

Číselné algoritmy

Rozvoj odmocniny do řetězového zlomku

3. 5. 2021

Klasické řetězové zlomky

Pro $a_0 \in \mathbb{R}$ a $a_1, a_2, \dots, a_n \in \mathbb{R}^+$ budeme označovat $[a_0; a_1, \dots, a_n]$ reálné číslo, které obdržíme ze vztahů

$$[a_0] := a_0, [a_0; a_1] := a_0 + \frac{1}{a_1}, [a_0; a_1, a_2] := a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$$

$$[a_0; a_1, \dots, a_n] := a_0 + \frac{1}{[a_1; a_2, \dots, a_n]}$$

Konvergency řetězového zlomku

Tvrzení

Pro $a_0 \in \mathbb{Z}$, $a_1, a_2, \dots \in \mathbb{N}$ definujme posloupnosti

$$p_{-2}, p_{-1}, p_0, p_1, \dots$$

$$q_{-2}, q_{-1}, q_0, q_1, \dots$$

rekurentními vztahy

$$p_{-2} = 0, p_{-1} = 1, p_n = a_n p_{n-1} + p_{n-2}, n \geq 0$$

$$q_{-2} = 1, q_{-1} = 0, q_n = a_n q_{n-1} + q_{n-2}, n \geq 0$$

Pak pro každé $n \in \mathbb{N}_0$ platí

- ▶ $[a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}$
- ▶ $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$
- ▶ posloupnost $\frac{p_n}{q_n}$, $n \geq 0$ je konvergentní

Hodnota nekonečného řetězového zlomku

Definice

Necht' $a_0 \in \mathbb{Z}$, $a_1, a_2, \dots \in \mathbb{N}$. Označme p_i, q_i jako výše.
Hodnotou nekonečného řetězového zlomku $[a_0; a_1, a_2, \dots]$ rozumíme číslo

$$\alpha := \lim_{n \rightarrow \infty} \frac{p_n}{q_n},$$

píšeme

$$\alpha = [a_0; a_1, a_2, \dots]$$

Racionální čísla $\frac{p_n}{q_n}$ nazýváme konvergenty řetězového zlomku.

Poznámka: Rekursivní vztahy pro posloupnosti p_i, q_i lze využít i pro spočtení hodnoty konečného řetězového zlomku $[a_0; a_1, \dots, a_n]$, kde $a_0 \in \mathbb{R}$ a $a_1, \dots, a_n \in \mathbb{R}^+$:

$$p_{-2} = 0, p_{-1} = 1, p_i = a_i p_{i-1} + p_{i-2}, i \geq 0$$

$$q_{-2} = 1, q_{-1} = 0, q_i = a_i q_{i-1} + q_{i-2}, i \geq 0$$

Pak je $[a_0; a_1, \dots, a_i] = \frac{p_i}{q_i}$ pro každé $i = 0, 1, \dots, n$.

Řetězový rozvoj iracionálního čísla

Tvrzení

Pro každé $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ existuje posloupnost $a_0 \in \mathbb{Z}, a_1, a_2, a_3, \dots \in \mathbb{N}$ taková, že

$$\alpha = [a_0; a_1, a_2, \dots]$$

Tato posloupnost je navíc dána jednoznačně.

Idea důkazu: Definujeme posloupnosti $\alpha_0, \alpha_1, \dots \in \mathbb{R}$ a $a_0, a_1, \dots \in \mathbb{Z}$ takto:

$$\begin{aligned}\alpha_0 &:= \alpha, a_0 = \lfloor \alpha_0 \rfloor, \alpha_1 := \frac{1}{\alpha_0 - a_0}, a_1 = \lfloor \alpha_1 \rfloor \\ \alpha_2 &:= \frac{1}{\alpha_1 - a_1}, a_2 = \lfloor \alpha_2 \rfloor, \dots, \alpha_n := \frac{1}{\alpha_{n-1} - a_{n-1}}, a_n = \lfloor \alpha_n \rfloor \\ &\dots\end{aligned}$$

Snadno nahlédneme, že $\alpha_1, \alpha_2, \dots \in (1, \infty)$, proto také $a_1, a_2, \dots \in \mathbb{N}$

Důkaz tvrzení pokrač.

Chceme dokázat, že $\alpha = [a_0; a_1, a_2, \dots]$.

Pro každé $n \geq 2$ jistě platí

$$\alpha = [a_0; a_1, \dots, a_{n-1}, \alpha_n]$$

Proto také (tento vztah budeme potřebovat později)

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

kde $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \dots$ jsou konvergenty $[a_0; a_1, a_2, \dots]$

$$\begin{aligned} \text{Pak } \left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| &= \left| \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} \right| = \\ &= \left| \frac{\alpha_n p_{n-1} q_{n-1} + p_{n-2} q_{n-1} - \alpha_n q_{n-1} p_{n-1} - q_{n-2} p_{n-1}}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} \right| = \left| \frac{p_{n-2} q_{n-1} - q_{n-2} p_{n-1}}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} \right| \leq \\ &= \frac{|(-1)^{n+1}|}{q_{n-1}^2}. \end{aligned}$$

Snadno se nahlédne, že $\lim_{n \rightarrow \infty} q_n = \infty$

Hledání řetězového rozvoje odmocniny

Pro $N \in \mathbb{N}$ takové, že $\sqrt{N} \notin \mathbb{Q}$ chceme najít $a_0, a_1, \dots \in \mathbb{N}$ tak, aby platilo $\sqrt{N} = [a_0; a_1, a_2, \dots]$.

Tvrzení

Necht' $N \in \mathbb{N}$ splňuje $\sqrt{N} \notin \mathbb{Q}$. Označme $\alpha_0, \alpha_1, \dots \in \mathbb{R}$ a $a_0, a_1, \dots \in \mathbb{Z}$ dané vztahy

$$\alpha_0 := \sqrt{N}, a_0 = \lfloor \alpha_0 \rfloor, \alpha_1 := \frac{1}{\alpha_0 - a_0}, a_1 = \lfloor \alpha_1 \rfloor$$

$$\dots, \alpha_n := \frac{1}{\alpha_{n-1} - a_{n-1}}, a_n = \lfloor \alpha_n \rfloor, \dots$$

Pro každé $n \in \mathbb{N}_0$ existují $R_n, S_n \in \mathbb{Z}$, $S_n \neq 0$ takové, že

$$\alpha_n = \frac{R_n + \sqrt{N}}{S_n}, a_n = \left\lfloor \frac{R_n + \sqrt{N}}{S_n} \right\rfloor = \left\lfloor \frac{R_n + \lfloor \sqrt{N} \rfloor}{S_n} \right\rfloor.$$

Poznámka:

Z důkazu uvidíme i postup pro výpočet čísel R_i, S_i :

$R_0 := 0, S_0 := 1$ a pro $i \geq 0$ je $R_{i+1} = a_i S_i - R_i$ a $S_{i+1} = \frac{N - R_{i+1}^2}{S_i}$

Důkaz tvrzení:

Položíme $R_0 := 0, S_0 := 1$. Pak $\alpha_0 = \sqrt{N} = \frac{R_0 + \sqrt{N}}{S_0}$.

Přepokládejme, že platí $\alpha_i = \frac{R_i + \sqrt{N}}{S_i}$. Prvek $\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$ vyjádříme ve tvaru $q_1 + q_2\sqrt{N}$, $q_1, q_2 \in \mathbb{Q}$, ze kterého dostaneme vzorce pro S_{i+1} a R_{i+1} . Nakonec dokážeme $S_{i+1}, R_{i+1} \in \mathbb{Z}$ a $S_{i+1} \neq 0$.

$$\begin{aligned}\alpha_{i+1} &= \frac{1}{\alpha_i - a_i} = \frac{1}{\frac{R_i + \sqrt{N}}{S_i} - a_i} = \frac{S_i}{R_i - a_i S_i + \sqrt{N}} = \\&= \frac{S_i}{R_i - a_i S_i + \sqrt{N}} \cdot \frac{R_i - a_i S_i - \sqrt{N}}{R_i - a_i S_i - \sqrt{N}} = \frac{S_i(R_i - a_i S_i - \sqrt{N})}{(R_i - a_i S_i)^2 - N} = \\&= \frac{a_i S_i - R_i + \sqrt{N}}{\frac{N - (R_i - a_i S_i)^2}{S_i}}\end{aligned}$$

Nabízí se proto definovat $R_{i+1} := a_i S_i - R_i$ a $S_{i+1} = \frac{N - R_{i+1}^2}{S_i}$.

Důkaz tvrzení pokrač:

Definujeme $R_0 := 0$, $S_0 := 1$ a pro $i \in \mathbb{N}$ položíme

$$R_{i+1} := a_i S_i - R_i \text{ a } S_{i+1} := \frac{N - R_{i+1}^2}{S_i}, \text{ kde } a_i := \left\lfloor \frac{R_i + \sqrt{N}}{S_i} \right\rfloor.$$

Indukcí dokážeme, že $R_i, S_i \in \mathbb{Z}$ a $S_i \neq 0$ pro každé $i \in \mathbb{N}$.

Pokud máme $a_i, S_i, R_i \in \mathbb{Z}$ bude $R_{i+1} \in \mathbb{Z}$ a $S_{i+1} \neq 0$ (jinak je N čtverec celého čísla).

Zbývá proto dokázat, že $S_{i+1} = \frac{N - R_{i+1}^2}{S_i} \in \mathbb{Z}$. Máme

$$N - R_{i+1}^2 = N - (R_i - a_i S_i)^2 = N - R_i^2 + 2a_i R_i S_i - a_i^2 S_i^2$$

Protože je $N - R_i^2 = S_i S_{i-1}$ bude z $S_{i-1} \in \mathbb{Z}$ plynout $S_i \mid N - R_{i+1}^2$.

Dokončení důkazu

Zbývá ještě ověřit $\lfloor \frac{R_n + \sqrt{N}}{S_n} \rfloor = \lfloor \frac{R_n + \lfloor \sqrt{N} \rfloor}{S_n} \rfloor$.

Později ukážeme, že $S_n > 0$.

Označme $A_n, B_n \in \mathbb{Z}$ taková, že

$$R_n + \lfloor \sqrt{N} \rfloor = A_n S_n + B_n, B_n \in \{0, 1, \dots, S_n - 1\}$$

Pak $A_n = \lfloor \frac{R_n + \lfloor \sqrt{N} \rfloor}{S_n} \rfloor$

Označme dále $\varepsilon \in (0, 1)$ tak, že $\sqrt{N} = \lfloor \sqrt{N} \rfloor + \varepsilon$. Pak

$$\lfloor \frac{R_n + \sqrt{N}}{S_n} \rfloor = \lfloor \frac{R_n + \lfloor \sqrt{N} \rfloor + \varepsilon}{S_n} \rfloor = \lfloor \frac{A_n S_n + B_n + \varepsilon}{S_n} \rfloor$$

Tedy skutečně $\lfloor \frac{R_n + \sqrt{N}}{S_n} \rfloor = \lfloor \frac{R_n + \lfloor \sqrt{N} \rfloor}{S_n} \rfloor = A_n$

Algoritmus pro řetězový rozvoj $\sqrt{N}$

Vstup: $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{Q}$, $k \in \mathbb{N}$

Výstup: $a_0, a_1, \dots, a_k \in \mathbb{N}$, počátek řetězového rozvoje $\sqrt{N}$,
 $p_i, q_i \in \mathbb{N}$ splňující $[a_0; a_1, \dots, a_i] = \frac{p_i}{q_i}$

1. $R_0 := 0$, $S_0 := 1$, $g := \lfloor \sqrt{N} \rfloor$, $a_0 := g$, $p_0 := g$, $q_0 := 1$,
 $p_{-1} := 1$, $q_{-1} := 0$

2. **for** $i = 1$ **to** k **do**

$$R_i := a_{i-1}S_{i-1} - R_{i-1}, S_i := \frac{N - R_i^2}{S_{i-1}}$$

$$a_i := \lfloor \frac{R_i + g}{S_i} \rfloor$$

$$p_i := a_i p_{i-1} + p_{i-2}, q_i := a_i q_{i-1} + q_{i-2}$$

3. **return** $a_0, a_1, \dots, a_k$, $p_0, p_1, \dots, p_k$, $q_0, q_1, \dots, q_k$

Generátor relací pro CFRAC

Tvrzení

Máme $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{Q}$, necht' $\sqrt{N}$ je hodnota nekonečného řetězového zlomku

$$\sqrt{N} = [a_0; a_1, a_2, \dots]$$

Necht' $p_{-2}, p_{-1}, p_0, \dots, q_{-2}, q_{-1}, q_0, \dots, R_0, R_1, \dots, S_0, S_1, \dots$ jsou posloupnosti definované vztahy

$$p_{-2} := 0, p_{-1} := 1, p_i = a_i p_{i-1} + p_{i-2}, i \geq 0$$

$$q_{-2} := 1, q_{-1} := 0, q_i = a_i q_{i-1} + q_{i-2}, i \geq 0$$

$$R_0 = 0, S_0 = 1, R_i := a_{i-1} S_{i-1} - R_{i-1}, S_i := \frac{N - R_i^2}{S_{i-1}}, i \geq 1$$

Pak pro každé $n \geq 0$ je

$$p_{n-1}^2 - N q_{n-1}^2 = (-1)^n S_n, p_{n-1}^2 \equiv (-1)^n S_n \pmod{N}.$$

$$\text{Důkaz } p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$$

Pro $n = 0$ máme $1^2 - N \cdot 0^2 = (-1)^0 \cdot 1$.

Při zavedeném značení

$$\sqrt{N} = \alpha_0 = [a_0; a_1, \dots, a_{n-1}, \alpha_n]$$

pro každé $n \in \mathbb{N}$, přičemž $\alpha_n = \frac{R_n + \sqrt{N}}{S_n}$.

Dále využijeme vztahu

$$[a_0; a_1, \dots, a_{n-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

Pokračování důkazu $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$

Dostaneme

$$\sqrt{N} = \frac{\frac{R_n + \sqrt{N}}{S_n} p_{n-1} + p_{n-2}}{\frac{R_n + \sqrt{N}}{S_n} q_{n-1} + q_{n-2}} = \frac{R_n p_{n-1} + \sqrt{N} p_{n-1} + p_{n-2} S_n}{R_n q_{n-1} + \sqrt{N} q_{n-1} + q_{n-2} S_n}$$

$$Nq_{n-1} + (R_n q_{n-1} + q_{n-2} S_n) \sqrt{N} = (R_n p_{n-1} + p_{n-2} S_n) \cdot 1 + p_{n-1} \sqrt{N}$$

Protože $1, \sqrt{N}$ jsou lineárně nezávislé prvky v $\mathbb{Q}$ -lineárním prostoru $\mathbb{R}$, lze předchozí rovnost roztrhnout na dvě.

$$R_n p_{n-1} + p_{n-2} S_n = Nq_{n-1}$$

$$R_n q_{n-1} + q_{n-2} S_n = p_{n-1}$$

Dokončení důkazu $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$

Máme vztahy

$$R_n q_{n-1} + q_{n-2} S_n = p_{n-1}$$

$$R_n p_{n-1} + p_{n-2} S_n = N q_{n-1}$$

První přenásobíme p_{n-1} , druhý q_{n-1} a odečteme

$$p_{n-1}^2 - Nq_{n-1}^2 = R_n q_{n-1} p_{n-1} + q_{n-2} p_{n-1} S_n - R_n p_{n-1} q_{n-1} - p_{n-2} q_{n-1} S_n$$

$$p_{n-1}^2 - Nq_{n-1}^2 = S_n(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}).$$

K dokončení důkazu stačí využít $p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$ pro každé $i \geq 0$

Proč je každé $S_n > 0$?

Při značení z předešlého tvrzení je $\sqrt{N} = \lim_{n \rightarrow \infty} \frac{p_n}{q_n}$. Není těžké si rozmyslet, že platí

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \sqrt{N} < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Pro $n \geq 1$ uvažme rovnost $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$ ve tvaru

$$\frac{p_{n-1}^2}{q_{n-1}^2} - N = (-1)^n \frac{S_n}{q_{n-1}^2}$$

Pokud n je liché, bude na levé straně záporné číslo. Aby bylo i na pravé straně záporné číslo, musí platit $S_n > 0$.

Pokud je n sudé, je na levé straně kladné číslo. Aby bylo i na pravé straně kladné číslo, musí být $S_n > 0$

To je pro dešek vše

Děkuji za pozornost.