Automatsko rezonovanje – beleške sa predavanja
Rezonovanje u logici prvog reda

Milan Banković (po slajdovima Filipa Marića)

*Matematički fakultet,
Univerzitet u Beogradu

Prolećni semestar 2023/24.

Pregled

Unutrašnja struktura iskaza

Izražajnost iskazne logike je ograničena:

- Iskazna logika iskaze smatra elementarnim objektima i ne zalazi u njihovu internu strukturu.
- Poželjno je izgraditi bogatiju logiku koja bi analizirala i unutrašnju strukturu iskaza.

Primer

- *Iskazi Sokrat je čovek. i Aristotel je čovek se smatraju različitim.*
- *Njihova untrašnja struktura je slična: . . . je čovek.*

Odnosi među objektima

Izražavanje svojstava i odnosa između objekata

- Iskazi obično govore o svojstvima objekata i odnosima među objektima.
- U zapisu iskaza, objekti su predstavljeni simbolima konstanti, a svojstva i odnosi relacijskim simbolima.

Primer

- *Sokrat je čovek* — *čovek(Sokrat).*
- *Broj* 3 *je paran* — $paran(3)$.
- *Broj* 3 *je manji od broja* 5 — $manji(3,5)$ *ili* $3 < 5$

Složeni iskazi

Složeni iskazi

Iskaze je moguće kombinovati na isti način kao u iskaznoj logici, upotrebom iskaznih veznika.

Primer

- *Ako je broj 4 paran, onda je broj 4 veći od 2* — $paran(4) \Rightarrow 4 > 2$.
- *Broj 15 je paran ili je deljiv brojem 3* — $paran(15) \vee 3 \mid 15$.

Funkcije

Izražavanje funkcionalnih zavisnosti

- Ponekad je potrebno izražavati funkcionalne zavisnosti, tj. predstaviti objekte koji su jednoznačno određeni na osnovu nekih datih objekata.
- U zapisu iskaza, funkcije se označavaju funkcijskim simbolima.

Primer

- *Sokratova majka je žena. — žena(majka(Sokrat)).*
- *Zbir brojeva 2 i 6 je paran — paran$(2+6)$.*

žena i paran označavaju svojstva, dok su majka i $+$ označavaju funkcije.

Kvantifikacija

Kvantifikacija po objektima

- U nekim slučajevima želimo da kažemo da svi objekti imaju neko svojstvo ili su u nekom odnosu.
- U nekim slučajevima želimo da kažemo da neki objekti imaju neko svojstvo ili su nekom odnosu.
- Kako bi se izricanje ovakvih tvrdnji omogućilo, uvode se promenljive i kvantifikatori:
  - u slučaju da objekata o kojima govorimo ima konačno mnogo, alternativa je da napravimo konjunkciju ili disjunkciju iskaza koji govore o pojedinačnim objektima
  - ipak, takvo izražavanje često nije praktično
  - u slučaju beskonačnih skupova objekata, tako nešto nije ni moguće, pa su nam kvantifikatori neophodni

Kvantifikacija

Primer

- *Svi ljudi su smrtni* — $\forall x. \check{c}ovek(x) \Rightarrow smrtan(x)$.
- *Ne postoji savršen čovek* — $\neg \exists x. \check{c}ovek(x) \wedge savr\check{s}en(x)$.
- *Svi parni brojevi su deljivi sa 2* — $\forall n. paran(n) \Rightarrow 2 \mid n$.
- *Sledbenici nekih parnih brojeva su deljivi sa 3* — $\exists n. paran(n) \wedge 3 \mid (n+1)$.

Kvantifikatori se primenjuju na promenljive koje učestvuju u izrazima ravnopravno sa simbolima konstanti.

Kvantifikacija prvog reda

Kvantifikacija prvog reda

- U okviru logike prvog reda, kvantifikacija se vrši samo po primitivnim objektima — funkcijski i relacijski simboli se ne mogu kvantifikovati. Npr. rečenica da neki objekat a ima sva moguća svojstva ($\forall p.p(a)$) nije rečenica logike prvog reda.
- Logike višeg reda dopuštaju kvantifikaciju funkcijskih (odnosno relacijskih) simbola (tj. pored „objektnih" promenljivih, postoje relacijske i funkcijske promenljive)

Pregled

Jezik (signatura)

Šta čini jezik logike prvog reda?

- U zapisu formula logike prvog reda, pored logičkih simbola, učestvuju:
  - simboli konstanti
  - funkcijski simboli
  - relacijski (predikatski) simboli
- Svakom simbolu je pridružena arnost — broj argumenata na koji se funkcijski ili relacijski simbol primenjuje.
- Simboli konstanti se mogu shvatiti kao funkcijski simboli arnosti 0.
- Atomički iskazi (iskazna slova) se mogu shvatiti kao relacijski simboli arnosti 0.
- Neki binarni funkcijski ili relacijski simboli se obično pišu infiksno (npr. umesto $+(3,2)$, pišemo $3+2$).

Jezik (signatura)

Definicija (Jezik (signatura))

Jezik (ili signatura) $\mathcal{L} = (\Sigma, \Pi, ar)$ čini skup funkcijskih simbola Σ, skup relacijskih simbola Π i funkcija $ar : (\Sigma \cup \Pi) \rightarrow \mathbb{N}$ koja svakom simbolu dodelju arnost.

Sintaksa

Sintaksa iskazne logike

- Sintaksu logike prvog reda definišemo u nekoliko faza:
  - Termovi
  - Atomičke formule
  - Formule
- Intuitivno, termovi označavaju objekte iz nekog domena, dok formule predstavljaju (složene) iskaze nad tim objektima koji mogu biti tačni ili netačni

Termovi

Definicija

Skup termova (jezika $\mathcal{L}$) je najmanji skup koji zadovoljava:

- *Svaka promenljiva je term.*
- *Ako je c simbol konstante (jezika $\mathcal{L}$), onda je c term.*
- *Ako su $t_1, \ldots, t_k$ termovi, i f funkcijski simbol (jezika $\mathcal{L}$) arnosti k, onda je i $f(t_1, \ldots, t_k)$ takođe term.*

Termovi — primeri

Primer

Neka je $\mathcal{L}$ jezik sa konstantnim simbolima a i b, funkcijskim simbolom f arnosti 2 i g arnosti 1.
Neki od termova jezika $\mathcal{L}$ su:

- a, b, x, y
- $f(a,a), f(x,b), g(a)$
- $f(x,g(a)), f(f(a,b),g(x)), \ldots$

Napomena

Obično promenljive označavamo sa $x, y, z, \ldots$, konstante sa $a, b, c, \ldots$, funkcijske simbole (arnosti veće od nula) sa $f, g, h, \ldots$, a predikatske simbole sa $p, q, r, \ldots$

Implementacija u funkcionalnom jeziku

Primer implementacije

```
type FSym = [Char]
type Var = [Char]
data Term =
     VarTerm Var |
     FnTerm FSym [Term]
     deriving (Show, Read, Eq, Ord)

-- pomocna funkcija za konstante
constTerm :: FSym -> Term
constTerm a = FnTerm a []
```

Napomena

Obično se u apstraktnoj sintaksi ne vrši provera ispravnosti terma (arnosti funkcija) već se takva provera vrši prilikom parsiranja (obrade konkretne sintakse).

Atomičke formule

Definicija

Skup atomičkih formula (jezika $\mathcal{L}$) je najmanji skup koji zadovoljava:

- *logičke konstante ($\top$ i $\bot$) su atomičke formule*
- *iskazno slovo (relacijski simbol arnosti 0) je atomička formula*
- *ako je p relacijski simbol jezika $\mathcal{L}$ arnosti k, i $t_1, \dots, t_k$ termovi (jezika $\mathcal{L}$), onda je $p(t_1, \dots, t_k)$ atomička formula*

Napomena

Atomičke formule koje nisu logičke konstante, tj. koje se formiraju pomoću predikatskih simbola, nazivamo atomima prvog reda (ili samo atomima).

Atomičke formule — primeri

Primer

- $0 < 1$, $2 + x \geq 5$, $x = 3$
- $paran(3)$, $4 \mid f(x)$
- $između(A, B, C)$, $podudarno(A, B, A_1, B_1)$

Formule

Definicija

Skup formula je najmanji skup koji zadovoljava:

- *Atomičke formule su formule*
- *Ako je A formula onda je $\neg A$ formula*
- *Ako su A i B formule, onda su i $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$ formule.*
- *Ako je A formula, a x promenljiva onda su i $\forall x.A$ i $\exists x.A$ formule.*
- *Ako je A formula, tada je i (A) formula.*

Prioriteti operatora

Prioriteti operatora

Sledeća lista prikazuje operatore prema opadajućim prioritetima:

- funkcijski operatori u atomima (npr. $\cdot$, $+$, $\ldots$)
- predikatski operatori u atomima (npr. $<$, $\geq$, $=$, $|$, $\ldots$)
- $\neg$
- $\wedge$ (levo asocijativno)
- $\vee$ (levo asocijativno)
- $\Rightarrow$ (desno asocijativno)
- $\Leftrightarrow$ (desno asocijativno)
- $\forall$, $\exists$

Napomena

Prema našem dogovoru, kvantifikatori imaju najniži prioritet, pa se kvantifikator uvek primenjuje na celu formulu koja sledi, osim ako zagradama nije određeno drugačije. U literaturi se često javlja i drugačija konvencija, po kojoj kvantifikatori imaju najveći prioritet.

Prioriteti operatora

Primer

$$\forall x.\ x + y < 3 \land \neg x = 5 \Rightarrow \exists y.\ g(y) = x$$

je ekvivalentno sa:

$$\forall x.\ ((((x + y) < 3) \land (\neg(x = 5))) \Rightarrow (\exists y.\ (g(y) = x)))$$

Primer

Uzastopni kvantifikatori istog tipa se mogu prilikom zapisa sažeti u jedan:

$$\forall xyz.\ p(f(x, y), z)$$

je skraćeni zapis za

$$\forall x.\ \forall y.\ \forall z.\ p(f(x, y), z)$$

Implementacija u funkcionalnom jeziku

Primer implementacije

```
type PSym = [Char]

data Formula =
  TRUE |
  FALSE |
  Atom PSym [Term] |
  Not Formula |
  And Formula Formula |
  Or Formula Formula |
  Imp Formula Formula |
  Iff Formula Formula |
  Forall Var Formula |
  Exists Var Formula
  deriving (Show, Read, Eq, Ord)

-- pomocna funkcija za iskazna slova
propAtom :: PSym -> Formula
propAtom p = Atom p []
```

Slobodna i vezana pojavljivanja promenljivih

Slobodna i vezana pojavljivanja promenljivih

Pojavljivanja promenljive su vezana ako su pod dejstvom nekog kvantifikatora, a slobodna inače. Formalno, imamo sledeću definiciju.

Definicija

- *Svako pojavljivanje promenljive u okviru atomičke formule je slobodno.*
- *Sva slobodna pojavljivanja promenljvih u formuli A su slobodna i u $\neg A$.*
- *Sva slobodna pojavljivanja promenljvih u formulama A i B su slobodna i u $A \wedge B$, $A \vee B$, $A \Rightarrow B$ i $A \Leftrightarrow B$.*
- *Sva slobodna pojavljivanja promenljive različite od x u formuli A su slobodna i u $\forall x.\ A$ i $\exists x.\ A$.*

Sva pojavljivanja promenljive u formuli koja nisu slobodna su vezana. Pritom, za slobodna pojavljivanja promenljive x u formuli A kažemo da su u formuli $\forall x.\ A$ vezana kvantifikatorom $\forall x$ (analogno za $\exists x.\ A$)

Slobodna i vezana pojavljivanja — primer

Primer

- *U formuli* $p(x, y) \Rightarrow (\forall x.\ q(x))$, *prvo pojavljivanje promenljive* x *i pojavljivanje promenljive* y *su slobodna, dok je drugo pojavljivanje promenljive* x *vezano.*
- *U formuli* $\exists x.\ p(x) \wedge (\forall x.\ q(x))$, *oba pojavljivanja promenljive* x *su vezana, pri čemu je pojavljivanje u okviru* $p(x)$ *pod dejstvom univerzalnog, a pojavljivanje u okviru* $q(x)$ *pod dejstvom egzistencijalnog kvantifikatora.*

Slobodne promenljive — implementacija

Primer implementacije izdvajanja slobodnih promenljivih

```
import qualified Data.Set as Set

freeVarsTerm :: Term -> Set.Set Var
freeVarsTerm (VarTerm v) = Set.singleton v
freeVarsTerm (FnTerm f ts) = Set.unions (map freeVarsTerm ts)

freeVars :: Formula -> Set.Set Var
freeVars TRUE = Set.empty
freeVars FALSE = Set.empty
freeVars (Atom p ts) = Set.unions (map freeVarsTerm ts)
freeVars (Not f) = freeVars f
freeVars (And f g) = Set.union (freeVars f) (freeVars g)
freeVars (Or f g) = Set.union (freeVars f) (freeVars g)
freeVars (Imp f g) = Set.union (freeVars f) (freeVars g)
freeVars (Iff f g) = Set.union (freeVars f) (freeVars g)
freeVars (Forall v f) = Set.difference (freeVars f) (Set.singleton v)
freeVars (Exists v f) = Set.difference (freeVars f) (Set.singleton v)
```

Rečenice. Bazne formule

Definicija

- *Formula je rečenica (ili zatvorena formula) akko nema slobodnih promenljivih.*
- *Formula je bazna akko nema promenljivih.*

Primedba

Svaka bazna formula je rečenica, ali obrnuto ne mora da važi.

Interpretacija

Šta označavaju simboli koji se pojavljuju u formuli?

Obično, kada se napiše formula, implicitno se podrazumeva na koji skup objekata se formula odnosi (koje objekte konstante označavaju, šta su domeni promenljivih, koje funkcije i koje relacije su označene relacijskim i funkcijskim simbolima).

Primer

$$\forall x.\ 6|x \Rightarrow \neg paran(x+1)$$

Podrazumeva se da 6 *označava prirodan broj šest,* 1 *označava prirodan broj* 1*, da* $+$ *označava funkciju sabiranja dva prirodna broja, da* $|$ *označava relaciju deljivosti na skupu prirodnih brojeva dok paran označava svojstvo parnosti prirodnih brojeva.*

Domeni promenljivih

Domeni promenljivih

Da li je tvrđenje dato formulom tačno ili ne može zavisiti od domena nad kojim se tvrđenje razmatra.

Primer

- *Formula* $\forall x.\ \exists y. y + 1 = x$ *je tačna ako je domen skup celih brojeva, a netačna ako je domen skup prirodnih brojeva.*
- *Formula* $\forall x\ y.\ x < y \Rightarrow \exists z.\ (x < z \land z < y)$ *je tačna ako je domen skup realnih brojeva a netačna ako je domen skup celih brojeva.*

$\mathcal{L}$-strukture

Definicija

Neka je dat jezik $\mathcal{L}$. $\mathcal{L}$-strukturu $\mathfrak{D}$ čini:

- *Neprazan skup objekata (domen) D*
- *Za svaki funkcijski simbol f arnosti k, njegova interpretacija $f_{\mathfrak{D}} : D^k \to D$ (tj. funkcija sa k argumenata nad D). Specijalno, za svaki simbol konstante c, njegova interpretacija $c_{\mathfrak{D}} \in D$ je fiksirani element domena D*
- *Za svaki relacijski simbol p arnosti k, njegova interpretacija $p_{\mathfrak{D}} \subseteq D^k$ (tj. relacija arnosti k nad D). Specijalno, ako je p iskazno slovo, tada je njegova interpretacija $p_{\mathfrak{D}} \in \{0, 1\}$ (ili $\{true, false\}$) fiksirana istinitosna vrednost*

Napomena

Na dalje ćemo obično pretpostavljati da je jezik $\mathcal{L}$ fiksiran pa ćemo umesto ,,$\mathcal{L}$-struktura" govoriti samo ,,struktura".

Istinitosna vrednost formule

Istinitonosna vrednost formule

- Istinitosna vrednost proizvoljne formule u opštem slučaju zavisi od strukture koju razmatramo, ali i od značenja slobodnih promenljivih koje se u formuli pojavljuju
- Sa druge strane, istinitosna vrednost rečenica (tj. formula koje ne sadrže slobodne promenljive) zavisi samo od strukture (tj. od domena i interpretacije simbola).
- Mi obično razmatramo rečenice, jer smo promenljive i uveli da bismo ih kvantifikovali
- Ipak, da bismo definisali istinitosnu vrednost rečenice, moramo razmatrati istinitosne vrednosti njenih podformula, koje ne moraju biti zatvorene, i to za različite vrednosti njihovih slobodnih promenljivih.
  - npr. vrednost formule $\forall x.\ x > 0$ zavisi od vrednosti formule $x > 0$, pri čemu je potrebno razmatrati sve moguće vrednosti promenljive x
- Zbog toga se, u opštem slučaju, razmatra vrednost formule u datoj strukturi $\mathfrak{D}$ za datu valuaciju promenljivih v.

Vrednost termova

Definicija (Valuacija prvog reda)

Neka je data struktura $\mathfrak{D}$ sa domenom D i prebrojiv skup promenljivih V. Valuacija prvog reda nad V (ili samo valuacija) je funkcija $v : V \to D$.

Definicija (Vrednost terma $\mathfrak{D}_v(t)$)

- *Ako je term t promenljiva x, onda je njegova vrednost vrednost promenljive x u valuaciji v, tj. $\mathfrak{D}_v(t) = v(x)$.*
- *Ako je term t konstantni simbol c, onda je njegova vrednost interpretacija simbola c u strukturi $\mathfrak{D}$, tj. $\mathfrak{D}_v(t) = c_{\mathfrak{D}}$.*
- *Ako je term t oblika $f(t_1, \ldots, t_k)$, onda je njegova vrednost jednaka rezultatu primene funkcije koja je interpretacija simbola f u strukturi $\mathfrak{D}$ na vrednosti termova $t_1, \ldots t_k$,*
  tj. $\mathfrak{D}_v(t) = f_{\mathfrak{D}}(\mathfrak{D}_v(t_1), \ldots, \mathfrak{D}_v(t_k))$.

Tačnost formule

Tačnost formule

Činjenicu da je formula F tačna u strukturi $\mathfrak{D}$ pri valuaciji v označavaćemo sa $(\mathfrak{D}, v) \models F$. Kažemo još i da valuacija v zadovoljava formulu F u strukturi $\mathfrak{D}$, kao i da je par $(\mathfrak{D}, v)$ model formule F.

Tačnost formule

Tačnost formule

- Konstanta $\top$ je tačna u svakoj strukturi i valuaciji $((\mathfrak{D}, v) \models \top)$. Konstanta $\bot$ je netačna u svakoj strukturi i valuaciji $((\mathfrak{D}, v) \not\models \bot)$.
- Atomička formula $p(t_1, \ldots, t_k)$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models p(t_1, \ldots, t_k)$) akko važi $(\mathfrak{D}_v(t_1), \ldots, \mathfrak{D}_v(t_k)) \in p_{\mathfrak{D}}$, gde je $\mathfrak{D}_v(t)$ funkcija vrednosti terma u strukturi $\mathfrak{D}$ pri valuaciji v.
- Formula oblika $\neg F$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko je formula F netačna u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models \neg F$ akko $(\mathfrak{D}, v) \not\models F$).
- Formula oblika $F_1 \wedge F_2$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko su obe formule F_1 i F_2 tačne u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models F_1 \wedge F_2$ akko $(\mathfrak{D}, v) \models F_1$ i $(\mathfrak{D}, v) \models F_2$).

Tačnost formule

Tačnost formule (nastavak)

- Formula oblika $F_1 \vee F_2$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko je bar jedna od formula F_1 i F_2 tačna u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models F_1 \vee F_2$ akko $(\mathfrak{D}, v) \models F_1$ ili $(\mathfrak{D}, v) \models F_2$).
- Formula oblika $F_1 \Rightarrow F_2$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko je formula F_1 netačna ili je formula F_2 tačna u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models F_1 \Rightarrow F_2$ akko $(\mathfrak{D}, v) \not\models F_1$ ili $(\mathfrak{D}, v) \models F_2$).
- Formula oblika $F_1 \Leftrightarrow F_2$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko su formule F_1 i F_2 istovremeno tačne ili istovremeno netačne u strukturi $\mathfrak{D}$ pri valuaciji v (tj. $(\mathfrak{D}, v) \models F_1 \Leftrightarrow F_2$ akko $(\mathfrak{D}, v) \models F_1$ i $(\mathfrak{D}, v) \models F_2$ ili $(\mathfrak{D}, v) \not\models F_1$ i $(\mathfrak{D}, v) \not\models F_2$).

Tačnost formule

Tačnost formule (nastavak)

- Formula oblika $\exists x. F$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko postoji valuacija v' dobijena od v samo izmenom vrednosti promenljive x takva da je F tačna u strukturi $\mathfrak{D}$ pri valuaciji v' (tj. $(\mathfrak{D}, v) \models \exists x.\ F$ ako postoji v' tako da $(\mathfrak{D}, v') \models F$). Drugim rečima, $(\mathfrak{D}, v) \models \exists x.\ F$ akko postoji element a iz domena D, tako da $(\mathfrak{D}, v(x \mapsto a)) \models F$.
- Formula oblika $\forall x. F$ je tačna u strukturi $\mathfrak{D}$ pri valuaciji v akko za svaku valuaciju v' dobijenu od v samo izmenom vrednosti promenljive x važi da je F tačna u strukturi $\mathfrak{D}$ pri valuaciji v' (tj. $(\mathfrak{D}, v) \models \forall x.\ F$ ako za svaku v' važi $(\mathfrak{D}, v') \models F$). Drugim rečima $(\mathfrak{D}, v) \models \forall x.\ F$ akko za svaki element a iz domena D, važi $(\mathfrak{D}, v(x \mapsto a)) \models F$.

Problem određivanja tačnosti formule

Određivanje tačnosti za datu valuaciju

- U iskaznoj logici, u trenutku kada je data (iskazna) valuacija, vrednost formule je moguće jednostavno odrediti.
- U logici prvog reda, čak i kada je fiksirana valuacija (prvog reda) i struktura, vrednost formule je komplikovano odrediti:
  - direktno na osnovu definicije je moguće odrediti samo u slučaju konačnog domena D
  - u slučaju beskonačnog domena, striktno po definiciji bi, kod kvantifikacije, bilo potrebno razmatrati vrednost podformule u besknačno mnogo različitih valuacija, što nije izvodljivo u praksi

Tačnost rečenica ne zavisi od valuacije

Stav

Ako se valuacija v i v' poklapaju za sve slobodne promenljive formule F, onda $(\mathfrak{D}, v) \models F$ ako i samo ako $(\mathfrak{D}, v') \models F$.

Dokaz

Indukcijom po strukturi formule F.

- *Ako je F oblika $\top$ ili $\perp$, tvrđenje trivijalno važi.*
- *Ako je F oblika $\neg F'$, onda se skup slobodnih promenljivih za F i F' poklapa. $(\mathfrak{D}, v) \models F$ akko $(\mathfrak{D}, v) \not\models F'$. Po induktivnoj hipotezi, ovo važi akko $(\mathfrak{D}, v') \not\models F'$ akko $(\mathfrak{D}, v') \models F$.*

Tačnost rečenica ne zavisi od valuacije

Dokaz

- *Ako je F oblika $F' \wedge F''$, onda je skup slobodnih promenljivih formule F jednak uniji skupova slobodnih promenljivih formula F' i F'', pa se valuacije v i v' poklapaju i na skupovima slobodnih promenljivih formula F' i F'', pa se na ove formule sme primeniti induktivna hipoteza. $(\mathfrak{D}, v) \models F$ važi akko važi $(\mathfrak{D}, v) \models F'$ i $(\mathfrak{D}, v) \models F''$. Na osnovu i.h. ovo važi akko $(\mathfrak{D}, v') \models F'$ i $(\mathfrak{D}, v') \models F''$, a ovo važi akko $(\mathfrak{D}, v') \models F$.*
- *Ostali iskazni veznici se analogno razmatraju.*

Tačnost rečenica ne zavisi od valuacije

Dokaz

- *Ako je F oblika $\forall x.\ F'$, onda je skup slobodnih promenljivih formule F jednak skupu slobodnih promenljivih formule F', bez promenljive x. $(\mathfrak{D}, v) \models F$ važi akko za svako a iz D, $(\mathfrak{D}, v(x \mapsto a)) \models F'$. Valuacije $v(x \mapsto a)$ i $v'(x \mapsto a)$ se poklapaju na skupu slobodnih promenljivih formule F' te na osnovu i.h. $(\mathfrak{D}, v(x \mapsto a)) \models F'$ važi akko $(\mathfrak{D}, v'(x \mapsto a)) \models F'$, što važi akko $(\mathfrak{D}, v') \models F$.*
- *Slučaj kada je F oblika $\exists x.\ F'$ se razmatra analogno.*

Tačnost rečenica ne zavisi od valuacije

Posledica

Vrednost rečenica ne zavisi od valuacije, već zavisi samo od interpretacije nelogičkih simbola. Preciznije, za svake dve valuacije v *i* v' *i rečenicu* F, $(\mathfrak{D}, v) \models F$ *važi ako i samo ako* $(\mathfrak{D}, v') \models F$.

Definicija

Ako je rečenica F *tačna u strukturi* $\mathfrak{D}$, *tada ćemo pisati* $\mathfrak{D} \models F$. *Kažemo i da struktura* $\mathfrak{D}$ *zadovoljava rečenicu* F, *ili da je* $\mathfrak{D}$ *model rečenice* F.

Semantika — primeri

Primer

Neka je dat jezik $\mathcal{L} = (0, 1, +, \cdot, =)$*. Posmatrajmo domen* $D = \mathbb{N}$*. Neka je struktura* $\mathfrak{D}_{\mathbb{N}}$ *određena na sledeći način:*

1. *Simbol* 0 *se interpretira prirodnim brojem* 0
2. *Simbol* 1 *se interpretira prirodnim brojem* 1
3. *Simbol* $+$ *se interpretira operacijom sabiranja prirodnih brojeva*
4. *Simbol* $\cdot$ *se interpretira operacijom množenja prirodnih brojeva*
5. *Simbol* $=$ *se interpretira jednakošću prirodnih brojeva*

Primer

(nastavak) Sledeće rečenice su tačne u $\mathfrak{D}_{\mathbb{N}}$:

- $\neg(0 = 1)$
- $\forall x.\ \neg(x + 1 = 0)$
- $\forall x\ y.\ x \cdot (y + 1) = x \cdot y + x$
- $\forall x.\ x = 0 \vee \neg(x = 0)$
- $\neg(\forall x.\ x = 0) \Leftrightarrow (\exists x.\ \neg(x = 0))$

Sledeće rečenice su netačne u $\mathfrak{D}_{\mathbb{N}}$:

- $\forall x.\ \exists y.\ y + 1 = x$
- $\forall x.\ \exists y.\ x + y = 0$

Vrednost formula koje nisu rečenice zavisi od valuacije:

- *Formula $x + 1 = 1$ je tačna u valuacijama u kojima je vrednost x prirodan broj nula, a netačna u valuacijama u kojima je vrednost x različita od prirodnog broja nula.*

Semantika — primeri

Primer

Neka je dat jezik $\mathcal{L} = (0, 1, +, \cdot, =)$. *Posmatrajmo domen* $D_{bool} = \{\top, \bot\}$. *Neka je struktura* $\mathfrak{D}_{bool}$ *određena na sledeći način:*

1. *simbol* 0 *se interpretira elementom* $\bot$,
2. *simbol* 1 *se interpretira elementom* $\top$,
3. *simbol* $+$ *se interpretira funkcijom koja elemente* x *i* y *iz* D_{bool} *slika u* $\top$ *akko je* $x \wedge y$ *tačna tj.*

$+$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

4. *simbol* $\cdot$ *se interpretira funkcijom koja elemente* x *i* y *iz* D_{bool} *slika u* $\top$ *akko je* $\neg(x \Leftrightarrow y)$ *tačna, tj.*

$\cdot$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$

5. *simbol* $=$ *se interpretira kao jednakost*

Semantika — primeri

Primer

Sledeće rečenice su tačne u $\mathfrak{D}_{bool}$:

- $\forall x.\ x = 0 \vee x = 1$
- $\forall x.\ \exists y.\ x + y = 0$
- $\forall x.\ x = 0 \vee \neg(x = 0)$
- $\neg(\forall x.\ x = 0) \Leftrightarrow (\exists x.\ \neg(x = 0))$

Sledeće rečenice su netačne u $\mathfrak{D}_{bool}$:

- $0 = 1$
- $\forall x.\ \neg(x + 1 = 0)$

Semantika — primeri

Primer

(nastavak) Da bi $\forall x.\ \exists y.\ x + y = 0$ bila tačna u valuaciji v, potrebno je da:

1. *formula $\exists y.\ x + y = 0$ bude tačna u valuaciji $v(x \mapsto \top)$*
   - *Da bi formula $\exists y. x + y = 0$ bila tačna u valuaciji $v(x \mapsto \top)$, potrebno je da postoji element d iz D takav da je $x + y = 0$ tačna u valuaciji $v(x \mapsto \top, y \mapsto d)$. Zaista, formula $x + y = 0$ je tačna za $d = \bot$, tj. u valuaciji $v' = v(x \mapsto \top, y \mapsto \bot)$. Zaista, vrednost oba terma $x + y$ i 0 u v' je $\bot$, te su oni jednaki.*
2. *formula $\exists y.\ x + y = 0$ bude tačna u valuaciji $v(x \mapsto \bot)$*
   - *Da bi formula $\exists y. x + y = 0$ bila tačna u valuaciji $v(x \mapsto \bot)$, potrebno je da postoji element d iz D takav da je $x + y = 0$ tačna u valuaciji $v(x \mapsto \bot, y \mapsto d)$. Zaista, formula $x + y = 0$ je tačna za, npr. $d = \bot$, tj. u valuaciji $v' = v(x \mapsto \top, y \mapsto \bot)$. Zaista, vrednost oba terma $x + y$ i 0 u v' je $\bot$, te su oni jednaki.*

Semantika — primeri

Primer

Neka je dat jezik $\mathcal{L} = (0, 1, +, \cdot, =)$*. Za* $n \geq 2$*, posmatrajmo domen* $D_{mod_n} = \{0, 1, \ldots n-1\}$*. Neka je struktura* $\mathfrak{D}_{mod_n}$ *određena na sledeći način:*

1. *simbol* 0 *se interpretira brojem* 0*,*
2. *simbol* 1 *se interpretira brojem* 1*,*
3. *simbol* $+$ *se interpretira funkcijom koja sabira brojeve* x *i* y *iz* D *po modulu* n*,*
4. *simbol* $\cdot$ *se interpretira funkcijom koja množi elemente* x *i* y *po modulu* n*,*
5. *simbol* $=$ *se interpretira kao jednakost.*

Semantika — primeri

Primer

(nastavak)

- *Rečenica* $\forall x.\ x = 0 \vee \neg(x = 0)$ *je tačna u svim* $\mathfrak{D}_{mod_n}$.
- *Rečenica* $\neg(\forall x.\ x = 0) \Leftrightarrow (\exists x.\ \neg(x = 0))$ *je tačna u svim* $\mathfrak{D}_{mod_n}$.
- *Rečenica* $\forall x.\ x = 0 \vee x = 1$ *je tačna u* $\mathfrak{D}_{mod_2}$, *a netačna u* $\mathfrak{D}_{mod_3}$.
- *Rečenica* $\forall x.\ \neg(x = 0) \Rightarrow \exists y.\ x \cdot y = 1$ *je tačna u* $\mathfrak{D}_{mod_n}$ *akko je n prost broj.*

Valjanost

Definicija

Formula je valjana ako tačna u svakoj valuaciji, pri svakoj interpretaciji. Da je formula F valjana zapisujemo ovako:

$$\models F$$

Stav

- *Rečenica je valjana akko je tačna pri svakoj interpretaciji.*
- *Formula F koja ima slobodne promenljive $x_1, \dots x_n$ je valjana akko je valjano njeno univerzalno zatvorenje $\forall x_1, \dots, x_n.\ F$.*

Valjane formule — primeri

Primer

- *Rečenica* $\forall x.\ x = 0 \vee \neg(x = 0)$ *je valjana.*
- *Rečenica* $\neg(\forall x.\ x = 0) \Leftrightarrow (\exists x.\ \neg(x = 0))$ *je valjana.*
- $(\forall x.P(x)) \Rightarrow P(a)$ *je valjana, dok formula* $P(x) \Rightarrow P(a)$ *i formula* $\forall x.P(x) \Rightarrow P(a)$ *to nisu.*

Valjane formule — primeri

Primer (Paradoks pijanca)

Rečenica $\exists x.\ p(x) \Rightarrow \forall y. p(y)$ *je valjana.*
Time je tačna i sledeća interpretacija: ,,Postoji čovek, takav da ako on pije, onda svi piju".
Zaista, ako postoji čovek koji ne pije, on je taj traženi jer je u tom slučaju premisa netačna. Sa druge strane, ako svi piju, onda je konkluzija tačna pa bilo ko može biti traženi čovek (pretpostavka o nepraznosti domena je ključna kako bi se izbegao slučaj da nijedan čovek ne postoji).

Zadovoljivost

Definicija

Formula F je zadovoljiva ako postoji struktura $\mathfrak{D}$ i valuacija v takva da je $(\mathfrak{D}, v) \models F$.
Specijalno, rečenica F je zadovoljiva ako postoji struktura $\mathfrak{D}$ takva da je $\mathfrak{D} \models F$.

Stav

- *Formula F je valjana akko je $\neg F$ nezadovoljiva.*
- *Formula F koja sadrži slobodne promenljive $x_1, \ldots, x_n$ je zadovoljiva akko je zadovoljivo njeno egzistencijalno zatvorenje $\exists x_1 \ldots x_n . F$.*

Logičke posledice

Definicija

Formula F je logička posledica skupa formula Γ (što označavamo sa $\Gamma \models F$) akko za svaku interpretaciju $\mathfrak{D}$ i valuaciju v važi da ako $(\mathfrak{D}, v)$ zadovoljava svaku formulu iz Γ, onda zadovoljava i F (tj. ako je svaki model za skup Γ istovremeno i model za formulu F).

Primer

- *Rečenica $smrtan(Sokrat)$ je logička posledica rečenica $čovek(Sokrat)$ i $\forall x.\ čovek(x) \Rightarrow smrtan(x)$.*

Logičke posledice

Stav

Važi $\{G_1, \ldots, G_n\} \models F$ *akko je* $G_1 \wedge \ldots \wedge G_n \Rightarrow F$ *valjana.*

Logička ekvivalentnost

Definicija

Formule F i G su logički ekvivalentne (u oznaci $F \equiv G$) akko za svaku strukturu $\mathfrak{D}$ i valuaciju v važi da je $(\mathfrak{D}, v) \models F$ akko $(\mathfrak{D}, v) \models G$.

Stav

Važi $F \equiv G$ akko $F \models G$ i $G \models F$.

Stav

Važi $F \equiv G$ akko $\models F \Leftrightarrow G$.

Ekvizadovoljivost

Definicija

Formule F i G su ekvizadovoljive (u oznaci $F \equiv_s G$) akko su ili obe zadovoljive ili obe nezadovoljive.

Zamena

Razmatramo različite vrste zamena:

- zamena promenljive termom u termu
- zamena promenljive termom u formuli
- zamena formule formulom

Zamena promenljive termom u termu

Definicija (Zamena promenljive termom u termu)

Term $t[x \to t']$ *je zamena promenljive* x *u termu* t *termom* t' *ako je dobijen tako što se na mesto svakog pojavljivanja promenljive* x *u termu* t *postavi term* t'*:*

- $x[x \to t'] = t'$
- $y[x \to t'] = y$
- $f(t_1, \dots, t_n)[x \to t'] = f(t_1[x \to t'], \dots, t_n[x \to t'])$
  - *specijalno,* $c[x \to t'] = c$

Zamena promenljive termom u termu — implementacija

Implementacija

```
tsubst :: Var -> Term -> Term -> Term
tsubst x tp (VarTerm v) | x == v = tp
                        | otherwise = VarTerm v
tsubst x tp (FnTerm f ts) = FnTerm f (map (tsubst x tp) ts)
```

Zamena promenljive termom u termu — svojstva

Stav

Neka je v' *valuacija dobijena od* v *tako što se promenljivoj* x *dodeljuje vrednost terma* t' *u valuaciji* v*, tj.* $v' = v(x := \mathfrak{D}_v(t'))$*. Onda je*

$$\mathfrak{D}_v(t[x \to t']) = \mathfrak{D}_{v'}(t)$$

Zamena promenljive termom u formuli

Zamena promenljive termom u formuli

Postojanje slobodnih i vezanih promenljivih čini zamenu promenljive termom u okviru formule komplikovanijom operacijom:

- želimo da zamenjujemo samo slobodna pojavljivanja promenljivih
- ne želimo da zamenom kreiramo nova vezana pojavljivanja promenljivih

Primer

- *Zamena promenljive x termom t ne bi trebalo da promeni formulu $\forall x.\ x = x$.*
- *Zamena promenljive x promenljivom y u formuli $\exists\ y.\ y + 1 = x$ je moguća tek nakon preimenovanja vezane promenljive y, tj. vrednost zamene može biti formula $\exists y'.\ y' + 1 = y$. Direktna zamena dovodi do $\exists y.\ y + 1 = y$, što nije ono što se želi.*

Zamena promenljive termom u formuli

Definicija

Zamena promenljive termom u formuli Zamenu promenljive x termom t u formuli F (u oznaci $F[x \to t]$) definišemo na sledeći način:

- $\top[x \to t] = \top, \bot[x \to t] = \bot$
- $p(t_1, \ldots, t_n)[x \to t] = p(t_1[x \to t], \ldots, t_n[x \to t])$
  - *specijalno,* $p[x \to t] = p$*, gde je* p *iskazno slovo*
- $(\neg F)[x \to t] = \neg F[x \to t]$
- $(F \otimes G)[x \to t] = F[x \to t] \otimes G[x \to t]$ $(\otimes \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\})$
- $(Qx.F)[x \to t] = Qx.F$ $(Q \in \{\forall, \exists\})$
- $(Qy.F)[x \to t] = Qy.F[x \to t]$, *, ako* t *ne sadrži* y $(Q \in \{\forall, \exists\})$
- $(Qy.F)[x \to t] = Qy'.F[y \to y'][x \to t]$ *ako* t *sadrži* y $(Q \in \{\forall, \exists\}$*,* y' *se ne pojavljuje ni u* t *ni u* $F)$*.*

Napomena

Transformacija formule $Qy.F$ u $Qy'.F[y \to y']$, gde je $Q \in \{\forall, \exists\}$, a F ne sadrži y', naziva se alfa konverzija (ili preimenovanje vezane promenljive). Važi:

$$Qy.F \equiv Qy'.F[y \to y']$$

što opravdava upotrebu ove operacije gde god je to potrebno.

Zamena promenljive u formuli — implementacija

Implementacija

```
-- (freshVarNotIn t f) vraca novu promenljivu koja se ne javlja ni u t ni u f
freshVarNotIn :: Term -> Formula -> Var

subst :: Var -> Term -> Formula -> Formula
subst x t TRUE = TRUE
subst x t FALSE = FALSE
subst x t (Atom p ts) = Atom p (map (tsubst x t) ts)
subst x t (Not f) = Not (subst x t f)
subst x t (And f g) = And (subst x t f) (subst x t g)
subst x t (Or f g) = Or (subst x t f) (subst x t g)
subst x t (Imp f g) = Imp (subst x t f) (subst x t g)
subst x t (Iff f g) = Iff (subst x t f) (subst x t g)
subst x t (Forall y f) | x == y = Forall y f
                       | notMember y (freeVarsTerm t) = Forall y (subst x t f)
                       | otherwise = let y' = (freshVarNotIn t f) in
                                     Forall y' (subst x t (subst y y' f))
subst x t (Exists y f) | x == y = Exists y f
                       | notMember y (freeVarsTerm t) = Exists y (subst x t f)
                       | otherwise = let y' = (freshVarNotIn t f) in
                                     Exists y' (subst x t (subst y y' f))
```

Zamena promenljive termom u formuli — primeri

Primer

- $(\forall x.\ P(x))[x \rightarrow y] = \forall x.P(x)$ – *ne dešava se ništa*
- $(\forall z.\ P(x,z))[x \rightarrow f(y)] = \forall z.P(f(y),z)$ – α *konverzija nije potrebna u ovom primeru, jer* $f(y)$ *ne sadrži* z
- $(\forall y.\ P(x,y))[x \rightarrow f(y)] = \forall y'.P(f(y),y')$ – α *konverzija jeste neophodna u ovom primeru, jer* $f(y)$ *sadrži* y

Zamena promenljive termom u formuli — svojstva

Stav

Neka je v' valuacija dobijena od v tako što se promenljivoj x dodeljuje vrednost terma t u valuaciji v, tj. $v' = v(x := \mathfrak{D}_v(t))$. Onda je

$$(D, v) \models F[x \to t] \ \mathit{akko}\ (D, v') \models F$$

Uopštena zamena

Definicija

Uopštena zamena $F[x_1 \to t_1, \ldots, x_n \to t_n]$ *je formula koja nastaje od formule* F *istovremenom zamenom promenljivih* $x_1, \ldots, x_n$ *termovima* $t_1, \ldots, t_n$*, respektivno.*

Napomena

Obratiti pažnju na to da se zamena svih promenljivih vrši istovremeno: zamenjuju se samo slobodna pojavljivanja koja postoje u originalnoj formuli, a ne pojavljivanja koja eventualno nastanu zamenom neke druge promenljive

Primer

Ako u formul $p(x,y)$ *izvršimo zamenu* $p(x,y)[x \to f(y), y \to c]$*, dobićemo formulu* $p(f(y),c)$*, a ne formulu* $p(f(c),c)$*, što bismo dobili kada bismo zamenjivali jednu po jednu promenljivu* $p(x,y)[x \to f(y)][y \to c]$*.*

Instance formule

Definicija

Za formulu F' koja se dobija (uopštenom) zamenom termova od formule F kažemo da je instanca formule F.

Napomena

Problem ispitivanja da li je formula F' instanca formule F poznat je i kao problem uparivanja (engl. matching problem). Ovaj problem je odlučiv.

Za vežbu

Pokušajte da osmislite algoritam koji rešava problem uparivanja.

Zamena formule formulom

Zamena formule formulom

Pored zamene promenljive termom u formuli, moguće je definisati i zamenu potformule drugom formulom u okviru date formule. Ova zamena se izvodi na isti način kao u iskaznoj logici.

Primer

Rezultat zamene formule $\neg(P(x) \vee Q(x))$ *formulom* $\neg P(x) \wedge \neg Q(x)$ *u formuli* $\forall x.\ \neg(P(x) \vee Q(x)) \wedge R(x)$ *je formula* $\forall x.\ (\neg P(x) \wedge \neg Q(x)) \wedge R(x)$.

Napomena

U logici prvog reda takođe važi teorema o zameni: Ako je $F_1 \equiv F_2$, tada je $F[F_1 \to F_2] \equiv F$. Ova teorema je osnov svođenja na normalne forme, što sledi u nastavku.

Pregled

Eliminacija konstanti

Eliminacija konstanti u logici prvog reda

Eliminacija konstanti u logici prvog reda vrši se primenom istih zakona kao i u iskaznoj logici. Dodatno, primenjuju se zakoni:

$$\forall x.\top \equiv \top \quad \forall x.\bot \equiv \bot \quad \exists x.\top \equiv \top \quad \exists x.\bot \equiv \bot$$

Opštije, mogu se primenjivati zakoni:

$$\forall x.A \equiv A \quad \exists x.A \equiv A$$

gde je A bilo koja formula koja ne sadrži slobodna pojavljivanja promenljive x.

Negaciona normalna forma

NNF u logici prvog reda

Negaciona normalna forma se definiše na sličan način kao i u iskaznoj logici.

Definicija

Formula prvog reda je u negacionoj normalnoj formi (NNF) akko je izgrađena od literala (prvog reda) korišćenjem isključivo veznika $\wedge$ i $\vee$ i kvantifikatora ili je logička konstanta ($\top$ ili $\bot$).

Svođenje na NNF

Pri svođenju date formule na NNF, pored logičkih zakona nasleđenih iz iskazne logike koriste se i zakoni:

$$\neg \forall x.\ A \equiv \exists x.\ \neg A$$

$$\neg \exists x.\ A \equiv \forall x.\ \neg A$$

Prenex normalna forma

Definicija

Formula je prenex normalnoj formi ako je oblika

$$Q_1\ x_1.\ \ldots\ Q_n\ x_n.\ F,$$

pri čemu su Q_i kvantifikatori $\forall$ ili $\exists$, a formula F ne sadrži kvantifikatore.

Svođenje na prenex normalnu formu

Postupak svođenja na prenex normalnu formu

Formula koja je u NNF se može prevesti u prenex normalnu formu primenama sledećih ekvivalencija:

$$
\begin{array}{rcl@{\qquad\qquad}rcl}
(\forall x.A) \wedge B & \equiv & \forall x.\ A \wedge B & (\exists x.A) \wedge B & \equiv & \exists x.\ A \wedge B \\
(\forall x.A) \vee B & \equiv & \forall x.\ A \vee B & (\exists x.A) \vee B & \equiv & \exists x.\ A \vee B \\
B \wedge (\forall x.A) & \equiv & \forall x.\ B \wedge A & B \wedge (\exists x.A) & \equiv & \exists x.\ B \wedge A \\
B \vee (\forall x.A) & \equiv & \forall x.\ B \vee A & B \vee (\exists x.A) & \equiv & \exists x.\ B \vee A
\end{array}
$$

pri čemu formula B ne sadrži slobodna pojavljivanja promenljive x.

Napomena

Ako se promenljiva x javlja slobodna u B, potrebno je najpre izvršiti njeno preimenovanje (α-konverziju) u formuli $\forall x.\ A$ (odnosno $\exists x.\ A$).

Specijalni slučajevi

Specijalni slučajevi

U nekim slučajevima, moguće je koristiti i naredna pravila koja smanjuju broj kvantifikatora.

$$(\exists x.\ A) \vee (\exists x.\ B) \equiv (\exists x.\ A \vee B)$$
$$(\forall x.\ A) \wedge (\forall x.\ B) \equiv (\forall x.\ A \wedge B)$$

Obratiti pažnju da naredna pravila ne predstavljaju ekvivalencije i ne mogu se koristiti za prevođenje u prenex normalnu formu.

$$(\exists x.\ A) \wedge (\exists x.\ B) \not\equiv (\exists x.\ A \wedge B)$$
$$(\forall x.\ A) \vee (\forall x.\ B) \not\equiv (\forall x.\ A \vee B)$$

Teorema Prenex

Teorema

Za svaku formulu postoji formula koja je u prenex normalnoj formi i koja joj je ekvivalentna.

Skolemizacija

Definicija

Formula je u Skolemovoj normalnoj formi ukoliko je oblika

$$\forall x_1.\ \dots\ \forall x_n.\ F$$

pri čemu formula F ne sadrži kvantifikatore. Formule u Skolemoj normalnoj formi nazivamo i univerzalno kvantifikovane formule. Formulu F nazivamo matricom univerzalno kvantifikovane formule.

Napomena

Postupak svođenja na Skolemovu normalnu formu naziva se skolemizacija.

Postupak skolemizacije

Postupak skolemizacije

Procedura skolemizacije se zasniva na uzastopnoj primeni sledećih transformacija:

- Ako je formula oblika $\exists x.A$, bira se novi simbol konstante c (koji ne pripada jeziku $\mathcal{L}$) i formula se zamenjuje formulom $A[x \to c]$.
- Ako je formula oblika $\forall x_1 \dots \forall x_n.\exists x.\ A$, bira se novi funkcijski simbol f (koji ne pripada jeziku $\mathcal{L}$) i formula se zamenjuje formulom $\forall x_1 \dots \forall x_n.A[x \to f(x_1, \dots, x_n)]$.

Na dobijenu formulu se u oba slučaja rekurzivno primenjuje isti postupak, sve dok se ne dođe do formule koja ne sadrži egzistencijalne kvantifikatore.

Ekvizadovoljivost pri skolemizaciji

Semantička priroda skolemizacije

Postupak skolemizacije čuva ekvizadovoljivost formule.

- na žalost, u opštem slučaju nije moguće ukloniti egzistencijalne kvantifikatore, a pritom zadržati logičku ekvivalentnost
- dakle, ekvizadovoljivost je najviše što možemo postići

Skolemizacija — primeri

Primer

Posmatrajmo formulu $\exists x.\ p(x)$ *jezika* $\mathcal{L} = \{p\}$ *i formulu* $p(c)$*, gde je* c *novi simbol konstante (ne pripada jeziku* $\mathcal{L}$*). Neka je* $\mathcal{L}' = \mathcal{L} \cup \{c\}$.

- *Ukoliko je rečenica* $\exists x.\ p(x)$ *zadovoljiva, postoji* $\mathcal{L}$*-struktura* $\mathfrak{D}$ *takva da* $\mathfrak{D} \vDash \exists x.\ p(x)$*. To znači da u domenu* D *postoji element* $\hat{x}$ *takav važi* $p_{\mathfrak{D}}(\hat{x})$*. Ukoliko posmatramo* $\mathcal{L}'$*-strukturu* $\mathfrak{D}'$ *dobijenu od* $\mathfrak{D}$ *dodatnim interpretiranjem simbola* c *elementom* $\hat{x}$ *(tj.* $c_{\mathfrak{D}'} = \hat{x}$*), važi* $\mathfrak{D}' \vDash p(c)$*, te je i rečenica* $p(c)$ *zadovoljiva.*
- *Ukoliko je* $\mathfrak{D}'$ $\mathcal{L}'$*-struktura takva da važi* $\mathfrak{D}' \vDash p(c)$*, tada važi* $p(c_{\mathfrak{D}'})$*, te važi da* $\mathfrak{D}' \vDash \exists x.\ p(x)$*.*

Skolemizacija — primeri

Primer

Posmatrajmo formulu $\forall x.\ \exists y.\ p(x,y)$ *jezika* $\mathcal{L} = \{p\}$ *i formulu* $\forall x.\ p(x, f(x))$, *gde je* f *novi funkcijski simbol (ne pripada jeziku* $\mathcal{L}$*). Neka je* $\mathcal{L}' = \mathcal{L} \cup \{f\}$.

- *Ukoliko je rečenica* $\forall x.\ \exists y.\ p(x,y)$ *zadovoljiva, postoji* $\mathcal{L}$*-struktura* $\mathfrak{D}$ *takva da za svaki element* $\hat{x} \in D$ *postoji element* $\hat{y} \in D$ *takav važi* $p_{\mathfrak{D}}(\hat{x}, \hat{y})$. *Dakle (pod pretpostavkom aksiome izbora), postoji funkcija* $\hat{f} : D \to D$ *koja elementima* $\hat{x}$ *dodeljuje odgovarajuće* $\hat{y}$. *Ukoliko posmatramo* $\mathcal{L}'$*-strukturu* $\mathfrak{D}'$ *dobijenu od* $\mathfrak{D}$ *dodatnim interpretiranjem simbola* f *funkcijom* $\hat{f}$ *(tj.* $f_{\mathfrak{D}'} = \hat{f}$*), važi* $\mathfrak{D}' \models \forall x. p(x, f(x))$, *te je ova rečenica zadovoljiva.*
- *Ukoliko je* $\mathfrak{D}'$ $\mathcal{L}'$*-struktura takva da važi* $\mathfrak{D}' \models \forall x.\ p(x, f(x))$, *tada za svaki element* $\hat{x} \in D$ *važi* $p(\hat{x}, f_{\mathfrak{D}'}(\hat{x}))$, *te važi da* $\mathfrak{D}' \models \forall x.\ \exists y.\ p(x,y)$.

Teorema o skolemizaciji

Teorema

Formula dobijena skolemizacijom formule F je ekvizadovoljiva formuli F.

Dokaz

Teorema se dokazuje na način sličan opisanom u prethodna dva primera.

Posledica

Za svaku formulu postoji unverzalno kvantifikovana formula koja joj je ekvizadovoljiva.

VAŽNA NAPOMENA

Prethodna posledica na važi za ekvivaljanost.

Eliminacija slobodnih promenljivih

Eliminacija slobodnih promenljivih

Ukoliko univerzalno kvantifikovana formula $\forall x_1 \dots x_n.F$ sadrži slobodne promenljive $y_1, \dots, y_k$, tada je ona ekvizadovoljiva sa njenim egzistencijalnim zatvorenjem $\exists y_1 \dots y_k.\forall x_1 \dots x_n.F$. Skolemizacijom, dobijamo da je polazna formula ekvizadovoljiva sa rečenicom:

$$\forall x_1 \dots x_n.F[y_1 \to c_1, \dots, y_k \to c_k]$$

gde su $c_1, \dots, c_k$ novouvedeni simboli konstanti. Iz ovog razmatranja sledi sledeća teorema.

Teorema

Za svaku formulu postoji univerzalno kvantifikovana rečenica koja joj je ekvizadovoljiva.

Eliminacija univerzalnih kvantifikatora

Eliminacija univerzalnih kvantifikatora

- Da li je moguće ukloniti univerzalne kvantifikatore tako da formula ostane ekvizadovoljiva?
- Odgovor je na žalost negativan.

Primer

Formula $p(x) \wedge \neg p(y)$ *je zadovoljiva, dok formula* $\forall xy.p(x) \wedge \neg p(y)$ *to nije.*

Klauzalna forma

Definicija

- *KNF i DNF formula bez kvantifikatora logike prvog reda se definišu analogno iskaznoj logici.*
- *Formula je u klauzalnoj formi ukoliko je oblika*

$$\forall x_1. \ \dots \ \forall x_n. \ F,$$

pri čemu je F u KNF.

Teorema o klauzalnoj formi

Teorema

Za svaku formulu postoji formula u klauzalnoj formi koja joj je ekvizadovoljiva.

Dokaz

Na formulu se primeni eliminacija konstanti, NNF, prenex, skolemizacija i konverzija matrice u KNF.

Napomena

I u logici prvog reda, direktno svođenje matrice na KNF može dovesti do eksponencijalnog uvećanja formule. Da li imamo nešto poput Cajtinove transformacije, što čuva ekvizadovoljivost a ne uvećava formulu značajno?

Cajtinova transformacija u logici prvog reda?

Primer

Pretpostavimo da imamo formulu $\forall xy.(p(a) \wedge \neg p(b)) \vee (p(x) \wedge \neg p(y))$. *Ako bismo (naivno) Cajtinovu transformaciju primenjivali kao u iskaznoj logici, imali bismo* $(\forall xy.(p(a) \wedge \neg p(b)) \vee s) \wedge (\forall xy.s \Leftrightarrow (p(x) \wedge \neg p(y)))$. *Medjutim, lako se vidi da ovo nije ekvizadovoljivo. Naime, prva formula je zadovoljiva (jer možemo interpretirati p bilo kojim pravim nepraznim podskupom domena, tako da* $\mathfrak{D}(a)$ *bude u tom podskupu, a* $\mathfrak{D}(b)$ *da ne bude). Sa druge strane, druga formula je netačna u bilo kojoj strukturi* $\mathfrak{D}$*: ako bi s bilo tačno u* $\mathfrak{D}$*, tada bi moralo da važi* $\forall xy.p(x) \wedge \neg p(y)$ *što nije tačno ni u jednoj strukturi; ako bi s bilo netačno u* $\mathfrak{D}$*, tada bi moralo da važi* $p(a)$, $\neg p(b)$ *i* $\forall xy.\neg(p(x) \wedge \neg p(y))$*, što opet ne može da važi ni u jednoj strukturi (jer formula* $\neg(p(x) \wedge \neg p(y))$ *nije tačna za* $v(x) = \mathfrak{D}(a)$ *i* $v(y) = \mathfrak{D}(b)$*).*

Preimenovanje formule

Preimenovanje formule

Problem u prethodnom primeru je što smo podformulu $p(x) \wedge \neg p(y)$ zamenjivali iskaznim slovom s (tj. predikatskim simbolom arnosti 0), iako interpretacija ove podformule zavisi od x i y. Umesto toga, trebalo je uvesti novi predikatski simbol s arnosti 2: sada se formula $\forall xy.(p(a) \wedge \neg p(b)) \vee (p(x) \wedge \neg p(y))$ može zameniti ekvizadovoljivom formulom
$(\forall xy.(p(a) \wedge \neg p(b)) \vee s(x,y)) \wedge (\forall xy.s(x,y) \Leftrightarrow (p(x) \wedge \neg p(y)))$. Ova formula je zadovoljiva, zato što se sada s može interpretirati binarnom relacijom nad domenom strukture $\mathfrak{D}$ takvom da su $v(x)$ i $v(y)$ u relaciji akko je $(\mathfrak{D}, v) \models p(x) \wedge \neg p(y)$.

Opisani postupak se ponekad zove i preimenovanje formule (engl. formula renaming) i ekvivalent je Cajtinovoj transformaciji u iskaznoj logici.

Napomena

Preimenovanje formule je potrebno sprovesti odmah nakon eliminacije konstanti, tj. pre NNF transformacije koju je potrebno izbeći (jer takođe može dovesti do eksponencijalnog uvećanja formule). Nakon preimenovanja formule potrebno je sprovesti prenex i skolemizaciju na uobičajen način.

Preimenovanje formule

Primer

Neka je data formula $\forall x.p(x) \Rightarrow (\exists y.q(x,y) \wedge r(x))$*. Kako formula* $q(x,y) \wedge r(x)$ *sadrži slobodne promenljive* x *i* y*, uvodimo predikatski simbol* s_1 *arnosti 2 i dobijamo sledeću ekvizadovoljivu formulu:*

$$(\forall x.p(x) \Rightarrow (\exists y.s_1(x,y))) \wedge (\forall xy.s_1(x,y) \Leftrightarrow q(x,y) \wedge r(x))$$

Dalje, s obzirom da formula $\exists y.s_1(x,y)$ *sadrži slobodnu promenljivu* x*, uvodimo novi predikatski simbol* s_2 *arnosti* 1*, te dobijamo sledeću ekvizadovoljivu formulu:*

$$\begin{array}{l}(\forall x.p(x) \Rightarrow s_2(x)) \wedge \\ (\forall xy.s_1(x,y) \Leftrightarrow q(x,y) \ \wedge r(x)) \wedge \\ (\forall x.s_2(x) \Leftrightarrow (\exists y.s_1(x,y)))\end{array}$$

Najzad, formula $p(x) \Rightarrow s_2(x)$ *sadrži slobodnu promenljivu* x*, pa uvodimo simbol* s_3 *arnosti* 1*:*

$$\begin{array}{l}(\forall x.s_3(x)) \wedge \\ (\forall xy.s_1(x,y) \Leftrightarrow q(x,y) \ \wedge r(x)) \wedge \\ (\forall x.s_2(x) \Leftrightarrow (\exists y.s_1(x,y))) \wedge \\ (\forall x.s_3(x) \Leftrightarrow (p(x) \Rightarrow s_2(x)))\end{array}$$

Preimenovanje formula

Primer

(nastavak) Sada svaku definiciju svedemo na KNF, na uobičajen način:

$$
\begin{aligned}
&(\forall x. s_3(x)) \wedge \\
&(\forall xy. (\neg s_1(x,y) \vee q(x,y)) \wedge (\neg s_1(x,y) \vee r(x)) \\
&\qquad \wedge (\neg q(x,y) \vee \neg r(x) \vee s_1(x,y))) \wedge \\
&(\forall x. (\neg s_2(x) \vee (\exists y. s_1(x,y))) \wedge ((\forall y. \neg s_1(x,y)) \vee s_2(x))) \wedge \\
&(\forall x. (\neg s_3(x) \vee \neg p(x) \vee s_2(x)) \wedge (p(x) \vee s_3(x)) \wedge (\neg s_2(x) \vee s_3(x)))
\end{aligned}
$$

Izvlačenjem kvantifikatora u trećem konjunktu, dobijamo:

$$
\begin{aligned}
&(\forall x. s_3(x)) \wedge \\
&(\forall xy. (\neg s_1(x,y) \vee q(x,y)) \wedge (\neg s_1(x,y) \vee r(x)) \\
&\qquad \wedge (\neg q(x,y) \vee \neg r(x) \vee s_1(x,y))) \wedge \\
&(\forall x. \exists y. \forall y'. (\neg s_2(x) \vee s_1(x,y)) \wedge (\neg s_1(x,y') \vee s_2(x))) \wedge \\
&(\forall x. (\neg s_3(x) \vee \neg p(x) \vee s_2(x)) \wedge (p(x) \vee s_3(x)) \wedge (\neg s_2(x) \vee s_3(x)))
\end{aligned}
$$

Preimenovanje formule

Primer

(nastavak) Sada unverzalni kvantifikatora $\forall x$ *izvlačimo istovremeno iz svih konjunkata:*

$$\begin{array}{l}
\forall x. \\
s_3(x) \wedge \\
(\forall y.(\neg s_1(x,y) \vee q(x,y)) \wedge (\neg s_1(x,y) \vee r(x)) \\
\quad\quad \wedge\ (\neg q(x,y) \vee \neg r(x) \vee s_1(x,y))) \wedge \\
(\exists y.\forall y'.(\neg s_2(x) \vee s_1(x,y)) \wedge (\neg s_1(x,y') \vee s_2(x))) \wedge \\
(\neg s_3(x) \vee \neg p(x) \vee s_2(x)) \wedge (p(x) \vee s_3(x)) \wedge (\neg s_2(x) \vee s_3(x))
\end{array}$$

Na kraju izvlačimo i ostale kvantifikatore (najpre egzistencijalni, zbog jednostavnije skolemizacije):

$$\begin{array}{l}
\forall x.\exists y.\forall y'y''. \\
s_3(x) \wedge \\
(\neg s_1(x,y'') \vee q(x,y'')) \wedge (\neg s_1(x,y'') \vee r(x)) \\
\quad\quad \wedge\ (\neg q(x,y'') \vee \neg r(x) \vee s_1(x,y'')) \wedge \\
(\neg s_2(x) \vee s_1(x,y)) \wedge (\neg s_1(x,y') \vee s_2(x)) \wedge \\
(\neg s_3(x) \vee \neg p(x) \vee s_2(x)) \wedge (p(x) \vee s_3(x)) \wedge (\neg s_2(x) \vee s_3(x))
\end{array}$$

Preimenovanje formule

Primer

(nastavak) Skolemizacijom najzad dobijamo sledeću formulu u klauzalnoj formi, ekvizadovoljivu sa polaznom:

$$
\begin{aligned}
&\forall x y' y''. \\
&s_3(x) \wedge \\
&(\neg s_1(x, y'') \vee q(x, y'')) \wedge (\neg s_1(x, y'') \vee r(x)) \\
&\qquad \wedge (\neg q(x, y'') \vee \neg r(x) \vee s_1(x, y'')) \wedge \\
&(\neg s_2(x) \vee s_1(x, f(x))) \wedge (\neg s_1(x, y') \vee s_2(x)) \wedge \\
&(\neg s_3(x) \vee \neg p(x) \vee s_2(x)) \wedge (p(x) \vee s_3(x)) \wedge (\neg s_2(x) \vee s_3(x))
\end{aligned}
$$

gde je f novi funkcijski simbol arnosti 1.

Pregled

Iskazna zadovoljivost

Definicija

Neka je data formula prvog reda F bez kvantifikatora. Njena iskazna apstrakcija (u oznaci $\hat{F}$) je iskazna formula koja nastaje tako što se atomi prvog reda zamene iskaznim slovima (pri čemu se različiti atomi zamenjuju različitim, a isti atomi istim iskaznim slovom).

Primer

Jedna iskazna apstrakcija formule $p(x) \Rightarrow (p(x) \wedge q(x))$ je iskazna formula $u \Rightarrow (u \wedge v)$, gde je $p(x)$ zamenjeno sa u, a $q(x)$ sa v.

Definicija

Za formulu F bez kvantifikatora kažemo da je iskazno zadovoljiva, ako je njena iskazna apstrakcija zadovoljiva.

Primer

Formula iz prethodnog primera je iskazno zadovoljiva, jer je takva njena iskazna apstrakcija $u \Rightarrow (u \wedge v)$.

Zadovoljivost formule bez kvantifikatora

Stav

Formula bez kvantifikatora je zadovoljiva akko je iskazno zadovoljiva.

Dokaz

Neka je data formula bez kvantifikatora F, i neka je $\hat{F}$ njena iskazna apstrakcija. Pretpostavimo najpre da je F zadovoljiva. Tada postoji struktura $\mathfrak{D}$ i valuacija prvog reda v takva da je $(\mathfrak{D}, v) \models F$. Označimo sa $\hat{A}$ iskazno slovo kojim je apstrahovan atom A formule F u $\hat{F}$. Tada za iskaznu valuaciju I definisanu sa:

$$I(\hat{A}) = 1 \text{ akko } (\mathfrak{D}, v) \models A$$

važi da $I \models \hat{F}$ akko $(\mathfrak{D}, v) \models F$. Ova činjenica se može dokazati indukcijom po složenosti formule F. Otuda i iskazna apstrakcija $\hat{F}$ mora biti zadovoljiva, budući da važi $(\mathfrak{D}, v) \models F$ po pretpostavci.

Zadovoljivost formule bez kvantifikatora

Dokaz

(nastavak) Obrnuto, pretpostavimo da je $\hat{F}$ zadovoljiva. Neka je I iskazna valuacija za koju je $I \vDash \hat{F}$. Konstruišimo strukturu prvog reda $\mathfrak{D}_I^{\mathcal{L}}$ nad jezikom (signaturom) $\mathcal{L}$ formule F na sledeći način. Domen strukture $D^{\mathcal{L}}$ će biti skup svih termova nad $\mathcal{L}$ i skupom promenljivih V. Svaki funkcijski simbol f arnosti n interpretiramo funkcijom $f^{\mathcal{L}}$ takvom da za svaka n terma $t_1, \ldots, t_n$ nad $\mathcal{L}$ važi $f^{\mathcal{L}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$. Svaki predikatski simbol p arnosti n interpretiraćemo relacijom $p_I^{\mathcal{L}} \subseteq (D^{\mathcal{L}})^n$ takvom da za svaka n terma $t_1, \ldots, t_n$ važi $(t_1, \ldots, t_n) \in p_I^{\mathcal{L}}$ akko $I \vDash \widehat{p(t_1, \ldots, t_n)}$. Najzad, uzmimo valuaciju prvog reda $v^{\mathcal{L}}$ takvu da je $v^{\mathcal{L}}(x) = x$ za svaku promenljivu $x \in V$. Za ovako definisan par $(\mathfrak{D}_I^{\mathcal{L}}, v^{\mathcal{L}})$ važe sledeća dva svojstva:

- *svaki term se interpretira samim sobom, tj. ${\mathfrak{D}_I^{\mathcal{L}}}_{v^{\mathcal{L}}}(t) = t$ za svako t nad $\mathcal{L}$ i V*
- *za svaku formulu bez kvantifikatora G važi $(\mathfrak{D}_I^{\mathcal{L}}, v^{\mathcal{L}}) \vDash G$ akko $I \vDash \hat{G}$*

Oba ova svojstva se mogu dokazati indukcijom po složenosti formule. Kako znamo da je $I \vDash \hat{F}$, tada je i $(\mathfrak{D}_I^{\mathcal{L}}, v^{\mathcal{L}}) \vDash F$, pa je i F zadovoljiva.

Zadovoljivost bazne formule

Posledica

Bazna formula je zadovoljiva akko je iskazno zadovoljiva.

Dokaz

Sledi iz prethodne teoreme, s obzirom da bazna formula nema promenljive, pa nema ni kvantifikatore.

Zadovoljivost egzistencijalno kvantifikovane formule

Definicija

Za formulu kažemo da je egzistencijalno kvantifikovana ako je oblika:

$$\exists x_1.\exists x_2.\ldots.\exists x_n.\ F$$

pri čemu formula F ne sadrži kvantifikatore.

Stav

Egzistencijalno kvantifikovana formula $\exists x_1.\exists x_2.\ldots.\exists x_n.\ F$ je zadovoljiva akko je formula F iskazno zadovoljiva.

Dokaz

Formula $\exists x_1.\exists x_2.\ldots.\exists x_n.\ F$ je egzistencijalno zatvorenje formule F, pa su otuda ove dve formule ekvizadovoljive. Na osnovu prethodne teoreme F je zadovoljiva akko je iskazno zadovoljiva, odakle sledi ovaj stav.

Zadovoljivost egzistencijalno kvantifikovane formule

Zadovoljivost egzistencijalno kvantifikovane formule ⇔ SAT

- Iz prethodnog razmatranja sledi da se zadovoljivost baznih formula, formula bez kvantifikatora i egzistencijalno kvantifikovanih formula trivijalno svodi na SAT problem
- Ako bismo proizvoljnu formulu prvog reda mogli svesti na ekvizadovoljivu formulu nekog od ovog oblika, tada bi opšti problem zadovoljivosti prvog reda bio svodljiv na SAT
- Na žalost – tako nešto u opštem slučaju nije moguće!

A šta je sa univerzalno kvantifikovanim formulama?

- Od ranije znamo da se proizvoljna formula prvog reda može svesti na ekvizadovoljivu univerzalno kvantifikovanu formulu
- Kakva svojstva imaju ove formule kada je zadovoljivost u pitanju?

Zadovoljivost univerzalno kvantifikovanih formula

Stav

Ako je univerzalno kvantifikovana formula $\forall x_1 \ldots . \forall x_n . F$ *zadovoljiva, tada je njena matrica* F *iskazno zadovoljiva.*

Dokaz

Ako je ova formula zadovoljiva, tada postoji struktura $\mathfrak{D}$ *takva da za svaku valuaciju* v *važi* $(\mathfrak{D}, v) \models F$*, odakle sledi i da je* F *zadovoljiva. Iz prethodnog razmatranja sledi da je* F *i iskazno zadovoljiva.*

Zadovoljivost univerzalno kvantifikovanih formula

Da li važi i obrnuto?

Naredni primer pokazuje da drugi smer ne važi.

Primer

Formula $P(x) \wedge \neg P(y)$ *je iskazno zadovoljiva u valuaciji u kojoj je* $\widehat{P(x)}$ *tačno, a* $\widehat{P(y)}$ *netačno. Međutim formula* $\forall x.\, \forall y. P(x) \wedge \neg P(y)$ *nije zadovoljiva formula logike prvog reda.*

Posledice

- ako je matrica univerzalno kvantifikovane formule iskazno nezadovoljiva, tada znamo da je i sama formula nezadovoljiva
  - formula $\forall x. P(x) \wedge \neg P(x)$ je očito nezadovoljiva, jer je $P(x) \wedge \neg P(x)$ iskazno nezadovoljiva
- sa druge strane, ako je matrica iskazno zadovoljiva, tada univerzalno kvantifikovana formula može, a ne mora biti zadovoljiva

Pitanje: kako u tom slučaju da znamo odgovor?

(Ne)odlučivost logike prvog reda

Teorema

Problem ispitivanja zadovoljivosti univerzalno kvantifikovane formule prvog reda je neodlučiv.

Dokaz

Dokaz se izvodi svođenjem halting problema (za koji znamo da je neodlučiv) na ovaj problem (Tjuring).

Posledica

Problem ispitivanja zadovoljivosti formule prvog reda u opštem obliku je neodlučiv.

(Ne)odlučivost logike prvog reda

Problem nezadovoljivosti

Problem komplementaran problemu ispitivanja zadovoljivosti je ispitivanje nezadovoljivosti.

Teorema

Problem ispitivanja nezadovoljivosti univerzalno kvantifikovane formule je poluodlučiv.

Dokaz

Dokaz će slediti iz postojanja efektivnih postupaka poluodlučivanja koje ćemo razmotriti kasnije.

Posledica

Problem ispitivanja nezadovoljivosti formule prvog reda u opštem obliku je poluodlučiv.

Dokaz

Sledi iz prethodne teoreme i činjenice da se svaka formula može svesti na ekvizadovoljivu univerzalno kvantifikovanu formulu.

Valjanost

Problem valjanosti

Problem valjanosti formule F je dualan problemu nezadovoljivosti formule $\neg F$ (koji je komplementaran problemu zadovoljivosti formule $\neg F$).

Posledica

Problem valjanosti formula prvog reda u opštem obliku je neodlučiv, ali jeste poluodlučiv.

Napomena

U praksi ćemo valjanost obično dokazivati pobijanjem, tj. dokazivanjem da je negacija date formule nezadovoljiva:

- procedura poluodlučivanja će u konačnom broju koraka pobiti svaku nezadovoljivu formulu
- u slučaju da je formula zadovoljiva, tada procedura poluodlučivanja može raditi beskonačno dugo

Pregled

Metod tabloa

Metod tabloa

- Metod tabloa za iskaznu logiku se može proširiti i na logiku prvog reda
- Pravila za iskazne veznike ostaju ista kao i ranije
- Uvode se nova pravila za tretman kvantifikatora
- Nezadovoljivost se dokazuje konstrukcijom tabloa čije su sve grane zatvorene
- Valjanost se dokazuje tako što se dokaže da je negacija nezadovoljiva

Iskazni tablo – podsetnik

Pravila za iskazne veznike

$$\frac{\neg\neg A}{A}$$

$$\frac{A \wedge B}{\begin{array}{c} A \\ B \end{array}}$$

$$\frac{\neg(A \vee B)}{\begin{array}{c} \neg A \\ \neg B \end{array}}$$

$$\frac{\neg(A \Rightarrow B)}{\begin{array}{c} A \\ \neg B \end{array}}$$

$$\frac{\neg(A \wedge B)}{\neg A \mid \neg B}$$

$$\frac{A \vee B}{A \mid B}$$

$$\frac{A \Rightarrow B}{\neg A \mid B}$$

Pravila za kvantifikatore

Uvodimo dodatna pravila za kvantifikatore:

$$\frac{\forall x.A}{A[x \to t]} \qquad \frac{\exists x.A}{A[x \to a]}$$

$$\frac{\neg\exists x.A}{\neg A[x \to t]} \qquad \frac{\neg\forall x.A}{\neg A[x \to a]}$$

U gornjim pravilima:

- t je bilo koji bazni term
- a je novi simbol konstante
- Leva pravila se mogu primenjivati više puta za istu formulu (ali za različite termove t)
- Desna pravila se za svaku formulu tog tipa primenjuju samo jednom

Metod tabloa

Primer

$$\neg(\exists x.P(x) \Rightarrow (\forall y.P(y)))$$
$$|$$
$$\neg(P(a) \Rightarrow (\forall y.P(y)))$$
$$|$$
$$P(a)$$
$$|$$
$$\neg\forall y.P(y)$$
$$|$$
$$\neg P(b)$$
$$|$$
$$\neg(P(b) \Rightarrow (\forall y.P(y)))$$
$$|$$
$$P(b)$$
$$|$$
$$\neg\forall y.P(y)$$

Metod tabloa

Primer

$$\neg((\exists x.\forall y.P(x,y)) \Rightarrow (\forall y.\exists x.P(x,y)))$$
$$|$$
$$\exists x.\forall y.P(x,y)$$
$$|$$
$$\neg(\forall y.\exists x.P(x,y))$$
$$|$$
$$\forall y.P(a,y)$$
$$|$$
$$\neg(\exists x.P(x,b))$$
$$|$$
$$P(a,b)$$
$$|$$
$$\neg P(a,b)$$

Pregled

Erbranova teorema

O Erbranovoj teoremi

- Erbran (fr. Herbrand) 1930. — tragovi u ranijim radovima Skolema i Gedela
- Erbranova teorema daje jedan od načina da se konstruiše postupak poluodlučivanja, tj. algoritam koji za svaku nezadovoljivu formulu može da dokaže da je nezadovoljiva
- Dualno, ovakav postupak omogućava da se za svaku valjanu formulu dokaže da je valjana
- Erbranova teorema u izvesnom smislu uspostavlja veze između logike prvog reda i iskazne logike.

Zadovoljivost univerzalno kvantifikovanih formula – ponovo

Intuitivni pogled na univerzalno kvantifikovane formule

- Univerzalno kvantifikovane formule se mogu razumeti kao „beskonačne konjunkcije":
  - npr. $\forall x.\ p_1(x, c_1) \vee p_2(f(x), c_2)$ predstavlja konjunkciju

    $$(p_1(\alpha_1, c_1) \vee p_2(f(\alpha_1), c_2)) \wedge (p_1(\alpha_2, c_1) \vee p_2(f(\alpha_2), c_2)) \wedge \dots,$$

    gde α_1, α_2, ... predstavljaju različite elemente domena
  - ključno pitanje je: koji domen razmatrati?

Zadovoljivost univerzalno kvantifikovanih formula – ponovo

Kakve domene moramo razmatrati?

- Erbranova teorema tvrdi da je, umesto proizvoljnih domena, pri razmatranju zadovoljivosti dovoljno posmatrati domene koji se sastoje iz svih baznih termova datog jezika:
  - u prethodnom primeru, domen bi se sastojao iz termova c_1, c_2, $f(c_1)$, $f(c_2)$, $f(f(c_1))$, $f(f(c_2))$, ...
  - sada formula $\forall x.\ p_1(x, c_1) \vee p_2(f(x), c_2)$ intuitivno predstavlja beskonačnu konjunkciju:

$$\begin{array}{rcl}
(p_1(c_1, c_1) \vee p_2(f(c_1), c_2)) & \wedge & \\
(p_1(c_2, c_1) \vee p_2(f(c_2), c_2)) & \wedge & \\
(p_1(f(c_1), c_1) \vee p_2(f(f(c_1)), c_2)) & \wedge & \ldots
\end{array}$$

Erbranov univerzum

Definicija

Skup svih baznih termova jezika $\mathcal{L}$ nazivamo Erbranov univerzum nad $\mathcal{L}$ i označavamo sa $H(\mathcal{L})$.

Kakav može biti ovaj skup?

- Ako jezik $\mathcal{L}$ sadrži samo funkcijske simbole arnosti 0 (konstante), tada je $H(\mathcal{L})$ konačan skup
  - npr. ako $\mathcal{L}$ od funkcijskih simbola sadrži samo konstante c_1 i c_2, tada su to ujedno i jedini bazni termovi nad $\mathcal{L}$
- Ako jezik $\mathcal{L}$ sadrži bar jedan funkcijski simbol arnosti veće od nula, kao i bar jednu konstantu, tada je Erbranov univerzum prebrojivo beskonačan:
  - npr. ako $\mathcal{L}$ sadrži konstantu c i funkcijski f simbol arnosti 1, tada imamo bazne termove c, $f(c)$, $f(f(c))$, $f(f(f(c)))$, $\ldots$
- Ukoliko jezik $\mathcal{L}$ ne sadrži ni jednu konstantu, u njega se, po dogovoru, umeće novi simbol konstante (npr. c) kako Erbranov unverzum ne bi bio prazan:
  - npr. ako jezik sadrži binarne funkcijske simbole $+$ i $\cdot$, a ni jednu konstantu, tada dodajemo konstantu c u jezik. Sada je Erbranov univerzum $\{c, c+c, c\cdot c, c+c+c, c+c\cdot c, c\cdot c+c, c\cdot c\cdot c, \ldots\}$

Erbranov univerzum formule i njene bazne instance

Definicija

Erbranov univerzum formule $H(F)$ je Erbranov univerzum jezika sačinjenog od simbola koji se javljaju u toj formuli.

Bazne instance

- primetimo da ako u formuli F bez kvantifikatora sve njene promenljive zamenimo elementima Erbranovog univerzuma, dobijamo baznu formulu
- ovako dobijene formule nazivamo baznim instancama formule F

Erbranova interpretacija

Definicija

Za strukturu $\mathfrak{D}^H$ nad jezikom $\mathcal{L}$ kažemo da je Erbranova interpretacija, ako važi:

- *domen strukture $\mathfrak{D}^H$ je Erbranov univerzum $H(\mathcal{L})$*
- *svaki simbol konstante se interpretira samim sobom*
- *svaki funkcijski simbol f arnosti n se interpretira funkcijom f^H takvom da važi $f^H(t_1, \dots, t_n) = f(t_1, \dots, t_n)$ za svako $t_1, \dots, t_n \in H(\mathcal{L})$*
- *predikatski simboli se interpretiraju proizvoljnim relacijama odgovarajuće arnosti nad $H(\mathcal{L})$*

Primedba

Za isti jezik $\mathcal{L}$ postoje različite Erbranove interpretacije koje se međusobno razlikuju samo po interpretaciji predikatskih simbola.

Erbranova interpretacija

Stav

Neka je $\mathfrak{D}^H$ proizvoljna Erbranova interpretacija nad jezikom $\mathcal{L}$:

1. *svaki bazni term se interpretira samim sobom, tj.* $\mathfrak{D}^H(t) = t$
2. *Za term t koji sadrži promenljive $x_1, \ldots, x_n$ i proizvoljnu valuaciju prvog reda v važi da je* $\mathfrak{D}^H_v(t) = t[x_1 \to v(x_1), \ldots, x_n \to v(x_n)]$, *gde $v(x_i)$ označava vrednost promenljive x_i u toj valuaciji (ova vrednost je takođe element Erbranovog univerzuma, tj. bazni term)*
3. *Za proizvoljan bazni atom $p(t_1, \ldots, t_k)$ važi da je* $\mathfrak{D}^H \models p(t_1, \ldots, t_k)$ *akko* $(t_1, \ldots, t_n) \in p_{\mathfrak{D}^H}$, *gde je $p_{\mathfrak{D}^H}$ relacija kojom se intepretira p u $\mathfrak{D}^H$*
4. *Za proizvoljan atom $p(t_1, \ldots, t_k)$ koji sadrži promenljive $x_1, \ldots, x_n$ i proizvoljnu valuaciju prvog reda v važi* $(\mathfrak{D}^H, v) \models p(t_1, \ldots, t_k)$ *akko* $\mathfrak{D}^H \models p(t_1, \ldots, t_k)[x_1 \to v(x_1), \ldots, x_n \to v(x_n)]$
5. *za proizvoljnu formulu F bez kvantifikatora koja sadrži promenljive $x_1, \ldots, x_n$ i proizvoljnu valuaciju prvog reda v važi* $(\mathfrak{D}^H, v) \models F$ *akko* $\mathfrak{D}^H \models F[x_1 \to v(x_1), \ldots, x_n \to v(x_n)]$

Erbranova interpretacija

Dokaz

Prva i druga tačka se dokazuju indukcijom po strukturi termova. Za treću tačku imamo niz ekvivalencija: $\mathfrak{D}^H \models p(t_1, \dots, t_k)$ *akko* $(\mathfrak{D}^H(t_1), \dots, \mathfrak{D}^H(t_k)) \in p_{\mathfrak{D}^H}$ *akko* $(t_1, \dots, t_k) \in p_{\mathfrak{D}^H}$. *Za četvrtu tačku imamo niz ekvivalencija:* $(\mathfrak{D}^H, v) \models p(t_1, \dots, t_k)$ *akko* $(\mathfrak{D}^H_v(t_1), \dots, \mathfrak{D}^H_v(t_k)) \in p_{\mathfrak{D}^H}$ *akko* $(t_1[x_1 \to v(x_1), \dots, x_n \to v(x_n)], \dots, t_k[x_1 \to v(x_1), \dots, x_n \to v(x_n)]) \in p_{\mathfrak{D}^H}$ *akko* $(\mathfrak{D}^H(t_1[x_1 \to v(x_1), \dots, x_n \to v(x_n)]), \dots, \mathfrak{D}^H(t_k[x_1 \to v(x_1), \dots, x_n \to v(x_n)])) \in p_{\mathfrak{D}^H}$ *akko* $\mathfrak{D}^H \models p(t_1[x_1 \to v(x_1), \dots, x_n \to v(x_n)], \dots, t_k[x_1 \to v(x_1), \dots, x_n \to v(x_n)])$ *akko* $\mathfrak{D}^H \models p(t_1, \dots, t_k)[x_1 \to v(x_1), \dots, x_n \to v(x_n)]$. *Peta tačka se dokazuje indukcijom po strukturi formule.*

Erbranova interpretacija

Erbranove interpretacije i iskazne valuacije

- na osnovu prethodnog stava (tačka 3), svaka Erbranova interpretacija jednoznačno je određena interpretacijom baznih atoma:
  - ako je Erbranov univerzum konačan, tada će i skup baznih atoma biti konačan, pa će takav biti i skup različitih Erbranovih interpretacija
  - ako je Erbranov univerzum prebrojivo beskonačan, tada će i skup baznih atoma biti prebrojivo beskonačan, pa će skup svih Erbranovih interpretacija biti (neprebrojivo) beskonačan
- ako bazne atome apstrahujemo iskaznim slovima, tada svakoj Erbranovoj interpretaciji odgovara jedna iskazna valuacija nad tako definisanim skupom iskaznih slova

Erbranova teorema

Teorema (Erbran)

Univerzalno kvantifikovana formula je zadovoljiva akko je skup svih baznih instanci njene matrice zadovoljiv. Preciznije, formula $\forall x_1 \ \ldots \ x_n.F$ *je zadovoljiva akko je zadovoljiv skup* $\{F[x_1 \rightarrow t_1, \ldots, x_n \rightarrow t_n] \mid t_1, \ldots, t_n \in H(F)\}$.

Dokaz

Radi pojednostavljivanja zapisa, bazne instance $F[x_1 \rightarrow t_1, \ldots, x_n \rightarrow t_n]$ *ćemo kraće označavati sa* $F[x_i \rightarrow t_i]$. *Ako je* $\forall x_1 \ \ldots \ x_n.F$ *zadovoljiva, tada* F *važi u nekom modelu* $\mathfrak{D}$ *i u svakoj valuaciji* v. *Posmatrajmo proizvoljnu baznu instancu* $F[x_i \rightarrow t_i]$ $(t_i \in H(F))$ *i dokažimo da je ona tačna u strukturi* $\mathfrak{D}$ *(vrednost bazne formule ne zavisi od valuacije). Neka je* v *valuacija dobijena tako što se svakoj promenljivoj* x_i *dodeljuje vrednost terma* t_i *u strukturi* $\mathfrak{D}$. *Tada* $\mathfrak{D} \models F[x_i \rightarrow t_i]$ *akko* $(\mathfrak{D}, v) \models F$, *sto sledi iz stava o zameni (slajd 64). Međutim, kako je* $\mathfrak{D}$ *model za* $\forall x_1 \ \ldots \ x_n.F$, *sledi da važi* $(\mathfrak{D}, v) \models F$, *pa i* $\mathfrak{D} \models F[x_i \rightarrow t_i]$.

Dokaz

Obratno, neka struktura $\mathfrak{D}$ *zadovoljava sve bazne instance formule* F*. Neka je* $\mathfrak{D}^H$ *Erbranova interpretacija nad* $H(F)$ *takva da za svaki bazni atom* A *važi:* $\mathfrak{D}^H \models A$ *akko* $\mathfrak{D} \models A$ *(setimo se da je Erbranova interpretacija potpuno određena interpretacijom baznih atoma). Neka je* v *proizvoljna valuacija prvog reda koja preslikava promenljive u elemente Erbranovog univerzuma* $H(F)$*. Potrebno je pokazati da* $(\mathfrak{D}^H, v) \models F$*. Zaista, ovo je ekvivalentno sa* $\mathfrak{D}^H \models F[x_i \to v(x_i)]$ *(na osnovu prethodnog stava), što je dalje ekvivalentno sa* $\mathfrak{D} \models F[x_i \to v(x_i)]$ *(dokaz ove druge ekvivalencije ide indukcijom po strukturi formule* F*, imajući u vidu pretpostavku da je* $\mathfrak{D}^H \models A$ *akko* $\mathfrak{D} \models A$ *za svaki bazni atom* A*). Tvrđenje odavde sledi jer je* $F[x_i \to v(x_i)]$ *bazna instanca koja je tačna u* $\mathfrak{D}$*.*

Erbranova teorema

Posledica

Svaka zadovoljiva formula prvog reda ima Erbranov model (tj. postoji Erbranova interpretacija u kojoj je ta formula tačna).

Dokaz

Bez ograničenja opštosti možemo posmatrati samo univerzalno kvantifikovane formule. Ako je univerzalno kvantifikovana formula zadovoljiva, tada je skup svih njenih baznih instanci zadovoljiv. Iz dokaza Erbranove teoreme sledi da tada postoji Erbranova interpretacija koja zadovoljava datu formulu.

Skolem-Lovenhajmova teorema

Posledica

Formula logike prvog reda je zadovoljiva akko ima model koji je najviše prebrojiv.

Napomena

Navedena posledica poznata je i kao Skolem-Lovenhajmova teorema ,,na dole''.

Skolem-Lovenhajmova teorema

Moguće je dokazati i sledeću teoremu:

Teorema

Ako formula prvog reda ima model $\mathfrak{D}$ kardinalnosti $\mathcal{K}$, tada ona ima i model $\mathfrak{D}'$ proizvoljne veće kardinalnosti $\mathcal{K}'$.

Dokaz

Neka je D domen modela $\mathfrak{D}$ i $|D| = \mathcal{K}$, tada je dovoljno uzeti skup S disjunktan sa D takav da je $|S \cup D| = \mathcal{K}'$. Sada se može odabrati proizvljan element $a \in D$ i proširiti interpretacija svih funkcijskih i relacijskih simbola tako da se svi elementi iz S tretiraju kao a.

Ova teorema je poznata i kao Skolem-Lovenhajmova teorema „na gore”. Zajedno, ove dve varijante Skolem-Lovenhajmove teoreme mogu se formulisati ovako:

Teorema

Ako je formula prvog reda zadovoljiva, ona ima model bilo koje beskonačne kardinalnosti $\mathcal{K}$.

Skolem-Lovenhajmova teorema

Skolem-Lovenhajmova teorema se može formulisati i za skupove formula:

Teorema

Neka je dat najviše prebrojiv skup formula prvog reda Δ. Ako je ovaj skup zadovoljiv, tada on ima model bilo koje beskonačne kardinalnosti.

Dokaz

Na sličan način kao i ranije, može se pokazati da ako je Δ zadovoljiv, tada on ima Erbranov model. Kako je skup Δ najviše prebrojiv, tada je takva i signatura (tj. skup funkcijskih i relacijskih simbola koji se javljaju u Δ), pa je i Erbranov univerzum najviše prebrojiv. Odatle sledi teorema „na dole". Teorema „na gore" se dokazuje slično kao i za jednu formulu.

Teorema kompaktnosti

Teorema

Neka je dat proizvoljan skup rečenica prvog reda Δ. Ovaj skup je zadovoljiv akko je zadovoljiv svaki njegov konačan podskup.

Dokaz

Bez umanjenja opštosti, pretpostavimo da su formule iz Δ univerzalno kvantifikovane (ako nisu, možemo ih svesti na ekvizadovoljive formule koje jesu). Skup Δ je zadovoljiv akko je zadovoljiv skup svih baznih instanci svih formula iz Δ. Ovaj skup baznih instanci se može posmatrati kao skup iskaznih formula, gde se svi bazni atomi prvog reda smatraju iskaznim slovima. Na osnovu kompaktnosti iskazne logike, ovaj skup je zadovoljiv akko je zadovoljiv svaki njegov konačni podskup. Medjutim, kako svaki konačni podskup skupa baznih instanci formula iz Δ potiče od konačno mnogo formula iz Δ, sledi da će skup svih konačnih podskupova baznih instanci formula iz Δ biti zadovoljiv akko je zadovoljiv svaki konačan podskup formula iz Δ.

Napomena

Teorema kompaktnosti je uz Skolem-Lovenhajmovu teoremu najznačajnija karakteristika logike prvog reda. Već u logici drugog reda ni jedna od ove dve teoreme ne važi!!

Posledice Skolem-Lovenhajmove teoreme

Primer

Neka je data signatura $\Sigma = (0, Suc, +, \cdot, =)$*, kao i skup aksioma:*

- $\forall x. Suc(x) \neq 0$
- $\forall xy. x \neq y \Rightarrow Suc(x) \neq Suc(y)$
- $\forall x. x + 0 = x$
- $\forall xy. x + Suc(y) = Suc(x + y)$
- $\forall x. x \cdot 0 = 0$
- $\forall xy. x \cdot Suc(y) = x \cdot y + x$
- $\phi[0] \wedge (\forall x. \phi[x] \Rightarrow \phi[Suc(x)]) \Rightarrow \forall x. \phi[x]$*, gde je* $\phi[x]$ *proizvoljna formula sa slobodnom promenljivom* x *(indukcijska shema).*

Ove aksiome definišu tzv. Peanovu aritmetiku prvog reda. Njena standardna interpretacija je struktura prirodnih brojeva (tj. prebrojiv model). Medjutim, iz Skolem-Lovenhajmove teoreme „na gore" sledi da postoje i nestandardni modeli ovog skupa aksioma koji nisu prebrojivi.

Posledice Skolem-Lovenhajmove teoreme

Primer

Neka je data signatura $\Sigma = (0, 1, +, \cdot, =, \leq)$*, kao i skup aksioma koje definišu tzv. realno zatvoreno polje (tj. uredjeno polje u kome svaki nenegativan element ima kvadratni koren, i svaki polinom neparnog stepena ima bar jednu nulu). Standardni model ovog skupa aksioma je struktura realnih brojeva. Medjutim, iz Skolem-Lovenhajmove teoreme „na dole" sledi da postoje i prebrojivi modeli za ovaj skup aksioma.*

Posledice Skolem-Lovenhajmove teoreme

Nekategoričnost u logici prvog reda

- Uopšte, u logici prvog reda se ne može aksiomatski zadati teorija tako da ima svojstvo kategoričnosti, tj. da svi modeli njenog skupa aksioma budu medjusobno izomorfni.
- U primeru sa prirodnim brojevima se umesto indukcijske sheme (tj. prebrojivog skupa aksioma parametrizovanog formulom $\phi[x]$) može koristiti jedna aksioma: $\forall P. P(0) \wedge (\forall x. P(x) \Rightarrow P(Suc(x))) \Rightarrow \forall x. P(x)$. Na ovaj način se obezbedjuje kategoričnost, ali je ova aksioma drugog reda (jer imamo kvantifikator po relaciji P).
- U primeru sa realnim brojevima se često u literaturi umesto zahteva da svaki polinom neparnog stepena ima bar jednu nulu (što se može iskazati prebrojivim skupom aksioma prvog reda) koristi npr. aksioma supremuma (svaki neprazan odozgo ograničen skup ima supremum). Ovim se postiže kategoričnost, ali je ovo opet aksioma drugog reda (jer kvantifikujemo po skupovima).

Mehanizacija Erbranove teoreme

Kako iskoristiti Erbranovu teoremu u praksi?

- Ispitivanje zadovoljivosti se svodi na ispitivanje zadovoljivosti skupa svih baznih instanci
- Ovaj skup može biti beskonačan
- Ipak, kompaktnost obezbeđuje potrebnu konačnost

Teorema

Univerzalno kvantifikovana formula je nezadovoljiva akko postoji konačan nezadovoljiv podskup njenih baznih instanci.

Mehanizacija Erbranove teoreme

Procedure poluodlučivanja zasnovane na Erbranovoj teoremi

- Procedure poluodlučivanja Erbranovog tipa nabrajaju skupove baznih instanci dodajući nove bazne instance u tekući skup:
  - Ukoliko se utvrdi nezadovoljivost tekućeg skupa instanci, polazna formula je nezadovoljiva
  - Ukoliko se iscrpe sve bazne instance, a nezadovoljivost se ne utvrdi, polazna formula je zadovoljiva
  - S obzirom na kompaktnost, u slučaju nezadovoljive formule ćemo sigurno u konačnom broju koraka doći do konačnog nezadovoljivog podskupa, pod uslovom da se bazne instance nabrajaju sistematski
  - U slučju da je formula zadovoljiva, takvog konačnog nezadovoljivog podskupa nema, pa će u slučaju beskonačnog Erbranovog univerzuma procedura beskonačno dodavati nove bazne instance i neće se zaustaviti
- Ispitivanje zadovoljivosti konačnog skupa baznih instanci se svodi na SAT, iskaznom apstrakcijom
- Najčuvenija je Gilmorova procedura (prva implementirana) koja instance prevodi u DNF i tako ispituje njihovu zadovoljivost
- Moderniji pristup može podrazumevati upotrebu CDCL SAT rešavača za ispitivanje zadovoljivosti skupova baznih instanci (transformisanih u KNF)

Erbranova teorema — primeri

Primer

Pokažimo da je rečenica $\exists x.\ \forall y. P(x,y) \Rightarrow \forall y.\ \exists x.\ P(x,y)$ *valjana. Pobijanjem, potrebno je pokazati da je njena negacija nezadovoljiva. Nakon NNF transformacije, dobija se formula* $\exists x.\ \forall y.\ P(x,y) \wedge \exists y.\ \forall x. \neg P(x,y)$*. Prenex trasformacija daje njoj ekvivalentnu formulu* $\exists z. \exists u. \forall w.\ P(z,w) \wedge \neg P(w,u)$*. Skolemizacijom se dobija formula* $\forall w.\ P(c_1,w) \wedge \neg P(w,c_2)$ *koja je nezadovoljiva akko je polazna formula valjana.*
Na osnovu Erbranove teoreme, prethodna formula je zadovoljiva akko je iskazno zadovoljiva formula

$$P(c_1,c_1) \wedge \neg P(c_1,c_2) \wedge P(c_1,c_2) \wedge \neg P(c_2,c_2),$$

što nije slučaj.

Primer

Paradoks berberina: Nije moguće da postoji berberin koji brije sve one koji sami sebe ne briju:

$$\neg(\exists b.\ \forall x.\ brije(b,x) \Leftrightarrow \neg brije(x,x))$$

Da bi se pokazalo da je prethodna formula valjana, pokažimo da je njena negacija nezadovoljiva. Nakon svođenja u normalnu formu, dobija se:

$$\forall x.\ (\neg brije(c,x) \vee \neg brije(x,x)) \wedge (brije(c,x) \vee brije(x,x))$$

Jedina Erbranova instanca ove formule je:

$$(\neg brije(c,c) \vee \neg brije(c,c)) \wedge (brije(c,c) \vee brije(c,c)),$$

koja je očigledno iskazno nezadovoljiva.

Erbranova teorema – primeri

Primer

Pokažimo da je formula $\exists x.\ (P(x) \Rightarrow \forall y.\ P(y))$ *valjana. Primenimo metodu pobijanja i transformacije normalnih formi.*

$$\neg(\exists x.\ (P(x) \Rightarrow \forall y.\ P(y)))$$

$$\forall x.\ (P(x) \wedge (\exists y.\ \neg P(y)))$$

$$\forall x.\ \exists y.\ (P(x) \wedge \neg P(y))$$

$$\forall x.\ (P(x) \wedge \neg P(f(x)))$$

Konjunkcija naredne dve instance je iskazno nezadovoljiva:

$$(P(c) \wedge \neg P(f(c))) \wedge (P(f(c)) \wedge \neg P(f(f(c))))$$

Erbranova teorema – primeri

Primer

Dokažimo da je formula $\forall x.\ \exists y.\ q(x,y)$ *logička posledica formula* $\forall x.\ \exists y. p(x,y)$ *i* $\forall x.\ \forall y.\ p(x,y) \Rightarrow q(x,y)$. *Potrebno je dokazati da je*

$$((\forall x.\ \exists y. p(x,y)) \wedge (\forall x.\ \forall y.\ p(x,y) \Rightarrow q(x,y))) \Rightarrow \forall x.\ \exists y.\ q(x,y)$$

valjana formula. NNF negacije prethodne formule je:

$$(\forall x.\ \exists y.\ p(x,y)) \wedge (\forall x.\ \forall y.\ \neg p(x,y) \vee q(x,y)) \wedge (\exists x.\ \forall y.\ \neg q(x,y))$$

Prenex transformacija daje:

$$\exists x.\ \forall z.\ \exists y.\ \forall w.\ p(z,y) \wedge (\neg p(z,w) \vee q(z,w)) \wedge \neg q(x,z)$$

Nakon skolemizacije, dobija se

$$\forall z.\ \forall w.\ p(z,f(z)) \wedge (\neg p(z,w) \vee q(z,w)) \wedge \neg q(c,z)$$

Erbranova teorema – primeri

Primer

Instance

$$p(c, f(c)) \wedge (\neg p(c, f(c)) \vee q(c, f(c))) \wedge \neg q(c, c)$$

i

$$p(f(c), f(f(c))) \wedge (\neg p(f(c), c) \vee q(f(c), c)) \wedge \neg q(c, f(c))$$

su zajedno nezadovoljive.

Primer

Primetimo, da je nezadovoljivost bilo moguće detektovati i jednostavnije da prilikom prenex transformacije nije vršena ,,ušteda" broja kvantifikatora.

$$\exists x.\ \forall x'.\ \exists y.\ \forall x''.\ \forall y'.\ \forall y''.\ p(x', y) \wedge (\neg p(x'', y') \vee q(x'', y')) \wedge \neg q(x, y''),$$

tj., nakon Skolemizacije

$$\forall x'.\ \forall x''.\ \forall y'.\ \forall y''.\ p(x', f(x')) \wedge (\neg p(x'', y') \vee q(x'', y')) \wedge \neg q(c, y'')$$

Tada bi postojala jedna jedina Erbranova instanca koja je nezadovoljiva:

$$p(c, f(c)) \wedge (\neg p(c, f(c)) \vee q(c, f(c))) \wedge \neg q(c, f(c)))$$

Erbranova teorema — zasebno instanciranje klauza

Erbranova teorema za klauzalnu formu

Prethodno zapažanje važi i generalno. Naime, uvođenjem novih univerzalnih kvantifikatora, moguće je postići da su slobodne promenljive u svim klauzama razdvojene (npr. $\forall x. P(x) \wedge Q(x)$ je ekvivalentno sa $(\forall x. P(x)) \wedge (\forall x. Q(x))$, odnosno sa $(\forall x'. P(x')) \wedge (\forall x''. Q(x''))$, tj. sa $\forall x'. \forall x''. P(x') \wedge P(x''))$.

Teorema

Neka je $F \equiv \forall x_1 \ldots x_n. C_1(x_1, \ldots, x_n) \wedge \ldots \wedge C_k(x_1, \ldots, x_n)$ formula u klauzalnoj normalnoj formi. Formula je zadovoljiva ako i samo ako je skup svih baznih instanci pojedinačnih klauza iskazno zadovoljiv, tj. ako je zadovoljiv skup $\{C_i[x_1 \to t_1, \ldots, x_n \to t_n] \mid t_1, \ldots, t_n \in H(F), 1 \leq i \leq k\}$.

Erbranova teorema – zasebno instanciranje klauza

Klauzalna forma kao skup klauza prvog reda

Imajući prethodno u vidu, formulu u klauzalnoj formi ćemo često predstavljati skupom svojih klauza, od kojih je svaka klauza skup literala prvog reda:

- pritom, sve klauze su, svaka ponaosob, univerzalno kvantifikovane (ovo ne zapisujemo, već implicitno podrazumevamo)
- skupovi promenljivih u različitim klauzama su međusobno disjunktni (ovo uvek možemo postići preimenovanjem)

Pregled

Neefikasnost Erbran-Gilmorove metode

- Osnovni problem Erbran-Gilmorovog metoda dokazivanja je bio kako pronaći bazne instance koje daju nezadovoljivost
- Faza generisanja skupova baznih instanci i faza ispitivanja njihove nezadovoljivosti su potpuno razdvojene
- Da li je moguće nekako objediniti ove dve faze?

Primer

Posmatrajmo univerzalno kvantifikovanu formulu koja se sastoji iz klauza:

$$\begin{array}{ll} 1. & \{p(x,y), q(y,f(u))\} \\ 2. & \{\neg q(z,z)\} \\ 3. & \{\neg p(w,f(w)), \neg p(f(w),f(w))\} \end{array}$$

(klauze su predstavljene kao skupovi literala i implicitno su univerzalno kvantifikovane). Da bismo dokazali nezadovoljivost ovog skupa klauza, razmatramo sledeće bazne instance gornjih klauza:

$$\begin{array}{llll} 4. & \{p(c,f(c)), q(f(c),f(c))\}, & \textit{iz } 1, & x \to c, y \to f(c), u \to c \\ 5. & \{\neg q(f(c),f(c))\}, & \textit{iz } 2, & z \to f(c) \\ 6. & \{\neg p(c,f(c)), \neg p(f(c),f(c))\}, & \textit{iz } 3, & w \to c \\ 7. & \{p(f(c),f(c)), q(f(c),f(c))\}, & \textit{iz } 1, & x \to f(c), y \to f(c), u \to c \end{array}$$

Primenom (iskazne) rezolucije, lako se iz dobijenih baznih instanci izvodi prazna klauza (iz 4 i 5 se dobija klauza $\{p(c,f(c))\}$*, iz 5 i 7 se dobija klauza* $\{p(f(c),f(c))\}$*. Sada klauza* $\{p(c,f(c))\}$ *sa klauzom 6 daje* $\{\neg p(f(c),f(c))\}$*, što sa klauzom* $\{p(f(c),f(c))\}$ *daje praznu klauzu).*

Primer

(nastavak) Primetimo da je na klauzu 5 (instancu klauze 2) dva puta primenjivano pravilo rezolucije, oba puta nad (različitim) instancama klauze 1:

$$\frac{\{p(c, f(c)), q(f(c), f(c))\} \quad \{\neg q(f(c), f(c))\}}{\{p(c, f(c))\}}$$
$$\frac{\{p(f(c), f(c)), q(f(c), f(c))\} \quad \{\neg q(f(c), f(c))\}}{\{p(f(c), f(c))\}}$$

Po sličnom principu, umesto ove dve instance klauze 1 mogla je da stoji bilo koja instanca ove klauze kod koje je y zamenjeno sa $f(c)$, a x proizvoljnim baznim termom t:

$$\frac{\{p(t, f(c)), q(f(c), f(c))\} \quad \{\neg q(f(c), f(c))\}}{\{p(t, f(c))\}}$$

(rezultujuća klauza sadrži term $p(t, f(c))$). Uočeni „šablon" bismo mogli predstaviti na sledeči način:

$$\frac{\{p(x, f(c)), q(f(c), f(c))\} \quad \{\neg q(f(c), f(c))\}}{\{p(x, f(c))\}}$$

Primer

(nastavak) Dobijeno pravilo:

$$\frac{\{p(x, f(c)), q(f(c), f(c))\} \quad \{\neg q(f(c), f(c))\}}{\{p(x, f(c))\}}$$

predstavlja pravilo rezolucije prvog reda. Ono je na izvestan način uopštenje svih ranije opisanih primena pravila iskazne rezolucije nad instancama klauza 1 i 2, u smislu da se svaka primena pravila iskazne rezolucije nad baznim instancama klauza 1 i 2 može dobiti instanciranjem promenljive x *odgovarajućim baznim termom* t *u gornjem pravilu. Dobijena rezolventa* $\{p(x, f(c))\}$ *je uopštenje svih baznih rezolventi dobijenih na ovaj način.*

- *Gornje zapažanje se može formulisati i ovako: kada primenimo navedeno pravilo rezolucije prvog reda, efekat je kao da smo istovremeno primenili pravilo iskazne rezolucije nad svim baznim instancama klauza 1 i 2 gornjeg oblika.*
- *Na ovaj način, rezolucijom prvog reda se objedinjuju (ranije razdvojene) faze generisanja baznih instanci klauza i dokazivanja nezadovoljivosti.*

Primer

(nastavak) Primetimo da je za ovako nešto bilo neophodno „parcijalno” instancirati klauze 1 i 2 tako da se dobiju dve klauze koje sadrže suprotne literale $q(f(c), f(c))$ *i* $\neg q(f(c), f(c))$. *Da bismo ovo postigli, bilo je potrebno pronaći uopštenu zamenu* σ *takvu da je* $q(y, f(u))\sigma = q(z, z)\sigma$. *U gornjem pravilu, korišcena je zamena* $\sigma = [y \to f(c), u \to c, z \to f(c)]$. *Za ovakvu zamenu kažemo da je* unifikator *za atome* $q(y, f(u))$ *i* $q(z, z)$. *Sada gornje pravilo rezolucije prvog reda možemo zapisati u obliku:*

$$\frac{\{p(x, y), q(y, f(u))\}\sigma \quad \{\neg q(z, z)\}\sigma}{\{p(x, y)\}\sigma}$$

Definicija

Unifikator dva atoma (ili terma) P i Q je uopštena zamena σ *takva da je* $P\sigma = Q\sigma$. *Za atome (termove) P i Q kažemo da su unifikabilni ako za njih postoji unifikator.*

Važna napomena

Unifikator ne mora biti jedinstven.

Primer

(nastavak) Posmatrajmo ponovo klauze 1 i 2 iz našeg primera (tj. klauze $\{p(x,y), q(y,f(u))\}$ *i* $\{\neg q(z,z)\}$*). Unifikator* $\sigma = [y \to f(c), u \to c, z \to f(c)]$ *primenjen na ove dve klauze daje nam instance* $\{p(x,f(c)), q(f(c),f(c))\}$ *i* $\{\neg q(f(c),f(c))\}$*, iz kojih se pravilom rezolucije:*

$$\frac{\{p(x,f(c)), q(f(c),f(c))\} \quad \{\neg q(f(c),f(c))\}}{\{p(x,f(c))\}}$$

dobija rezolventa $\{p(x,f(c))\}$*. Sa druge strane, da smo umesto unifikatora* σ *koristili unifikator* $\tau = [y \to f(f(c)), u \to f(c), z \to f(f(c))]$*, dobili bismo instance* $\{p(x,f(f(c))), q(f(f(c)),f(f(c)))\}$ *i* $\{\neg q(f(f(c)),f(f(c)))\}$*, kao i pravilo:*

$$\frac{\{p(x,f(f(c))), q(f(f(c)),f(f(c)))\} \quad \{\neg q(f(f(c)),f(f(c)))\}}{\{p(x,f(f(c)))\}}$$

iz koga se dobija rezolventa $\{p(x,f(f(c))\}$*.*

- *Jasno je da dobijena dva pravila ,,pokrivaju" različite skupove baznih instanci klauza 1 i 2.*
- *Da li je moguće naći opštije pravilo rezolucije prvog reda koje pokriva sve moguće primene pravila iskazne rezolucije nad baznim instancama klauza 1 i 2 po baznim instancama literala* $q(y,f(u))$*, odnosno* $\neg q(z,z)$*?*

Definicija

Kompozicija uopštenih zamena σ i τ je uopštena zamena $\sigma\tau$ definisana na sledeći način: $E(\sigma\tau) = (E\sigma)\tau$, za svaki izraz (atom ili term) E.

Definicija

Za unifikator σ atoma (termova) P i Q kažemo da je najopštiji ako je svaki drugi unifikator τ ovih atoma (termova) oblika $\tau = \sigma\tau'$, tj. τ je kompozicija unifikatora σ i neke zamene τ'.

Napomena

Primetimo da za unifikator τ važi $P\tau = Q\tau$, tj. $(P\sigma)\tau' = (Q\sigma)\tau'$. Kako je $P\sigma = Q\sigma$, ovo znači da je zajednička instanca od P i Q dobijena unifikatorom τ ujedno i instanca zajedničke instance od P i Q dobijene unifikatorom σ. Dakle, najopštiji unifikator nam daje najopštiju zajedničku instancu datih izraza P i Q.

Teorema

Za svaka dva unifikabilna atoma (ili terma) P i Q postoji najopštiji unifikator koji je jedinstven do na preimenovanje promenljivih.

Dokaz

Dokaz postojanja najopštijeg unifikatora izostavljamo zbog kompleksnosti. Dokažimo samo jedinstvenost. Neka su σ_1 *i* σ_2 *dva najopštija unifikatora za termove* t *i* s*. Iz činjenice da je* σ_1 *najopštiji unifikator sledi da se unifikator* σ_2 *može zapisati kao* $\sigma_2 = \sigma_1\tau_1$*. Slično, iz činjenice da je* σ_2 *najopštiji unifikator sledi da se unifikator* σ_1 *može zapisati kao* $\sigma_1 = \sigma_2\tau_2$*. Otuda je* $\sigma_2 = (\sigma_2\tau_2)\tau_1 = \sigma_2(\tau_2\tau_1)$*. Ovo znači da je zamena* $\tau_2\tau_1$ *identička zamena (koja svaku promenljivu zamenjuje samom sobom), što je moguće samo ako su* τ_1 *i* τ_2 *preimenovanja promenljivih (tj. svaku promenljivu zamenjuju nekom drugom promenljivom). Drugim rečima, najopštiji unifikator je jedinstven do na preimenovanje promenljivih.*

Primer

(nastavak) Za atome $q(y, f(u))$ *i* $q(z, z)$ *najopštiji unifikator je* $\sigma = [y \to f(u), z \to f(u)]$. *Ovim se oba atoma prezapisuju u* $q(f(u), f(u))$ *što je najopštija zajednička instanca ovih atoma. Sada najopštije pravilo rezolucije prvog reda za klauze 1 i 2 glasi:*

$$\frac{\{p(x, f(u)), q(f(u), f(u))\} \quad \{\neg q(f(u), f(u))\}}{\{p(x, f(u))\}}$$

Ovo pravilo pokriva sve moguče primene pravila iskazne rezolucije nad baznim instancama klauza 1 i 2 po baznim instancama literala $q(z, f(u)$ *i* $\neg q(z, z))$, *kao i sve moguće rezolvente koje se na taj način mogu dobiti (svaka tako dobijena bazna rezolventa će biti instanca rezolvente* $\{p(x, f(u))\}$*).*

Zaključujemo

- Umesto da generišemo bazne instance i nad njima sprovodimo iskaznu rezoluciju, možemo primenjivati pravilo rezolucije prvog reda nad klauzama prvog reda na koje je primenjen najopštiji unifikator za odgovarajuće literale po kojima se rezolucija vrši
- Ostaje otvoreno pitanje: kako pronaći najopštiji unifikator?

Najopštiji unifikator: ideja algoritma

Kako pronaći najopštiji unifikator?

- Želimo da pronađemo najopštiji unifikator za dva atoma (ili terma) P i Q
- Ukoliko su vodeći simboli izraza P i Q različiti, jasno je da se oni ne mogu unifikovati (ovo zovemo kolizija)
- Ako su im vodeći simboli jednaki (npr. $P = r(t_1, \ldots, t_n)$ i $Q = r(s_1, \ldots, s_n)$), tada je potrebno istovremeno unifikovati parove podtermova $(t_1, s_1), \ldots, (t_n, s_n)$ (tj. pronaći zamenu σ takvu da istovremeno važi $t_1\sigma = s_1\sigma, t_2\sigma = s_2\sigma, \ldots, t_n\sigma = s_n\sigma$). Ovaj korak zovemo dekompozicija.
- Zbog toga su algoritmi za pronalaženje najopštijeg unifikatora obično i konstruisani tako da razmatraju više parova termova instovremeno na ulazu
- Dekompozicija nas u krajnjoj instanci dovodi ili do kolizije, ili do situacije u kojoj je jedan od termova u paru promenljiva. Tada je jasno da se ta promenljiva mora instancirati drugim termom u paru (ovo zovemo aplikacija)
- Problem: ako imamo par (x, t), pri čemu term t sadrži promenljivu x, tada se ta dva terma ne mogu unifikovati (ovo zovemo cikličnost). Na primer, za par $(x, f(x))$, čime god da zamenimo x imaćemo jedno f ,,viška'' u desnom termu.

Algoritam za najopštiji unifikator

Algoritam

- Ulaz algoritma je skup parova termova (ili atoma) $(t_1, s_1), \ldots, (t_n, s_n)$ koje treba istovremeno unifikovati
- Izlaz algoritma je skup parova $(x_1, r_1), (x_2, r_2), \ldots, (x_k, r_k)$, gde je x_i promenljiva, a r_i term koji ne sadrži x_i, ili informacija o neuspehu u slučaju neunifikabilnih termova.
- Dokle god je moguće, primenjuju se sledeći koraci (u navedenom redosledu):
  - ako postoje dva ili više identičnih parova, tada se svi osim jednog brišu (pravilo faktorisanja)
  - ako postoji par (t, t), on se uklanja iz skupa (pravilo tautologija)
  - ako postoji par (t, x), gde t nije promenljiva, tada se ovaj par zamenjuje parom (x, t) (pravilo orijentacija)
  - ako postoji par $(f(t_1, \ldots, t_n), g(s_1, \ldots, s_m))$, tada se algoritam prekida, jer ne postoji unifikator (pravilo kolizija)
  - ako postoji par $(f(t_1, \ldots, t_n), f(s_1, \ldots, s_n))$, tada se taj par zamenjuje parovima $(t_1, s_1), \ldots, (t_n, s_n)$ (pravilo dekompozicija)
  - ako postoji par (x, t) pri čemu t ne sadrži promenljivu x, tada se u svim ostalim parovima x zamenjuje termom t (pravilo aplikacija)
  - ako postoji par (x, t), pri čemu t sadrži x, tada se algoritam prekida, jer ne postoji unifikator (pravilo cikličnost)
- Ukoliko algoritam nije prekinut zbog neuspeha, iz rezultujućeg skupa parova se direktno određuje najopštiji unifikator $\sigma = [x_1 \to r_1, \ldots x_k \to r_k]$.

Primer

Unifikacija atoma $q(y, f(u))$ *i* $q(z, z)$ *iz prethodnog primera se dekompozicijom svodi na istovremenu unifikaciju parova* (y, z) *i* $(f(u), z)$. *Pravilo orijentacije nam daje skup parova* $(y, z), (z, f(u))$, *a pravilo aplikacije nam daje skup parova* $(y, f(u)), (z, f(u))$. *Dalje se ne može primeniti ni jedno od pravila, pa je rezultujući najopštiji unifikator* $[y \to f(u), z \to f(u)]$.

Pregled

Metod rezolucije

O metodu rezolucije

- Zasniva se na ranije uvedenom pravilu rezolucije prvog reda
- U pitanju je procedura poluodlučivanja (za svaku nezadovoljivu formulu može izvođenjem prazne klauze dokazati da je nezadovoljiva)
- Pored potpunosti (za pobijanje) ima i svojstvo saglasnosti: iz zadovoljivog skupa klauza ne može se izvesti prazna klauza
- Za zadovoljiv skup klauza postoje dva scenarija: ili se više ne mogu izvoditi nove klauze pravilom rezolucije (procedura vraća odgovor da) ili se nove klauze beskonačno izvode, pa se procedura nikada ne završava (dakle, metod nema svojstvo zaustavljanja)

Pravilo binarne rezolucije prvog reda

Pravilo binarne rezolucije prvog reda

Pravilo binarne rezolucije prvog reda glasi:

$$\frac{C_1 \vee A_1 \quad C_2 \vee \neg A_2}{(C_1 \vee C_2)\sigma}$$

gde je σ najopštiji unifikator atoma A_1 i A_2.

- Pravilo se zove binarno, jer uvek rezolvira dva literala (po jedan iz svake klauze).
- Da li je ovako formulisano pravilo dovoljno za dokazivanje nezadovoljivosti?
- Podsetimo se: pravilo rezolucije prvog reda bi trebalo da pokrije sve odgovarajuće primene pravila iskazne rezolucije nad baznim instancama datih klauza

Pravilo binarne rezolucije

Primer

Neka je dat skup klauza prvog reda („paradoks berberina"):

$$\begin{array}{ll} 1. & \{\neg p(x,x), \neg p(c,x)\} \\ 2. & \{p(y,y), p(c,y)\} \end{array}$$

Ovaj skup klauza je nezadovoljiv. Zaista, ako u prvoj klauzi zamenimo x *sa* c*, dobijamo baznu instancu* $\{\neg p(c,c), \neg p(c,c)\}$*, što je ekvivalentno sa* $\{\neg p(c,c)\}$*. Slično, zamenom* y *sa* c *u drugoj klauzi dobijamo baznu instancu* $\{p(c,c)\}$*. Iz ove dve bazne klauze se direktno izvodi prazna klauza.*
Sa druge strane, primenom pravila rezolucije prvog reda (nad, npr. prvim literalima obe klauze) dobijamo:

$$\frac{\{\neg p(x,x), \neg p(c,x)\} \quad \{p(y,y), p(c,y)\}}{\{\neg p(c,y), p(c,y)\}}$$

pri čemu je na klauze primenjen najopštiji unifikator atoma $p(x,x)$ *i* $p(y,y)$ *(to je zamena* $\sigma = [x \to y]$*). Dobijena klauza* $\{\neg p(c,y), p(c,y)\}$ *je ekvivalentna sa* $\top$ *i iz nje se dalje ništa ne može izvesti. Sličan rezultat bismo dobili za bilo koji par unifikabilnih atoma iz ovih klauza.*

Pravilo binarne rezolucije

U čemu je problem?

- Problem u prethodnom primeru je to što smo za izvođenje prazne klauze koristili bazne instance u kojima se dva različita literala prvog reda svode na isti bazni literal (npr. $p(y, y)$ i $p(c, y)$ se instanciranjem svode na bazni literal $p(c, c)$).
- Ovo dovodi do toga da bazna instanca ima manje literala od polazne klauze prvog reda
- Pravilo binarne rezolucije prvog reda ne može da „pokrije" iskaznu rezoluciju nad ovakvim baznim instancama
- Dva moguća rešenja ovog problema:
  - Grupisanje: parcijalno instanciranje klauze tako da se „slični" literali svedu na jedan, pre rezolucije
  - Uopšteno pravilo rezolucije: rezolucija koja se vrši istovremeno nad više literala iz svake od klauza

Pravilo grupisanja

Definicija

Pravilo grupisanja ima sledeći oblik:

$$\frac{C \vee L_1 \vee L_2 \vee \ldots \vee L_m}{(C \vee L_1)\sigma}$$

gde je $C \vee L_1 \vee \ldots \vee L_m$ *klauza prvog reda takva da su literali* $L_1, \ldots, L_m$ *unifikabilni sa najopštijim unifikatorom* σ*, tj. važi da je:*

$$L_1\sigma = L_2\sigma = \ldots = L_m\sigma$$

a C *je proizvoljna disjunkcija literala prvog reda (eventualno prazna).*
NAPOMENA: primetimo da svi literali $L_1, \ldots, L_m$ *moraju biti istog polariteta (ili su svi atomi, ili su svi negacije atoma)*

Napomena

Ovo pravilo uz pravilo binarne rezolucije garantuje potpunost za pobijanje, jer omogućava izvođenje klauza koje su uopštenja baznih instanci kod kojih se više literala redukuju u jedan

Pravilo grupisanja

Primer

(nastavak) Primenom pravila grupisanja na klauzu $\{p(y,y), p(c,y)\}$ *dobija se klauza* $\{p(c,c)\}$ *(najopštiji unifikator za literale* $p(y,y)$ *i* $p(c,y)$ *je zamena* $[y \to c]$*). Slično, primenom pravila grupisanja na klauzu* $\{\neg p(x,x), \neg p(c,x)\}$ *dobija se klauza* $\{\neg p(c,c)\}$*. Iz ove dve klauze se lako izvodi prazna klauza (binarnom rezolucijom).*

Uopšteno pravilo rezolucije

Definicija

Uopšteno pravilo rezolucije prvog reda ima sledeći oblik:

$$\frac{C' \vee A'_1 \vee A'_2 \vee \ldots \vee A'_m \quad C'' \vee \neg A''_1 \vee \neg A''_2 \vee \ldots \vee \neg A''_n}{(C' \vee C'')\sigma}$$

pri čemu su $C' \vee A'_1 \vee A'_2 \vee \ldots \vee A'_m$ *i* $C'' \vee \neg A''_1 \vee \neg A''_2 \vee \ldots \vee \neg A''_n$ *klauze prvog reda takve da su svi atomi* $A'_1, \ldots, A'_m, A''_1, \ldots, A''_n$ *unifikabilni sa najopštijim unifikatorom* σ*, tj. važi da je:*

$$A'_1\sigma = \ldots = A'_m\sigma = A''_1\sigma = \ldots = A''_n\sigma$$

a C' *i* C'' *su proizvoljne disjunkcije literala prvog reda (eventualno prazne).*

Napomene

- Ovo pravilo objedinjuje pravila binarne rezolucije i grupisanja
- Njegov efekat je isti kao da smo prvo grupisali literale $A'_1, \ldots, A'_m$ u prvoj klauzi i $\neg A''_1, \ldots, \neg A''_n$ u drugoj klauzi, a zatim primenili binarnu rezoluciju nad dobijenim literalima
- Ovo pravilo je dovoljno (samo za sebe) da obezbedi potpunost (za pobijanje)

Uopšteno pravilo rezolucije

Primer

(nastavak) Primenom uopštenog pravila rezolucije nad klauzama $\{p(y,y), p(c,y)\}$ *i* $\{\neg p(x,x), \neg p(c,x)\}$ *dobijamo praznu klauzu u jednom koraku, jer je najopštiji unifikator za atome* $p(y,y)$, $p(c,y)$, $p(x,x)$ *i* $p(c,x)$ *zamena* $\sigma = [x \to c, y \to c]$.

Preimenovanje promenljivih u klauzama

Podsetnik – napomena

- Setimo se da su sve klauze implicitno univerzalno kvantifikovane, svaka za sebe
- Ovo znači da možemo smatrati da su skupovi promenljivih koje se javljaju u različitim klauzama disjunktni (ovo uvek možemo postići preimenovanjem promenljivih).
- Ova činjenica nam daje dodatnu slobodu prilikom unifikacije

Primer

Skup klauza $\{p(x)\}$, $\{\neg p(f(x))\}$ *je nezadovoljiv iako na prvi pogled deluje da* $p(x)$ *i* $p(f(x))$ *nisu unifikabilni. Kako su ove dve klauze nezavisno (svaka za sebe) univerzalno kvantifikovane, možemo npr. u prvoj preimenovati promenljivu* x *u* x'*. Sada su atomi* $p(x')$ *i* $p(f(x))$ *unifikabilni (unifikator je* $[x' \to f(x)]$*, odakle izvodimo praznu klauzu.*

PREPORUKA

Pre primene pravila rezolucije uvek obezbediti da skupovi promenljivih u dvema odabranim klauzama budu disjunktni (preimenovanjem)

Metod rezolucije

Primer

Vratimo se ponovo na primer sa početka:

$$\begin{array}{ll} 1. & \{p(x,y), q(y,f(u))\} \\ 2. & \{\neg q(z,z)\} \\ 3. & \{\neg p(w,f(w)), \neg p(f(w),f(w))\} \end{array}$$

i dokažimo metodom rezolucije prvog reda da je ovaj skup klauza nezadovoljiv. Najpre primenjujemo pravilo rezolucije nad klauzama 1 *i* 2 *(najopštiji unifikator za atome* $q(y,f(u))$ *i* $q(z,z)$ *je* $[y \to f(u), z \to f(u)]$*). Dobijamo klauzu:*

$$4. \quad \{p(x,f(u))\}$$

Dalje, primenjujemo pravilo rezolucije nad klauzama 3 *i* 4 *za prvi literal klauze* 3 *(najopštiji unifikator za atome* $p(w,f(w))$ *i* $p(x,f(u))$ *je* $[x \to w, u \to w]$*). Dobijamo rezolventu:*

$$5. \quad \{\neg p(f(w),f(w))\}$$

Najzad, primenom rezolucije nad klauzama 4 *i* 5 *(unifikator* $[x \to f(w), u \to w]$*) dobijamo praznu klauzu.*

Metod rezolucije

Primer

Neka je dat skup klauza:

$$\begin{array}{ll} 1. & \{p(x,y), q(x,y)\} \\ 2. & \{\neg p(x,y), \neg q(x,y)\} \end{array}$$

Ovaj skup klauza je zadovoljiv, jer se iz njega ne može nikako izvesti prazna klauza (zašto?). Međutim, studenti često pogrešno primene pravilo rezolucije tako što istovremeno „ponište" dva para literala: literal $p(x,y)$ sa $\neg p(x,y)$, a literal $q(x,y)$ sa $\neg q(x,y)$, i na taj način dobiju praznu klauzu. Ovako nešto nije bilo moguće ni u iskaznoj rezoluciji (npr. iz klauza $\{p,q\}$ i $\{\neg p, \neg q\}$ nije moguće izvesti praznu klauzu). Dakle, svaka primena pravila rezolucije se uvek primenjuje nad samo jednim parom literala.
Zabuna (verovatno) nastaje zbog pogrešnog razumevanja uopštenog pravila rezolucije: i ovo pravilo se uvek primenjuje nad samo jednim parom literala, s tim što se prethodno više „sličnih" (unifikabilnih) literala u svakoj od klauza mogu grupisati u jednu zajedničku instancu, pre primene rezolucije. Gornji primer je nešto sasvim drugo i to ne treba mešati.

Pregled

Deduktivni sistemi

Dedukcija

- Dedukcijski sistemi predstavljaju treći aspekt svakog logičkog sistema (pored sintakse i semantike)
- Dedukcija se bavi konstrukcijom dokaza i ispitivanjem dokazivosti tvrđenja u datom logičkom sistemu
- Uobičajeno je da tvrđenje bude dokazivo (tj.teorema) u deduktivnom sistemu akko je u pitanju semantički valjana formula (saglasnost i potpunost deduktivnog sistema)
- Ipak, dedukcija se obično posmatra kao ,,simbolička igra", lišena svakog unapred zadatog značenja
- deduktivne sisteme možemo razmatrati i u iskaznoj logici, kao i u logici prvog reda
- ipak, u logici prvog reda je značaj deduktivnih sistema mnogo veći, imajući u vidu beskonačnost domena koje razmatramo
- Neki sistemi (poput prirodne dedukcije) podrazumevaju dokaze koji su čitljivi za čoveka, jer prate uobičajen način rezonovanja prilikom dokazivanja teorema (za razliku od npr. rezolucijskih dokaza nezadovoljivosti)
- Hilbertov sistem, Prirodna dedukcija, Račun sekvenata ...

Dedukcija

Dedukcioni sistem

- Pravila izvođenja oblika: $\frac{P_1,\ldots,P_n}{Q}$ ($P_1, \ldots, P_n$ su premise, a Q je zaključak pravila)
- Aksiome: tvrđenja za koja pretpostavljamo da važe uvek
- Pretpostavke: dodatna tvrđenja za koje pretpostavljamo da važe u nekom kontekstu
- Dokaz: izvođenje iz aksioma i pretpostavki primenom pravila (u vidu niza ili stabla)
- $\Delta \vdash F$: F je dokaziva iz Δ (i aksioma)
- $\vdash F$: F je teorema, tj. dokaziva bez dodatnih pretpostavki (samo iz aksioma)
- Saglasnost: ako $\vdash F$, onda $\models F$
- Potpunost: ako $\models F$, onda $\vdash F$

Prirodna dedukcija u logici prvog reda

Prirodna dedukcija

- Deduktivni sistem koji je najbliži načinu rezonovanja čoveka prilikom dokazivanja matematičkih tvrđenja
- U iskaznoj varijanti, postoje pravila uvođenja i pravila eliminacije iskaznih veznika
- U sistemu prirodne dedukcije za logiku prvog reda dodatno postoje i pravila za uvođenje i eliminaciju kvantifikatora
- U prirodnoj dedukciji razlikujemo klasičnu i intuicionističku logiku

Pravila prirodne dedukcije za iskazne veznike

Negacija

$$\dfrac{\begin{array}{c}[A]^1\\ \vdots \\ \bot\end{array}}{\neg A}\ \neg I^1 \qquad\qquad \dfrac{A \qquad \neg A}{\bot}\ \neg E$$

Konjunkcija

$$\dfrac{A \qquad B}{A \wedge B}\ \wedge I \qquad\qquad \dfrac{A \wedge B}{A}\ \wedge E1 \qquad \dfrac{A \wedge B}{B}\ \wedge E2$$

Disjunkcija

$$\dfrac{A}{A \vee B}\ \vee I1 \qquad \dfrac{B}{A \vee B}\ \vee I2 \qquad \dfrac{A \vee B \qquad \begin{array}{c}[A]^1\\ \vdots \\ C\end{array} \qquad \begin{array}{c}[B]^2\\ \vdots \\ C\end{array}}{C}\ \vee E^{1,2}$$

Pravila prirodne dedukcije za iskazne veznike

Implikacija

$$\frac{\begin{array}{c}[A]^1 \\ \vdots \\ B\end{array}}{A \Rightarrow B} \Rightarrow I^1 \qquad \frac{A \qquad A \Rightarrow B}{B} \Rightarrow E$$

Logičke konstante

$$\frac{\bot}{A} \bot E \qquad \frac{}{\top} \top I$$

Klasična naspram intuicionističke logike

Klasična pravila

$$\frac{}{A \vee \neg A}\ \text{ExcludedMiddle} \qquad \frac{\neg\neg A}{A}\ \text{DoubleNegation} \qquad \dfrac{\begin{matrix}[\neg A]^1 \\ \vdots \\ \bot\end{matrix}}{A}\ \mathit{Contradiction}^1$$

Pravila za kvantifikatore

Univerzalni kvantifikator

$$\frac{A[x \to y]}{\forall x.A} \ \forall I \qquad\qquad \frac{\forall x.A}{A[x \to t]} \ \forall E$$

Egzistencijalni kvantifikator

$$\frac{A[x \to t]}{\exists x.A} \ \exists I \qquad\qquad \frac{\exists x.A \qquad \begin{array}{c}[A[x \to y]]^1 \\ \vdots \\ B\end{array}}{B} \ \exists E^1$$

Dokaz

Dokaz u prirodnoj dedukciji je stablo u čijim se čvorovima nalaze formule. U korenom čvoru se nalazi formula koja se dokazuje, u listovima se nalaze aksiome (tj. formule koje se mogu izvesti pravilima bez premisa) ili pretpostavke (od kojih neke mogu biti oslobođene primenom određenih pravila), a svaki čvor v koji nije list sadrži formulu koja se dobija od formula u čvorovima koji su deca čvora v, primenom nekog od pravila. Formula je teorema ako za nju postoji dokaz bez neoslobođenih pretpostavki.

- Pišemo: $H_1, \ldots, H_k \vdash A$ ako postoji dokaz formule A sa neoslobodjenim pretpostavkama $H_1, \ldots, H_k$
- Pišemo: $\vdash A$ ako postoji dokaz formule A bez neoslobodjenih pretpostavki

Prirodna dedukcija – primer

Primer

$$
\dfrac{
\dfrac{\dfrac{[\neg(A \vee B)]^1 \qquad \dfrac{[A]^2}{A \vee B}\,\vee I1}{\bot}\,\neg E}{\neg A}\,\neg I^2
\qquad
\dfrac{\dfrac{[\neg(A \vee B)]^1 \qquad \dfrac{[B]^3}{A \vee B}\,\vee I2}{\bot}\,\neg E}{\neg B}\,\neg I^3
}{
\dfrac{\neg A \wedge \neg B}{\neg(A \vee B) \Rightarrow \neg A \wedge \neg B}\,\Rightarrow I^1
}
$$

Uvođenje univerzalnog kvantifikatora

Uvođenje univerzalnog kvantifikatora

Pravilo za uvođenje univerzalnog kvantifikatora glasi:

$$\frac{A[x \to y]}{\forall x.A}\ \forall I$$

uz dodatni uslov da se promenljiva y ne nalazi kao slobodna ni u $\forall x.A$ ni u bilo kojoj neoslobođenoj pretpostavci u stablu dokaza formule $A[x \to y]$. Intuitivno, ovo znači sledeće: ako formula A važi za neki element y o kome nemamo nikakvih pretpostavki (tj. potpuno je proizvoljan), tada A važi za svaki element x. Specijalno, ako uzmemo da je $x = y$, tada dobijamo oblik:

$$\frac{A}{\forall x.A}\ \forall I$$

uz uslov da se promenljiva x ne nalazi slobodna u neoslobođenim pretpostavkama u dokazu formule A (tj. A važi za proizvoljan element x). Sledeći primer ilustruje neophodnost ovog dodatnog uslova.

Primer

Setimo se formule $p(x) \Rightarrow \forall x.p(x)$*. Ova formula nije valjana, pa ne bi trebalo da bude ni dokaziva (ako želimo da naš deduktivni sistem bude saglasan). Ipak, kada ne bismo imali dodatni uslov u pravilu za uvođenje univerzalnog kvantifikatora, tada bismo mogli da iz pretpostavke* $p(x)$ *izvedemo* $\forall x.p(x)$*, a da zatim pravilom uvođenja implikacije izvedemo formulu* $p(x) \Rightarrow \forall x.p(x)$ *(uz oslobađanje pretpostavke* $p(x)$*), što bi značilo da je* $p(x) \Rightarrow \forall x.p(x)$ *teorema prirodne dedukcije.*
Dodatni uslov u pravilu uvođenja univerzalnog kvantifikatora sprečava kreiranje ovakvog dokaza, zato što zabranjuje izvođenje univerzalno kvantifikovane formule $\forall x.p(x)$ *iz pretpostavke* $p(x)$ *koja sadrži kvantifikovanu promenljivu* x *kao slobodnu.*

Eliminacija univerzalnog kvantifikatora

Pravilo za eliminaciju univerzalnog kvantifikatora glasi:

$$\frac{\forall x.A}{A[x \to t]}\ \forall E$$

Ovo pravilo je prilično intuitivno: ako A važi za svako x, tada to x možemo zameniti bilo kojim termom t (tj. važi proizvoljna instanca (po x) formule A). Ograničenje za primenu ovog pravila je da term t ne sme sadržati promenljive koje bi zamenom x sa t u A postale vezane.

Primer

Pođimo od pretpostavke $\forall x.\exists y.p(x,y)$*. Ako ne bi bilo ograničenja u primeni pravila eliminacije univerzalnog kvantifikatora, tada bismo mogli da njegovom primenom iz ove pretpostavke izvedemo formulu* $\exists y.p(y,y)$*. Dalje bismo mogli primenom pravila uvođenja implikacije da izvedemo formulu* $(\forall x.\exists y.p(x,y)) \Rightarrow \exists y.p(y,y)$ *(uz oslobađanje pretpostavke). Za ovu formulu smo ranije konstatovali da nije valjana. Ovaj primer ilustruje neophodnost uvedenog ograničenja prilikom primene pravila eliminacije univerzalnog kvantifikatora.*

Uvođenje egzistencijalnog kvantifikatora

Pravilo za uvođenje egzistencijalnog kvantifikatora glasi:

$$\frac{A[x \to t]}{\exists x.A}\ \exists I$$

Ovo pravilo je takođe prilično intuitivno: ako važi neka instanca (po x) formule A, tj. važi $A[x \to t]$ za neko t, tada znači da postoji neka vrednost promenljive x za koju je formula A tačna. Otuda, važi $\exists x.A$. Ograničenje za primenu ovog pravila je da term t ne sme sadržati promenljive koje bi postale vezane zamenom x sa t u A.

Primer

Pođimo od pretpostavke $\forall y.p(y,y)$. *Kada ne bi bilo dodatnog uslova u primeni pravila za uvođenje egzistencijalnog kvantifikatora, mogli bismo da njegovom primenom izvedemo npr. formulu* $\exists x.\forall y.p(x,y)$. *Sada bismo primenom pravila uvođenja implikacije, uz eliminaciju pretpostavke, dobili formulu* $(\forall y.p(y,y)) \Rightarrow \exists x.\forall y.p(x,y)$. *Ova formula nije valjana (uzmimo proizvoljnu strukturu sa bar dva elementa i interpretirajmo* $p(x,y)$ *kao „x je jednako y").*

Eliminacija egzistencijalnog kvantifikatora

Pravilo eliminacije egzistencijalnog kvantifikatora glasi:

$$\dfrac{\exists x.A \qquad \begin{array}{c}[A[x \to y]]^1 \\ \vdots \\ B\end{array}}{B}\ \exists E^1$$

uz dodatni uslov da se promenljiva y ne pojavljuje kao slobodna ni u formuli B, ni u formuli $\exists x.A$, ni u neoslobođenim pretpostavkama u dokazu formule B, osim možda u samoj formulu $A[x \to y]$. Intuitivno, ovo znači sledeće: ako pretpostavimo da formula A važi za neki proizvoljan element y (tj. za element za koji nema nikakvih dodatnih pretpostavki), i ako iz te pretpostavke možemo da dokažemo formulu B, to znači da iz $\exists x.A$ možemo da dokažemo B.

Primer

Sledeći primer ilustruje neophodnost uvođenja dodatnih uslova u pravilo eliminacije egzistencijalnog kvantifikatora: pretpostavimo da imamo pretpostavku $\exists x.p(x)$. *Kada ne bi bilo dodatnih uslova u pravilu za eliminaciju egzistencijalnog kvantifikatora, tada bismo mogli da (stavljanjem* $A = B = p(x)$ *i* $y = x$*) ovim pravilom izvedemo* $p(x)$. *Dalje bismo mogli da, primenom pravila uvođenja univerzalnog kvantifikatora, izvedemo formulu* $\forall x.p(x)$ *(jer jedina neoslobođena pretpostavka u dokazu formule* $p(x)$*, tj. formula* $\exists x.p(x)$ *ne sadrži slobodna pojavljivanja promenljive* x*). Dalje se primenom pravila uvođenja implikacije oslobađa pretpostavka* $\exists x.p(x)$ *i izvodi se formula* $(\exists x.p(x)) \Rightarrow (\forall x.p(x))$*, koja naravno ne bi trebalo da bude dokaziva, jer nije valjana. Dodatni uslov u pravilu eliminacije egzistencijalnog kvantifikatora sprečava ovakva izvođenja.*

Meta-tvrđenja o prirodnoj dedukciji

Teorema

Sistem prirodne dedukcije za klasičnu logiku prvog reda je saglasan, tj. u njemu je moguće dokazati samo valjane formule prvog reda.

Teorema

Sistem prirodne dedukcije za klasičnu logiku prvog reda je potpun, tj. u njemu je moguće dokazati svaku valjanu formulu prvog reda.

Teorema

U sistemu prirodne dedukcije za klasičnu logiku važi $\Delta \vdash F$ *akko* $\Delta \models F$ *(čak i ako nisu sve formule iz* Δ *rečenice).*

Primer

Dokažimo da važi $\vdash (\exists x.\forall y.p(x,y)) \Rightarrow (\forall y.\exists x.p(x,y))$*. Dokaz se može predstaviti sledećim stablom:*

$$\dfrac{[\exists x.\forall y.p(x,y)]^2 \qquad \dfrac{\dfrac{\dfrac{[\forall y.p(x',y)]^1}{p(x',y')}\,\forall E}{\exists x.p(x,y')}\,\exists I}{\forall y.\exists x.p(x,y)}\,\forall I}{\dfrac{\forall y.\exists x.p(x,y)}{(\exists x.\forall y.p(x,y)) \Rightarrow (\forall y.\exists x.p(x,y))}\,\Rightarrow I, 2}\,\exists E, 1$$

Intuitivno, dokaz teče na sledeći način: da bismo dokazali tvrđenje, treba da dokažemo da se formula $\forall y.\exists x.p(x,y)$ *može dokazati iz* $\exists x.\forall y.p(x,y)$ *(nakon toga je dovoljno primeniti pravilo uvođenja implikacije). Da bismo ovo dokazali, treba da dokažemo formulu* $\forall y.\exists x.p(x,y)$ *polazeći od formule* $\forall y.p(x',y)$ *(tj. polazimo od toga da* $\forall y.p(x',y)$ *važi za neko proizvoljno* x' *o kome ništa drugo ne znamo). Zbog univerzalnog kvantifikatora važi* $p(x',y')$ *za to izabrano* x' *i za proizvoljno* y'*, odakle važi* $\exists x.p(x,y')$ *za proizvoljno* y'*. Zbog proizvoljnosti* y' *sada važi* $\forall y.\exists x.p(x,y)$*, što je i trebalo dokazati.*

Primer

Dokažimo sledeću formulu: $(\neg\exists x.p(x)) \Rightarrow (\forall y.\neg p(y))$. *Dokaz se može predstaviti sledećim stablom:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[p(z)]^{1}}{\exists x.p(x)}\,\exists I \qquad [\neg\exists x.p(x)]^{2}}{\bot}\,\neg E}{\neg p(z)}\,\neg I, 1}{\forall y.\neg p(y)}\,\forall I}{(\neg\exists x.p(x)) \Rightarrow (\forall y.\neg p(y))}\,\Rightarrow I, 2$$

Intuitivno: potrebno je dokazati formulu $\forall y.\neg p(y)$ *iz pretpostavke* $\neg\exists x.p(x)$. *Neka* $p(z)$ *važi za neko proizvoljno* z. *Tada važi tvrđenje* $\exists x.p(x)$, *što je u kontradikciji sa pretpostavkom* $\neg\exists x.p(x)$. *Ovo znači da nije* $p(z)$, *tj. da važi* $\neg p(z)$. *Kako je* z *proizvoljno, tj. za njega ne važe nikakve dodatne pretpostavke, možemo da zaključimo da važi* $\forall y.\neg p(y)$. *Otuda sledi tvrđenje.*

Eksplicitni konteksti

Izvođenje dokaza u prirodnoj dedukciji

- Dokazi u prirodnoj dedukciji se obično konstruišu primenom pravila unazad, polazeći od formule koju dokazujemo:
  - drugim rečima: da bih dokazao zaključak pravila Q, dovoljno je da dokažem sve njegove premise $P_1, \dots, P_k$
- Problem predstavljaju pravila koja oslobađaju pretpostavke:
  - primenom ovakvih pravila unazad dodajemo novu pretpostavku u skup pretpostavki koje možemo koristiti u dokazivanju premisa
  - sada je potrebno u svakoj grani dokaza pamtiti pretpostavke koje su nam na raspolaganju
- Ovaj problem se rešava eksplicitnim navođenjem konteksta:
  - u svakom čvoru stabla sada nije formula, već kontekst oblika $\Gamma \vdash A$ čije je intuitivno značenje: ,,dokazujem A pod pretpostavkama Γ"
  - u korenu stabla je tvrđenje $\Gamma \vdash A$ koje dokazujemo (Γ može biti i prazno)
- Neophodno je najpre i sama pravila formulisati na takav način

Pravila sa kontekstima

Negacija

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg I \qquad\qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg E$$

Konjunkcija

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge I \qquad\qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge E1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge E2$$

Disjunkcija

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee I1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee I2 \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee E$$

Pravila sa kontekstima

Implikacija

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow I \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash A \Rightarrow B}{\Gamma \vdash B} \Rightarrow E$$

Logičke konstante

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \bot E \qquad \frac{}{\Gamma \vdash \top} \top I$$

Pravila klasične logike

$$\frac{}{\Gamma \vdash A \vee \neg A} \mathit{ExclMiddle} \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A} \mathit{DoubleNeg} \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} \mathit{Contr}$$

„Važi po pretpostavci"

$$\frac{}{\Gamma, A \vdash A} \mathrm{ass}$$

Pravila sa kontekstima

Univerzalni kvantifikator

$$\frac{\Gamma \vdash A[x \to y]}{\Gamma \vdash \forall x.A}\ \forall I \qquad \frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[x \to t]}\ \forall E$$

Egzistencijalni kvantifikator

$$\frac{\Gamma \vdash A[x \to t]}{\Gamma \vdash \exists x.A}\ \exists I \qquad \frac{\Gamma \vdash \exists x.A \qquad \Gamma, A[x \to y] \vdash B}{\Gamma \vdash B}\ \exists E$$

Primer

Primer

$$
\dfrac{\dfrac{\dfrac{\neg(A \lor B) \vdash \neg(A \lor B) \qquad \dfrac{A \vdash A}{A \vdash A \lor B}\,\lor I1}{\neg(A \lor B), A \vdash \bot}\,\neg E}{\neg(A \lor B) \vdash \neg A}\,\neg I \qquad \dfrac{\dfrac{\neg(A \lor B) \vdash \neg(A \lor B) \qquad \dfrac{B \vdash B}{B \vdash A \lor B}\,\lor I2}{\neg(A \lor B), B \vdash \bot}\,\neg E}{\neg(A \lor B) \vdash \neg B}\,\neg I}{\dfrac{\neg(A \lor B) \vdash \neg A \land \neg B}{\vdash \neg(A \lor B) \Rightarrow \neg A \land \neg B}\,\Rightarrow I}
$$

Napomena

Zbog kompaktnosti zapisa, mi smo na pojedinim mestima iz skupa pretpostavki uklanjali pretpostavke koje nisu potrebne u nastavku te grane dokaza:

- formalno, trebalo bi uvesti i strukturna pravila kojima se brišu nepotrebne pretpostavke, zamenjuje redosled pretpostavki, uklanjaju duplikati iz skupa pretpostavki i sl.

Primer

Primer

$$\dfrac{\dfrac{\exists x.\forall y.p(x,y) \vdash \exists x.\forall y.p(x,y) \qquad \dfrac{\dfrac{\dfrac{\forall y.p(x',y) \vdash \forall y.p(x',y)}{\forall y.p(x',y) \vdash p(x',y')}\;\forall E}{\forall y.p(x',y) \vdash \exists x.p(x,y')}\;\exists I}{\forall y.p(x',y) \vdash \forall y.\exists x.p(x,y)}\;\forall I}{\exists x.\forall y.p(x,y) \vdash \forall y.\exists x.p(x,y)}\;\exists E}{\vdash (\exists x.\forall y.p(x,y)) \Rightarrow (\forall y.\exists x.p(x,y))}\;\Rightarrow I$$