Náhodnosť

IB110

Alternatívne spôsoby počítania

Motivácia

existencia veľkej triedy prakticky neriešiteľných (*ale rozhodnuteľných*) problémov, ktoré potrebujeme prakticky riešiť!

Idea

relaxovať požiadavky, ktoré kladieme na výpočty

- náhodnostné algoritmy
- aproximatívne algoritmy

pomôže to ???

náhodnostný protokol pre večerajúcich filozofov

Porovnávanie reťazcov

Na počítačoch A a B sú uložené databázy x a y; nech x a y sú binárne reťazce dĺžky n. Úlohou je rozhodnúť, či x a y sú zhodné. Zaujíma nás, koľko bitov si musia počítače A a B vymeniť, aby dokázali vyriešiť problém rovnosti.

Dá sa dokázať, že neexistuje deterministický komunikačný protokol, ktorý by riešil problém rovnosti a pritom si A a B vymenili nanajvýš $n - 1$ bitov. T.j. protokol, v ktorom A pošle celý reťazec x počítaču B je optimálny.

Porovnávanie reťazcov

Randomizovaný protokol pre problém rovnosti

Vstup $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_n$

Krok 1 A vyberie náhodne prvočíslo p z intervalu $[2, n^2]$.

Krok 2 A vypočíta číslo $s = x \mod p$ a pošle čísla s, p počítaču B.

Krok 3 B vypočíta číslo $q = y \mod p$.
Ak $q \neq s$, tak B vráti odpoveď $x \neq y$.
Ak $q = s$, tak B vráti odpoveď $x = y$.

počet bitov, ktoré si počítače pošlú je $2 \cdot \lceil \log_2 n^2 \rceil \leq 4 \cdot \lceil \log_2 n \rceil$
pravdepodobnosť, že protokol vráti nesprávnu odpoveď je $\leq \frac{\ln n^2}{n}$

Ak $n = 10^{16}$, tak zložitosť deterministického protokolu je 10^{16}, zatiaľ čo zložitosť randomizovaného protokolu je 256.
Pravdepodobnosť, že randomizovaný protokol vráti nesprávnu odopoveď je $\leq 0.36892 \cdot 10^{-14}$.

Randomizovaný Quicksort

Rand-Quicksort(A)

Vstup zoznam prvkov A

Krok 1 ak A má jeden prvok, je utriedený
ak A má viac prvkov, tak náhodne vyber prvok x z A

Krok 2 vytvor zoznam $A_<$ obsahujúci prvky z A menšie než x
vytvor zoznam $A_>$ obsahujúci prvky z A väčšie než x

Krok 3 výstup je *Rand-Quicksort*($A_<$), x, *Rand-Quicksort*($A_>$)

očakávaná zložitosť algoritmu je $\mathcal{O}(N \log N)$

Typy náhodnostných algoritmov

Monte Carlo s ohraničenou pravdepodobnosťou je odpoveď nesprávna
príklad: randomizovaný protokol pre problém rovnosti

Las Vegas odpoveď je vždy správna;
cieľ: očakávaná zložitosť Las Vegas algoritmu pre problém je lepšia než zložitosť (deterministického) algorimtu
príklad: randomizovaný Quicksort

Náhodnostné zložitostné triedy

Pravdepodobnostný Turingov stroj

pracuje ako nedeterministický TS s tým rozdielom, že nedeterministický výber kroku výpočtu interpretujeme ako náhodnostnú voľbu

Trieda RP

obsahuje rozhodovacie problémy, pre ktoré existuje polynomiálne časovo ohraničený pravdepodobnostný Turingov stroj s vlastnosťou:
ak odpoveďou pre vstup X je "Nie", tak s pravdepodobnosťou 1 stroj dá správnu odpoveď
ak odpoveďou je "Áno", tak stroj s pravdepodobnosťou $\geq 1/2$ dá *yes*.

$$P \subseteq RP \subseteq NP$$

náhodnostné algoritmy nemôžu efektívne riešiť problémy mimo NP; problémy z NP ale dokážu (často) riešiť s väčšou efektivitou