 \tilde{d}_2 \tilde{d}_3 \cdots \tilde{d}_j \quad \leftarrow \quad \text{rewriting rule}$$

Examples: rewriting rules for pre-processing

- $\beta = 4$, $\mathcal{A} = \{\overline{2}, \overline{1}, 0, 1, 2\}$: no rewriting rules needed
- $\beta = 2$, $\mathcal{A} = \{\overline{1}, 0, 1\}$: rewriting rules $\pm\{\bullet 1(-1) = \bullet 01\}$
- $\beta^2 = \beta + 1$, $\mathcal{A} = \{\overline{1}, 0, 1\}$: rewriting rules
$\pm\{\bullet 10(-1) = \bullet 010, \bullet 1(-1)0 = \bullet 001, \bullet 1(-1)(-1) = \bullet 000\}$

Linear time complexity

Goal: obtain the n-th digit of the result with $O(n)$ **time complexity**.

- $W_k := \beta(W_{k-1} - p_{k-1}) + (x_k Y_{k-1} + y_k X_k)$
- $p_k := \mathrm{Select}_M(W_k) \in \mathcal{A}$
- $W_k := \beta(W_{k-1} - q_{k-1} D_{k-1+\delta}) + \beta^{-\delta}(n_{k+\delta} - Q_{k-1} d_{k+\delta})$
- $q_k := \mathrm{Select}_D(W_k, D_{k+\delta}) \in \mathcal{A}$

Besides the properties already required from numeration system $(\beta, \mathcal{A})$:

- parallel $\boxplus$ and $\boxminus$,
- on-line $\boxtimes$ and $\boxdiv$, and
- pre-processing of divisor,

we also need to process the Select functions in constant time:

- normalize representations of interim variables (W_k) from left side: by applying the same rewriting rules as for divisor pre-processing;
- evaluate just truncated representations of $(W_k), (D_k)$ from right side: as of a suitably fixed position.

Linear time complexity

Additionally, an alphabet $\mathcal{A} = \mathcal{A} \cdot \mathcal{A}$ closed under multiplication would greatly speed up calculation of (W_k) - such as:

- base $\beta = 2$ with alphabet $\mathcal{A} = \{0, \pm 1\}$
- base $\beta^2 = \beta + 1$ with alphabet $\mathcal{A} = \{0, \pm 1\}$
- Penney base $\beta = \imath - 1$ with alphabet $\mathcal{A} = \{0, \pm 1, \pm \imath\}$
- Eisenstein base $\beta = \omega - 1$ with alphabet $\mathcal{A} = \{0, \pm 1, \pm \omega, \pm \omega^2\}$