Základy složitosti a vyčíslitelnosti

NTIN090

Jirka Fink

https://ktiml.mff.cuni.cz/~fink/

Katedra teoretické informatiky a matematické logiky
Matematicko-fyzikální fakulta
Univerzita Karlova v Praze

Zimní semestr 2017/18

Poslední změna 20. listopadu 2017

Definice

Jazyk A je *polynomiálně převoditelný* na jazyk B, psáno $A \leq_m^P B$, pokud existuje funkce $f : \Sigma^* \mapsto \Sigma^*$ vyčíslitelná v polynomiálním čase, pro kterou platí

$$(\forall w \in \Sigma^*) \, [w \in A \Longleftrightarrow f(w) \in B] \, .$$

Polynomiální převoditelnost

Definice

Jazyk A je *polynomiálně převoditelný* na jazyk B, psáno $A \leq_m^P B$, pokud existuje funkce $f : \Sigma^* \mapsto \Sigma^*$ vyčíslitelná v polynomiálním čase, pro kterou platí

$$(\forall w \in \Sigma^*)\,[w \in A \iff f(w) \in B]\,.$$

Pozorování

- $\leq_m^P$ je reflexivní a tranzitivní relace (kvaziuspořádání).
- Pokud $A \leq_m^P B$ a $B \in \mathrm{P}$, pak $A \in \mathrm{P}$.
- Pokud $A \leq_m^P B$ a $B \in \mathrm{NP}$, pak $A \in \mathrm{NP}$.

NP-úplnost

Definice

- Jazyk B je NP-těžký, pokud je na něj převoditelný kterýkoli problém $A \in \mathrm{NP}$.
- NP-těžký jazyk B, který navíc patří do NP, zveme NP-úplným.

NP-úplnost

Definice

- Jazyk B je NP-těžký, pokud je na něj převoditelný kterýkoli problém $A \in \mathrm{NP}$.
- NP-těžký jazyk B, který navíc patří do NP, zveme NP-úplným.

Pozorování

- Jestliže pro libovolný NP-úplný problém existuje polynomiální algoritmus, pak $\mathrm{P} = \mathrm{NP}$.
- Jestliže pro problém B existuje NP-úplný problém A polynomiálně převoditelný na B (tj. $A \leq_m^P B$), pak B je NP-těžký.

NP-úplný problém

Problém Kachlíkování (Tiling)

Instance: Množina barev B, přirozené číslo s, čtvercová mřížka rozměrech $s \times s$, v níž jsou vnější hrany krajních buněk obarveny barvami z B, množina typů kachlíků K, každý má tvar čtverce s okraji obarvenými barvami z B.

Otázka: Je možné buňkám S přiřadit typy kachlíků z K (bez otáčení) tak, aby sousední kachlíky měly shodnou barvu na sdílené hraně a aby kachlíky v krajních buňkách měly odpovídající okrajovou barvu?

NP-úplný problém

Problém Kachlíkování (Tiling)

Instance: Množina barev B, přirozené číslo s, čtvercová mřížka rozměrech $s \times s$, v níž jsou vnější hrany krajních buněk obarveny barvami z B, množina typů kachlíků K, každý má tvar čtverce s okraji obarvenými barvami z B.

Otázka: Je možné buňkám S přiřadit typy kachlíků z K (bez otáčení) tak, aby sousední kachlíky měly shodnou barvu na sdílené hraně a aby kachlíky v krajních buňkách měly odpovídající okrajovou barvu?

Věta

Kachlíkování je NP-úplný problém.

NP-úplný problém

Problém Kachlíkování (Tiling)

Instance: Množina barev B, přirozené číslo s, čtvercová mřížka rozměrech $s \times s$, v níž jsou vnější hrany krajních buněk obarveny barvami z B, množina typů kachlíků K, každý má tvar čtverce s okraji obarvenými barvami z B.

Otázka: Je možné buňkám S přiřadit typy kachlíků z K (bez otáčení) tak, aby sousední kachlíky měly shodnou barvu na sdílené hraně a aby kachlíky v krajních buňkách měly odpovídající okrajovou barvu?

Věta

Kachlíkování je NP-úplný problém.

Pozorování

Kachlíkování patří do NP.

NP-těžkost kachlíkování

Každý problém $A \in$ NP je polynomiálně redukovatelný na kachlíkování

- Existuje NTS M přijímající A v polynomiálním čase $p(n)$.

Každý problém $A \in \mathrm{NP}$ je polynomiálně redukovatelný na kachlíkování

- Existuje NTS M přijímající A v polynomiálním čase $p(n)$.
- Pro zjednodušení předpokládejme:
  1. $F = \{q_1\}$, kde $q_1 \neq q_0$ a pro všechna $\delta(q_1, a) = \emptyset$.
  2. Když výpočet M skončí, pak je páska prázdná (přijímací konfigurace je jednoznačná).
  3. Páska je jednostranně nekonečná.

Každý problém $A \in$ NP je polynomiálně redukovatelný na kachlíkování

- Existuje NTS M přijímající A v polynomiálním čase $p(n)$.
- Pro zjednodušení předpokládejme:
  1. $F = \{q_1\}$, kde $q_1 \neq q_0$ a pro všechna $\delta(q_1, a) = \emptyset$.
  2. Když výpočet M skončí, pak je páska prázdná (přijímací konfigurace je jednoznačná).
  3. Páska je jednostranně nekonečná.
- Nechť x je instance A a $s = p(|x|)$.

NP-těžkost kachlíkování

Každý problém $A \in$ NP je polynomiálně redukovatelný na kachlíkování

- Existuje NTS M přijímající A v polynomiálním čase $p(n)$.
- Pro zjednodušení předpokládejme:
  1. $F = \{q_1\}$, kde $q_1 \neq q_0$ a pro všechna $\delta(q_1, a) = \emptyset$.
  2. Když výpočet M skončí, pak je páska prázdná (přijímací konfigurace je jednoznačná).
  3. Páska je jednostranně nekonečná.
- Nechť x je instance A a $s = p(|x|)$.
- Řádky odpovídají konfiguracím M dávající výpočet M:
  - Množina barev je $\Sigma \cup Q \times (\Sigma \cup \{L, R\})$.
  - Horní a dolní strana mřížky je obarvena podle počáteční a příjímají konfigurace.
  - Levá a pravá strana mřížky je obarvena λ.
  - Typy kachlíků odpovídají krokům $M \dots$

NP-těžkost kachlíkování

Každý problém $A \in \mathrm{NP}$ je polynomiálně redukovatelný na kachlíkování

- Existuje NTS M přijímající A v polynomiálním čase $p(n)$.
- Pro zjednodušení předpokládejme:
  1. $F = \{q_1\}$, kde $q_1 \neq q_0$ a pro všechna $\delta(q_1, a) = \emptyset$.
  2. Když výpočet M skončí, pak je páska prázdná (přijímací konfigurace je jednoznačná).
  3. Páska je jednostranně nekonečná.
- Nechť x je instance A a $s = p(|x|)$.
- Řádky odpovídají konfiguracím M dávající výpočet M:
  - Množina barev je $\Sigma \cup Q \times (\Sigma \cup \{L, R\})$.
  - Horní a dolní strana mřížky je obarvena podle počáteční a příjímají konfigurace.
  - Levá a pravá strana mřížky je obarvena λ.
  - Typy kachlíků odpovídají krokům M ...
- Ke každému přípustnému vykachlíkování existuje výpočet M.
  - V posloupnosti barev mezi i-tým a $(i+1)$-ním řádkem existuje právě jedna barva z $Q \times \Sigma$ a ostatních barvy jsou z Q.
  - Posloupnosti barev mezi i-tým a $(i+1)$-ním řádkem a mezi $(i+1)$-ním a $(i+2)$-hým řádkem odpovídají jednomu kroku výpočtu M.

Terminologie

Literál: Proměnná (např. x) nebo její negace (např. $\overline{x}$).

Klauzule: Disjunkce literálů.

Konjunktivně normální forma (KNF): Formule je v KNF, pokud jde o konjunkci klauzulí.

Splnitelnosti (SAT)

Terminologie

Literál: Proměnná (např. x) nebo její negace (např. $\overline{x}$).

Klauzule: Disjunkce literálů.

Konjunktivně normální forma (KNF): Formule je v KNF, pokud jde o konjunkci klauzulí.

Splnitelnost (SAT)

Instance: Formule φ v KNF

Otázka: Existuje ohodnocení proměnných v, pro které je $\varphi(v)$ splněno?

Terminologie

Literál: Proměnná (např. x) nebo její negace (např. $\overline{x}$).

Klauzule: Disjunkce literálů.

Konjunktivně normální forma (KNF): Formule je v KNF, pokud jde o konjunkci klauzulí.

Splnitelnost (SAT)

Instance: Formule φ v KNF

Otázka: Existuje ohodnocení proměnných v, pro které je $\varphi(v)$ splněno?

Cookova-Levinova věta

Splnitelnost je NP-úplný problém.

SAT je NP-těžký problém

1. Máme dány množiny barev B a typů kachlíků K a mřížku $s \times s$.
2. Proměnné jsou $x_{i,j,k}$ pro $i, j = 1, \ldots, s$ a $k = K$.
3. Ohodnocení $x_{i,j,k} = 1$ znamená, že na pozici (i, j) patří kachlík typu $s \times s$.

SAT je NP-těžký problém

1. Máme dány množiny barev B a typů kachlíků K a mřížku $s \times s$.
2. Proměnné jsou $x_{i,j,k}$ pro $i, j = 1, \ldots, s$ a $k = K$.
3. Ohodnocení $x_{i,j,k} = 1$ znamená, že na pozici (i, j) patří kachlík typu $s \times s$.
4. Na každé pozici (i, j) je právě jeden kachlík:
   - $\bigvee_{k \in K} x_{i,j,k}$
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ pro všechny barvy $k \neq k'$.

SAT je NP-těžký problém

1. Máme dány množiny barev B a typů kachlíků K a mřížku $s \times s$.
2. Proměnné jsou $x_{i,j,k}$ pro $i, j = 1, \dots, s$ a $k = K$.
3. Ohodnocení $x_{i,j,k} = 1$ znamená, že na pozici (i, j) patří kachlík typu $s \times s$.
4. Na každé pozici (i, j) je právě jeden kachlík:
   - $\bigvee_{k \in K} x_{i,j,k}$
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ pro všechny barvy $k \neq k'$.
5. Na všech pozicích (i, j) a $(i, j + 1)$ jsou kompatibilní barvy:
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ kdykoliv se pravá hrana kachlíku k na pozici (i, j) neshoduje s levým okrajem kachlíku k' na pozici $(i, j + 1)$.

SAT je NP-těžký problém

1. Máme dány množiny barev B a typů kachlíků K a mřížku $s \times s$.
2. Proměnné jsou $x_{i,j,k}$ pro $i,j = 1,\dots,s$ a $k = K$.
3. Ohodnocení $x_{i,j,k} = 1$ znamená, že na pozici (i,j) patří kachlík typu $s \times s$.
4. Na každé pozici (i,j) je právě jeden kachlík:
   - $\bigvee_{k \in K} x_{i,j,k}$
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ pro všechny barvy $k \neq k'$.
5. Na všech pozicích (i,j) a $(i,j+1)$ jsou kompatibilní barvy:
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ kdykoliv se pravá hrana kachlíku k na pozici (i,j) neshoduje s levým okrajem kachlíku k' na pozici $(i,j+1)$.
6. Barva horního okraje mřížky je kompatibilní s prvním řádkem:
   - $\bigvee_{k \in U_j} x_{i,j,k}$, kde U_j je množina kachlíků mající horní hranu stejnou jako j-tý sloupec horního okraje mřížky.

SAT je NP-těžký problém

1. Máme dány množiny barev B a typů kachlíků K a mřížku $s \times s$.
2. Proměnné jsou $x_{i,j,k}$ pro $i, j = 1, \dots, s$ a $k = K$.
3. Ohodnocení $x_{i,j,k} = 1$ znamená, že na pozici (i, j) patří kachlík typu $s \times s$.
4. Na každé pozici (i, j) je právě jeden kachlík:
   - $\bigvee_{k \in K} x_{i,j,k}$
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ pro všechny barvy $k \neq k'$.
5. Na všech pozicích (i, j) a $(i, j+1)$ jsou kompatibilní barvy:
   - $\overline{x}_{i,j,k} \vee \overline{x}_{i,j,k'}$ kdykoliv se pravá hrana kachlíku k na pozici (i, j) neshoduje s levým okrajem kachlíku k' na pozici $(i, j+1)$.
6. Barva horního okraje mřížky je kompatibilní s prvním řádkem:
   - $\bigvee_{k \in U_j} x_{i,j,k}$, kde U_j je množina kachlíků mající horní hranu stejnou jako j-tý sloupec horního okraje mřížky.
7. Podobně kompatibilita pozic (i, j) a $(i+1, j)$ a všech okrajů mřížky.
8. KNF φ je konjunkce všech uvedených literálů.

Definice

Formule φ je v k-KNF, pokud se skládá z klauzulí, z nichž každá obsahuje právě k literály, kde k je přirozené číslo.

3-Splnitelnost

Definice

Formule φ je v k-KNF, pokud se skládá z klauzulí, z nichž každá obsahuje právě k literály, kde k je přirozené číslo.

Splnitelnost (SAT)

Instance: Formule φ v 3-KNF

Otázka: Existuje ohodnocení proměnných v, pro které je $\varphi(v)$ splněno?

3-Splnitelnost

Definice

Formule φ je v k-KNF, pokud se skládá z klauzulí, z nichž každá obsahuje právě k literály, kde k je přirozené číslo.

Splnitelnost (SAT)

Instance: Formule φ v 3-KNF

Otázka: Existuje ohodnocení proměnných v, pro které je $\varphi(v)$ splněno?

Věta

3-SAT je NP-úplný problém.

3-Splnitelnost

Definice

Formule φ je v k-KNF, pokud se skládá z klauzulí, z nichž každá obsahuje právě k literály, kde k je přirozené číslo.

Splnitelnost (SAT)

Instance: Formule φ v 3-KNF

Otázka: Existuje ohodnocení proměnných v, pro které je $\varphi(v)$ splněno?

Věta

3-SAT je NP-úplný problém.

Poznámka

2-SAT je polynomiálně řešitelný.

Vrcholové pokrytí (Vertex Cover)

Instance: Neorientovaný graf $G = (V, E)$ a přirozené číslo k

Otázka: Existuje množina vrcholů S, která má neprázdný průnik s každou hranou grafu G a která má velikost nejvýš k? *Množina vrcholů S tedy „pokrývá“ všechny hrany.*

Vrcholové pokrytí (Vertex Cover)

Instance: Neorientovaný graf $G = (V, E)$ a přirozené číslo k

Otázka: Existuje množina vrcholů S, která má neprázdný průnik s každou hranou grafu G a která má velikost nejvýš k? *Množina vrcholů S tedy „pokrývá“ všechny hrany.*

Věta

Vrcholové pokrytí je NP-úplný problém.

Vrcholové pokrytí (Vertex Cover)

Instance: Neorientovaný graf $G = (V, E)$ a přirozené číslo k

Otázka: Existuje množina vrcholů S, která má neprázdný průnik s každou hranou grafu G a která má velikost nejvýš k? *Množina vrcholů S tedy „pokrývá“ všechny hrany.*

Věta

Vrcholové pokrytí je NP-úplný problém.

Další NP-úplné problémy

Nezávislá množina: Obsahuje graf alespoň k vrcholů mající nejvýše jeden koncový vrchol každé hrany?

Hranové pokrytí: Obsahuje graf nejvýše k hran pokrývající všechny vrcholy?

Klika: Obsahuje graf úplný podgraf na k vrcholech?

Hamiltonovská kružnice (Hamiltonian cycle)

Instance: Neorientovaný graf $G = (V, E)$.

Otázka: Existuje v grafu G cyklus vedoucí přes všechny vrcholy?

Hamiltonovská kružnice

Hamiltonovská kružnice (Hamiltonian cycle)

Instance: Neorientovaný graf $G = (V, E)$.

Otázka: Existuje v grafu G cyklus vedoucí přes všechny vrcholy?

Obchodní cestující (Travelling salesman problem, TSP)

Instance: Množina měst (vrcholů) C, vzdálenost $d_{i,j} \in \mathbb{N}$ každé dvojice měst i, j vzdálenost a přirozené číslo d.

Otázka: Existuje Hamiltonovská kružnice se součtem vzdáleností nejvýše d?

Hamiltonovská kružnice

Hamiltonovská kružnice (Hamiltonian cycle)

Instance: Neorientovaný graf $G = (V, E)$.

Otázka: Existuje v grafu G cyklus vedoucí přes všechny vrcholy?

Obchodní cestující (Travelling salesman problem, TSP)

Instance: Množina měst (vrcholů) C, vzdálenost $d_{i,j} \in \mathbb{N}$ každé dvojice měst i, j vzdálenost a přirozené číslo d.

Otázka: Existuje Hamiltonovská kružnice se součtem vzdáleností nejvýše d?

Věta (bez důkazu)

Hamiltonovká kružnice i obchodní cestující jsou NP-úplné problémy.

Trojrozměrné párování

Instance: Množina $M \subseteq W \times X \times Y$, kde W, X a Y jsou množiny velikosti q.

Otázka: Má M perfektní párování? Tj. existuje množina velikosti q, která neobsahuje dvojici trojic, jež by se shodovaly v nějaké souřadnici?

Trojrozměrné párování

Trojrozměrné párování

Instance: Množina $M \subseteq W \times X \times Y$, kde W, X a Y jsou množiny velikosti q.

Otázka: Má M perfektní párování? Tj. existuje množina velikosti q, která neobsahuje dvojici trojic, jež by se shodovaly v nějaké souřadnici?

Věta

Trojrozměrné párování je NP-úplný problém.

Subset-sum

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ a cílový součet t.

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = t$?

Loupežníci

Subset-sum

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ a cílový součet t.

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = t$?

Loupežníci (Partition)

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ (váha, cena, velikost).

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = \sum_{a \in A \setminus B} s(a)$?

Loupežníci

Subset-sum

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ a cílový součet t.

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = t$?

Loupežníci (Partition)

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ (váha, cena, velikost).

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = \sum_{a \in A \setminus B} s(a)$?

3-Partition

Instance: Množina předmětů A velikosti $3n$, s každým předmětem $a \in A$ asociovanou váhu $s(a)$.

Otázka: Je možné A rozdělit do n skupin po 3 prvcích tak, že všechny skupiny mají stejnou váhu?

Subset-sum

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ a cílový součet t.

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = t$?

Loupežníci (Partition)

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociované přirozené číslo $s(a)$ (váha, cena, velikost).

Otázka: Existuje $B' \subseteq A$, pro kterou platí, že $\sum_{a \in B} s(a) = \sum_{a \in A \setminus B} s(a)$?

3-Partition

Instance: Množina předmětů A velikosti $3n$, s každým předmětem $a \in A$ asociovanou váhu $s(a)$.

Otázka: Je možné A rozdělit do n skupin po 3 prvcích tak, že všechny skupiny mají stejnou váhu?

Věta

Subset-sum, loupežníci a 3-partition jsou NP-úplné problémy.

Batoh (Knapsack)

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociovaná velikost $s(a) \in \mathbb{N}$ a cena $v(a) \in \mathbb{N}$, velikost batohu $b \in \mathbb{N}$ a limit na cenu $k \in \mathbb{N}$

Otázka: Lze vybrat množinu předmětů $C \subseteq A$ tak, aby platilo

$$\sum_{a \in C} s(a) \leq b \text{ a } \sum_{a \in C} v(a) \geq k?$$

Batoh (Knapsack)

Instance: Množina předmětů A, s každým předmětem $a \in A$ asociovaná velikost $s(a) \in \mathbb{N}$ a cena $v(a) \in \mathbb{N}$, velikost batohu $b \in \mathbb{N}$ a limit na cenu $k \in \mathbb{N}$

Otázka: Lze vybrat množinu předmětů $C \subseteq A$ tak, aby platilo

$$\sum_{a \in C} s(a) \leq b \text{ a } \sum_{a \in C} v(a) \geq k?$$

Věta

Batoh je NP-úplný problém.

Rozvrhování (Scheduling)

Instance: Množina úloh U, s každou úlohou $u \in U$ asociovaná doba zpracování $d(u) \in \mathbb{N}$, počet procesorů m, limit $d \in \mathbb{N}$.

Otázka: Lze úlohy U rozdělit na m procesorů tak, aby byly všechny úlohy zpracované v časovém limitu d?

Rozvrhování (Scheduling)

Instance: Množina úloh U, s každou úlohou $u \in U$ asociovaná doba zpracování $d(u) \in \mathbb{N}$, počet procesorů m, limit $d \in \mathbb{N}$.

Otázka: Lze úlohy U rozdělit na m procesorů tak, aby byly všechny úlohy zpracované v časovém limitu d?

Věta

Rozvrhování je NP-úplný problém.