Logika i automaty

Filip Murlak
Instytut Informatyki, MIM UW

Będlewo 2015

Entscheidungsproblem

Problem (Hilbert 1928)

Podać algorytm, który dla zadanej formuły $\varphi \in \mathrm{FO}$ *odpowiada na pytanie, czy* φ *jest tautologią.*

Entscheidungsproblem

Problem (Hilbert 1928)

Podać algorytm, który dla zadanej formuły $\varphi \in \mathrm{FO}$ odpowiada na pytanie, czy φ jest tautologią.

Twierdzenie (o pełności; Gödel 1929)

Istnieje pełny i poprawny system dowodowy dla FO; można efektywnie wygenerować wszystkie tautologie FO.
(Zbiór tautologii FO jest częściowo rozstrzygalny.)

Entscheidungsproblem

Problem (Hilbert 1928)

Podać algorytm, który dla zadanej formuły $\varphi \in \mathrm{FO}$ odpowiada na pytanie, czy φ jest tautologią.

Twierdzenie (o pełności; Gödel 1929)

Istnieje pełny i poprawny system dowodowy dla FO; można efektywnie wygenerować wszystkie tautologie FO.
(Zbiór tautologii FO jest częściowo rozstrzygalny.)

Twierdzenie (Church 1936; Turing 1937)

Nie istnieje algorytm, o który pytał Hilbert.
(Zbiór tautologii FO jest nierozstrzygalny.)

Pierwsza droga: ograniczyć logikę

Twierdzenie

- *Dla sygnatur relacyjnych unarnych (monadyczny rach. predykatów), zbiór tautologii* FO *jest rozstrzygalny. (Löwenheim 1915; Behmann 1922)*
- *Jeśli dopuścimy choć jedną relację większej arności, zbiór tautologii* FO *jest nierozstrzygalny.*

Twierdzenie

Problem spełnialności jest rozstrzygalny dla formuł FO *postaci:*

- $\exists^*\forall^*$ *(Bernays, Schönfinkel 1928);*
- $\exists^*\forall\exists^*$ *(Ackermann 1928);*
- $\exists^*\forall\forall\exists^*$ *(Gödel 1932).*

Dla wszystkich innych prefiksów spełnialność jest nierozstrzygalna.

Druga droga: ograniczyć rozważane struktury

Twierdzenie

- *Teoria* FO $\langle \mathbb{N}, +, \cdot \rangle$ *jest nierozstrzygalna (Gödel 1931).*
- *Teoria* FO $\langle \mathbb{N}, + \rangle$ *jest rozstrzygalna (Presburger 1929).*
- *Teoria* FO $\langle \mathbb{R}, +, \cdot \rangle$ *jest rozstrzygalna (Tarski 1948).*

Czy można pójść dalej? Co z logiką drugiego rzędu?

Jeśli dopuścić kwantyfikowanie po relacjach binarnych, to problem jest nierozstrzygalny (mamy dowolnie interpretowane relacje).

Pozostaje logika monadyczna drugiego rzędu (MSO).

Rozstrzygalność teorii MSO

Twierdzenie

- *Teoria* MSO $\langle \mathbb{N}, + \rangle$ *jest nierozstrzygalna.*
  (Można zakodować kratownicę $n \times k$*, używając* $+1$ *oraz* $+k$ *do poruszania się w kierunkach lewo/prawo i góra/dół.)*
- *Teoria* MSO $\langle \mathbb{R}, + \rangle$ *jest nierozstrzygalna.*
  (Można prawie zdefiniować liczby naturalne.)

Jaki jest kolejny kandydat?

Rozstrzygalność teorii MSO

Twierdzenie

- *Teoria* MSO $\langle \mathbb{N}, + \rangle$ *jest nierozstrzygalna.*
  (Można zakodować kratownicę $n \times k$*, używając* $+1$ *oraz* $+k$ *do poruszania się w kierunkach lewo/prawo i góra/dół.)*
- *Teoria* MSO $\langle \mathbb{R}, + \rangle$ *jest nierozstrzygalna.*
  (Można prawie zdefiniować liczby naturalne.)

Jaki jest kolejny kandydat?

Twierdzenie (Büchi 1962)

Teoria MSO $\langle \mathbb{N}, \mathit{succ} \rangle$ *jest rozstrzygalna.*

Zastosowanie

Wniosek

Teoria FO $\langle \mathbb{N}, + \rangle$ *jest rozstrzygalna.*

Zastosowanie

Wniosek

Teoria $\mathrm{FO}\ \langle \mathbb{N}, + \rangle$ *jest rozstrzygalna.*

Dowód. W $\langle \mathbb{N}, \mathit{succ} \rangle$ interpretujemy $\langle \mathbb{N}, + \rangle$, liczba to zbiór:

$$
\begin{aligned}
x < y &\equiv \exists X\ x \in X \wedge \forall z\ \big(s(z) \in X \implies z \in X\big) \wedge y \notin X \\
\mathit{nat}(X) &\equiv \exists z\ \forall x\ \big(x \in X \implies x \leq z\big) \\
\mathit{zero}(X) &\equiv \forall z\ z \notin X \\
X + Y = Z &\equiv \mathit{nat}(X) \wedge \mathit{nat}(Y) \wedge \mathit{nat}(Z) \wedge \\
&\quad 0 \in Z \iff (0 \in X \vee 0 \notin Y) \vee (0 \notin X \wedge 0 \in Y) \wedge \\
&\quad \forall x\ \big(x \notin X \wedge x \notin Y \wedge s(x) \notin X \wedge s(x) \notin Y \implies s(x) \notin Z\big) \wedge \\
&\quad \forall x\ \big(x \notin X \wedge x \notin Y \wedge s(x) \notin X \wedge s(x) \in Y \implies s(x) \in Z\big) \wedge \\
&\quad \ldots \\
&\quad \forall x\ \big(x \in X \wedge x \in Y \wedge s(x) \in X \wedge s(x) \in Y \implies s(x) \in Z\big) \\
\exists x\ \psi(x) &\rightsquigarrow \exists X\ \mathit{nat}(X) \wedge \widehat{\psi}(X)
\end{aligned}
$$

$$
\langle \mathbb{N}, + \rangle \models \varphi \iff \langle \mathbb{N}, \mathit{succ} \rangle \models \widehat{\varphi}
$$

□

Twierdzenie Büchiego i automaty

Twierdzenie (Büchi 1962)

Dla każdego $\varphi(X_1, \ldots, X_n) \in \mathrm{MSO}$ *można skonstruować automat* $\mathcal{A}$ *wczytujący słowa nieskończone nad alfabetem* $\{0,1\}^n$, *taki że*

$$\langle \mathbb{N}, \mathit{succ}, U_1, \ldots, U_n \rangle \models \varphi(X_1, \ldots, X_n) \iff \mathcal{A} \text{ akceptuje } \chi_{U_1,\ldots,U_n}.$$

Fakt

Można rozstrzygnąć, czy dany automat $\mathcal{A}$ *akceptuje jakieś słowo.*

Twierdzenie Büchiego i automaty

Twierdzenie (Büchi 1962)

Dla każdego $\varphi(X_1, \ldots, X_n) \in \mathrm{MSO}$ *można skonstruować automat* $\mathcal{A}$ *wczytujący słowa nieskończone nad alfabetem* $\{0,1\}^n$*, taki że*

$$\langle \mathbb{N}, \mathit{succ}, U_1, \ldots, U_n \rangle \models \varphi(X_1, \ldots, X_n) \iff \mathcal{A} \text{ akceptuje } \chi_{U_1,\ldots,U_n}.$$

Fakt

Można rozstrzygnąć, czy dany automat $\mathcal{A}$ *akceptuje jakieś słowo.*

Büchi pokazał postać normalną dla $\varphi(X_1, X_2, \ldots, X_n) \in \mathrm{MSO}$:

$\exists Q_0 \exists Q_1 \ldots \exists Q_m$

- $\forall x \bigoplus_i x \in Q_i$ (czyli $\bar{Q}$ jest podziałem uniwersum) $\wedge$
- $0 \in Q_0$ $\wedge$
- $\bigwedge_i \forall x \left(s(x) \in Q_i \implies \psi_i(\bar{X}, \bar{Q}, x) \right)$ $\wedge$
- $\forall x \exists y \;\; y > x \wedge y \in \bigcup_{i \in F} Q_i$ (czyli $\bigcup_{i \in F} Q_i$ jest nieskończony)

dla pewnego $F \subseteq \{0, 1, \ldots, m\}$.

Definicja automatu

Definicja

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$*, gdzie*

- Σ *to skończony alfabet (u nas* $\{0,1\}^n$*),*
- Q *to skończony zbiór stanów,*
- $q_0 \in Q$ *to stan początkowy,*
- $\delta \subseteq Q \times \Sigma \times Q$ *to relacja przejścia,*
- $F \subseteq Q$ *to zbiór stanów akceptujących.*

Bieg na słowie $w \in \Sigma^\omega$ *to takie słowo* $\rho \in Q^\omega$*, że*

$$\rho(0) = q_0 \quad \textit{oraz} \quad \big\langle \rho(i), w(i), \rho(i+1) \big\rangle \in \delta\,.$$

Bieg ρ *jest akceptujący jeśli* $\exists^\infty i\ \rho(i) \in F$*.*

Definicja automatu

Definicja

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$*, gdzie*

- Σ *to skończony alfabet (u nas* $\{0,1\}^n$*),*
- Q *to skończony zbiór stanów,*
- $q_0 \in Q$ *to stan początkowy,*
- $\delta \subseteq Q \times \Sigma \times Q$ *to relacja przejścia,*
- $F \subseteq Q$ *to zbiór stanów akceptujących.*

Bieg na słowie $w \in \Sigma^\omega$ *to takie słowo* $\rho \in Q^\omega$*, że*

$$\rho(0) = q_0 \quad \textit{oraz} \quad \big\langle \rho(i), w(i), \rho(i+1) \big\rangle \in \delta\,.$$

Bieg ρ *jest akceptujący jeśli* $\exists^\infty i\ \rho(i) \in F$*.*

Przykład. „Bloki pozycji w X są parzystej długości” i „X jest (nie)skończony”.

Definicja automatu

Definicja

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$*, gdzie*

- Σ *to skończony alfabet (u nas* $\{0,1\}^n$*),*
- Q *to skończony zbiór stanów,*
- $q_0 \in Q$ *to stan początkowy,*
- $\delta \subseteq Q \times \Sigma \times Q$ *to relacja przejścia,*
- $F \subseteq Q$ *to zbiór stanów akceptujących.*

Bieg na słowie $w \in \Sigma^\omega$ *to takie słowo* $\rho \in Q^\omega$*, że*

$$\rho(0) = q_0 \quad \textit{oraz} \quad \big\langle \rho(i), w(i), \rho(i+1) \big\rangle \in \delta\,.$$

Bieg ρ *jest akceptujący jeśli* $\exists^\infty i\ \rho(i) \in F$*.*

Przykład. „Bloki pozycji w X są parzystej długości" i „X jest (nie)skończony".

Uwaga. Aby sprawdzić, czy $\mathcal{A}$ akceptuje jakiekolwiek słowo, wystarczy znaleźć stan q osiągalny z q_0 i taki, że z q da się wrócic do q przechodząc przez stan z F.

Uproszczone MSO

MSO używa $\exists X$, $\exists x$, $\vee$, $\neg$, $s(x)$, $x \in Y$, $=$, ale wystarczą

$$\exists X, \quad \vee, \quad \neg, \quad s(X), \quad X \subseteq Y,$$

gdzie $Y = s(X)$ znaczy $\exists x\, X = \{x\} \wedge Y = \{s(x)\}$.

Uproszczone MSO

MSO używa $\exists X$, $\exists x$, $\vee$, $\neg$, $s(x)$, $x \in Y$, $=$, ale wystarczą

$$\exists X, \quad \vee, \quad \neg, \quad s(X), \quad X \subseteq Y,$$

gdzie $Y = s(X)$ znaczy $\exists x\, X = \{x\} \wedge Y = \{s(x)\}$.

$$\begin{aligned} \mathit{singleton}(X) &\equiv \forall Y \left(Y \subseteq X \implies X \subseteq Y \vee \forall Z\ Y \subseteq Z \right) \\ \exists x \ldots &\rightsquigarrow \exists X_x\ \mathit{singleton}(X_x) \wedge \ldots \\ x \in Y &\rightsquigarrow X_x \subseteq Y \end{aligned}$$

Konstrukcja automatu dla formuły $\varphi(X_1, X_2, \ldots, X_n)$

Każdy kwantyfikator wprowadza inną zmienna X_j dla $n < j \leq m$.

- $X_i = s(X_j)$ i $X_i \subseteq X_j$ łatwo;
- $\vee$ odpowiada sumie języków;
- $\exists X_i$ odpowiada rzutowaniu języka na współrzędne różne od i: wystarczy zrzutować relację $\delta \subseteq Q \times \{0,1\}^n \times Q$ pomijając i-tą współrzędną litery;
- $\neg$ to główna trudność; wykorzystamy twierdzenia Ramseya i proste koncepcje algebraiczne.

Cel

Aby udowodnić twierdzenie Büchiego pozostaje wykazać następujący lemat:

Lemat

Dla danego automatu $\mathcal{A}$ nad alfabetem Σ można skonstruować automat $\mathcal{B}$ rozpoznający język $\Sigma^\omega - L(\mathcal{A})$.

Inaczej: $\mathcal{B}$ ma akceptować słowa, w których każdy bieg automatu $\mathcal{A}$ przechodzi skończenie wiele razy przez stany akceptujące.

Przypomnienie definicji automatu

Definicja

Automat $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$ *nad alfabetem* Σ *ma*

- *skończony zbiór stanów* Q,
- *stan początkowy* $q_0 \in Q$,
- *relację przejścia* $\delta \subseteq Q \times \Sigma \times Q$,
- *zbiór stanów akceptujących* $F \subseteq Q$.

Bieg na słowie $w \in \Sigma^\omega$ *to takie słowo* $\rho \in Q^\omega$, *że*

$$\rho(0) = q_0 \quad \textit{oraz} \quad \big\langle \rho(i), w(i), \rho(i+1) \big\rangle \in \delta \,.$$

Bieg ρ *jest akceptujący jeśli* $\exists^\infty i \ \rho(i) \in F$.

Próba konstrukcji dopełnienia (naiwna)

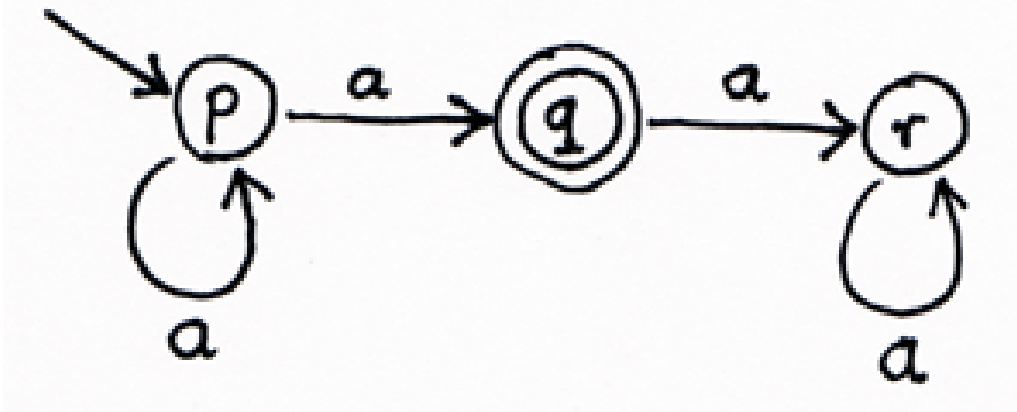
- Stany $\mathcal{B}$ to podzbiory stanów $\mathcal{A}$.
- Stan $\mathcal{B}$ po przeczytaniu słowa $a_1 a_2 \ldots a_n$ to zbiór stanów, jakie $\mathcal{A}$ może mieć po przeczytaniu $a_1 a_2 \ldots a_n$.
- Stan początkowy $\mathcal{B}$ to zbiór stanów początkowych $\mathcal{A}$.
- $\mathcal{B}$ akceptuje, jeśli od pewnego momentu już nie ma stanów akceptujących $\mathcal{A}$.

To nie jest warunek Büchiego, ale łatwo ten automat przerobić na automat Büchiego: trzeba niedeterministycznie wybierać moment, od którego nie ma stanów akceptujących.

Dlaczego konstrukcja ta nie działa?

$w \in L(\mathcal{B}) \implies w \notin L(\mathcal{A})$, ale nie odwrotnie.

Kontrprzykład



- $L(\mathcal{A}) = \emptyset$ (każdy bieg co najwyżej raz odwiedza stan akceptujący)
- Jedyny bieg $\mathcal{B}$ na słowie $aaa\ldots$ (jedynym nad alfabetem $\{a\}$):

$$\{p\}, \quad \{p,q\}, \quad \{p,q,r\}, \quad \{p,q,r\}, \quad \{p,q,r\}, \quad \ldots$$

- Czyli $\mathcal{B}$ nie akceptuje słowa $aaa\ldots$ (a powinien).
- Kłopot: $\mathcal{A}$ ma dowolnie długie biegi dochodzące do stanu akceptującego q, ale nie dają się one połączyć w jeden bieg.
- Potrzebna jest inna, subtelniejsza konstrukcja automatu $\mathcal{B}$. Trzeba więcej pamiętać o wczytanym słowie!

Informacje o biegach na słowach skończonych

Słowu skończonemu $w \in \Sigma^*$ przyporządkowujemy informację o możliwych biegach $\mathcal{A}$, opisaną macierzą M_w:

- M_w jest rozmiaru $|Q| \times |Q|$,
- wiersze i kolumny M_w są indeksowane stanami automatu $\mathcal{A}$,
- elementy M_w należą do zbioru $\{\bot; 1; 0\}$.

Informacje o biegach na słowach skończonych

Słowu skończonemu $w \in \Sigma^*$ przyporządkowujemy informację o możliwych biegach $\mathcal{A}$, opisaną macierzą M_w:

- M_w jest rozmiaru $|Q| \times |Q|$,
- wiersze i kolumny M_w są indeksowane stanami automatu $\mathcal{A}$,
- elementy M_w należą do zbioru $\{\bot; 1; 0\}$.

W komórce (p, q) wartość macierzy M_w to

$\bot$ jeśli nie istnieje bieg $\mathcal{A}$ postaci $p \xrightarrow{w} q$;

1 jeśli istnieje bieg $p \xrightarrow{w} q$ przechodzący przez stan akceptujący;

0 jeśli istnieją biegi $p \xrightarrow{w} q$, ale żaden nie przechodzi przez stan akceptujący.

Aby uzyskać informację dla konkatenacji $w \cdot v$ wystarczy znać informację dla w i v.

Rozważmy półpierścień (przemienny)

$$\mathbb{P} = \langle \{\bot, 1, 0\}, \max, \cdot \rangle$$

- max wg. porządku $\bot < 0 < 1$,
- $\bot \cdot$ cokolwiek $=$ cokolwiek $\cdot \bot = \bot$
  $1 \cdot 1 = 1 \cdot 0 = 0 \cdot 1 = 1$
  $0 \cdot 0 = 0$

Mnożenie macierzy z $\mathbb{M} = \mathrm{M}_{Q \times Q}(\mathbb{P})$ jest zdefiniowane jak zwykle:

$$(M \cdot N)(p, q) = \max_{r \in Q} M(p, r) \cdot N(r, q).$$

Wtedy $\quad M_{w \cdot v} = M_w \cdot M_v$.

Funkcja $w \mapsto M_w$ jest homomorfizmem monoidów $\langle \Sigma^*, \cdot \rangle \to \mathbb{M}$,

$$M_{w \cdot v} = M_w \cdot M_v \,.$$

Sprawdźmy:

- $M_{w \cdot v}(p, q) = \bot$

  $\iff$ dla każdego r jedno z dwóch przejść jest niemożliwe:

  $$p \xrightarrow{w} r \quad \text{lub} \quad r \xrightarrow{v} q$$

  $\iff$ dla każdego r, $M_w(p, r) = \bot$ lub $M_v(r, q) = \bot$

- $M_{w \cdot v}(p, q) = 1$

  $\iff$ istnieje taki r, że są możliwe przejścia

  $$p \xrightarrow{w} r \quad \text{oraz} \quad r \xrightarrow{v} q$$

  i jedno z nich odwiedza stan akceptujący

  $\iff$ istnieje r, że $\big\langle M_w(p, r), M_v(r, q) \big\rangle$ to $\langle 0, 1 \rangle$, $\langle 1, 0 \rangle$, lub $\langle 1, 1 \rangle$.

Lemat (kluczowy)

Niech $w \in \Sigma^\omega$. *Wówczas istnieją*

- *macierze* M, N, *takie że* $M \cdot N = M$ *i* $N \cdot N = N$,
- *podział* $w = w_0 w_1 w_2 w_3 \ldots$, $|w_i| > 0$,

takie że

- $M_{w_0} = M$,
- $M_{w_i} = N$ *dla* $i > 0$.

Zatem

- słowu $w_0 w_1 w_2 \ldots w_i$ odpowiada macierz M (dla $i \geq 0$),
- słowu $w_i w_{i+1} w_{i+2} \ldots w_j$ odpowiada macierz N (dla $j > i > 0$).

Twierdzenie (Ramseya)

Niech $\alpha\colon [\mathbb{N}]^2 \to K$ *będzie kolorowaniem dwuelementowych podzbiorów* $\mathbb{N}$ *kolorami ze skończonego zbioru* K*.*

Wtedy istnieje zbiór nieskończony $X \subseteq \mathbb{N}$ *oraz kolor* $k \in K$*, taki że*

$$\forall_{i,j \in X}\ \alpha(i,j) = k\,.$$

Dowod kluczowego lematu

Niech $w = a_1 a_2 a_3 \ldots$ oraz $\alpha(i,j) = \alpha(j,i) = M_{a_i \ldots a_{j-1}}$ dla $i < j$.

Tw. Ramseya daje pozycje $i_1 < i_2 < i_3 < \ldots$ i macierz N, takie że:

$$\forall_{j,k} \;\; \alpha(i_j, i_k) = N\,.$$

$$\overbrace{\underbrace{a_1 a_2 \cdots a_{i_1-1}}_{N_0}\underbrace{a_{i_1} \cdots a_{i_2-1}}_{N}}^{M=N_0 \cdot N}\underbrace{a_{i_2} \cdots a_{i_3-1}}_{N}\underbrace{a_{i_3} \cdots a_{i_4-1}}_{N}\cdots$$

$$w_0 \qquad\qquad w_1 \qquad\qquad w_2$$

Sprawdzamy warunki na mnożenie macierzy z tezy lematu:

$$N \cdot N = \alpha(i_2, i_3) \cdot \alpha(i_3, i_4) = \alpha(i_2, i_4) = N$$

$$M \cdot N = N_0 \cdot N \cdot N = N_0 \cdot N = M$$

$\square$

Lemat (charakteryzujący)

Dla każdych M, N i $w = w_0 w_1 w_2 \ldots$ jak w kluczowym lemacie,

$$w \in L(\mathcal{A}) \quad \Longleftrightarrow \quad \underbrace{M(q_0, q) \neq \perp,\ N(q, q) = 1 \ \textit{dla pewnego } q}_{\star} \ .$$

Lemat (charakteryzujący)

Dla każdych M, N i $w = w_0 w_1 w_2 \ldots$ jak w kluczowym lemacie,

$$w \in L(\mathcal{A}) \quad \Longleftrightarrow \quad \underbrace{M(q_0, q) \neq \perp,\ N(q, q) = 1 \ \textit{dla pewnego } q}_{\star} .$$

Dowód. ($\Leftarrow$) Składamy bieg akceptujący z kawałków.
($\Rightarrow$) Rozważmy bieg akceptujący $\mathcal{A}$ na w. Niech q_i to stan po przeczytaniu prefiksu $w_0 w_1 \ldots w_i$. Wśród q_i pewien stan q pojawia się nieskończenie wiele razy, powiedzmy dla $i \in I$.
Ponieważ $M_{w_0 w_1 \ldots w_i} = MN^i = M$, mamy $M(q_I, q_i) \neq \perp$ dla $i \geq 1$, czyli również $M(q_I, q) \neq \perp$.
Ponieważ bieg jest akceptujący, nieskończenie wiele razy pojawiają się stany akceptujące. Zatem można wybrać taki nieskończony zbiór $\{j_0, j_1, j_2, \ldots\} \subseteq I$, że dla każdego k stan akceptujący pojawia się podczas czytania podsłowa $w_{j_k+1} \ldots w_{j_{k+1}}$. Czyli macierz słowa $w_{j_k+1} \ldots w_{j_{k+1}}$ ma 1 w komórce (q, q). Ponieważ ta macierz to N, dostajemy $N(q, q) = 1$. □

Wniosek

Dla słowa $w \in \Sigma^\omega$ następujące warunki są równoważne:

1. *w nie jest akceptowane przez $\mathcal{A}$;*
2. *istnieją $M, N \in \mathbb{M}$ oraz $w = w_0 w_1 w_2 \ldots$ jak w kluczowym lemacie takie, że M, N nie spełniają $(\star)$;*
3. *w należy do języka opisanego wyrażeniem*

$$\bigcup_{\substack{M,N \text{ nie spełniają } (\star) \\ M \cdot N = M,\ N \cdot N = N}} L_M (L_N)^\omega$$

gdzie $L_X = \{w \in \Sigma^* \colon M_w = X\}$.

Fakt

Dla danych macierzy $M, N \in \mathbb{M}$, można skonstruować automat rozpoznający język $L_M (L_N)^\omega$.

To kończy dowód tw. Büchiego.

Bardziej skomplikowane struktury

Pokazaliśmy, że teoria MSO struktury $\langle \mathbb{N}, \mathit{succ} \rangle$ jest rozstrzygalna. Czy da się to uogólnić?

Bardziej skomplikowane struktury

Pokazaliśmy, że teoria MSO struktury $\langle \mathbb{N}, \mathit{succ} \rangle$ jest rozstrzygalna. Czy da się to uogólnić?

$\langle \mathbb{N}, \mathit{succ} \rangle$ to struktura wolna z jednym generatorem i jednoargumentowym symbolem fynkcyjnym s.

A co jeśli mamy więcej symboli funkcyjnych?

Bardziej skomplikowane struktury

Pokazaliśmy, że teoria MSO struktury $\langle \mathbb{N}, \mathit{succ} \rangle$ jest rozstrzygalna. Czy da się to uogólnić?

$\langle \mathbb{N}, \mathit{succ} \rangle$ to struktura wolna z jednym generatorem i jednoargumentowym symbolem fynkcyjnym s.

A co jeśli mamy więcej symboli funkcyjnych?

Twierdzenie (Rabin 1969)

Teoria MSO *struktury* $\langle \{0,1\}^*, \cdot 0, \cdot 1 \rangle$ *jest rozstrzygalna.*

Bardziej skomplikowane struktury

Pokazaliśmy, że teoria MSO struktury $\langle \mathbb{N}, \mathit{succ} \rangle$ jest rozstrzygalna. Czy da się to uogólnić?

$\langle \mathbb{N}, \mathit{succ} \rangle$ to struktura wolna z jednym generatorem i jednoargumentowym symbolem fynkcyjnym s.

A co jeśli mamy więcej symboli funkcyjnych?

Twierdzenie (Rabin 1969)

Teoria MSO *struktury* $\langle \{0,1\}^*, \cdot 0, \cdot 1 \rangle$ *jest rozstrzygalna.*

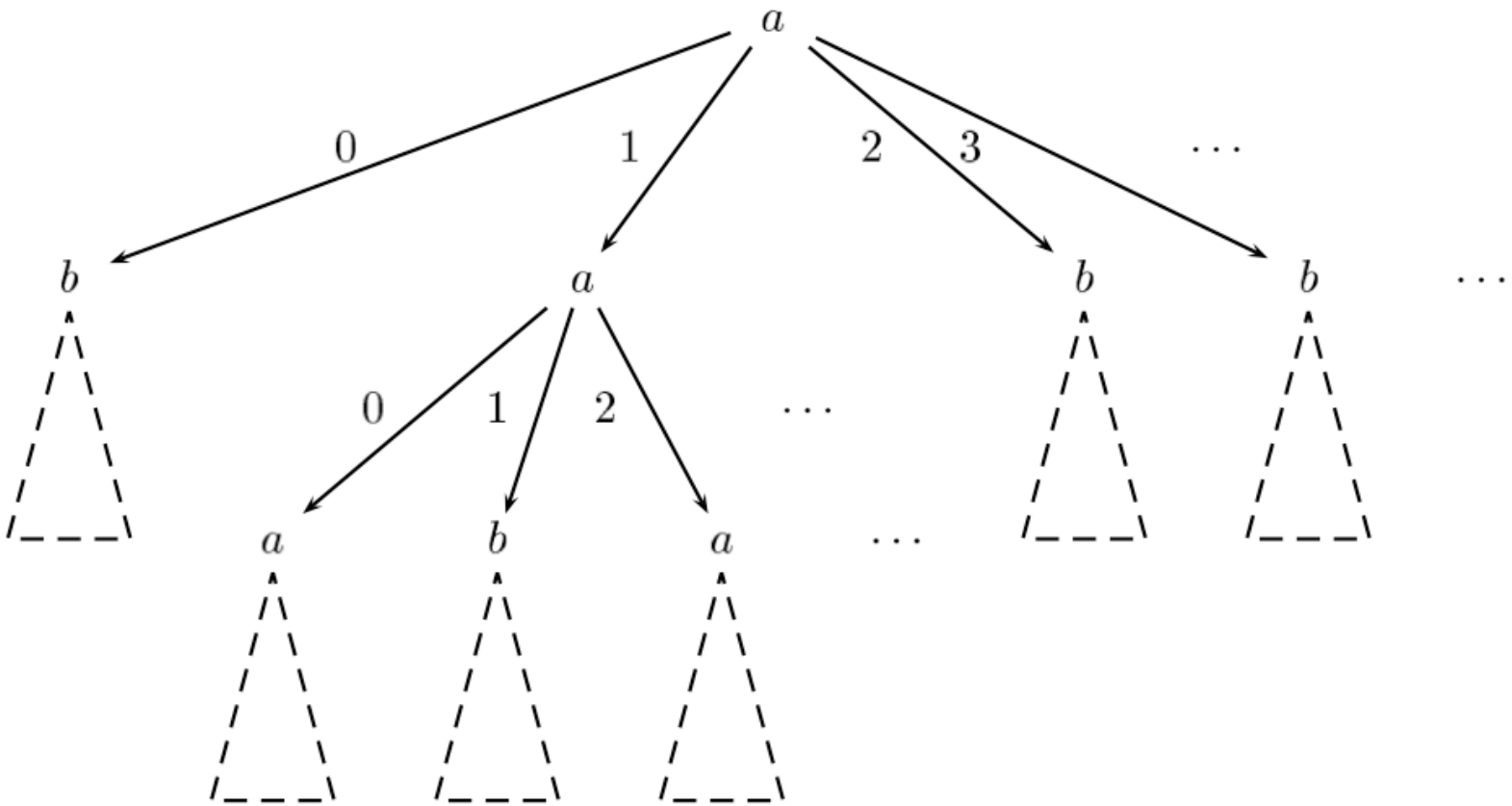
Wniosek

Rozstrzygalne są teorie MSO

- *struktury* $\langle \{0,1,\ldots,i\}^*, \cdot 0, \cdot 1, \ldots, \cdot i \rangle$;
- *struktur* $\langle \mathbb{N}^*, \cdot 0, \cdot 1, \cdot 2, \ldots \rangle$ *i* $\langle \mathbb{N}^*, \prec \rangle$;
- *przeliczalnych gęstych liniowych porządków bez końców;*
- *przeliczalnych liniowych porządków.*

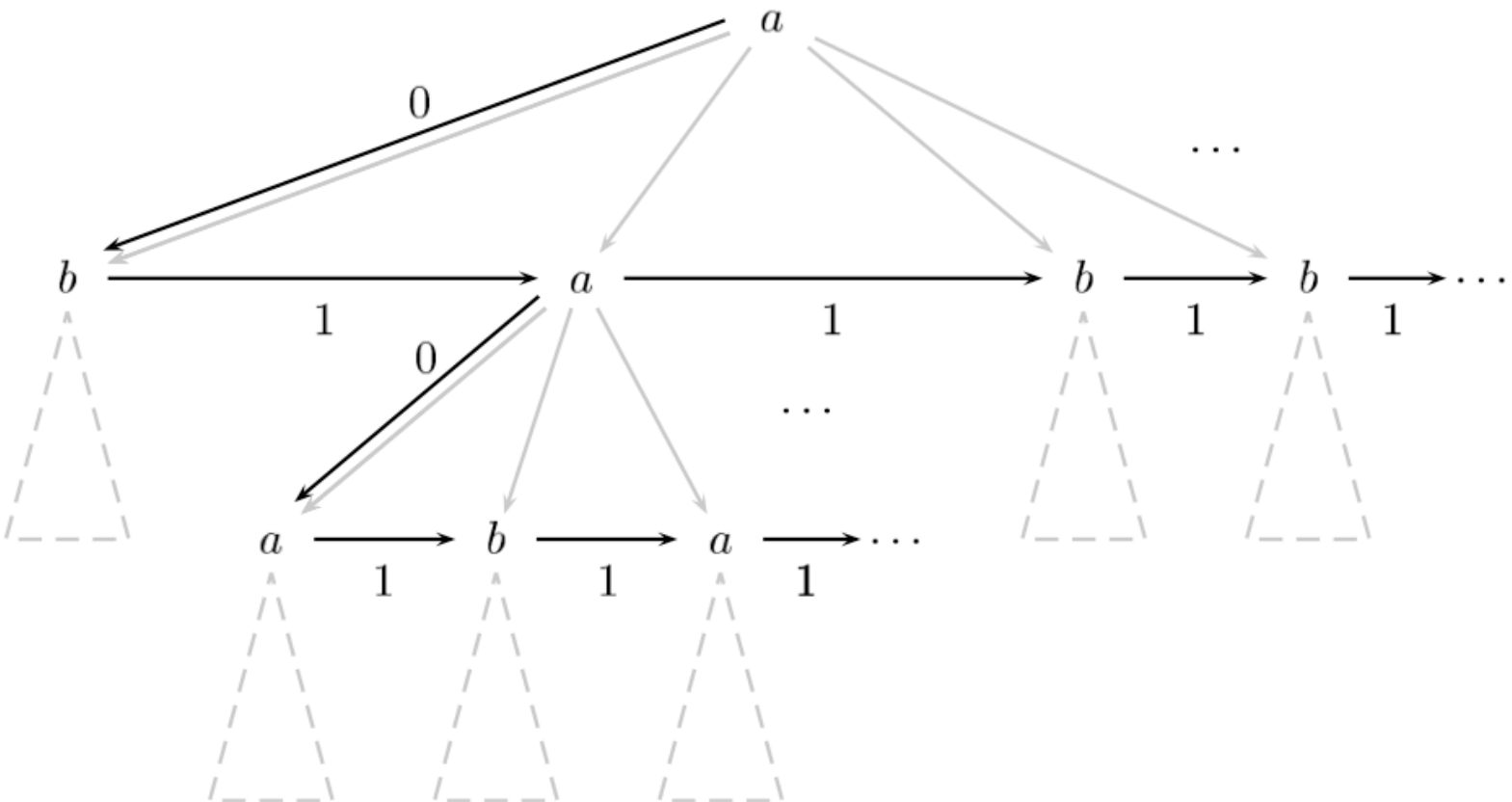
Wniosek

Teoria MSO *struktury* $\langle \mathbb{N}^*, \cdot 0, \cdot 1, \cdot 2, \ldots \rangle$ *jest rozstrzygalna.*



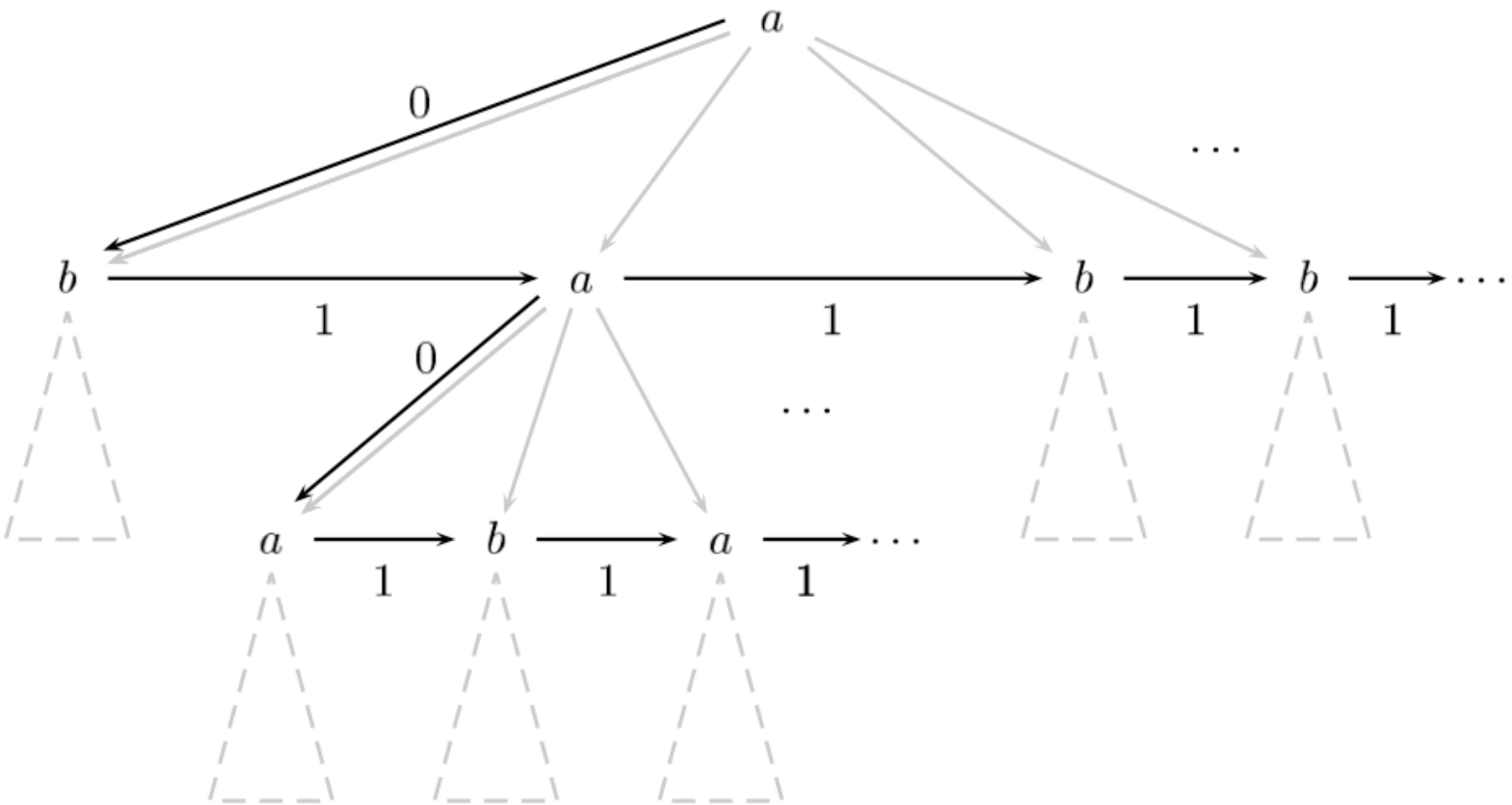
Wniosek

Teoria MSO *struktury* $\langle \mathbb{N}^*, \cdot 0, \cdot 1, \cdot 2, \ldots \rangle$ *jest rozstrzygalna.*



Wniosek

Teoria MSO *struktury* $\langle \mathbb{N}^*, \cdot 0, \cdot 1, \cdot 2, \dots \rangle$ *jest rozstrzygalna.*



$$\exists X \dots \quad \rightsquigarrow \quad \exists X \big(\forall y \; y \in X \implies s_0(\varepsilon) \prec y \big) \wedge \dots$$

$$s_0(X) = Y \quad \rightsquigarrow \quad s_0(X) = Y$$

$$s_n(X) = Y \quad \rightsquigarrow \quad \underbrace{s_1 s_1 \dots s_1}_{n} \, s_0(X) = Y$$

Wniosek

Teoria MSO *przeliczalnych gęstych liniowych porządków bez końców jest rozstrzygalna.*

Fakt

Wszystkie przeliczalne gęste liniowe porządki bez końców są izomorficzne.

Zatem wystarczy zdefiniować taki porządek w $\langle \{0,1\}^*, \cdot 0, \cdot 1 \rangle$.

Wniosek

Teoria MSO *przeliczalnych gęstych liniowych porządków bez końców jest rozstrzygalna.*

Fakt

Wszystkie przeliczalne gęste liniowe porządki bez końców są izomorficzne.

Zatem wystarczy zdefiniować taki porządek w $\langle \{0,1\}^*, \cdot 0, \cdot 1 \rangle$.

Niech $x \leq y$, o ile x jest na lewo od y, czyli:

$$\begin{aligned} x < y &= \forall p \left(\curlywedge(p,x,y) \implies p \cdot 0 \preceq x \vee p \cdot 1 \preceq y \right) \\ \curlywedge(p,x,y) &= \forall z \left(z \preceq x \wedge z \preceq y \implies p \preceq z \right) \\ x \preceq y &= \forall X \left(y \in X \wedge \forall z (z \cdot 0 \in X \vee z \cdot 1 \in X \implies z \in X) \right. \\ &\qquad \left. \implies y \in X \right) \end{aligned}$$

Sprawdźmy gęstość. Niech $x < y$.
Jeśli $p \cdot 0 \preceq x$, to $x < x \cdot 1 < y$; jeśli $p \cdot 1 \preceq y$, to $x < y \cdot 0 < y$.

Twierdzenie Rabina i automaty

Krok 1

Indukcyjnie konstruujemy dla formuły $\varphi(\bar{X}) \in \mathrm{MSO}$ *automat* $\mathcal{A}_\varphi$ *wczytujący drzewa nieskończone nad alfabetem* $\{0,1\}^n$*, taki że*

$$\langle \{0,1\}^*, \cdot 0, \cdot 1, \bar{U} \rangle \models \varphi(\bar{X}) \quad \Longleftrightarrow \quad \mathcal{A} \text{ akceptuje } \chi_{\bar{U}}\,.$$

Krok 2

Rozstrzygamy, czy $\mathcal{A}_\varphi$ *akceptuje jakieś drzewo.*

- Jak wygladają automaty? Inaczej.
- Jak sprawdzać, czy $\mathcal{A}$ akceptuje jakieś drzewo? Trudno.
- Jak je zanegować? Bardzo trudno.

Definicja automatu z warunkiem Büchiego

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$, *gdzie*

- Σ, Q, q_0, F *są jak wcześniej,*
- *a* δ *ogranicza stany możliwe w obojgu dzieciach:*

$$\delta \subseteq Q \times \Sigma \times Q \times Q\,.$$

Bieg na drzewie $t \in \mathcal{T}_\Sigma$ *to takie drzewo* $\rho \in \mathcal{T}_Q$, *że*

$$\rho(\varepsilon) = q_0 \quad \textit{oraz} \quad \big\langle \rho(v), t(v), \rho(v \cdot 0), \rho(v \cdot 1) \big\rangle \in \delta\,.$$

Definicja automatu z warunkiem Büchiego

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$, *gdzie*

- Σ, Q, q_0, F *są jak wcześniej,*
- *a* δ *ogranicza stany możliwe w obojgu dzieciach:*

$$\delta \subseteq Q \times \Sigma \times Q \times Q\,.$$

Bieg na drzewie $t \in \mathcal{T}_\Sigma$ *to takie drzewo* $\rho \in \mathcal{T}_Q$, *że*

$$\rho(\varepsilon) = q_0 \quad \textit{oraz} \quad \big\langle \rho(v), t(v), \rho(v \cdot 0), \rho(v \cdot 1) \big\rangle \in \delta\,.$$

ρ *jest akceptujący jeśli* ***na każdej gałęzi*** $v_1 v_2 v_3 \ldots$ *mamy*

$$\exists^\infty i \; \rho(v_i) \in F\,.$$

Definicja automatu z warunkiem Büchiego

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$, *gdzie*

- Σ, Q, q_0, F *są jak wcześniej,*
- *a* δ *ogranicza stany możliwe w obojgu dzieciach:*

$$\delta \subseteq Q \times \Sigma \times Q \times Q\,.$$

Bieg na drzewie $t \in \mathcal{T}_\Sigma$ *to takie drzewo* $\rho \in \mathcal{T}_Q$, *że*

$$\rho(\varepsilon) = q_0 \quad \textit{oraz} \quad \big\langle \rho(v), t(v), \rho(v \cdot 0), \rho(v \cdot 1) \big\rangle \in \delta\,.$$

ρ *jest akceptujący jeśli* ***na każdej gałęzi*** $v_1 v_2 v_3 \ldots$ *mamy*

$$\exists^\infty i \; \rho(v_i) \in F\,.$$

Przykład. „Na każdej gałęzi nieskończenie wiele 1”.

Definicja automatu z warunkiem Büchiego

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, F \rangle$, *gdzie*

- Σ, Q, q_0, F *są jak wcześniej,*
- *a* δ *ogranicza stany możliwe w obojgu dzieciach:*

$$\delta \subseteq Q \times \Sigma \times Q \times Q\,.$$

Bieg na drzewie $t \in \mathcal{T}_\Sigma$ *to takie drzewo* $\rho \in \mathcal{T}_Q$, *że*

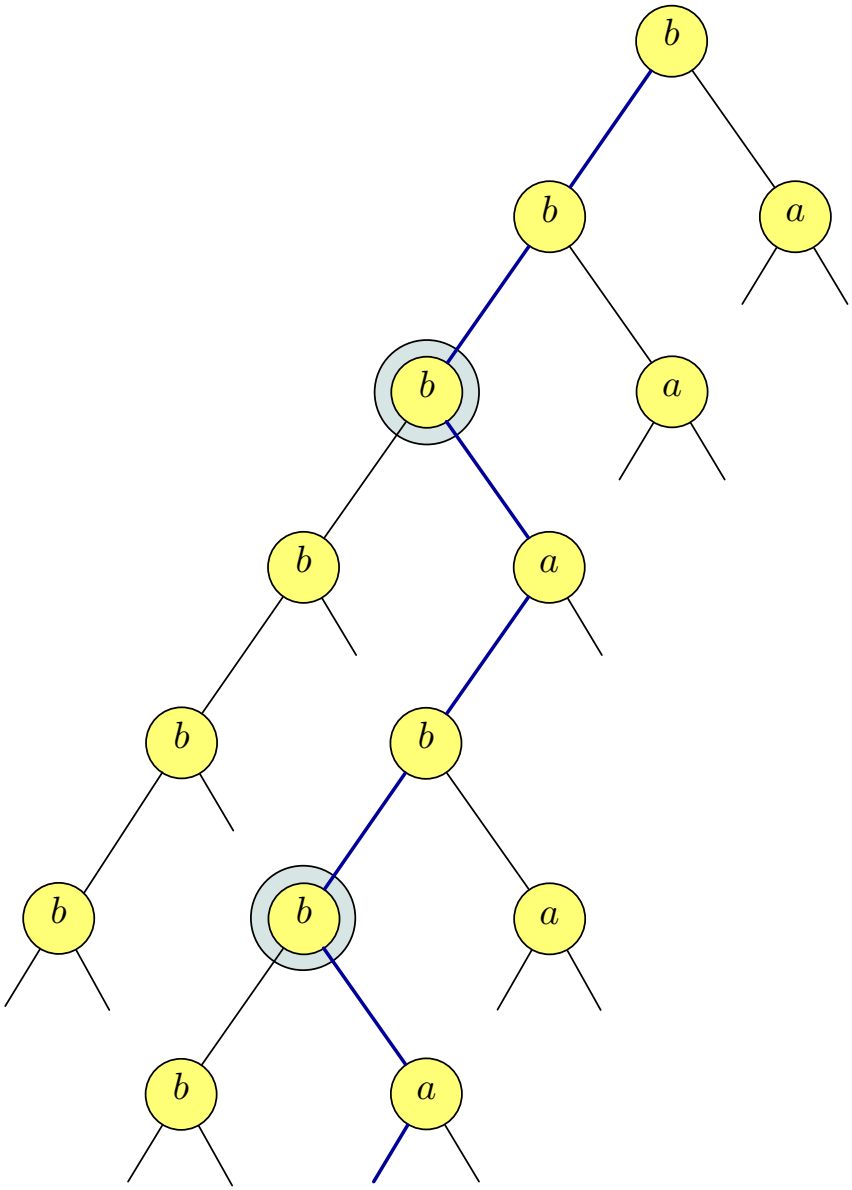
$$\rho(\varepsilon) = q_0 \quad \textit{oraz} \quad \big\langle \rho(v), t(v), \rho(v \cdot 0), \rho(v \cdot 1) \big\rangle \in \delta\,.$$

ρ *jest akceptujący jeśli* ***na każdej gałęzi*** $v_1 v_2 v_3 \ldots$ *mamy*

$$\exists^\infty i \; \rho(v_i) \in F\,.$$

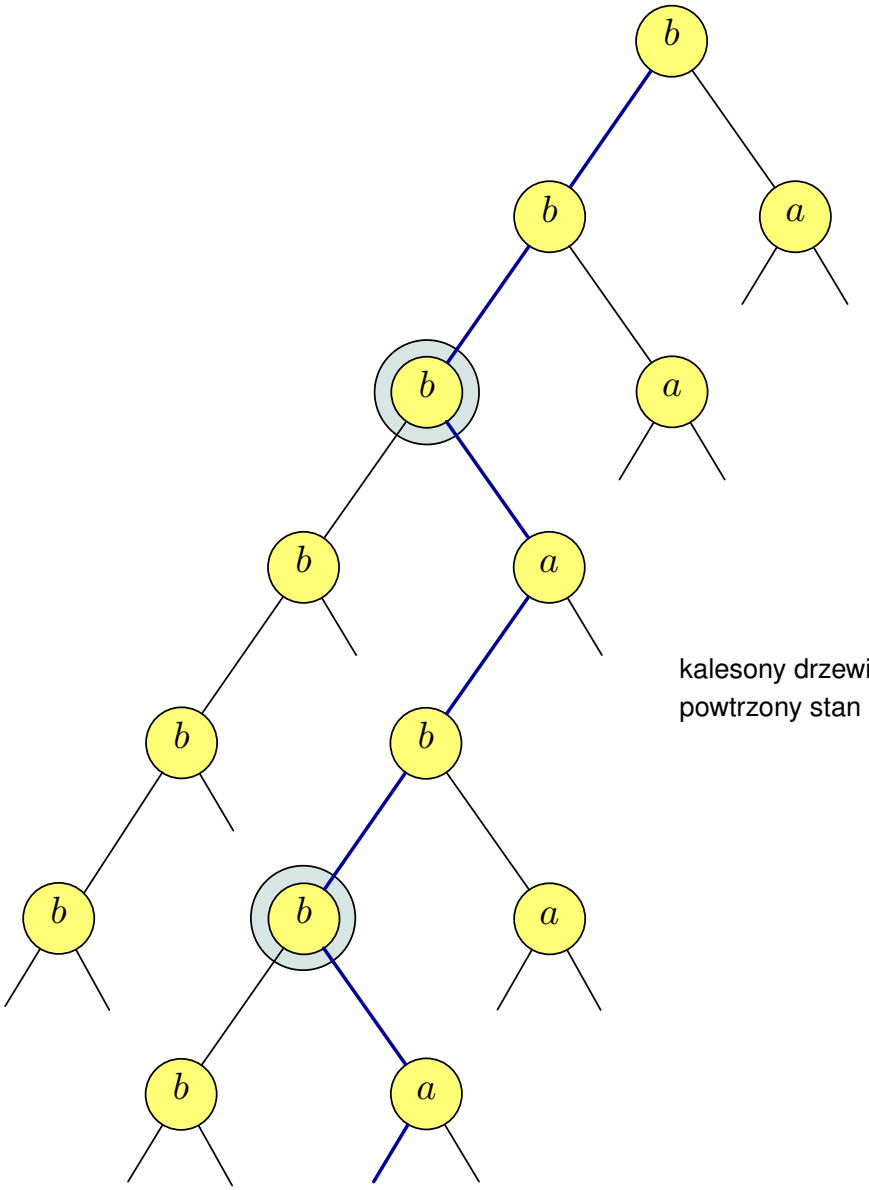
Przykład. „Na każdej gałęzi nieskończenie wiele 1".
(Kontr)przykład. „Na każdej gałęzi skończenie wiele 1".

$$\begin{aligned} \varphi(X) &= \forall G \, \big(\text{gałąź}(G) \implies \exists x \in G \, \forall y \in G \, (x \prec y \implies y \notin X)\big) \\ \text{gałąź}(G) &= \forall x \forall y x \in G \wedge y \in G \implies x \preceq y \vee y \preceq x \end{aligned}$$

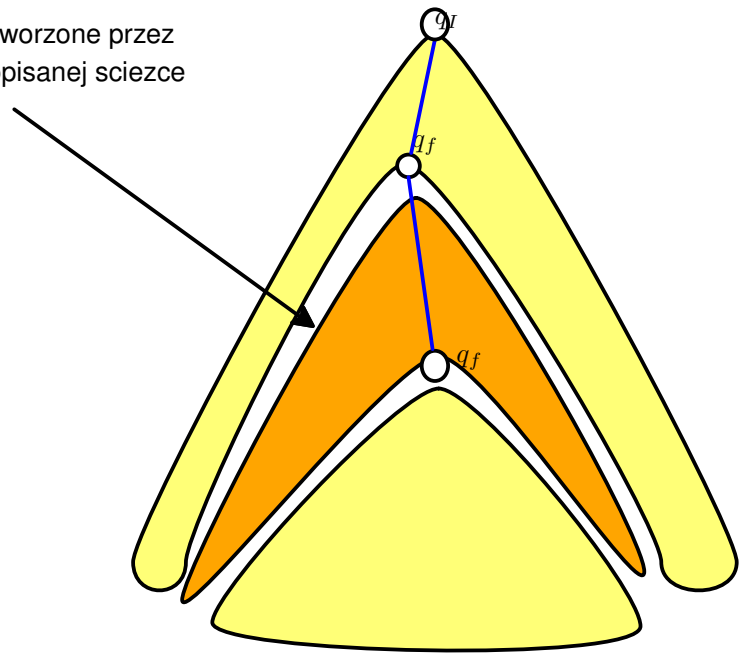


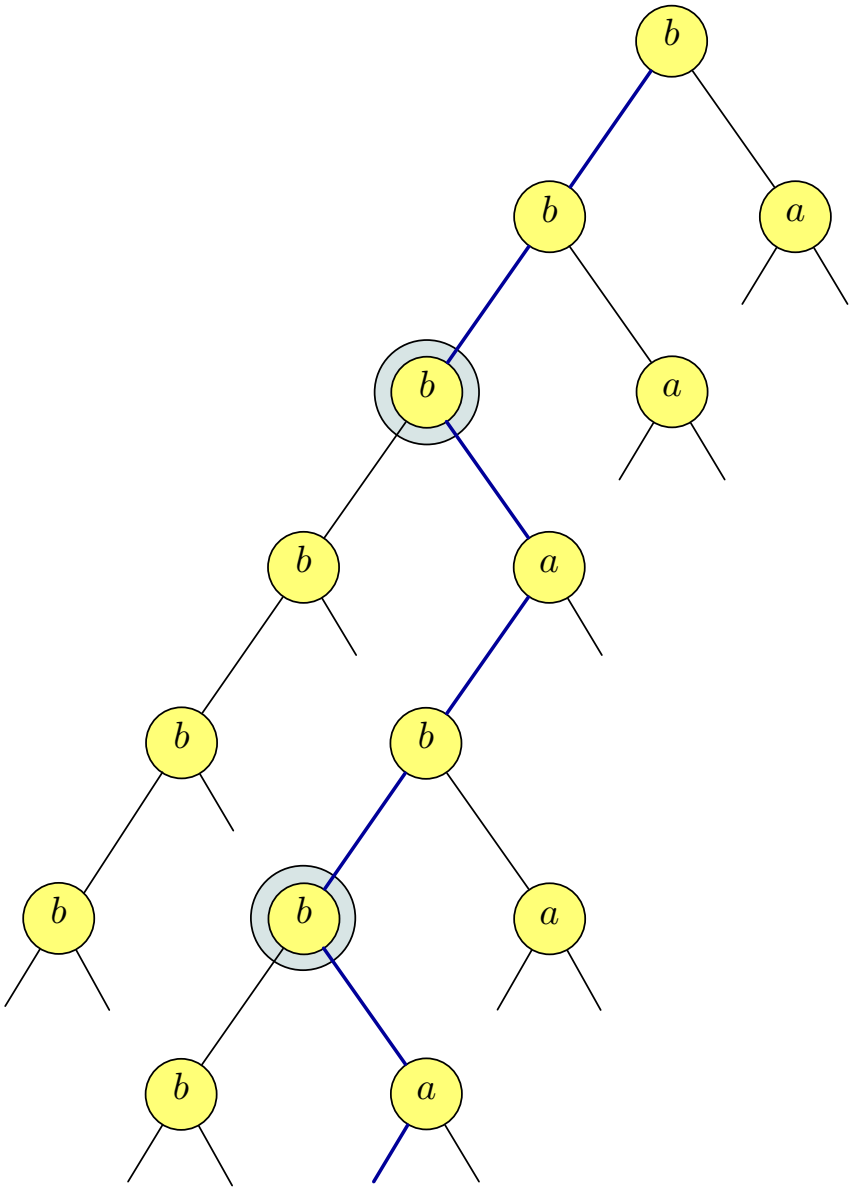
a w wierzchołkach $(0^*1)^k$
dla $k \leq |Q| + 1$;
b we wszystkich pozostałych.

a w wierzchołkach $(0^*1)^k$
dla $k \leq |Q| + 1$;
b we wszystkich pozostałych.

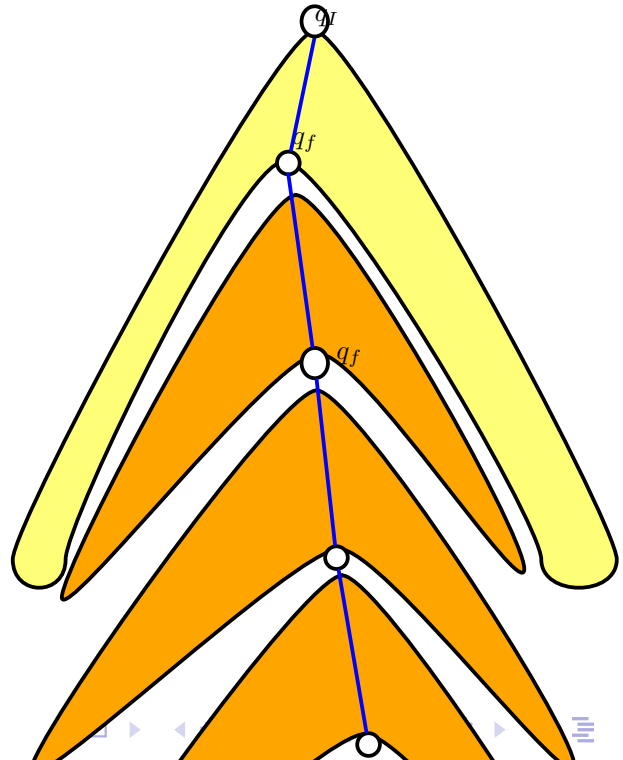


kalesony drzewiaste utworzone przez powtrzony stan q_f na opisanej sciezce





a w wierzchołkach $(0^*1)^k$
dla $k \leq |Q| + 1$;
b we wszystkich pozostałych.



Definicja automatu z warunkiem parzystości

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, \mathit{rank} \rangle$*, gdzie*

- Σ*,* Q*,* q_0*,* δ *jak wcześniej,*
- $\mathit{rank} \colon Q \to \mathbb{N}$ *funkcja zadająca priorytet stanów.*

Bieg jest akceptujący jeśli ***na każdej gałęzi*** *zachodzi warunek:*

wśród stanów odwiedzanych nieskończenie często
najwyższy priorytet jest ***parzysty****.*

Definicja automatu z warunkiem parzystości

Automat to $\mathcal{A} = \langle \Sigma, Q, q_0, \delta, \mathit{rank} \rangle$*, gdzie*

- Σ, Q, q_0, δ *jak wcześniej,*
- $\mathit{rank} \colon Q \to \mathbb{N}$ *funkcja zadająca priorytet stanów.*

Bieg jest akceptujący jeśli ***na każdej gałęzi*** *zachodzi warunek:*

wśród stanów odwiedzanych nieskończenie często
najwyższy priorytet jest ***parzysty****.*

Warunek Büchiego symulujemy kładąc

$$\mathit{rank}(q) = \begin{cases} 2 & \text{dla } q \in F \\ 1 & \text{dla } q \notin F \end{cases}$$

Gry parzystości i niepustość

Niepustość $L(\mathcal{A})$ można scharakteryzować za pomocą gry:

- Dwaj gracze, Automat i Tropiciel, wyknują ruchy w rundach.
- Gra rozpoczyna się w stanie początkowym q_0 i trwa ω rund.
- W rundzie $i \in \omega$
  - Automat wybiera krotkę $\langle q_{i-1}, a, q', q'' \rangle \in \delta$;
  - Tropiciel wybiera stan q_i spośród q', q''.
- Automat wygrywa, jeśli w ciągu stanów $q_0 q_1 q_2 \ldots$ najwyższy priorytet występujący nieskończenie często jest parzysty.

Fakt

$L(\mathcal{A}) \neq \emptyset \iff$ *Automat ma strategię wygrywającą.*

Twierdzenie

W każdej grze parzystości któryś gracz ma bezpamięciową strategię wygrywającą.

Konstrukcja automatu dla formuły $\varphi(X_1, X_2, \ldots, X_n)$

Każdy kwantyfikator wprowadza inną zmienna X_j dla $n < j \leq m$.

- $X_i = s_0(X_j)$, $X_i = s_1(X_j)$ i $X_i \subseteq X_j$ łatwo;
- $\vee$ odpowiada sumie języków;
- $\exists X_i$ odpowiada rzutowaniu liter na współrzędne różne od i;
- $\neg$ to główna trudność: wykorzystuje się bezpamięciową determinację gier parzystości (na przeliczanych grafach) oraz poniższe (trudne) twierdzenie.

Twierdzenie (McNaughton'66; Safra'88; Muller&Schupp'95)

Dla danego automatu Büchiego $\mathcal{A}$ na słowach można skonstruować ***deterministyczny*** *automat parzystości, rozpoznający $L(\mathcal{A})$.*

Zadanie 1: teoria MSO $\langle \mathbb{N}, succ \rangle$ jest nieelementarna

Formułę $\varphi(x, y)$ nazwiemy linijką długości d, jeśli jest prawdziwa dokładnie wtedy, gdy odległość między x a y to d.

- Pokazać, że dla dowolnego n istnieje linijka długości większej niż $\exp(n) = 2^n$, która opisuje się formułą MSO rozmiaru wielomianowego ze względu na n.
- Uogólnić powyższe: dla dowolnego n istnieje linijka długości większej niż $\exp^{(k)}(n)$, która opisuje się formułą MSO rozmiaru wielomianowego ze względu na n. Stałe i wykładnik wielomianu mogą zależeć od k.
- Korzystając z linijki udowodnić, że nie istnieje algorytm rozstrzygający prawdziwość danej formuły MSO w strukturze $\langle \mathbb{N}, succ \rangle$ i działający w czasie wykładniczym, czy też podwójnie wykładniczym, potrójnie wykładniczym, itd.

Zadanie 2: języki i siła wyrazu MSO

Słowo nieskończone nad alfabetem Σ można traktować jak $\langle \mathbb{N}, succ \rangle$ poszerzone o dodatkowe predykaty $X_a \subseteq \mathbb{N}$ dla $a \in \Sigma$. Zatem do definiowania językow słów nad alfabetem Σ można używać MSO (z dodatkowymi symbolami relacyjnymi X_a).

- MSO definiuje dokładnie te same języki, co automaty.
- Każdy język definiowalny w MSO można zdefiniować formułą postaci $\exists X \varphi(X)$, gdzie φ nie uzywa kwantyfikatorów drugiego rzędu. Warto zacząć od $\exists X_1 \exists X_2 \ldots \exists X_n \varphi(X_1, X_2, \ldots, X_n)$.
- Pokazać, że następujący język nie definiuje się w MSO:

$$\{a^{n_1} b a^{n_2} b \cdots : \lim_{i \to \infty} n_i = \infty\}.$$

- Słowo ostatecznie okresowe to słowo postaci $wvvv\ldots$ dla $w, v \in \Sigma^*$. Dwa języki definiowalne w MSO zawierające te same słowa ostatecznie okresowe muszą być równe.

Zadanie 3: rozstrzygalność logik

- Dla sygnatur zawierających wyłącznie relacje unarne, istnieje algorytm rozstrzygający czy zadana formuła MSO jest prawdziwa w każdej strukturze.
- Dla formuł FO typu $\exists^*\forall^*$ (tzn. ciąg kwantyfikatorów egzystencjalnych, potem ciąg kwantyfikatorów uniwersalnych, a potem formula bez kwantyfikatorów), istnieje algorytm rozstrzygający czy dana formuła jest spełnialna (tzn. spełniona w jakiejś strukturze).

Bibliografia

- W. Thomas, *Languages, Automata, and Logic*
  Kiel 1996 (dostępne online).
- M. Weyer, *Decidability of S1S and S2S*
  E. Grädel, W. Thomas, T. Wilke (Eds.), *Automata Logics, and Infinite Games. A guide to current research*, Lecture Notes in Computer Science, Vol. 2500, Springer 2002.
- M. Bojańczyk, *Automaty a logika. Skrypt z wykładu i ćwiczeń*
  Uniwersytet Warszawski 2009/2010.