Konstrukce algoritmů pro paralelní sčítání

Jan Legerský

TIGR
jan.legersky@gmail.com

Školitel: Ing. Štěpán Starosta, PhD.

Předdiplomní seminář

31. března 2016

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

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

kde

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

Sčítání

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

kde

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

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

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

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

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

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

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

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

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

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

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

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:

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

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

Standardní sčítání:

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

Paralelní sčítání (Avizienis, 1961):

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

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

Standardní sčítání:

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

Paralelní sčítání (Avizienis, 1961):

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

Najít algoritmus pro paralelní sčítání = určit váhové koeficienty q_j závislé pouze 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.

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 $q_j = q(w_j, \ldots, w_{j-M+1})$.

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

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

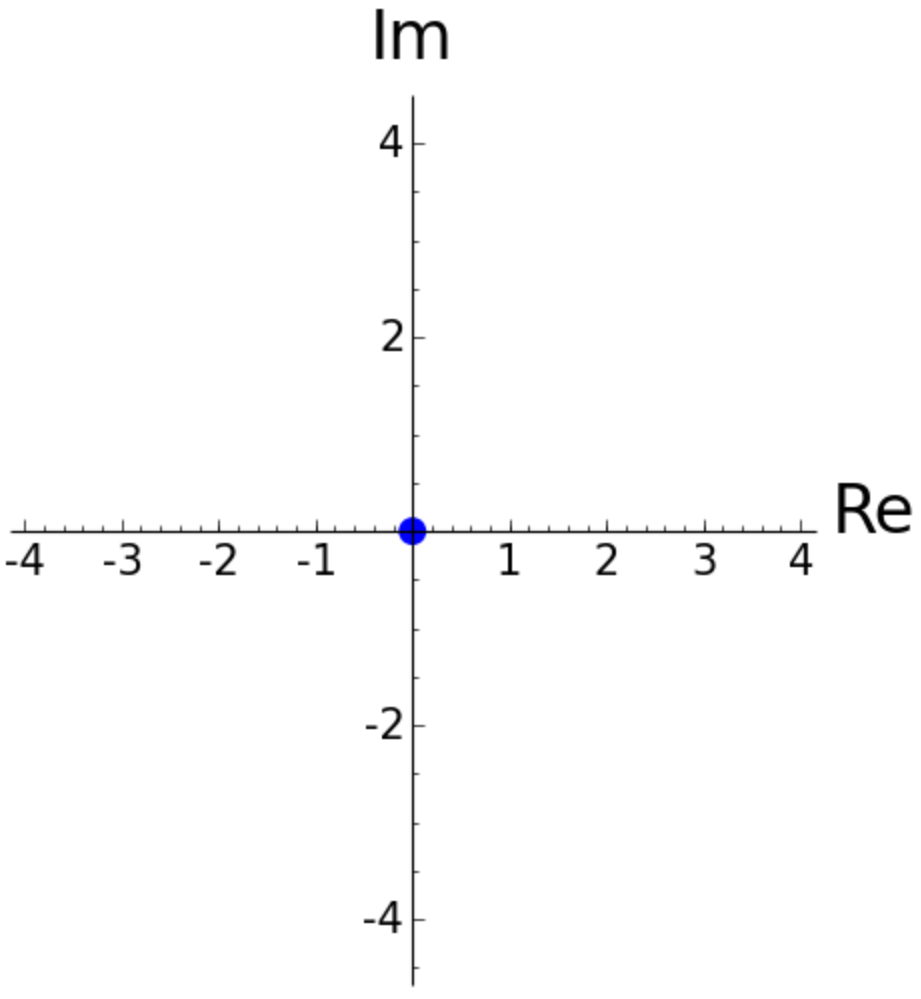
Odtud, pro všechny $q_{j-1} \in \mathcal{Q}$ a $w_j \in \mathcal{A}+\mathcal{A}$ existuje $q_j \in \mathcal{Q}$ takové, že

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

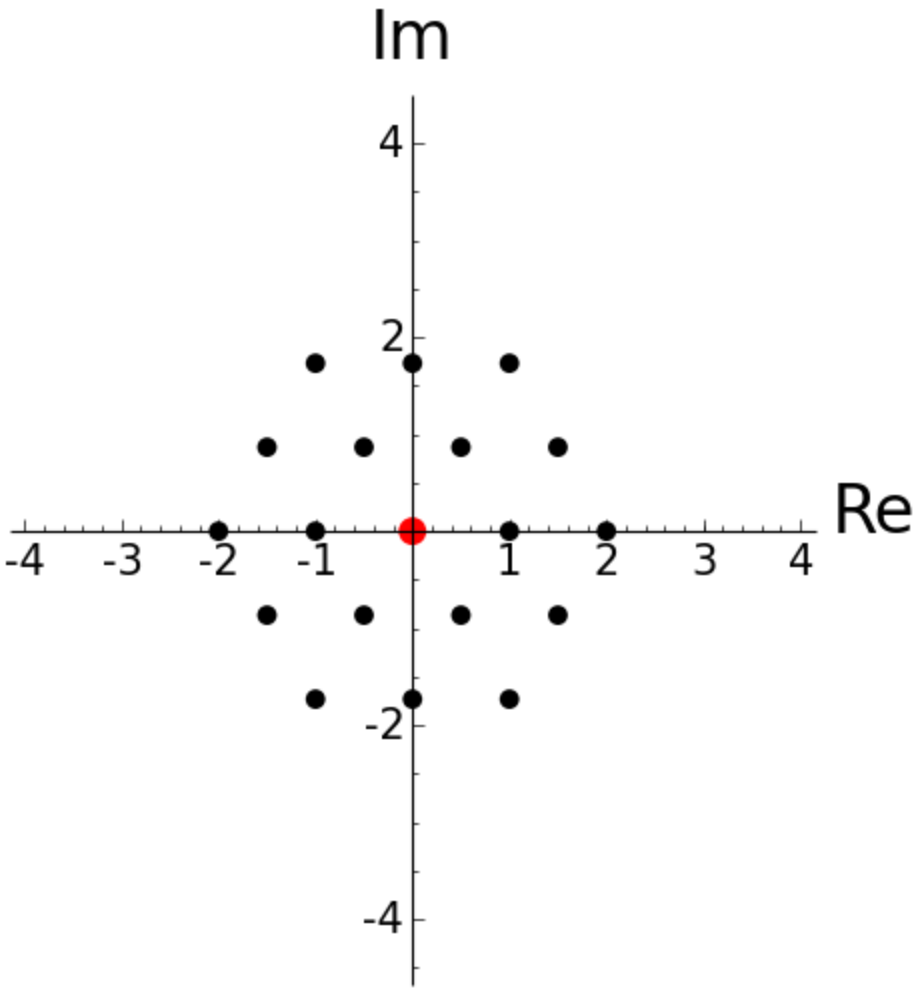
Příklad – fáze 1

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 $\mathcal{B} = \mathcal{A} + \mathcal{A}$.

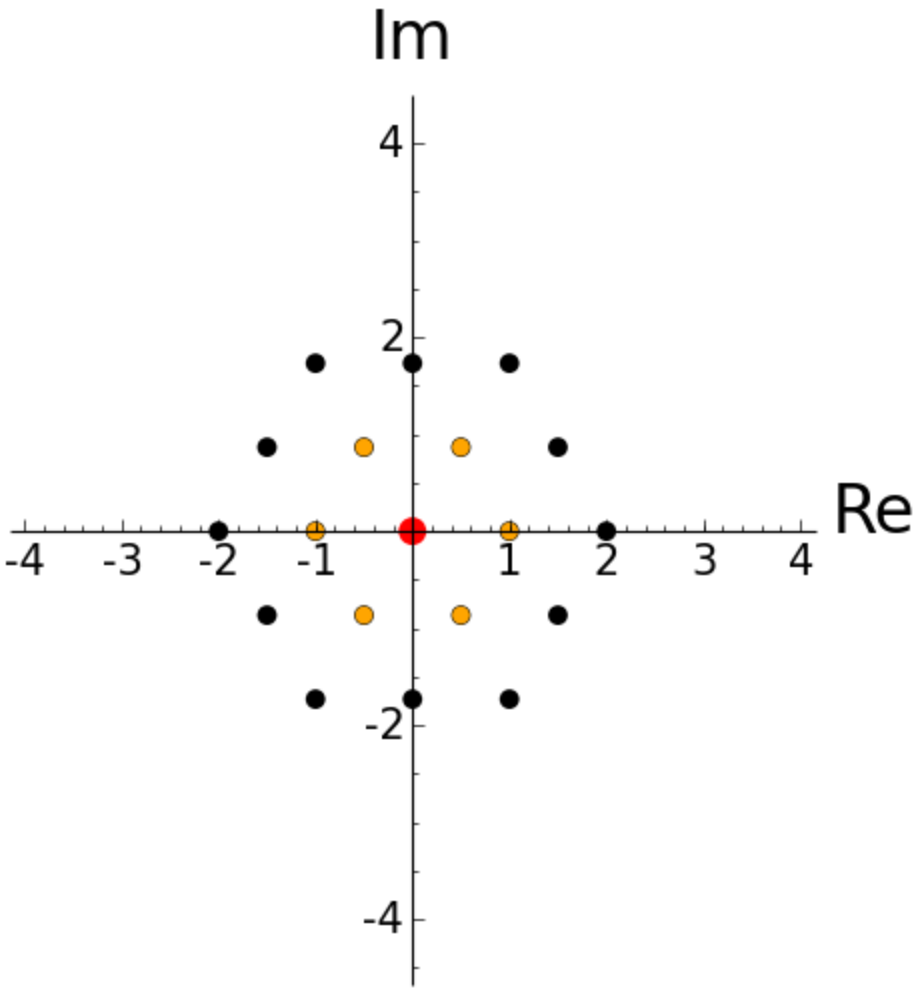


$\mathcal{Q}_0$

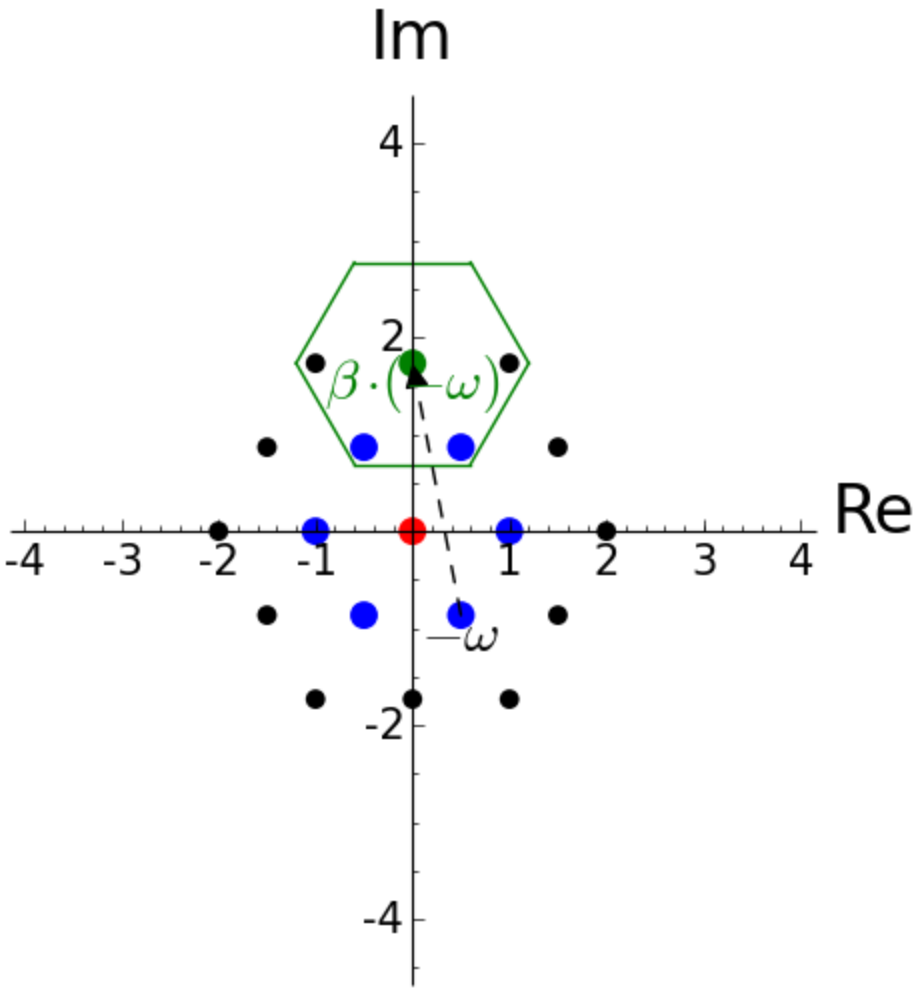


$\mathcal{Q}_0$

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



$$\mathcal{Q}_0$$
$$\mathcal{B} + \mathcal{Q}_0$$
$$?$$
$$\subset$$
$$\mathcal{A} + \beta \cdot \mathcal{Q}_0$$

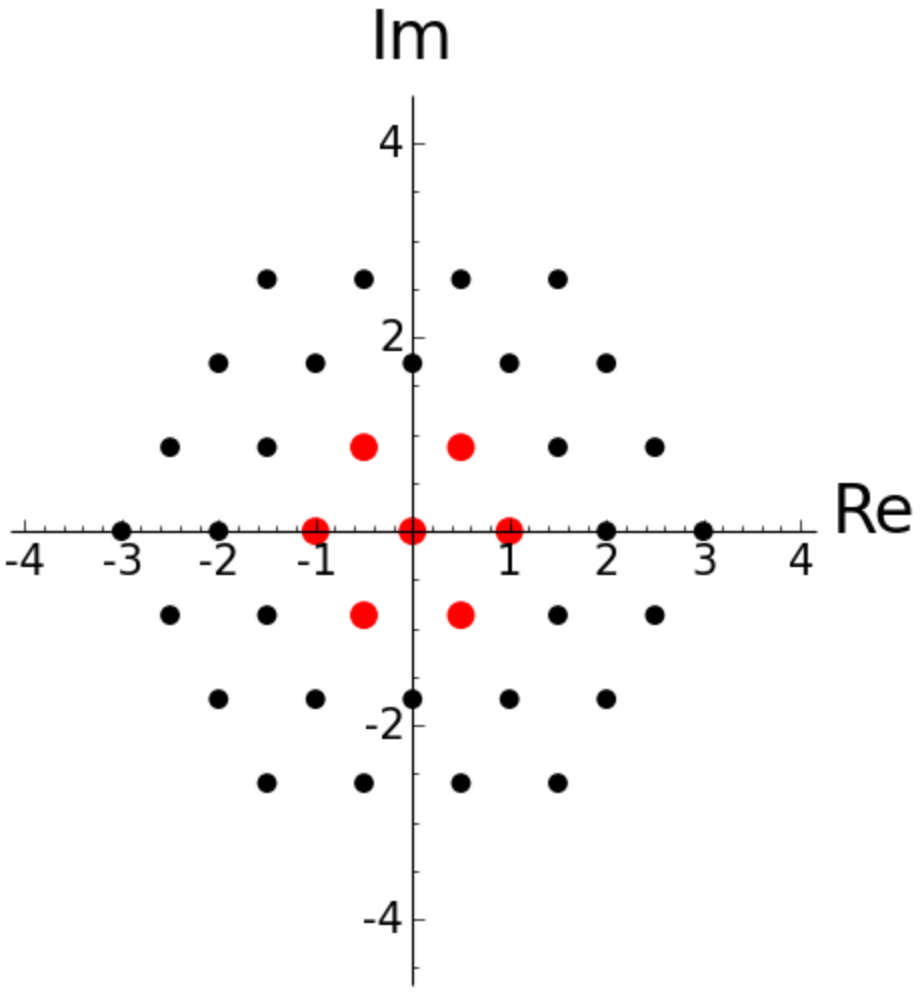


$\mathcal{Q}_0$

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

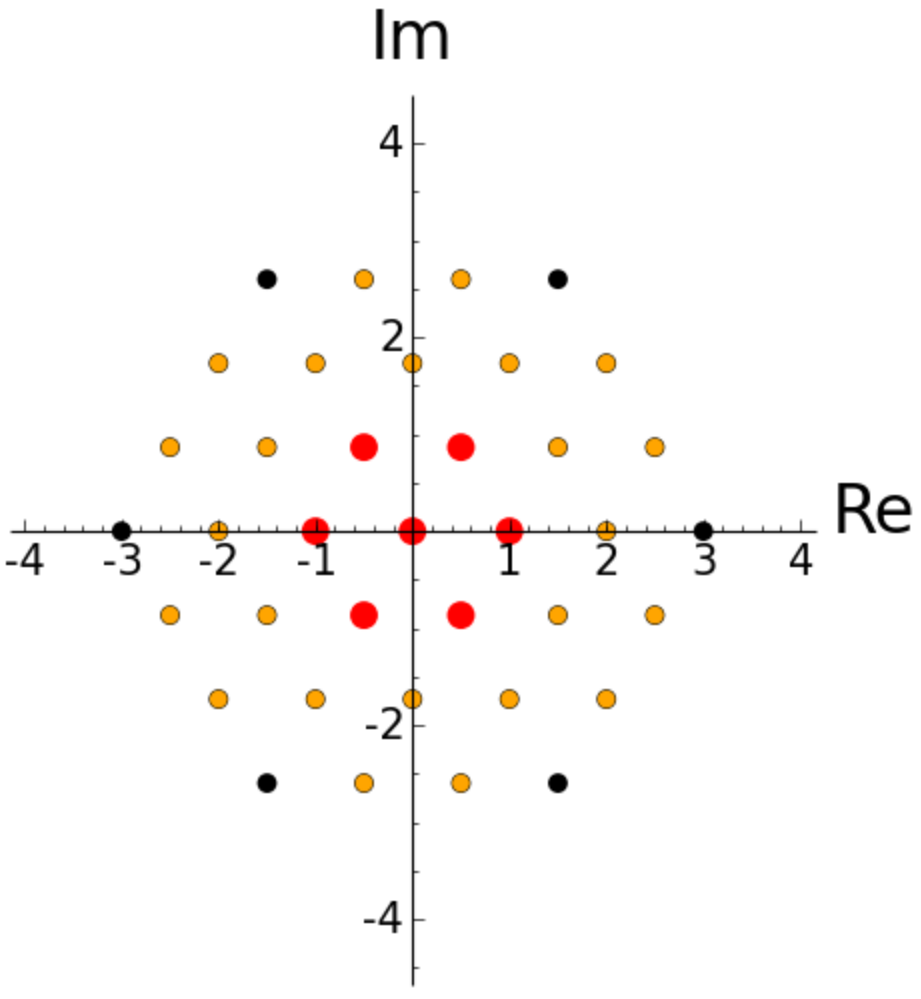
$\mathcal{A} + \beta \cdot (-\omega)$

$\mathcal{Q}_1 \setminus \mathcal{Q}_0$

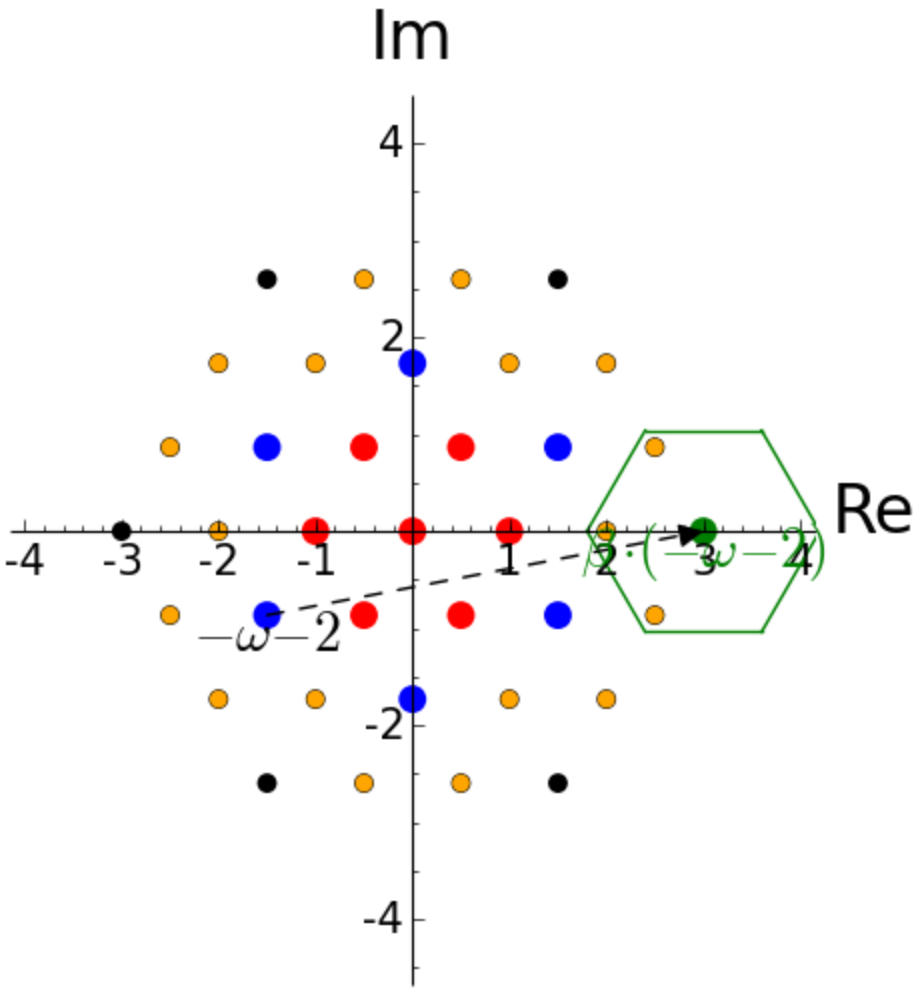


$\mathcal{Q}_1$

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



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

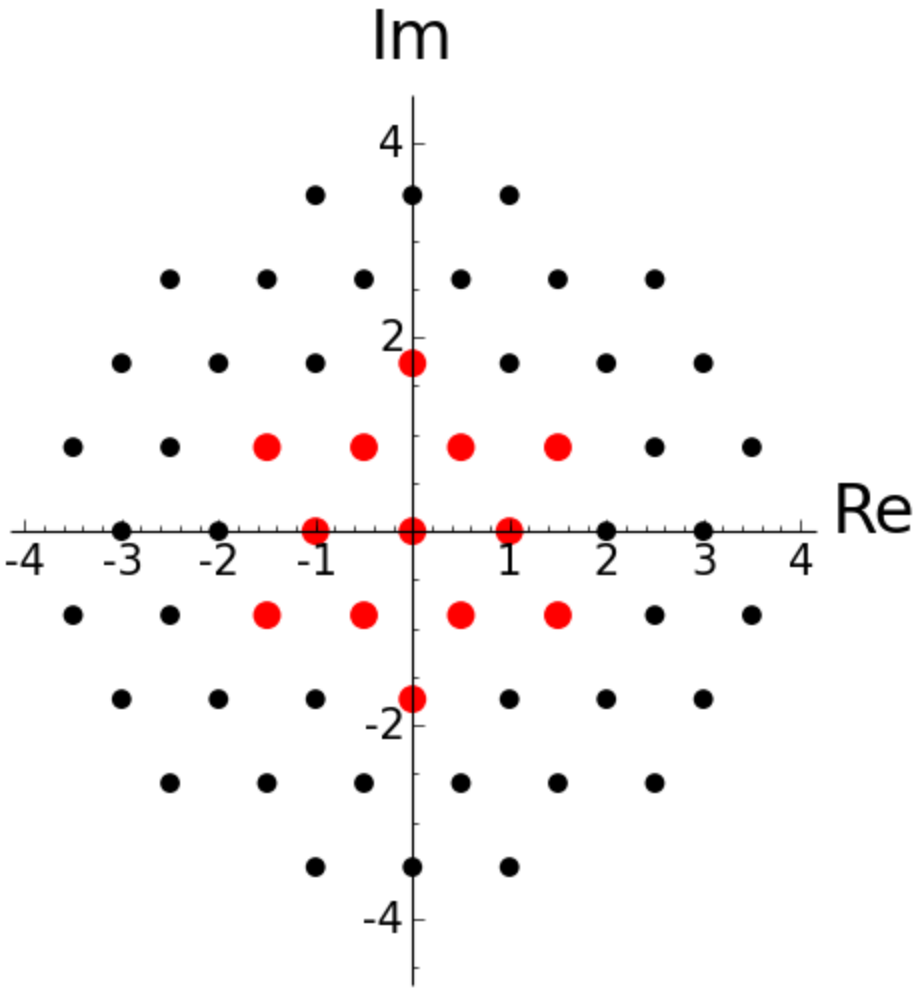


$\mathcal{Q}_1$

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

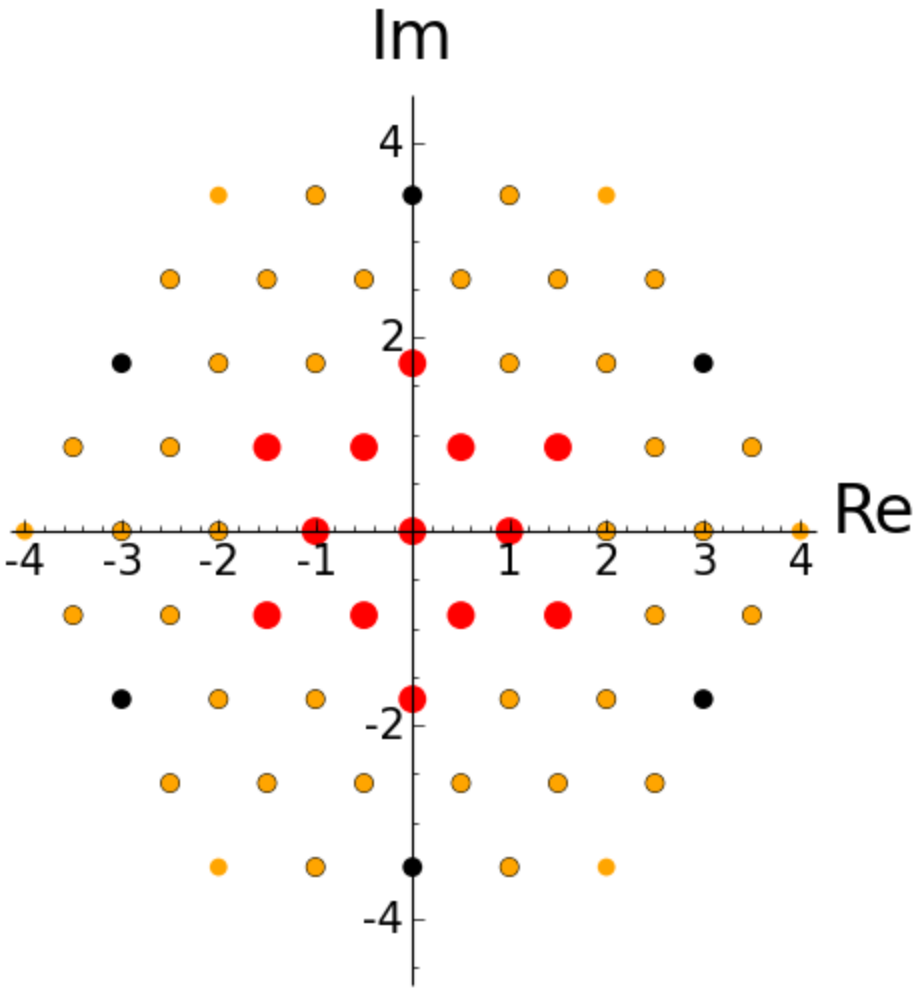
$\mathcal{A}+\beta\cdot(-\omega-2)$

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



$\mathcal{Q}_2$

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



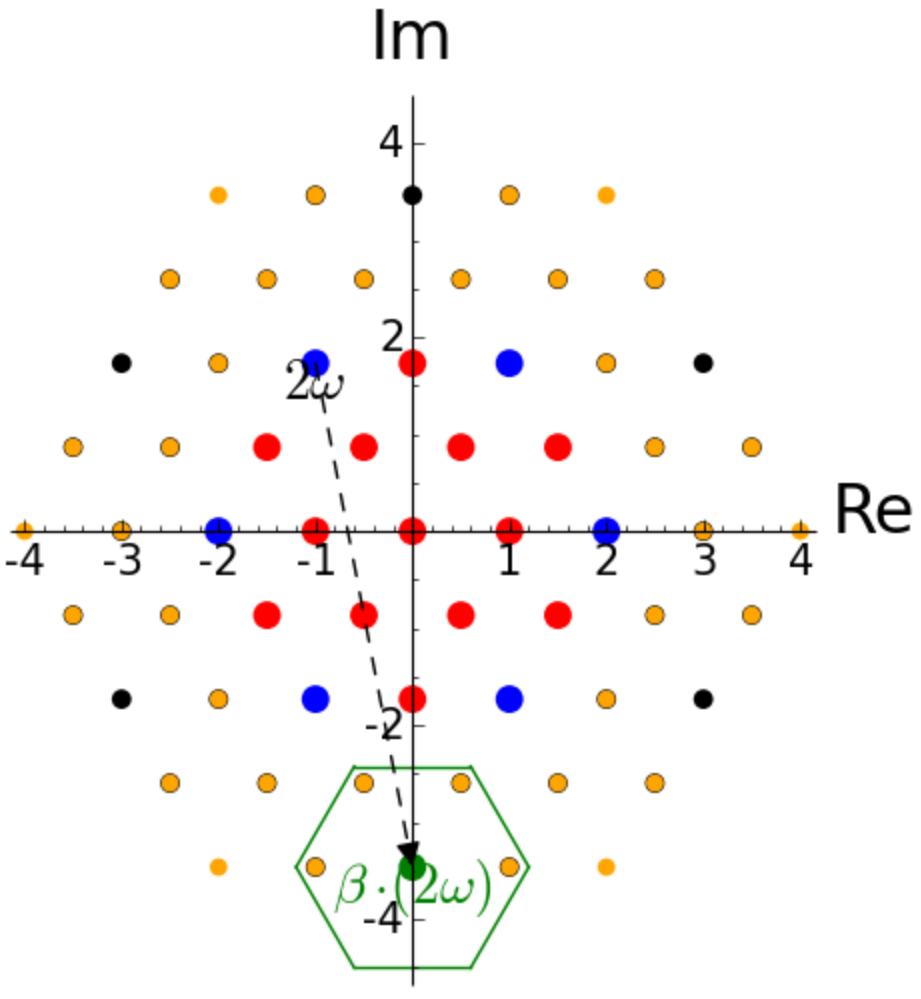
$$\mathcal{Q}_2$$

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

$$?$$

$$\subset$$

$$\mathcal{A} + \beta \cdot \mathcal{Q}_2$$

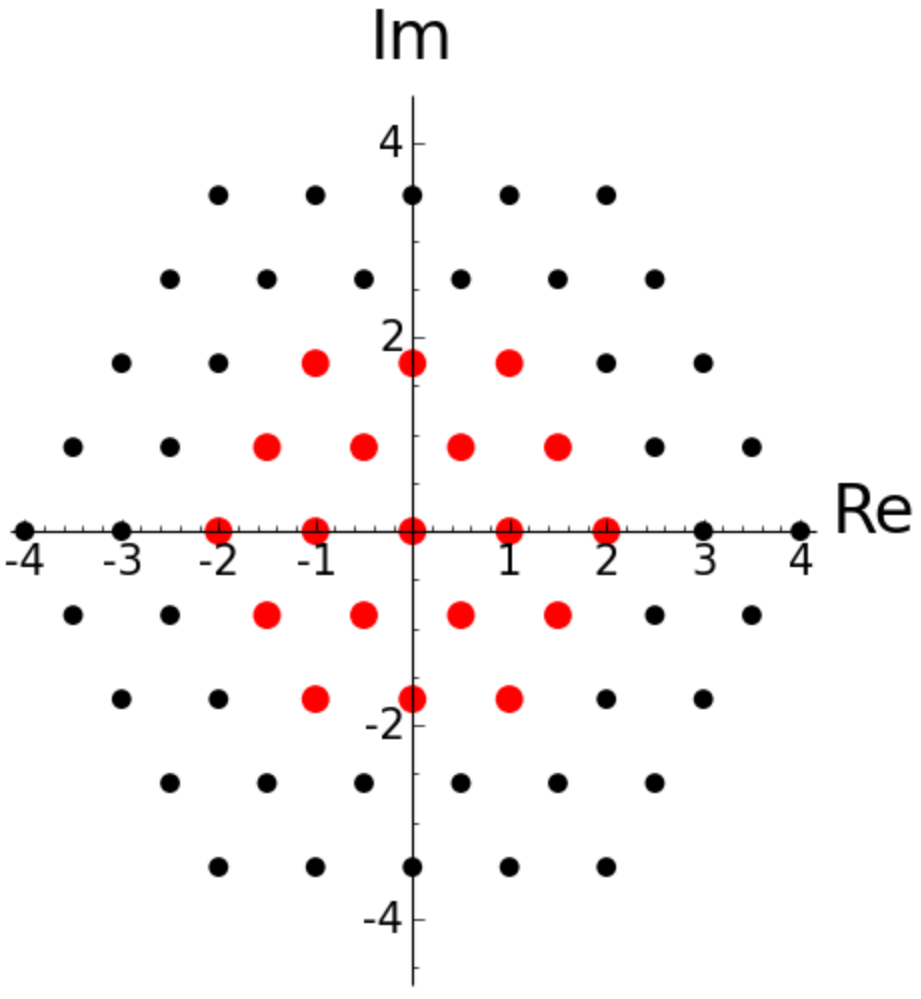


$\mathcal{Q}_2$

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

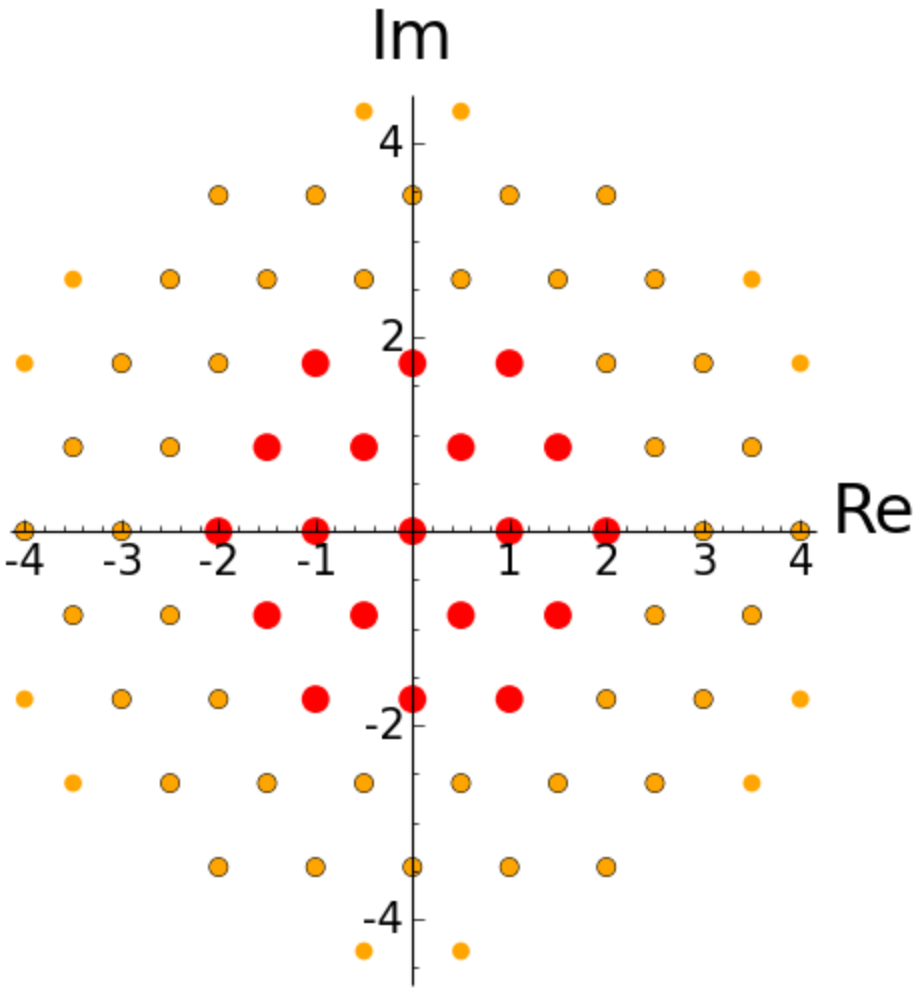
$\mathcal{A} + \beta \cdot (2\omega)$

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



$\mathcal{Q}_3$

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

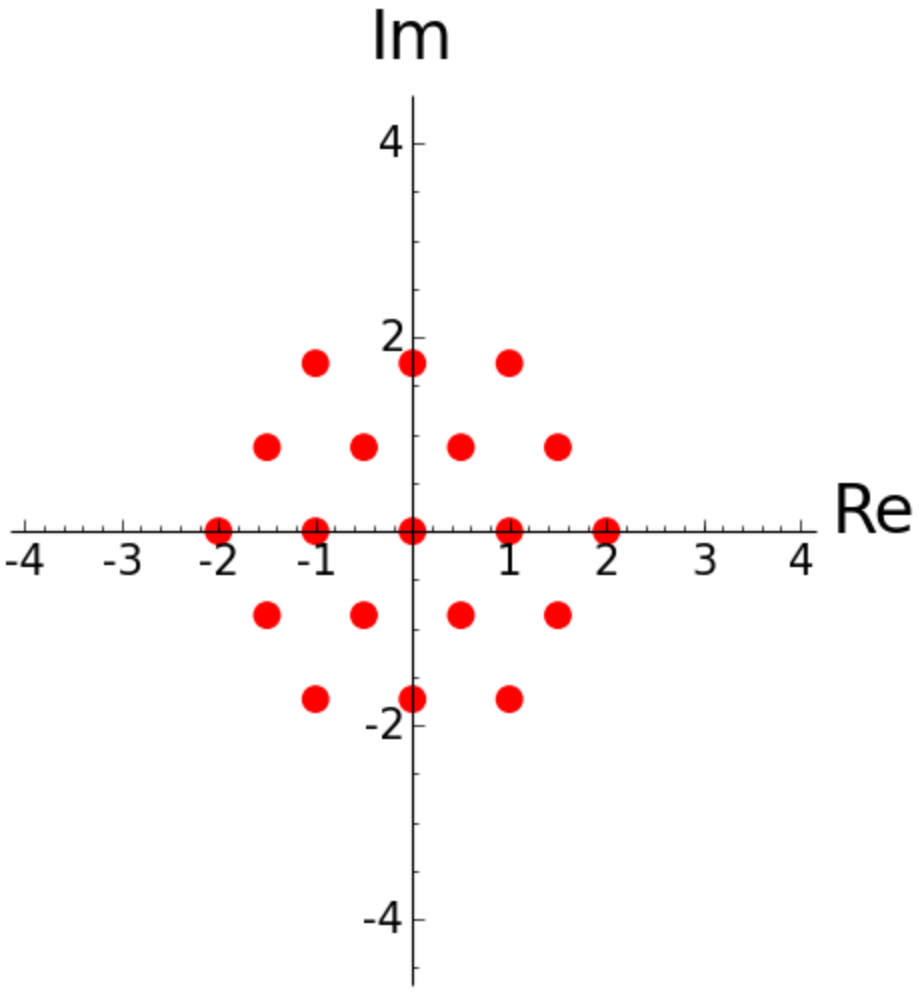


$$\mathcal{Q}_3$$

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

$$\stackrel{?}{\subset}$$

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



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

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

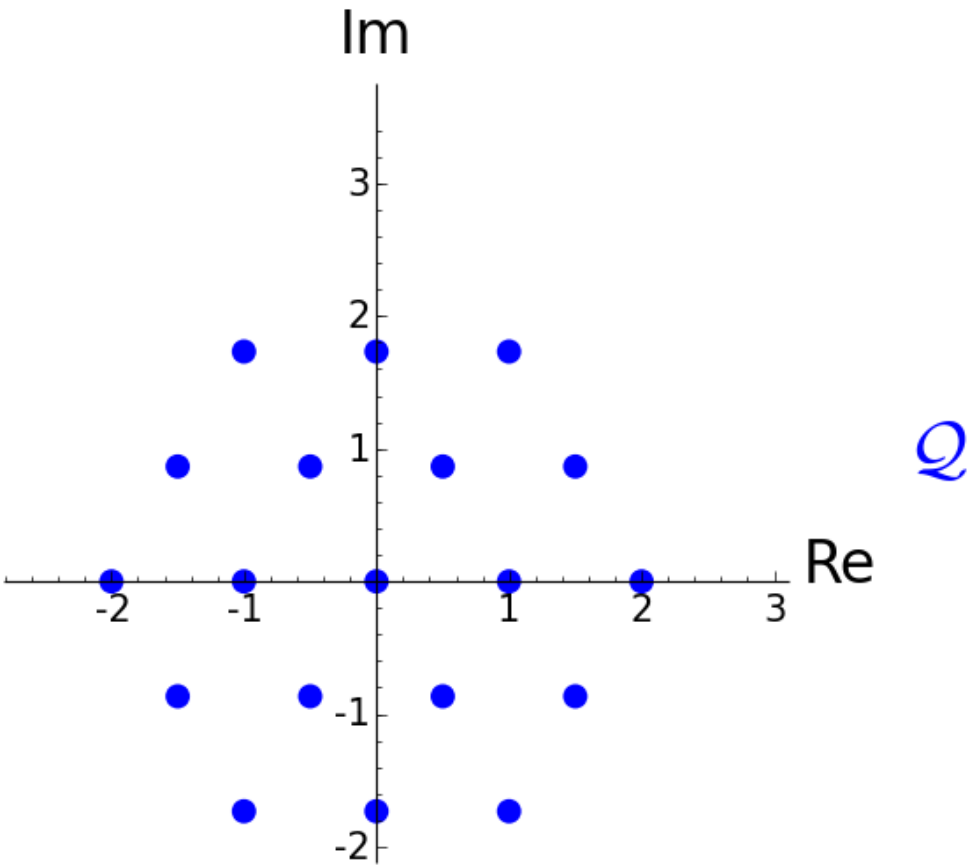
Hledáme šířku okna M a váhovou funkci $q : (\mathcal{A} + \mathcal{A})^M \to \mathcal{Q}$.
Předpokládejme, že šířka okna je m.
Zkontrolujeme všechny přenosy zprava q_{j-1} a určíme $q_j \in \mathcal{Q}$ takové, že

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

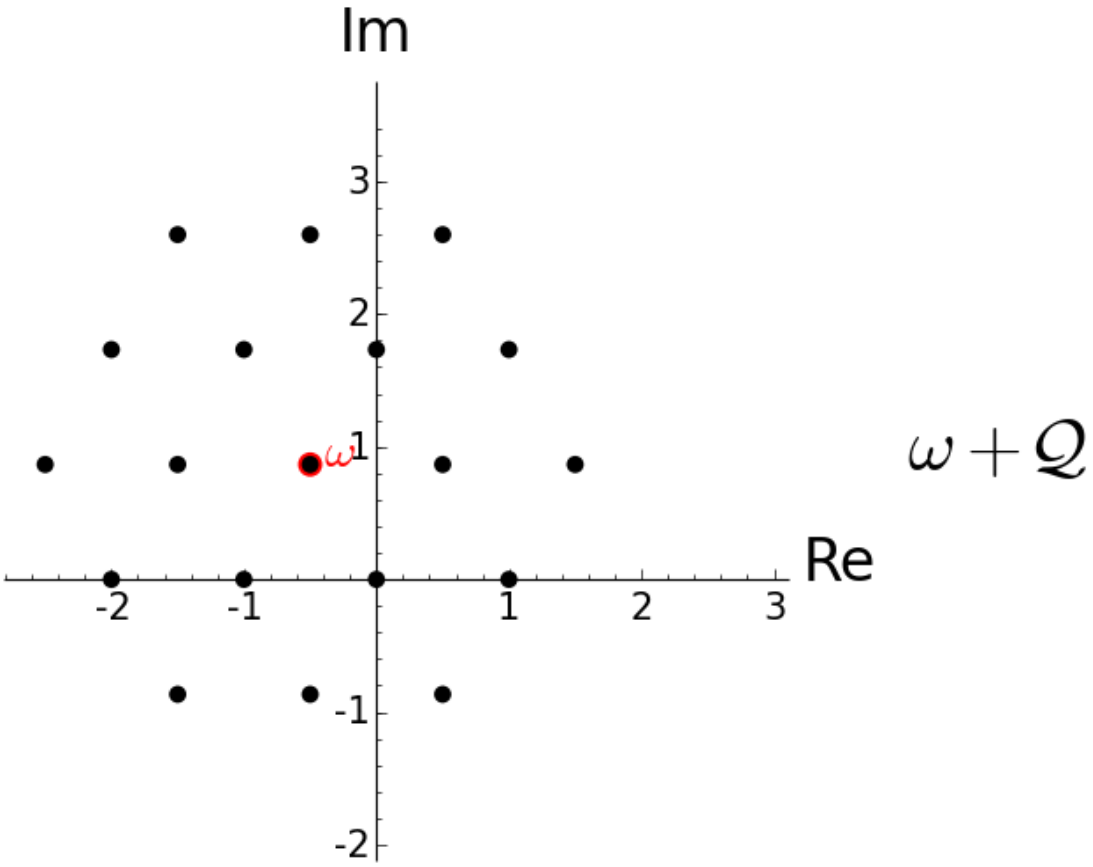
Množinu všech možných hodnot q_j označíme $\mathcal{Q}_{[w_j,\ldots,w_{j-m+1}]} \subset \mathcal{Q}$.
Šířka okna M a váhová funkce q je nalezena, když

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

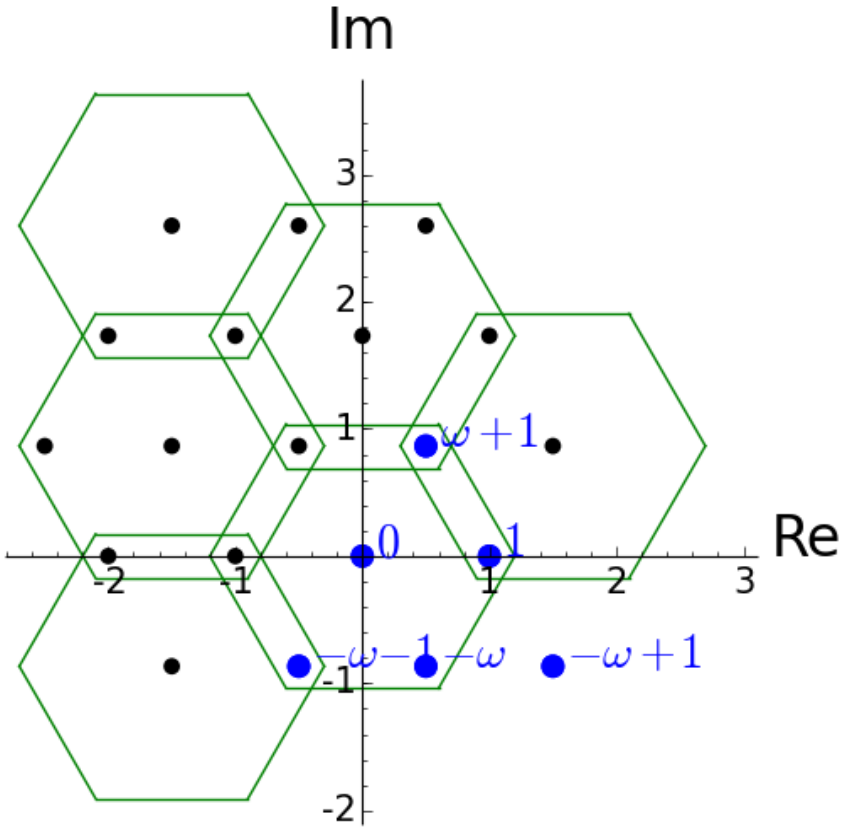
pro všechny $w_j, \ldots, w_{j-M+1} \in (\mathcal{A} + \mathcal{A})^M$.


Im
Re
3
2
1
-1
-2
-2
-1
1
2
3
$\mathcal{Q}$

Vstup: (ω)



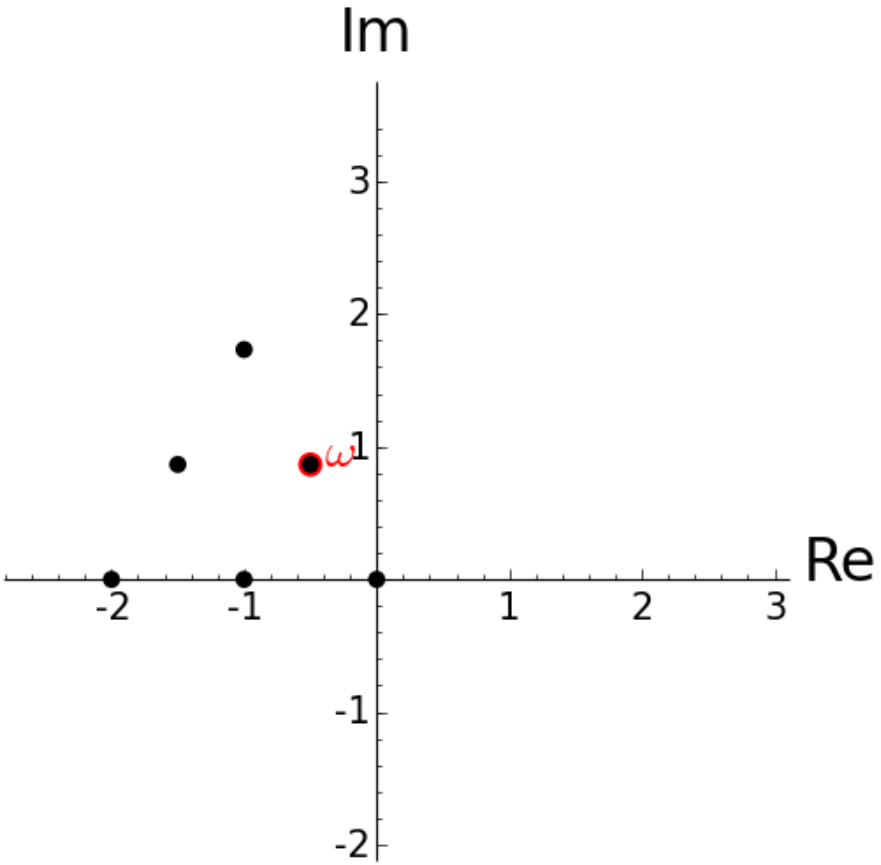
Vstup: (ω)



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

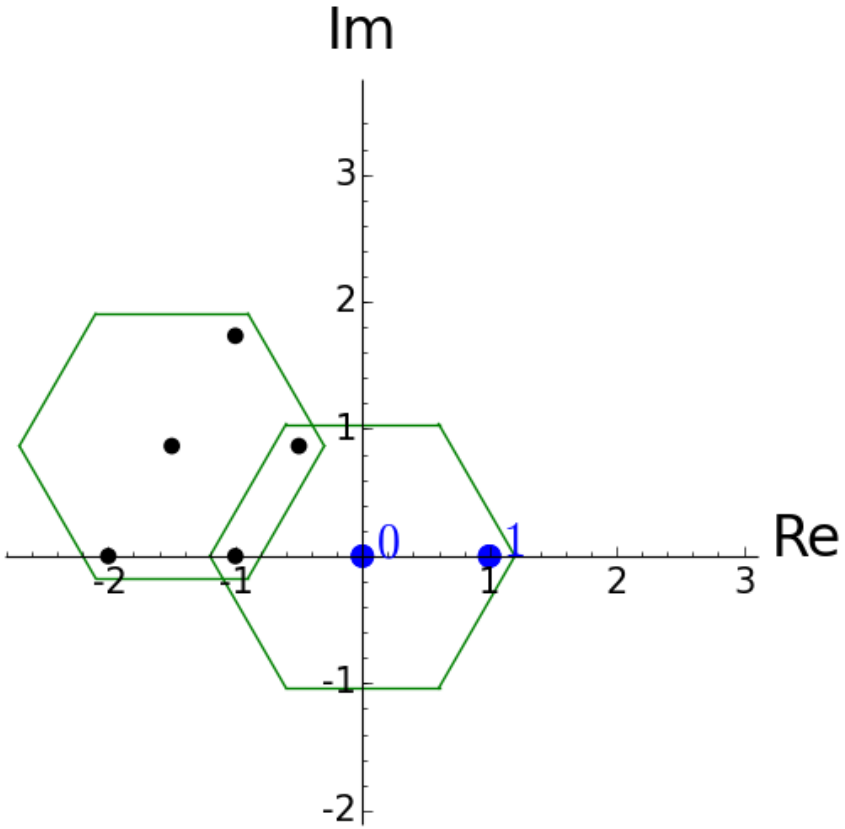
$$\mathcal{Q}_{[\omega]}$$

Vstup: $(\omega\, 1)$



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

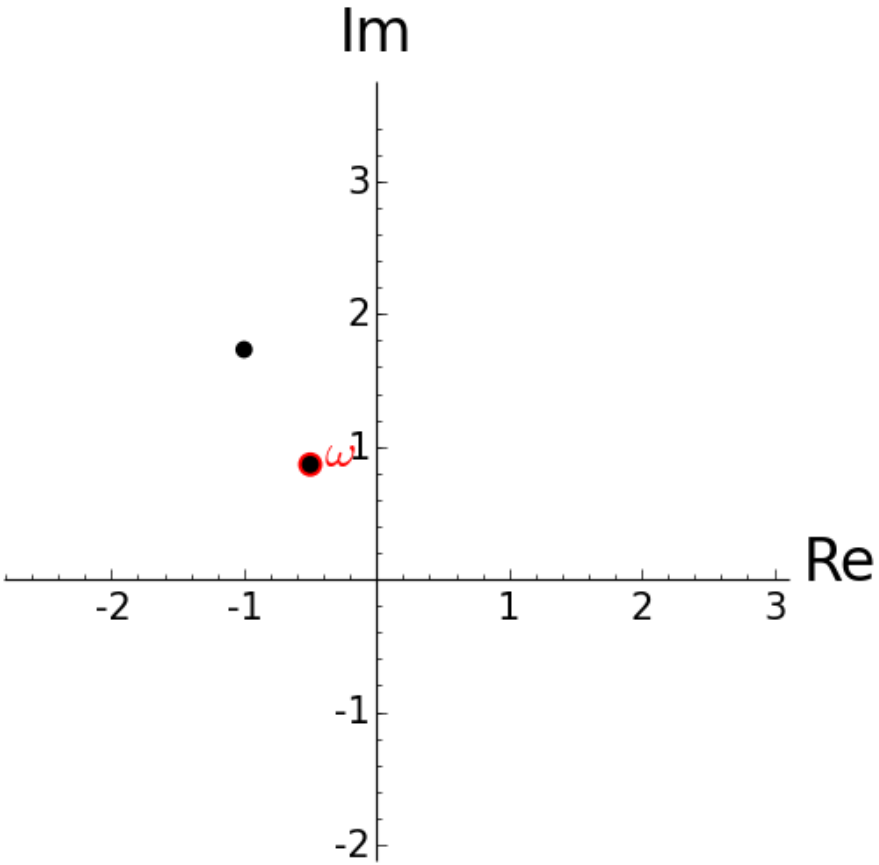
Vstup: $(\omega\, 1)$



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

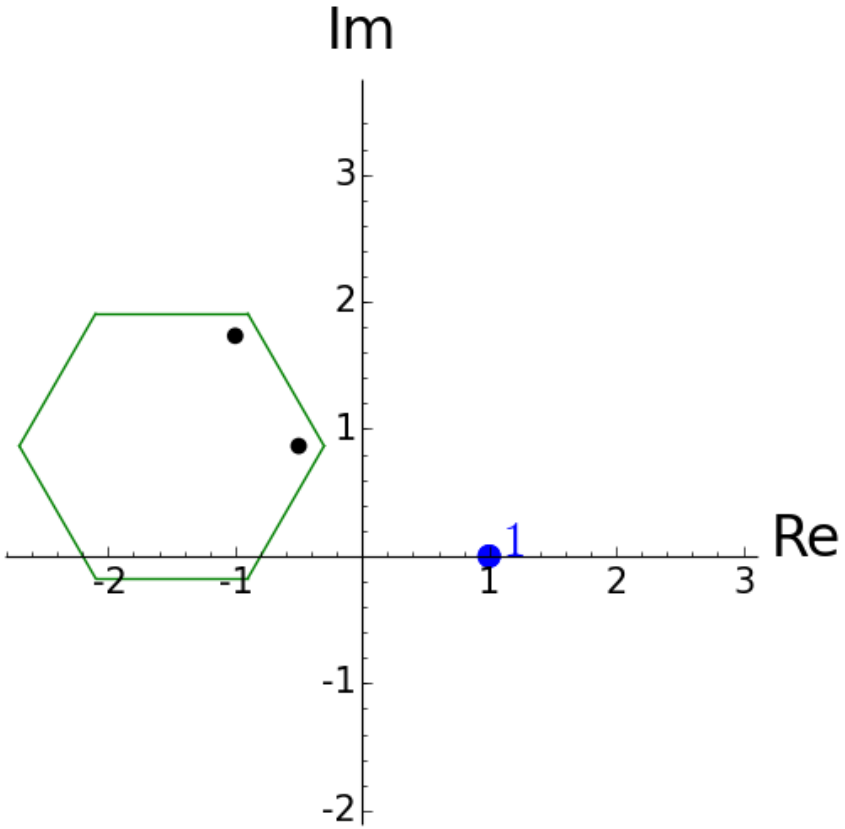
$$\mathcal{Q}_{[\omega,1]}$$

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



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

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



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

$$\subset$$

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

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

Dolní odhad velikosti abecedy

Abeceda $\mathcal{A} \subset \mathbb{Z}[\beta]$ taková, že $0 \in \mathcal{A}$ a $1 \in \mathcal{A}[\beta]$.
Pokud existuje algoritmus pro paralelní sčítání v poziční soustavě $(\beta, \mathcal{A})$, který používá přepisovací pravidlo $x - \beta$, pak

$$\#\mathcal{A} \geq \max\{|m_\beta(0)|, |m_\beta(1)|\}\,,$$

kde m_β je minimální polynom báze β. Navíc, pokud β má reálný sdružený kořen větší než 1, pak

$$\#\mathcal{A} \geq \max\{|m_\beta(0)|, |m_\beta(1)| + 2\}\,.$$

Fáze 1 – postačující a nutná podmínka konvergence

Nechť abeceda $\mathcal{A} \subset \mathbb{Z}[\omega]$ obsahuje alespoň jednoho reprezentanta každé třídy kongruence modulo β v $\mathbb{Z}[\omega]$.

Pokud je β expandující, pak Fáze 1 konverguje.

Naopak, pokud existuje algoritmus pro paralelní sčítání v soustavě $(\beta, \mathcal{A})$ s přepisovacím pravidlem $x - \beta$, pak je β expandující.

Fáze 2 – zastavovací podmínka

Vrcholy Rauzyho grafu Fáze 2 pro šířku okna k jsou kombinace $(w_{-1}, \ldots, w_{-k}) \in (\mathcal{A} + \mathcal{A})^k$ takové, že

$$\#\mathcal{Q}_{[w_{-1},\ldots,w_{-k}]} = \#\mathcal{Q}_{[w_{-1},\ldots,w_{-(k-1)}]}\,.$$

Z $(w_{-1}, \ldots, w_{-k})$ do $(w'_{-1}, \ldots, w'_{-k})$ vede hrana právě tehdy, když

$$(w_{-2}, \ldots, w_{-k}) = (w'_{-1}, \ldots, w'_{-(k-1)})\,.$$

Nechť $w_0, w_{-1}, \ldots, w_{-k} \in (\mathcal{A} + \mathcal{A})$ jsou takové, že $\#\mathcal{Q}_{[w_0,\ldots,w_{-k}]} = \#\mathcal{Q}_{[w_0,\ldots,w_{-(k-1)}]} > 1$.

Pokud existuje nekonečná cesta v Rauzyho grafu Fáze 2 pro šířku okna k začínající hranou $(w_0, \ldots, w_{-(k-1)}) \to (w_{-1}, \ldots, w_{-k})$, pak ve Fázi 2 došlo k zacyklení.

Testované příklady

ω	Base	$\#\mathcal{A}$	m_β	Phase 1	bbb	Phase 2
$1/2 \cdot I\sqrt{15} - 1/2$	ω	6	$x^2 + x + 4$	✓	✓	✗
$1/2 \cdot I\sqrt{11} + 1/2$	$-2\omega - 2$	27	$x^2 + 6x + 20$	✓	✓	✓
$1/2 \cdot I\sqrt{11} + 1/2$	$-\omega + 1$	3	$x^2 - x + 3$	✓	✓	✗
$1/2 \cdot I\sqrt{7} - 1/2$	ω	4	$x^2 + x + 2$	✓	✓	✓
$1/2 \cdot I\sqrt{7} + 1/2$	ω	2	$x^2 - x + 2$	✓	✓	✗
$1/2 \cdot I\sqrt{7} + 3/2$	ω	4	$x^2 - 3x + 4$	✓	✗	-
$I\sqrt{3}$	$-\omega$	4	$x^2 + 3$	✓	✓	✓
$1/2 \cdot I\sqrt{3} + 1/2$	$-3\omega + 2$	7	$x^2 - x + 7$	✓	✓	✗
$I\sqrt{2}$	$-\omega$	3	$x^2 + 2$	✓	✓	✓
$I\sqrt{2} - 1$	ω	6	$x^2 + 2x + 3$	✓	✓	✗
$I - 1$	ω	5	$x^2 + 2x + 2$	✓	✓	✓
I	-3ω	10	$x^2 + 9$	✓	✓	✗
$-1/2\sqrt{5} + 3/2$	$-2\omega - 2$	31	$x^2 + 10x + 20$	✓	✓	✓
$-1/2\sqrt{5} + 3/2$	$3\omega - 3$	13	$x^2 - 3x - 9$	✓	✓	✗
$1/2\sqrt{13} - 3/2$	$\omega - 3$	27	$x^2 + 9x + 17$	✓	✓	✗
$1/2\sqrt{13} + 1/2$	$-2\omega + 2$	16	$x^2 - 2x - 12$	✓	✗	-
$1/2\sqrt{17} - 3/2$	$\omega - 3$	26	$x^2 + 9x + 16$	✓	✓	✓

Výsledky

Konvergence:

- dolní odhad velikosti abecedy ze $\mathbb{Z}[\beta]$
- nutná a postačující podmínka konvergence Fáze 1
- algoritmus pro odhalování zacyklení fáze 2

Výsledky

Konvergence:

- dolní odhad velikosti abecedy ze $\mathbb{Z}[\beta]$
- nutná a postačující podmínka konvergence Fáze 1
- algoritmus pro odhalování zacyklení fáze 2

Implementace v SageMath:

- extending window method včetně mnoha různých možností výběru v obou fázích
- navržený algoritmus pro odhalování zacyklení fáze 2
- generování možné abecedy k zadané bázi

Výsledky

Konvergence:

- dolní odhad velikosti abecedy ze $\mathbb{Z}[\beta]$
- nutná a postačující podmínka konvergence Fáze 1
- algoritmus pro odhalování zacyklení fáze 2

Implementace v SageMath:

- extending window method včetně mnoha různých možností výběru v obou fázích
- navržený algoritmus pro odhalování zacyklení fáze 2
- generování možné abecedy k zadané bázi

Testování

- velké množství vstupů (díky automatickému ukládání do google tabulky)
- úspěšné nalezení algoritmu paralelního sčítání pro téměř 70 pozičních soustav

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

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

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