Konstrukce algoritmů pro paralelní sčítání

Jan Legerský

TIGR
jan.legersky@gmail.com

Obhajoba výzkumného úkolu

10. září 2015

Poziční soustava

Algebraické celé číslo ω stupně d.

$$\mathbb{Z}[\omega] = \left\{ \sum_{j=0}^{d-1} a_j \omega^j \ : a_j \in \mathbb{Z} \right\}$$

Poziční soustava

Algebraické celé číslo ω stupně d.

$$\mathbb{Z}[\omega] = \left\{ \sum_{j=0}^{d-1} a_j \omega^j \ : a_j \in \mathbb{Z} \right\}$$

Poziční soustava je dána

- bází $\beta \in \mathbb{Z}[\omega]$, $|\beta| > 1$ a
- abecedou $\mathcal{A} \subset \mathbb{Z}[\omega], 0 \in \mathcal{A}$.

Poziční soustava

Algebraické celé číslo ω stupně d.

$$\mathbb{Z}[\omega] = \left\{ \sum_{j=0}^{d-1} a_j \omega^j \ : \ a_j \in \mathbb{Z} \right\}$$

Poziční soustava je dána

- bází $\beta \in \mathbb{Z}[\omega]$, $|\beta| > 1$ a
- abecedou $\mathcal{A} \subset \mathbb{Z}[\omega], 0 \in \mathcal{A}$.

Komplexní číslo x má konečnou $(\beta, \mathcal{A})$-reprezentaci, pokud $x = \sum_{j=-m}^{n} x_j \beta^j$ s koeficienty $x_j \in \mathcal{A}$.

$$(x)_{\beta,\mathcal{A}} = x_n x_{n-1} \cdots x_1 x_0 \bullet x_{-1} x_{-2} \cdots x_{-m}$$

Sčítání

$$\begin{array}{r}
(x)_{\beta,\mathcal{A}} = \; x_{n'}\; x_{n'-1} \cdots x_1\; x_0 \bullet x_{-1}\; x_{-2}\; \cdots x_{-m'} \\
(y)_{\beta,\mathcal{A}} = \; y_{n'}\; y_{n'-1} \cdots y_1\; y_0 \bullet y_{-1}\; y_{-2}\; \cdots y_{-m'} \\
\hline
(w)_{\beta,\mathcal{A}+\mathcal{A}} = w_{n'} w_{n'-1} \cdots w_1 w_0 \bullet w_{-1} w_{-2} \cdots w_{-m'}\,,
\end{array}$$

kde

$$w_j = x_j + y_j \in \mathcal{A} + \mathcal{A}\,.$$

Sčítání

$$\begin{array}{r}
(x)_{\beta,\mathcal{A}} = \ x_{n'}\ x_{n'-1} \cdots x_1\ x_0 \bullet x_{-1}\ x_{-2}\ \cdots x_{-m'} \\
(y)_{\beta,\mathcal{A}} = \ y_{n'}\ y_{n'-1} \cdots y_1\ y_0 \bullet y_{-1}\ y_{-2}\ \cdots y_{-m'} \\
\hline
(w)_{\beta,\mathcal{A}+\mathcal{A}} = w_{n'} w_{n'-1} \cdots w_1 w_0 \bullet w_{-1} w_{-2} \cdots w_{-m'} \,,
\end{array}$$

kde

$$w_j = x_j + y_j \in \mathcal{A} + \mathcal{A} \,.$$

Chceme najít $(\beta, \mathcal{A})$-reprezentaci součtu

$$z_n z_{n-1} \cdots z_1 z_0 \bullet z_{-1} z_{-2} \cdots z_{-m} = (w)_{\beta,\mathcal{A}} \,.$$

$$R(x) = x - \beta \implies 0 = R(\beta) = \beta - \beta$$

$$\implies 0 = q_j \beta^j \cdot R(\beta) = q_j \cdot \beta^{j+1} - \beta q_j \cdot \beta^j$$

$$R(x) = x - \beta \implies 0 = R(\beta) = \beta - \beta$$

$$\implies 0 = q_j \beta^j \cdot R(\beta) = q_j \cdot \beta^{j+1} - \beta q_j \cdot \beta^j$$

$$\begin{array}{ccccccc}
w_{n'}\, w_{n'-1} & \cdots & w_{j+1} & {\color{red} w_j} & w_{j-1} & \cdots & w_1\, w_0 \bullet \\
 & & & & q_{j-2} & \iddots & \\
 & & & {\color{red} q_{j-1}} & -\beta q_{j-1} & & \\
 & & q_j & {\color{red} -\beta q_j} & & & \\
 & \iddots & -\beta q_{j+1} & & & & \\
\hline
z_n \cdots z_{n'}\, z_{n-1} & \cdots & z_{j+1} & {\color{red} z_j} & z_{j-1} & \cdots & z_1\ z_0 \bullet
\end{array}$$

$$R(x) = x - \beta \implies 0 = R(\beta) = \beta - \beta$$

$$\implies 0 = q_j \beta^j \cdot R(\beta) = q_j \cdot \beta^{j+1} - \beta q_j \cdot \beta^j$$

$$\begin{array}{ccccccc}
w_{n'} w_{n'-1} & \cdots & w_{j+1} & w_j & w_{j-1} & \cdots & w_1 w_0 \bullet \\
 & & & & q_{j-2} & \cdot^{\cdot^{\cdot}} & \\
 & & & q_{j-1} & -\beta q_{j-1} & & \\
 & & q_j & -\beta q_j & & & \\
 & \cdot^{\cdot^{\cdot}} & -\beta q_{j+1} & & & & \\
\hline
z_n \cdots z_{n'} z_{n-1} & \cdots & z_{j+1} & z_j & z_{j-1} & \cdots & z_1 \ z_0 \bullet
\end{array}$$

Jak volit váhový koeficient q_j tak, aby

$$z_j = w_j + q_{j-1} - q_j \beta \in \mathcal{A}\,?$$

$$z_j = w_j + q_{j-1} - q_j\beta$$

Standardní sčítání:

$$\begin{array}{rl} w_n w_{n-1} \cdots w_{j+1} w_j w_{j-1} \cdots w_1 w_0 \bullet & , w_i \in \mathcal{A} + \mathcal{A}, \\ \longrightarrow z_{n+1}\, z_n\, z_{n-1}\, \cdots z_{j+1} z_j\, z_{j-1}\, \cdots\, z_1\, z_0 \bullet & , z_i \in \mathcal{A}. \end{array}$$

$$z_j = w_j + q_{j-1} - q_j\beta$$

Standardní sčítání:

$$\begin{array}{rl} w_n w_{n-1} \cdots w_{j+1} w_j w_{j-1} \cdots w_1 w_0 \bullet & , w_i \in \mathcal{A} + \mathcal{A}, \\ \longrightarrow z_{n+1}\ z_n\ z_{n-1}\ \cdots z_{j+1} z_j\ z_{j-1}\ \cdots\ z_1\ z_0 \bullet & , z_i \in \mathcal{A}. \end{array}$$

Paralelní sčítání (Avizienis, 1961):

$$\begin{array}{rl} \cdots w_{j+t+1} w_{j+t} \cdots w_{j+1} w_j w_{j-1} \cdots w_{j-r} w_{j-r-1} \cdots & , w_i \in \mathcal{A} + \mathcal{A}, \\ \longrightarrow \cdots z_{j+t+1}\ z_{j+t}\ \cdots\ z_{j+1} z_j\ z_{j-1}\ \cdots z_{j-r}\ z_{j-r-1}\ \cdots & , z_i \in \mathcal{A}. \end{array}$$

$$z_j = w_j + q_{j-1} - q_j\beta$$

Standardní sčítání:

$$\begin{array}{ll} w_n w_{n-1} \cdots w_{j+1} w_j w_{j-1} \cdots w_1 w_0 \bullet & , w_i \in \mathcal{A} + \mathcal{A}, \\ \longrightarrow z_{n+1}\ z_n\ z_{n-1}\ \cdots z_{j+1} z_j\ z_{j-1}\ \cdots\ z_1\ z_0 \bullet & , z_i \in \mathcal{A}. \end{array}$$

Paralelní sčítání (Avizienis, 1961):

$$\begin{array}{ll} \cdots w_{j+t+1} w_{j+t} \cdots w_{j+1} w_j w_{j-1} \cdots w_{j-r} w_{j-r-1} \cdots & , w_i \in \mathcal{A} + \mathcal{A}, \\ \longrightarrow \cdots z_{j+t+1}\ z_{j+t}\ \cdots\ z_{j+1} z_j\ z_{j-1}\ \cdots z_{j-r}\ z_{j-r-1}\ \cdots & , z_i \in \mathcal{A}. \end{array}$$

Najít algoritmus pro paralelní sčítání = určit váhové koeficienty q_j závislé na pevném počtu vstupních cifer takové, že

$$z_j = \underbrace{w_j}_{\in \mathcal{A}+\mathcal{A}} + q_{j-1} - q_j\beta \in \mathcal{A}$$

pro všechny vstupy $(w)_{\beta,\mathcal{A}+\mathcal{A}}$ a každou pozici j.

`https://cloud.sagemath.com/projects`

Extending window method

Hledáme šířku okna $M \in \mathbb{N}$ a váhovou funkci $q : (\mathcal{A} + \mathcal{A})^M \to \mathcal{Q} \subset \mathbb{Z}[\omega]$ takovou, že $q_j = q(w_j, \dots, w_{j-M+1})$.

Extending window method

Hledáme šířku okna $M \in \mathbb{N}$ a váhovou funkci $q : (\mathcal{A} + \mathcal{A})^M \to \mathcal{Q} \subset \mathbb{Z}[\omega]$ takovou, že $q_j = q(w_j, \ldots, w_{j-M+1})$.

Metoda:

1. Najdeme množinu váhových koeficientů $\mathcal{Q} \subset \mathbb{Z}[\omega]$.
2. Zvětšujeme šířku okna M a pro všechny $(w_j, w_{j-1}, \ldots, w_{j-M+1}) \in (\mathcal{A} + \mathcal{A})^M$ zkoušíme najít váhový koeficient z množiny $\mathcal{Q}$ pro definování váhové funkce q.

Fáze 1 – hledání množiny váhových koeficientů

Hledáme množinu váhových koeficientů $\mathcal{Q} \subset \mathbb{Z}[\omega]$ takovou, že

$$\underbrace{(\mathcal{A}+\mathcal{A})} + \underbrace{\mathcal{Q}} \subset \underbrace{\mathcal{A}} + \underbrace{\beta\mathcal{Q}}$$

Fáze 1 – hledání množiny váhových koeficientů

Hledáme množinu váhových koeficientů $\mathcal{Q} \subset \mathbb{Z}[\omega]$ takovou, že

$$\underbrace{(\mathcal{A}+\mathcal{A})}_{w_j \in} + \underbrace{\mathcal{Q}}_{q_{j-1} \in} \subset \underbrace{\mathcal{A}}_{z_j \in} + \underbrace{\beta\mathcal{Q}}_{\beta q_j \in}$$

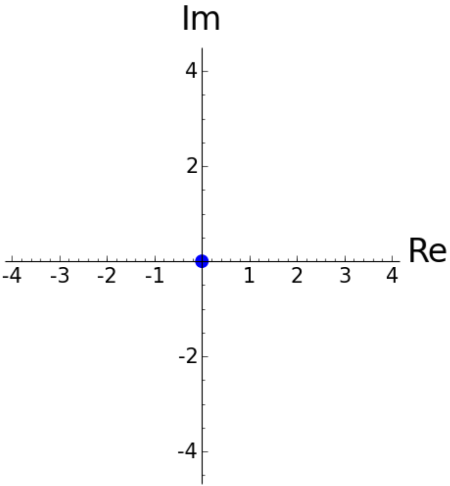
Odtud, pro všechny $q_{j-1} \in \mathcal{Q}$ a $w_j \in \mathcal{A} + \mathcal{A}$ existuje $q_j \in \mathcal{Q}$ takové, že

$$z_j = w_j + q_{j-1} - q_j\beta \in \mathcal{A}\,.$$

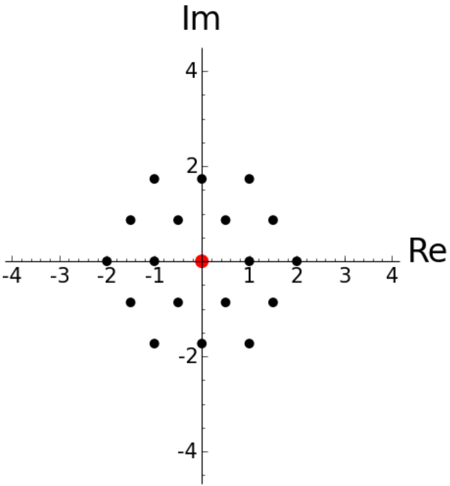
Příklad – fáze 1

Eisensteinova báze

- Báze $\beta = \omega - 1$, kde $\omega = \exp(\frac{2\pi i}{3}), \omega^2 + \omega + 1 = 0$.
- Minimální polynom báze je $\beta^2 + 3\beta + 3$.
- Abeceda $\mathcal{A} = \{0, 1, -1, \omega, -\omega, -\omega - 1, \omega + 1\} \subset \mathbb{Z}[\omega]$.
- Označme $\mathcal{B} = \mathcal{A} + \mathcal{A}$.

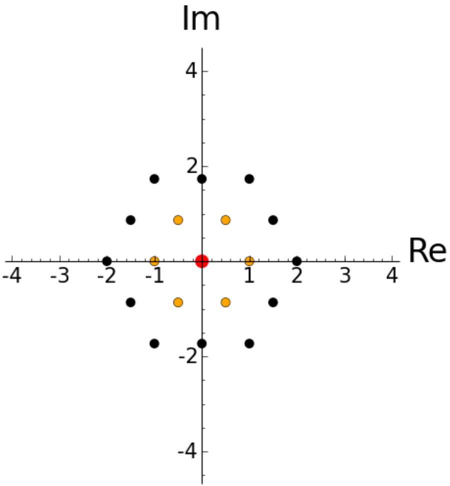


$\mathcal{Q}_0$



$\mathcal{Q}_0$

$\mathcal{B} + \mathcal{Q}_0$

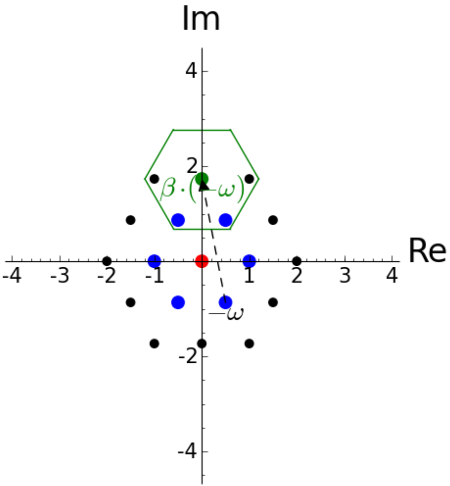


$\mathcal{Q}_0$

$\mathcal{B} + \mathcal{Q}_0$

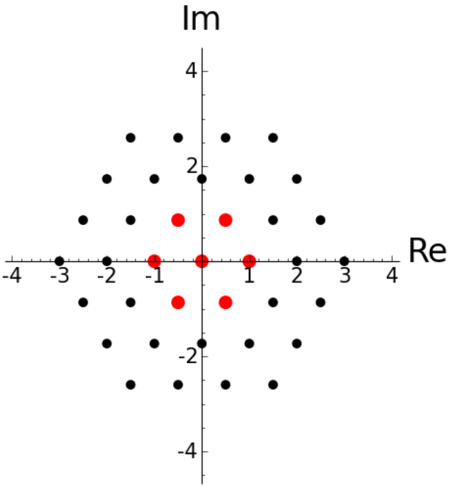
$\overset{?}{\subset}$

$\mathcal{A} + \beta \cdot \mathcal{Q}_0$



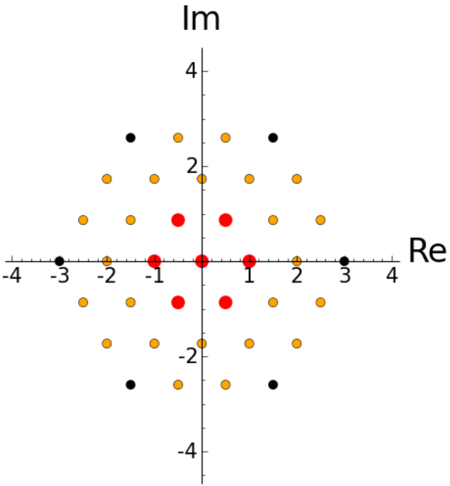
$\mathcal{Q}_0$
$\mathcal{B}+\mathcal{Q}_0$

$\mathcal{A}+\beta\cdot(-\omega)$
$\mathcal{Q}_1\setminus\mathcal{Q}_0$



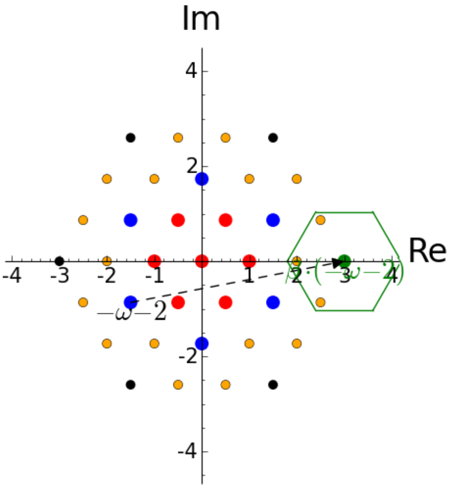
$\mathcal{Q}_1$

$\mathcal{B} + \mathcal{Q}_1$



$$\mathcal{Q}_1$$

$$\mathcal{B} + \mathcal{Q}_1 \overset{?}{\subset} \mathcal{A} + \beta \cdot \mathcal{Q}_1$$

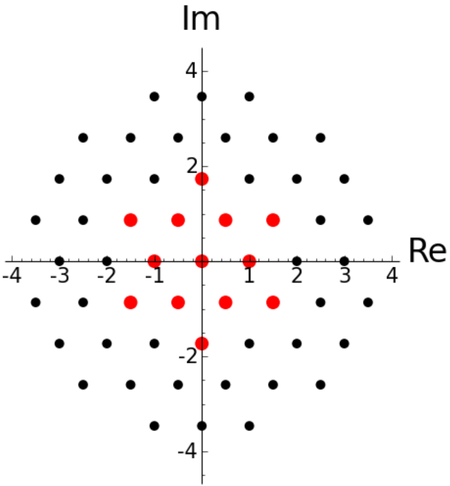


$\mathcal{Q}_1$

$\mathcal{B}+\mathcal{Q}_1$

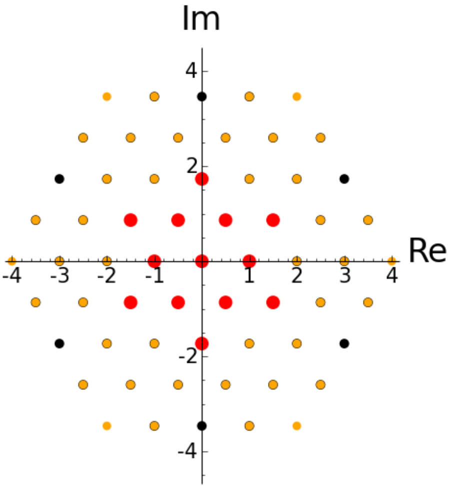
$\mathcal{A}+\beta\cdot(-\omega-2)$

$\mathcal{Q}_2\setminus\mathcal{Q}_1$



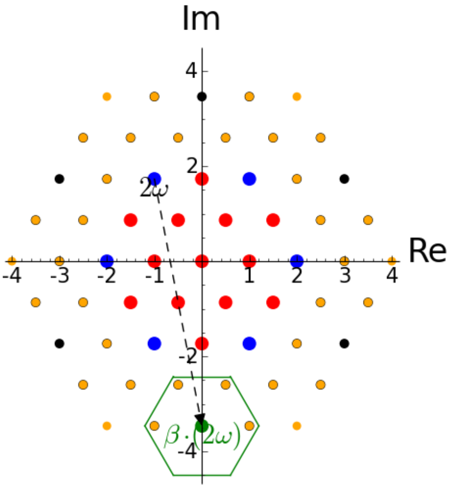
$\mathcal{Q}_2$

$\mathcal{B} + \mathcal{Q}_2$



$$\mathcal{Q}_2$$

$$\mathcal{B} + \mathcal{Q}_2 \overset{?}{\subset} \mathcal{A} + \beta \cdot \mathcal{Q}_2$$

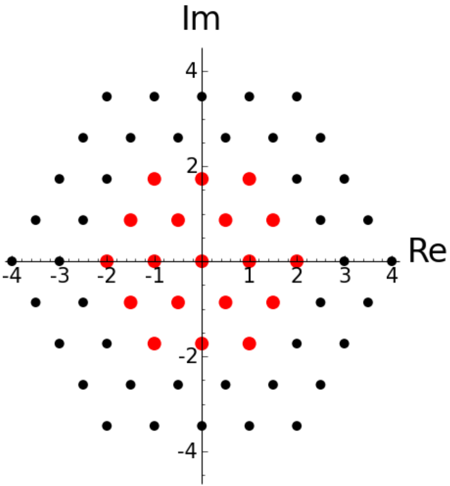


$\mathcal{Q}_2$

$\mathcal{B}+\mathcal{Q}_2$

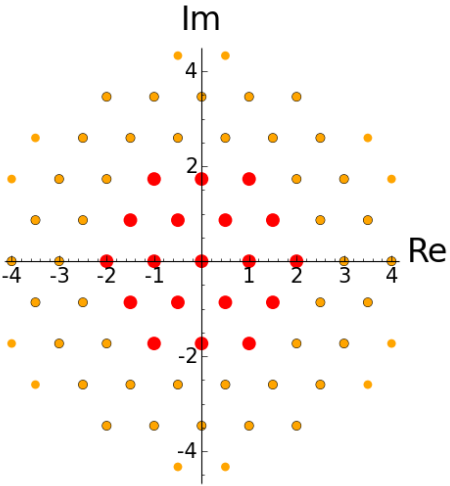
$\mathcal{A}+\beta\cdot(2\omega)$

$\mathcal{Q}_3\setminus\mathcal{Q}_2$



$\mathcal{Q}_3$

$\mathcal{B} + \mathcal{Q}_3$

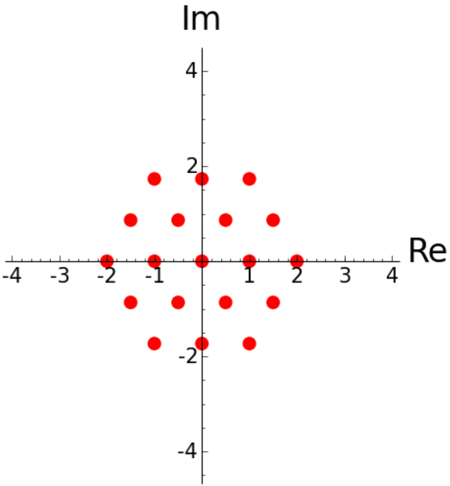


$\mathcal{Q}_3$

$\mathcal{B} + \mathcal{Q}_3$

$\overset{?}{\subset}$

$\mathcal{A} + \beta \cdot \mathcal{Q}_3$



$$\mathcal{Q} = \mathcal{Q}_3$$

Fáze 2 – hledání váhové funkce

Hledáme šířku okna M a váhovou funkci $q : (\mathcal{A} + \mathcal{A})^M \to \mathcal{Q}$.

Fáze 2 – hledání váhové funkce

Hledáme šířku okna M a váhovou funkci $q : (\mathcal{A}+\mathcal{A})^M \to \mathcal{Q}$.
Předpokládejme, že šířka okna je m.
Zkontrolujeme všechny přenosy zprava q_{j-1} a určíme $q_j \in \mathcal{Q}$ takové, že

$$z_j = w_j + q_{j-1} - q_j\beta \in \mathcal{A}\,.$$

Množinu všech možných hodnot q_j označíme $\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} \subset \mathcal{Q}$.

Fáze 2 – hledání váhové funkce

Hledáme šířku okna M a váhovou funkci $q : (\mathcal{A}+\mathcal{A})^M \to \mathcal{Q}$.
Předpokládejme, že šířka okna je m.
Zkontrolujeme všechny přenosy zprava q_{j-1} a určíme $q_j \in \mathcal{Q}$ takové, že

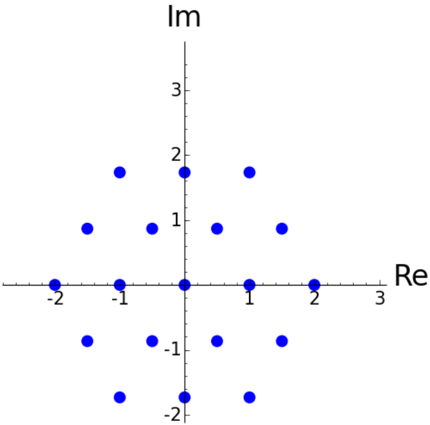
$$z_j = w_j + q_{j-1} - q_j\beta \in \mathcal{A}\,.$$

Množinu všech možných hodnot q_j označíme $\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} \subset \mathcal{Q}$.
Šířka okna M a váhová funkce q je nalezena když

$$\#\mathcal{Q}_{[w_j,\ldots,w_{j-M+1}]} = 1$$

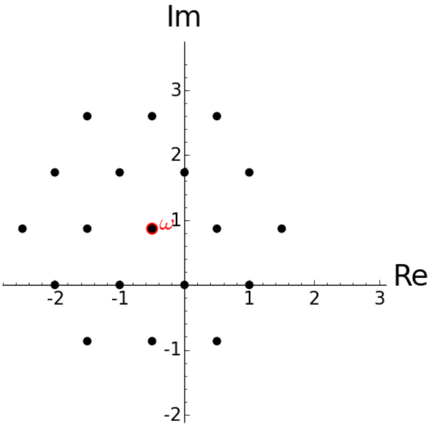
pro všechny $w_j, \ldots, w_{j-M+1} \in (\mathcal{A}+\mathcal{A})^M$.

Vstup: $(\omega\, 1\, 2)$



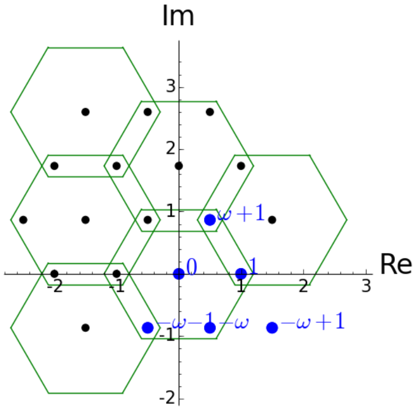
$\mathcal{Q}$

Vstup: $(\omega\, 1\, 2)$



$\omega + \mathcal{Q}$

Vstup: $(\omega\,1\,2)$



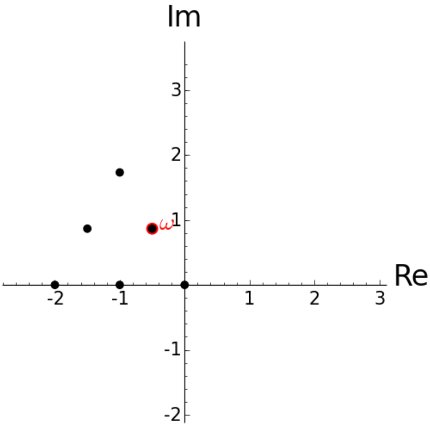
$\omega + \mathcal{Q}$

$\subset$

$\mathcal{A} + \beta \cdot \mathcal{Q}_{[\omega]}$

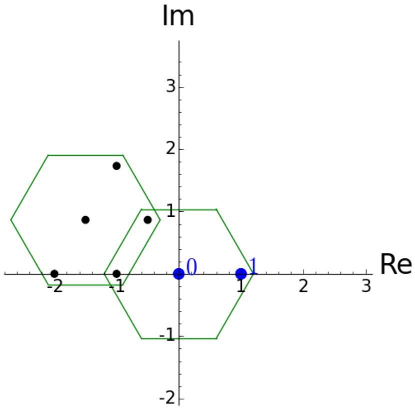
$\mathcal{Q}_{[\omega]}$

Vstup: $(\omega\,1\,2)$



$$\omega + \mathcal{Q}_{[1]}$$

Vstup: $(\omega\, 1\, 2)$



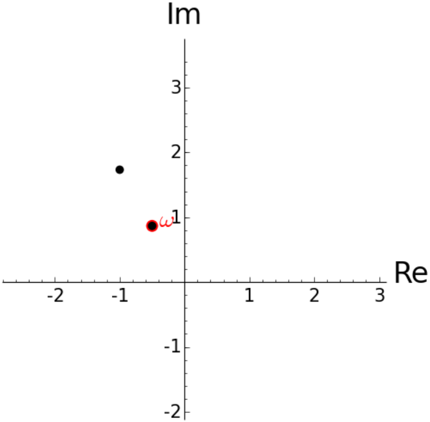
$\omega + \mathcal{Q}_{[1]}$

$\subset$

$\mathcal{A} + \beta \cdot \mathcal{Q}_{[\omega,1]}$

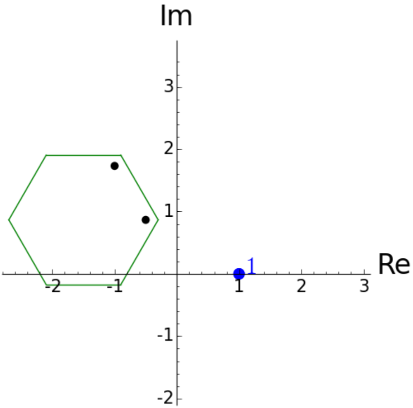
$\mathcal{Q}_{[\omega,1]}$

Vstup: $(\omega\,1\,2)$



$$\omega + \mathcal{Q}_{[1,2]}$$

Vstup: $(\omega\,1\,2)$



$$\omega + \mathcal{Q}_{[1,2]}$$

$$\subset$$

$$\mathcal{A} + \beta \cdot \mathcal{Q}_{[\omega,1,2]}$$

$$\mathcal{Q}_{[\omega,1,2]}$$

Nutná podmínka na abecedu

Pro existenci algoritmu pro paralelní sčítání je nezbytné, aby abeceda $\mathcal{A}$ obsahovala:

- všechny reprezentanty modulo β,
- všechny reprezentanty modulo $\beta - 1$.

Fáze 1 – postačující podmínka konvergence

Pokud je algebraické celé číslo ω stupně 1 nebo je komplexní stupně 2, fáze 1 konverguje.

Fáze 2 – nutná podmínka konvergence

Pokud algoritmus pro paralelní sčítání existuje, fáze 2 konverguje pro vstupy $(b, \ldots, b)$ pro všechny $b \in \mathcal{A} + \mathcal{A}$.

Máme algoritmus, který určí, jestli je fáze 2 konečná pro vstupy tohoto tvaru.

Testované příklady

Jméno	Abec.	Post. p.	Fáze 1	Nut. p.	Fáze 2
Eisenstein_1-block_complex	ano	ano	✓	✓	✓
Eisenstein_1-block_integer	ano	ano	✓	✗	–
Eisenstein_1-block_small_complex	ne	–	–	–	–
Eisenstein_2-block	ne	–	–	–	–
Eisenstein_2-block_4elements	ano	ano	✓	✗	–
Penney_1-block_complex	ano	ano	✓	✓	✓
Penney_1-block_small_complex	ne	–	–	–	–
Penney_1-block_integer	ano	ano	✓	✗	–
Penney_2-block_integer	ano	ano	✓	✓	✓
Quadratic+1-2+2_1-block_complex	ano	ano	✓	✓	✓
Quadratic+1-2+2_1-block_integer	ano	ano	✓	✗	–
Quadratic+1+4+5_1-block_complex	ano	ano	✓	✓	✓
Quadratic+1+3+5_1-block_complex	ano	ano	✓	✓	✗
Quadratic+1-5+3_1-block_integer	ano	ne	✗	–	–
Quadratic+1-5+5_1-block_real	ano	ne	✓	✗	–
base_2	ano	ano	✓	✓	✓
base_4	ano	ano	✓	✓	✓
Cubic+1+1-1+1_complex	ano	ne	✗	–	–
Cubic+1+1-5+5_complex	ano	ne	✓	✗	–

Výsledky

- Implementace v SageMath:
  `https://cloud.sagemath.com/projects`
- Vstupní kontrola abecedy.
- Algoritmus pro kontrolu nutné podmínky konvergence fáze 2.
- Zkoušení různých modifikací výběru prvků ve fázi 2.
- Testování příkladů.

Děkuji

Množinu $\mathcal{Q}$ konstruujeme iterativně:

Fáze 1

$k := 0$

$\mathcal{Q}_0 := \{0\}$

Množinu $\mathcal{Q}$ konstruujeme iterativně:

Fáze 1

$k := 0$
$\mathcal{Q}_0 := \{0\}$
Repeat:

- rozšiř $\mathcal{Q}_k$ na $\mathcal{Q}_{k+1}$ tak, že

$$(\mathcal{A} + \mathcal{A}) + \mathcal{Q}_k \subset \mathcal{A} + \beta \mathcal{Q}_{k+1} \,,$$

- $k := k + 1$

Množinu $\mathcal{Q}$ konstruujeme iterativně:

Fáze 1

$k := 0$
$\mathcal{Q}_0 := \{0\}$
Repeat:

- rozšiř $\mathcal{Q}_k$ na $\mathcal{Q}_{k+1}$ tak, že

$$(\mathcal{A} + \mathcal{A}) + \mathcal{Q}_k \subset \mathcal{A} + \beta \mathcal{Q}_{k+1} \,,$$

- $k := k + 1$

until $\mathcal{Q}_k = \mathcal{Q}_{k+1}$.

Množinu $\mathcal{Q}$ konstruujeme iterativně:

Fáze 1

$k := 0$

$\mathcal{Q}_0 := \{0\}$

Repeat:

- rozšiř $\mathcal{Q}_k$ na $\mathcal{Q}_{k+1}$ tak, že

$$(\mathcal{A} + \mathcal{A}) + \mathcal{Q}_k \subset \mathcal{A} + \beta \mathcal{Q}_{k+1} ,$$

- $k := k + 1$

until $\mathcal{Q}_k = \mathcal{Q}_{k+1}$.

$\mathcal{Q} := \mathcal{Q}_k$

Fáze 2

$m := 1$

Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

Fáze 2

$m := 1$

Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

While $(\max\{\#\mathcal{Q}_{[w_j,\dots,w_{j-m+1}]} : (w_j, \dots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m\} > 1)$ do:

Fáze 2

$m := 1$

Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

While $(\max\{\#\mathcal{Q}_{[w_j,\dots,w_{j-m+1}]} : (w_j, \dots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m\} > 1)$ do:

- $m := m + 1$

Fáze 2

$m := 1$

Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

While $(\max\{\#\mathcal{Q}_{[w_j,\dots,w_{j-m+1}]} : (w_j, \dots, w_{j-m+1}) \in (\mathcal{A} + \mathcal{A})^m\} > 1)$ do:

- $m := m + 1$
- Pro všechny $(w_j, \dots, w_{j-m+1}) \in (\mathcal{A} + \mathcal{A})^m$ najdi množinu $\mathcal{Q}_{[w_j,\dots,w_{j-m+1}]} \subset \mathcal{Q}_{[w_j,\dots,w_{j-m+2}]}$ takovou, že

$$w_j + \mathcal{Q}_{[w_{j-1},\dots,w_{j-m+1}]} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j,\dots,w_{j-m+1}]} \,,$$

Fáze 2

$m := 1$

Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

While $(\max\{\#\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} : (w_j, \ldots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m\} > 1)$ do:

- $m := m + 1$
- Pro všechny $(w_j, \ldots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m$ najdi množinu $\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} \subset \mathcal{Q}_{[w_j,\ldots,w_{j-m+2}]}$ takovou, že

$$w_j + \mathcal{Q}_{[w_{j-1},\ldots,w_{j-m+1}]} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]}\,,$$

$M := m$

Fáze 2

$m := 1$
Pro každé $w_j \in \mathcal{A} + \mathcal{A}$ najdi množinu $\mathcal{Q}_{[w_j]} \subset \mathcal{Q}$ takovou, že

$$w_j + \mathcal{Q} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j]}$$

While $(\max\{\#\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} : (w_j, \ldots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m\} > 1)$ do:

- $m := m + 1$
- Pro všechny $(w_j, \ldots, w_{j-m+1}) \in (\mathcal{A}+\mathcal{A})^m$ najdi množinu $\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} \subset \mathcal{Q}_{[w_j,\ldots,w_{j-m+2}]}$ takovou, že

$$w_j + \mathcal{Q}_{[w_{j-1},\ldots,w_{j-m+1}]} \subset \mathcal{A} + \beta \mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]},$$

$M := m$
$q(w_j, \ldots, w_{j-M+1}) :=$ jediný prvek $\mathcal{Q}_{[w_j,\ldots,w_{j-M+1}]}$