Języki, automaty i obliczenia

Wykład 11: Nieobliczalność

Sławomir Lasota

Uniwersytet Warszawski

22 maja 2024

Plan

Problem $L \subseteq A^*$ *redukuje się* (*sprowadza się*) do problemu $K \subseteq B^*$ jeśli istnieje funkcja obliczalna

$$f : A^* \to B^*$$

taka, że

$$w \in L \iff f(w) \in K, \quad \text{dla każdego } w \in A^*.$$

rysunek

Ozn. $L \leq K$.

Fakt

Jeśli $L \leq K$ to $\bar{L} \leq \bar{K}$.

Fakt

Jeśli $L \leq K$ i problem K jest (częściowo) rozstrzygalny to problem L jest też (częściowo) rozstrzygalny.

Dowód:

...

rysunek

Dowód nierozstrzygalności

Niech $A = \{0, 1\}$.

Problem stopu

Dane:	maszyna Turinga $\mathcal{M}$ i słowo w
Wynik:	czy $w \in L(\mathcal{M})$?

$\leq$

Niepustość języka maszyny Turinga

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $L(\mathcal{M}) \neq \emptyset$?

funkcja obliczalna:	$\mathcal{M}, w$	$\longmapsto$	$\mathcal{M}'$
poprawność:	$w \in L(\mathcal{M})$	$\iff$	$L(\mathcal{M}') \neq \emptyset$

Maszyna $\mathcal{M}'$ działa następująco:

- ignoruje swoje słowo wejściowe
- pisze na taśmie słowo w
- symuluje maszynę M na słowie w
- akceptuje, gdy M akceptuje

Dowód nierozstrzygalności

Ta sama redukcja dowodzi:

Problem stopu

Dane:	maszyna Turinga $\mathcal{M}$ i słowo w
Wynik:	czy $w \in L(\mathcal{M})$?

$\leq$

Problem stopu na ε

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $\varepsilon \in L(\mathcal{M})$?

Problem stopu

Dane:	maszyna Turinga $\mathcal{M}$ i słowo w
Wynik:	czy $w \in L(\mathcal{M})$?

$\leq$

Uniwersalność języka maszyny T.

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $L(\mathcal{M}) = A^*$?

Nierozstrzygalność x 2

Problem stopu

Dane: maszyna Turinga $\mathcal{M}$ i słowo w

Wynik: czy $w \in L(\mathcal{M})$?

$\leq$

Uniwersalność języka maszyny T.

Dane: maszyna Turinga $\mathcal{M}$

Wynik: czy $L(\mathcal{M}) = A^*$?

Problem stopu

Dane: maszyna Turinga $\mathcal{M}$ i słowo w

Wynik: czy $w \in L(\mathcal{M})$?

$\leq$

Nieuniwersalność języka maszyny T.

Dane: maszyna Turinga $\mathcal{M}$

Wynik: czy $L(\mathcal{M}) \neq A^*$?

Dowód nierozstrzygalności

Niepustość języka maszyny Turinga

Dane: maszyna Turinga $\mathcal{M}$

Wynik: czy $L(\mathcal{M}) \neq \emptyset$?

$\leq$

Nieuniwersalność języka bezkont.

Dane: język bezkontekstowy $L \subseteq A^*$

Wynik: czy $L \neq A^*$?

funkcja obliczalna: $\mathcal{M} \longmapsto \mathcal{G}$

poprawność: $L(\mathcal{M}) = \emptyset \iff L(\mathcal{G}) = A^*$

Bieg maszyny $\mathcal{M}$:

$$\rho = c_0 \longrightarrow_{\mathcal{M}} c_1 \longrightarrow_{\mathcal{M}} \ldots \longrightarrow_{\mathcal{M}} c_n$$

$$w_\rho = \$c_0\$c_1\$ \ldots \$c_n\$$$

Niech $L(\mathcal{G}) = \overline{\{ w_\rho : \rho \text{ bieg akceptujący maszyny } \mathcal{M} \}}$

Fakt

Język $\overline{\{ c\$c' : c \longrightarrow_{\mathcal{M}} c' \}}$ jest bezkontekstowy.

Problem stopu jest zupełny

Twierdzenie

Każdy problem częściowo rozstrzygalny redukuje się do problemu stopu.

Dowód:

Niech L częściowo rozstrzygalny i niech $L = L(\mathcal{M})$.

$$\begin{array}{rccc} \text{funkcja obliczalna:} & w & \longmapsto & \mathcal{M}, w \\ \text{poprawność:} & w \in L & \iff & w \in L(\mathcal{M}) \end{array}$$

Wniosek

Jeśli (problem stopu) $\leq L$ *to* L *też jest zupełny.*

Wszystkie własności języków cz.r. są nierozstrzygalne

Ustalmy A, np. $A = \{0, 1\}$. *Własność* języków to dowolny podzbiór $\mathcal{L} \subseteq \mathcal{P}(A^*)$.

Własność $\mathcal{L}$ jest *trywialna* jeśli

- albo $\mathcal{L}$ nie zawiera żadnego języka częściowo rozstrzygalnego,
- albo $\mathcal{L}$ zawiera je wszystkie.

Przykładowe własności nietrywialne:

- skończoność,
- ko-skończoność,
- rozstrzygalność,
- język zawiera wszystkie słowa długości parzystej.

Twierdzenie Rice'a

Dla każdej *nietrywialnej* własności $\mathcal{L}$, następujący problem jest nierozstrzygalny:

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $L(\mathcal{M}) \in \mathcal{L}$?

Dowód:

B.u.o. załóżmy, że $\emptyset \notin \mathcal{L}$. Wybierzmy dowolną maszynę $\mathcal{M}_0$ t.że $L(\mathcal{M}_0) \in \mathcal{L}$.

Problem stopu na ε

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $\varepsilon \in L(\mathcal{M})$?

$$\leq$$

Własność $\mathcal{L}$

Dane:	maszyna Turinga $\mathcal{M}$
Wynik:	czy $L(\mathcal{M}) \in \mathcal{L}$?

Funkcja obliczalna:

$\mathcal{M} \quad \mapsto \quad \mathcal{M}'$: najpierw sprawdź, czy $\varepsilon \in L(\mathcal{M})$, ignorując słowo wejściowe; następnie uruchom $\mathcal{M}_0$ na słowie wejściowym.

Poprawność:

$$\varepsilon \in L(\mathcal{M}) \iff L(\mathcal{M}') \in \mathcal{L}$$

Problem odpowiedniości Posta (PCP)

Dane: ciąg par słów $(w_1, v_1), \ldots, (w_n, v_n)$.

Wynik: czy istnieje niepusty ciąg $(i_1, \ldots, i_m)$ t. że $w_{i_1} \ldots w_{i_m} = v_{i_1} \ldots v_{i_m}$?

Odpowiedni ciąg $(i_1, \ldots, i_m)$ nazywamy *rozwiązaniem*.

Inne sformułowanie

Przykład

Instancja

$$(b, bbb),\ (babbb, ba),\ (ba, a)$$

1	b	bbb
2	babbb	ba
3	ba	a

ma rozwiązanie $(2, 1, 1, 3)$:

$$babbb\ b\ b\ ba \ = \ ba\ bbb\ bbb\ a$$

a poniższa instancja nie ma rozwiązań:

$$(ba, bab),\ (abb, bb),\ (bab, abb)$$

1	ba	bab
2	abb	bb
3	bab	abb

Twierdzenie

Problem odpowiedniości Posta jest nierozstrzygalny.

Ograniczony problem odpowiedniości Posta (ograniczony PCP)

Dane: ciąg par słów $(w_1, v_1), \ldots, (w_n, v_n)$.

Wynik: czy istnieje niepusty ciąg $(i_1, \ldots, i_m)$ t. że $w_{i_1} \ldots w_{i_m} = v_{i_1} \ldots v_{i_m}$ i $i_1 = 1$?

Lemat

Ograniczony PCP $\leq$ *PCP.*

Dowód:

1	b	bbb
2	babbb	ba
3	ba	a

$\longmapsto$

0	$*$b$*$	$*$b$*$b$*$b
1	b$*$	$*$b$*$b$*$b
2	b$*$a$*$b$*$b$*$b$*$	$*$b$*$a
3	b$*$a$*$	$*$a
4	$	$*$$

$(1, i_2, \ldots, i_m)$ jest rozwiązaniem $\iff$ $(0, i_2, \ldots, i_m, n+1)$ jest rozwiązaniem

Dowód nierozstrzygalności PCP (c.d.)

Lemat

Problem stopu $\leq$ *ograniczony PCP.*

Dowód:

Bieg akceptujący maszyny $\mathcal{M}$ na słowie w, czyli $q_0 w \longrightarrow_{\mathcal{M}} c_1 \longrightarrow_{\mathcal{M}} \ldots \longrightarrow_{\mathcal{M}} c_n$, odpowiada rozwiązaniu PCP postaci $\$q_0 w\$c_1\$ \ldots \$c_n\$d_1\$ \ldots \$d_j\$q_{\mathrm{tak}}\$\$$.

$\mathcal{M}, w \qquad \longmapsto$

	$\$$	$\$q_0 w\$$	
	0	0	
	1	1	
	$\mathbb{B}$	$\mathbb{B}$	
	$\$$	$\$$	
	$q\ a$	$q'\ a'$	jeśli $(q, a, q', a', \circlearrowright) \in \delta$
	$q\ a$	$a'\ q'$	jeśli $(q, a, q', a', \rightarrow) \in \delta$
	$b\ q\ a$	$q'\ b\ a'$	jeśli $(q, a, q', a', \leftarrow) \in \delta$
	$q\ \$$	$a'\ q'\ \$$	jeśli $(q, \mathbb{B}, q', a', \rightarrow) \in \delta$
	$\$\ q\ a$	$\$\ q'\ \mathbb{B}\ a'$	jeśli $(q, a, q', a', \leftarrow) \in \delta$
	$\ldots$	$\ldots$	
	$q_{\mathrm{tak}}\ a$	q_{tak}	
	$a\ q_{\mathrm{tak}}$	q_{tak}	
	$q_{\mathrm{tak}}\ \$\$$	$\$$	

Plan

1. Jak dowodzić nierozstrzygalności?
2. „Najprostszy'' problem nierozstrzygalny
3. Funkcje nieobliczalne: pracowite bobry

Modele obliczeń równoważne maszynom Turinga

- gramatyki typu 0
- automaty z wieloma stosami
- automaty z licznikami
- automaty z kolejką
- maszyny RAM (ang. *random access machines*) albo maszyny rejestrowe
- while-programy
- rachunek λ
- ...

Automaty z licznikami

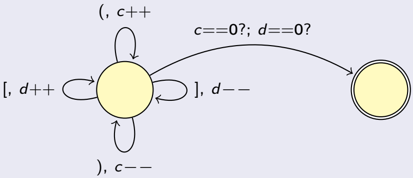
$$\mathcal{A} \;=\; (A, Q, q_0, q_{\mathrm{stop}}, \boxed{C}, \delta)$$

- A – alfabet
- Q – skończony zbiór stanów
- q_0 – stan początkowy
- q_{stop} – stan akceptujący
- C – skończony zbiór liczników
- $\delta \subseteq (Q - \{q_{\mathrm{stop}}\}) \times (A \cup \{\varepsilon\}) \times \boxed{\{\, c{+}{+}, c{-}{-}, c{=}{=}0? \;:\; c \in C \,\}} \times Q$

Przykład

$A \;=\; \{(,), [,]\}$

$C \;=\; \{c, d\}$



$L(\mathcal{A}) \;=\; ?$

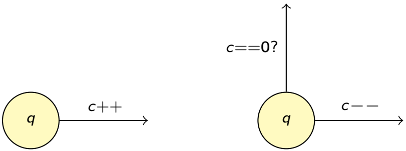
Konfiguracje $= Q \times \mathbb{N}^C$

Deterministyczne automaty z licznikami

Automaty bez wejścia: $\delta \subseteq (Q - \{q_{\mathsf{stop}}\}) \times \{\, c{+}{+}, c{-}{-}, c{=}{=}0? \;:\; c \in C \,\} \times Q$.

Pytanie

Kiedy automat z licznikami jest deterministyczny?



Automaty z licznikami są równoważne maszynom Turinga

Twierdzenie

(Deterministyczne) maszyny Turinga $\equiv$ *(deterministyczne) automaty z licznikami.*

Dowód (idea):

Maszyna Turinga $\rightsquigarrow$ automat z 3 licznikami:

$$\begin{array}{cccccccccccccc} & & & & & & & q & & & & & & \\ & & & & & & & \nabla & & & & & & \\ \ldots & \mathbb{B} & \mathbb{B} & \mathbb{B} & 1 & 1 & 0 & 1 & 1 & 0 & 1 & \mathbb{B} & \mathbb{B} & \ldots \end{array}$$

$$\begin{array}{ccccccccc} & & & & q & & & \\ & & & & \nabla & & & \\ 1 & 1 & 0 & & 1 & 1 & 0 & 1 \end{array}$$

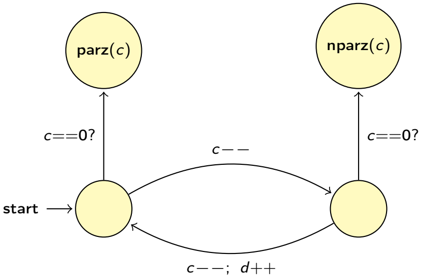
$$6 = 4 + 2 + 0 \qquad 1 + 2 + 0 + 8 = 11$$

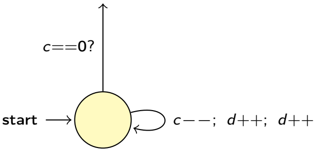
Potrzebne operacje na licznikach:

$$\text{parz}(c)? \qquad \text{nparz}(c)? \qquad c = c >> 1 \qquad c = c << 1$$

Potrzebne operacje na licznikach:

$$\text{parz}(c)? \qquad \text{nparz}(c)? \qquad c = c >> 1 \qquad c = c << 1$$





Jeśli maszyna deterministyczna to automat też.

Twierdzenie

Automaty z 2 licznikami potrafią symulować automaty z 3 licznikami.

Dowód (idea):

3 liczniki c, d, e symulujemy za pomocą 2 liczników x, y:

$$x = 2^c \cdot 3^d \cdot 5^e$$

Pytanie

Czy automaty z 1 licznikiem potrafią symulować automaty z 2 licznikami?

„Najprostszy" problem nierozstrzygalny

Dane:	$\mathcal{A}$ – automat deterministyczny z 2 licznikami c_1, c_2 bez wejścia
Wynik:	czy $\mathcal{A}$ zatrzyma się, jeśli rozpocznie w konfiguracji $(q_0, c_1 = 0, c_2 = 0)$?

Plan

Ustalmy alfabet taśmowy $T = \{a, \mathbb{B}\}$.

Bóbr $\stackrel{\text{def}}{=}$ deterministyczna maszyna Turinga $\mathcal{M}$,

$$\delta : (Q - \{q_{\text{stop}}\}) \times T \to Q \times T \times \{\leftarrow, \circlearrowleft, \rightarrow\},$$

która *zatrzymuje się* na słowie pustym:

$$q_0\, \varepsilon \longrightarrow^*_{\mathcal{M}} u\, q_{\text{stop}}\, v \qquad \text{dla pewnych } u, v \in T^*.$$

Bóbr zaczyna obliczenie z pustą taśmą, a jego *wynik* to liczba symboli a na taśmie w momencie zatrzymania.*

Bobra o najlepszym wyniku spośród bobrów o n stanach (nie licząc q_{stop}) nazwijmy *pracowitym.*

$BB(n) \stackrel{\text{def}}{=}$ wynik pracowitego bobra o n stanach.

$$\begin{array}{llll} BB(1) = 1 & BB(2) = 4 & BB(3) = 6 & BB(4) = 13, \\ BB(5) \geq 4098 & BB(6) \geq 10^{1439} & \dots & \end{array}$$

* inna wersja: liczba kroków, po której się zatrzymuje.

Twierdzenie (Radó 1962)

Funkcja $BB : \mathbb{N} \to \mathbb{N}$ jest nieobliczalna.

Dowód:

Przypuśćmy, że jest. Wtedy obliczalna jest również funkcja $F(n) = BB(2n) + 1$, czyli $F = F(\mathcal{M})$ dla pewne całkowitej maszyny $\mathcal{M}$. Niech N liczba stanów $\mathcal{M}$.

Niech $\mathcal{M}_N$ będzie maszyną, która rozpoczynając z pustą taśmą wypisuje a^N i zatrzymuje się. Jej liczba stanów wynosi N. Złożenie maszyn

$$\mathcal{M}_N;\ \mathcal{M}$$

to maszyna o $2N$ stanach, która osiąga wynik $BB(2N) + 1$. Sprzeczność.

Wniosek

Funkcja BB dominuje,[a] *dla wystarczająco dużych argumentów, każdą funkcję obliczalną.*

[a] Dla każdej funkcji obliczalnej $f : \mathbb{N} \to \mathbb{N}$ istnieje $n_0 \in \mathbb{N}$ takie, że $f(n) < BB(n)$ dla $n > n_0$.

Ciekawostka: wartość $BB(748)$ nie może być wyznaczona na gruncie teorii zbiorów.

W następnym odcinku:

Złożoność czasowa i pamięciowa, klasa NP