# Języki, automaty i obliczenia

## Wykład 11: Obliczalność i nieobliczalność

Sławomir Lasota

Uniwersytet Warszawski

6 maja 2015

# Plan

# Maszyny Turinga

Maszyny Turinga:

$$\longleftarrow \qquad q \qquad \longrightarrow$$
$$\nabla$$

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ... | $\mathbb{B}$ | $\mathbb{B}$ | $\mathbb{B}$ | a | b | a | a | b | a | b | $\mathbb{B}$ | $\mathbb{B}$ | ... |

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

$$\text{maszyna } \mathcal{M} \qquad \longmapsto \qquad \text{kod}_{\mathcal{M}} \in \{0,1\}$$

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

$$00\#000000\#001000\#000011\#000\#\#000100\#001\#010000\#100\#001\#\# \ldots$$

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

$$00\ 1\ 000000\ 1\ 001000\ \ 000011\ \ 000\ \ \ 000100\ \ 001\ \ 010000\ \ 100\ \ 001\ \ldots$$

**Twierdzenie**

*Język uniwersalny (problem stopu)*

$$\begin{aligned} L_u &= \{\ \ (\mathcal{M}, w) \quad : \ w \in L(\mathcal{M})\} \\ L_u &= \{kod_{\mathcal{M}}\,\$\,w \ : \ w \in L(\mathcal{M})\} \ \subseteq \ \{0,1,\$\}^* \end{aligned}$$

*jest rekurencyjnie przeliczalny.*

**Pytanie**

Czy każdy język jest rekurencyjnie przeliczalny?

# Problem nie rekurencyjnie przeliczalny

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

$$\text{kod}_{\mathcal{M}} \in \{0,1\}^* \quad \longleftarrow \quad \text{maszyna } \mathcal{M}$$

$$w \in \{0,1\}^* \quad \longmapsto \quad \text{maszyna } \mathcal{M}(w) = \begin{cases} \mathcal{M}, & \text{jeśli kod}_{\mathcal{M}} = w \\ \mathcal{M}_{\emptyset}, & \text{w p.p.} \end{cases}$$

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

Język „przekątniowy”:

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

**Twierdzenie**

*Język $L_p$ nie jest rekurencyjnie przeliczalny.*

*Dowód:*

**paradoks golibrody**

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

$$\mathrm{kod}_{\mathcal{M}} \in \{0,1\}^* \qquad \longleftarrow \qquad \text{maszyna } \mathcal{M}$$

$$w \in \{0,1\}^* \qquad \longmapsto \qquad \text{maszyna } \mathcal{M}(w) = \begin{cases} \mathcal{M}, & \text{jeśli } \mathrm{kod}_{\mathcal{M}} = w \\ \mathcal{M}_\emptyset, & \text{w p.p.} \end{cases}$$

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

Język „przekątniowy”:

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

**Twierdzenie**

*Język $L_p$ nie jest rekurencyjnie przeliczalny.*

*Dowód:*

**paradoks golibrody**

Przypuśćmy, że $L(\mathcal{M}_p) = L_p$. Niech $w_p = \mathrm{kod}_{\mathcal{M}_p}$. Wtedy

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

# Plan

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

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

**Twierdzenie**

*Dla każdej maszyny Turinga istnieje równoważna maszyna deterministyczna.*

*Dowód:*

?

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

- $q_{\mathsf{tak}} \in Q$ – stan akceptujący
- $q_{\mathsf{nie}} \in Q$ – stan odrzucający
- $\delta : (Q - \{q_{\mathsf{tak}}, q_{\mathsf{nie}}\}) \times T \to Q \times T \times \{\leftarrow, \circlearrowright, \to\}$

Konfiguracje *końcowe*:

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

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

$$q_0\, w \longrightarrow^*_{\mathcal{M}} c$$

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

# Przykład (maszyna całkowita i deterministyczna)

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

| | $a$ | $b$ | $\mathbb{B}$ | $\#$ |
|---|---|---|---|---|
| $\text{start}_{\rightarrow}$ | $(\text{cont}_{\rightarrow}, \#, \rightarrow)$ | $(\text{check}, b, \rightarrow)$ | $(\text{nok}, \mathbb{B}, \circlearrowleft)$ | $(\text{nok}, \#, \circlearrowleft)$ |
| $\text{cont}_{\rightarrow}$ | $(\text{cont}_{\rightarrow}, a, \rightarrow)$ | $(\text{cont}_{\rightarrow}, b, \rightarrow)$ | $(\text{start}_{\leftarrow}, \mathbb{B}, \leftarrow)$ | $(\text{start}_{\leftarrow}, \#, \leftarrow)$ |
| $\text{start}_{\leftarrow}$ | $(\text{cont}_{\leftarrow}, \#, \leftarrow)$ | $(\text{nok}, b, \circlearrowleft)$ | $(\text{nok}, \mathbb{B}, \circlearrowleft)$ | $(\text{nok}, \#, \circlearrowleft)$ |
| $\text{cont}_{\leftarrow}$ | $(\text{cont}_{\leftarrow}, a, \leftarrow)$ | $(\text{cont}_{\leftarrow}, b, \leftarrow)$ | $(\text{nok}, \mathbb{B}, \circlearrowleft)$ | $(\text{start}_{\rightarrow}, \#, \rightarrow)$ |
| check | $(\text{nok}, a, \circlearrowleft)$ | $(\text{nok}, b, \circlearrowleft)$ | $(\text{nok}, \mathbb{B}, \circlearrowleft)$ | $(\text{ok}, \#, \circlearrowleft)$ |

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?

# 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**

Problem stopu

$$L_u = \{\mathrm{kod}_{\mathcal{M}} \$ w \ : \ w \in L(\mathcal{M})\}$$

jest częściowo rozstrzygalny. Czy jest rozstrzygalny?

**Twierdzenie**

*Problem stopu $L_u$ jest nierozstrzygalny.*

*Dowód:*

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

**rysunek**

Przykładowe problemy nierozstrzygalne:

**Pustość języka maszyny Turinga**

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

**Uniwersalność języka bezkontektowego**

| | |
|---|---|
| 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 niedeterministycznych maszyn $M$ i $\bar{M}$ dla języków $L$ i $\bar{L}$ skonstruujemy całkowitą deterministyczną maszynę dla $L$...

**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*

# Plan

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

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

Funkcję częściową $f : (A^*)^n \to A^*$ nazywamy

*częściowo obliczalną*, albo *częściowo rekurencyjną*,

jeśli

$$L_f \;=\; \{w_1\$w_2\$\ldots\$w_n\$f(w_1, w_2, \ldots, w_n) \;:\; (w_1, w_2, \ldots, w_n) \in \mathrm{dom}(f)\}$$

jest językiem częściowo rozstrzygalnym.

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

*obliczalną*, albo *rekurencyjną*.

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

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

Funkcja częściowa

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

obliczana przez maszynę $\mathcal{M}$:

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

Funkcję częściową $f : (A^*)^n \to A^*$ nazywamy

*częściowo obliczalną*, albo *częściowo rekurencyjną*,

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

**Pytanie**

Czy te dwie definicje są równoważne?

# Podsumowanie

| | niedeterministyczne maszyny Turinga | całkowite deterministyczne maszyny Turinga |
|---|---|---|
| języki (problemy) | częściowo rozstrzygalne<br>rekurencyjnie przeliczalne | rozstrzygalne<br>rekurencyjne |
| funkcje | częściowo obliczalne<br>częściowo rekurencyjne | obliczalne<br>rekurencyjne |

# Plan

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

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

taka, że

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

rysunek

Ozn. $L \leq K$, gdy $L$ redukuje się do $K$.

**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: | $\mathcal{M}, w$ | $\longmapsto$ | $\mathcal{M}'$ |
| 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

**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: $\mathcal{M} \longmapsto \mathcal{G}$

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

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

$$\mathrm{kod}_\rho = \$c_0\$c_1\$ \dots \$c_n\$$$

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

**Fakt**

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

### 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*.

### 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

**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 $(q, a, q', a', \circlearrowleft) \in \delta$ |
| | $q\ a$ | $a'\ q'$ | 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 $(q, a, q', a', \leftarrow) \in \delta$ |
| | $\ldots$ | $\ldots$ | |
| | $q_{\mathrm{tak}}\ a$ | $q_{\mathrm{tak}}$ | |
| | $a\ q_{\mathrm{tak}}$ | $q_{\mathrm{tak}}$ | |
| | $q_{\mathrm{tak}}\ \$\$$ | $\$$ | |

**Twierdzenie**

*Każdy problem częściowo rozstrzygalny redukuje się do problemu stopu.*

*Dowód:*

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

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

## W następnym odcinku:

Gramatyki równoważne maszynom Turinga