Złożoność obliczeniowa algorytmów

Algorytmy probabilistyczne

Kordian A. Smoliński

Wydział Fizyki i Informatyki Stosowanej

2024/2025

Algorytmy probabilistyczne

Treść wykładu

Probabilistyczna maszyna Turinga

Probabilistyczna maszyna Turinga

Niedetrministyczna maszyna Turinga, która wybór ścieżki obliczeń podejmuje losowo zgodnie z pewnym rozkładem prawdopodobieństwa.

Probabilistyczna maszyna Turinga

Probabilistyczna maszyna Turinga

Niedetrministyczna maszyna Turinga, która wybór ścieżki obliczeń podejmuje losowo zgodnie z pewnym rozkładem prawdopodobieństwa.

Definicja

Niech M będzie probabilistyczną maszyną Turinga, a w jej słowem wejściowym. $P_M(w)$ oznacza prawdopodobieństwo zaakceptowania słowa w prze maszynę M.

Probabilistyczna maszyna Turinga

Probabilistyczna maszyna Turinga

Niedetrministyczna maszyna Turinga, która wybór ścieżki obliczeń podejmuje losowo zgodnie z pewnym rozkładem prawdopodobieństwa.

Definicja

Niech M będzie probabilistyczną maszyną Turinga, a w jej słowem wejściowym. $P_M(w)$ oznacza prawdopodobieństwo zaakceptowania słowa w prze maszynę M.

$P_M(w)$ obliczamy na podstawie analizy możliwych ścieżek obliczeń.

Probabilistyczna maszyna Turinga

Deterministyczna maszyna Turinga jest probabilistyczną maszyną Turinga, dla której w każdym kroku jedna ze ścieżek obliczeń ma prawdopodobieństwo wyboru 1, a pozostałe 0. Jeżeli L jest językiem rozstrzyganym przez deterministyczną maszynę Turinga M, to:

$$\begin{aligned} w \in L &\implies P_M(w) = 1, \\ w \notin L &\implies P_M(w) = 0. \end{aligned}$$

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ
Uniwersytet Łódzki

Probabilistyczna maszyna Turinga

Deterministyczna maszyna Turinga jest probabilistyczną maszyną Turinga, dla której w każdym kroku jedna ze ścieżek obliczeń ma prawdopodobieństwo wyboru 1, a pozostałe 0. Jeżeli L jest językiem rozstrzyganym przez deterministyczną maszynę Turinga M, to:

$$\begin{aligned} w \in L &\implies P_M(w) = 1, \\ w \notin L &\implies P_M(w) = 0. \end{aligned}$$

Chcemy powiązać prawdopodobieństwo akceptacji słowa w z jego przynależnością do języka L dla ogólnej probabilistycznej maszyny Turinga. Dopuszczamy przy tym, że maszyna probabilistyczna może się mylić.

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

L język;

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

L język;

w słowo wejściowe maszyny M.

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

L język;

w słowo wejściowe maszyny M.

Definicje

Maszyna M może udzielić fałszywej odpowiedzi

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ
Uniwersytet Łódzki

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

L język;

w słowo wejściowe maszyny M.

Definicje

Maszyna M może udzielić fałszywej odpowiedzi negatywnej jeżeli $w \in L$, a $P_M(w) \neq 1$;

Błąd maszyny probabilistycznej

Niech:

M probabilistyczna maszyna Turinga;

L język;

w słowo wejściowe maszyny M.

Definicje

Maszyna M może udzielić fałszywej odpowiedzi

negatywnej jeżeli $w \in L$, a $P_M(w) \neq 1$;

pozytywnej jeżeli $w \notin L$, a $P_M(w) \neq 0$.

Algorytmy Monte Carlo

Algorytmy Monte Carlo to algorytmy probabilistyczne, dla których jest określone prawdopodobieństwo błędu.

Algorytmy Monte Carlo

Algorytmy Monte Carlo to algorytmy probabilistyczne, dla których jest określone prawdopodobieństwo błędu.

Definicja

RP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) \geqslant \frac{1}{2},$$
$$w \notin L \implies P_M(w) = 0.$$

Algorytmy Monte Carlo

Algorytmy Monte Carlo to algorytmy probabilistyczne, dla których jest określone prawdopodobieństwo błędu.

Definicja

RP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$\begin{aligned} w \in L &\implies P_M(w) \geqslant \frac{1}{2}, \\ w \notin L &\implies P_M(w) = 0. \end{aligned}$$

- Maszyna nie daje fałszywych odpowiedzi pozytywnych.

Algorytmy Monte Carlo to algorytmy probabilistyczne, dla których jest określone prawdopodobieństwo błędu.

Definicja

RP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) \geqslant \frac{1}{2},$$
$$w \notin L \implies P_M(w) = 0.$$

- Maszyna nie daje fałszywych odpowiedzi pozytywnych.
- Prawdopodobieństwo fałszywej odpowiedzi negatywnej jest ograniczone.

Algorytmy Monte Carlo

Tabela: Prawdopodobieństwo odpowiedzi algorytmu **RP**: 1 przebieg

	Odpowiedź	
	$w \in L$	$w \notin L$
$w \in L$	$\geqslant \frac{1}{2}$	$\leqslant \frac{1}{2}$
$w \notin L$	0	1

Tabela: Prawdopodobieństwo odpowiedzi algorytmu **RP**: n przebiegów

	Odpowiedź	
	$w \in L$	$w \notin L$
$w \in L$	$\geqslant 1 - \frac{1}{2^n}$	$\leqslant \frac{1}{2^n}$
$w \notin L$	0	1

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ Uniwersytet Łódzki

Algorytmy Monte Carlo

Definicja

coRP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) = 1,$$
$$w \notin L \implies P_M(w) \leqslant \frac{1}{2}.$$

Algorytmy Monte Carlo

Definicja

coRP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) = 1,$$
$$w \notin L \implies P_M(w) \leqslant \frac{1}{2}.$$

Nie wiadomo, czy

$$\mathbf{RP} \stackrel{?}{=} \mathbf{coRP}?$$

Algorytmy Monte Carlo

Definicja

BPP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) \geqslant \frac{2}{3},$$
$$w \notin L \implies P_M(w) \leqslant \frac{1}{3}.$$

Algorytmy Monte Carlo

Definicja

BPP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w czasie wielomianowym, o własności

$$w \in L \implies P_M(w) \geqslant \frac{2}{3},$$
$$w \notin L \implies P_M(w) \leqslant \frac{1}{3}.$$

$$\mathbf{RP} \subseteq \mathbf{BPP}, \qquad \mathbf{coRP} \subseteq \mathbf{BPP}.$$

Algorytmy Monte Carlo

Tabela: Prawdopodobieństwo odpowiedzi algorytmu **BPP**: 1 przebieg

	Odpowiedź	
	$w \in L$	$w \notin L$
$w \in L$	$\geqslant \frac{2}{3}$	$\leqslant \frac{1}{3}$
$w \notin L$	$\leqslant \frac{1}{3}$	$\geqslant \frac{2}{3}$

Tabela: Prawdopodobieństwo odpowiedzi algorytmu **BPP**: n przebiegów

	Odpowiedź	
	$w \in L$	$w \notin L$
$w \in L$	$\geqslant 1 - \frac{1}{3^n}$	$\leqslant \frac{1}{3^n}$
$w \notin L$	$\leqslant \frac{1}{3^n}$	$\geqslant 1 - \frac{1}{3^n}$

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ Uniwersytet Łódzki

Algorytmy Las Vegas

Algorytmy Las Vegas to algorytmy probabilistyczne, które zawsze dają poprawną odpowiedź, jednak czas jego działania jest nieokreślony; wielomianowy jest jedynie czas oczekiwany.

Algorytmy Las Vegas

Algorytmy Las Vegas to algorytmy probabilistyczne, które zawsze dają poprawną odpowiedź, jednak czas jego działania jest nieokreślony; wielomianowy jest jedynie czas oczekiwany.

Definicja

ZPP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w oczekiwanym czasie wielomianowym, rozstrzygająca L bez popełniania błędu.

Algorytmy Las Vegas

Algorytmy Las Vegas to algorytmy probabilistyczne, które zawsze dają poprawną odpowiedź, jednak czas jego działania jest nieokreślony; wielomianowy jest jedynie czas oczekiwany.

Definicja

ZPP to klasa języków L, dla których istnieje maszyna probabilistyczna M, działająca w oczekiwanym czasie wielomianowym, rozstrzygająca L bez popełniania błędu.

$$\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}.$$

Generowanie ciągów losowych

- Idealne źródło bitów losowych generuje je tak, aby każdy bit zachowywał się jak niezależna próba losowa.

Generowanie ciągów losowych

- Idealne źródło bitów losowych generuje je tak, aby każdy bit zachowywał się jak niezależna próba losowa.
- Idealne źródło bitów losowych jest symetryczne — jednakowe prawdopodobieństwo 0 i 1 w każdym kroku.

Generowanie ciągów losowych

- Idealne źródło bitów losowych generuje je tak, aby każdy bit zachowywał się jak niezależna próba losowa.
- Idealne źródło bitów losowych jest symetryczne — jednakowe prawdopodobieństwo 0 i 1 w każdym kroku.
- Każdy ciąg n bitów wygenerowanych przez idealne źródło bitów losowych jest jednakowo prawdopodobny.

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ
Uniwersytet Łódzki

Generowanie ciągów losowych

- Idealne źródło bitów losowych generuje je tak, aby każdy bit zachowywał się jak niezależna próba losowa.
- Idealne źródło bitów losowych jest symetryczne — jednakowe prawdopodobieństwo 0 i 1 w każdym kroku.
- Każdy ciąg n bitów wygenerowanych przez idealne źródło bitów losowych jest jednakowo prawdopodobny.
- Nie jest znane żadne fizyczne idealne źródło bitów losowych — fizyczne źródła wykazują tendencję do korelowania kolejnych prób, co zakłóca niezależność.

WYDZIAŁ FIZYKI I INFORMATYKI STOSOWANEJ
Uniwersytet Łódzki

Generowanie ciągów losowych

- Idealne źródło bitów losowych generuje je tak, aby każdy bit zachowywał się jak niezależna próba losowa.
- Idealne źródło bitów losowych jest symetryczne — jednakowe prawdopodobieństwo 0 i 1 w każdym kroku.
- Każdy ciąg *n* bitów wygenerowanych przez idealne źródło bitów losowych jest jednakowo prawdopodobny.
- Nie jest znane żadne fizyczne idealne źródło bitów losowych — fizyczne źródła wykazują tendencję do korelowania kolejnych prób, co zakłóca niezależność.
- Źródła bitów pseudolosowych („nieprzewydywalnych”) z teoretycznego punktu widzenia nie spełniają kryteriów losowości.