Problem Skolema – Seminarium Logika i Teoria obliczeń

Marcin Wierzbiński

2 grudnia 2020

Wstęp

- Dlaczego problem równania rekurencyjnego liniowego jest na seminarium LATO?
- Co mają wspólnego równania rekurencyjne liniowe i macierze?
- Jak trudny jest problem Skolema?
- Co mają wspólnego liczby algebraiczne z problemem Skolema?

Zacznijmy od prostego programu

$\vec{u} \in \mathbb{Z}$
$\vec{x} := \vec{a}, \quad \vec{a} \in \mathbb{Z}^k$ ▷ Wejście
while $u^T \cdot \vec{x} \neq 0$ **do**
    $\vec{x} := M\vec{x}$ ▷ $M \in \mathbb{Z}^{k \times k}$

- Jestem zainteresowany problemem stopu dla tego programu
- Zakładamy nieskończoną pamięć, ponieważ $\vec{x}$ może rosnąć bardzo szybko do nieskończoności, np. przy $M = 2$.
- Czy jest to problem rozstrzygalny?

Inne pytanie z terminów automatów

Mamy alfabet Σ oraz A, B skończony automat deterministyczny nad Σ

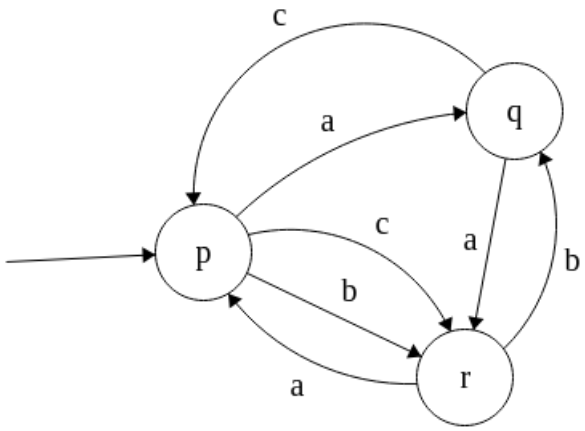
- u_n jest liczbą słów długości n akceptowanych przez A
- v_n jest liczbą słów długości n akceptowanych przez B

Pytanie:

- Czy istnieje n takie, że ilość słów akceptowanych przez A jest równa liczbie słów akceptowanych przez B
- Nie wiadomo, czy problem jest rozstrzygalny czy nierozstrzygalny.

Znana jest rozstrzygalność dla automatów rozmiaru 4

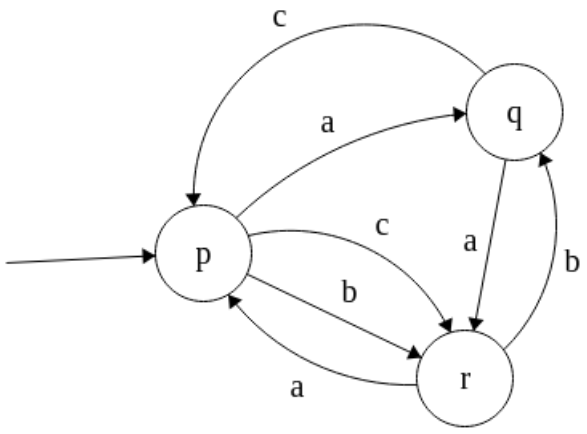
Równoważność pytania – przykład



Rysunek: Automat skończony ze stanami p, g, r i alfabetem $\Sigma = \{a, b, c\}$

$$\begin{cases} p_{n+1} = r_n + g_n \\ g_{n+1} = p_n + r_n \\ r_{n+1} = 2p_n + q_n \\ (p_0, q_0, r_0) = (1, 0, 0) \end{cases}$$

Macierz przejścia dla automatu



Rysunek: Automat skończony ze stanami p, g, r i alfabetem $\Sigma = \{a, b, c\}$

$$(p_{n+1}, q_{n+1}, r_{n+1}) = (p_n, q_n, r_n) \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Liniowe równanie rekurencyjne

$$a_0, \ldots, a_{k-1} \in \mathbb{Z}$$

$$u_0, \ldots, u_{k-1} \in \mathbb{Z} \tag{1}$$

Liniowe równanie rekurencyjne:

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n \tag{2}$$

Zwykłe oznaczenie $<u_n>_{n=1}^{\infty}$ $a_0 \neq 0$

Przykład równania liniowego rekurencyjnego rzędu 2:

Przykład

Ciąg Fibonacciego:

$$\begin{cases} u_{n+2} = u_{n+1} + u_n \\ u_1 = 1 \\ u_0 = 0 \end{cases}$$

Zapis macierzowy

$$\exists v, w \in \mathbb{Z}^k, M \in \mathbb{Z}^{k \times k}$$

$$u_n = v^t M^n w$$

$$M = \begin{bmatrix} a_{k-1} & 1 & \dots & 0 & 0 \\ a_{k-2} & 0 & \dots & 0 & 0 \\ \vdots & 0 & \dots & 1 & 0 \\ a_1 & 0 & \dots & 0 & 1 \\ a_0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad v = \begin{bmatrix} u_{k-1} \\ u_{k-2} \\ \vdots \\ u_0 \end{bmatrix} \quad w = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Ciąg Fibonacciego – Zapis macierzowy:

$$\begin{cases} u_{n+2} = u_{n+1} + u_n \\ u_1 = 1 \\ u_0 = 0 \end{cases}$$

$$\begin{bmatrix} u_{n+2} & u_{n+1} \\ u_{n+1} & u_n \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} u_{n+3} & u_{n+2} \\ u_{n+2} & u_{n+1} \end{bmatrix}$$

Ponieważ równocześnie:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} u_2 & u_1 \\ u_1 & u_0 \end{bmatrix}$$

to indukcyjnie:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{bmatrix} \quad \left| \quad \begin{bmatrix} u_{n+1} \\ u_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \cdot \begin{bmatrix} u_1 \\ u_0 \end{bmatrix} \right.$$

Suma ciągów liniowych rekurencyjnych

Weźmy dwa ciągi liniowe rekurencyjne f_n, g_n

$$f_n = [1,0]\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}^n\begin{bmatrix}1 & 0\end{bmatrix}$$

$$g_n = [2,5]\begin{bmatrix}3 & 2\\ 0 & -1\end{bmatrix}^n\begin{bmatrix}2 & -1\end{bmatrix}$$

$u_n = f_n - g_n$ jest ciągiem rekurencyjnym

$$f_n - g_n = [1,0|2,5]\left[\begin{array}{cc|cc} 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ \hline 0 & 0 & 3 & 2\\ 0 & 0 & 0 & -1\end{array}\right]\left[\begin{array}{c} 1\\ 0\\ \hline -2\\ 1\end{array}\right]$$

Wielomian charakterystyczny

$$M \in \mathbb{Z}^{k \times k} \tag{3}$$

Definicja

Wielomian charakterystyczny $p_A(t)$ macierzy kwadratowej M definiuje się jako:

$$p_M(\lambda) = \det(\mathrm{M} - \lambda \mathbb{1}). \tag{4}$$

Definicja

Zbiór wartości własnych λ_i to pierwiastki tego wielomianu.

Lemat redukcji

Twierdzenie (Cayleya-Hamiltona)

Jeśli $p_M(t)$ jest wielomianem charakterystycznym dla macierzy M, wtedy macierz $p_M(M)$ jest macierzą zerową.

Twierdzenie

Niech $v, w \in \mathbb{Z}^k, M \in \mathbb{Z}^{k\times k}$, $u_n = v^t M^n w \in \mathbb{Z}$ oraz

$$M = \begin{bmatrix} a_{k-1} & 1 & \dots & 0 & 0 \\ a_{k-2} & 0 & \dots & 0 & 0 \\ \vdots & 0 & \dots & 1 & 0 \\ a_1 & 0 & \dots & 0 & 1 \\ a_0 & 0 & \dots & 0 & 0 \end{bmatrix} \quad v = \begin{bmatrix} u_{k-1} \\ u_{k-2} \\ \vdots \\ u_0 \end{bmatrix} \quad w = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Wtedy i tylko wtedy $<u_n>_{n=1}^{\infty}$ jest liniowym równaniem rekurencyjnym.

Twierdzenie c.d

Dowód.

Weźmy M z twierdzenia CH:

$$M^k = a_1 M^{k-1} + \ldots + a_k \mathbb{1} \tag{5}$$

$$v^t M^k = a_1 v^t M^{k-1} + \ldots + a_k v^t \mathbb{1} \tag{6}$$

$$v^t M^k M^n = a_1 v^t M^{k-1} M^n + \ldots + a_k v^t \mathbb{1} M^n \tag{7}$$

$$v^t M^{k+n} w = a_1 v^t M^{k-1+n} w + \ldots + a_k v^t M^n w \tag{8}$$

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n \tag{9}$$

□

W drugą stronę

Dowód.

Niech $<u_n>_{n=1}^{\infty}$ będzie równaniem liniowym rekurencyjnym z warunkiem początkowym: $u_0 \ldots u_{k-1} \in \mathbb{Z}$ i dla $n \geqslant k$

$$u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_k$$

Sprawdźmy bazę indukcyjną:

$n = 0$, wtedy dla $v = \begin{bmatrix} u_{k-1} \\ u_{k-2} \\ \vdots \\ u_0 \end{bmatrix}$ $w = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$

$u_0 = v^t \mathbb{1} w = u_0$,

dalej indukcyjnie

□

Równania rekurencyjne

Równanie rekurencyjne Fibonacciego:

$$u_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n .$$

Jak zapisać ciągi za pomocą równania liniowego rekurencyjnego?

- $u_n = n$
- $u_n = u_{n-1} + 1$
- $u_n = n^2$
- $u_n = 3u_{n+2} - 3u_{n+1} + u_n$

Rozkład dla ciągu Fibonacciego

$$\begin{bmatrix} u_{n+1} \\ u_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} u_1 \\ u_0 \end{bmatrix} \tag{10}$$

Liczymy rozkład $M = PDP^{-1}$ i uzyskujemy
$\lambda_1 = \frac{1}{2}\left(1 - \sqrt{5}\right), \lambda_2 = \frac{1}{2}\left(1 - \sqrt{5}\right)$

$$u_n = \begin{bmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix} \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & \lambda_2 \\ -1 & \lambda_1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{11}$$

$$u_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}} \tag{12}$$

Liczby algebraiczne

Definicja

Powiemy, że a jest liczbą algebraiczną, jeżeli jest pierwiastkiem niezerowego wielomianu $p \in \mathbb{Q}[x]$. Zbiór liczb algebraicznych oznaczmy jako $\mathbb{A}$.

Przykład

Liczba $\sqrt{2}$ jest liczbą algebraiczną wielomianu $p(x) = x^2 - 2$

Problem Skolema dla równania rzędu 2

Twierdzenie

Niech u_n będzie równaniem rekurencyjnym liniowym rzędu 2

$$u_n = c_1 u_{n+1} + c_2 u_n$$

$$c_1, c_2 \in \mathbb{Q}$$

$$u_0, u_1 \in \mathbb{Q}$$

wówczas jest rozstrzygalny tj. potrafimy określić czy $\exists n : u_n = 0$?

Przykłady problemów

- $u_{n+2} = u_{n+1} + u_n$
- $u_1 = 1,\ u_2 = 1$
  - u_n nigdy nie jest zero, jest dodatni
  - i $\lambda_1 > \lambda_2$
- $u_n = -2u_{n-1} + u_{n-2}$,
  - dla $u_0 = 2, u_1 = 1$ n $= 3$ i tylko dla niego
  - $u_n = (1 - \frac{3}{2\sqrt{2}})(-1 - \sqrt{2})^n + \frac{1}{4}(4 + 3\sqrt{2})(\sqrt{2} - 1)^n$
  - współczynnik z lewej strony dominuje dla dużego n

Przykłady problemów

- $u_n = 2x_{n-1} - 3x_{n-2}$
- $u_0 = 0, u_1 = 1$
  - $\lambda_1 = 1 + i\sqrt{2}, \lambda_2 = 1 - i\sqrt{2}$
  - $|\lambda_1| = |\lambda_2|$
  - tylko $u_0 = 0$ spełnia (trudne)
- $u_n = u_{n-2}$
- $u_0 = 0,\ u_1 = 1$
  - dla n parzystego mamy $u_n = 0$ [1]

[1] [2]

$\lambda_1 = \lambda_2$

Dowód.

$$u_n = 0 \iff u_n = an\lambda^n + b\lambda^n = 0$$

$$an\lambda^n + b\lambda^n = 0$$

$$an + b = 0$$

Rozwiązywalne dla $a, b \in \mathbb{A}$ $\square$

Szkic dowodu $\lambda_1 \neq \lambda_2$

Dla: $|\lambda_1| > |\lambda_2|, \lambda_1, \lambda_2 \in \mathbb{R}$ otrzymujemy równanie charakterystyczne:

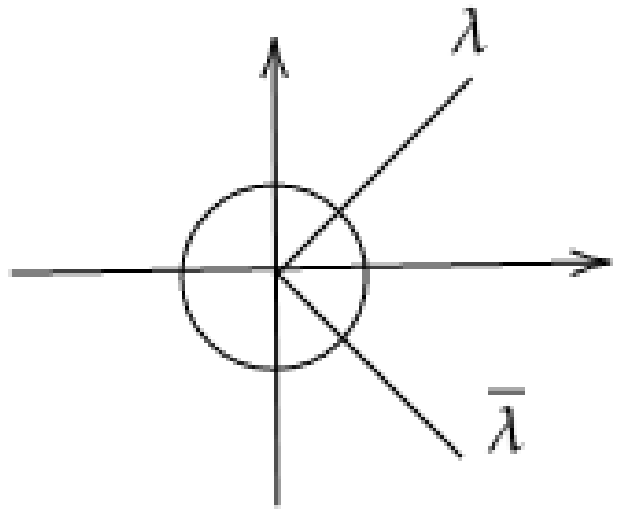
$$a_1\lambda_1^n + a_2\lambda_2^n = 0$$

$$-\frac{a_1}{a_2} = (\frac{\lambda_2}{\lambda_1})^n$$

Powyżej pewnego n nie ma szans na równość

$|\lambda_1| = |\lambda_2|$ i $\lambda_1 \neq \lambda_2$

Wiemy, że występują w parach sprzężonych.



$$u_n = a\lambda^n + \overline{a}\overline{\lambda}^n$$

$$u_n = 0$$

$$a\lambda^n + \overline{a}\overline{\lambda}^n = 0 \iff Re(a\lambda^n) = 0$$

$|\lambda_1| = |\lambda_2|$ i $\lambda_1 \neq \lambda_2$

Weźmy:

$$v = \frac{\lambda}{|\lambda|} \qquad\qquad |v| = 1$$

$$\frac{u_n}{|\lambda|^n} = 0 \iff u_n = 0$$

$$\frac{u_n}{|\lambda|^n} = av^n + \overline{av}^n$$

av^n zanika na osi rzeczywistej $\iff u_n = 0 \iff$

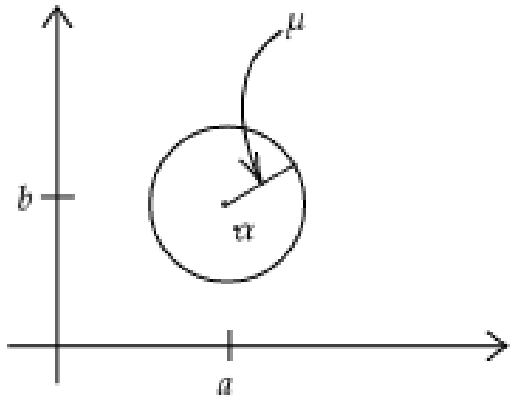
$$v^n = \frac{ic}{a} \qquad\qquad \text{gdzie} \quad |\frac{c}{a}| = 1$$

$v^n = \beta$ gdzie β jest pewną liczbą algebraiczną o module 1

Potrzebujemy rozwiązać równanie $v^n = \beta, v, \beta \in \mathbb{A}$

Reprezentacja liczb algebraicznych

Mamy wielomian $p(x) = a_0 + a_1 x + \ldots a_t x^t$ stopnia t, niech α będzie jedynym pierwiastkiem, d jest stopniem wielomianu $p(x)$.



Rysunek: Otoczenie liczby algebraicznej

współczynniki $a, b, \mu \in \mathbb{Q}$, gdzie α jest unikatowym pierwiastkiem wielomianu p w obrębie μ

Reprezentacja liczb algebraicznych

$$H(P) = \max\{|a_0|, \ldots, |a_t|\}$$

$$deg = deg(p)$$

Twierdzenie (Mignotte)

Jeśli $\alpha, \beta \in \mathbb{A}$ są różnymi pierwiastkami wielomianu p, to $|\alpha - \beta| > \frac{\sqrt{6}}{deg^{\frac{deg+1}{2}} H(P)^{deg-1}}$

$\exists n : u_n = 0$ dla równania $a^n = \beta$

Niech $a \in \mathbb{Z}$

$$v_p(a) = \begin{cases} 0 & \text{dla} \quad p \\ k & \text{dla} \quad p^k | a \quad \text{i} \quad a \nmid p^{k+1} \\ \infty & \text{dla} \quad a = 0 \end{cases} \tag{13}$$

Własność: $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$

$$v_p(a^n) = v_p(\beta)$$

$$n \cdot v_p(a) = v_p(\beta)$$

Powyżej pewnego n nie ma szans na równość.

Podsumowanie

- Dla liniowych rekurencyjnych ciągów o wyrazach całkowitych problem Skolema jest znany jako NP-trudny. [1]
- Potrzebna jest algebraiczna teoria liczb do rozwiązania prostego problemu rzędu 2 [3]
- Problemy z reprezentacją liczb algebraicznych można zastąpić poprzez jej wielomiany i bliskie otoczenia zer. [4]
- Nierozstrzygalność dla ciągów liniowych rekurencyjnych rzędu 5.

Referencje


Vincent D. Blondel and Natacha Portier.
The presence of a zero in an integer linear recurrent sequence is np-hard to decide.
Linear Algebra and its Applications, 351-352:91 – 98, 2002.
Fourth Special Issue on Linear Systems and Control.


Daniel Litt.
Zeroes of integer linear recurrences.


Filip Mazowiecki and Joël Ouaknine.
Automata and sequences course.


Joel Ouaknine and James Worrell.
Ultimate positivity is decidable for simple linear recurrence sequences, 2017.

Koniec

Dziękuje za uwagę