Problém spektra

Ondřej Ježil

MFF UK

14. března 2020

Historie

- Problém spektra je otevřený problém na pomezí teorie složitosti a logiky.
- Souvisí i s deskriptivní teorií složitosti. „Když je něco těžké popsat, je to těžké i spočítat?“
- Formuloval jej Günter Asser ve svém článku z roku 1955.
- Jedna z nejstarších formulací problému, který se vztahuje k $\mathbf{P} = \mathbf{NP}$.

Logika prvního řádu

- Jde o „dotazovací jazyk“ matematických struktur.

Definice

Ať $\{R_1, \ldots, R_n\}$ jsou symboly (nazýváme je relační symboly), pro každý tento symbol R máme kladné celé číslo $a(R)$, zvaný arita.
$\{R_1, \ldots, R_n\}$-struktura je $(n+1)$-tice $\mathcal{A} = (A, R_1^{\mathcal{A}}, \ldots, R_n^{\mathcal{A}})$, kde A je neprázdná množina a pro všechny $i \in \{1, \ldots, n\}$, platí $R_i^{\mathcal{A}} \subseteq A^{a(R_i)}$. A nazýváme nosnou množinou struktury $\mathcal{A}$.

- Množina $\{R_1, \ldots, R_m\}$ s očíslováním a se nazývá vokabulář/jazyk, značí se τ.
- Existují i funkční symboly, ale pro náše potřeby je zavádět nebudeme. Jdou nahradit symboly relačními jak bude později ukázáno.
- Příklad: Každý graf je $\{E\}$-struktura pro E binární relační symbol, $G = (V, E^G)$.

Logika prvního řádu

Definice

Ať τ je jazyk, τ-formulí φ myslím slovo, které získám aplikací následujících pravidel.

- $x = y$ *je* τ*-formule pro* x, y *proměnné.*
- $R(x_1, \ldots, x_n)$ *pro* $R \in \tau$, $a(R) = n$ *a* $x_1, \ldots, x_n$ *proměnné.*
- *Pro* $\varphi_1(x_1, \ldots, x_k), \varphi_2(y_1, \ldots, y_l)$ τ*-formule, jsou i*
  - $\neg\varphi$ τ*-formule*
  - $\varphi_1 \wedge \varphi_2$ τ*-formule*
  - $\varphi_1 \vee \varphi_2$ τ*-formule*
  - $(\exists x_1)\varphi(x_2, \ldots, x_k)$ τ*-formule*
  - $(\forall x_1)\varphi(x_2, \ldots, x_k)$ τ*-formule.*

Pokud navíc jsou všechny promenné ve φ *kvantifikované, nazýváme jí* τ*-sentencí.*

Platnost formule ve struktuře, modely

Definice

Ať φ je τ-sentence a $\mathcal{A}$ je τ-struktura, potom lze definovat platnost φ v $\mathcal{A}$ rekurzí na složitosti formule. Pokud sentence φ v $\mathcal{A}$ platí značíme to

$$\mathcal{A} \models \varphi. \tag{1}$$

Definice

Model τ-sentence nazveme každou τ-strukturu takovou, že $\mathcal{A} \models \varphi$.

Příklady

- Ať $\tau = \{A, M, Z, O\}$. Kde A, M mají aritu 3, a Z, O mají aritu 1.
- Ať φ_{fld} je konjunkce všech axiomů těles, kde $M(a, b, c)$ chápeme jako $a \cdot b = c$, $A(a, b, c)$ jako $a + b = c$, $Z(a)$ jako $a = 0$ a $O(a)$ jako $a = 1$.
- Potom modely φ_{fld} jsou přesně tělesa, která mají místo operací $\cdot, +$ jejich tabulky M a A.
- Podobně můžeme postupovat pro monoidy, grupy, okruhy, obory integrity, vektorové prostory a moduly (zde je třeba být trochu opatrný).
- Jako modely sentencí prvního řádu můžeme mít třeba právě k-obarvitelné grafy, které mají binarání relaci hrany a unární relace pro každou barvu, úplné grafy, atd. . (**Zajímavost!** (Ne)souvislé grafy v logice prvního řádu „axiomatizovat“ nelze.)

Spektra

Definice

Ať φ je τ-sentence. Spektrem φ rozumíme množinu velikostí nosných množin všech jejích konečných modelů. Značíme

$$Spec(\varphi) := \{|A|; \mathcal{A} \models \varphi, |A| < \aleph_0\}. \tag{2}$$

- Lze nahlédnout, že Spec(φ_{fld}) jsou právě mocniny prvočísel.
- Další spektra mohou být sudá čísla (axiom relace ekvivalence s bloky velikosti 2), lichá (to stejné ale jeden blok velikosti 1), prvočísla (to už není tak jednoduché).
- Skoro každá množina co člověk jednoduše popíše spektrum bude.

Definice

Množinu všech spekter značíme SPEC.

Spektra - základní poznatky

Není těžké dokázat následující lemma.

Lemma

Ať $A, B \in SPEC$, potom

$$A \cup B \in SPEC \tag{3}$$

$$A \cap B \in SPEC \tag{4}$$

$$A \cdot B \in SPEC \text{ (násobení po prvcích).} \tag{5}$$

Dokonce platí, že pro $f : \mathbb{N} \to \mathbb{N}$ funkci, pro jejíž výpočet existuje polynomiální algoritmus, a pro $A \in \mathrm{SPEC}$:

$$\{f(a); a \in A\} \in \mathrm{SPEC}. \tag{6}$$

To už je těžší dokázat.

Problém spektra

- Jsou spektra uzavřená na doplňek? **Neví se!**
- Modely negace formule mohou nabývat stejné velikosti jako modely původní formule. Např. $\mathrm{Spec}(\neg\varphi_{\mathsf{fld}}) = \mathbb{N}$, nalézt na každém počtu prvků strukturu, která není tělesem není těžké.
- Jistě vždy platí $\mathrm{Spec}(\neg\varphi) \supseteq \mathbb{N} \setminus \mathrm{Spec}(\varphi)$.
- Předpokládá se, že to nejde. Pokud by se tato domněnka dokázala $\Longrightarrow$ $\mathbf{P} \neq \mathbf{NP}$. Proč?

Teorie složitosti

- Zkoumá jak složité jsou výpočetní problémy.

Definice

Množina $A \subseteq \mathbb{N}$ se nazývá rozhodovací problém. Algoritmus tento problém umí rozhodnout, pokud pro každé $x \in \mathbb{N}$ umí určit zda-li $x \in A$.

Definice

P *je třída všech rozhodovacích problémů, pro které existuje (deterministický=běžný) algoritmus, bežící v polynomiálním čase, který jej umí rozhodnout.*

- Např $2\mathbb{N} \in \mathbf{P}, 2\mathbb{N}+1 \in \mathbf{P}, \mathbb{P} \in \mathbf{P}$ (toto bylo dokázáno až 2004).

Definice

E *je třída všech rozhodovacích problémů, pro které existuje (deterministický=běžný) algoritmus, běžící v čase $\mathcal{O}(2^{n \cdot c})$, který jej umí rozhodnout.*

Nedeterminismus

Definice

NP *je třída složitosti, obsahující ty rozhodovací problémy, pro které existuje nedetermisitický algoritmus, běžící v polynomiálním čase.*

- Nedeterministický algoritmus je algoritmus jehož „řádky“ mohou být nejednoznačné, např. ”zapiš na pásku 1/zapiš na pásku 0”. Výpočet tohoto algoritmu je definovaný tak, že při nedeterministické instrukci algoritmus udělá operace obě, ale každou v novém paralelním výpočtu. Algoritmus odpoví ANO, pokud alespoň jedna větev výpočtu odpověděla ANO, jinak odpoví NE.
- Není lehké obrátit výsledek výpočtu, když znegujeme výslednou hodnotu, jenom se prohodí ANO/NE na všech větvích, ale to neznamená, že přestane existovat nějaká větev, která odpoví ANO.
- **coNP** je třída všech rozhodovacích problémů, jejichž doplněk je v **NP**.
- Analogicky se definují i třídy **NE**, **coNE**.

Vztahy složitostních tříd

- Znalosti vztahů mezi složitostními třídami (jejich inkluze) jsou dost omezené.
- O vztahu nedeterminismu a determinismu se neví skoro nic!

Věta (Důsledek věty o časové hierarchii)

$$\boldsymbol{P} \subsetneq \boldsymbol{E}$$

- Dále se ví $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{E}$. Ale netuší se, které z těchto nerovností jsou neostré, předpokládá se, že oboje.
- Neví se ani vztah nedeterminismu a conedeterminismu (tedy nedeterministických algoritmů, které naopak odpoví NE, pokud existuje alespoň jedna větev výpočtu s odpovědí NE). Tedy $\mathbf{NP} \stackrel{?}{=} \mathbf{coNP}$, $\mathbf{NE} \stackrel{?}{=} \mathbf{coNE}$.

Faginova věta

Věta (Fagin)

$$SPEC = \mathbf{NE}$$

- Tato věta přímo popisuje vztah spekter sentencí prvního řádu a teorií složitostí.
- Z ní plyne: Spektra nejsou uzavřená na doplněk
  $\implies \mathbf{NE} \neq \mathbf{coNE} \overset{\text{„padding argument“}}{\implies} \mathbf{NP} \neq \mathbf{coNP} \overset{\mathbf{P}=\mathbf{coP}}{\implies} \mathbf{P} \neq \mathbf{NP}$.
- Ve své bakalářské práci předvedu alternativní důkaz této věty.