AD4M33AU
Automatické uvažování

Úvod, historie

Petr Pudlák

Organizační informace

- Tyto slidy jsou pomocný studijní materiál.
- Na přednášce budou uváděny další informace a příklady, které ve slidech nejsou.
- Pro obsah zkoušky je podstatné to, co je řečeno na přednášce.

Získávání znalostí

Neformálně můžeme rozdělit získávání znalostí o objektech (ať už skutečných nebo myšlenkových) na:

- pozorování a
- uvažování.

Pozorování

- Pozorováním lze získat jen omezené znalosti týkající se objektů v našem dosahu.
- Příklad: Pozorováním mohu získat znalost:
  Pes, kterého vidím, má čtyři nohy.
- Ale nemohu pozorováním zjisit platnost tvrzení:
  Všichni psi mají nejvýše čtyři nohy.
  Protože není v mých silách prozkoumat všechny psy na světě.

Co je uvažování?

- Konstruování (neintuitivních) závěrů z daných předpokladů.
- Cílem uvažování je odvodit znalost, kterou nemůžeme (nebo nechceme) získat pozorováním.
- Uvažování je smysluplné (korektní), pokud jím získané závěry jsou pravdivé.

Příklad uvažování

- Předpokládám, že platí:
  - *Všichni muži jsou smrtelní.*
  - *Sokrates je člověk.*
- Zkoumám, zda platí:
  - *Sokrates je smrtelný.*
- Platnost závěru mohu ověřit:
  - Pozorováním či experimentem (nepraktické/amorální).
  - Deduktivní úvahou.

Logika

Matematický obor zkoumající exaktní postupy uvažování.

Logika – syntaxe

- **Syntaxe** logiky je ta část logiky, která se zabývá formální popisem logického jazyka, aniž by mu přiřazovala význam či zkoumala pravdivost.
- Formálně popisuje:
  - Jazyk, ve kterém zapisujeme tvrzení (daná i odvozovaná) tak, aby byl smysl těchto tvrzení zcela jasný.
    - symboly,
    - platné posloupnosti symbolů (formule).
  - Definuje postupy, kterými lze dospět k tvrzení, které považujeme v daném kontextu za pravdivé.

Logika – sémantika

- **Sémantika** je ta část logiky, která se zabývá přiřazováním významu symbolům a dalším konstrukcím jazyka logiky.
- Zabývá se (mimo jiné):
  - Jak přiřazovat symbolům logiky konkrétní objekty a nebo vlastnosti.
  - Jak intepretovat pro dané přiřazení pravdivost formulí.
  - Jakým logickým teoriím (a jak) lze přiřadit význam tak, aby byly interpretace všech daných formulí pravdivé (hledání modelů).

Spojení sémantiky a syntaxe

- Máme dánu (matematickou) strukturu, jejíž vlastnosti zkoumáme.
- Identifikujeme základní prvky struktury a označíme je *symboly* v jazyce logiky [syntaxe]. Tím zároveň přiřadíme symbolům určitý *význam* v této struktuře [sémantika].
- Identifikujeme základní vlastnosti prvků struktury a pomocí jím přiřazeným symbolům tyto vlastnosti popíšeme v jazyce logiky [sémantika].

Spojení sémantiky a syntaxe ...

- ...
- Identifikujeme základní vlastnosti prvků struktury a pomocí jím přiřazeným symbolům tyto vlastnosti popíšeme v jazyce logiky [sémantika].

- Za pomocí čistě syntaktických pravidel pro uvažování odvodíme nové poznatky [syntaxe].
- Tyto poznatky zpětně interpretujeme v původní struktuře [sémantika], čímž získáme o této struktuře nové znalosti.

Korektnost (logického) uvažování

- Uvažování (v logice i jinde) přináší prospěch jen pokud jeho výsledky jsou pravdivá tvrzení.
- Takovému uvažování (takovým deduktivním pravidlům) říkáme *korektní*.
- Korektnost logického systému nahlédneme tak, že ukážeme, že ve všech možných interpretacích odvozují všechny povolené způsoby odvozování z pravdivých tvrzení zase jen pravdivá tvrzení.

Potřebujeme pro uvažování formální logiku?

- Neformální (nebo i nevhodně definované formální postupy uvažování), často vyústí
  - v nekonzistentní systémy, tedy systémy, v nichž lze dokázat nepravdivá tvrzení, nebo také
  - v neúplné systémy, ve kterých nelze dokázat to, co potřebujeme.
- Takové chyby často nejsou na první pohled zřejmé!

Russelův paradox

- Znám také jako paradox holiče.
- Objevený E. Zermelem 1900, ale publikovaný Russelem 1901.
- Pokud použijeme neformální definici množiny:

  Všechny objekty s danou vlastnosti tvoří množinu.

- Problém: Buď $R = \{ S \mid S \notin S \}$.
  Je potom $R \in R$ nebo $R \notin R$?

Ignoramus et ignorabimus (neznáme a nepoznáme)

- Existují tvrzení, jejichž pravdivost nemůžeme rozhodnout logickým uvažováním?
- Na přelomu 19. a 20. století se mnoho matematiků (např. David Hilbert) domnívalo, že každý problém má eventuálně formální řešení.
- Výsledky z 1. poloviny 20. století (Gödel) ale ukázaly, že ne všechna pravdivá tvrzení lze formálně dokázat.

Automatické uvažování

- Jestliže je proces uvažování zformalizován nějakým logickým systémem, nabízí se možnost tento proces automatizovat počítačem.

Lze každé dokazatelné tvrzení dokázat strojově?

- ANO, přinejmenším algoritmem Britského muzea:
- Pomocí odvozovacích pravidel postupně generujeme důkazy všech pravdivých tvrzení.
- Jistě takto jednou najdeme i důkaz tvrzení, které chceme dokázat.

Lze každé dokazatelné tvrzení dokázat strojově?

- Proč „algoritmus Britského muzea“:
- „... protože se to zdá asi tak efektivní jako posadit opice před psací stroje a čekat, až eventuálně vytvoří všechny knihy v Britském muzeu.“ (Newell, Shaw, and Simon)

Lze každé dokazatelné tvrzení *efektivně* dokázat strojově?

- Obecně NE.
- Kdybychom uměli obecně efektivně dokázat jakékoliv pravdivé tvrzení, uměli bychom efektivně algoritmizovat všechny řešitelné úlohy, což nelze.
- (Kromě toho existují tvrzení, která mají už z principu dlouhé dukazy.)

Cíle automatického uvažování

- Hledat algoritmy pro automatické uvažování, které jsou efektivní (v rámci možností).
- Hledat logické systémy, které nám umožní postihnout pro daný účel dostatečně silné vyjadřovací a důkazové možnosti, ale ve kterých se dá efektivně uvažovat.

Rozdělení automatického uvažování

- Automatické dokazování, zkratka ATP (automated theorem proving).
- Hledání modelů (model finding).
- Kontrola modelů.

Automatické dokazování

- Cílem je počítačem z dané množiny předpokladů logicky odvodit platnost daného závěru.
- Výsledkem je:
  - důkaz závěru z předpokladů (nebo jen konstatování, že je tvrzení dokazatelné).
  - Nebo konstatování, že tvrzení je nedokazatelné (pouze někdy!).
  - Nebo není schopen systém rozhodnout v rámci daných omezení (čas, paměť, ...).

Využití ATP

- V matematice – dokazování matematických vět, např.
  - Robbinsův problém – booleovské algebry.
  - Algebraické problémy (kvazigrupy).
  - Verifikace formálně zapsaných důkazů (Mizar Mathematical Library)
- Konstrukce software (rozvíjející se obor).
- Verifikace software (např. systém PVS).
- Verifikace hardware – nejčastější průmyslová aplikace ATP.

Kontrola modelů

- Nezkoumáme obecnou platnost tvrzení, jen v rámci konkrétní struktury.
- Formálně: zkoumáme, zda platí tvrzení v dané interpretaci – v rámci daného přiřazení významu logického jazyka.
- Typicky používáme při verifikaci vlastností systémů s konečně mnoha stavy.

Hledání modelů

- Hledáme jednu konkrétní strukturu a k ní interpretaci daného logického jazyka tak, aby v této interpretaci platila všechna tvrzení z dané množiny.
- Formálně: hledáme model množiny formulí.
- Používáme obvykle pro nalezení protipříkladu, tedy když chceme ukázat, že dané tvrzení není dokazatelné z dané množiny předpokladů.

Interaktivní vs. automatické

- Interaktivní systémy pracují v menších krocích. Operátor systému „napovídá“, jaké taktiky má zkoušet a směruje ho tak k cíli.
- Plně automatické systémy se snaží zcela samostatně vyřešit úlohu.

Dostupné nástroje automatického uvažování

- Pro predikátovou logiku prvního řádu: E, Otter, Prover9, SPASS, Vampire, Waldmeister (rovnicový), aj.
- Pro logiky vyšších řádů: ACL2, Coq, HOL, Isabelle, Nqthm, Agda, aj.
- Knihovna TPTP (www.tptp.org) s problémy zapsanými v predikátové logice prvního řádu. Má interface na webu.

Nároky na operátora

- Znát logický kalkulus, v němž daný systém pracuje.
- Znát výhody a nevýhody daného logického kalkulu a systému.
- Analyzovat úlohu, popsat formálními prostředky, a zvolit přitom popis vhodný pro daný systém a jeho logický kalkulus.
- Zapsat formalizovanou úlohu v jazyce systému.
- Správně aplikovat systém na formalizovanou úlohu. Např. nastavit správně parametry atp.
- Umět interpretovat výstup systému.