Układy równań nad zbiorami liczb naturalnych

Artur Jeż

14 września 2010

Równania nad zbiorami liczb naturalnych

$$\varphi_j(X_1, \ldots, X_n) = \psi_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

- $X_i \subseteq \mathbb{N}$
- operacje: $\cup$, $\cap$, $+$

Równania nad zbiorami liczb naturalnych

$$\varphi_j(X_1, \ldots, X_n) = \psi_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

- $X_i \subseteq \mathbb{N}$
- operacje: $\cup$, $\cap$, $+$

$$X + Y = \{x + y \mid x \in X, y \in Y\}$$

Równania nad zbiorami liczb naturalnych

$$\varphi_j(X_1, \ldots, X_n) = \psi_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

- $X_i \subseteq \mathbb{N}$
- operacje: $\cup$, $\cap$, $+$

$$X + Y = \{x + y \mid x \in X, y \in Y\}$$

Przykład

- $X = \{0\} \cup (X + \{2\})$ $\quad X =$ zbiór liczb parzystych

Równania nad zbiorami liczb naturalnych

$$\varphi_j(X_1, \ldots, X_n) = \psi_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

- $X_i \subseteq \mathbb{N}$
- operacje: $\cup$, $\cap$, $+$

$$X + Y = \{x + y \mid x \in X, y \in Y\}$$

Przykład

- $X = \{0\} \cup (X + \{2\})$ $\quad X =$ zbiór liczb parzystych
- $X + \{1\} = (X + X) \cup \{2\}$ $\quad$ wiele rozwiązań, w tym $\{1\}$ oraz $\{1, 2, 3, \ldots\}$

Równania nad zbiorami liczb naturalnych

$$\varphi_j(X_1, \ldots, X_n) = \psi_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

- $X_i \subseteq \mathbb{N}$
- operacje: $\cup$, $\cap$, $+$

$$X + Y = \{x + y \mid x \in X, y \in Y\}$$

Przykład

- $X = \{0\} \cup (X + \{2\})$ $\quad X =$ zbiór liczb parzystych
- $X + \{1\} = (X + X) \cup \{2\}$ $\quad$ wiele rozwiązań, w tym $\{1\}$ oraz $\{1, 2, 3, \ldots\}$

- Charakteryzacja rozwiązań.

Języki formalne

Języki formalne

- Język: czysto syntaktycznie
- Bez wnikania w znaczenie
- Jak zdefiniowany

Języki formalne

- Język: czysto syntaktycznie
- Bez wnikania w znaczenie
- Jak zdefiniowany

Definicja

- alfabet Σ: skończony zbiór liter
- słowo: ciąg (skończony) liter
- język: zbiór skończonych słów (podzbiory Σ^*)
- formalnie zdefiniowany

Języki formalne

- Język: czysto syntaktycznie
- Bez wnikania w znaczenie
- Jak zdefiniowany

Definicja

- alfabet Σ: skończony zbiór liter
- słowo: ciąg (skończony) liter
- język: zbiór skończonych słów (podzbiory Σ^*)
- formalnie zdefiniowany

Modele

- maszyna
- gramatyka
- ...

Układy równań języków formalnych

$$\begin{cases} \varphi_1(X_1, \ldots, X_n) &= \psi_1(X_1, \ldots, X_n) \\ & \vdots \\ \varphi_m(X_1, \ldots, X_n) &= \psi_m(X_1, \ldots, X_n) \end{cases}$$

- X_i: podzbiór Σ^*.
- φ_i: zmienne, stałe, operacje na językach

$$L \cdot L' = \{ww' \mid w \in L, w' \in L'\}$$

Układy równań języków formalnych

$$\begin{cases} \varphi_1(X_1, \ldots, X_n) &= \psi_1(X_1, \ldots, X_n) \\ & \vdots \\ \varphi_m(X_1, \ldots, X_n) &= \psi_m(X_1, \ldots, X_n) \end{cases}$$

- X_i: podzbiór Σ^*.
- φ_i: zmienne, stałe, operacje na językach

$$L \cdot L' = \{ww' \mid w \in L, w' \in L'\}$$

- prosty
- łatwo przyciąć do potrzeb
- unifikuje gramatyki i automaty

Trudność obliczeniowa

- Ogólny przypadek

Trudność obliczeniowa

- Ogólny przypadek

Twierdzenie (Okhotin)

$L \subseteq \Sigma^*$ jest jedynym (najmniejszym, największym) rozwiązaniem układu równań w postaci uwikłanej, z operacjami $\{\cup, \cap, \cdot\}$

wtedy i tylko wtedy

L jest rekurencyjny (rek. przeliczalny, ko-rek. przeliczalny)

Trudność obliczeniowa

- Ogólny przypadek

Twierdzenie (Okhotin)

$L \subseteq \Sigma^*$ jest jedynym (najmniejszym, największym) rozwiązaniem układu równań w postaci uwikłanej, z operacjami $\{\cup, \cap, \cdot\}$

wtedy i tylko wtedy

L jest rekurencyjny (rek. przeliczalny, ko-rek. przeliczalny)

- $a, b \in \Sigma$

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ &\vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ & \vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

- Ginsburg i Rice ($\cup$, $\cdot$): gramatyki bezkontekstowe

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ & \vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

- Ginsburg i Rice $(\cup, \cdot)$: gramatyki bezkontekstowe
- wada gramatyk bezkontekstowych: nie są zamknięte na przecięcie

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ & \vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

- Ginsburg i Rice ($\cup$, $\cdot$): gramatyki bezkontekstowe
- wada gramatyk bezkontekstowych: nie są zamknięte na przecięcie
- rozszerzone przez Okhotina ($\cap$, $\cup$ i $\cdot$): gramatyki koniunkcyjne

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ & \vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

- Ginsburg i Rice ($\cup$, $\cdot$): gramatyki bezkontekstowe
- wada gramatyk bezkontekstowych: nie są zamknięte na przecięcie
- rozszerzone przez Okhotina ($\cap$, $\cup$ i $\cdot$): gramatyki koniunkcyjne
- rozwiązanie $(S_1, \ldots, S_n)$ jest najmniejsze: $S_i \subseteq S'_i$, dla każdego rozwiązania $(S'_1, \ldots, S'_n)$
- zawsze istnieje (tw. Tarskiego) bez ^{c} !

Układy równań w postaci nieuwikłanej: gramatyki

$$\begin{cases} X_1 &= \varphi_1(X_1, \ldots, X_n) \\ & \vdots \\ X_n &= \varphi_n(X_1, \ldots, X_n) \end{cases}$$

- Ginsburg i Rice ($\cup$, $\cdot$): gramatyki bezkontekstowe
- wada gramatyk bezkontekstowych: nie są zamknięte na przecięcie
- rozszerzone przez Okhotina ($\cap$, $\cup$ i $\cdot$): gramatyki koniunkcyjne
- rozwiązanie $(S_1, \ldots, S_n)$ jest najmniejsze: $S_i \subseteq S'_i$, dla każdego rozwiązania $(S'_1, \ldots, S'_n)$
- zawsze istnieje (tw. Tarskiego) bez ^{c} !
- rozwiązanie największe: analogicznie

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\Sigma = \{a\}$.

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\Sigma = \{a\}$.
- nieuwikłane $\{\cup, \cdot\}$: tylko języki regularne

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\Sigma = \{a\}$.
- nieuwikłane $\{\cup, \cdot\}$: tylko języki regularne
- $\{\cdot, {}^c\}$: przykład języka nieregularnego [Leiss 1994]

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\Sigma = \{a\}$.
- nieuwikłane $\{\cup, \cdot\}$: tylko języki regularne
- $\{\cdot, {}^c\}$: przykład języka nieregularnego [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\Sigma = \{a\}$.
- nieuwikłane $\{\cup, \cdot\}$: tylko języki regularne
- $\{\cdot, {}^c\}$: przykład języka nieregularnego [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

- jedyna informacja: długość $a^n \longleftrightarrow$ liczba n

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\mathbb{N}$
- nieuwikłane $\{\cup, \cdot\}$: okresowe
- $\{\cdot, {}^c\}$: nieokresowe [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\mathbb{N}$
- nieuwikłane $\{\cup, \cdot\}$: okresowe
- $\{\cdot, {}^c\}$: nieokresowe [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

- wyrażenia arytmetyczne (wyrażenie regularne)
- obwody arytmetyczne
- automaty
- gramatyki

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\mathbb{N}$
- nieuwikłane $\{\cup, \cdot\}$: okresowe
- $\{\cdot, {}^c\}$: nieokresowe [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

- wyrażenia arytmetyczne (wyrażenie regularne)
- obwody arytmetyczne
- automaty
- gramatyki
- układy równań

Języki formalne i zbiory liczb naturalnych

- prosty przypadek: $\mathbb{N}$
- nieuwikłane $\{\cup, \cdot\}$: okresowe
- $\{\cdot, {}^c\}$: nieokresowe [Leiss 1994]
- nieuwikłane $\{\cup, \cap, \cdot\}$: ?

- wyrażenia arytmetyczne (wyrażenie regularne)
- obwody arytmetyczne
- automaty
- gramatyki
- układy równań

$$L_X \cdot L_Y \implies X + Y = \{x + y \mid x \in X, y \in Y\}$$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$X_1 = (X_2 + X_2 \cap X_1 + X_3) \cup \{1\}$$
$$X_2 = (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\}$$
$$X_3 = (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\}$$
$$X_{12} = X_3 + X_3 \cap X_1 + X_2$$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$
\begin{aligned}
X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\
X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\
X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\
X_{12} &= X_3 + X_3 \cap X_1 + X_2
\end{aligned}
\qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)
$$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$
\begin{aligned}
X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\
X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\
X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\
X_{12} &= X_3 + X_3 \cap X_1 + X_2
\end{aligned}
\qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)
$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 =$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$
\begin{aligned}
X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\
X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\
X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\
X_{12} &= X_3 + X_3 \cap X_1 + X_2
\end{aligned}
\qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)
$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$\begin{aligned} X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\ X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\ X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\ X_{12} &= X_3 + X_3 \cap X_1 + X_2 \end{aligned} \qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup (20^*20^*)_4$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$
\begin{aligned}
X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\
X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\
X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\
X_{12} &= X_3 + X_3 \cap X_1 + X_2
\end{aligned}
\qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)
$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup (20^*20^*)_4$
- $X_1 + X_3 = (10^*)_4 + (30^*)_4 =$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$\begin{aligned} X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\ X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\ X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\ X_{12} &= X_3 + X_3 \cap X_1 + X_2 \end{aligned} \qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup (20^*20^*)_4$
- $X_1 + X_3 = (10^*)_4 + (30^*)_4 = (10^+)_4 \cup$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$\begin{aligned} X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\ X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\ X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\ X_{12} &= X_3 + X_3 \cap X_1 + X_2 \end{aligned} \qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup (20^*20^*)_4$
- $X_1 + X_3 = (10^*)_4 + (30^*)_4 = (10^+)_4 \cup (10^*30^*)_4 \cup (30^*10^*)_4$

Zapis pozycyjny

- Liczby w zapisie k-pozycyjnym: ciągi cyfr z $\Sigma_k = \{0, 1, \ldots, k-1\}$.
- $(a_1 \ldots a_\ell)_k$: liczba zapisana jako $a_1 \ldots a_\ell$ w notacji k-pozycyjnej
- zbiór liczb $\longleftrightarrow$ język formalny nad Σ_k

Przykład

$$\begin{aligned} X_1 &= (X_2 + X_2 \cap X_1 + X_3) \cup \{1\} \\ X_2 &= (X_{12} + X_2 \cap X_1 + X_1) \cup \{2\} \\ X_3 &= (X_{12} + X_{12} \cap X_1 + X_2) \cup \{3\} \\ X_{12} &= X_3 + X_3 \cap X_1 + X_2 \end{aligned} \qquad ((10^*)_4, (20^*)_4, (30^*)_4, (120^*)_4)$$

- $X_2 + X_2 = (20^*)_4 + (20^*)_4 = (10^+)_4 \cup (20^*20^*)_4$
- $X_1 + X_3 = (10^*)_4 + (30^*)_4 = (10^+)_4 \cup (10^*30^*)_4 \cup (30^*10^*)_4$
- $(X_2 + X_2) \cap (X_1 + X_3) = (10^+)_4$

Uogólnienie przykładu

Odpowiedź na pytanie o okresowość rozwiązań.

Uogólnienie przykładu

Odpowiedź na pytanie o okresowość rozwiązań.

- Rozszerzanie o wiodącą cyfrę
- Odpowiada automatowi skończonemu

Uogólnienie przykładu

Odpowiedź na pytanie o okresowość rozwiązań.

- Rozszerzanie o wiodącą cyfrę
- Odpowiada automatowi skończonemu

Twierdzenie

Dla automatu skończonego M istnieje nieuwikłany system z $\{\cup, \cap, +\}$ o najmniejszym rozwiązaniu $(L(M))_k$.

Uogólnienie przykładu

Odpowiedź na pytanie o okresowość rozwiązań.

- Rozszerzanie o wiodącą cyfrę
- Odpowiada automatowi skończonemu

Twierdzenie

Dla automatu skończonego M istnieje nieuwikłany system z $\{\cup, \cap, +\}$ o najmniejszym rozwiązaniu $(L(M))_k$.

- Rozszerzenia w jedną stronę: kres możliwości
- Rozszerzenia w obie strony? (niejasne jak).

Uogólnienie przykładu

Odpowiedź na pytanie o okresowość rozwiązań.

- Rozszerzanie o wiodącą cyfrę
- Odpowiada automatowi skończonemu

Twierdzenie

Dla automatu skończonego M istnieje nieuwikłany system z $\{\cup, \cap, +\}$ o najmniejszym rozwiązaniu $(L(M))_k$.

- Rozszerzenia w jedną stronę: kres możliwości
- Rozszerzenia w obie strony? (niejasne jak).
- Zmieniamy reprezentację
- Liczbę $(aub)_k$ można zdefiniować przez $(au)_k$ oraz $(ub)_k$

Automaty kratowe

Definicja (Culik, Gruska, Salomaa)

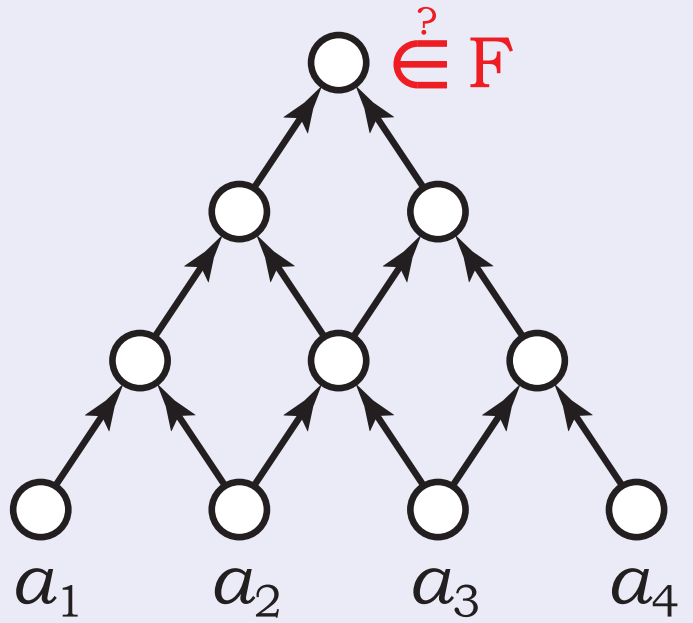
Automat kratowy to $M = (\Sigma, Q, I, \delta, F)$:

Automaty kratowe

Definicja (Culik, Gruska, Salomaa)

Automat kratowy to $M = (\Sigma, Q, I, \delta, F)$:

- Σ: alfabet wejściowy;
- Q: skończony zbiór stanów;
- $I : \Sigma \to Q$ ustala stany początkowe;
- $\delta : Q \times Q \to Q$, funkcja przejścia
- $F \subseteq Q$: stany akceptujące.

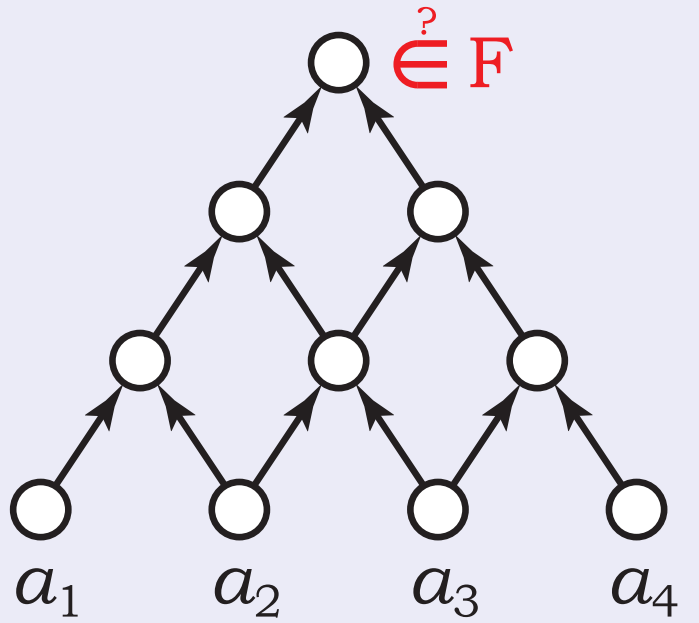


Automaty kratowe

Definicja (Culik, Gruska, Salomaa)

Automat kratowy to $M = (\Sigma, Q, I, \delta, F)$:

- Σ: alfabet wejściowy;
- Q: skończony zbiór stanów;
- $I : \Sigma \to Q$ ustala stany początkowe;
- $\delta : Q \times Q \to Q$, funkcja przejścia
- $F \subseteq Q$: stany akceptujące.



Twierdzenie

Dla automatu kratowego M istnieje nieuwikłany system używający operacji $\{\cup, \cap, +\}$ z $(L(M))_k$ jako najmniejszym rozwiązaniem.

Złożoność obliczeniowa

Problem przynależności

Dla nieuwikłanego układu równań i n zdecydować, czy n należy do najmniejszego rozwiązania.

Złożoność obliczeniowa

Problem przynależności

Dla nieuwikłanego układu równań i n zdecydować, czy n należy do najmniejszego rozwiązania.

Twierdzenie (Huynh)

Układy z $\cup$, $+$: NP-zupełny.

Złożoność obliczeniowa

Problem przynależności

Dla nieuwikłanego układu równań i n zdecydować, czy n należy do najmniejszego rozwiązania.

Twierdzenie (Huynh)

Układy z $\cup$, $+$: NP-zupełny.

Twierdzenie (Nowe!)

Układy z $\cup$, $\cap$, $+$: EXPTIME-zupełny.

Złożoność obliczeniowa

Problem przynależności

Dla nieuwikłanego układu równań i n zdecydować, czy n należy do najmniejszego rozwiązania.

Twierdzenie (Huynh)

Układy z $\cup$, $+$: NP-zupełny.

Twierdzenie (Nowe!)

Układy z $\cup$, $\cap$, $+$: EXPTIME-zupełny.

Idea dowodu

- kodowanie obliczeń ATM o ograniczonej taśmie

Złożoność obliczeniowa

Problem przynależności

Dla nieuwikłanego układu równań i n zdecydować, czy n należy do najmniejszego rozwiązania.

Twierdzenie (Huynh)

Układy z $\cup$, $+$: NP-zupełny.

Twierdzenie (Nowe!)

Układy z $\cup$, $\cap$, $+$: EXPTIME-zupełny.

Idea dowodu

- kodowanie obliczeń ATM o ograniczonej taśmie
- konfiguracja $\longrightarrow (a_1\ 0\ a_2\ 0 \ldots 0\ a_\ell\ q\ a_{\ell+1}\ 0 \ldots a_n\ 0)_k$
- przejście: zmiana wartości liczbowej $(+)$
- symulacja alternacji: $\cup$ oraz $\cap$

Równania w postaci uwikłanej

$$\begin{cases} \varphi_1(X_1, \ldots, X_n) & = & \psi_1(X_1, \ldots, X_n) \\ & \vdots & \\ \varphi_m(X_1, \ldots, X_n) & = & \psi_m(X_1, \ldots, X_n) \end{cases}$$

- X_i: podzbiór $\mathbb{N}$.
- φ_i: zmienne, stałe, operacje na zbiorach.

Równania w postaci uwikłanej

$$\begin{cases} \varphi_1(X_1, \ldots, X_n) &= \psi_1(X_1, \ldots, X_n) \\ & \vdots \\ \varphi_m(X_1, \ldots, X_n) &= \psi_m(X_1, \ldots, X_n) \end{cases}$$

- X_i: podzbiór Σ^*.
- φ_i: zmienne, stałe, operacje na językach.

Twierdzenie (Okhotin)

$L \subseteq \Sigma^*$ jest jedynym (najmniejszym, największym) rozwiązaniem układu równań w postaci uwikłanej, z operacjami $\{\cup, \cap, \cdot\}$

wtedy i tylko wtedy

L jest rekurencyjny (rek. przeliczalny, ko-rek. przeliczalny)

Równania w postaci uwikłanej

$$\begin{cases} \varphi_1(X_1, \ldots, X_n) &= \psi_1(X_1, \ldots, X_n) \\ & \vdots \\ \varphi_m(X_1, \ldots, X_n) &= \psi_m(X_1, \ldots, X_n) \end{cases}$$

- X_i: podzbiór $\mathbb{N}$.
- φ_i: zmienne, stałe, operacje na zbiorach.

Twierdzenie (Nowe!)

$S \subseteq \mathbb{N}$ jest jedynym (najmniejszym, największym) rozwiązaniem układu równań w postaci uwikłanej, z operacjami $\{\cup, +\}$ lub $\{\cap, +\}$

wtedy i tylko wtedy

S jest rekurencyjny (rek. przeliczalny, ko-rek. przeliczalny)

Równania z jedną zmienną

- Powrót do początku

Czy można wymusić okresowość rozwiązań?

Równania z jedną zmienną

- Powrót do początku

Czy można wymusić okresowość rozwiązań?

- Np. ilość zmiennych

Równania z jedną zmienną

- Powrót do początku

Czy można wymusić okresowość rozwiązań?

- Np. ilość zmiennych

Twierdzenie (Okhotin)

Istnieje nieuwikłany układ równań z jedną zmienną i operacjami $\cup$, $\cap$, $+$ *o nieokresowym rozwiązaniu.*

- Kodowanie pierwszego przykładu

Równania z jedną zmienną

- Powrót do początku

Czy można wymusić okresowość rozwiązań?

- Np. ilość zmiennych

Twierdzenie (Okhotin)

Istnieje nieuwikłany układ równań z jedną zmienną i operacjami $\cup$, $\cap$, $+$ *o nieokresowym rozwiązaniu.*

- Kodowanie pierwszego przykładu

Czy można to uogólnić?

Jedna zmienna

- Uogólnienie: kodowanie dowolnego układu

Jedna zmienna

- Uogólnienie: kodowanie dowolnego układu

Kodowanie zbioru: $A \longrightarrow \{kn + i \mid n \in A\}$.

Jedna zmienna

- Uogólnienie: kodowanie dowolnego układu

Kodowanie zbioru: $A \longrightarrow \{kn + i \mid n \in A\}$.

Twierdzenie

Istnieje efektywne kodowanie dowolnego układu równań w postaci nieuwikłanej w równaniu $X = \varphi(X)$.

Jedna zmienna

- Uogólnienie: kodowanie dowolnego układu

Kodowanie zbioru: $A \longrightarrow \{kn + i \mid n \in A\}$.

Twierdzenie

Istnieje efektywne kodowanie dowolnego układu równań w postaci nieuwikłanej w równaniu $X = \varphi(X)$.
Rozwiązania nowego równania są postaci $S = \bigcup_{j=0}^{m} \{kn + p_j \mid n \in S_j\}$, *gdzie* $(S_1, \ldots, S_m)$ *są rozwiązaniami oryginalnego równania.*

Jedna zmienna

- Uogólnienie: kodowanie dowolnego układu

Kodowanie zbioru: $A \longrightarrow \{kn + i \mid n \in A\}$.

Twierdzenie

Istnieje efektywne kodowanie dowolnego układu równań w postaci nieuwikłanej w równaniu $X = \varphi(X)$.
Rozwiązania nowego równania są postaci $S = \bigcup_{j=0}^{m} \{kn + p_j \mid n \in S_j\}$, *gdzie* $(S_1, \ldots, S_m)$ *są rozwiązaniami oryginalnego równania.*

Twierdzenie

Istnieje efektywne kodowanie dowolnego układu równań w równaniu $\psi(X) = \varphi(X)$.
Rozwiązania nowego równania są postaci $S = \bigcup_{j=0}^{m} \{kn + p_j \mid n \in S_j\} \cup C$, *gdzie* $(S_1, \ldots, S_m)$ *są rozwiązaniami oryginalnego równania.*

Równania z $+$

Pytanie

Czy można użyć tylko jednej operacji?

Równania z $+$

Pytanie

Czy można użyć tylko jednej operacji?

Twierdzenie (Kunc)

Dla $\{a, b\} \subseteq \Sigma$ istnieje skończona stała L, taka że równanie

$$X \cdot L = L \cdot X$$

ma ko-rek. przeliczalne trudne największe rozwiązanie.

Równania z $+$

Pytanie

Czy można użyć tylko jednej operacji?

Twierdzenie (Kunc)

Dla $\{a, b\} \subseteq \Sigma$ istnieje skończona stała L, taka że równanie

$$X \cdot L = L \cdot X$$

ma ko-rek. przeliczalne trudne największe rozwiązanie.

Twierdzenie

System używający $\cup$, $+$ można zakodować w systemie używającym $+$.

Trudne rozwiązania

Rek. przeliczalne-trudne, ko-rek. przeliczalne trudne rozwiązania.

Idea kodowania

- wiele zmiennych
- nowa zmienna koduje starą

Idea kodowania

- wiele zmiennych
- nowa zmienna koduje starą
- weryfikowalne

$$\psi(X) = \varphi(X) \iff X = \sigma(A)$$

Idea kodowania

- wiele zmiennych
- nowa zmienna koduje starą
- weryfikowalne

$$\psi(X) = \varphi(X) \iff X = \sigma(A)$$

- koduje $+$:

$$A + B = C \iff \psi_+(\sigma(A), \sigma(B)) = \varphi_+(\sigma(C))$$

Idea kodowania

- wiele zmiennych
- nowa zmienna koduje starą
- weryfikowalne

$$\psi(X) = \varphi(X) \iff X = \sigma(A)$$

- koduje $+$:

$$A + B = C \iff \psi_+(\sigma(A), \sigma(B)) = \varphi_+(\sigma(C))$$

- koduje $\cup$:

$$A \cup B = C \iff \psi_\cup(\sigma(A), \sigma(B)) = \varphi_\cup(\sigma(C))$$

Podsumowanie

- Badamy układy równań nad zbiorami liczb naturalnych
- Operacje $\cup$, $\cap$, $+$

Podsumowanie

- Badamy układy równań nad zbiorami liczb naturalnych
- Operacje $\cup$, $\cap$, $+$
- Rozwiązania układów równań w postaci nieuwikłanej są skomplikowane (EXPTIME-zupełne)
- Jedyne (najmniejsze, największe) rozwiązania układów równań w postaci uwikłanej to dokładnie zbiory rekurencyjne (rek. przeliczalne, ko-rek. przeliczalne)

Podsumowanie

- Badamy układy równań nad zbiorami liczb naturalnych
- Operacje $\cup$, $\cap$, $+$
- Rozwiązania układów równań w postaci nieuwikłanej są skomplikowane (EXPTIME-zupełne)
- Jedyne (najmniejsze, największe) rozwiązania układów równań w postaci uwikłanej to dokładnie zbiory rekurencyjne (rek. przeliczalne, ko-rek. przeliczalne)
- Wyniki nawet dla jednej zmiennej i jednego równania
- Wyniki dla operacji $+$ (równania uwikłane)

Podsumowanie

- Badamy układy równań nad zbiorami liczb naturalnych
- Operacje $\cup$, $\cap$, $+$
- Rozwiązania układów równań w postaci nieuwikłanej są skomplikowane (EXPTIME-zupełne)
- Jedyne (najmniejsze, największe) rozwiązania układów równań w postaci uwikłanej to dokładnie zbiory rekurencyjne (rek. przeliczalne, ko-rek. przeliczalne)
- Wyniki nawet dla jednej zmiennej i jednego równania
- Wyniki dla operacji $+$ (równania uwikłane)

Dziękuję za uwagę!