Rozhodnuteľnosť a praktická riešiteľnosť

IB110

Praktická použiteľnosť algoritmov

Je každý algoritmus prakticky použiteľný?

$N = 1\ 000\ 000$

vyhľadávanie v utriedenom zozname $\mathcal{O}(\log N) \ldots 20$

vyhľadávanie v zozname $\mathcal{O}(N) \ldots 1\ 000\ 000$

triedenie zoznamu $\mathcal{O}(N \log N) \ldots 20\ 000\ 000$

Hanojské veže $\mathcal{O}(2^N) \ldots$ milión presunov za minútu $\Rightarrow$ 500 000 rokov

Je riešením výkonnejší hardware a väčšia trpezlivosť?

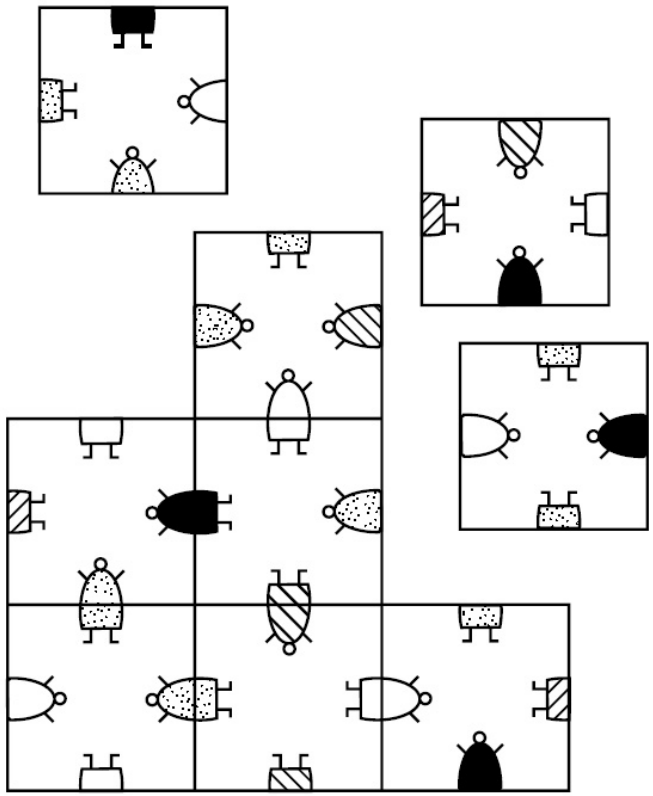
Monkey Puzzle Problem

http://www.keithharingart.com/

MP hlavolam

Vstup N kariet ($N = M^2$)

Otázka Dajú sa karty usporiadať do štvorca $M \times M$ tak, aby sa susediace hrany zhodovali?



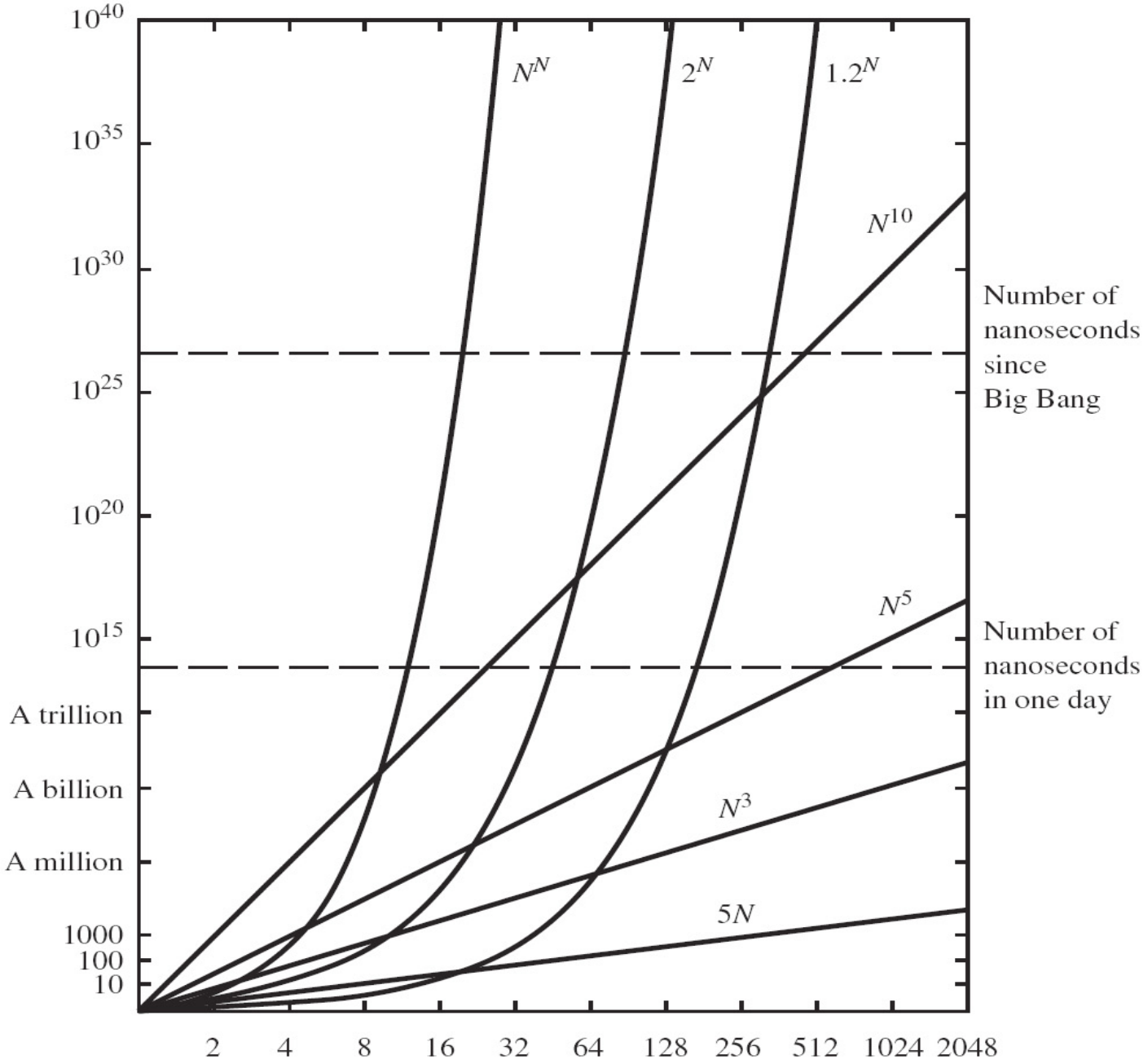
Karty majú fixnú orientáciu (nemôžeme ich otáčať)
Zaujíma nás len existencia riešenia (nepotrebujeme poznať usporiadanie vyhovujúce podmienkam)

MP hlavolam - riešenie

- je daný konečný počet kariet
- každú kartu môžeme umiestniťna konečný počet pozícií
- môžeme vyskúšať všetky možnosti
- $N = 25 \times 25$, počet možností $25 \times 24 \cdots \times 3 \times 2 \times 1$
- 10^9 možností za sekundu $\Rightarrow$ 490 miliónov rokov

Hranice praktickej použiteľnosti

	N / Function	20	60	100	300	1000
Polynomial	$5N$	100	300	500	1500	5000
	$N \times \log_2 N$	86	354	665	2469	9966
	N^2	400	3600	10,000	90,000	1 million (7 digits)
	N^3	8000	216,000	1 million (7 digits)	27 million (8 digits)	1 billion (10 digits)
Exponential	2^N	1,048,576	a 19-digit number	a 31-digit number	a 91-digit number	a 302-digit number
	$N!$	a 19-digit number	an 82-digit number	a 161-digit number	a 623-digit number	unimaginably large
	N^N	a 27-digit number	a 107-digit number	a 201-digit number	a 744-digit number	unimaginably large


10^{40}
10^{35}
10^{30}
10^{25}
10^{20}
10^{15}
A trillion
A billion
A million
1000
100
10
N^N
2^N
1.2^N
N^{10}
N^5
N^3
$5N$
Number of nanoseconds since Big Bang
Number of nanoseconds in one day
2
4
8
16
32
64
128
256
512
1024
2048

Hranice praktickej použiteľnosti

	Function \ N	20	40	60	100	300
Polynomial	N^2	1/2500 millisecond	1/625 millisecond	1/278 millisecond	1/100 millisecond	1/11 millisecond
Polynomial	N^5	1/300 second	1/10 second	78/100 second	10 seconds	40.5 minutes
Exponential	2^N	1/1000 second	18.3 minutes	36.5 years	400 billion centuries	a 72-digit number of centuries
Exponential	N^N	3.3 billion years	a 46-digit number of centuries	an 89-digit number of centuries	a 182-digit number of centuries	a 725-digit number of centuries

hranica: polynomiálna zložitosť

prakticky riešiteľné vs prakticky neriešiteľné problémy

Prakticky neriešiteľné problémy

- použiť výkonnejší počítač?
  pre algoritmus zložitosti 2^N: ak dnes vyriešime inštancie veľkosti max. C, tak 1000 krát rýchlejším počítačom vyriešime inštancie veľkosti max. $C + 9.97$.
- zintenzívniť výzkum a nájsť efektívnejší algoritmus?
- dokázať, že neexistuje efektívnejší algoritmus?
  Millenium Prize Problem, 1 000 000
  `http://www.claymath.org/millennium/`
- je otázka dôležitá?
  existujú aj iné (dôležité) problémy podobného charakteru?

NP-úplné problémy

NP-úplné problémy

problémy, pre ktoré majú lineárny dolný odhad zložitosti a exponenciálny horný odhad zložitosti

nepoznáme lepší než exponenciálny algoritmus a zároveň nevieme dokázať, či existuje alebo neexistuje asymptoticky efektívnejší algoritmus

NP-úplné problémy - príklady

dvojrozmerné pokrytie daných je N štvoruholníkov; je možné pokryť nimi štvorcovú plochu?

Hamiltonovská cesta daný je neorientovaný graf; existuje v grafe cesta, ktorá navštívi každý vrchol práve jeden krát?

obchodný cestujúci daný je neorientovaný graf s ohodnotenými hranami a konštanta K; existuje v grafe Hamiltonovská cesta dĺžky nanajvýš K?

problém rozvrhu daných je M miestností a N prednášok, každá prednáška má určený začiatok a koniec; je možné rozdeliť prednášky do daných miestností?

splniteľnosť daná je logická formula; existuje priradenie hodôt jej premenným, pre ktoré je formula splnená?

. . . a tisíce ďalších

NP-úplné problémy - spoločná charakteristika

- rozhodovacie problémy (*odpoveď je "Áno" alebo "Nie"*)
- existencia čiastočných riešení
- hľadanie riešenia problému pomocou zpaätného vyhľadávania (*backtracking*); exponenciálny algoritmus

- je extrémne ťažké rozhodnúť, či reišením vstupnej inštancie je "Áno" aelbo "Nie"
- ak riešením inštancie je "Áno", tak je veľmi jednoduché dokázať to — pomocou tzv. certifikátu
- obvykle je certifikát krátky reťazec (lineárny voči N) a jeho overenie je možné v polynomiálnom čase

Alternatívna charakterizácia NP-úplných problémov

- predpokladajme, že máme magickú micu, ktorú budeme používať pri zpätnom vyhľadávaní (*backtrackovaní*) riešenia inštancie
- vždy, keď sa máme rozhodnúť, ako rozšíriť čiastočné riešenie, rozhodnutie urobíme tak, že si hodíme mincou
- "magično" — minca vždy vyberie možnosť, ktorá vedie k riešeniu "Áno" (samozrejme, len ak existuje)
- pojem nedeterminizmu
- pre NP-úplné problémy máme nedeterministické polynomiálne algoritmy
- NP v názve NP-úplný je skratka pre pre nedeterministický polynomiálny

Pojem úplnosti

buď všetky NP-úplné problémy sú prakticky riešiteľné
alebo žiaden z nich nie je prakticky riešiteľný

- ak pre jeden NP-úplný problém skonštruujeme polynomiálny algoritmus, tak máme polynomiálne algoritmy pre všetky NP-úplné problémy
- ak pre niektorý NP-úplný problém dokážeme neexistenciu polynomiálneho algoritmu, tak polynomiálny algoritmus neexistuje pre žiaden NP-úplný problém

Dôkaz úplnosti

Polynomiálna časová redukcia

Pre dané dva rozhodovacie problémy P_1 a P_2; polynomiálna časová redukcia je algoritmus $\mathcal{A}$ taký, že

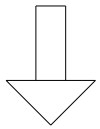
- $\mathcal{A}$ má polynomiálnu časovú zložitosť a
- vstupnú inštanciu X problému P_1 transformuje na vstupnú inštanciu Y problému P_2 takú, že riešením X je "Áno" vtedy a len vtedy, ak riešení Y je tiež "Áno".

Polynomiálna redukcia - príklad

redukcia problému Hamiltonovskej cesty na problém obchodného cestujúceho

Transformácia

graf $G = (V, H)$
(inštancia problému Hamiltonovskej cesty)



graf $\overline{G} = (\overline{V}, \overline{H})$ s ohodnotením $w : \overline{H} \to \mathbb{N}$ a konštanta K, kde $\overline{V} = V$, $\overline{H} = H$, $w(h) = 1$ pre všetky hrany $h \in \overline{H}$ a $K = |V| + 1$
(inštancia problému obchodného cestujúceho)

- transformácia sa dá vypočítať v polynomiálnom čase
- v G existuje Hamiltonovská cesta vtedy a len vtedy ak riešením inštancie $(\overline{G}, w, K)$ problému obchodného cestujúceho je "Áno"

Polynomiálna redukcia a existencia algoritmu

Predpokladajme, že máme polynomiálny algoritmus $\mathcal{O}$ pre problém obchodného cestujúceho.
Ukážeme, ako za tohto predpokladu skonštruujeme polynomiálny algoritmus $\mathcal{H}$ pre problém Hamiltonovskej cesty.

Algoritmus $\mathcal{H}$

1. vstup G transformuj na $(\overline{G}, w, K)$
2. aplikuj $\mathcal{O}$ na $(\overline{G}, w, K)$
3. ak riešením $(\overline{G}, w, K)$ je "Áno", tak vráť odpoveď "Áno"
4. v opačnom prípade vráť odpoveď "Nie"

Polynomiálna reduckia a úplnosť

Fakt

Všetky NP-úplné problémy sú vzájomne polynomiálne redukovateľné

- ak chceme o probléme R dokázať, že je NP-úplný, nemusíme ukazovať redukciu medzi R a vetkými ostatnými NP-úplnými problémami
- stačí ukázať polynomiálnu redukciu problému R na jeden konkrétny NP-úplný problém
- redukcia je tranzitívna

Cookova veta

Problém splniteľnosti je NP-úplný.

Polynomiálna redukcia - príklad 2

Redukcia 3-zafarbenia mapy na problém splniteľnosti

P=NP? problém

P je trieda prakticky riešiteľných problémov (tj. problémov, pre ktoré existujú polynomiálne algoritmy)

Fakt

$$P \subseteq NP$$

Otvorený problém

$$P = NP \ ?$$

Dôsledky riešenia problému.

Čiastočné riešenie NP-úplných problémov

- pseudopolynomiálne algoritmy
- aproximatívne algoritmy
- náhodnostné algoritmy
- kvantové algoritmy
- genetické algoritmy

Ešte ťažšie problémy

- NP-úplné problémy môžu mať polynomiálne algoritmy
- existujú problémy, ktoré dokázateľne nemôžu mať efektívnejšie než exponenciálne (prípadne ešte zložitejšie) algoritmy

Príklady: pravdivosť formule v bohatšej logike

Priestorová zložitosť

- časová zložitosť $\geq$ priestorová zložitosť
- polynomiálny priestor (PSPACE)
- PSPACE-úplné problémy

Teória výpočtovej zložitosti

- pojem zložitostnej triedy
- vzťahy medzi zložitostnými triedami
- LOGTIME $\subseteq$ LOGSPACE$\subseteq$ PTIME $\subseteq$ PSPACE $\subseteq$ EXPTIME $\subseteq$ EXPSPACE . . .
- analogicky pre nedeterminizmus
- kľúčová otázka presného vzťahu

$$P \subseteq NP \subseteq PSPACE$$