

Języki, automaty i obliczenia

Wykład 11: Obliczalność i nieobliczalność

Sławomir Lasota

Uniwersytet Warszawski

25 maja 2016

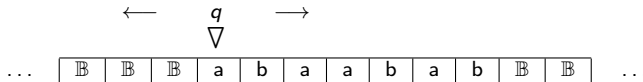
1 Problemy częściowo rozstrzygalne

2 Problemy rozstrzygalne

3 Funkcje (częściowo) obliczalne

4 Jak dowodzić nierozstrzygalności?

Maszyny Turinga:



Język (problem) $L \subseteq A^*$ nazywamy

częściowo rozstrzygalnym, albo *rekurencyjnie przeliczalnym*,

jeśli $L = L(\mathcal{M})$ dla pewnej maszyny Turinga $\mathcal{M}$.

Słowo $w \in A^*$ nazywamy *instancją* problemu.

Przykład

Dane wejściowe: graf skierowany G

Wynik: rozstrzygnąć, czy G ma cykl Hamiltona?

Graf można opisać jako słowo nad $A = \{0, 1, \#\}$, np. 110#101#001

$$\text{maszyna } \mathcal{M} \quad \mapsto \quad w_{\mathcal{M}} \in \{0, 1\}^*$$

Maszynę $\mathcal{M}$ można opisać jako słowo $w_{\mathcal{M}} \in \{0, 1, \#\}^*$, na przykład

00#000000#001000#000011#000##000100#001#010000#100#001##...

albo jako słowo $w_{\mathcal{M}} \in \{0, 1\}^*$, na przykład

00 1 000000 1 001000 000011 000 000100 001 010000 100 001 ...

Twierdzenie

Język uniwersalny (problem stopu)

$$L_u = \{ (\mathcal{M}, w) : w \in L(\mathcal{M}) \}$$

$$L_u = \{ w_{\mathcal{M}} \$ w : w \in L(\mathcal{M}) \} \subseteq \{0, 1, \$\}^*$$

jest częściowo rozstrzygalny.

Pytanie

Czy każdy język jest częściowo rozstrzygalny?

Problem nie częściowo rozstrzygalny

Maszyny Turinga = słowa nad $\{0, 1\}$:

$w_{\mathcal{M}} \in \{0, 1\}^*$ $\longleftrightarrow$ maszyna $\mathcal{M}$

$w \in \{0, 1\}^*$ $\mapsto$ maszyna $\mathcal{M}_w = \begin{cases} \mathcal{M}, & \text{jeśli } w_{\mathcal{M}} = w \\ \mathcal{M}^\emptyset, & \text{w p.p.} \end{cases}$

$$L(\mathcal{M}^\emptyset) = \emptyset$$

Język „przekątniowy”:

$$L_p = \{ w : w \notin L(\mathcal{M}_w) \}$$

$$L_p = \{ \mathcal{M} : \mathcal{M} \notin L(\mathcal{M}) \}$$

Twierdzenie

Język L_p nie jest częściowo rozstrzygalny.

Dowód:

Przypuśćmy, że $L(\mathcal{M}) = L_p$. Wtedy

paradoks golibrody

$$\mathcal{M} \in L(\mathcal{M}) \iff \mathcal{M} \notin L(\mathcal{M})$$

$$w_{\mathcal{M}} \in L(\mathcal{M}) \iff w_{\mathcal{M}} \notin L(\mathcal{M}_{w_{\mathcal{M}}}) \iff w_{\mathcal{M}} \notin L(\mathcal{M}).$$

1 Problemy częściowo rozstrzygalne

2 Problemy rozstrzygalne

3 Funkcje (częściowo) obliczalne

4 Jak dowodzić nierozstrzygalności?

Deterministyczna maszyna Turinga $\mathcal{M} = (A, Q, q_0, q_{\text{tak}}, T, \mathbb{B}, \delta)$

- $q_{\text{tak}} \in Q$ – stan akceptujący
- $\delta : (Q - \{q_{\text{tak}}\}) \times T \rightarrow Q \times T \times \{\leftarrow, \circlearrowleft, \rightarrow\}$

Twierdzenie

Dla każdej maszyny Turinga istnieje równoważna maszyna deterministyczna.

Dowód:

?

Deterministyczna maszyna Turinga $\mathcal{M} = (A, Q, q_0, q_{\text{tak}}, q_{\text{nie}}, T, \mathbb{B}, \delta)$

- $q_{\text{tak}} \in Q$ – stan akceptujący
- $q_{\text{nie}} \in Q$ – stan odrzucający
- $\delta : (Q - \{q_{\text{tak}}, q_{\text{nie}}\}) \times T \rightarrow Q \times T \times \{\leftarrow, \circ, \rightarrow\}$

Konfiguracje **końcowe**:

$$T^*\{q_{\text{tak}}, q_{\text{nie}}\}T^* = \{w q w' : q \in \{q_{\text{tak}}, q_{\text{nie}}\}; w, w' \in T^*\}$$

Deterministyczna maszyna Turinga $\mathcal{M}$ **zatrzymuje się** dla słowa wejściowego w jeśli

$$q_0 w \xrightarrow{*}_{\mathcal{M}} c$$

dla jakiejś konfiguracji końcowej c .

Maszyna $\mathcal{M}$ jest **całkowita**, jeśli zatrzymuje się dla każdego słowa wejściowego.

$$L(\mathcal{M}) = \{a^n b a^n : n \in \mathbb{N}\}$$

	a	b	$\mathbb{B}$	$\#$
start $\rightarrow$	(cont $\rightarrow$, #, $\rightarrow$)	(check, b , $\rightarrow$)	(nok, $\mathbb{B}$, $\circ$)	(nok, #, $\circ$)
cont $\rightarrow$	(cont $\rightarrow$, a , $\rightarrow$)	(cont $\rightarrow$, b , $\rightarrow$)	(start $\leftarrow$, $\mathbb{B}$, $\leftarrow$)	(start $\leftarrow$, #, $\leftarrow$)
start $\leftarrow$	(cont $\leftarrow$, #, $\leftarrow$)	(nok, b , $\circ$)	(nok, $\mathbb{B}$, $\circ$)	(nok, #, $\circ$)
cont $\leftarrow$	(cont $\leftarrow$, a , $\leftarrow$)	(cont $\leftarrow$, b , $\leftarrow$)	(nok, $\mathbb{B}$, $\circ$)	(start $\rightarrow$, #, $\rightarrow$)
check	(nok, a , $\circ$)	(nok, b , $\circ$)	(nok, $\mathbb{B}$, $\circ$)	(ok, #, $\circ$)

Problemy rozstrzygalne

Język (problem) $L \subseteq A^*$ nazywamy

rozstrzygalnym, albo *rekurencyjnym*,

jeśli $L = L(\mathcal{M})$ dla pewnej całkowitej deterministycznej maszyny Turinga $\mathcal{M}$.

Pytanie

Czy języki bezkontekstowe są rozstrzygalne? A ich dopełnienia?

Fakt

Jeśli $L \subseteq A^$ jest rozstrzygalny to $\bar{L} = A^* - L$ też.*

Pytanie

Język uniwersalny

$$L_u = \{ (\mathcal{M}, w) : w \in L(\mathcal{M}) \}$$

jest częściowo rozstrzygalny. Czy jest rozstrzygalny?

Język uniwersalny jest nierozstrzygalny

Twierdzenie

L_u jest nierozstrzygalny.

Dowód:

Przypuśćmy, że $L_u = L(\mathcal{M}_u)$, dla całkowitej deterministycznej maszyny $\mathcal{M}_u$.
Skonstruujemy (całkowitą deterministyczną) maszynę $\mathcal{M}_p$ dla języka $L_p \dots$

rysunek

Przykładowe problemy nierozstrzygalne:

Pustość języka maszyny Turinga

Dane: maszyna Turinga $\mathcal{M}$

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

Uniwersalność języka bezkontekstowego

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

Wynik: czy $L = A^*$?

Fakt

Jeśli L i $\bar{L}$ są częściowo rozstrzygalne, to są rozstrzygalne.

Dowód:

Z dwóch (nie)deterministycznych maszyn M i $\bar{M}$ dla języków L i $\bar{L}$ skonstruujemy całkowitą deterministyczną maszynę dla $L \dots$

rysunek

Wniosek

Dla każdego języka L zachodzi dokładnie jeden z warunków:

- *L jest rozstrzygalny (i $\bar{L}$ też)*
- *L jest częściowo rozstrzygalny, $\bar{L}$ nie jest częściowo rozstrzygalny*
- *$\bar{L}$ jest częściowo rozstrzygalny, L nie jest częściowo rozstrzygalny*
- *L i $\bar{L}$ nie są częściowo rozstrzygalne*

- 1 Problemy częściowo rozstrzygalne
- 2 Problemy rozstrzygalne
- 3 Funkcje (częściowo) obliczalne
- 4 Jak dowodzić nierozstrzygalności?

Relację $R \subseteq (A^*)^n$ możemy utożsamić z językiem

$$L_R = \{ w_1 \$ w_2 \$ \dots \$ w_n : (w_1, w_2, \dots, w_n) \in R \}$$

Definicja 1: Funkcję częściową $f : (A^*)^n \rightarrow A^*$ nazywamy

częściowo obliczalną, albo *częściowo rekurencyjną*,

jeśli język

$$L_f = \{ w_1 \$ w_2 \$ \dots \$ w_n \$ f(w_1, w_2, \dots, w_n) : (w_1, w_2, \dots, w_n) \in \text{dom}(f) \}$$

jest częściowo rozstrzygalny.

Całkowitą, częściowo obliczalną funkcję $f : (A^*)^n \rightarrow A^*$ nazywamy

obliczalną, albo *rekurencyjną*.

Pytanie

No dobrze, ale jak *obliczyć* wartość funkcji?

Deterministyczna maszyna Turinga $\mathcal{M} = (A, Q, q_0, q_{\text{wynik}}, T, \mathbb{B}, \delta)$

- $q_{\text{wynik}} \in Q$ – stan końcowy
- $\delta : (Q - \{q_{\text{wynik}}\}) \times T \rightarrow Q \times T \times \{\leftarrow, \circlearrowleft, \rightarrow\}$

Funkcja częściowa

$$F(\mathcal{M}) : (A^*)^n \rightarrow A^*$$

obliczana przez maszynę $\mathcal{M}$:

$$F(\mathcal{M})(w_1, \dots, w_n) = v \iff q_0 w_1 \$ w_2 \$ \dots \$ w_n \xrightarrow{*}_{\mathcal{M}} q_{\text{wynik}} v$$

Definicja 2: Funkcję częściową $f : (A^*)^n \rightarrow A^*$ nazywamy

częściowo obliczalną, albo *częściowo rekurencyjną*,

jeśli $f = F(\mathcal{M})$ dla jakiejś maszyny $\mathcal{M}$.

Funkcja częściowa $f : (A^*)^n \rightarrow A^*$.

Definicja 1: Język

$$L_f = \{ w_1 w_2 \dots w_n f(w_1, w_2, \dots, w_n) : (w_1, w_2, \dots, w_n) \in \text{dom}(f) \}$$

jest częściowo rozstrzygalny.

Definicja 2: $f = F(\mathcal{M})$ dla jakiejś maszyny $\mathcal{M}$.

Pytanie

Czy te dwie definicje są równoważne?

	(nie)deterministyczne maszyny Turinga	całkowite deterministyczne maszyny Turinga
języki (problemy)	częściowo rozstrzygalne rekurencyjnie przeliczalne	rozstrzygalne
funkcje	częściowo obliczalne częściowo rekurencyjne	obliczalne rekurencyjne

- 1 Problemy częściowo rozstrzygalne
- 2 Problemy rozstrzygalne
- 3 Funkcje (częściowo) obliczalne
- 4 Jak dowodzić nierozstrzygalności?

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

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

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

Problem stopu

Dane: maszyna Turinga $\mathcal{M}$ nad alfabetem $\{0, 1\}$ i słowo $w \in \{0, 1\}^*$

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:

$\mathcal{M}, w \mapsto \mathcal{M}'$

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

Pustość języka maszyny Turinga

Dane: maszyna Turinga $\mathcal{M}$

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

$\leq$

Uniwersalność języka bezkont.

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

Wynik: czy $L = A^*$?

funkcja obliczalna:

$\mathcal{M} \mapsto \mathcal{G}$

poprawność:

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

Bieg maszyny $\mathcal{M}$:
 $\rho = c_0 \rightarrow_{\mathcal{M}} c_1 \rightarrow_{\mathcal{M}} \dots \rightarrow_{\mathcal{M}} c_n$
 $w_\rho = \$c_0\$c_1\$ \dots \$c_n\$$

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

Fakt

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

Problem odpowiedniości Posta (PCP)

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

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

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

Przykład

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

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	b	bbb
2	babbb	ba
3	ba	a

1	ba	bab
2	abb	bb
3	bab	abb

Twierdzenie

Problem odpowiedniości Posta jest nierozstrzygalny.

Dowód nierozstrzygalności PCP

Ograniczony problem odpowiedniości Posta (ograniczony PCP)

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

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

Lemat

Ograniczony PCP $\leq$ PCP.

Dowód:

1	b	bbb		0	*b*	*b*b*b
2	babbb	ba	$\mapsto$	1	b*	*b*b*b
3	ba	a		2	b*a*b*b*b*	*b*a
				3	b*a*	*a
				4	\$	*\$

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

Lemat

Problem stopu $\leq$ ograniczony PCP.

Dowód:

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

$\mathcal{M}, w$

$\mapsto$

	\$	$\$q_0 w \$$
	0	0
	1	1
	$\mathbb{B}$	$\mathbb{B}$
	\$	\$
	$q a$	$q' a'$
	$q a$	$a' q'$
	$b q a$	$q' b a'$
	$q \$$	$a' q' \$$
	$\$ q a$	$\$ q' \mathbb{B} a'$
	...	...
	$q_{\text{tak}} a$	q_{tak}
	$a q_{\text{tak}}$	q_{tak}
	$q_{\text{tak}} \$\$$	$\$$

jeśli $(q, a, q', a', \circ) \in \delta$

jeśli $(q, a, q', a', \rightarrow) \in \delta$

jeśli $(q, a, q', a', \leftarrow) \in \delta$

jeśli $(q, \mathbb{B}, q', a', \rightarrow) \in \delta$

jeśli $(q, a, q', a', \leftarrow) \in \delta$

Twierdzenie

Każdy problem częściowo rozstrzygalny redukuje się do problemu stopu.

Dowód:

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

funkcja obliczalna:	w	$\mapsto$	$\mathcal{M}, w$
poprawność:	$w \in L$	$\iff$	$w \in L(\mathcal{M})$

W następnym odcinku:

Gramatyki równoważne maszynom Turinga