Matematička logika u računarstvu

Slavko Moconja

2024/25.

1. čas

2. čas

3. čas

4. čas

5. čas

6. čas

7. čas

8. čas

Jezik i formule iskazne logike

Jezik iskazne logike:

- iskazna slova: $p, q, r, \ldots, p_0, p_1, p_2, \ldots$;
- logičke konstante: $\bot$ i $\top$;
- logički veznici: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \veebar$;
- pomoćni simboli zagrada.

Formule iskazne logike:

- slova i konstante su formule;
- ako su φ i ψ formule, to su i $\neg\varphi$ i $(\varphi * \psi)$, za bilo koji binarni veznik $*$;
- formule se grade u konačno mnogo koraka pomoću prethodna dva pravila.

Oznake:

- $\mathcal{P}$ – skup slova;
- $\mathcal{F}$ – skup formula;
- $\mathcal{P}_\varphi$ – konačan skup slova u formuli φ.

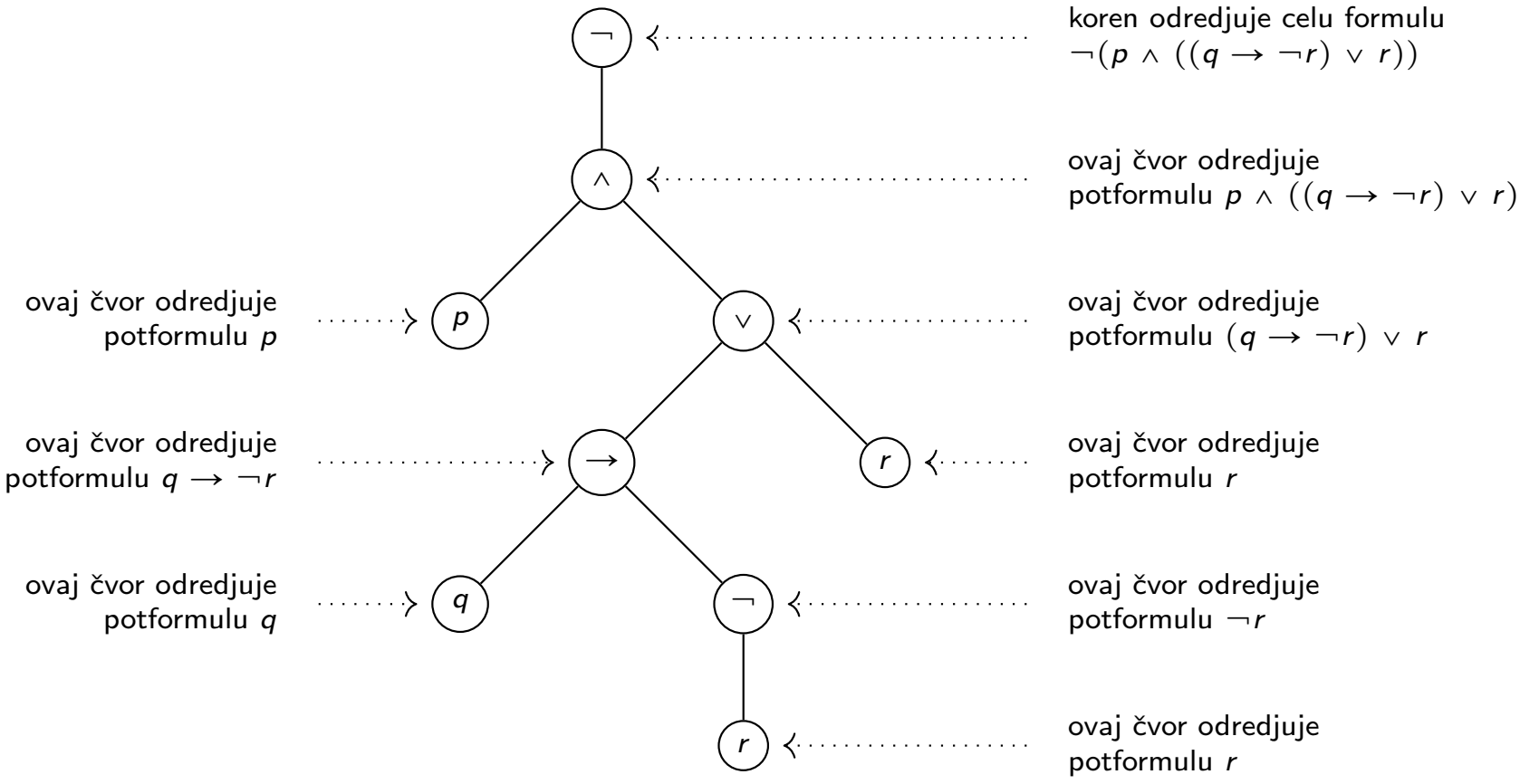
Prioritet veznika u brisanju zagrada:

- $\neg$: najviši;
- $\wedge$ i $\vee$: srednji;
- $\rightarrow$, $\leftrightarrow$ i $\veebar$: najniži.

Složenost, potformula i drvo formule

Složenost formule φ, $\mathrm{sl}(\varphi)$, je broj veznika u φ.

Komentar. Dužina formule složenosti n je najviše $4n + 1$.



Semantika iskazne logike: valuacije i tačnost u valuaciji

$0 =$ netačno, $1 =$ tačno.

Valuacija je preslikavanje $v : \mathcal{P} \to \{0, 1\}$.

Tačnost formule φ u valuaciji v, $\varphi[v]$, definišemo rekurzijom po složenosti:

- $\bot[v] \stackrel{def}{=} 0$, $\top[v] \stackrel{def}{=} 1$, i $p[v] \stackrel{def}{=} v(p)$ za $p \in \mathcal{P}$;
- $(\neg\varphi)[v] = 1 \stackrel{def}{\iff} \varphi[v] = 0$;
- $(\varphi \wedge \psi)[v] = 1 \stackrel{def}{\iff} \varphi[v] = 1$ i $\psi[v] = 1$;
- $(\varphi \vee \psi)[v] = 1 \stackrel{def}{\iff} \varphi[v] = 1$ ili $\psi[v] = 1$;
- $(\varphi \to \psi)[v] = 1 \stackrel{def}{\iff} \varphi[v] = 0$ ili $\psi[v] = 1$;
- $(\varphi \leftrightarrow \psi)[v] = 1 \stackrel{def}{\iff} \varphi[v] = \psi[v]$;
- $(\varphi \veebar \psi)[v] = 1 \stackrel{def}{\iff} \varphi[v] \neq \psi[v]$.

Teorema. Vrednost $\varphi[v]$ zavisi samo od $v|_{\mathcal{P}_\varphi}$.

Dokaz. Indukcijom po složenosti formule φ.

Relacija zadovoljivosti, logička posledica

- v *zadovoljava* φ ili v *je model za* φ, $v \models \varphi$, ako $\varphi[v] = 1$;
- $\mathrm{Mod}(\varphi) = \{v : \mathcal{P}_\varphi \to \{0,1\} \mid v \models \varphi\}$;
- v *poriče* φ ili v *je kontramodel za* φ, $v \not\models \varphi$, ako $\varphi[v] = 0$;
- φ je *zadovoljiva* ako postoji v koja je zadovojava; u suprotnom, φ je *kontradikcija*;
- φ je *poreciva* ako postoji v koja je poriče; u suprotnom, φ je *tautologija*.

- ψ je *logička posledica* od φ, $\varphi \models \psi$, ako $(\forall v)(v \models \varphi \Rightarrow v \models \psi)$;
- φ i ψ su *logički ekvivalentne*, $\varphi \equiv \psi$, ako $(\forall v)(v \models \varphi \Leftrightarrow v \models \psi)$;
- φ i ψ su *ekvizadovoljive* ako

$$\varphi \text{ je zadovoljiva} \Leftrightarrow \psi \text{ je zadovoljiva.}$$

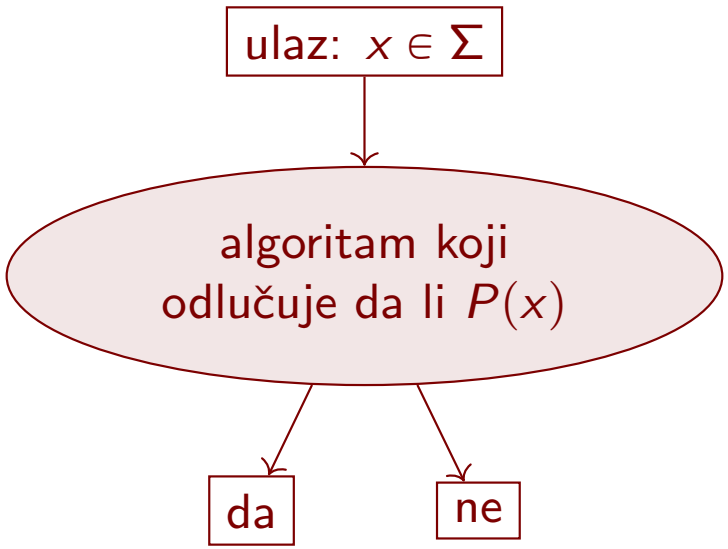
Tvrdjenje.

1. $\varphi \models \psi$ ako i samo ako $\models \varphi \to \psi$;
2. $\varphi \equiv \psi$ ako i samo ako $\varphi \models \psi$ i $\psi \models \varphi$ ako i samo ako $\models \varphi \leftrightarrow \psi$.

Problemi odlučivanja

Neka su $P \subseteq \Sigma$ prebrojivi skupovi (P je unaran predikat na skupu Σ).
Par (Σ, P) zovemo *problem odlučivanja*.

Problem (Σ, P) je *odlučiv* ako postoji algoritam koji za ulaz $x \in \Sigma$ korektno daje odgovor na pitanje ,,Da li važi $P(x)$ (tj. $x \in P$)?".



(Stroge definicije sledećeg semestra u Teoriji algoritama.)

Problem zadovoljivosti (SAT)

Problem zadovoljivosti je par $(\mathcal{F}, SAT)$, ili, kraće, samo SAT, gde je $SAT \subseteq \mathcal{F}$ skup zadovoljivih formula, tj. problem zadovoljivosti je pitanje da li je formula na ulazu zadovoljiva ili ne.

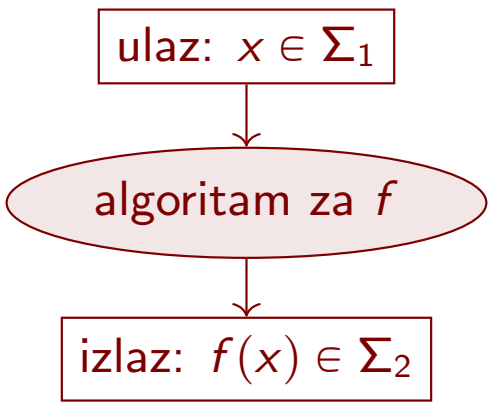
Teorema. Problem zadovoljivosti je odlučiv.

Dokaz. Sledeći algoritam odlučuje problem zadovoljivosti: Za ulaznu formulu φ računamo njenu tačnost u svim valuacija njenih slova (drugim rečima, formiramo istinitosnu tablicu formule φ). Ako je $\varphi[v] = 1$ za neku v, vraćamo ,,da"; u suprotnom, vraćamo ,,ne".

Svodjenje

Svodjenje problema (Σ_1, P_1) na problem (Σ_2, P_2) je funkcija $f : \Sigma_1 \to \Sigma_2$ koja zadovoljava $(\forall x \in \Sigma_1)(\ P_1(x) \Leftrightarrow P_2(f(x))\ )$.

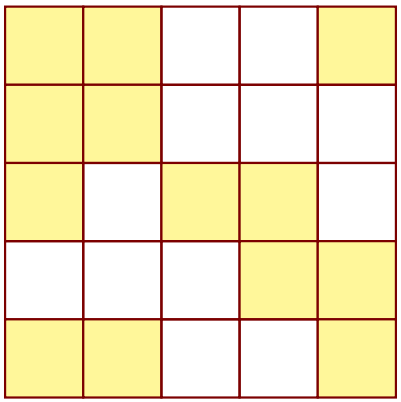
Problem (Σ_1, P_1) se *efektivno svodi* na (Σ_2, P_2), $(\Sigma_1, P_1) \leqslant (\Sigma_2, P_2)$, ako postoji svodjenje f i algoritam koji za ulaz $x \in \Sigma_1$ vraća $f(x)$.



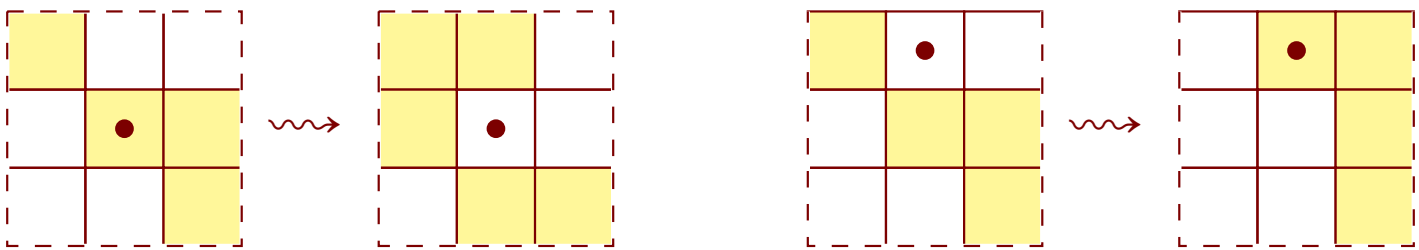
Teorema. Ako $(\Sigma_1, P_1) \leqslant (\Sigma_2, P_2)$ i (Σ_2, P_2) je odlučiv, onda je i (Σ_1, P_1) odlučiv.

Svodjenje na SAT: Lights Out I

Data nam je tabla $m \times n$ na kojoj je svako polje obojeno belo ili žuto (ako je polje žuto zamišljamo da je svetlo u tom polju upaljeno).



U svakom koraku možemo da promenimo boju bilo kog polja, ali takav potez automatski menja boje i u svim susednim poljima (susedna su polja iznad, ispod, levo i desno, ako postoje).



Zadatak je da pogasimo sva svetla.

Svodjenje na SAT: Lights Out II

Primetimo:

- svaki potez je involucija (sam je sebi inverz);
- potezi komutiraju;
- dakle, ako postoji rešenje, onda postoji rešenje u kome smo svaki potez odigrali najviše jednom.

- Uvedimo slova p_{ij}, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$.
- Svaka valuacija v ovih slova odgovara igri koju možemo da odigramo:

$$v(p_{ij}) = 1 \Leftrightarrow \text{igramo potez na polju } (i, j).$$

- Pri ovoj korespodenciji, valuacija v je rešenje problema ako su posle njenog igranja sva polja pogašena.

Svodjenje na SAT: Lights Out III

Neka je ulaz m, n i 0/1-matrica A tipa $m \times n$, gde 0 u polju znači da je svetlo ugašeno, a 1 da je svetlo upaljeno. Neka je v potencijalno rešenje.

- Ako je svetlo u polju (i, j) ugašeno, igrajući igru ono će na kraju biti ugašeno akko ga palimo/gasimo parno mnogo puta, tj.:

$$\underbrace{\neg(p_{i-1,j} \veebar p_{i,j-1} \veebar p_{i,j} \veebar p_{i,j+1} \veebar p_{i+1,j})}_{\theta_{ij}}[v] = 1;$$

- ako je svetlo u polju (i, j) upaljeno, igrajući igru će na kraju biti ugašeno akko ga palimo/gasimo neparno mnogo puta, tj.:

$$\underbrace{(p_{i-1,j} \veebar p_{i,j-1} \veebar p_{i,j} \veebar p_{i,j+1} \veebar p_{i+1,j})}_{\theta_{ij}}[v] = 1.$$

  (Ako neko od susednih polja ne postoji, njemu dodeljeno slovo ne učestvuje u ekskluzivnoj disjunkciji.)

- Dakle, v je rešenje akko $v \models \bigwedge_{ij} \theta_{ij}$.
- Prema tome, rešenje postoji akko $\bigwedge_{ij} \theta_{ij}$ je zadovoljiva.

Ovime smo opisali algoritam svodjenja postavke igre na SAT.

Svodjenje na SAT: ± 1 I

Problem sa codeforces.com.

Ana i Bane igraju sledeću igru.

- Ana bira broj n i matricu A tipa $3 \times n$ čiji su svi unosi oblika x_i ili $-x_i$, gde $1 \leqslant i \leqslant n$.
- Bane dodeljuje svakom x_i vrednost 1 ili -1, i sračuna datu matricu.
- Ana sortira u neopadajućem poretku svaku kolonu.
- Bane je pobedio ako su u srednjoj koloni sve jedinice.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -1 & 1 & 1 & -1 \end{pmatrix}$$

$$\begin{bmatrix} -x_4 & -x_1 & x_2 & -x_3 \\ x_1 & x_3 & x_3 & -x_4 \\ x_3 & -x_2 & x_4 & x_3 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \overset{\text{sortiranje}}{\rightsquigarrow} \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Pitanje: Da li za Anin unos Bane može da pobedi?

Svodjenje na SAT: ± 1 II

- Uvedimo slova p_i, $1 \leqslant i \leqslant n$.
- Valuacija ovih slova v odgovara valuaciji promenljivih x_i sa $x_i = (-1)^{v(p_i)}$.
- Primetimo $(-1)^e x_i = (-1)^{e+v(p_i)} = (-1)^{\neg p_i^e[v]}$, gde $p_i^1 \stackrel{def}{=} p_i$ i $p_i^0 \stackrel{def}{=} \neg p_i$.
- Valuacija daje rešenje problema akko za svaku kolonu račun kolone daje najviše jednu -1.
- Kolona $K_m = \begin{bmatrix}(-1)^a x_i & (-1)^b x_j & (-1)^c x_k\end{bmatrix}^T$ sadrži najviše jednu -1 akko $\{\neg p_i^a[v], \neg p_j^b[v], \neg p_k^c[v]\}$ sadrži najviše jednu 1 akko

$$v \models \underbrace{(p_i^a \vee p_j^b) \wedge (p_i^a \vee p_k^c) \wedge (p_j^b \vee p_k^c)}_{\theta_m}.$$

- v je rešenje akko $v \models \bigwedge_m \theta_m$.
- Rešenje postoji akko $\models \bigwedge_m \theta_m$ je zadovoljiva.

Opisali smo algoritam svodjenja postavke na SAT.

Zadaci

Svesti sledeće probleme na SAT:

1. Za date formule φ i ψ, da li $\varphi \models \psi$?
2. Za date formule φ i ψ, da li $\varphi \equiv \psi$?
3. Da li data sudoku postavka ima rešenje?
4. Da li se čvorovi datog neusmerenog graf mogu obojiti u $k \geqslant 2$ boja tako da su susedni čvorovi obojeni različitim bojama?
5. Da li dati usmeren graf sadrži ciklus?

Odlučivost i svodjenje u polinomijalnom vremenu

Klasa P. Problem odlučivanja (Σ, P) je u klasi P ako postoji polinom p i algoritam koji za ulaz $x \in \Sigma$ odlučuje $x \in P$ u najviše $p(|x|)$ koraka, gde je $|x|$ je veličina ulaza x.

Problem (Σ_1, P_1) se svodi u polinomijalnom vremenu na (Σ_2, P_2), $(\Sigma_1, P_1) \leqslant_P (\Sigma_2, P_2)$ ako postoji svodjenje f, polinom p i algoritam koji za ulaz $x \in \Sigma_1$ vraća $f(x)$ u najviše $f(|x|)$ koraka.

Normalne forme

- *Literal* je slovo (*pozitivan literal*) ili negacija slova (*negativan literal*).
- *Klauza* je disjunkcija literala.
- $\wedge$-*klauza* je konjunkcija literala.
- Formula je u *KNF* ako je konjunkcija klauza.
- Formula je u *DNF* ako je disjunkcija $\wedge$-klauza.

Tvrdjenje.

1. Svaka formula je ekvivalentna nekoj u KNF i DNF.
2. (KDNF) Ako $\mathcal{P}_\varphi = \{p_1, p_2, \ldots, p_n\}$, onda $\varphi \equiv \bigvee_{\{v \mid v \models \varphi\}} \bigwedge_{i=1}^{n} p_i^{v(p_i)}$.
3. (KKNF) Ako $\mathcal{P}_\varphi = \{p_1, p_2, \ldots, p_n\}$, onda $\varphi \equiv \bigwedge_{\{v \mid v \not\models \varphi\}} \bigvee_{i=1}^{n} p_i^{\neg v(p_i)}$.

KNF-SAT

Problem KNF-SAT. Za datu formulu φ u KNF na ulazu odrediti da li je φ zadovoljiva.

Ubuduće pod SAT podrazumevamo KNF-SAT.

Teorema (Kuk). SAT je NP-potpun.

Posledica. Ako je P$\neq$NP, SAT nije odlučiv u polinomijalnom vremenu (i obratno).

DNF-SAT

Problem DNF-SAT. Za datu formulu φ u DNF na ulazu odrediti da li je φ zadovoljiva.

Teorema. DNF-SAT je u P.

Dokaz.

Formula $\varphi = \bigvee \theta_i$ je zadovoljiva akko θ_i je zadovoljiva za neko i, akko θ_i ne sadrži konfliktne literale (literale oblika p i $\neg p$ za neko slovo p) za neko i. Ovo možemo proveriti u $O(\mathrm{sl}(\varphi))$ koraka. □

Tvrdjenje. DNF formule nije izračunljiv u polinomijalnom vremenu.

Dokaz.

Može se pokazati da bilo koji DNF formule $\varphi = \bigwedge_{i=1}^{n}(p_i^1 \vee p_i^2)$, gde su sva slova različita, ima bar 2^n disjunkata.

$$\varphi \equiv \bigvee_{\eta \in \{1,2\}^n} \bigwedge_{j=1}^{n} p_j^{\eta(j)}.$$

□

XOR-SAT

XOR-KNF. Formula je u XOR-KNF ako je konjunkcija XOR-klauza, tj. ekskluzivna disjunkcija literala.

Problem XOR-SAT. Za datu formulu φ u XOR-KNF na ulazu odrediti da li je φ zadovoljiva.

Teorema. XOR-SAT je u P.

Dokaz.

Kako je $(\ldots \veebar \neg p \veebar \ldots) \equiv \neg(\ldots \veebar p \veebar \ldots)$, XOR-klauza je ekvivalentna ili sa θ ili sa $\neg\theta$, gde je θ ekskluzivna disjunkcija slova.

$v \models \theta = \bigveebar p_i$ akko v odredjuje rešenje jednačine $\sum p_i = 1$ nad $\mathbb{Z}_2$, a $v \models \neg\theta$ akko v odredjuje jednačine $\sum p_i = 0$ nad $\mathbb{Z}_2$. Dakle, formula u XOR-KNF je zadovoljiva akko dodeljen sistem jednačina ima rešenje nad $\mathbb{Z}_2$.

Poslednje je rešivo u polinomijalnom vremenu Gausovom eliminacijom. $\square$

HORN-SAT I

HORN-KNF. Hornova klauza je disjunkcija literala u kojoj je najviše jedan literal pozitivan. Formula je u HORN-KNF ako je konjunkcija Hornovih klauza.

Problem HORN-SAT. Za datu formulu φ u HORN-KNF na ulazu odrediti da li je φ zadovoljiva.

Teorema. HORN-SAT je u P.

Zapišimo Hornove klauze u sledećem obliku:

- $\neg p_1 \vee \ldots \neg p_n \vee q \equiv p_1 \wedge \cdots \wedge p_n \rightarrow q$, gde $n \geqslant 1$;
- $\neg p_1 \vee \cdots \vee \neg p_n \equiv p_1 \wedge \cdots \wedge p_n \rightarrow \bot$, gde $n \geqslant 1$;
- $q \equiv \top \rightarrow q$.

HORN-SAT II

Algoritam.

ulaz je Hornova formula φ
postavi $v :\equiv 0$
dok $\varphi[v] = 0$:
  izaberi klauzu $\theta = \bigwedge p_i \to q$ za koju $\theta[v] = 0$
  ako je q slovo:
    postavi $v(q) := 1$
  inače (ako je $q = \bot$):
    vrati „φ nije zadovoljiva”
vrati „φ je zadovoljiva” (i v je valuacija koja je zadovoljava)

Dokaz korektnosti: (tabla).

Svodjenje na HORN-SAT: Postojanje direktnog puta

Problem. Za dati usmereni graf G i dva čvora x i y odrediti da li postoji usmereni put od x do y.

Uvedimo slova $p_{a,b}$ za $a, b \in G$. Značenje slova $p_{a,b}$ je ,,od a do b postoji usmeren put".

Uočimo formulu:

$$\varphi = \bigwedge_{\substack{a,b \in G \\ a \to b}} p_{a,b} \wedge \bigwedge_{a,b,c \in G} (p_{a,b} \wedge p_{b,c} \to p_{a,c}) \wedge \neg p_{x,y}.$$

Od x do y postoji usmereni put akko φ nije zadovoljiva. (Dokaz na tabli.)

Prethodna analiza pokazuje da se odlučivanje gornjeg problema svodi na (komplement) HORN-SAT u polinomijalnom vremenu.

Posledica. Gornji problem je u P.

2SAT I

2KNF. Formula je u 2KNF ako je konjunkcija najviše dvočlanih klauza.

Problem 2SAT. Za datu formulu φ u 2KNF na ulazu odrediti da li je φ zadovoljiva.

Teorema. 2SAT je u P.

Pretpostavimo da su sve klauze dvočlane: ako je l jedna klauza, zapišemo je kao $l \vee l$.

Neka su $\{p_1, \ldots, p_n\}$ slova u φ. Na skupu čvorova $\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ formiramo graf na sledeći način: Za klauzu $l_1 \vee l_2$ dodamo strelice $\bar{l}_1 \to l_2$ i $\bar{l}_2 \to l_1$, gde je

$$\bar{l} = \begin{cases} \neg p & \text{ako je } l = p \text{ slovo} \\ p & \text{ako je } l = \neg p \text{ negacija slova} \end{cases}$$

Primetimo $l_1 \vee l_2 \equiv \bar{l}_1 \to l_2 \equiv \bar{l}_2 \to l_1$.
Dakle, ako $v \models \varphi$ i u grafu $a \to b$, onda $a[v] \leqslant b[v]$.

2SAT II

Neka $a \dashrightarrow b$ znači da od a do b postoji usmereni put.

Formula φ je zadovoljiva akko $(\forall i)\neg(p_i \dashrightarrow \neg p_i \wedge \neg p_i \dashrightarrow p_i)$.
(Dokaz na tabli.)

Ovo dokazuje da je 2SAT u P.

3KNF. Formula je u 3KNF ako je konjunkcija najviše tročlanih klauza.

Problem 3SAT. Za datu formulu φ u 3KNF na ulazu odrediti da li je φ zadovoljiva.

Teorema. 3SAT je NP-potpun.

Dokaz.

Imamo SAT $\leqslant_P$ 3SAT: Za klauzu $l_1 \vee \cdots \vee l_n$, $n > 3$, uvedemo nova slova $q_1, \ldots, q_{n-3}$, i dodelimo joj konjunkciju klauza:

$$(l_1 \vee l_2 \vee q_1) \wedge (\neg q_1 \vee l_3 \vee q_2) \wedge (\neg q_2 \vee l_4 \vee q_3) \wedge \cdots \wedge (\neg q_{n-3} \vee l_{n-1} \vee l_n).$$

Primetimo da svodimo formulu na ekvizadovoljivu formulu. □

Cejtinova transformacija I

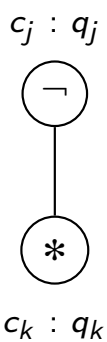
φ – formula nad slovima $\mathcal{P}_\varphi = \{p_0, p_1, \ldots, p_n\}$

Uočimo drvo formule φ. Neka su $c_0, c_1, \ldots, c_m$ čvorovi drveta koji nisu lišće (tj. svaki od c_j je označen logičkim veznikom), gde je c_0 koren drveta.

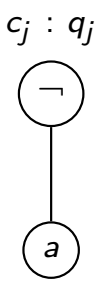
Svakom c_j dodelimo *novo* slovo q_j.

Formuli φ pridružujemo njenu *Cejtinovu formulu* φ_C nad slovima $\{p_0, p_1, \ldots, p_n, q_0, q_1, \ldots, q_m\}$ na sledeći način.

Za čvor c_j, ako je c_j označen negacijom ($\neg$) imamo da je njegov naslednik ili neki od preostalih čvorova c_k (označen nekim veznikom $*$) ili je list označen sa a, gde je a neko od slova p_l ili neka konstanta $\bot$ ili $\top$.



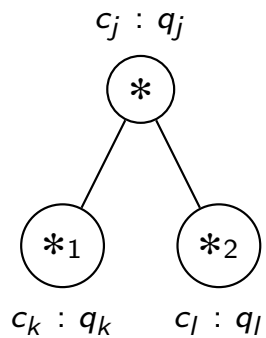
$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow \neg q_k$$



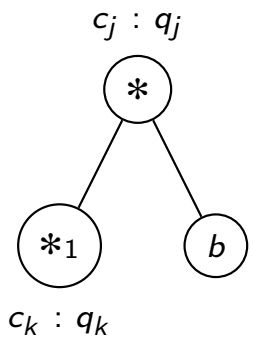
$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow \neg a$$

Cejtinova transformacija II

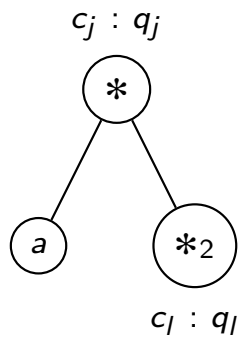
Ako je c_j označen nekim binarnim veznikom $*$, onda c_j ima dva naslednika od kojih svaki može da bude ili neki od čvorova c_k ili neki list.



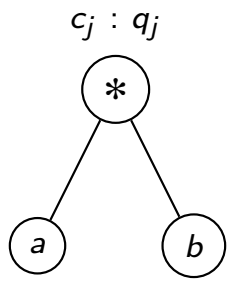
$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow (q_k * q_l)$$



$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow (q_k * b)$$



$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow (a * q_l)$$



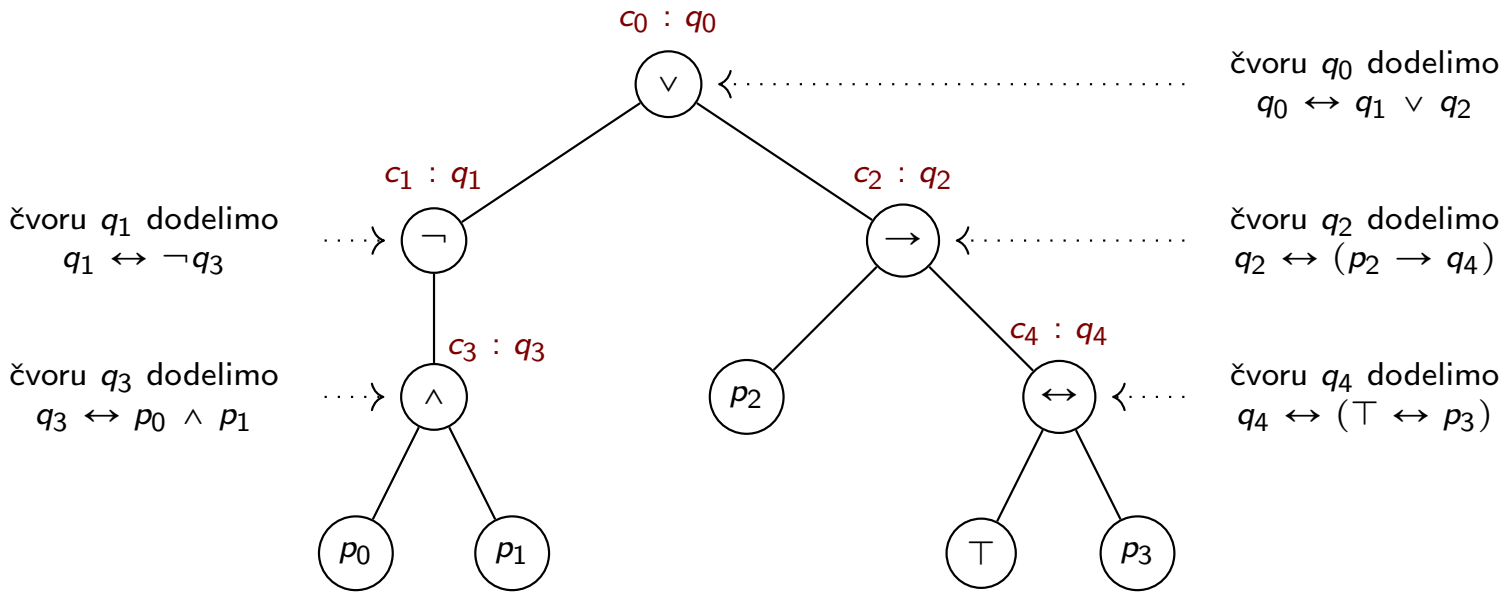
$$\gamma_j \stackrel{def}{=} q_j \leftrightarrow (a * b)$$

Cejtinovu formulu φ_C definišemo da bude:

$$\varphi_C \stackrel{def}{=} q_0 \wedge \bigwedge_{j=0}^{m} \gamma_j.$$

Cejtinova transformacija III

$\varphi = \neg(p_0 \wedge p_1) \vee (p_2 \rightarrow (\top \leftrightarrow p_3))$:



Pridružena Cejtinova formula φ_C sad je konjunkcija formula
q_0, $q_0 \leftrightarrow q_1 \vee q_2$, $q_1 \leftrightarrow \neg q_3$, $q_2 \leftrightarrow (p_2 \rightarrow q_4)$, $q_3 \leftrightarrow p_0 \wedge p_1$ i $q_4 \leftrightarrow (\top \leftrightarrow p_3)$.

Cejtinova transformacija IV

Teorema. Neka je φ formula nad $\mathcal{P}_\varphi$, i neka je φ_C Cejtinova formula pridružena φ nad slovima $\mathcal{P}_{\varphi_C} = \mathcal{P}_\varphi \cup \mathcal{Q}$. Preslikavanje:

$$r : \mathrm{Mod}(\varphi_C) \to \mathrm{Mod}(\varphi)$$

dato restrikcijom (za $v \in \mathrm{Mod}(\varphi_C)$, $r(v) = v|_{\mathcal{P}_\varphi}$) je dobro definisana bijekcija.

(Dokaz na tabli.)

$$\begin{aligned}
p \leftrightarrow \neg q &\equiv (p \vee q) \wedge (\neg p \vee \neg q);\\
p \leftrightarrow q \wedge r &\equiv (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q) \wedge (\neg p \vee r);\\
p \leftrightarrow q \vee r &\equiv (p \vee \neg q) \wedge (p \vee \neg r) \wedge (\neg p \vee q \vee r);\\
p \leftrightarrow (q \to r) &\equiv (p \vee q) \wedge (p \vee \neg r) \wedge (\neg p \vee \neg q \vee r);\\
p \leftrightarrow (q \leftrightarrow r) &\equiv (p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge\\
&\quad (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r);\\
p \leftrightarrow (q \veebar r) &\equiv (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge\\
&\quad (p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee \neg r).
\end{aligned}$$

Dakle, Cejtinova transformacija svodi originalni SAT na 3SAT u polinomijalnom vremenu.

Rezolucija I

- Posmatramo formule u KNF;
- klauzu zapisujemo kao skup literala;
- formulu zapisujemo kao skup klauza;
- primetimo, za klauzu γ, $v \models \gamma \Leftrightarrow (\exists \ell \in C)\ v \models \ell$;
- specijalno, prazna klauza je kontradikcija;
- pisaćemo $\square$ sa praznu klauzu;
- primetimo, za formulu φ, $v \models \varphi \Leftrightarrow (\forall C \in \varphi)\ v \models C$;
- specijalno, prazna formula je tautologija.

Zloupotreba notacije:

- $C' = C\ell$ znači $C' = C \cup \{\ell\}$;
- $C' = C \setminus \ell$ znači $C' = C \setminus \{\ell\}$;
- $\varphi' = \varphi C$ znači $\varphi' = \varphi \cup \{C\}$;
- $\varphi' = \varphi \setminus C$ znači $\varphi' = \varphi \setminus \{C\}$;
- i sl.

Rezolucija II

Resolventa. Ako su C_1 i C_2 klauze i p slovo, *resolventa* klauza C_1 i C_2 u odnosu na p je klauza:

$$Res(C_1, C_2; p) = (C_1 \setminus p)(C_2 \setminus \neg p).$$

Pravilo rezolucije. Ako su C_1 i C_2 klauze i p slovo:

$$\frac{C_1 \qquad C_2}{Res(C_1, C_2; p)}.$$

Lema o saglasnosti pravila rezolucije.

Ako $v \models C_1$ i $v \models C_2$, onda $v \models Res(C_1, C_2; p)$.

(Dokaz na tabli.)

Rezolucija III

Dokaz klauze u rezoluciji. Klauza C je *posledica* formule φ *u rezoluciji*, $\varphi \vdash_{\text{Res}} C$, ako postoji niz klauza $C_1, C_2, \ldots, C_n$ takav da $C_n = C$ i za svako $i \leqslant n$ važi:

- $C_i \in \varphi$ (C_i je premisa) ili
- $C_i = Res(C_j, C_k; p)$ za neke $j, k < i$ i slovo p.

Svaki takav niz je *dokaz u rezoluciji* za $\varphi \vdash_{\text{Res}} C$.

Primer.

$\neg pq, \neg q\neg r, p\neg r \vdash_{\text{Res}} \neg r$

1.	$\neg pq$	premisa
2.	$\neg q\neg r$	premisa
3.	$p\neg r$	premisa
4.	$\neg p\neg r$	$Res(1, 2; q)$
5.	$\neg r$	$Res(3, 4; p)$

$p\neg q, q\neg r, \neg p, qrs, \neg s \vdash_{\text{Res}} \square$

1.	$p\neg q$	premisa
2.	$q\neg r$	premisa
3.	$\neg p$	premisa
4.	qrs	premisa
5.	$\neg s$	premisa
6.	$\neg q$	$Res(1, 3; p)$
7.	qs	$Res(4, 2; r)$
8.	q	$Res(7, 5; s)$
9.	$\square$	$Res(8, 6; q)$

Rezolucija IV

Lema. Ako $\varphi, C \vdash_{\text{Res}} D$, onda $\varphi, C\ell \vdash_{\text{Res}} D$ ili $\varphi, C\ell \vdash_{\text{Res}} D\ell$.

(Dokaz na tabli.)

Složenost.

- za klauzu C, $\text{sl}(C) = |C| - 1 =$ broj simbola $\vee$ u C;
- za formulu φ, $\text{sl}(\varphi) = \sum_{C \in \varphi} \text{sl}(C)$.

Teorema potpunosti za rezoluciju.

φ je zadovoljiva ako i samo ako $\varphi \nvdash_{\text{Res}} \square$.

(Dokaz na tabli.)

Problem bijekcije I

$[n] = \{1, 2, \ldots, n\}$

Neka su $p_{i,j}$, $i \in [n]$ i $j \in [n-1]$, slova. Imamo korespondenciju:

$$\begin{array}{ccc} \text{valuacija slova } p_{i,j} & \leftrightsquigarrow & \text{relacije iz } [n] \text{ u } [n-1] \\ \hline v & \rightsquigarrow & R_v(i,j) \overset{def}{\iff} v \models p_{i,j} \\ v_R \models p_{i,j} \overset{def}{\iff} R(i,j) & \leftsquigarrow & R \end{array}$$

Neka je κ_n formula:

$$\bigwedge_{i=1}^{n} \bigwedge_{1 \leqslant j_1 < j_2 < n} (\neg p_{i,j_1} \vee \neg p_{i,j_2}) \wedge \bigwedge_{1 \leqslant i_1 < i_2 \leqslant n} \bigwedge_{j=1}^{n} (\neg p_{i_1,j} \vee \neg p_{i_2,j}) \wedge \bigwedge_{j=1}^{n-1} \bigvee_{i=1}^{n} p_{i,j}.$$

Primetimo: $v \models \kappa_n$ akko $R_v : [n] \to [n-1]$ je parcijalna bijekcija (specijalno, za jedinstveno $i \in [n]$, $R_v(i) \uparrow$).

Problem bijekcije II

Neka su:

$$C_{n,i} \stackrel{def}{=} \bigvee_{j=1}^{n-1} p_{i,j}, \text{ za } i \in [n], \text{ i } \psi_I \stackrel{def}{=} \bigwedge_{i \in I} C_{n,i}, \text{ za } I \subseteq [n].$$

Primetimo: za $v \models \kappa_n$, $v \models C_{n,i}$ akko $R_v(i) \downarrow$, i $v \models \psi_I$ akko $R_v(i) \downarrow$ za sve $i \in I$.

Kako ne postoji bijekcija $[n] \to [n-1]$, $\kappa_n, \psi_{[n]} \models \bot$, pa $\kappa_n, \psi_{[n]} \vdash_{\mathsf{Res}} \square$.

Pitanje. Kolika je dužina dokaza za $\kappa_n, \psi_{[n]} \vdash_{\mathsf{Res}} \square$?

Teorema. Postoji konstanta $c > 0$ takva da je svaki dokaz za $\kappa_n, \psi_{[n]} \vdash_{\mathsf{Res}} \square$ dužine bar 2^{cn}.

Problem bijekcije III

Za klauzu D, neka je $w(D)$ – *širina od* D, broj:

$$w(D) = \min\{|I| : I \subseteq [n],\ \kappa_n, \psi_I \models D\}.$$

Primetimo: $w(D) \leqslant n$ i $w(\square) = n$.

Niz *pozitivnih* klauza $D_1, \ldots, D_m$ je *pseudodokaz* za $\kappa_n, \psi_{[n]} \models \square$ ako je $D_m = \square$ i za sve $k \leqslant m$ važi:

- $\kappa_n, C_{n,i} \models D_k$ za neko $i \in [n]$; ili
- $\kappa_n, D_s, D_t \models D_k$ za neke $s, t < k$.

Ako je D_k dobijena koristeći prvo pravilo: $w(D_k) \leqslant 1$; ako je D_k dobijane koristeći drugo pravilo: $w(D_k) \leqslant w(D_s) + w(D_t)$.

Problem bijekcije IV

Za klauzu D, označimo sa $\widehat{D}$ pozitivnu klauzu dobijenu od D tako što svaki litearal $\neg p_{i,j}$ u D zamenimo sa $\bigvee_{i' \neq i} p_{i',j}$.

Lema.

1. Za sve klauze D važi $\kappa_n \models D \leftrightarrow \widehat{D}$.
2. Ako je $D_1, \ldots, D_m$ dokaz za $\kappa_n, \psi_{[n]} \vdash_{\mathsf{Res}} \square$, onda je $\widehat{D}_1, \ldots, \widehat{D}_m$ pseudodokaz za $\kappa_n, \psi_{[n]} \models \square$.

Posledica. Dovoljno je da nadjemo donje ograničenje za dužine pseudodokaza.

Problem bijekcije V

Lema. U svakom pseudodokazu postoji klauza sa bar $\frac{n^2}{8}$ literala.

Lema. Neka je $D_1, \ldots, D_m$ pseudodokaz za $\kappa_n, \psi_{[n]} \models \square$. Uradimo sledeće:

- ako $p_{n,n-1} \in D_k$, obrišemo D_k;
- ako $p_{n,j} \in D_k$, gde $j < n-1$, obrišemo $p_{n,j}$ iz D_k;
- ako $p_{i,n-1} \in D_k$, gde $i < n$, obrišemo $p_{i,n-1}$ iz D_k.

Dobijeni niz je pseudodokaz za $\kappa_{n-1}, \psi_{[n-1]} \models \square$.

Dokaz teoreme. ...

DPLL algoritam I

Davis–Putnam–Logemann–Loveland

Neka je φ formula u KNF i v parcijalna valuacija. Označimo sa $\varphi|_v$ formulu dobijenu na sledeći način:

- ako klauza $C \in \varphi$ sadrži literal ℓ za koji $v \models \ell$, obrišemo klauzu C;
- ako klauza $C \in \varphi$ sadrži literal ℓ za koji $v \not\models \ell$, obrišemo ℓ iz C.

Lema. $\varphi|_v$ je zadovoljiva akko v se može proširiti do $v' \models \varphi$.

DPLL algoritam II

Algoritam DPLL.

Ulaz: φ u KNF

Funkcija $DPLL(\varphi)$:

- $v = \varnothing$
- dok φ sadrži jednočlanu klauzu $\{\ell\}$
  - $v = v \cup \{\ell \to 1\}$
  - $\varphi = \varphi|_v$
  - ako $\varphi|_v = \varnothing$, vrati **TRUE**
  - ako $\square \in \varphi|_v$, vrati **FALSE**
- dok φ sadrži monoton literal ℓ
  - $v = v \cup \{\ell \to 1\}$
  - $\varphi = \varphi|_v$
  - ako $\varphi|_v = \varnothing$, vrati **TRUE**
- izaberi literal ℓ koji se pojavljuje u φ i vrati

$$DPLL(\varphi, \{\ell\}) \vee DPLL(\varphi, \{\neg\ell\}).$$

ℓ je *monoton* u φ ako se φ pojavljuje u φ, i $\bar{\ell}$ se ne pojavljuje u φ.

Teorema kompaktnosti

Skup formula Σ je:

- *zadovoljiv* ako $(\exists v)(\forall \sigma \in \Sigma)\ v \models \sigma$;
- *konačno zadovoljiv* ako $(\forall \Sigma_0 \underset{kon.}{\subseteq} \Sigma)\ \Sigma_0$ je zadovoljiv;
- *zatvoren za slova* ako $(\forall p \in \mathcal{P})(p \in \Sigma \vee \neg p \in \Sigma)$.

Lema 1. Neka je Σ k.z. i $\varphi \in \mathcal{F}$. Tada je bar jedan od $\Sigma \cup \{\varphi\}$ i $\Sigma \cup \{\neg\varphi\}$ k.z.

Lema 2. Neka je $(\Sigma_i)_{i \in I}$ lanac (za sve $i, j \in I$ važi $\Sigma_i \subseteq \Sigma_j$ ili $\Sigma_j \subseteq \Sigma_i$) k.z. skupova. Tada je $\Sigma^* = \bigcup_{i \in I} \Sigma_n$ k.z.

Hauzdorfov princip maksimalnosti (Aksioma izbora). Svako parcijalno uredjenje ima maksimalan lanac.

Lema 3. Ako je Σ k.z. skup, onda postoji k.z. skup Σ^* takav da $\Sigma \subseteq \Sigma^*$ i Σ^* je zatvoren za slova.

Lema 4. Ako je Σ k.z. i zatvoren za slova, onda je Σ zadovoljiv.

Teorema kompaktnosti. Σ je zadovoljiv ako i samo ako Σ je k.z.

Sintaksa logike prvog reda I

Jezik logike prvog reda:

- jezik prvog reda $\mathcal{L}$ čine:
  - *simboli konstanti* $\mathrm{Const}_{\mathcal{L}}$;
  - *funkcijski simboli* $\mathrm{Fun}_{\mathcal{L}}$;
  - *relacijski simboli* $\mathrm{Rel}_{\mathcal{L}}$;
  - *funkcija arnosti*: $\mathrm{ar} : \mathrm{Fun}_{\mathcal{L}} \cup \mathrm{Rel}_{\mathcal{L}} \to \mathbb{N}^{+}$;
- *promenljive* Var;
- logičke konstante i veznici;
- *kvanitifikatori* $\exists$ i $\forall$;
- znak jednakosti $=$;
- pomoćni simboli zagrada i zareza.

Sintaksa logike prvog reda II

$\mathcal{L}$-*termi*:

- simboli konstanti i promenljive su termi;
- ako je $f \in \mathrm{Fun}_{\mathcal{L}}$, $\mathrm{ar}(f) = n$, i $t_1, \ldots, t_n$ su termi, onda je i $f(t_1, \ldots, t_n)$ term;
- termi se grade u konačno mnogo koraka pomoću prethodna dva pravila.

- $\mathcal{T}_{\mathcal{L}}$ – skup $\mathcal{L}$-terma;
- $\mathcal{L}$-term je *zatvoren* ako ne sadrži promenljive;
- $\mathrm{sl}(t)$ – složenost terma t je broj funkcijskih simbola u t.

Sintaksa logike prvog reda III

Atomske $\mathcal{L}$-formule:

- ako su t_1 i t_2 termi, $t_1 = t_2$ je atomska formula;
- ako je $R \in \mathrm{Rel}_{\mathcal{L}}$, $\mathrm{ar}(R) = n$, i $t_1, t_2, \ldots, t_n$ su termi, $R(t_1, \ldots, t_n)$ je atomska formula.

$\mathcal{L}$-formule:

- atomske formule su formule;
- ako su φ i ψ formule, onda su i $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, ... formule;
- ako je φ formula i $x \in \mathrm{Var}$, onda su i $\exists x\, \varphi$ i $\forall x\, \varphi$ formule;
- formule se grade u konačno mnogo koraka pomoću prethodna tri pravila.

- $\mathcal{F}_{\mathcal{L}}$ – skup $\mathcal{L}$-formula;
- $\mathrm{sl}(\varphi)$ – složenost formule φ je broj veznika i kvantifikatora u φ;
- $\mathrm{qd}(\varphi)$ – *kvantifikatorska dubina* formule φ definisana je sa:
  - $\mathrm{qd}(\varphi) \stackrel{def}{=} 0$ ako je φ atomska formula;
  - $\mathrm{qd}(\neg\varphi) \stackrel{def}{=} \mathrm{qd}(\varphi)$;
  - $\mathrm{qd}(\varphi \wedge \psi) = \ldots \stackrel{def}{=} \max\{\mathrm{qd}(\varphi), \mathrm{qd}(\psi)\}$;
  - $\mathrm{qd}(\exists x\, \varphi) = \mathrm{qd}(\forall x\, \varphi) \stackrel{def}{=} \mathrm{qd}(\varphi) + 1$.

Sintaksa logike prvog reda IV

- U formuli $\exists x\, \varphi$ ili $\forall x\, \varphi$, φ je *domet* kvantifikatora $\exists x$, tj. $\forall x$.
- Pojavljivanje promenljive x u formuli φ je *vezano* ako je u dometu $\exists x$ ili $\forall x$; u suprotnom, pojavljivanje je *slobodno*.
- *$\mathcal{L}$-rečenica* ili *zatvorena $\mathcal{L}$-formula* je formula u kojoj nijedna promenljiva nema slobodna pojavljivanja.
- $\mathcal{S}_{\mathcal{L}}$ – skup $\mathcal{L}$-rečenica.

Semantika logike prvog reda I

Neka je $\mathcal{L}$ jezik prvog reda.

$\mathcal{L}$-struktura ili *$\mathcal{L}$-model* je par $\mathcal{M} = (M, s^{\mathcal{M}})_{s \in \mathcal{L}}$, gde:

- M je neprazan skup – *domen* ili *univerzum* strukture $\mathcal{M}$;

  (ako govorimo o čisto relacijskom jeziku, tj. $\mathcal{L} = \mathrm{Rel}_{\mathcal{L}}$, možemo da dozvolimo i da je $M = \emptyset$, i to je ponekad zgodno);
- $s^{\mathcal{M}} \in M$ ako $s \in \mathrm{Const}_{\mathcal{L}}$;
- $s^{\mathcal{M}} : M^{\mathrm{ar}(s)} \to M$ ako $s \in \mathrm{Fun}_{\mathcal{L}}$;
- $s^{\mathcal{M}} \subseteq M^{\mathrm{ar}(s)}$ ako $s \in \mathrm{Rel}_{\mathcal{L}}$.

Semantika logike prvog reda II

Fiksirajmo $\mathcal{L}$-model $\mathcal{M} = (M, s^{\mathcal{M}})_{s \in \mathcal{L}}$.

Valuacija u $\mathcal{M}$ je preslikavanje $v : \mathrm{Var} \to M$.

Vrednost terma t pri valuaciji v, $t[v]$, definisana je sa:

- ako je $t = x$, $t[v] \stackrel{def}{=} v(x)$;
- ako je $t = c \in \mathrm{Const}_{\mathcal{L}}$, $t[v] \stackrel{def}{=} c^{\mathcal{M}}$;
- ako je $t = f(t_1, \ldots, t_n)$, onda je $t[v] \stackrel{def}{=} f^{\mathcal{M}}(t_1[v], \ldots, t_n[v])$.

Komentar. Primetimo da $t[v]$ **zavisi** od $\mathcal{M}$, pa bi bilo preciznije da pišemo $t^{\mathcal{M}}[v]$ umesto $t[v]$. Medjutim, nećemo da opterećujemo zapis, a $\mathcal{M}$ će uvek biti jasno iz konteksta.

Semantika logike prvog reda III

Tačnost formule φ pri valuaciji v, $\varphi[v]$ (preciznije bi bilo $\varphi^{\mathcal{M}}[v]$), definisana je sa:

- ako je $\varphi = (t_1 = t_2)$, $\varphi[v] = 1 \overset{def}{\iff} t_1[v] = t_2[v]$;
- ako je $\varphi = R(t_1, \ldots, t_n)$, $\varphi[v] = 1 \overset{def}{\iff} R^{\mathcal{M}}(t_1[v], \ldots, t_n[v])$;
- $(\neg\varphi)[v]$, $(\varphi \wedge \psi)[v]$, ... računaju se po tablicama;
- ako je $\varphi = \exists x\, \psi$, $\varphi[v] = 1 \overset{def}{\iff} \psi[v_{m/x}] = 1$ za neko $m \in M$;
- ako je $\varphi = \forall x\, \psi$, $\varphi[v] = 1 \overset{def}{\iff} \psi[v_{m/x}] = 1$ za sve $m \in M$.

Ovde $v_{m/x}$, gde $m \in M$, je valuacija:

$$v_{m/x}(z) \overset{def}{=} \begin{cases} v(z) & \text{ako } z \neq x \\ m & \text{ako } z = x \end{cases}.$$

Naglasimo:

- $(\exists x\, \psi)[v] = 0 \Leftrightarrow \psi[v_{m/x}] = 0$ za sve $m \in M$;
- $(\forall x\, \psi)[v] = 0 \Leftrightarrow \psi[v_{m/x}] = 0$ za neko $m \in M$.

Semantika logike prvog reda IV

- $\mathcal{M}$ je *model* za φ, $\mathcal{M} \models \varphi$, ako za svaku valuaciju v u $\mathcal{M}$ važi $\varphi[v] = 1$; u suprotnom $\mathcal{M}$ je *kontramodel* za φ, $\mathcal{M} \not\models \varphi$.
- φ je *zadovoljiva* ako postoji model $\mathcal{M}$ i valuacija v takvi da $\varphi[v] = 1$; u suprotnom, φ je *kontradikcija*.
- φ je *poreciva* ako ima kontramodel; u suprotnom, φ je *valjana*, $\models \varphi$.

Primer. Neka je $\varphi = \varphi(p_1, \ldots, p_n)$ iskazna formula, i $\psi_1, \ldots, \psi_n$ formule prvog reda. Ako $\models \varphi$, onda $\models \varphi(\psi_1, \ldots, \psi_n)$.

- Pišemo $t = t(x_1, \ldots, x_n)$, ako su promenljive koje se pojavljuju u termu t neke od $x_1, \ldots, x_n$;
- pišemo $\varphi = \varphi(x_1, \ldots, x_n)$, ako su promenljive koje se pojavljuju **slobodno** u formuli φ neke od $x_1, \ldots, x_n$.

Lema 1. Neka su v, w valuacije u $\mathcal{M}$ i $t = t(x_1, \ldots, x_n)$ term. Ako $v(x_i) = w(x_i)$ za sve $i \leqslant n$, onda $t[v] = t[w]$.

Lema 2. Neka su v, w valuacije u $\mathcal{M}$ i $\varphi = \varphi(x_1, \ldots, x_n)$ formula. Ako $v(x_i) = w(x_i)$ za sve $i \leqslant n$, onda $\varphi[v] = \varphi[w]$.

Posledica. Vrednost rečenice u $\mathcal{M}$ ne zavisi od valuacije (samo od $\mathcal{M}$). Specijalno, rečenica je zadovoljiva ako i samo ako ima model.

Logička ekvivalentnost

$\mathcal{L}$-formule φ i ψ su *logički ekvivalentne*, $\varphi \equiv \psi$, ako za svaki $\mathcal{L}$-model $\mathcal{M}$ i svaku valuaciju v u $\mathcal{M}$, $\varphi[v] = \psi[v]$.

Ekvivalentno, $\models \varphi \leftrightarrow \psi$.

Primer. Neka su $\varphi_1 = \varphi_1(p_1, \ldots, p_n)$ i $\varphi_2 = \varphi_2(p_1, \ldots, p_n)$ iskazne formule, i $\psi_1, \ldots, \psi_n, \theta_1, \ldots, \theta_n$ formule prvog reda. Ako su $\varphi_1 \equiv \varphi_2$, $\psi_i \equiv \theta_i$ za sve $i \leqslant n$, onda su i $\varphi_1(\psi_1, \ldots, \psi_n) \equiv \varphi_2(\theta_1, \ldots, \theta_n)$.

Lema. Ako $\varphi \equiv \psi$, onda i $\exists x\, \varphi \equiv \exists x\, \psi$ i $\forall x\, \varphi \equiv \forall x\, \psi$.

Osnovne ekvivalencije:

- $\neg \forall x\, \varphi \equiv \exists x\, \neg \varphi$ i $\neg \exists x\, \varphi \equiv \forall x\, \neg \varphi$;
- $\exists x\, \varphi \wedge \psi \equiv \exists x(\varphi \wedge \psi)$, $\exists x\, \varphi \vee \psi \equiv \exists x(\varphi \vee \psi)$, $\forall x\, \varphi \wedge \psi \equiv \forall x(\varphi \wedge \psi)$ i $\forall x\, \varphi \vee \psi \equiv \forall x(\varphi \vee \psi)$, gde x nije slobodno u ψ;
- $\exists x\, \varphi \vee \exists x\, \psi \equiv \exists x(\varphi \vee \psi)$ i $\forall x\, \varphi \wedge \forall x\, \psi \equiv \forall x(\varphi \wedge \psi)$;
- $\exists x \exists y\, \varphi \equiv \exists y \exists x\, \varphi$ i $\forall x \forall y\, \varphi \equiv \forall y \forall x\, \varphi$.

Smena

Neka je φ formula, t term i x promenljiva. Sa $\varphi[t/x]$ označavamo formulu dobijenu zamenom svih slobodnih pojavljivanja promenljive x sa t.

Smena t/x je *regularna* za φ, ili kraće ,,smena $\varphi[t/x]$ je regularna", ako nijedna promenljiva terma t nije postala vezana nakon smene.

Lema. Pretpostavimo $x \neq y$, y nije slobodna u φ i $\varphi[y/x]$ je regularna smena. Tada $\exists x\, \varphi \equiv \exists y\, \varphi[y/x]$ i $\forall x\, \varphi \equiv \forall y\, \varphi[y/x]$.

Lema o smeni.

1. $(s[t/x])[v] = s[v_{t[v]/x}]$, gde $s[t/x]$ ima jasno značenje.
2. Ako je smena $\varphi[t/x]$ regularna, onda $(\varphi[t/x])[v] = \varphi[v_{t[v]/x}]$.

Preneks normalna forma (PNF) I

Definicija. Formula φ je u *preneks normalnoj formi (PNF)* ako je oblika:

$$\mathbf{Q}_1 x_1 \, \mathbf{Q}_2 x_2 \, \ldots \, \mathbf{Q}_n x_n \, \psi,$$

gde $\mathbf{Q}_i \in \{\exists, \forall\}$ za sve $i \leqslant n$ i ψ je *beskvantorna formula*, tj. formula u kojoj se ne pojavljuju kvantifikatori.

Teorema. Svaka formula je ekvivalentna formuli u PNF.

Preneks normalna forma (PNF) II

Algoritam.

- Koristeći zakone iskazne logike elimišemo sve veznike osim $\neg, \wedge, \vee$;
- koristteći De Morganove zakone za $\wedge, \vee, \forall, \exists$,,ubacimo" sve negacije do atomskih formula;
- ,,izvlačimo" kvantifikatore ispred zagrada koristeći:

$$\mathbf{Q}_1 x\, \varphi * \mathbf{Q}_2 y\, \psi \equiv \mathbf{Q}_1 x \mathbf{Q}_2 y (\varphi * \psi),$$

gde $\mathbf{Q}_1, \mathbf{Q}_2 \in \{\forall, \exists\}$, $* \in \{\wedge, \vee\}$, x nije slobodno u ψ i y nije slobodno u φ;

- ako nije moguće primeniti prethodni korak jer neka promenljiva ima slobodno pojavljivanje u odgovarajućoj formuli, primenimo najpre:

$$\mathbf{Q} x\, \varphi \equiv \mathbf{Q} z\, \varphi[z/x],$$

gde $\mathbf{Q} \in \{\forall, \exists\}$, z nije slobodno u φ, smena $\varphi[z/x]$ je regularna i omogućava primenu prethodnoh pravila;

- u specijalnim slučajevima možemo da primenimo:

$$\forall x\, \varphi \wedge \forall x\, \psi \equiv \forall x (\varphi \wedge \psi) \text{ i } \exists x\, \varphi \vee \exists x\, \psi \equiv \forall x (\varphi \vee \psi).$$

Primer. $\exists x\, P(x) \leftrightarrow \forall x \exists y\, Q(x, y)$.

Skolemova normalna forma (SNF)

Definicija. Formula u PNF je u *Skolemovoj normalnoj formi (SNF)* ako ne sadrži nijedan egzistencijalni kvantifikator.

Tvrdjenje. Neka je $\varphi = \forall x_1 \ldots \forall x_n \exists y \, \psi$. Tada je φ ekvizadovoljiva sa formulom:

$$\varphi' = \forall x_1 \ldots \forall x_n \, \psi[f(x_1, \ldots, x_n)/y],$$

gde je f novi (ne pojavljuje se u φ) n-arni funkcijski simbol. U slučaju, $n = 0$, f je konstanti simbol.

Komentar. Neka je $\psi = \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ beskvantorna formula i $\varphi = \mathbf{Q}x_1 \ldots \mathbf{Q}x_n \, \psi$; primetimo $\varphi = \varphi(y_1, \ldots, y_n)$.
Formula φ je zadovoljiva ako i samo ako $\exists y_1 \ldots y_m \, \varphi$ je zadovoljiva, ako i samo ako $\varphi(c_1, \ldots, c_m)$ je zadovoljiva, gde su $c_1, \ldots, c_m$ nove konstante.
Sada primenom skolemizacije na $\varphi(c_1, \ldots, c_m)$ dobijamo rečenicu koja je ekvizadovoljiva sa φ.

Erbranova teorema I

Definicija. Pretpostavimo $\text{Const}_{\mathcal{L}} \neq \emptyset$. $\mathcal{L}$-struktura $\mathcal{H} = (H, \dots)$ je *Erbranova struktura* ako:

- H je skup zatvorenih $\mathcal{L}$-terma;
- za $c \in \text{Const}_{\mathcal{L}}$, $c^{\mathcal{H}} = c$;
- za $f \in \text{Fun}_{\mathcal{L}}$, $\text{ar}(f) = n$, $t_1, \dots, t_n \in H$, $f^{\mathcal{H}}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$.

Primer. Neka je $\mathcal{L} = \{c, f, P\}$, gde su f i P unarni. Erbranova $\mathcal{L}$-struktura je bilo koja struktura $\mathcal{H} = (H, c^{\mathcal{H}}, f^{\mathcal{H}}, P^{\mathcal{H}})$ definisana sa:

- $H = \{a, f(a), f(f(a)), \dots\}$;
- $a^{\mathcal{H}} = a$;
- $f^{\mathcal{H}}(f^n(a)) = f^{n+1}(a)$;
- $P^{\mathcal{H}}$ je proizvoljni unarni predikat.

Lema. Ako je $\mathcal{H}$ Erbranova struktura i t zatvoren term, onda je $t[v] = t$ za sve valuacije v.

Lema (o smeni). Ako je $\mathcal{H}$ Erbranova struktura, φ formula i t zatvoren term, onda $(\varphi[t/x])[v] = \varphi[v_{t/x}]$.

Erbranova teorema II

Teorema (Erbranova teorema). Neka je φ rečenica u SNF. Tada φ je zadovoljiva ako i samo ako φ ima Erbranov model.

Dokaz. Smer ($\Leftarrow$) je očigledan.
($\Rightarrow$) Neka $\mathcal{M} \models \varphi$. Treba da definišemo Erbranovu strukturu $\mathcal{H}$ takvu da $\mathcal{H} \models \varphi$; s obzirom da su interpretacije konstantnih i funkcijskih simbola odredjeni, treba samo da interpretiramo relacijske simbole. Stavimo:

$$P^{\mathcal{H}}(t_1, \ldots, t_n) \overset{def}{\iff} \mathcal{M} \models P(t_1, \ldots, t_n).$$

Lema. Za SNF rečenicu θ važi $\mathcal{M} \models \theta \Rightarrow \mathcal{H} \models \theta$; specijalno $\mathcal{H} \models \varphi$.

Dokaz leme. Indukcijom po broju kvantifikatora u θ. $\square_L$ $\square$

Primer. Ispitati da li je $\exists xyz(\neg(P(x) \vee P(y)) \wedge \neg(P(z) \rightarrow P(x)))$ zadovoljiva.

Komentar. Ako je $\varphi = \exists x_1 \ldots x_n \psi$ PNF rečenica takva da ψ ne sadrži funkcijske simbole, onda je φ zadovoljiva ako i samo ako φ ima konačan model.

Zatvorena rezolucija

Komentar. Zadovoljiva formula ne mora da ima konačan model.

Definicija. Neka je $\varphi = \forall x_1 \dots x_n \psi$ SNF rečenica. *Erbranova ekspanzija* od φ je skup:

$$E(\varphi) \stackrel{def}{=} \{\psi[t_1/x_1, \dots, t_n/x_n] \mid t_1, \dots, t_n - \text{zatvoreni termi}\}.$$

Komentari.

1. Element u $E(\varphi)$ je Bulova kombinacija zatvorenih atomskih formula.
2. Skup $E(\varphi)$ ima Erbranov model ako i samo ako je iskazno zadovoljiv kad posmatramo zatvorene atomske formule kao iskazna slova.

Teorema. SNF rečenica φ je zadovoljiva ako i samo ako skup $E(\varphi)$ je iskazno zadovoljiv (u navedenom smislu).

Teorema o zatvorenoj rezoluciji. SNF rečenica φ je kontradiktorna ako i samo ako $E(\varphi) \vdash_{\text{Res}} \square$ (u iskaznom smislu).

Primeri

Primer 1. Posmatrajmo rečenice:

A. Svi u kafani su veseli, pripiti ili mrtvi pijani.

B. Svi pripiti su veseli.

C. Neko u kafani nije mrtav pijan.

D. Neko u kafani je veseo.

Dokazati $A, B, C \models D$.

Primer 2. Dokazati $\models \forall x \exists y (P(x) \to Q(y)) \to \exists y \forall x (P(x) \to Q(y))$.