Základy složitosti a vyčíslitelnosti

NTIN090

Petr Kučera

2022/23 (12. přednáška)

Zjemnělá složitost

Složitost uvnitř P

- NP-úplnost je příliš hrubá pro studium složitosti problémů uvnitř třídy P
- Rozdíl mezi $O(n)$ a $O(n^5)$
- Někdy je i kvadratický čas příliš
  - velká data (big data)
- Zajímají nás dolní odhady složitosti problémů řešitelných v polynomiálním čase
- Netriviální nepodmíněné dolní odhady je velmi těžké dokázat
  - je-li to vůbec možné

Zjemnělá složitost

Podmíněné dolní odhady

- Dolní odhad složitosti je založen na široce přijímané hypotéze
- Používáme zjemnělou převoditelnost

Výpočetní model

RAM s logaritmickou cenou operací

Klíčové hypotézy

k-splnitelnost

k-KNF klauzule obsahují nejvýš k literálů

k-SAT

Instance: Formule φ v k-KNF na n proměnných.

Otázka: Je φ splnitelná?

- Lze vyřešit v čase $O(2^n n^k)$

Silná hypotéza o exponenciálním čase

Pro každé $\delta > 0$ existuje $k \geq 3$, pro něž platí, že k-SAT nelze vyřešit algoritmem se složitostí $O(2^{(1-\delta)n})$.

- Strong Exponential Time Hypothesis (SETH)

Ortogonální vektory

Ortogonální vektory (OV)

Instance: Množiny A a B obsahující po n vektorech z $\{0,1\}^d$.

Otázka: Existují navzájem ortogonální vektory $a \in A$ a $b \in B$ (tj. $a[i] \cdot b[i] = 0$ pro všechna $i = 1, \ldots, d$)?

- Lze vyřešit v čase $O(n^2 d)$ vypočtením skalárních součinů všech dvojic vektorů

Hypotéza o ortogonálních vektorech (OV)

OV nelze vyřešit v čase $O(n^{2-\delta} d^c)$ pro žádné $\delta, c > 0$.

Nejkratší cesty mezi všemi dvojicemi vrcholů

Nejkratší cesty mezi všemi dvojicemi vrcholů (APSP)

Instance: Orientovaný graf G s n vrcholy a kladnými délkami hran.

Cíl: Pro každou dvojici vrcholů určit délku nejkratší cesty, která je spojuje.

- Lze vyřešit v čase $O(n^3)$ Floydovým-Warshallovým algoritmem

Hypotéza o nejkratších cestách mezi všemi dvojicemi vrcholů

APSP nelze vyřešit v čase $O(n^{3-\delta})$ pro žádné $\delta > 0$.

3SUM

3SUM

Instance: Množina X s n celými čísly

Otázka: Platí $a + b + c = 0$ pro nějakou trojici $a, b, c \in X$?

- Lze vyřešit v čase $O(n^2)$

Hypotéza o 3SUM

3SUM nelze vyřešit v čase $O(n^{2-\delta})$ pro žádné $\delta > 0$.

Zjemnělá převoditelnost

Zjemnělá převoditelnost

Pro jednoduchost uvažujeme jen many-one převoditelnost.

Definice

Uvažme rozhodovací problémy A a B a funkce časové složitosti t_A a t_B. Zjemnělým převodem (A, t_A) na (B, t_B) míníme funkci $f : \Sigma^* \to \Sigma^*$ splňující následující vlastnosti:

1. Pro každý řetězec $x \in \Sigma^*$ platí $x \in A \iff f(x) \in B$
2. Pro každé $\varepsilon > 0$ existuje $\delta > 0$, pro něž platí

$$t_B(|f(x)|)^{1-\varepsilon} = O(t_A(|x|)^{1-\delta})$$

3. $f(x)$ je vyčíslitelná v čase $O(t_A(|x|)^{1-\gamma})$ pro nějaké $\gamma > 0$

Použití zjemnělé převoditelnosti

- Mějme zjemnělý převod z (A, t_A) do (B, t_B)
- Předpokládejme algoritmus rozhodující B v čase $O(t_B(n)^{1-\varepsilon})$ pro nějaké $\varepsilon > 0$
- Pak otázku, zda $x \in A$, umíme rozhodnout v čase

$$\begin{aligned} & O(t_A(|x|)^{1-\gamma} + t_B(|f(x)|)^{1-\varepsilon}) \\ &= O(t_A(|x|)^{1-\gamma} + t_A(|x|)^{1-\delta}) \\ &= O(t_A(|x|)^{1-\delta'}) \end{aligned}$$

for some $\delta' > 0$

Zlepšení složitosti pro B implikuje zlepšení složitosti pro A.

SETH implikuje OV

SETH implikuje OV

Věta

Silná hypotéza o exponenciálním čase implikuje hypotézu o ortogonálních vektorech.

- Popíšeme zjemnělý převod k-SAT na problém Ortogonálních vektorů

Shoda s regulárním výrazem

Regulární výrazy

- Omezíme se na velmi jednoduché regulární výrazy
- Regulární výraz R reprezentuje množinu řetězců $L(R)$

Definice

Předpokládejme abecedu Σ.

1. Pro každý znak $c \in \Sigma$ je $R = c$ regulární výraz s $L(R) = \{c\}$
2. Jsou-li R_1, R_2 regulární výrazy, pak
   1. $R = R_1|R_2$ je regulární výraz s
   $$L(R) = L(R_1) \cup L(R_2)$$
   2. $R = R_1 \cdot R_2$ je regulární výraz s
   $$L(R) = L(R_1) \cdot L(R_2) = \{uv \mid u \in L(R_1) \wedge v \in L(R_2)\}$$

Shoda podřetězce s regulárním výrazem

Shoda podřetězce s regulárním výrazem

Instance: Regulární výraz R a text $T \in \Sigma^*$.

Otázka: Obsahuje T podřetězec $t \in L(R)$?

- Lze vyřešit v čase $O(nm)$, kde $n = |T|$ a $m = |R|$

Věta

Problém shody podřetězce s regulárním výrazem nelze vyřešit v čase $O((n+m)^{2-\varepsilon})$ pro žádné $\varepsilon > 0$, pokud platí hypotéza o ortogonálních vektorech.

Vyčíslitelnost (NTIN064, doc. Antonín Kučera)

- Základy vyčíslitelnosti
  - Algoritmicky vyčíslitelné funkce, numerace, s-m-n věta
  - Základní vlastnosti rekurzivních a rekurzivně spočetných množin — shrnutí
  - Věty o rekurzi a jejich aplikace
  - Produktivní a kreativní množiny a jejich vlastnosti
  - Efektivně neoddělitelné dvojice množin, Gödelovy věty o neúplnosti
- Relativní vyčíslitelnost
  - Relativní vyčíslitelnost, částečně rekurzivní funkcionály, Turingovská převeditelnost
  - Stupně nerozhodnutelnosti, operace skoku, relativizovaný halting problém
  - Limitní vyčíslitelnost
  - Aritmetická hierarchie, věta o hierarchii
  - Aplikace teorie vyčíslitelnosti

Složitost (NTIN063, doc. Ondřej Čepek)

- Turingovy stroje s orákulem
- Polynomiální hierarchie (definice pomocí orákulí a pomocí alternujicích kvantifikátorů, důkaz ekvivalence)
- Kvantifikované booleovské formule QBF a jejich úplnost pro PSPACE a Σ_i
- Nedeterministická hierarchie
- Log-space převoditelnost, P-úplnost a její důsledky
- Věta Szelepcsenyi-Immermana a $\mathrm{NL} = \mathrm{co\text{-}NL}$
- Neuniformní výpočetní modely — radící funkce, booleovské obvody, třídy NC a $\mathrm{P/poly}$, funkce s maximální velikostí obvodu.
- Pravděpodobnostní algoritmy — třídy RP, $\mathrm{co\text{-}RP}$, ZPP a BPP
- Redukce chyby pro BPP, BPP je v $\mathrm{P/poly}$, BPP je v Σ_2
- NP-úplnost UNIQUE-SAT (pravděpodobnostní redukce)
- PCP věta (bez důkazu) a její využití pro neaproximovatelnost.

Rozhodovací procedury a SAT/SMT řešiče (NAIL094)

Pokud vás zajímá, jak řešit SAT prakticky …