Sveučilište u Zagrebu
PMF-Matematički odjel

Mladen Vuković

PRIMIJENJENA LOGIKA

predavanja poslijediplomskog kolegija

Zagreb, 2011.

Sadržaj

Predgovor

Ovaj nastavni materijal iz matematičke logike nastao je na osnovu zabilješki iz poslijediplomskog kolegija *Primijenjena logika* koji sam nekoliko godina predavao na Matematičkom odsjeku PMF–a u Zagrebu. Nadam se da će tekst zanimati sve one koji žele dublje proniknuti u osnove matematike, ili pak žele svoje prije stečeno znanje osvježiti.

Osnovne teme ovog nastavnog materijala su teorija modela i Gödelovi teoremi nepotpunosti. Dane su osnovne definicije i rezultati o apstraktnoj teoriji modela, teoriji rekurzije, teoriji složenosti i teoriji konačnih modela.

Svaki ispravak, ili pak sugestije, koje bi mogle doprinijeti poboljšanju ovog teksta, rado ću prihvatiti.

U Zagrebu, travanj 2011. Mladen Vuković

Uvod

Kolegij Primijenjena logika trebao bi biti opće–obrazovni (što god da to značilo; svakako nije koncipiran kao specijalni) kolegij iz matematičke logike s naglascima na primjenama u matematici.

O poželjnom predznanju: Bilo bi jako dobro da ste odslušali (i uspješno položili) dodiplomske kolegije Teorija skupova, Matematička logika i Matematička teorija računarstva, ali to nije nužno za slušanje ovog kolegija.

Centralni dio kolegija, odnosno prvo poglavlje, je teorija modela. Proučavat ćemo osnovne pojmove i konstrukcije modela kao što su:

- elementarna ekvivalencija
- (jaki) homomorfizmi
- (parcijalni) izomorfizmi
- (elementarna) smještenja
- (elementarni) podmodeli
- (elementarni) lanci
- Henkinova metoda konstrukcije pomoću konstanti
- metoda dijagrama
- reducirani produkti i ultraprodukti
- eliminacija kvantifikatora
- saturacija
- tipovi

"Naoružani" tim tehnikama i rezultatima promotrit ćemo primjene teorije modela redom na:

- Ramseyev teorem

- definabilnost u logici prvog reda
- Axov teorem
- Hilbertov Nullstellensatz

Na kraju poglavlja o teoriji modela razmatrat ćemo tzv. apstraktnu teoriju modela gdje ćemo dokazati Lindströmove teoreme o karakterizaciji logike prvog reda. Dio predavanja bit će posvećen teoriji konačnih modela. Kao osnovnu tehniku za tu teoriju razmatrat ćemo Ehrenfeuchtove igre.

U drugom poglavlju razmatrat ćemo osnovne tehnike teorije dokaza:

- normalizacija izvoda u sistemu prirodne dedukcije;
- eliminacija reza u sistemu sekvenata

U trećem poglavlju proučavat ćemo Gödelove teoreme nepotpunosti.

O literaturi:

- osnovna literatura za teoriju modela su knjige [7] i [6]
- osnovna literatura za teoriju dokaza su knjige [27] i [26]
- osnovna literatura za Gödelove teoremi nepotpunosti je knjiga [5]

Poglavlje 1

Teorija modela

1.1 Osnovni pojmovi i oznake

Ponavljamo osnovne pojmove iz logike prvog reda koji su nam potrebni.
Signatura σ (neke teorije prvog reda) je unija skupova A_1, A_2 i A_3 gdje su redom skupovi A_i definirani sa:

$A_1 = \{R_k^{n_k} \ : \ k \in I\}$, skup čije elemente nazivamo **relacijski simboli.** Skup I je neki podskup $\mathbb{N}$. Prirodan broj n_k se naziva mjesnost relacijskog simbola. Pretpostavljamo da ovaj skup sadrži barem jedan dvomjesni relacijski simbol.

$A_2 = \{f_k^{m_k} \ : \ k \in J\}$, skup čije elemente nazivamo **funkcijski simboli.** Skup J je neki podskup $\mathbb{N}$, možda i prazan. Prirodan broj m_k se naziva mjesnost funkcijskog simbola.

$A_3 = \{c_k \ : \ k \in K\}$, skup čije elemente nazivamo **konstantski simboli.** Skup K je neki podskup $\mathbb{N}$, možda i prazan.

U definiciji smo naveli da pretpostavljamo da skup A_1 sadrži barem jedan dvomjesni relacijski simbol (rezerviran je za relaciju jednakosti). Skupovi funkcijskih i konstantskih simbola mogu biti i prazni.

Logika prvog reda je jedna istaknuta teorija prvog reda, koju ćemo označavati s FO (eng. first order logic). Signatura σ_{FO} logike prvog reda je unija prebrojivo mnogo relacijskih simbola, prebrojivo mnogo funkcijskih simbola i prebrojivo mnogo konstantskih simbola. Štoviše, smatramo da za svaki $k \in \mathbb{N}$ postoji prebrojivo mnogo relacijskih i funkcijskih simbola mjesnosti k.

U sljedećim definicijama σ–terma i σ–formule pretpostavljamo da je σ neka

proizvoljna signatura.

$\sigma-$**term**, odnosno kratko **term**, je riječ definirana sljedećom induktivnom definicijom:

a) svaka individualna varijabla i svaki konstantski simbol koji pripada σ su termi;

b) ako je f neki $n-$mjesni funkcijski simbol iz σ i $t_1, \ldots, t_n$ σ-termi, tada je riječ $f(t_1, \ldots, t_n)$ term;

c) riječ je σ-term ako i samo ako je nastala pomoću konačno mnogo primjena pravila a) i b).

Ako je R neki n–mjesni relacijski simbol iz σ, te su $t_1, \ldots, t_n$ termi, tada riječ $R(t_1, \ldots, t_n)$ nazivamo **atomarna formula.** Pojam σ–**formule**, odnosno kratko **formule**, definiran je sljedećom induktivnom definicijom:

a) svaka atomarna formula je formula;

b) ako su A i B formule tada su $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ i $(A \leftrightarrow B)$ također formule;

c) ako je A formula, a x varijabla, tada su riječi $(\forall x A)$ i $(\exists x A)$ također formule;

d) riječ je σ–formula ako i samo ako je nastala primjenom konačno mnogo puta pravila a), b) i c).

Smatramo da su sljedeći pojmovi dobro poznati: konvencija o ispuštanju zagrada, složenost formule, potformula, shema formule, slobodni i vezani nastup varijable u formuli, zatvorena formula ili rečenica, ... (vidi [28]).

σ-struktura, odnosno kratko **struktura**, je uređeni par $\mathfrak{M} = (M, \varphi)$, gdje je M neprazni skup koji nazivamo **nosač**, a φ je preslikavanje sa skupa nelogičkih simbola σ koje ima sljedeća svojstva:

a) svakom relacijskom simbolu $R_k^{n_k}$ iz σ pridružuje se n_k-mjesna relacija $\varphi(R_k^{n_k})$ na M;

b) svakom funkcijskom simbolu $f_k^{m_k}$ iz σ pridružuje se m_k-mjesna funkcija $\varphi(f_k^{m_k})$ sa M^{m_k} u M;

c) svakom konstantskom simbolu c_k iz σ pridružuje se neki element $\varphi(c_k)$ iz M.

Ako je $\mathfrak{M} = (M, \varphi)$ struktura ponekad ćemo umjesto M koristiti i oznaku $|\,\mathfrak{M}\,|$. Zatim, umjesto $\varphi(R)$, $\varphi(f)$ i $\varphi(c)$ redom ćemo koristiti oznake $R^{\mathfrak{M}}$, $f^{\mathfrak{M}}$ i $c^{\mathfrak{M}}$.

Kardinalnost strukture $\mathfrak{M}$ je kardinalni broj skupa $|\,\mathfrak{M}\,|$, pa ćemo tako govoriti o konačnim i beskonačnim, odnosno o prebrojivim i neprebrojivim strukturama.

Za danu strukturu $\mathfrak{M}$ svaku funkciju sa skupa individualnih varijabli u nosač strukture nazivamo **valuacija.**

Lema 1.1. *Neka je $\mathfrak{M}$ neka σ–struktura i v neka valuacija. Postoji jedinstveno proširenje v' od v koje je definirano na skupu svih terma, koji određuje dani skup nelogičkih simbola σ, te v' ima sljedeća svojstva:*

$$\begin{aligned} v'(x_k) &= v(x_k), \\ v'(c) &= c^{\mathfrak{M}}, \\ v'(f(t_1,\ \ldots,\ t_n)) &= f^{\mathfrak{M}}(v'(t_1),\ \ldots,\ v'(t_n)), \end{aligned}$$

za sve varijable x_k, sve konstantske simbole c i sve funkcijske simbole f iz σ, te za sve σ–terme t_i.

U daljnjem tekstu smatramo da je svaka valuacija definirana na skupu svih terma, i to na način kao što je navedeno u iskazu prethodne leme.

Ako je $\mathfrak{M}$ neka σ–strukura, v valuacija na $\mathfrak{M}$ i t term, tada ćemo obično umjesto $v(t)$ pisati $t^{\mathfrak{M}}[v]$. Odnosno, ako je sa $t(x_1, \ldots, x_n)$ označen term čiji je skup varijabli podskup od $\{x_1, \ldots, x_n\}$, te su $a_1, \ldots, a_n \in |\mathfrak{M}|$, tada sa $t^{\mathfrak{M}}[a_1, \ldots, v_n]$ označavamo valuaciju terma pri čemu vrijedi $v(x_i) = a_i$, za sve $i = 1, \ldots, n$.

Svaki uređeni par neke σ–strukture $\mathfrak{M}$ i proizvoljne valuacije v na M nazivamo σ–**interpretacija**, ili kratko **interpretacija**.

Za danu valuaciju v i varijablu x sa v_x označavamo svaku valuaciju koja se podudara sa v na svim varijablama osim možda na varijabli x.

Neka je $(\mathfrak{M}, v)$ neka σ–interpretacija. **Istinitost** σ–**formule** F za danu interpretaciju, u oznaci $\mathfrak{M} \models_v F$, definiramo induktivno po složenosti formule F ovako:

a) ako je F atomarna formula, tj. F je oblika $R(t_1,\ \ldots,\ t_n)$, tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako $(t_1^{\mathfrak{M}}[v],\ \ldots,\ t_n^{\mathfrak{M}}[v]) \in R^{\mathfrak{M}}$;

b) ako je F formula oblika $\neg G$ tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako ne vrijedi $\mathfrak{M} \models_v G$;

c) ako je F formula oblika $A \wedge B$ tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_v A$ i $\mathfrak{M} \models_v B$;

d) ako je F formula oblika $A \vee B$ tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_v A$ ili $\mathfrak{M} \models_v B$;

e) ako je F formula oblika $A \to B$ tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako ne vrijedi $\mathfrak{M} \models_v A$ ili vrijedi $\mathfrak{M} \models_v B$;

f) ako je F formula oblika $A \leftrightarrow B$ tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako vrijedi da je $\mathfrak{M} \models_v A$ ekvivalentno sa $\mathfrak{M} \models_v B$;

g) ako je F formula oblika $\forall x G$ ($\exists x G$) tada definiramo:

$\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_{v_x} G$ za svaku (neku) valuaciju v_x.

U daljnjem tekstu umjesto "ne vrijedi $\mathfrak{M} \models_v F$" pisat ćemo samo kratko $\mathfrak{M} \not\models_v F$, i govorit ćemo da je formula F **neistinita** za danu interpretaciju. Ako je $F(x_1, \ldots, x_n)$ formula, te v valuacija na $\mathfrak{M}$, tada umjesto $\mathfrak{M} \models_v F$ koristimo i oznaku $\mathfrak{M} \models F[a_1, \ldots, a_n]$, gdje je $a_i = v(x_i)$, za sve $i = 1, \ldots, n$. Neka je Γ skup formula, te $\mathfrak{M}$ struktura za Γ i v valuacija na M. Sa $\mathfrak{M} \models_v \Gamma$ kratko označavamo da za sve $F \in \Gamma$ vrijedi $\mathfrak{M} \models_v F$.

Kažemo da je formula F **ispunjiva** (**oboriva**) ako postoji interpretacija $(\mathfrak{M}, v)$ tako da vrijedi $\mathfrak{M} \models_v F$ ($\mathfrak{M} \not\models_v F$). Kažemo da je struktura $\mathfrak{M}$ **model** za formulu F ako je to struktura za F i vrijedi $\mathfrak{M} \models_v F$ za sve valuacije v. Tu činjenicu označavamo sa $\mathfrak{M} \models F$. Kažemo da je formula **valjana** ako je istinita za svaku interpretaciju.

Za dvije σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su **elementarno ekvivalentne** ako za sve zatvorene formule F vrijedi

$$\mathfrak{M} \models F \quad \text{ako i samo ako} \quad \mathfrak{N} \models F$$

Oznaka: $\mathfrak{M} \equiv \mathfrak{N}$

1.2 Preslikavanja između struktura

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ neke dvije σ–strukture. **Homomorfizam** je svaka funkcija $h : M \to N$ koja ima sljedeća svojstva:

(i) za svaki relacijski simbol $R \in S$ i sve $a_1, \ldots, a_n \in M$ vrijedi

$$\text{ako } \; R^{\mathfrak{M}}(a_1, \ldots, a_n) \; \text{ tada } \; R^{\mathfrak{N}}(h(a_1), \ldots, h(a_n));$$

(ii) za svaki funkcijski simbol $f \in S$ i sve $a_1, \ldots, a_n \in M$ vrijedi:

$$h(f^{\mathfrak{M}}(a_1, \ldots, a_n)) = f^{\mathfrak{N}}(h(a_1), \ldots, h(a_n));$$

(iii) za svaki konstantski simbol $c \in S$ vrijedi $h(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$.

Primjer 1.2. *Homomorfizam grupa:*

$$h : (G, \cdot) \to (G', \circ), \qquad f(a \cdot b) = f(a) \circ f(b)$$

Homomorfizam vektorskih prostora (linearni operator):

$$h : U \to V, \qquad h(v + w) = h(v) + h(w), \qquad h(\alpha v) = \alpha h(v)$$

Lema 1.3. *Neka je h homomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. Tada za svaki term $t(x_1, \ldots, x_n)$ i sve $a_1, \ldots, a_n \in |\mathfrak{M}|$ vrijedi:*

$$h(t^{\mathfrak{M}}[a_1, \ldots, a_n]) = t^{\mathfrak{N}}[h(a_1), \ldots, h(a_n)].$$

Posebno, ako je t zatvoreni term tada vrijedi $h(t^{\mathfrak{M}}) = t^{\mathfrak{N}}$.

Napomena 1.4. *Neka je h homomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. Tada niti čak za svaku formulu $F(x_1, \ldots, x_n)$ bez kvantifikatora ne mora vrijediti:*

$$\textit{ako } \; \mathfrak{M} \models F[a_1, \ldots, a_n] \; \textit{ tada } \; \mathfrak{N} \models F[h(a_1), \ldots, h(a_n)]$$

gdje su $a_1, \ldots, a_n \in M$. Npr. neka je $\sigma = \{=\}$, te $\mathfrak{M} = (\mathbb{Z}, =)$ i $\mathfrak{N} = (\mathbb{N}, =)$ normalne strukture. Preslikavanje $h : \mathbb{Z} \to \mathbb{N}$ koje je definirano sa $h(x) = |x|$ je očito homomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. Očito vrijedi $\mathfrak{M} \models \neg(x = y)[-1, 1]$, ali $\mathfrak{N} \not\models \neg(x = y)[h(-1), h(1)]$.

Homomorfizam $h : M \to N$ nazivamo **jaki homomorfizam** ako za svaki relacijski simbol R i sve $a_1, \ldots, a_n \in M$ vrijedi

$$R^{\mathfrak{M}}(a_1, \ldots, a_n) \; \text{ ako i samo ako } \; R^{\mathfrak{N}}(h(a_1), \ldots, h(a_n)).$$

Propozicija 1.5. *Neka je h jaki homomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. Tada za svaku formulu $F(x_1, \ldots, x_n)$ bez kvantifikatora i sve $a_1, \ldots, a_n \in M$ vrijedi:*

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \quad \textit{ako i samo ako} \quad \mathfrak{N} \models F[h(a_1), \ldots, h(a_n)]$$

Napomena 1.6. *Tvrdnja prethodne propozicije općenito ne vrijedi za svaku formulu. Npr. funkcija $h : \mathbb{N} \to \mathbb{Z}$, $h(x) = x$, je jaki homomorfizam struktura $(\mathbb{N}, <)$ i $(\mathbb{Z}, <)$. No, imamo $\mathbb{N} \models \exists x \forall y (x \leq y)$, ali $\mathbb{Z} \not\models \exists x \forall y (x \leq y)$.*

Jaki homomorfizam koji je injekcija nazivamo **smještenje**.

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Kažemo da je $\mathfrak{M}$ **podmodel** od $\mathfrak{N}$, i pišemo $\mathfrak{M} \subseteq \mathfrak{N}$, ako vrijedi:

(i) $M \subseteq N$

(ii) za svaki relacijski simbol R vrijedi $R^{\mathfrak{N}}|_M = R^{\mathfrak{M}}$

(iii) za svaki funkcijski simbol f vrijedi $f^{\mathfrak{N}}|_M = f^{\mathfrak{M}}$

(iv) za svaki konstantski simbol c vrijedi $c^{\mathfrak{M}} = c^{\mathfrak{N}}$

Oznaka: $\mathfrak{M} \subseteq \mathfrak{N}$. Ako je $\mathfrak{M}$ podmodel od $\mathfrak{N}$ tada kažemo još da je $\mathfrak{N}$ **proširenje modela** $\mathfrak{M}$.

Lema 1.7. *Neka $\mathfrak{M} \subseteq \mathfrak{N}$ i v valuacija na $\mathfrak{M}$. Tada:*

(i) za svaki term t vrijedi $t^{\mathfrak{M}}[v] = t^{\mathfrak{N}}[v]$;

(ii) za svaku formulu F bez kvantifikatora vrijedi

$$\mathfrak{M} \models_v F \quad \textit{ako i samo ako} \quad \mathfrak{N} \models_v F.$$

Izomorfizam struktura je jaki homorfizam koji je bijekcija. Oznaka: $\mathfrak{M} \simeq \mathfrak{N}$

Propozicija 1.8. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Sljedeće tvrdnje su ekvivalentne:*

a) postoji smještenje $h : M \to N$;

b) postoji podmodel $\mathfrak{U}$ od $\mathfrak{N}$ tako da vrijedi $\mathfrak{M} \simeq \mathfrak{U}$.

c) za svaku atomarnu formulu $F(x_1, \ldots, x_n)$ i sve $a_1, \ldots, a_n \in M$ vrijedi:

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \quad \textit{ako i samo ako} \quad \mathfrak{N} \models F[h(a_1), \ldots, h(a_n)]$$

Lema 1.9. *Neka je $h : M \to N$ izomorfizam struktura. Tada za svaku valuaciju v na M vrijedi:*

(i) $h(t^{\mathfrak{M}}[v]) = t^{\mathfrak{N}}[h \circ v]$, *za svaki terme* t;

(ii) $\mathfrak{M} \models_v F$ *ako i samo ako* $\mathfrak{N} \models_{h \circ v} F$, *za svaku formulu* F.

Teorem 1.10. *Ako vrijedi $\mathcal{M} \simeq \mathcal{N}$ tada vrijedi i $\mathcal{M} \equiv \mathcal{N}$.*

Obrat prethodnog teorema općenito ne vrijedi. Kasnije ćemo dokazati da vrijedi $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$. Očito $(\mathbb{Q}, <) \not\simeq (\mathbb{R}, <)$. No, vrijedi nešto oslabljena verzija.

Propozicija 1.11. *Ako je $\mathfrak{M}$ konačna struktura, te vrijedi $\mathfrak{M} \equiv \mathfrak{N}$, tada imamo i $\mathfrak{M} \simeq \mathfrak{N}$.*

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Preslikavanje $h : M \to N$ nazivamo **elementarno preslikavanje** ako za svaku formulu $F(x_1, \ldots, x_n)$ i sve $a_1, \ldots, a_n \in M$ vrijedi

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \text{ ako i samo ako } \mathfrak{N} \models [h(a_1), \ldots, h(a_n)]$$

Napomena 1.12. *Očito homomorfizam i jaki homomorfizam nisu nužno i elementarna preslikavanja. Svaki izomorfizam je elementarno preslikavanje. Ako između struktura postoji elementarno preslikavanje tada su te strukture posebno elementarno ekvivalentne. Elementarno preslikavanje na normalnim strukturama je jaki homomorfizam.*

Neka $\mathfrak{M} \subseteq \mathfrak{N}$. Kažemo da je $\mathfrak{M}$ **elementarni podmodel** od $\mathfrak{N}$ ako za svaku formulu $F(x_1, \ldots, x_n)$ i sve $a_1, \ldots, a_n \in M$ vrijedi

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \text{ ako i samo ako } \mathfrak{N} \models [a_1, \ldots, a_n]$$

Oznaka: $\mathfrak{M} \prec \mathfrak{N}$. Ako je $\mathfrak{M}$ elementarni podmodel od $\mathfrak{N}$ tada kažemo još da je $\mathfrak{N}$ **elementarno proširenje** od $\mathfrak{M}$.

Napomena 1.13. *U definiciji elementarnog podmodela suvišno je zahtijevati da vrijedi $\mathfrak{M} \subseteq \mathfrak{N}$. Uočimo prvo da iz uvjeta da za sve $a_1, \ldots, a_n \in M$ vrijedi:*

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \text{ ako i samo ako } \mathfrak{N} \models F[a_1, \ldots, a_n]$$

trivijalno slijedi $M \subseteq N$. Neka je c proizvoljni konstantski simbol. Tada iz definicije elementarnog podmodela slijedi da za formulu $x = c$ vrijedi:

$$\mathfrak{M} \models x = c[c^{\mathfrak{M}}] \quad \textit{ako i samo ako} \quad \mathfrak{N} \models x = c[c^{\mathfrak{M}}]$$

Pošto očito vrijedi $\mathfrak{M} \models x = c[c^{\mathfrak{M}}]$ (implicite pretpostavljamo da je interpretacija simbola $=$ jedna refleksivna relacija!), tada imamo i $\mathfrak{N} \models x = c[c^{\mathfrak{M}}]$. Iz ovog posljednjeg slijedi $c^{\mathfrak{M}} = c^{\mathfrak{N}}$. Analogno bi dokazali da tvrdnja vrijedi za relacijske i funkcijske simbole.

Propozicija 1.14. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ–strukture. Tada vrijedi:*

(i) ako $\mathfrak{M} \prec \mathfrak{N}$ tada $\mathfrak{M} \equiv \mathfrak{N}$;

(ii) ako $\mathfrak{M} \prec \mathfrak{U}$, $\mathfrak{N} \prec \mathfrak{U}$, $\mathfrak{M} \subseteq \mathfrak{N}$ tada $\mathfrak{M} \prec \mathfrak{N}$.

Sljedeći važan teorem lako je dokazati indukcijom po složenosti formule.

Teorem 1.15. *(Tarski–Vaughtov kriterij za elementarne podmodele)*
Neka $\mathfrak{M} \subseteq \mathfrak{N}$, te neka za svaku formulu $F(x_1, \ldots, x_k, x)$ i sve $a_1, \ldots, a_k \in |\mathfrak{M}|$ vrijedi:

ako $\mathfrak{N} \models \exists x F[a_1, \ldots, a_k]$ tada postoji $a \in |\mathfrak{M}|$ takav da $\mathfrak{N} \models F[a_1, \ldots, a_k, a]$.

Tada vrijedi $\mathfrak{M} \prec \mathfrak{N}$.

Primjer 1.16. *Vrijedi $(\mathbb{Q}, <) \prec (\mathbb{R}, <)$, a onda i $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$ (vidi propoziciju 1.14.).*
Uputa: ako $q_1, \ldots, q_n \in \mathbb{Q}$ i $r \in \mathbb{R}$ tada postoji automorfizam $h : \mathbb{R} \to \mathbb{R}$ takav da je $h(q_i) = q_i$ i $h(r) \in \mathbb{Q}$. Primijenite Tarski–Vaughtov kriterij za elementarne podmodele.

Očita posljedica prethodnog primjera je da aksiom potpunosti skupa $\mathbb{R}$ ne možemo izraziti nekom rečenicom prvog reda.

Napomena 1.17. *Podmodel može biti čak izomorfan nekom svom proširenju, ali ipak nije elementarni podmodel. Navodimo tri primjera za to. Očito vrijedi $(2\mathbb{Z}, 0, +) \subseteq (\mathbb{Z}, 0, +)$, te $(2\mathbb{Z}, 0, +) \simeq (\mathbb{Z}, 0, +)$, ali ne vrijedi $(2\mathbb{Z}, 0, +) \prec (\mathbb{Z}, 0, +)$. Očito $(\mathbb{Z}, 0, +) \subseteq (\mathbb{Q}, 0, +)$, ali ne vrijedi $(\mathbb{Z}, 0, +) \prec (\mathbb{Q}, 0, +)$. Polje racionalnih brojeva je podmodel polja $\mathbb{R}$, ali nije elementarni podmodel.*

Neka je h smještenje strukture $\mathfrak{M}$ u strukturu $\mathfrak{N}$ (tj. h je jaki homomorfizam koji je injekcija). Kažemo da je h **elementarno smještenje** ako je $h(\mathfrak{M})$ elementarni podmodel od $\mathfrak{N}$.

Propozicija 1.18. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture, te neka je h neka funkcija iz $|\mathfrak{M}|$ u $|\mathfrak{N}|$. Tada vrijedi:*

a) funkcija h je smještenje ako i samo ako za svaku formulu F bez kvantifikatora i svaku valuaciju v na $\mathfrak{M}$ vrijedi da je $\mathfrak{M} \models_v F$ ekvivalentno s $\mathfrak{N} \models_{h \circ v} F$;

b) funkcija h je elementarno smještenje ako i samo ako za svaku formulu F i svaku valuaciju v na $\mathfrak{M}$ vrijedi da je $\mathfrak{M} \models_v F$ ekvivalentno s $\mathfrak{N} \models_{h \circ v} F$.

Propozicija 1.19. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Tada vrijedi: postoji elementarno smještenje strukture $\mathfrak{M}$ u strukturu $\mathfrak{N}$ ako i samo ako postoji elementarni podmodel $\mathfrak{U}$ od $\mathfrak{N}$ tako da vrijedi $\mathfrak{M} \simeq \mathfrak{U}$.*

Neka je $(I, <)$ linearno uređen skup (tj. relacija $<$ je irefleksivna, tranzitivna i linearna). Za familiju σ–struktura $\{\mathfrak{M}_i : i \in I\}$ kažemo da je **(elementarni) lanac struktura** ako za sve $i, j \in I$ takve da je $i < j$ vrijedi $\mathfrak{M}_i \subseteq \mathfrak{M}_j$ ($\mathfrak{M}_i \prec \mathfrak{M}_j$).

Teorem 1.20. *(Teorem o uniji (elementarnog) lanca struktura)*
Neka je $(I, <)$ neki linearno uređeni skup i $\{\mathfrak{M}_i : i \in I\}$ neki (elementarni) lanac σ–struktura. Označimo sa $\mathfrak{M}$ σ–strukturu čiji je nosač unija nosača dane familije σ–struktura, te su na analogni način (pomoću unije) definirane interpretacije simbola iz σ. Tada za svaki $i \in I$ vrijedi $\mathfrak{M}_i \subseteq \mathfrak{M}$ ($\mathfrak{M}_i \prec \mathfrak{M}$).

Dokaz. Indukcijom po složenosti formule treba provjeriti da je ispunjen Tarski–Vaughtov kriterij za elementarne podmodele.

1.3 Parcijalni izomorfizmi

Ova tema je prirodan nastavak proučavanja preslikavanja među strukturama (homomorfizmi, smještenja, izomorfizmi, ...) Bili smo dokazali da $\mathfrak{M} \simeq \mathfrak{N}$ povlači $\mathfrak{M} \equiv \mathfrak{N}$. Istaknuli smo da obrat prethodne tvrdnje općenito ne vrijedi. Iz tog razloga prirodno se postavlja pitanje što najviše o "izomorfnosti" struktura možemo dobiti ako su strukture elementarno ekvivalentne. No, ipak glavni razlog uvrštavanja ove teme je dokaz Fraïsséovog teorema koji se koristi u dokazu Lindströmovog prvog torema koji karakterizira logiku prvog reda. Parcijalni izomorfizmi poslužit će nam i kao motivacija za Ehrenfeuchtove igre. Detalje o parcijalnim izomorfizmima možete čitati u knjizi [8].

Definicija 1.21. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture.* **Parcijalni izomorfizam** *je svaka injekcija $p : S \subseteq M \to N$ koja ima svojstva:*

a) za svaki relacijski simbol $R^n \in \sigma$ i sve $a_1, \ldots, a_n \in S$ vrijedi:

$$(a_1, \ldots, a_n) \in R^{\mathfrak{M}} \quad \textit{ako i samo ako} \quad (p(a_1), \ldots, p(a_n)) \in R^{\mathfrak{N}}$$

b) za svaki funkcijski simbol $f^n \in \sigma$ i sve $a_1, \ldots, a_n \in S$, takve da je $f^{\mathfrak{M}}(a_1, \ldots, a_n) \in S$, vrijedi:

$$p(f^{\mathfrak{M}}(a_1, \ldots, a_n)) \;=\; f^{\mathfrak{N}}(p(a_1), \ldots, p(a_n))$$

c) za svaki konstantski simbol $c \in \sigma$, takav da je $c^{\mathfrak{M}} \in S$, vrijedi $p(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$.

Uočite da o parcijalnom izomorfizmu p ne možemo govoriti kao o izomorfizmu nekih podmodela, jer $Dom(p)$ ne mora biti podmodel (ne mora sadržavati interpretacije svih konstantskih simbola, te skup $Dom(p)$ ne mora biti zatvoren na interpretacije svakog funkcijskog simbola).

Lema 1.22. *Neka je σ relacijski skup nelogičkih simbola, te neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Neka su $a_1, \ldots, a_n \in M$ i $b_1, \ldots, b_n \in N$ proizvoljni. Tada je ekvivalentno:*

a) parcijalna funkcija p iz M u N definirana sa $p : \{a_1, \ldots, a_n\} \to \{b_1, \ldots, b_n\}$, $p(a_i) = b_i$, je parcijalni izomorfizam.

b) za svaki relacijski simbol $R^m \in \sigma$ vrijedi

$$\mathfrak{M} \models R[a_{i_1}, \ldots, a_{i_m}] \quad \textit{ako i samo ako} \quad \mathfrak{N} \models R[b_{i_1}, \ldots, b_{i_m}]$$

Definicija 1.23. *Za σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su* **konačno izomorfne** *ako postoji niz $(I_n)_{n\in\mathbb{N}}$ nepraznih skupova parcijalnih izomorfizama tako da vrijedi:*

(forth) *za sve $p \in I_{n+1}$ i $a \in M$ postoji parcijalni izomorfizam $q \in I_n$ tako da vrijedi $a \in Dom(q)$ i $q \supseteq p$*

(back) *za sve $p \in I_{n+1}$ i $b \in N$ postoji parcijalni izomorfizam $q \in I_n$ tako da vrijedi $b \in Rng(q)$ i $q \supseteq p$*

Oznake: $(I_n) : \mathfrak{M} \simeq_f \mathfrak{N}, \qquad \mathfrak{M} \simeq_f \mathfrak{N}$

Definicija konačne izomorfnosti, odnosno uvjeti (forth) i (back), analogni su Cantorovom dokazu teorema o uređanoj karakteristici skupa $\mathbb{Q}$ (vidi npr. [29]), odnosno ta definicija je analogna definiciji bisimulacije u modalnoj logici (vidi npr. [3]). Fraïsséov teorem tvrdi da vrijedi:

$$\mathfrak{M} \equiv \mathfrak{N} \text{ ako i samo ako } \mathfrak{M} \simeq_f \mathfrak{N}$$

(samo za konačne skupove nelogičkih simbola). Fraïsséov teorem dokazujemo nizom lema.
Neka je σ fiksirani konačni skup relacijskih simbola, te $r \in \mathbb{N}$. Tada sa L_r^σ označavamo skup svih σ–formula čije varijable pripadaju skupu $\{v_1, \ldots, v_r\}$.

Dokazat ćemo da tvrdnja Fraïsséovog teorema vrijedi za konačne relacijske jezike. Može se dokazati da tvrdnja vrijedi za proizvoljne konačne signature.

Definicija 1.24. *Svakoj σ–formuli pridružujemo* **kvantifikatorski rang** *koji je induktivno definiran sa:*

$$qr(F) = 0, \quad \text{ako je } F \text{ atomarna formula}$$

$$qr(\neg F) = qr(F)$$

$$qr(F \circ G) = \max\{qr(F), qr(G)\}, \quad \text{gdje je } \circ \in \{\wedge, \vee, \to, \leftrightarrow\}$$

$$qr(\exists x F) = qr(\forall x F) = qr(F) + 1$$

Grubo rečeno kvantifikatorski rang neke formule je duljina maksimalnog niza uklopljenih kvantifikatora koji se pojavljuju u toj formuli.

Lema 1.25. *Neka je $(I_n)_{n\in\mathbb{N}} : \mathfrak{M} \simeq_f \mathfrak{N}$, te $F \in L_r^\sigma$ takva da je $qr(F) \leq n$. Tada za svaki $p \in I_n$ i sve $a_1, \ldots, a_r \in Dom(p)$ vrijedi*

$$\mathfrak{M} \models F[a_1, \ldots, a_r] \text{ ako i samo ako } \mathfrak{N} \models F[p(a_1), \ldots, p(a_r)]$$

Dokaz. Indukcijom po složenosti formule F.

Korolar 1.26. *Neka je σ konačan skup relacijskih simbola. Za svake dvije σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ vrijedi:*

$$\text{ako } \mathfrak{M} \simeq_f \mathfrak{N} \text{ tada } \mathfrak{M} \equiv \mathfrak{N}$$

(Tvrdnja korolara slijedi direktno iz leme 1.25. primjenom na zatvorene formule).

Ponovimo definiciju relacije logičke posljedice. Neka je F neka σ–rečenica i S neki skup σ–rečenica. Kažemo da formula F **logički slijedi** iz skupa formula S ako za svaku σ–strukturu $\mathfrak{M}$ vrijedi da $\mathfrak{M} \models S$ povlači $\mathfrak{M} \models F$. To kratko označavamo sa $S \models F$. Relaciju $\models$ nazivamo **relacija logičke posljedice**. Ako je skup S jednočlan, tj. $S = \{A\}$, tada umjesto $\{A\} \models B$ pišemo i $A \Rightarrow B$. Kažemo da su σ–rečenice F i G **logički ekvivalentne** ako vrijedi $F \Rightarrow G$ i $F \Rightarrow G$. Tu činjenicu označavamo sa $F \Leftrightarrow G$.

Definicija 1.27. *Neka je Σ neki skup σ–formula. Sa $\langle\Sigma\rangle$ ćemo označavati najmanji skup σ–formula koji sadrži Σ i zatvoren je na propozicionalne veznike.*

Istaknimo dva očigledna svojstva upravo definiranog operatora $\langle\rangle$:

a) Neka su Σ_1 i Σ_2 skupovi σ–formula koji imaju svojstvo da za svaki $F \in \Sigma_1$ postoji $G \in \Sigma_2$ tako da vrijedi $F \Leftrightarrow G$. Tada to isto vrijedi i za skupove $\langle\Sigma_1\rangle$ i $\langle\Sigma_2\rangle$

b) Ako je $F \in L_r^\sigma$ i $qr(F) \leq n+1$ tada vrijedi

$$F \in \langle \quad \{G \in L_r^\sigma : qr(G) \leq n\} \cup \{\exists x G \in L_r^\sigma : qr(G) \leq n\} \cup$$

$$\{\forall x G \in L_r^\sigma : qr(G) \leq n\} \ \rangle$$

Te činjenice trebaju za dokaz sljedeće leme.

Lema 1.28. *Neka su $n, r \in \mathbb{N}$ proizvoljni. Tada postoji konačno mnogo, do na logičku ekvivalenciju, različitih formula iz L_r^σ, čiji je kvantifikatorski rang manji ili jednak n.*

Dokaz. Indukcijom po n. Ovdje je važna konačnost skupa σ.

Lema 1.29. *Neka je σ konačan skup relacijskih simbola, te neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Ako $\mathfrak{M} \equiv \mathfrak{N}$ tada $\mathfrak{M} \simeq_f \mathfrak{N}$.*

Dokaz. Za svaki $n \in \mathbb{N}$ definiramo skup I_n parcijalnih izomorfizama:

$$\begin{aligned} p \in I_n \Leftrightarrow \;& p \text{ je parcijalni izomorfizam iz } \mathfrak{M} \text{ u } \mathfrak{N}, \\ & \text{postoji } r \in \mathbb{N}, \text{ postoje } a_1, \ldots, a_r \in M \text{ takvi da} \\ & Dom(p) = \{a_1, \ldots, a_r\} \text{ i} \\ & \text{za svaku formulu } F \in L^\sigma_r \text{ za koje je } qr(F) \leq n \text{ vrijedi:} \\ & \mathfrak{M} \models F[a_1, \ldots, a_r] \text{ ako i samo ako } \mathfrak{N} \models F[p(a_1), \ldots, p(a_r)] \end{aligned}$$

Primijetimo da za svaki $n \in \mathbb{N}$ imamo $I_n \neq \emptyset$, jer je $\emptyset \in I_n$. Dokažimo sada da niz $(I_n)_{n\in\mathbb{N}}$ ima svojstvo (forth). Neka su $p \in I_{n+1}$ i $a \in M$ proizvoljni. Označimo $Dom(p) = \{a_1, \ldots, a_r\}$ (primijetimo da za svaki $n \in \mathbb{N}$ i $p \in I_n$ u ovoj lemi vrijedi da je $Dom(p)$ konačan skup). Iz leme 1.28. slijedi da postoji konačan podskup $\{F_1, \ldots, F_s\}$ od L^σ_{r+1} tako da je $qr(F_i) \leq n$ i za svaku formulu $F \in L^\sigma_{r+1}$ postoji $i \in \{1, \ldots, s\}$ tako da vrijedi $F \Leftrightarrow F_i$. Za svaki $i \in \{1, \ldots, s\}$ definiramo formulu G_i ovako:

$$G_i \equiv \begin{cases} F_i, & \text{ako } \mathfrak{M} \models F[a_1, \ldots, a_r, a] \\ \neg F_i, & \text{ako } \mathfrak{M} \models \neg F[a_1, \ldots, a_r, a] \end{cases}$$

Iz definicija formula G_i očigledno slijedi:

$$\mathfrak{M} \models \exists v_{r+1}(G_1 \wedge \ldots \wedge G_s)[a_1, \ldots, a_r] \qquad (*)$$

Uočimo još da vrijedi:

$$qr(\exists v_{r+1}(G_1 \wedge \ldots \wedge G_s)) \leq n + 1$$

To znači da na danu formulu možemo primijeniti uvjet iz definicije niza (I_n). Time imamo da iz $(*)$ slijedi

$$\mathfrak{N} \models \exists v_{r+1}(G_1 \wedge \ldots \wedge G_s)[p(a_1), \ldots, p(a_r)]$$

Tada postoji $b \in N$ tako da vrijedi

$$\mathfrak{N} \models (G_1 \wedge \ldots \wedge G_s)[p(a_1), \ldots, p(a_r), b] \qquad (**)$$

Neka je $F \in L^\sigma_{r+1}$ formula takva da $qr(F) \leq n$. Iz definicije skupa formula $\{F_1, \ldots, F_s\}$ slijedi da postoji $i \in \{1, \ldots, s\}$ tako da vrijedi $F \Leftrightarrow F_i$.

Pretpostavimo sada da vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_r, a]$. Tada iz činjenice $F \Leftrightarrow F_i$ slijedi $\mathfrak{M} \models F_i[a_1, \ldots, a_r, a]$. Iz definicije formule G_i tada slijedi da je formula G_i jednaka formuli F_i. Sada iz $(**)$ posebno slijedi: $\mathfrak{N} \models G_i[p(a_1), \ldots, p(a_r), b]$, a onda $\mathfrak{N} \models F_i[p(a_1), \ldots, p(a_r), b]$. Iz činjenice $F \Leftrightarrow F_i$ posebno slijedi $\mathfrak{N} \models F[p(a_1), \ldots, p(a_r), b]$.

Rezimirajmo: za svaku formulu $F \in L^{\sigma}_{r+1}$ za koju je $qr(F) \leq n$ vrijedi:

$$\mathfrak{M} \models F[a_1, \ldots, a_r, a] \text{ ako i samo ako } \mathfrak{N} \models F[p(a_1), \ldots, p(a_r), b] \qquad (***)$$

(Mi smo bili dokazali jednu implikaciju. Analogno se dokazuje druga implikacija. Prisjetimo se da moramo dokazati da postoji proširenje q od p koje pripada skupu I_n, te vrijedi $a \in Dom(q)$).
Ako je $a \in Dom(p)$ tada uzmemo $q := p$. Promotrimo sada slučaj kada $a \notin Dom(p) = \{a_1, \ldots, a_r\}$. Tvrdimo da je $p \cup \{(a, b)\} \in I_n$, tj. da je to jedno traženo proširenje od p. Pokažimo prvo da je funkcija $p \cup \{(a, b)\}$ injekcija. Neka je $F \equiv \bigwedge_{i=1}^{r} v_i \neq v_{r+1}$. Uočimo da je $F \in L^{\sigma}_{r+1}$, te vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_r, a]$. Pošto je očito $qr(F) = 0$, tada je posebno $qr(F) \leq n$. Sada iz $(***)$ slijedi

$$\mathfrak{N} \models F[p(a_1), \ldots, p(a_r), b],$$

a onda iz toga i definicije formule F slijedi $b \notin \{p(a_1), \ldots, p(a_r)\}$.

Kako bi dokazali da funkcija $p \cup \{(a, b)\}$ pripada skupu I_n, potrebno je još vidjeti da za svaki relacijski simbol $R^k \in \sigma$ i sve $c_1, \ldots, c_k \in Dom(p)$ vrijedi

$$(c_1, \ldots, c_k) \in R^{\mathfrak{M}} \text{ ako i samo ako } (p(c_1), \ldots, p(c_k)) \in R^{\mathfrak{N}}$$

No, to slijedi iz $(***)$ i činjenice da je $Dom(p) = \{a_1, \ldots, a_r\}$. □

Teorem 1.30. *(***Fraïsséov teorem***). Neka je σ konačan relacijski skup nelogičkih simbola. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ proizvoljne dvije σ–strukture. Tada vrijedi:*

$$\mathfrak{M} \simeq_f \mathfrak{N} \text{ ako i samo ako } \mathfrak{M} \equiv \mathfrak{N}$$

Dokaz. Korolar 1.26. i lema 1.29.

Sada definiramo još jednu verziju izomorfnosti struktura, te navodimo lemu u kojoj ističemo veze između raznih pojmova izomorfnosti. Sve to ćemo koristiti u poglavlju o apstraktnoj teoriji modela.

Definicija 1.31. *Za σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su* **parcijalno izomorfne** *ako postoji neprazan skup I pracijalnih izomorfizama između struktura $\mathfrak{M}$ i $\mathfrak{N}$ tako da vrijedi:*

(forth) *za svaki $p \in I$ i $a \in M$ postoji $q \in I$ tako da imamo $a \in Dom(q)$ i $q \supseteq p$*

(back) *za svaki $p \in I$ i $b \in N$ postoji $q \in I$ tako da imamo $b \in Rng(q)$ i $q \supseteq p$*

Oznaka: $\mathfrak{M} \simeq_p \mathfrak{N}$

Lema 1.32. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Tada vrijedi:*

a) *ako $\mathfrak{M} \simeq \mathfrak{N}$ tada $\mathfrak{M} \simeq_p \mathfrak{N}$*

b) *ako $\mathfrak{M} \simeq_p \mathfrak{N}$ tada $\mathfrak{M} \simeq_f \mathfrak{N}$*

c) *ako $\mathfrak{M} \simeq_f \mathfrak{N}$ i struktura $\mathfrak{M}$ je konačna tada $\mathfrak{M} \simeq \mathfrak{N}$*

d) *ako $\mathfrak{M} \simeq_p \mathfrak{N}$, te su strukture $\mathfrak{M}$ i $\mathfrak{N}$ najviše prebrojive, tada $\mathfrak{M} \simeq \mathfrak{N}$ (***Karpov teorem***)*

Dokazujemo samo tvrdnju d), tj. Karpov teorem. Neka vrijedi $I : \mathfrak{M} \simeq_p \mathfrak{N}$. Zatim, neka je $|\mathfrak{M}| = \{a_0, a_1, a_2, \ldots\}$ i $|\mathfrak{N}| = \{b_0, b_1, b_2, \ldots\}$. Neka je $p_0 \in I$ proizvoljan ali fiksiran parcijalni izomorfizam. Primjenom uvjeta (forth) i (back) induktivno možemo konstruirati niz parcijalnih izomorfizama $(p_n) \subseteq I$ tako da vrijedi: $a_0 \in Dom(p_1)$, $b_0 \in Rng(p_2)$, $a_1 \in Dom(p_3)$, $b_1 \in Rng(p_4)$, $\ldots$, odnosno točnije niz (p_n) ima sljedeća svojstva:

a) za svaki $n \in \mathbb{N}$ vrijedi $p_n \subseteq p_{n+1}$

b) ako je n neparan broj, tj. $n = 2r + 1$, tada vrijedi $a_r \in Dom(p_n)$

c) ako je n paran broj, tj. $n = 2r$, tada vrijedi $b_r \in Rng(p_n)$

Iz uvjeta a) slijedi da je dobro definirana funkcija $p = \cup_n p_n$, koja je očito parcijalni izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. Iz uvjeta b) i c) slijedi $Dom(p) = |\mathfrak{M}|$ i $Rng(p) = |\mathfrak{N}|$. To znači da je p jedan izomorfizam struktura. □

1.4 Teorem kompaktnosti

U ovoj točki ćemo primjenom Henkinove konstrukcije dokazati teorem kompaktnosti za logiku prvog reda, te ilustrirati neke primjene teorema kompaktnosti.

Neka je S neki skup σ–rečenica i $\mathfrak{M}$ neka σ–struktura. Ako za svaku formulu $F \in S$ vrijedi $\mathfrak{M} \models F$, tada to označavamo sa $\mathfrak{M} \models S$.

Za skup S σ–rečenica kažemo da je **ispunjiv** ako postoji σ–struktura $\mathfrak{M}$ tako da vrijedi $\mathfrak{M} \models S$. Za skup S σ–rečenica kažemo da je **konačno ispunjiv** ako je svaki njegov konačni podskup ispunjiv.

Propozicija 1.33. *Sljedeće tvrdnje su ekvivalentne:*

a) svaki konačno ispunjiv skup rečenica je i ispunjiv.

b) za svaki skup rečenica S i svaku rečenicu F, takve da $S \models F$, postoji konačan podskup $S' \subseteq S$ tako da vrijedi $S' \models F$.

Teorem 1.34. *(Teorem kompaktnosti)*
Skup rečenica S je ispunjiv ako i samo ako je svaki konačan podskup od S ispunjiv.

Dokaz ovog važnog teorema ćemo provesti primjenom Henkinove konstrukcije modela pomoću konstanti. Na taj način je dokazan generalizirani teorem potpunosti za teorije prvog reda u skripti [28]. U istoj skripti teorem kompaktnosti je dobiven kao jednostavna posljedica generaliziranog teorema potpunosti za teorije prvog reda. No, sada uopće ne razmatramo formalni račun.

Za skup S σ–rečenica kažemo da je **potpun** ako za svaku σ–rečenicu F vrijedi $S \models F$ ili $S \models \neg F$.

Lema 1.35. *(Lindenbaumova lema)*
Za svaki konačno ispunjiv skup formula S postoji konačno ispunjiv potpun skup S' tako da vrijedi $S \subseteq S'$.

Skica dokaza. Neka je

$$\mathfrak{S} = \{T \ : \ S \subseteq T, \ T \ \text{ je konačno ispunjiv } \}.$$

Primjenom Zornove leme[1] slijedi da parcijalno uređen skup $(\mathfrak{S}, \subset)$ sadrži maksimalni element S'. Lako je vidjeti da je S' potpun skup rečenica. □

[1]Zornova lema: Neka je $(A, <)$ neprazan parcijalno uređen skup koji ima svojstvo da za svaki lanac od A postoji gornja međa. Tada skup A ima barem jedan maksimalni element.

Za skup S σ–rečenica kažemo je **Henkinov skup rečenica** ako za svaku formulu oblika $\exists x F(x)$ iz S postoji zatvoreni σ–term t tako da vrijedi $F(t/x) \in S$.

Za σ–strukturu $\mathfrak{M}$ kažemo da je **kanonski model** ako za svaki $a \in |\mathfrak{M}|$ postoji zatvoreni term t tako da vrijedi $t^{\mathfrak{M}} = a$.

Teorem 1.36. *Za svaki potpun konačno ispunjiv Henkinov skup σ–rečenica S postoji kanonski model.*

Skica dokaza. Neka je T skup svih zatvorenih terma. Na skupu T definiramo binarnu relaciju $\sim$ ovako:

$$t_1 \sim t_2 \text{ ako i samo ako } t_1 = t_2 \in S$$

Lako je provjeriti da je $\sim$ relacija ekvivalencije (pretpostavlja se da S sadrži sve instance shema aksioma za jednakost). Za $t \in T$ sa $[t]$ označavamo pripadnu klasu ekvivalencije. Neka je $M = \{[t] : t \in T\}$.

Na skupu M definiramo interpretaciju svakog nelogičkog simbola iz σ. Npr. za n–mjesni relacijski simbol R iz σ definiramo relaciju $R^{\mathfrak{M}}$ sa:

$$([t_1], \ldots, [t_n]) \in R^{\mathfrak{M}} \text{ ako i samo ako } R(t_1, \ldots, t_n) \in S$$

Analogno se definiraju interpretacije funkcijskih i konstantskih simbola. (Lako je dokazati neovisnost o izboru reprezentanata). Sada treba indukcijom po složenosti formule dokazati glavnu pomoćnu tvrdnju:

> za sve zatvorene terme $t_1, \ldots, t_n$ i svaku σ–formulu $F(x_1, \ldots, x_n)$ vrijedi
>
> $$\mathfrak{M} \models F[\, [t_1], \ldots, [t_n]\,] \text{ ako i samo ako } F(t_1, \ldots, t_n) \in S$$

Iz te pomoćne tvrdnje očito slijedi da je $\mathfrak{M}$ model za skup rečenica S. □

Lema 1.37. *Svaki konačno ispunjiv skup rečenica je ispunjiv.*

Skica dokaza. Neka je S_0 konačno ispunjiv skup σ_0–rečenica. Sada induktivno definiramo niz skupova nelogičkih simbola (σ_n) i niz skupova rečenica (S_n).

$$\sigma_{n+1} = \sigma_n \cup \{\ c_F : F \text{ je } \sigma_n\text{–formula s točno jednom slobodnom varijablom } \}$$

$$S_{n+1} = S_n \cup \{\ \exists x F(x) \to F(c_F/x) : F \text{ je } \sigma_n\text{–formula s točno jednom slobodnom varijablom } \}$$

Pretpostavljamo da je za svaki $n \in \mathbb{N}\setminus\{0\}$ i svaku σ_n–formulu F s točno jednom slobodnom varijablom c_F novi konstantski simbol, tj. $c_F \notin \sigma_n$, te za sve različite σ_n–formule F i G vrijedi $c_F \neq c_G$. Dokažimo indukcijom da je za svaki $n \in \mathbb{N}$ skup S_n konačno ispunjiv. Pretpostavimo da je $n \in \mathbb{N}$ takav da je skup S_n konačno ispunjiv. Neka je Σ proizvoljan konačan podskup od S_{n+1}. Zatim, neka je $\Sigma_1 = \Sigma \cap S_n$. Pošto je Σ_1 konačan podskup od S_n tada je on ispunjiv. Neka je $\mathfrak{M}$ neki model za skup Σ_1. Neka je $\{c_{F_1}, \ldots, c_{F_m}\}$ skup svih konstantskih simbola iz $\sigma_{n+1} \setminus \sigma_n$ koji se pojavljuju u formulama skupa Σ. Na σ_n–strukturi $\mathfrak{M}$ definiramo interpretaciju konstantskih simbola σ_{F_i} na sljedeći način:

$$c_{F_i} \mapsto \begin{cases} a \in |\mathfrak{M}| \ \text{ takav da vrijedi } \ \mathfrak{M} \models F_i[a], \ \text{ ako takav } \ a \ \text{ postoji} \\ \\ \text{proizvoljan } \ a \in |\mathfrak{M}|, \ \text{ inače} \end{cases}$$

Time smo dobili strukturu $\mathfrak{N}$ koja je očito model za skup rečenica Σ.

Neka je S' potpun konačno ispunjiv nadskup skupa formula $\cup S_n$ (iz Lindenbaumove leme slijedi da takav skup postoji). Očito je S' Henkinov skup formula. Iz teorema 1.36. slijedi da je S' ispunjiv skup formula. Neka je $\mathfrak{A}$ neki model za S'. Redukcijom strukture $\mathfrak{U}$ na signaturu σ_0 dobivamo traženi model za skup S_0. □

1.4.1 Definabilnost u logici prvog reda

Ako je S neki skup σ–formula tada uvodimo oznaku:

$$Mod(S) = \{\mathfrak{M} : \mathfrak{M} \ \text{ je } \sigma\text{–struktura takva da } \ \mathfrak{M} \models S\}$$

Definicija 1.38. *Neka je $\mathcal{K}$ neka klasa σ–struktura. Kažemo da je klasa $\mathcal{K}$* **elementarna** *ako postoji skup σ–formula S tako da vrijedi $Mod(S) = \mathcal{K}$.*

Primjeri elementarnih klasa:

- klasa svih parcijalno uređenih skupova
- klasa svih grupa
- klasa svih vektorskih prostora
- klasa svih prstenova
- klasa svih polja

Definicija 1.39. *Za neku klasu $\mathcal{K}$ σ–struktura kažemo da je* Δ**–elementarna** *ako postoji konačan skup σ–formula S tako da vrijedi $Mod(S) = \mathcal{K}$.*

Propozicija 1.40. *Neka je $\mathcal{K}$ Δ–elementarna klasa σ–struktura i S neki skup σ–formula tako da vrijedi $Mod(S) = \mathcal{K}$. Tada postoji konačan podskup $S' \subseteq S$ tako da vrijedi $Mod(S') = \mathcal{K}$.*

Dokaz. Pošto je po pretpostavci klasa $\mathcal{K}$ Δ–elementarna, tada postoji konačan skup rečenica Σ tako da vrijedi $\mathcal{K} = Mod(\Sigma)$. Pošto je Σ konačan skup formula, tada je dobro definirana formula $\bigwedge_{F\in\Sigma} F$. Očito vrijedi $\mathcal{K} = Mod(\bigwedge_{F\in\Sigma} F)$. Pošto $Mod(S) = \mathcal{K}$ tada posebno slijedi $S \models \bigwedge_{F\in\Sigma} F$. Iz **teorema kompaktnosti** slijedi da postoji konačan podskup $\{\varphi_1, \ldots, \varphi_n\}$ skupa S tako da vrijedi $\{\varphi_1, \ldots, \varphi_n\} \models \bigwedge_{F\in\Sigma} F$. Pošto $\{\varphi_1, \ldots, \varphi_n\} \subseteq S$ tada očito

$$Mod(\{\varphi_1, \ldots, \varphi_n\}) \supseteq Mod(S) = \mathcal{K}$$

U drugu ruku pošto $\{\varphi_1, \ldots, \varphi_n\} \models \bigwedge_{F\in\Sigma} F$ tada imamo

$$Mod(\{\varphi_1, \ldots, \varphi_n\}) \subseteq Mod(\bigwedge_{F\in\Sigma} F) = Mod(\Sigma) = \mathcal{K}$$

Time smo dokazali $\mathcal{K} = Mod(\{\varphi_1, \ldots, \varphi_n\})$. □

Propozicija 1.41. *Neka je $\mathcal{K}$ neka klasa σ–struktura. Sa $\mathcal{K}^c$ označimo klasu svih σ–struktura koje ne pripadaju $\mathcal{K}$. Tada vrijedi:*

klasa $\mathcal{K}$ je Δ–elementarna ako i samo ako klase $\mathcal{K}$ i $\mathcal{K}^c$ su elementarne

Dokaz. Pretpostavimo da su klase $\mathcal{K}$ i $\mathcal{K}^c$ elementarne. Neka su S_1 i S_2 skupovi formula za koje vrijedi $\mathcal{K} = Mod(S_1)$ i $\mathcal{K}^c = Mod(S_2)$. Očito vrijedi

$$\emptyset \;=\; \mathcal{K} \cap \mathcal{K}^c \;=\; Mod(S_1 \cup S_2)$$

To znači da skup formula $S_1 \cup S_2$ nije ispunjiv. Iz **teorema kompaktnosti** slijedi da postoje konačni podskupovi $\{\varphi_1, \ldots, \varphi_n\} \subseteq S_1$ i $\{\psi_1, \ldots, \psi_m\} \subseteq S_2$, takvi da skup formula $\{\varphi_1, \ldots, \varphi_n, \psi_1, \ldots, \psi_m\}$ nije ispunjiv. Tada očito vrijedi

$$Mod(\{\varphi_1, \ldots, \varphi_n\}) \cap Mod(\{\psi_1, \ldots, \psi_m\}) = \emptyset \qquad (*)$$

Zatim, iz $\{\varphi_1, \ldots, \varphi_n\} \subseteq S_1$ i $\{\psi_1, \ldots, \psi_m\} \subseteq S_2$ očito slijedi

$$Mod(\{\varphi_1, \ldots, \varphi_n\}) \supseteq Mod(S_1) = \mathcal{K} \qquad (**)$$

$$Mod(\{\psi_1, \ldots, \psi_m\}) \supseteq Mod(S_2) = \mathcal{K}^c \qquad (***)$$

Iz $(*)$, $(**)$ i $(***)$ slijedi $\mathcal{K} = Mod(\{\varphi_1, \ldots, \varphi_n\})$. Drugi smjer u tvrdnji propozicije slijedi direktno iz definicija. □

Primjer 1.42. *Klasa $\mathcal{K}_\infty$ svih beskonačnih skupova je elementarna, ali nije Δ–elementarna. Npr. za skup formula $S = \{\exists y_1 \ldots \exists y_n \bigwedge_{i \neq j} y_i \neq y_j : n \in \mathbb{N}\}$ očito vrijedi $Mod(S) = \mathcal{K}_\infty$ (promatramo samo normalne strukture). Kako bi dokazali da klasa $\mathcal{K}_\infty$ nije Δ–elementarna primijetimo prvo da klasa $\mathcal{K}_{<\infty}$ svih konačnih skupova nije elementarna. (Ako je S skup formula takav da za svaku konačnu strukturu $\mathfrak{M}$ vrijedi $\mathfrak{M} \models S$ tada iz Löweinheim–Skolemovog teorema slijedi da postoji beskonačna struktura $\mathfrak{N}$ tako da vrijedi $\mathfrak{N} \models S$). Očito vrijedi $\mathcal{K}_\infty^c = \mathcal{K}_{<\infty}$. Iz propozicije 1.41. slijedi da klasa $\mathcal{K}_\infty$ nije Δ–elementarna.*

Primjer 1.43. *Za fiksirani prosti broj p klasa svih polja karakteristike p je Δ–elementarna. Klasa $\mathcal{K}_0$ svih polja karakteristike nula je elementarna, ali nije Δ–elementarna.*

Označimo sa S_0 skup aksioma teorije polja (to su sve formule logike prvog reda!). Za proizvoljni prosti broj p sa $\overline{p}$ označimo term $1 + \ldots + 1$ (p–puta). Tada za

$$S = S_0 \cup \{\overline{2} \neq 0,\ \overline{3} \neq 0,\ \ldots\}$$

imamo $Mod(S) = \mathcal{K}_0$, pa je klasa $\mathcal{K}_0$ elementarna.

Pretpostavimo da je klasa $\mathcal{K}_0$ Δ–elementarna. Iz propozicije 1.40. slijedi da postoje prosti brojevi $p_1, \ldots, p_k$ tako da za konačan skup formula

$$S' = S_0' \cup \{\overline{p_1} \neq 0, \ldots, \overline{p_k} \neq 0\}$$

(S_0' je neki konačan podskup od S_0) vrijedi $Mod(S') = \mathcal{K}_0$. Neka je p prosti broj takav da je $p > p_i$, za svaki $i \in \{1, \ldots, k\}$. Tada očito vrijedi $\mathbb{Z}_p \models S'$, ali $\mathbb{Z}_p \notin \mathcal{K}_0$.

Klasa svih polja, čija je karakteristika različita od nule, nije elementarna. Klasa svih algebarski zatvorenih polja je elementarna, ali nije Δ–elementarna.

Primjer 1.44. *Neka je $(G, \circ)$ Abelova grupa, te $n \in \mathbb{N} \setminus \{0\}$ i $y \in G$. Tada sa ny označavamo $y \circ \ldots \circ y$ (n–puta). Za Abelovu grupu kažemo da je* **djeljiva** *ako za svaki $n \geq 1$ i $x \in G$ postoji $y \in G$ tako da vrijedi $ny = x$. Klasa svih djeljivih grupa je elementarna, ali nije Δ–elementarna.*

Samo ističemo da vrijedi sljedeće (vidi teorem 1.118. na strani 61) :

Neka je $\mathcal{K}$ neka klasa σ–struktura. Tada vrijedi:

a) Klasa $\mathcal{K}$ je elementarna ako i samo ako klasa $\mathcal{K}$ je zatvorena za ultraprodukte i elementarnu ekvivalenciju.

b) Klasa $\mathcal{K}$ je Δ–elementarna ako i samo ako klase $\mathcal{K}$ i $\mathcal{K}^c$ su zatvorene za ultraprodukte i elementarnu ekvivalenciju.

Pojam ultraprodukta ćemo definirati kasnije.

1.4.2 Neka proširenja logike prvog reda

Prethodni primjeri mogu nam poslužiti kao motivacija za razmatranje proširenja logike prvog reda. Ovdje navodimo neka proširenja logike prvog reda. U **logici drugog reda** dopuštena je i kvantifikacija po relacijskim i funkcijskim varijablama. U logici drugog reda mogu se definirati pojmovi "biti beskonačan" i "biti prebrojiv". No, u logici drugog reda ne vrijedi teorem kompaktnosti. To ističemo u sljedećoj propoziciji.

Propozicija 1.45. *Za logiku drugog reda ne vrijedi teorem kompaktnosti.*

Dokaz. Za svaki $n \in \mathbb{N},\ n \geq 2$ uvodimo formulu:

$$\varphi_{\geq n} \equiv \bigwedge_{0 \leq i < j \leq n} x_i \neq x_j$$

Zatim, neka je

$$\varphi_{fin} \equiv \text{"svaka injekcija na proizvoljnom skupu je i surjekcija"}$$

Lako je vidjeti da svaki konačan podskup od $\{\varphi_{fin}\} \cup \{\varphi_{\geq n} : n \geq 2\}$ ima model, ali sam skup nema model. □

Pošto ne vrijedi teorem kompkatnosti tada odmah slijedi da je u logici drugog reda nemoguće definirati relaciju izvoda $\vdash_{SO}$ analognu kao u logici prvog reda. To znači da za svaki skup formula $S \cup \{F\}$ ne vrijedi sljedeća ekvivalencija:

$$S \models F \qquad \text{ako i samo ako} \qquad S \vdash_{SO} F$$

Drugim riječima, u logici drugog reda ne vrijedi jaki teorem potpunosti. No, možemo se pitati vrijedi li tvrdnja za $S = \emptyset$, tj. vrijedi li za logiku drugog reda analogon Gödelovog teorema potpunosti. Može se pokazati da ne vrijedi, tj. da skup svih valjanih formula logike drugog reda nije rekurzivno prebrojiv.

Propozicija 1.46. *Za logiku drugog reda ne vrijedi ni Löwenheim–Skolemov teorem "na dolje".*

Dokaz. Definiramo formulu koja ima model, ali nema prebrojiv model.

$$\psi_{fin}(X) \equiv \text{"interpretacija od } X \text{ je konačna unarna relacija"}$$

Pomoću formule ψ_{fin} nije teško definirati sljedeću formulu.

$$\psi_p \equiv \text{"postoji relacija uređaja tako da}$$

$$\text{svaki element ima samo konačno mnogo prethodnika"}$$

Neka je $\psi_{nep} \equiv \neg\psi_p$. Očito za svaki model $\mathfrak{M}$ vrijedi:

$$\mathfrak{M} \models \psi_{nep} \qquad \text{ako i samo ako} \qquad \text{skup } |\mathfrak{M}| \text{ je neprebrojiv.} \ \square$$

U **beskonačnoj logici** dopuštene su beskonačne disjunkcije. Odnosno, točnije logika $L_{\omega_1\omega}$ dopušta i sljedeća pravila izgradnje formula:

ako je S prebrojiv skup formula tada su $\bigwedge S$ i $\bigvee S$ također formule.

Simbol $L_{\omega_1\omega}$ označava da je dozvoljeno prebrojivo mnogo ($< \omega_1$) konjunkcija i disjunkcija, te najviše konačno mnogo ($< \omega$) kvantifikatora. Löweinheim–Skolemov teorem "na dolje" vrijedi za logiku $L_{\omega_1\omega}$, a teorem kompaktnosti ne.

Promatraju se i druga proširenja logike prvog reda. Npr.: **višesortna logika prvog reda, slaba logika drugog reda, monadska logika drugog reda, logike s dodatnim kvantifikatorima**, itd. Logika prvog reda ima istaknuto mjesto među svim tim sistemima. O tome govore Lindströmovi teoremi. Njih razmatramo u poglavlju 1.15.

1.4.3 Ramseyev teorem

U grupi od 6 ljudi uvijek postoje 3 koje se međusobno poznaju, ili pak postoji grupa od 3 ljudi u kojoj nitko nikog ne poznaje. Kolika mora biti najmanja grupa ljudi tako da sigurno postoje 4 osobe koje se međusobno poznaju, ili pak postoji grupa od 4 osobe u kojoj nitko nikog ne poznaje?

Ovi primjeri su motivacijski primjeri za Ramseyev teorem koji jednostavno tvrdi da za svaki zadani $n \in \mathbb{N}$ postoji broj R_n tako da u svakoj grupi ljudi koja sadrži barem R_n ljudi, postoji grupa od n osoba koji se svi međusobno poznaju,

ili pak nitko nikog ne poznaje. Pošto je uobičajno Ramseyev teorem iskazati u terminima grafova tada prvo dajemo neke definicije iz teorije grafova.

Za proizvoljan skup V označimo $[V]^2 := \{\ \{a,b\} : a,b \in V, a \neq b\}$. **Graf** je uređeni par (V,E), gdje je V proizvoljan skup čije elemente nazivamo **čvorovi**, te $E \subseteq [V]^2$ čije elemente nazivamo **bridovi**. Za graf (U,F) kažemo da je **podgraf** grafa (V,E) ako je $U \subseteq V$, te je $F = E \cap [U]^2$. Za podgraf (U,F) grafa (V,E) kažemo da je **potpuni (prazni) podgraf** ako je $F = [U]^2$ $(F = \emptyset)$.

Teorem 1.47. *(Ramseyev teorem)*
Za svaki prirodan broj $n \in \mathbb{N} \setminus \{0\}$ postoji prirodan broj R_n (tzv. n–ti Ramseyev broj) tako da svaki graf koji ima najmanje R_n čvorova, sadrži barem jedan potpuni podgraf s n čvorova ili pak sadrži barem jedan prazan podgraf s n čvorova.

Vrijedi: $R_1 = 1$, $R_2 = 2$, $R_3 = 6$, ... Ramseyev teorem je relativno teško dokazati (vidi npr. D. Veljan, Kombinatorika i teorija grafova, ŠK, Zagreb) No, jednostavno je dokazati analogni rezultat za beskonačne grafove. Nakon toga ćemo relativno jednostavno primjenom tog rezultata i teorema kompaktnosti dokazati Ramseyev teorem.

Lema 1.48. *("Beskonačna" verzija Ramseyevog teorema)*
Svaki beskonačni graf (V,E) sadrži beskonačni potpun podgraf ili pak sadrži beskonačan prazan podgraf.

Dokaz. Neka je $a_0 \in V$ proizvoljan. Označimo:

$$V_\emptyset = \{x \in V \setminus \{a_0\} \ : \ \{a_0, x\} \notin E\}$$

$$V_\infty = \{x \in V \setminus \{a_0\} \ : \ \{a_0, x\} \in E\}$$

Očito vrijedi: $V_\emptyset \cup V_\infty = V$ i $V_\emptyset \cap V_\infty = \emptyset$. Pošto je po pretpostavci teorema skup V beskonačan, tada je barem od jedan od skupova $V_\emptyset$ i V_∞ beskonačan. Neka je

$$V_1 = \begin{cases} V_\emptyset, & \text{ako je skup } V_\emptyset \text{ beskonačan;} \\ V_\infty, & \text{inače.} \end{cases}$$

Neka je $a_1 \in V_1 \setminus \{a_0\}$ proizvoljan. Označimo:

$$W_\emptyset = \{x \in V_1 \setminus \{a_0, a_1\} \ : \ \{a_1, x\} \notin E\}$$

$$W_\infty = \{x \in V_1 \setminus \{a_0, a_1\} \ : \ \{a_1, x\} \in E\}$$

Pošto je skup $V_1 \setminus \{a_0, a_1\}$ beskonačan tada je barem jedan od skupova W_0 ili W_∞ beskonačan. Neka je

$$W_1 = \begin{cases} W_\emptyset, & \text{ako je skup } W_\emptyset \text{ beskonačan;} \\ W_\infty, & \text{inače.} \end{cases}$$

Na taj način konstruirali bi niz elemenata $a_0,\ a_1,\ a_2,\ \ldots$. Primijetimo da skup $\{a_n : n \in \mathbb{N}\}$ nije nužno potpun, a ni prazan podgraf. Npr. po definiciji elemenata a_n može npr. vrijediti $\{a_0, a_1\} \in E$, ali $\{a_1, a_2\} \notin E$. No, taj niz ipak ima važno sljedeće svojstvo:

$$(\forall n \in \mathbb{N})(\forall k > n)\{a_n, a_k\} \notin E \ \text{ ili } \ (\forall n \in \mathbb{N})(\forall k > n)\{a_n, a_k\} \in E$$

Neka je

$$B_1 = \{a_n \ : \ (\forall k > n)\{a_n, a_k\} \notin E\}$$

$$B_2 = \{a_n \ : \ (\forall k > n)\{a_n, a_k\} \in E\}$$

Očito vrijedi: $B_1 \cup B_2 = \{a_n : n \in \mathbb{N}\}$ i $B_1 \cap B_2 = \emptyset$, te je barem jedan od skupova B_i beskonačan. Dakle, ili je B_1 jedan beskonačan prazan podgraf, ili je B_2 jedan beskonačan potpun podgraf. □

Sada dokazujemo Ramseyev teorem. Pretpostavimo da Ramseyev teorem ne vrijedi, tj. da postoji $n_0 \in \mathbb{N}$ takav da ne postoji $R_{n_0} \in \mathbb{N}$ koji ima svojstvo da svaki graf s najmanje R_{n_0} čvorova sadrži potpuni podgraf s n_0 čvorova ili sadrži barem jedan prazan podgraf s n_0 čvorova. Odnosno,

$$(*) \begin{cases} \text{postoji } n_0 \in \mathbb{N} \text{ takav da za svaki } m \in \mathbb{N} \text{ postoji } p \geq m \\ \text{takav da postoji graf s } p \text{ čvorova koji ne sadrži potpuni} \\ \text{podgraf s } n_0 \text{ čvorova, a ni prazan podgraf s } n_0 \text{ čvorova.} \end{cases}$$

Uvodimo oznake za formule:

$$\varphi_k \equiv \quad \exists y_1 \ldots \exists y_k \bigwedge_{i \neq j} y_i \neq y_j, \quad \text{za svaki} \quad k \in \mathbb{N} \setminus \{0,1\}$$

$$\begin{aligned} Prazan_{n_0} \equiv \quad & \exists y_1 \ldots \exists y_{n_0} \Big(\bigwedge_{i \neq j} y_i \neq y_j \ \wedge \forall y (\bigvee_{i=1}^{n_0} y = y_i) \Big) \wedge \\ & \neg \exists x \exists y \ E(x,y) \end{aligned}$$

$$\begin{aligned} Potpun_{n_0} \equiv \quad & \exists y_1 \ldots \exists y_{n_0} \Big(\bigwedge_{i \neq j} y_i \neq y_j \ \wedge \forall y (\bigvee_{i=1}^{n_0} y = y_i) \Big) \wedge \\ & \forall x \forall y (x \neq y \rightarrow E(x,y)) \end{aligned}$$

Neka je $\Sigma = \{\varphi_k : k \in \mathbb{N} \setminus \{0,1\} \ \cup \ \{\neg Prazan_{n_0}, \ \neg Potpun_{n_0}\}$. Tvrdimo da je skup formula Σ konačno ispunjiv. Neka je Σ_0 proizvoljan konačan podskup od Σ. Neka je $m \in \mathbb{N}$ najveći prirodan broj takav da je $\varphi_m \in \Sigma_0$. Iz pretpostavke $(*)$ slijedi da postoji $p \geq m$ i graf G s p čvorova koji ne sadrži potpun podgraf s n_0 čvorova, a ni prazan podgraf s n_0 čvorova. Iz ovog posljednje očito slijedi $G \models \Sigma_0$. Pošto je, dakle, skup Σ konačno ispunjiv, tada iz teorema kompaktnosti slijedi da za Σ postoji model $\mathfrak{M}$. Očito je $\mathfrak{M}$ beskonačni graf koji ne sadrži potpun podgraf s n_0 čvorova, a ni prazan podgraf s n_0 čvorova. Tada, očito, graf $\mathfrak{M}$ ne sadrži ni beskonačni potpun podgraf, a ni beskonačan prazan podgraf, što je u suprotnosti s prije dokazanom lemom ("beskonačna" verzija Ramseyevog teorema). □

1.5 Löwenheim–Skolemov teorem "na dolje"

Kao još jednu primjenu Tarski–Vaughtov kriterija o elementarnim podmodelima ovdje dajemo dokaz Löwenheim–Skolemovog teorema "na dolje" u jačoj formi od one koju je navedena u diplomskom studiju, tj. koja je dana u skripti [28]. Prvo podsjećamo na izreke Löwenheim–Skolemovih teorema koje su dane na diplomskom studiju.

Löwenheim–Skolemov teorem "na dolje"
Svaka teorija prvog reda koja ima beskonačan model ima i prebrojiv model. (Važno je naglasiti da se ovdje misli na proizvoljne modele, a ne samo normalne).

Löwenheim–Skolemov teorem "na gore"
Neka je α beskonačan kardinalni broj i T proizvoljna konzistentna teorija prvog reda. Tada postoji model za T čiji je kardinalni broj jednak α.

Löwenheim–Skolemov teorem "na gore" ćemo dokazati nakon što obradimo metodu dijagrama. Za dokaz teorema koristit ćemo lemu o dijagramu i teorem kompaktnosti. Löwenheim–Skoelmov teorem "na gore" koristit ćemo za dokaz Łos–Vaughtovog testa za potpunost teorije.
U ovoj točki dopuštamo da skup nelogičkih simbola σ i skup svih varijabli mogu biti proizvoljnog kardinaliteta. Naravno, skup svih varijabli mora biti barem prebrojiv. Sa L_σ označavamo uniju skupa svih varijabli i skupa σ. Sada navodimo iskaz Löwenheim–Skolemovog teorema koji nam je glavni cilj u ovoj točki.

> *Neka je $\mathfrak{M}$ neka σ–struktura i $B \subseteq |\mathfrak{M}|$, te neka je $kard(L_\sigma) \leq kard(\mathfrak{M})$. Tada postoji elementarni podmodel $\mathfrak{U}$ od $\mathfrak{M}$, tako da vrijedi $B \subseteq |\mathfrak{U}|$ i $kard(\mathfrak{U}) = \max\{kard(B),\ kard(L_\sigma)\}$.*

Ovaj teorem u nazivu ima "na dolje" jer je $\mathfrak{U}$ minimalni podmodel u smislu kardinalnosti s danim svojstvima. Koliko je ovaj teorem općenitiji od teorema istog naziva navedenog na dodiplomskom studiju? Prije svega promatraju se proizvoljni alfabeti prvog reda, a ne samo prebrojivi. Zatim, tvrdi se egzistencija elementarnog podmodela koji mora sadržavati zadani podskup nosača. Primijetite da sada ne spominjemo teorije prvog reda, već je na početku zadana neka struktura $\mathfrak{M}$. To zapravo znači da promatramo teoriju $Th(\mathfrak{M}) = \{F : \mathfrak{M} \models F\}$.

Pošto ćemo ga nekoliko puta spominjati (zapravo, već smo ga spomenuli prilikom dokaza Fraïsséovog teorema) ovdje navodimo:

Knaster–Tarskijev teorem.

Neka je A proizvoljan skup, te $F : \mathcal{P}(A) \to \mathcal{P}(A)$ rastuća funkcija. Tada postoje $X_1, X_2 \subseteq A$ tako da vrijedi $F(X_i) = X_i$, te je X_1 najmanja fiksna točka, a X_2 je najveća fiksna točka funkcije F.

Pojmove i činjenice iz teorije skupova koje spominjemo možete pogledati u skripti [29].

Neka je $\mathfrak{M}$ neka σ–struktura, te neka je $B \subseteq |\mathfrak{M}|$ proizvoljan. Definiramo preslikavanje $F : \mathcal{P}(|\mathfrak{M}|) \to \mathcal{P}(|\mathfrak{M}|)$ sa

$$\begin{aligned} F(X) &= B \bigcup X \bigcup \{f^{\mathfrak{M}}(a_1, \ldots, a_k) : f \in \sigma,\ a_1, \ldots, a_k \in B \cup X\} \\ &\quad \bigcup \{c^{\mathfrak{M}} : c \in \sigma\} \end{aligned}$$

Očito je funkcija F rastuća pa iz Knaster–Tarskijevog teorema slijedi da postoji (najmanja!) fiksna točka X_0 za F. Očito je X_0 nosač podmodela od $\mathfrak{M}$. Taj podmodel nazivavamo **podmodel generiran sa skupom** B. Sljedeća propozicija jednostavno govori da je kardinalnost podmodela generiranog nekim skupom B jednaka $kard(B)$, ako je kardinalnost od B "dovoljno" velika.

Propozicija 1.49. *Neka je $\mathfrak{M}$ neka σ–struktura, te $B \subseteq |\mathfrak{M}|$ takav da vrijedi $kard(L_\sigma) \leq kard(B)$. Označimo sa $\mathfrak{N}$ podmodel od $\mathfrak{M}$ generiran sa skupom B. Tada vrijedi $kard(\mathfrak{N}) = kard(B)$.*

Dokaz. Svaki element skupa $|\mathfrak{N}|$ je interpretacija nekog σ–terma s "parametrima iz skupa B" (umjesto varijabli u terme stavljamo elemente skupa B. Npr. ako je $f^4 \in \sigma$, te $c_1, c_2 \in \sigma$ i $b_1, b_2 \in B$ tada je $f^4(b_1, c_1, c_2, b_2)$ jedan term s parametrima iz skupa B). Skup svih σ–terma s parametrima iz skupa B je podskup skupa svih konačnih nizova od $B \cup \sigma$, tj. skupa $(B \cup \sigma)^*$. Iz toga slijedi $kard(\mathfrak{N}) \leq kard((B \cup \sigma)^*) = kard(B)$.
Pošto je $B \subseteq |\mathfrak{N}|$ tada je $kard(B) \leq kard(\mathfrak{N})$. Iz Cantor–Schröder–Bernsteinovog teorema slijedi $kard(\mathfrak{N}) = kard(B)$. □

Sljedeću lemu ćemo koristiti u dokazu Löwenheim–Skolemovog teorema "na dolje".

Lema 1.50. *Neka je $\mathfrak{M}$ neka σ–struktura i $B \subseteq |\mathfrak{M}|$. Neka je μ kardinalni broj takav da $kard(L_\sigma) + kard(B) \leq \mu \leq kard(\mathfrak{M})$. Tada postoji podmodel $\mathfrak{N}$ od $\mathfrak{M}$, takav da $B \subseteq |\mathfrak{N}|$ i $kard(\mathfrak{N}) = \mu$.*

Dokaz. Neka je B_0 proizvoljan podskup od $|\mathfrak{M}|$ takav da $B \subseteq B_0$ i $kard(B_0) = \mu$. (Primijetimo da takav podskup B_0 postoji, jer je po pretpostavci leme $\mu \leq kard(\mathfrak{M})$ i $B \subseteq |\mathfrak{M}|$). Definiramo funkciju $F : \mathcal{P}(|\mathfrak{M}|) \to \mathcal{P}(|\mathfrak{M}|)$ sa:

$$F(X) = X \bigcup B_0 \bigcup \{c^{\mathfrak{M}} : c \in \sigma\}$$

$$\bigcup \{f^{\mathfrak{M}}(a_1, \ldots, a_n) : f \in \sigma,\ a_i \in B_0 \cup X\}$$

(Funkcija F je rastuća, pa iz Knaster–Tarskijevog teorema slijedi da za F postoji fiksna točka X_0. Skup X_0 je nadskup od B, te je nosač jednog podmodela od $\mathfrak{M}$. No, moramo pažljivije provesti razmatranja kako bismo dobili podmodel kardinalnosti μ.)

Za svaki $n \in \mathbb{N}$ definiramo $B_{n+1} = F(B_n)$. Pošto je $kard(B_0) = \mu$ i $kard(\sigma) \leq \mu$, tada za svaki $n \in \mathbb{N}$ vrijedi $kard(B_n) = \mu$. Tada je $kard(\bigcup_{n\in\mathbb{N}} B_n) = \mu$ (Ovdje koristimo sljedeće svojstvo kardinalnih brojeva: ako je $\aleph_0 \leq \mu$ tada $\aleph_0 \cdot \mu = \mu$). Očito je skup $\bigcup_{n\in\mathbb{N}} B_n$ jedna fiksna točka funkcije F, tj. $\bigcup_{n\in\mathbb{N}} B_n$ je nosač jednog podmodela od $\mathfrak{M}$ čija je kardinalnost μ, te sadrži skup B. □

Teorem 1.51. *(Löwenheim–Skolemov teorem "na dolje")*
Neka je $\mathfrak{M}$ neka σ–struktura i $B \subseteq |\mathfrak{M}|$, te neka je $kard(L_\sigma) \leq kard(\mathfrak{M})$. Tada postoji σ–struktura $\mathfrak{U}$ takva da: $\mathfrak{U} \prec \mathfrak{M}$, $B \subseteq |\mathfrak{U}|$ i $kard(\mathfrak{U}) = \max\{kard(B),\ kard(L_\sigma)\}$.

Dokaz. Dokazujemo prvo tvrdnju teorema uz pretpostavku $kard(B) \geq kard(L_\sigma)$. Pošto je $kard(L_\sigma)$ beskonačni kardinalni broj tada vrijedi $kard(B)+kard(L_\sigma) = kard(B)$. Tada iz prethodne leme (zadavši $\mu = kard(B)$) slijedi da postoji podmodel $\mathfrak{N}$ od $\mathfrak{M}$ takav da je $B \subseteq |\mathfrak{N}|$ i $kard(\mathfrak{N}) = kard(B)$. (Primjenom podmodela $\mathfrak{N}$ definirat ćemo traženi elementarni podmodel $\mathfrak{U}$. Nakon toga ćemo razmatrati slučaj kada je $kard(B) < kard(L_\sigma)$). Induktivno definiramo niz (A_n) podskupova od $|\mathfrak{M}|$ stavljajući prvo $A_0 = |\mathfrak{N}|$. Pretpostavimo da smo za neki $i \in \mathbb{N}$ definirali skup A_i. Kako bi definirali skup A_{i+1} tada za svaku σ–formulu $F(v_0, v_1, \ldots, v_n)$ i svaki niz elemenata $\vec{a} = (a_1, \ldots, a_n)$ iz A_i, za koji vrijedi $\mathfrak{M} \models \exists v_0 F[a_1, \ldots, a_n]$, izaberemo element $a_{F,\vec{a}} \in |\mathfrak{M}|$ tako da vrijedi $\mathfrak{M} \models F[a_{F,\vec{a}}, a_1, \ldots, a_n]$. Sada definiramo

$$B_i := A_i \bigcup \{a_{F,\vec{a}} : F(v_0, v_1, \ldots, v_n) \text{ je } \sigma\text{–formula},$$

$$a_1, \ldots, a_n \in A_i,\ \mathfrak{M} \models F[a_{F,\vec{a}}, a_1, \ldots, a_n]\}$$

Neka je A_{i+1} nosač podmodela koji je generiran sa skupom B_i. Primijetimo da za upravo definirani niz skupova (A_i) vrijedi:

a) $A_0 \subseteq A_1 \subseteq A_2 \subseteq \ldots$

b) $kard(A_i) = kard(A_0)$, za svaki $i \in \mathbb{N}$ (zbog propozicije **??**)

c) Skup $\cup A_i$ sadrži sve interpretacije konstantskih simbola, te je zatvoren za interpretacije svih funkcijskih simbola iz σ. Dakle, $\cup A_i$ je nosač nekog podmodela $\mathfrak{U}$

Vrijedi:

$$\begin{aligned} kard(\mathfrak{U}) &= kard(\cup_{i\in\mathbb{N}} A_i) = \sum_{i\in\mathbb{N}} kard(A_i) = \\ &= \sum_{i\in\mathbb{N}} kard(A_0) = \aleph_0 \cdot kard(A_0) = \\ &= \max\{kard(A_0), \aleph_0\} = kard(A_0) = \\ &= kard(B) \end{aligned}$$

Primjenom Tarski–Vaughtov kriterija o elementarnim podmodelima dokazujemo da vrijedi $\mathfrak{U} \prec M$. Neka je $F(v_0, v_1, \ldots, v_n)$ neka σ–formula, te $a_1, \ldots, a_n \in \cup A_i$ takvi da vrijedi $\mathfrak{M} \models \exists v_0 F[a_1, \ldots, a_n]$. Bili smo primijetili da je niz (A_i) rastući niz skupova. Tada postoji $i \in \mathbb{N}$ takav da je $a_1, \ldots, a_n \in A_i$. Iz definicije skupa A_{i+1} slijedi da postoji $a_{F,\vec{a}} \in A_{i+1}$ tako da vrijedi $\mathfrak{M} \models F[a_{F,\vec{a}}, a_1, \ldots, a_n]$. Iz Tarski–Vaughtov kriterija o elementarnim podmodelima slijedi $\mathfrak{U} \prec M$.

Rezimirajmo: ako je $kard(B) \geq kard(L_\sigma)$ tada smo dokazali egzistenciju elementarnog podmodela $\mathfrak{U}$ od $\mathfrak{M}$ za koju vrijedi $B \subseteq |\mathfrak{U}|$ i $kard(\mathfrak{U}) = kard(B)$, tj. $kard(\mathfrak{U}) = \max\{kard(B), kard(L_\sigma)\}$.
Promotrimo sada slučaj kada je $kard(B) < kard(L_\sigma)$. Neka je B' proizvoljan podskup od $|\mathfrak{M}|$ za koji vrijedi $B \subseteq B'$ i $kard(B') = kard(L_\sigma)$. Primjenom prethodno dokazane tvrdnje na skup B' slijedi da postoji elementarni podmodel $\mathfrak{U}'$ od $\mathfrak{M}$ tako da vrijedi $B' \subseteq |\mathfrak{U}'|$ i $kard(\mathfrak{U}') = \max\{kard(B'), kard(L_\sigma)\}$.
Očito vrijedi $B \subseteq |\mathfrak{U}'|$, te $kard(\mathfrak{U}') = \max\{kard(B), kard(L_\sigma)\}$. □

Primjer 1.52. *1. Neka je $\sigma = \{+, \cdot, 0, 1\}$ (signatura teorija polja). Neka je sa $\mathfrak{M}$ označeno polje realnih brojeva. Iz Löwenheim–Skolemovog teorema "na dolje" slijedi da postoji prebrojivo polje $\mathfrak{N}$ tako da vrijedi $\mathfrak{N} \prec \mathfrak{M}$.*

2. **Skolemov paradoks**. *Ako za teoriju skupova ZF postoji model tada za nju postoji i prebrojiv model. Pošto se u ZF može dokazati egzistencija neprebrojivih skupova (npr. $\mathbb{R}$), kako ZF može imati prebrojiv model?*

Odgovor je jednostavan: pojam prebrojivosti promatran u samom modelu i izvan modela nije isti.

1.6 Metoda dijagrama

Metoda dijagrama nam omogućava konstrukciju proširenja modela i elementarnih proširenja. Prije nego što napišemo definiciju dijagrama strukture prisjetimo se jednog analognog pojma. Grupe se mogu zadavati na razne načine. Jedan način je zadavanje tablice binarne operacije. Iz tablice možemo pročitati sve informacije o grupi. Uočimo ovdje još jedan detalj. Kako bismo mogli napisati tablicu za grupu moramo imati simbol za svaki element grupe.

Prije definicije dijagrama uvedimo jednu oznaku. Neka je $\mathfrak{M}$ neka σ–struktura. Označimo sa $\sigma_{\mathfrak{M}}$ skup nelogičkih simbola koji je dobiven dodavanjem skupu σ novih konstantskih simbola za svaki element od $\mathfrak{M}$. Dakle, $\sigma_{\mathfrak{M}} = \sigma \cup \{\overline{a} : a \in |\mathfrak{M}|\}$, pri čemu je za svaki $a \in |\mathfrak{M}|$ sa $\overline{a}$ označen konstantski simbol tako da vrijedi: $\overline{a} \notin \sigma$, te za $a \neq b$ imamo $\overline{a} \neq \overline{b}$. Na taj način smo za svaki element strukture u jezik dodali njegovo ime.

Za danu σ–strukturu $\mathfrak{M}$ sa $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|}$ označavamo $\sigma_{\mathfrak{M}}$–strukturu čiji je nosač $|\mathfrak{M}|$, za svaki simbol $s \in \sigma$ pripadna interpretacija je jednaka $s^{\mathfrak{M}}$, te za svaki $a \in |\mathfrak{M}|$ definiramo da je interpretacija konstantskog simbola $\overline{a}$ jednaka a.

Propozicija 1.53. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Tada vrijedi:*

1. *ako $\mathfrak{M} \subseteq \mathfrak{N}$ tada $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|} \subseteq (\mathfrak{N}, a)_{a\in|\mathfrak{M}|}$*
2. *ako $\mathfrak{M} \simeq \mathfrak{N}$ tada $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|} \simeq (\mathfrak{N}, a)_{a\in|\mathfrak{M}|}$*
3. *ako $\mathfrak{M} \prec \mathfrak{N}$ tada $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|} \prec (\mathfrak{N}, a)_{a\in|\mathfrak{M}|}$*

Definicija 1.54. *Neka je $\mathfrak{M}$ neka σ–struktura.* **Jednostavni dijagram** *strukture $\mathfrak{M}$ je sljedeći skup $\sigma_{\mathfrak{M}}$ rečenica:*

$$\Delta(\mathfrak{M}) = \{G(\overline{a_1}, \ \ldots, \overline{a_n}) \ : \ G \ \text{ je } \underline{\text{otvorena } \sigma\text{–formula}},$$
$$a_1, \ldots, a_n \in |\mathfrak{M}|, \ \text{ i vrijedi } \ \mathfrak{M} \models G[a_1, \ldots, a_n]\}$$

Potpuni dijagram *strukture $\mathfrak{M}$ je sljedeći skup $\sigma_{\mathfrak{M}}$–rečenica:*

$$\mathcal{D}(\mathfrak{M}) = \{F(\overline{a_1}, \ \ldots, \overline{a_n}) \ : \ F(v_1, \ldots, v_n) \ \text{ je } \underline{\sigma\text{–formula}},$$
$$a_1, \ldots, a_n \in |\mathfrak{M}|, \ \text{ i vrijedi } \ \mathfrak{M} \models F[a_1, \ldots, a_n]\}$$

Neka su σ i σ' dvije signature, takve da vrijedi $\sigma \subseteq \sigma'$. Neka je $\mathfrak{M}$ neka σ–struktura, a $\mathfrak{M}'$ neka σ'–struktura. Kažemo da je $\mathfrak{M}$ jedna σ–**redukcija** od $\mathfrak{M}'$ ako vrijedi $|\mathfrak{M}| = |\mathfrak{M}'|$, te $s^{\mathfrak{M}} = s^{\mathfrak{M}'}$, za svaki $s \in \sigma$. Kažemo još da je $\mathfrak{M}'$ jedna σ'–**ekspanzija** od $\mathfrak{M}$.

Lema 1.55. *(Lema o dijagramu)*
Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Tada vrijedi:

a) strukutru $\mathfrak{M}$ je moguće smjestiti u strukturu $\mathfrak{N}$ ako i samo ako postoji $\sigma_{\mathfrak{M}}$–ekspanzija od $\mathfrak{N}$ koja je model za jednostavni dijagram $\Delta(\mathfrak{M})$

b) strukutru $\mathfrak{M}$ je moguće elementarno smjestiti u strukturu $\mathfrak{N}$ ako i samo ako postoji $\sigma_{\mathfrak{M}}$–ekspanzija od $\mathfrak{N}$ koja je model za potpuni dijagram $\mathcal{D}(\mathfrak{M})$

Dokaz. Pretpostavimo prvo da je strukturu $\mathfrak{M}$ moguće smjestiti u strukturu $\mathfrak{N}$. Tada postoji podmodel $\mathfrak{A} \subseteq \mathfrak{N}$ tako da vrijedi $\mathfrak{M} \simeq \mathfrak{A}$. Neka je f neki izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{A}$. Označimo $\mathfrak{N}' = (\mathfrak{N}, f(a))_{a\in|\mathfrak{M}|}$.

Tvrdimo da je $\sigma_{\mathfrak{M}}$–struktura $\mathfrak{N}'$ jedan model za $\Delta(\mathfrak{M})$. Neka je $F(\overline{a_1}, \ldots, \overline{a_n})$ proizvoljna formula iz $\Delta(\mathfrak{M})$. Tada vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$. Iz ovog posljednjeg i činjenice da je f izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{A}$, očito slijedi da vrijedi i $\mathfrak{A} \models F[f(a_1), \ldots, f(a_n)]$. Pošto je F formula bez kvantifikatora, te imamo da vrijedi $\mathfrak{A} \subseteq \mathfrak{N}$, tada $\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$. Iz ovog posljednjeg očito slijedi $(\mathfrak{N}, f(a))_{a\in|\mathfrak{M}|} \models F(\overline{a_1}, \ldots, \overline{a_n})$, tj. imamo da vrijedi $\mathfrak{N}' \models F(\overline{a_1}, \ldots, \overline{a_n})$.
Dokažimo sada obrat. Pretpostavimo da je $\sigma_{\mathfrak{M}}$–ekspanzija $\mathfrak{N}'$ strukture $\mathfrak{N}$ jedan model za jednostavni dijagram $\Delta(\mathfrak{M})$. Definiramo funkciju $g : |\mathfrak{M}| \to |\mathfrak{N}|$ sa $g(a) = \overline{a}^{\mathfrak{N}'}$. Tvrdimo da je funkcija g smještenje strukture $\mathfrak{M}$ u strukturu $\mathfrak{N}$. U tu svrhu dokazujemo da je g injekcija i jaki homomorfizam. Neka su $a, b \in |\mathfrak{M}|$, $a \neq b$ proizvoljni. Očito vrijedi: $\mathfrak{M} \models (x \neq y)[a, b]$. To znači da vrijedi $\overline{a} \neq \overline{b} \in \Delta(\mathfrak{M})$. Pošto po pretpostavci leme imamo $\mathfrak{N}' \models \Delta(\mathfrak{M})$, tada posebno vrijedi $\mathfrak{N}' \models \overline{a} \neq \overline{b}$, odnosno $\overline{a}^{\mathfrak{N}'} \neq \overline{b}^{\mathfrak{N}'}$. Time imamo $g(a) \neq g(b)$. Dakle, funkcija g je injekcija.
Sada dokazujemo da je funkcija g jaki homomorfizam. U tu svrhu za svaki nelogički simbol iz σ provjeravamo uvjet iz definicije. Neka je $c \in \sigma$ proizvoljan konstantski simbol. Označimo $a = c^{\mathfrak{M}}$. Tada vrijedi: $g(c^{\mathfrak{M}}) = g(a) = \overline{a}^{\mathfrak{N}'}$. Očito vrijedi $\overline{a} = c \in \Delta(\mathfrak{M})$. No, pošto je $\mathfrak{N}'$ model za $\Delta(\mathfrak{M})$, tada posebno imamo $\mathfrak{N}' \models \overline{a} = c$, tj. $\overline{a}^{\mathfrak{N}'} = c^{\mathfrak{N}'}$. Sada iz $g(c^{\mathfrak{M}}) = \overline{a}^{\mathfrak{N}'}$ i $\overline{a}^{\mathfrak{N}'} = c^{\mathfrak{N}'}$ slijedi $g(c^{\mathfrak{M}}) = c^{\mathfrak{N}'}$. No, pošto je $\mathfrak{N}'$ ekspanzija σ–strukture $\mathfrak{N}$, tada je po definiciji $c^{\mathfrak{N}} = c^{\mathfrak{N}'}$. Time smo dokazali da vrijedi $g(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$. Sasvim analogno se dokazuje tvrdnja za funkcijske i relacijske simbole iz σ.
Tvrdnja b) dokazuje se sasvim analogno. □

Napomena 1.56. *Neka je $\mathfrak{M}$ proizvoljna σ–struktura. Pretpostavimo da smo na neki način uspjeli konstruirati $\sigma_{\mathfrak{M}}$–strukturu $\mathfrak{N}'$ koja je model za jednostavni (potpuni) dijagram $\Delta(\mathfrak{M})$ (odnosno, $\mathcal{D}(\mathfrak{M})$). Označimo sa $\mathfrak{N}$ pripadnu σ–redukciju od $\mathfrak{N}'$. Iz leme o dijagramu slijedi da je $\mathfrak{M}$ moguće (elementarno) smjestiti u strukturu $\mathfrak{N}$. Lako je vidjeti da bez smanjenja općenitosti možemo*

tada pretpostaviti da zapravo vrijedi $\mathfrak{M} \subseteq \mathfrak{N}$ *(odnosno* $\mathfrak{M} \prec \mathfrak{N}$*.) Upravo opisani postupak konstrukcije (elementarnog) proširenja zadane strukture nazivamo* **metoda dijagrama**.

Sada dajemo jednu vrlo jednostavnu primjenu metode dijagrama.

Propozicija 1.57. *Neka je* $\mathfrak{M}$ *neka beskonačna* σ*–struktura. Tada postoji* σ*–struktura* $\mathfrak{N}$ *za koju vrijedi* $\mathfrak{M} \neq \mathfrak{N}$ *i* $\mathfrak{M} \prec \mathfrak{N}$.

Dokaz. Neka je c novi konstantski simbol koji ne pripada skupu $\sigma_{\mathfrak{M}}$. Zatim, definiramo skup formula

$$S := \mathcal{D}(\mathfrak{M}) \bigcup \{c \neq \overline{a} : a \in |\mathfrak{M}|\}$$

Neka je S' proizvoljan konačan podskup od S. Tada postoji konačno mnogo $a \in |\mathfrak{M}|$ tako da se $\overline{a}$ pojavljuje u nekoj formuli skupa S'. Pošto je po pretpostavci skup $|\mathfrak{M}|$ beskonačan tada postoji $a_0 \in |\mathfrak{M}|$ takav da se konstantski simbol $\overline{a_0}$ ne pojavljuje niti u jednoj formuli skupa S'.

Neka je sa $\mathfrak{M}'$ označena $(\sigma_{\mathfrak{M}} \cup \{c\})$–ekspanzija od $(\mathfrak{M}, a)_{a \in |\mathfrak{M}|}$ pri čemu definiramo da je interpretacija konstantskog simbola c jednaka a_0. Očito vrijedi $\mathfrak{M}' \models S'$.

Iz **teorema kompaktnosti** slijedi da postoji barem jedan model za skup S. Dakle, postoji $(\sigma_{\mathfrak{M}} \cup \{c\})$–struktura $\mathfrak{N}'$ za koju vrijedi

$$\mathfrak{N}' \models \mathcal{D}(\mathfrak{M}) \bigcup \{c \neq \overline{a} : a \in |\mathfrak{M}|\}$$

Posebno, pošto je $\mathfrak{N}'$ model potpunog dijagrama $\mathcal{D}(\mathfrak{M})$ iz leme o dijagramu slijedi da je u σ–redukciju $\mathfrak{N}$ od $\mathfrak{N}'$ moguće elementarno smjestiti strukturu $\mathfrak{M}$. No, kao što smo već i bili spomenuli, strukturu $\mathfrak{N}$ možemo promatrati kao elementarno proširenje od $\mathfrak{M}$. Pošto vrijedi $\mathfrak{N}' \models \{c \neq \overline{a} : a \in |\mathfrak{M}|\}$, tada imamo $\mathfrak{M} \neq \mathfrak{N}$. □

1.7 Löwenheim–Skolemov teorem "na gore"

Vrlo važna primjena metode dijagrama je dokaz Löwenheim–Skolemovog teorema "na gore". Prisjetimo se izreke tog teorema koja je dana u dodiplomskom kolegiju *Matematička logika*, odnosno u skripti [28].

Löwenheim–Skolemov teorem "na gore"
Neka je α beskonačan kardinalni broj i T proizvoljna konzistentna teorija prvog reda. Tada postoji model za T čiji je kardinalni broj jednak α.

Sada dajemo sljedeću pojačanu verziju.

Teorem 1.58. *(Löwenheim–Skolemov teorem "na gore").*
Neka je $\mathfrak{M}$ neka beskonačna σ–struktura, te neka je λ kardinalni broj za kojeg vrijedi $\lambda \geq \max\{kard(\mathfrak{M}), kard(L_\sigma)\}$. Tada postoji σ–struktura $\mathfrak{N}$ za koju vrijedi $\mathfrak{M} \prec \mathfrak{N}$ i $kard(\mathfrak{N}) = \lambda$.

Dokaz. Dokazujemo prvo da postoji σ–struktura $\mathfrak{A}$ za koju vrijedi $\mathfrak{M} \prec \mathfrak{A}$ i $kard(\mathfrak{A}) \geq \lambda$. Za svaki kardinalni broj $i < \lambda$ uvodimo novi konstantski simbol c_i koji ne pripada σ, te definiramo sljedeći skup formula:

$$S = \mathcal{D}(\mathfrak{M}) \bigcup \{c_i \neq c_j : i, j < \lambda,\ i \neq j\}$$

Lako je vidjeti da je svaki konačan podskup od S ispunjiv (struktura $\mathfrak{M}$ je beskonačna pa uvijek za konačan $S' \subseteq S$ možemo definirati neku ekspanziju od $\mathfrak{M}$). Iz **teorema kompaktnosti** slijedi da postoji model $\mathfrak{A}'$ za skup formula S. Označimo sa $\mathfrak{A}$ pripadnu σ–redukciju od $\mathfrak{A}'$. Pošto $\mathfrak{A}' \models \mathcal{D}(\mathfrak{M})$ tada iz leme o dijagramu slijedi da strukturu $\mathfrak{M}$ možemo smjestiti u $\mathfrak{A}$. Bez smanjenja općenitosti možemo pretpostaviti da je $\mathfrak{M} \prec \mathfrak{A}$. Očito je $kard(\mathfrak{A}') \geq \lambda$, pa iz $|\mathfrak{A}| = |\mathfrak{A}'|$ slijedi i $kard(\mathfrak{A}) \geq \lambda$.

Preostalo je primjenom upravo dokazane tvrdnje dokazati tvrdnju teorema. Iz upravo dokazane tvrdnje slijedi da postoji elementarno proširenje $\mathfrak{A}$ od $\mathfrak{M}$ takvo da je $kard(\mathfrak{A}) \geq \lambda$. Neka je A proizvoljan podskup od $|\mathfrak{A}|$ za koji vrijedi $|\mathfrak{M}| \subseteq A$ i $kard(A) = \lambda$. Iz dokazanog Löwenheim–Skolemovog teorema "na dolje" slijedi da postoji σ–struktura $\mathfrak{N}$ za koju vrijedi

$$A \subseteq |\mathfrak{N}|, \quad \mathfrak{N} \prec \mathfrak{A}, \quad \text{te} \quad kard(\mathfrak{N}) = \lambda.$$

Primijetimo još samo da iz $\mathfrak{M} \prec \mathfrak{A}$, $\mathfrak{N} \prec \mathfrak{A}$ i $\mathfrak{M} \subseteq \mathfrak{N}$ primjenom propozicije 1.14. slijedi $\mathfrak{M} \prec \mathfrak{N}$. □

1.8 Łos–Vaughtov test potpunosti

Za zadanu signaturu σ proizvoljan skup σ–rečenica nazivamo **teorija**.

Definicija 1.59. *Za ispunjivu teoriju T kažemo da je* **kategorična** *ako su svi njeni modeli izomorfni.*

Iz Löwenheim–Skolemovog teorema "na gore" slijedi da niti jedna ispunjiva teorija nije kategorična. Iz tog razloga uvodimo pojam λ–kategoričnosti.

Definicija 1.60. *Neka je λ neki kardinalni broj. Kažemo da je neka teorija T* λ–**kategorična** *ako T ima barem jedan model kardinalnosti λ i ako su svi njeni modeli kardinalnosti λ izomorfni.*

Iz Cantorovog teorema o uređajnoj karakteristici skupa $\mathbb{Q}$ slijedi da je teorija gustih prebrojivih linearnih uređaja bez krajnjih točaka $\aleph_0$–kategorična.

Sada nam je cilj dokazati Łos–Vaughtov test potpunosti u kojem se primjenjuje λ–kategoričnost. U tu svrhu prvo dokazujemo sljedeću lemu.

Lema 1.61. *Neka je T teorija koja ima beskonačan model $\mathfrak{M}$, te neka je λ neki beskonačan kardinalni broj. Tada postoji model $\mathfrak{N}$ za T kardinalnosti λ koji je elementarno ekvivalentan s modelom $\mathfrak{M}$, tj. vrijedi $\mathfrak{M} \equiv \mathfrak{N}$.*

Dokaz. Označimo sa $Th(\mathfrak{M})$ skup svih zatvorenih formula istinitih na modelu $\mathfrak{M}$. (To nije dijagram struktrure $\mathfrak{M}$, jer se ne promatraju i zatvorene formule jezika $\sigma_{\mathfrak{M}}$). Pošto je $\mathfrak{M}$ beskonačan model za $Th(\mathfrak{M})$, tada iz Löwenheim–Skolemovog teorema "na gore" slijedi da postoji model $\mathfrak{N}$ za $Th(\mathfrak{M})$ kardinaliteta λ. Dakle, vrijedi $\mathfrak{N} \models Th(\mathfrak{M})$, tj. $Th(\mathfrak{M}) \subseteq Th(\mathfrak{N})$.

Za dokaz obratne inkluzije uzmimo proizvoljnu zatvorenu formulu F za koju vrijedi $\mathfrak{N} \models F$. Pretpostavimo $\mathfrak{M} \not\models F$. Tada vrijedi $\mathfrak{M} \models \neg F$. No, pošto je $Th(\mathfrak{M}) \subseteq Th(\mathfrak{N})$, tada vrijedi $\mathfrak{N} \models \neg F$. To je kontradikcija s pretpostavkom $\mathfrak{N} \models F$. □

Za teoriju T kažemo da je **potpuna** ako za svaku zatvorenu formulu F vrijedi: $T \models F$ ili $T \models \neg F$.

Lema 1.62. *Neka je T neka teorija. Sljedeće tvrdnje su ekvivalentne:*

a) teorija T je potpuna

b) svi modeli od T su elementarno ekvivalentni

Primjer 1.63. *a) Teorija grupa nije potpuna pošto svi njeni modeli nisu elementarno ekvivalentni (npr. komutativne i nekomutativne grupe)*

b) Teorija polja karakteristike nula nije potpuna.
Npr. polja $\mathbb{C}$ i $\mathbb{R}$ nisu elementarno ekvivalentna, jer je jedno algebarsko zatvoreno, a drugo nije.

c) Teorija ACF_0 algebarski zatvorenih polja karakteristike nula je potpuna. (Dokazat ćemo kasnije)

d) Teorija ACF (alegebarski zatvorena polja proizvoljne karakteristike) nije potpuna, jer svi njeni modeli nisu elementarno ekvivalentni. Npr. polje $\mathbb{C}$ nije elementarno ekvivalentno s algebarskim zatvorenjem niti jednog konačnog polja (svako konačno polje je karakteristike različite od nula, pa je i njegovo algebarsko zatvorenje karakteristike različite od nule).

Teorem 1.64. *(Łoś–Vaughtov test potpunosti)*
Neka je T teorija koja je λ–kategorična, za neki beskonačan kardinalni broj λ, te neka je svaki model od T beskonačan. Tada je T potpuna teorija.

Dokaz. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ proizvoljni modeli od T. Iz pretpostavke teorema slijedi da su to beskonačni modeli. Iz leme 1.61. slijedi da postoje modeli $\mathfrak{M}'$ i $\mathfrak{N}'$ kardinalnosti λ tako da vrijedi: $\mathfrak{M} \equiv \mathfrak{M}'$ i $\mathfrak{N} \equiv \mathfrak{N}'$. Pošto je po pretpostavci teorema teorija T λ–kategorična tada su modeli $\mathfrak{M}'$ i $\mathfrak{N}'$ izomorfni. Tada znamo da su ti modeli elementarno ekvivalentni, tj. vrijedi $\mathfrak{M}' \equiv \mathfrak{N}'$. Sada je lako vidjeti da vrijedi $\mathfrak{M} \equiv \mathfrak{N}$. Time smo dokazali da su svaka dva modela od T elementarno ekvivalentna. Iz leme 1.62. slijedi da je T potpuna teorija. □

Primjenom Łoś–Vaughtovog testa slijedi da je teorija gustih linearnih uređaja bez krajnjih točaka potpuna. No, spomenimo i ograničenost primjene Łoś–Vaughtovog testa. Postoje potpune teorije koje imaju samo beskonačne modele, ali nisu λ–kategorične niti za jedan beskonačni kardinalni broj λ. Zapravo, ograničenost primjene testa najbolje ocrtava sljedeći teorem:

Morleyev teorem. *Neka je T potpuna teorija koja je λ–kategorična za neki beskonačni neprebrojivi kardinalni broj λ, te nema konačnih modela. Tada je T μ–kategorična za svaki neprebrojivi kardinalni broj.*

Kao jednu primjenu Los–Vaughtovog testa dokazat ćemo da je teorija ACF_p potpuna (za p=0 ili p prost broj), a onda iz toga dobiti jednu verziju tzv. Lefschetzovog principa ("ono što je istinito za polje $\mathbb{C}$ istinito je i za svako algebarsko zatvoreno polje").

Nakon toga ćemo kao malu ilustraciju primjene dokazati sljedeći Axov teorem:

Svaka polinomijalna injekcija $f : \mathbb{C}^n \to \mathbb{C}^n$ je i surjekcija.

(Kažemo da je funkcija f polinomijalna ako je svaka njena koordinatna funkcija polinom).

Signatura teorije polja uz simbol za jednakost sadrži i dva binarna funkcijska simbola koja obično označavamo sa $+$ i $\cdot$, te dva konstantska simbola koja označavamo sa 0 i 1. Teorija algebarski zatvorenih polja ACF je skup sljedećih rečenica:

a) aksiomi polja

b) $\forall a_0 \forall a_1 \ldots \forall a_{n-1}(\forall a_n \neq 0)(\exists x)(a_n x^n + \ldots + a_1 x + a_0 = 0)$, za svaki $n \in \mathbb{N}$, $n > 0$.

Lema 1.65. *Svako algebarski zatvoreno polje je beskonačno.*

Dokaz. Neka je K algebarski zatvoreno polje (proizvoljne karakteristike). Dokazujemo da za svaki $n \in \mathbb{N}$ vrijedi $kard(K) > n$. Neka su $a_1, \ldots, a_n$ proizvoljni različiti elementi polja K, gdje je $n \geq 1$. Neka je polinom $f \in K[X]$ definiran sa $f(x) = (x - a_1) \ldots (x - a_n) + 1$. Pošto je po pretpostavci polje K algebarski zatvoreno, te je stupanj polinoma f barem 1, tada postoji $\alpha \in K$ tako da vrijedi $f(\alpha) = 0$. Očito je $\alpha \neq a_i$, za svaki $i \in \{1, \ldots, n\}$. □

Za svaki prosti broj p označimo $F_p \equiv \underbrace{1 + \ldots + 1}_{p\text{–puta}} = 0$. Za prosti broj p označimo sa ACF_p teoriju

$$ACF \ \cup \ \{\neg F_k : k \ \text{ je prosti broj}, \ \ k < p\} \ \cup \ \{F_p\}$$

Sa ACF_0 označavamo teoriju $ACF \cup \{\neg F_p : p \text{ je prosti broj }\}$.

Lema 1.66. *(Steinizov teorem)*
Svaka teorija ACF_p je λ–kategorična za svaki neprebrojivi kardinalni broj λ.

Skica dokaza. Za $X \subseteq K$ kažemo da je algebarski nezavisan ako za svaki polinom $q \in \mathbb{Z}[X_1, \ldots, X_n]$ i sve međusobno različite elemente $a_1, \ldots, a_n \in X$ za koje vrijedi $q(a_1, \ldots, a_n) = 0$ imamo $q \equiv 0$ nad poljem K.
Transcendentna baza nekog polja je svaki maksimalan algebarski nezavisan podskup. Stupanj transcendentnosti polja je kardinalitet proizvoljne transcendentne baze. Ključna činjenica za dokaz je sljedeće:

> *Dva algebarski zatvorena polja su izomorfna ako i samo ako su iste karakteristike, te imaju isti stupanj transcendentnosti.*

(Detalje o ovom dokazu možete pronaći u S. Lang, Algebra, Addison–Wesley, Reading, MA, 1971.)

Korolar 1.67. *Za svaki prosti broj p i $p = 0$ teorija ACF_p je potpuna.*

Dokaz. Primjenom lema 1.65. i 1.66., te Łos–Vaughtovog testa potpunosti.

Znamo da su svaka dva modela potpune teorije elementarno ekvivalentna. Posebno time imamo da za svako algebarski zatvoreno polje K karakteristike nula vrijedi $\mathbb{C} \equiv K$. No, vrijedi i više. To ističemo u sljedećoj propoziciji koja je verzija Lefschetzovog principa.

Propozicija 1.68. *Neka je F proizvoljna rečenica teorije polja. Sljedeće tvrdnje su ekvivalentne:*

a) $\mathbb{C} \models F$

b) za svako algebarsko zatvoreno polje K karakteristike nula vrijedi $K \models F$

c) postoji algebarski zatvoreno polje K karakteristike nula tako da $K \models F$

d) za svaki $m \in \mathbb{N}$ postoji prosti broj $p > m$ i postoji algebarski zatvoreno polje karakteristike p tako da $K \models F$

e) postoji $m \in \mathbb{N}$ takav da za svaki prosti broj $p > m$ i svako algebarski zatvoreno polje K karakteristike p vrijedi $K \models F$

Dokaz. Zbog potpunosti teorije ACF_0 vrijedi $(a) \Leftrightarrow (b) \Leftrightarrow (c)$. Zatim, očito vrijedi $(e) \Rightarrow (d)$.

Dokažimo $(b) \Rightarrow (e)$. Pretpostavimo da vrijedi $ACF_0 \models F$. Tada iz **teorema kompaktnosti** slijedi da postoje prosti brojevi $p_1, \ldots, p_n$ tako da vrijedi:

$$ACF \bigcup \{\neg F_{p_1}, \ldots, \neg F_{p_n}\} \models F \qquad (*)$$

Neka je $m \in \mathbb{N}$ najmanji prirodan broj takav da je $m > \max\{p_1, \ldots, p_n\}$. Tada za svaki prosti broj $p > m$ i svako algebarsko zatvoreno polje K karakteristike p očito vrijedi

$$K \models \neg F_{p_1} \wedge \ldots \wedge \neg F_{p_n}$$

Iz ovog posljednjeg i $(*)$ slijedi $K \models F$.

Preostalo je još dokazati implikaciju $(d) \Rightarrow (b)$. Pretpostavimo $ACF_0 \not\models F$. Tada iz potpunosti teorije ACF_0 slijedi $ACF_0 \models \neg F$. Ovo posljednje je ekvivalentno sa

$$ACF \bigcup \{\neg F_p : p \text{ prosti broj}\} \models \neg F.$$

Iz **teorema kompaktnosti** slijedi da postoje prosti brojevi $p_1, \ldots, p_n$ tako da vrijedi

$$ACF \bigcup \{\neg F_{p_1}, \ldots, \neg F_{p_n}\} \models \neg F.$$

Neka je p najmanji prosti broj takav da $p \geq \max\{p_1, \ldots, p_n\}$. Iz prethodno dokazane činjenice posebno slijedi

$$ACF \bigcup \{\neg F_{p_1}, \ldots, \neg F_{p_n}\} \bigcup \{F_p\} \models \neg F$$

Time imamo $ACF_p \models \neg F$, a onda i $ACF_p \not\models F$. □

Za funkciju $f : \mathbb{C}^n \to \mathbb{C}^n$ kažemo da je **polinomijalna** ako je svaka koordinatna funkcija polinom.

Teorem 1.69. *(Axov teorem)*
Za svaki $n \in \mathbb{N} \setminus \{0\}$ svaka polinomijalna injekcija $f : \mathbb{C}^n \to \mathbb{C}^n$ je i surjekcija.

Dokaz. Dokazujemo da tvrdnja vrijedi za svaku polinomijalnu injektivnu funkciju na proizvoljnom algebarski zatvorenom polju proizvoljno velike karakteristike p. Za sve $n, d \in \mathbb{N}$ označimo sa $\Phi_{n,d}$ rečenicu koja ima svojstvo da za svako polje K vrijedi slijedeće:

$K \models \Phi_{n,d}$ ako i samo ako svaka polinomijalna injekcija $g : K^n \to K^n$, čija je svaka koordinatna funkcija polinom najviše stupnja d, je surjekcija.

Npr. $\Phi_{2,2}$ je sljedeća rečenica

$$(\forall a_{0,0})\ (\forall a_{0,1})\quad (\forall a_{0,2})\ (\forall a_{1,0})\ (\forall a_{1,1})\ (\forall a_{2,0})\ (\forall b_{0,0})\ \ldots (\forall b_{2,0})$$

$$\Big(\forall x_1 \forall x_2 \forall y_1 \forall y_2 \quad \Big(\sum_{i,j=0,\ i+j\leq 2}^{2} a_{ij}\ x_1^i y_1^j = \sum_{i,j=0,\ i+j\leq 2}^{2} a_{ij}\ x_2^i y_2^j \ \wedge$$

$$\wedge \sum_{i,j=0,\ i+j\leq 2}^{2} b_{ij}\ x_1^i y_1^j = \sum_{i,j=0,\ i+j\leq 2}^{2} b_{ij}\ x_2^i y_2^j \Big) \ \rightarrow$$

$$\rightarrow (x_1 = x_2 \ \wedge \ y_1 = y_2) \Big) \ \rightarrow$$

$$\rightarrow \ \forall u \forall v \exists x \exists y \quad \Big(\sum_{i,j=0,\ i+j\leq 2}^{2} a_{ij}\ x_1^i y_1^j = u \ \wedge \sum_{i,j=0,\ i+j\leq 2}^{2} b_{ij}\ x_1^i y_1^j = v \Big) \Big)$$

Primijetite da je tu važno da promatramo polinome. Kvantifikacija po polinomima zapravo znači kvantifikaciju po koeficijentima polinoma. Naravno, ne

smatramo da su a_{ij} i b_{ij} elementi polja, a ni neki posebni simboli alfabeta. Mogli smo u formuli $\Phi_{2,2}$ te koeficijente označiti "običnim" varijablama.

Neka je K konačno polje. Tada je za svaki $n \in \mathbb{N}$ skup K^n također konačan. Iz toga slijedi da je svaka injekcija $f : K^n \to K^n$ ujedno i surjekcija. Označimo s $\overline{K}$ algebarsko zatvorenje polja K. Znamo (vidi npr. Langovu knjigu) da vrijedi $\overline{K} = \cup K_i$, gdje je (K_i) rastući niz konačnih polja (koje dobivamo rekurzivnim dodavanjem nul–točaka polinoma).

Neka je $f : \overline{K}^n \to \overline{K}^n$ proizvoljna polinomijalna injekcija. Neka je $d \in \mathbb{N}$ koji je jednak najvećem stupnju koordinatnog polinoma od f. Neka je $\vec{y} = (y_1, \ldots, y_n) \in \overline{K}^n$ proizvoljan. Tada postoje $i_1, \ldots, i_n \in \mathbb{N}$ takvi da je $y_j \in K_{i_j}$. Pošto je (K_i) rastući niz polja tada postoji $j_0 \in \{i_1, \ldots, i_n\}$ tako da vrijedi $y_1, \ldots, y_n \in K_{j_0}$. Pošto je $f|_{K_{j_0}^n}$ injekcija, te je $K_{j_0}^n$ konačan skup, tada je ta funkcija i surjekcija. To znači da za zadani $\vec{y}$ postoji $\vec{x} \in K_{j_0}^n$ tako da vrijedi $f(\vec{x}) = \vec{y}$.

Time smo dokazali da za sve $n, d \in \mathbb{N}$ postoji algebarski zatvoreno polje $\overline{K}$ tako da vrijedi $\overline{K} \models \Phi_{n,d}$. Zapravo, dokazali smo da za svaki $m \in \mathbb{N}$ postoji prosti broj $p > m$ i algebarski zatvoreno polje $\overline{K}$ karakteristike p tako da vrijedi $\overline{K} \models \Phi_{n,d}$. Iz prethodne propozicije slijedi $\mathbb{C} \models \Phi_{n,d}$. □

Napomena 1.70. *J. Ax je dokazao prethodno navedeni teorem u članku:*

> *J. Ax, The elementary theory of finite fields, Annals of Mathematics, 88 (1968), 239–271*

Isti rezultat za $\mathbb{R}^n$ je dokazan u članku

> *A. Bialynicki–Birula, M. Rosenlicht, Injective morphisms of real algebraic varieties, Proceedings of the American Mathematical Society, 102 (1988), 804–808*

1.9 Robinsonov teorem konzistentnosti

Ponovimo prvu definiciju teorije prvo reda. Neka je σ neka signatura. Svaki skup σ–zatvorenih formula nazivamo σ–**teorija**, ili samo kratko **teorija**. Za teoriju T kažemo da je **konzistentna** ako za nju postoji model.

Teorem 1.71. *(Robinsonov teorem konzistentnosti)*
Neka je T potpuna σ–teorija, te neka su σ_1 i σ_2 signature takve da vrijedi $\sigma = \sigma_1 \cap \sigma_2$. Neka je T_1 konzistentna σ_1–teorija i T_2 konzistentna σ_2–teorija, tako da vrijedi $T \subseteq T_1 \cap T_2$. Tada je teorija $T_1 \cup T_2$ konzistentna.

Prvo dokazujemo tri leme koje ćemo na kraju iskoristiti za dokaz Robinsonovog teorema. Neka su σ i σ' signature takve da vrijedi $\sigma \subseteq \sigma'$. Ako je $\mathfrak{A}$ neka σ'–struktura tada ćemo sa $\mathfrak{A}^-$ označiti σ–redukciju strukture $\mathfrak{A}$.

Lema 1.72. *Neka su σ i σ_2 signature takve da $\sigma \subseteq \sigma_2$. Zatim, neka je T neka potpuna σ–teorija, a T_2 neka konzistentna σ_2–teorija tako da vrijedi $T \subseteq T_2$. Ako je $\mathfrak{M}$ model za teoriju T tada postoji model $\mathfrak{B}$ za teoriju T_2 tako da vrijedi $\mathfrak{M} \prec \mathfrak{B}^-$.*
(Kraće: ako $\mathfrak{M} \models T$ tada postoji $\mathfrak{B} \models T_2$ takav da $\mathfrak{M} \prec \mathfrak{B}^-$)

Dokaz. Lemu ćemo dokazati primjenom metode dijagrama. Iz leme o dijagramu slijedi da je dovoljno dokazati da je teorija $T_2 \cup \mathcal{D}(\mathfrak{M})$ konzistentna. Pretpostavimo suprotno. Iz **teorema kompaktnosti** slijedi da postoji konačan podskup $S \subseteq T_2 \cup \mathcal{D}(\mathfrak{M})$ za koji ne postoji model. Pošto je svaki potpuni dijagram zatvoren na konjunkciju tada postoji formula $F(\overline{a_1}, \ldots, \overline{a_n}) \in \mathcal{D}(\mathfrak{M})$ koja je ekvivalentna konačnom skupu formula $S \cap \mathcal{D}(\mathfrak{M})$. Pošto za skup formula S ne postoji model, tada posebno vrijedi $T_2 \models \neg F(\overline{a_1}, \ldots, \overline{a_n})$, a onda i

$$T_2 \models \forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n) \qquad (*)$$

Formula $\forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n)$ je σ–formula. To znači da možemo razmatrati da li ta formula logički slijedi iz teorije T. Pretpostavimo li da iz teorije T logički slijedi formula $\neg\forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n)$, tada zbog $\sigma \subseteq \sigma_2$ i $T \subseteq T_2$, imamo $T_2 \models \neg\forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n)$.
Iz ovog posljednjeg i $(*)$ dobivamo kontradikciju s pretpostavkom da je T_2 konzistentna teorija. Dakle, $T \not\models \neg\forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n)$. Pošto je po pretpostavci leme teorija T potpuna, tada vrijedi $T \models \forall v_1 \ldots \forall v_n \neg F(v_1, \ldots, v_n)$. Time je dobivena kontradikcija, jer je $\mathfrak{M}$ model za teoriju T, te posebno iz pretpostavke $F(\overline{a_1}, \ldots, \overline{a_n}) \in \mathcal{D}(\mathfrak{M})$ slijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$. □

Lema 1.73. *Neka su σ i σ_1 signature takve da $\sigma \subseteq \sigma_1$. Zatim, neka je T neka potpuna σ–teorija, a T_1 neka konzistentna σ_1–teorija tako da vrijedi $T \subseteq T_1$. Neka $\mathfrak{M} \models T$ i $\mathfrak{A}_1 \models T_1$ tako da vrijedi $\mathfrak{A}_1^- \prec \mathfrak{M}$. Tada postoji $\mathfrak{A}_2$ model za T_1 tako da vrijedi*

$$\mathfrak{A}_1 \prec \mathfrak{A}_2 \quad i \quad \mathfrak{M} \prec \mathfrak{A}_2^-$$

Dokaz. Kao u i dokazu leme 1.72. znamo da je primjenom metode dijagrama dovoljno dokazati da je teorija $T' := \mathcal{D}(\mathfrak{M}) \cup \mathcal{D}(\mathfrak{A}_1)$ konzistentna. Pretpostavimo da teorija T' nije konzistentna. Primjenom **teorema kompaktnosti**, te činjenice da je svaki potpuni dijagram zatvoren za konjunkciju, slijedi da postoji σ–formula F, te $a_1, \ldots, a_n \in |\mathfrak{A}_1|$ i $a_{n+1}, \ldots, a_{n+p} \in |\mathfrak{M}| \setminus |\mathfrak{A}_1|$ tako da vrijedi:

$$F(\overline{a_1}, \ldots, \overline{a_n}, \overline{a_{n+1}}, \ldots, \overline{a_{n+p}}) \in \mathcal{D}(\mathfrak{M}) \qquad \text{i}$$

$$\mathcal{D}(\mathfrak{A}_1) \models \neg F(\overline{a_1}, \ldots, \overline{a_n}, \overline{a_{n+1}}, \ldots, \overline{a_{n+p}})$$

Tada vrijedi $\mathcal{D}(\mathfrak{A}_1) \models \forall v_1 \ldots \forall v_p \neg F(\overline{a_1}, \ldots, \overline{a_n}, v_1, \ldots, v_p)$, a onda i

$$\mathfrak{A}_1 \models \forall v_1 \ldots \forall v_p \neg F[a_1, \ldots, a_n]$$

Očito $\mathfrak{M} \models \exists v_1 \ldots \exists v_p F[a_1, \ldots, a_n]$. Time je dobivena kontradikcija s pretpostavkom $\mathfrak{A}_1^- \prec \mathfrak{M}$. □

Zamjenom teorije T_1 s teorijom T_2 u iskazu prošle leme dobivamo sljedeću lemu.

Lema 1.74. *Neka su σ i σ_2 signature takve da $\sigma \subseteq \sigma_2$. Zatim, neka je T neka potpuna σ–teorija, a T_2 neka konzistentna σ_2–teorija tako da vrijedi $T \subseteq T_2$. Neka $\mathfrak{M} \models T$ i $\mathfrak{B} \models T_2$ tako da vrijedi $\mathfrak{B}_1^- \prec \mathfrak{M}$. Tada postoji $\mathfrak{B}_2$ model za T_2 tako da vrijedi*

$$\mathfrak{B}_1 \prec \mathfrak{B}_2 \quad i \quad \mathfrak{M} \prec \mathfrak{B}_2^-$$

Dokažimo sada Robinsonov teorem. Neka je $\mathfrak{A}_1$ proizvoljan model teorije T_1 (po pretpostavci ta teorija je konzistentna). Pošto je po pretpostavci teorema $T \subseteq T_2$ tada očito vrijedi $\mathfrak{A}_1^- \models T$. Primjenom leme 1.72. slijedi da postoji model $\mathfrak{B}_1$ teorije T_2 tako da vrijedi $\mathfrak{A}_1^- \prec \mathfrak{B}_1^-$ (uzmemo $\mathfrak{M} := \mathfrak{A}_1^-$). Pošto $\mathfrak{B}_1 \models T_2$ i $T \subseteq T_2$ tada $\mathfrak{B}_1^- \models T$. Sada primjenom leme 1.73. (uzimajući $\mathfrak{M} := \mathfrak{B}_1^-$) slijedi da postoji model $\mathfrak{A}_2$ teorije T_1 tako da vrijedi:

$$\mathfrak{A}_1 \prec \mathfrak{A}_2 \qquad \text{i} \qquad \mathfrak{B}_1^- \prec \mathfrak{A}_2^-$$

Pošto je po pretpostavci teorema $T \subseteq T_2$ tada očito vrijedi $\mathfrak{A}_2^- \models T$. Sada primjenom leme 1.74. (uzimajući $\mathfrak{M} := \mathfrak{A}_2^-$) slijedi da postoji model $\mathfrak{B}_2$ teorije T_2 tako da vrijedi: $\mathfrak{B}_1 \prec \mathfrak{B}_2$ i $\mathfrak{A}_2^- \prec \mathfrak{B}_2^-$. Uzastopnom naizmjeničnom primjenom lema 1.73. i 1.74. dobili bi niz $(\mathfrak{A}_n)$ modela teorije T_1 i niz $(\mathfrak{B}_n)$ modela teorije T_2 tako da za svaki $n \in \mathbb{N}$ vrijedi:

$$\mathfrak{A}_n \prec \mathfrak{A}_{n+1}, \qquad \mathfrak{B}_n \prec \mathfrak{B}_{n+1}, \qquad \mathfrak{A}_n^- \prec \mathfrak{B}_n^- \qquad \text{i} \qquad \mathfrak{B}_n^- \prec \mathfrak{A}_{n+1}^-$$

Označimo $\mathfrak{A} = \bigcup_{n\in\mathbb{N}} \mathfrak{A}_n$ i $\mathfrak{B} = \bigcup_{n\in\mathbb{N}} \mathfrak{B}_n$. Iz teorema o uniji lanca elementarnih struktura, tj. teorema 1.20., slijedi posebno $\mathfrak{A}_1 \prec \mathfrak{A}$ i $\mathfrak{B}_1 \prec \mathfrak{B}$. Pošto je $\mathfrak{A}_1$ model teorije T_1 tada je i $\mathfrak{A}$ model teorije T_1. Iz analognog razloga $\mathfrak{B}$ je model teorije T_2. Očito je

$$\mathfrak{A}^- = \bigcup_{n\in\mathbb{N}} \mathfrak{A}_n^- = \bigcup_{n\in\mathbb{N}} \mathfrak{B}_n^- = \mathfrak{B}^-$$

Iz toga slijedi da je dobro definirana $(\sigma_1 \cup \sigma_2)$–struktura $\mathfrak{A} \cup \mathfrak{B}$ koja je očito model teorije $T_1 \cup T_2$. Time smo dokazali da je teorija $T_1 \cup T_2$ konzistentna. □

Napomena 1.75. *U knjizi [5] Robinsonov teorem konzistentnosti iskazan je u sljedećem obliku:*

> *Neka su T_1 i T_2 proizvoljne konzistentne teorije. Teorija $T_1 \cup T_2$ je konzistentna ako i samo ako ne postoji rečenica F tako da vrijedi $F \in T_1$ i $\neg F \in T_2$.*

U knjizi [5] prvo je dokazana Craigova lema, a onda je Robinsonov teorem dokazan njenom primjenom.

Jednostavna posljedica Robinsonovog teorema konzistentnosti je Craigova interpolacijska lema.

Lema 1.76. *(Craigova interpolacijska lema)*
Neka su F i G zatvorene formule za koje vrijedi $F \Rightarrow G$. Tada postoji zatvorena formula H tako da vrijedi:

1. *$F \Rightarrow H$*
2. *$H \Rightarrow G$*
3. *svaki nelogički simbol (osim simbola za jednakost) koji nastupa u formuli H nastupa u formulama F i G*

Formulu H nazivamo **interpolant** *formula F i G.*

Dokaz. Pretpostavimo da formula s navedenim svojstvima ne postoji. Osnovna ideja dokaza sastoji se od konstrukcije potpune teorije T za koju su teorije $T \cup \{F\}$ i $T \cup \{\neg G\}$ konzistentne. Tada iz Robinsonovog teorema slijedi da je teorija $T \cup \{F, \neg G\}$ konzistentna, što je nemoguće zbog pretpostavke da vrijedi $F \Rightarrow G$.

Označimo sa σ_F, odnosno sa σ_G, skup svih nelogičkih simbola koji nastupaju u fomuli F, odnosno u formuli G.

Neka je $\sigma = (\sigma_F \cap \sigma_G) \cup \{=\}$. Skup svih σ–rečenica je prebrojiv. Neka je $\{A_n : n \in \mathbb{N}\}$ skup koji sadrži sve σ–rečenice, pri čemu je $A_0 \equiv \exists v_0(v_0 = v_0)$. Konstruirat ćemo niz σ–rečenica $\{B_n : n \in \mathbb{N}\}$ koji ima sljedeća svojstva:

(i) formula $B_{n+1} \to B_n$ je valjana za svaki $n \in \mathbb{N}$

(ii) za svaki $n \in \mathbb{N}$ barem jedna od formula $B_n \to A_n$ i $B_n \to \neg A_n$ je valjana

(iii) niti za jedan $n \in \mathbb{N}$ ne postoji interpolant za formule $F \wedge B_n$ i $G \wedge B_n$

Neka je $B_0 := A_0$. Lako je provjeriti da B_0 ispunjava sva tri tražena uvjeta. Neka je za neki $n \in \mathbb{N}$ već definirana formula B_n. Prije definicije formule B_{n+1} ističemo sljedeću pomoćnu tvrdnju:

Moguća su samo sljedeća dva slučaja:

1. Ne postoji interpolant za formule $F \wedge B_n \wedge A_{n+1}$ i $G \wedge B_n \wedge A_{n+1}$
2. Ne postoji interpolant za formule $F \wedge B_n \wedge \neg A_{n+1}$ i $G \wedge B_n \wedge \neg A_{n+1}$

(Pretpostavimo suprotno, tj. da postoje σ–rečenice H_1 i H_2 tako da su sljedeće formule valjane:

$$(F \wedge B_n \wedge A_{n+1}) \to H_1, \qquad H_1 \to (G \wedge B_n \wedge A_{n+1}),$$

$$(F \wedge B_n \wedge \neg A_{n+1}) \to H_2, \qquad H_2 \to (G \wedge B_n \wedge \neg A_{n+1})$$

Tada su također valjane i sljedeće formule:

$$\Big((F \wedge B_n \wedge A_{n+1}) \ \vee \ (F \wedge B_n \wedge \neg A_{n+1})\Big) \to (H_1 \vee H_2) \qquad \text{i}$$

$$(H_1 \vee H_2) \to \Big((G \wedge B_n \wedge A_{n+1}) \ \vee \ (G \wedge B_n \wedge \neg A_{n+1})\Big)$$

Iz valjanosti posljednjih formula lako slijedi valjanost formula $(F \wedge B_n) \to (H_1 \vee H_2)$ i $(H_1 \vee H_2) \to (G \wedge B_n)$. No, to je zbog pretpostavke indukcije nemoguće (formula B_n mora ispunjavati svojstvo (iii).)

Sada definiramo traženu formulu B_{n+1} na sljedeći način:

- Ako ne postoji interpolant za formule $F \wedge B_n \wedge A_{n+1}$ i $G \wedge B_n \wedge A_{n+1}$ tada definiramo $B_{n+1} \equiv B_n \wedge A_{n+1}$
- Ako ne postoji interpolant za formule $F \wedge B_n \wedge \neg A_{n+1}$ i $G \wedge B_n \wedge \neg A_{n+1}$ tada definiramo $B_{n+1} \equiv B_n \wedge \neg A_{n+1}$

Lako je provjeriti da formula B_{n+1} zadovoljava sva tri tražena svojstva (i)–(iii).

Sada definiramo teoriju $T := \{B_n : n \in \mathbb{N}\}$. Redom dokazujemo da su teorije $T \cup \{F\}$ i $T \cup \{\neg G\}$ konzistentne, te da je teorija T potpuna.

U svrhu dokaza da je teorija $T \cup \{F\}$ konzistentna prvo dokazujemo da je za svaki $n \in \mathbb{N}$ formula $F \wedge B_n$ konzistentna. Lako je provjeriti da je formula F konzistentna (ako je F inkonzistentna tada je npr. formula $\neg\forall v_0(v_0 = v_0)$ jedan interpolant za formule F i G, što je u suprotnosti s početnom pretpostavkom da za te formule ne postoji interpolant). Pošto smo definirali $B_0 \equiv F \wedge \exists v_0(v_0 = v_0)$ tada je očito formula B_0 konzistentna. Neka je $n \in \mathbb{N}$ proizvoljan. Iz definicije niza (B_n) znamo da vrijedi:

$$B_{n+1} \equiv B_n \wedge A_{n+1} \qquad \text{ili} \qquad B_{n+1} \equiv B_n \wedge \neg A_{n+1}$$

Radi ilustracije razmatramo slučaj kada je $B_{n+1} \equiv B_n \wedge \neg A_{n+1}$. Tada znamo da za formule $A \equiv F \wedge B_n \wedge \neg A_{n+1}$ i $B \equiv G \wedge B_n \wedge \neg A_{n+1}$ ne postoji interpolant. Pretpostavimo da je formula $F \wedge B_{n+1}$ inkonzistentna. Pošto je $A \equiv F \wedge B_{n+1}$ tada formula A nije konzistentna. No, tada je npr. formula $\neg\forall v_0(v_0 = v_0)$ jedan interpolant za formule A i B što je suprotno pretpostavci.

Iz **teorema kompaktnosti** slijedi da je za dokaz konzistentnosti teorije $T \cup \{F\}$ dovoljno dokazati da je svaki njen konačan podskup konzistentan. Neka je $\{B_{i_1}, \ldots, B_{i_n}\}$ proizvoljan konačan podskup od T, pri čemu vrijedi $i_1 < \ldots < i_n$. Prije smo bili dokazali da je formula $F \wedge B_{i_n}$ konzistentna. Neka je $\mathfrak{M}$ neka σ_F–struktura koja je model za formulu $F \wedge B_{i_n}$. Iz uvjeta (i) iz definicije niza formula (B_k) znamo da je za sve $i < j$ formula $B_j \to B_i$ valjana. Iz toga slijedi da imamo $\mathfrak{M} \models B_{i_1} \wedge \ldots \wedge B_{i_n}$. Time smo dokazali da je svaki konačan podskup od $T \cup \{F\}$ konzistentan. Sasvim analogno bi dokazali da je teorija $T \cup \{\neg G\}$ konzistentna.

Dokažimo još da je teorija T potpuna. Neka je A proizvoljna zatvorena σ–formula. Tada postoji $n \in \mathbb{N}$ tako da vrijedi $A \equiv A_n$. Iz uvjeta (ii) iz definicije niza formula (B_n) slijedi da je barem jedna od formula $B_n \to A_n$ i $B_n \to \neg A_n$ valjana. Neka je $\mathfrak{M}$ proizvoljan model za teoriju T. Pošto je po

definiciji $T = \{B_k : k \in \mathbb{N}\}$ tada iz valjanosti formule $B_n \to A_n$ ili $B_n \to \neg A_n$ slijedi da vrijedi $\mathfrak{M} \models A_n$ ili $\mathfrak{M} \models \neg A_n$. Time smo dokazali da vrijedi $T \models A$ ili $T \models \neg A$, tj. da je teorija T potpuna. □

Korolar 1.77. *Neka je T_1 konzistentna σ_1–teorija, a T_2 konzistentna σ_2–teorija. Označimo $\sigma = \sigma_1 \cap \sigma_2$. Tada vrijedi:*

teorija $T_1 \cup T_2$ je konzistentna ako i samo ako ne postoji σ–rečenica F tako da vrijedi $T_1 \models F$ i $T_2 \models \neg F$.

Važnu primjenu Craigova lema (tj. Robinsonov teorem i metoda dijagrama) ima u teoriji definicija. To je Bethov teorem definabilnosti koji je zapravo obrat jednostavnog i klasičnog rezultata iz teorije definicija koji se naziva **Padoaova metoda**. Ta metoda se vrlo često primjenjuje kada se želi pokazati da određeni pojam ne može biti definiran pomoću nekih drugih danih pojmova.

Neka je T neka σ–teorija i P neki n–mjesni relacijski simbol takav da $P \notin \sigma$. Označimo $\sigma' = \sigma \cup \{P\}$. Neka je P_1 neki drugi n–mjesni relacijski simbol koji također ne pripada σ. Ako je G neka σ'–formula tada sa $G_{P_1/P}$ označavamo formulu dobivenu iz formule G zamjenom svakog relacijskog simbola P sa P_1.

Lema 1.78. *Ako je F neka σ–formula, a G neka σ'–formula, tada vrijedi:*

$$ako \quad F \Rightarrow G \quad tada \quad F \Rightarrow G_{P_1/P}$$

Definicija 1.79. *Neka je T neka $\sigma' = \sigma \cup \{P\}$–teorija ($P$ je n–mjesni relacijski simbol koji ne pripada σ). Kažemo da je relacijski simbol P* **implicitno definabilan u teoriji** *T ako za svaki n–mjesni relacijski simbol P_1 koji ne pripada signaturi σ vrijedi:*

$$T \cup T_1 \models \forall v_1 \ldots \forall v_n \Big(P(v_1, \ldots, v_n) \leftrightarrow P_1(v_1, \ldots, v_n) \Big)$$

gdje je T_1 teorija dobivena zamjenom svakog nastupa relacijskog simbola P sa P_1 u svakoj formuli iz T.

Propozicija 1.80. *Neka je T neka $\sigma' = \sigma \cup \{P\}$–teorija. Tada su sljedeće tvrdnje ekvivalentne:*

1. *relacijski simbol P je implicitno definabilan u teoriji T*
2. *Za svaku σ–strukturu $\mathfrak{M}$ postoji najviše jedna interpretacija relacijskog simbola P tako da je σ'–ekspanzija od $\mathfrak{M}$ model za T.*

Definicija 1.81. *Neka je T neka $\sigma \cup \{P\}$–teorija (P je n–mjesni relacijski simbol koji ne pripada σ). Kažemo da je relacijski simbol P* **eksplicitno definabilan u teoriji** *T ako postoji σ–formula $F(v_1, \ldots, v_n)$ tako da vrijedi:*

$$T \models \forall v_1 \ldots \forall v_n \Big(P(v_1, \ldots, v_n) \leftrightarrow F(v_1, \ldots, v_n) \Big)$$

Propozicija 1.82. *(Padoaova metoda)*
Neka je T neka $\sigma \cup \{P\}$–teorija (P je n–mjesni relacijski simbol koji ne pripada σ). Ako je relacijski simbol P eksplicitno definabilan u teoriji T tada je on i implicitno definabilan u teoriji T.

Primjer 1.83. *Neka je $\sigma = \{+, =\}$ ($+$ je dvomjesni relacijski simbol), i R neki dvomjesni relacijski simbol. Označimo sa T skup svih $\sigma \cup \{R\}$–rečenica F za koje vrijedi $(\mathbb{Z}, +, <) \models F$. Tvrdimo da relacijski simbol R nije eksplicitno definabilan u teoriji T. Uočimo da je $(\mathbb{Z}, +, >)$ također model za teoriju T jer vrijedi $(\mathbb{Z}, +, <) \simeq (\mathbb{Z}, + >)$ (izomorfizam je funkcija $x \mapsto -x$). To znači da ne postoji jedinstvena interpretacija relacijskog simbola R u σ–strukturi $(\mathbb{Z}, +)$ tako da je $\sigma \cup \{R\}$–ekspanzija od $(\mathbb{Z}, +)$ model za teoriju T. Iz propozicije 1.80. slijedi da relacijski simbol R nije implicitno definabilan u teoriji T, a iz propozicije 1.82. slijedi da tada nije ni eksplicitno definabilan u teoriji T.*

Teorem 1.84. *(Bethov teorem definabilnosti)*
Neka je T neka $\sigma \cup \{P\}$–teorija, gdje je P neki relacijski simbol koji ne pripada σ. Ako je relacijski simbol P implicitno definabilan u teoriji T tada je i eksplicitno definabilan.

Dokaz. Neka su $c_1, \ldots, c_n$ međusobno različiti konstantski simboli koji ne pripadaju σ. Neka je P_1 proizvoljan n–mjesni relacijski simbol koji ne pripada $\sigma \cup \{P\}$. Pošto je po pretpostavci relacijski simbol P implicitno definabilan u teoriji T tada vrijedi $T \cup T_1 \models \forall v_1 \ldots \forall v_n (P(v_1 \ldots, v_n) \leftrightarrow P_1(v_1, \ldots, v_n))$, pri čemu je T_1 teorija dobivena zamjenom svakog nastupa relacijskog simbola P sa P_1 u svakoj formuli iz T. Iz ovog posljednjeg lako slijedi da je inkonzistentna teorija $T \cup \{P(c_1, \ldots, c_n)\} \cup T_1 \cup \{\neg P_1(c_1, \ldots, c_n)\}$. Iz **teorema kompaktnosti** slijedi da postoje konačni podskupovi $S \subseteq T$ i $S' \subseteq T_1$ takvi da je inkonzistentna teorija $S \cup \{P(c_1, \ldots, c_n)\} \cup S' \cup \{\neg P_1(c_1, \ldots, c_n)\}$. Označimo $F \equiv \bigwedge_{A \in S} A$ i $G \equiv \bigwedge_{B \in S'} B$. Tada formula $F \wedge P(c_1, \ldots, c_n) \wedge G \wedge \neg P_1(c_1, \ldots, c_n)$ nije ispunjiva, pa je valjana formula $\neg \Big(F \wedge P(c_1, \ldots, c_n) \wedge G \wedge \neg P_1(c_1, \ldots, c_n) \Big)$, odnosno vrijedi $\Big(F \wedge P(c_1, \ldots, c_n) \Big) \Rightarrow \Big(G \rightarrow P_1(c_1, \ldots, c_n) \Big)$.

Iz Craigove interpolacijske leme slijedi da postoji $\sigma \cup \{c_1, \ldots, c_n\}$–rečenica H tako da vrijedi $\Big(F \wedge P(c_1, \ldots, c_n)\Big) \Rightarrow H$ i $H \Rightarrow \Big(G \rightarrow P_1(c_1, \ldots, c_n)\Big)$. Očito se relacijski simboli P i P_1 ne pojavljuju u formuli H. Pošto $S \subseteq T$ i $F \equiv \bigwedge_{A \in S} A$ tada očito vrijedi $T \models F$. Iz $T \models F$ i $\Big(F \wedge P(c_1, \ldots, c_n)\Big) \Rightarrow H$ slijedi $T \models P(c_1, \ldots, c_n) \rightarrow H$. Pošto $\{c_1, \ldots, c_n\} \cap \sigma = \emptyset$ tada iz posljednjeg slijedi

$$T \models \forall v_1 \ldots \forall v_n \Big(P(v_1, \ldots, v_n) \rightarrow H\Big) \qquad (*)$$

Pošto $T_1 \models G$ i $H \Rightarrow \Big(G \rightarrow P_1(c_1, \ldots, c_n)\Big)$ tada $T_1 \models H \rightarrow P_1(c_1, \ldots, c_n)$. Iz ovog posljednjeg zamjenom relacijskog simbola P_1 sa P, i primjenom leme 1.78., dobivamo $T \models H \rightarrow P(c_1, \ldots, c_n)$. Pošto $\{c_1, \ldots, c_n\} \cap \sigma = \emptyset$ tada dobivamo da vrijedi $T \models \forall v_1 \ldots \forall v_n \Big(H \rightarrow P(v_1, \ldots, v_n)\Big)$. Iz ovog posljednjeg i $(*)$ slijedi da je relacijski simbol P eksplicitno definabilan u teoriji T. $\square$

1.10 Ultrafiltri i ultraprodukti

U dokazu teorema kompaknosti koristili smo Henkinovu konstrukciju modela. Sada ćemo navesti još jednu metodu za konstrukciju modela. To su ultraprodukti. Kao jednu primjenu dat ćemo drugi dokaz teorema kompaktnosti za logiku prvog reda. No, prvo dajemo primjere koji ističu još jednu motivaciju za uvođenje ultraprodukata.

Primjer 1.85. Kartezijev produkt familije grupa je grupa.
Skicirajmo dokaz te tvrdnje. Neka je $\{(G_i, \circ_i) : i \in I\}$ *familija grupa. Označimo*

$$G = \prod_{i \in I} G_i = \{f \mid f : I \to \cup_{i \in I} G_i, \quad \text{za svaki } i \in I \quad \text{vrijedi } f(i) \in G_i\}$$

Zatim, neka je $\circ$ *binarna operacija na* G *definirana sa:*

$$(f \circ g)(i) = f(i) \circ_i g(i).$$

Lako je provjeriti da je za sve $f, g \in G$ *funkcija* $f \circ g$ *ponovno element od* G*, te da je* $(G, \circ)$ *grupa. To znači da je Kartezijev produkt proizvoljne familije grupa ponovno grupa.*

Primjer 1.86. Kartezijev produkt polja općenito nije polje.
Kako bi dokazali tu tvrdnju definirajmo prvo Kartezijev produkt polja. Neka je $I \neq \emptyset$*, te za svaki* $i \in I$ *neka je* $F_i = (A_i, +_i, \cdot_i, 0_i, 1_i)$ *polje. Označimo* $A = \prod_{i \in I} A_i$*. Redom definiramo:*

a) funkciju $0 : I \to \cup A_i$ *sa* $0(i) = 0_i$

b) funkciju $1 : I \to \cup A_i$ *sa* $1(i) = 1_i$

c) funkcije $+$ *i* $\cdot$ *sa:*

$$(f + g) : I \to \cup_{i \in I} A_i, \quad (f + g)(i) = f(i) +_i g(i)$$

$$(f \cdot g) : I \to \cup_{i \in I}, \quad (f \cdot g)(i) = f(i) \cdot_i g(i).$$

Uz tako definirane operacije Kartezijev produkt polja općenito nije polje. Npr. $\mathbb{R} \times \mathbb{R}$ *nije polje, jer uređeni parovi* $(0, 1)$ *i* $(1, 0)$ *različiti su od nule, ali* $(0, 1) \cdot (1, 0) = 0$.

Primjer 1.87. Kartezijev produkt linearno uređenih skupova općenito nije linearno uređen skup. *U svrhu dokaza te tvrdnje prvo uvodimo potrebne definicije. Neka je* $I \neq \emptyset$, *te za svaki* $i \in I$ *neka je* $\{(A_i, R_i), i \in I\}$ *neka familija linearno uređenih skupova (to znači da je svaka relacija* R_i *irefleksivna, tranzitivna i linearna). Označimo* $A = \prod_{i \in I} A_i$ *te definiramo relaciju* $R \subseteq A \times A$ *sa:*

$$f R g \qquad \text{ako i samo ako} \qquad \text{za svaki } \ i \in I \ \text{ vrijedi } \ f(i) R_i g(i).$$

Uz tako prirodno definiranu relaciju R *skup* (A, R) *općenito nije linearno uređen. (Npr. na* $\mathbb{R} \times \mathbb{R}$ *elementi* $(0,1)$ *i* $(1,0)$ *nisu usporedivi).*

Kako riješiti istaknute probleme? Ideja je jednostavna. Na Kartezijevom produktu $\prod_{i \in I} A_i$ definiramo posebnu relaciju ekvivalencije, te promatramo pripadni kvocijenti skup. U tu svrhu ćemo sada definirati pojmove filtra i ultrafiltra.

Definicija 1.88. *Neka je* $I \neq \emptyset$. *Za* $F \subseteq \mathcal{P}(I)$ *kažemo da je* **filtar** *nad skupom* I *ako vrijedi:*

(i) $I \in F$

(ii) ako su $X, Y \in F$ *tada* $X \cap Y \in F$
(zatvorenost na presjeke)

(iii) ako $X \in F$ *te* $X \subseteq Z \subseteq I$ *tada je* $Z \in F$
(zatvorenost za nadskupe)

Uočite da uvjet (i) u definiciji garantira nepraznost filtra. Ako bi na početku definicije zahtijevali $F \neq \emptyset$, tada uvjet (i) slijedi iz uvjeta (iii).

Primjer 1.89.

1. *Za svaki skup* I *je* $\{I\}$ *filtar. Nazivamo ga* **trivijalni** *filtar.*

2. *Za svaki skup* I *partitivni skup* $\mathcal{P}(I)$ *je filtar nad* I. *Nazivamo ga* **nepravi** *filtar.*

3. *Ako je* I *skup te* X *njegov proizvoljni podskup tada je skup* $F = \{Y \subseteq I \ : \ X \subseteq Y\}$ *filtar nad* I. *Nazivamo ga* **filtar generiran skupom** X. *Ako je* X *jednočlan skup tada* F *nazivamo* **glavni filtar.**

4. *Neka je* I *beskonačan skup. Tada je* $F = \{X : X \subseteq I, \ X^c \ \text{konačan}\}$ *filtar. Nazivamo ga* **Fréchetov filtar**.

5. *Neka je $(X, \mathcal{T})$ topološki prostor i $x \in X$. Tada je skup*

$$\{Y : Y \subseteq X \ \text{ takav da } \ (\exists U \in \mathcal{T})(x \in U \subseteq Y)\} \qquad \textit{filtar.}$$

Propozicija 1.90. *Neka je F filtar nad skupom I. Tada vrijedi:*

a) ako $X_1, \ldots, X_n \in F$ tada je $X_1 \cap \ldots \cap X_n \in F$;

b) ako $X, Y \in F$ tada je $X \cup Y \in F$;

c) ako je $\{X_j : j \in J\}$ familija skupova iz F tada je $\cup X_j \in F$.

Propozicija 1.91. *Neka je I neprazan skup, te $w \in I$. Tada je $\{X : X \subseteq I \ \text{ i } \ w \in X\}$ filtar nad I.*

Propozicija 1.92. *Svaki konačni filtar je glavni.*

Propozicija 1.93. *Neka je E proizvoljan podskup od $\mathcal{P}(I)$, i neka je*

$$F = \bigcap \{F' \ : \ F' \ \text{ je filtar nad } \ I, \ E \subseteq F'\}.$$

Tada vrijedi:

a) F je filtar nad I. Nazivamo ga **filtar generiran s podskupom** *E od $\mathcal{P}(I)$.*

b) $F = \{X \subseteq I \ : \ \text{ postoje } Y_1, \ldots, Y_n \in E \text{ tako da vrijedi } Y_1 \cap \ldots \cap Y_n \subseteq X\}$.

Propozicija 1.94. *Neka je E prebrojiv podskup od $\mathcal{P}(\mathbb{N})$. Tada je filtar generiran s E glavni filtar.*

Definicija 1.95. *Za filtar F nad skupom I kažemo da je* **pravi** *ako je:*

(iv) $F \neq \mathcal{P}(I)$.

Za pravi filtar nad skupom I kažemo da je **ultrafiltar** *ako za svaki $X \subseteq I$ vrijedi:*

(v) $X \in F$ ako i samo ako $I \backslash X \notin F$.

Napomena 1.96. *Za definiciju ultrafiltra uvjet (i) iz definicije filtra je suvišan, jer slijedi iz uvjeta (v) i (iii). Uvjeti iz definicije ultrafiltra biti će jasni kada se detaljno raspiše dokaz Łosovog teorema koji ćemo navesti kasnije.*

Svaki glavni filtar je ultrafiltar.

Propozicija 1.97. *Vrijedi:*

a) Filtar F je pravi ako i samo ako $\emptyset \notin F$.

b) Neka je $E \subseteq \mathcal{P}(I)$, te $F = \cap\{F' : F' \text{ je filtar nad } I \text{ takav da } E \subseteq F'\}$. Tada vrijedi: F je pravi filtar ako i samo ako E ima **svojstvo konačnih presjeka** *tj. za sve $X_1, \ldots, X_n \in E$ vrijedi $X_1 \cap \ldots X_n \neq \emptyset$.*

Propozicija 1.98. *Neka je I beskonačan skup. Za $X \subseteq I$ kažemo da je* **kofinitan** *ako je skup $I \setminus X$ konačan. Tada vrijedi:*

a) Skup svih kofinitnih podskupova od I ima svojstvo konačnih presjeka.

b) Postoje ultrafiltri nad I koji ne sadrže niti jedan konačan podskup od I.

c) Ultrafiltar U nad I nije glavni ako i samo ako U sadrži samo beskonačne skupove ako i samo ako U sadrži sve kofinitne podskupove od I.

d) Svaki ultrafiltar nad I ima beskonačno mnogo elemenata.

Propozicija 1.99. *Neka je F pravi filtar nad skupom I. Sljedeće tvrdnje su ekvivalentne:*

a) F je ultrafiltar.

b) F je maksimalan filtar, tj. ne postoji pravi filtar F' nad I takav da je F pravi podskup od F'.

c) za sve $X, Y \subseteq I$ vrijedi:

$$X \cup Y \in F \quad \text{ako i samo ako} \quad X \in F \quad \text{ili} \quad Y \in F.$$

Teorem 1.100. *Neka je I neprazan skup i $E \subseteq \mathcal{P}(I)$ koji ima svojstvo konačnih presjeka. Tada postoji ultrafiltar U nad I takav da je $E \subseteq U$.*

Dokaz. Označimo

$$F_0 = \bigcap\{F' \ : \ F' \ \text{ filtar nad } \ I \ \text{ i } \ E \subseteq F'\}$$

Iz propozicije 1.93. slijedi da je F_0 filtar, a iz propozicije 1.97. slijedi da je F_0 pravi filtar. Neka je $\mathcal{F} = \{F' : F' \text{ je pravi filtar nad } I \text{ i } E \subseteq F'\}$. Pošto je $F_0 \in \mathcal{F}$ tada je $\mathcal{F}$ neprazan skup. Skup $(\mathcal{F}, \subset)$ je parcijalno uređen skup. Neka je $\mathcal{L}$ proizvoljan lanac u $\mathcal{F}$. Označimo sa F_1 uniju svih filtera iz $\mathcal{L}$. Lako je provjeriti da je F_1 pravi filtar koji sadrži F. Time imamo da za svaki lancu $\mathcal{F}$ postoji gornja međa. Iz Zornove leme slijedi da postoji maksimalni element U u $\mathcal{F}$. Iz propozicije 1.99. slijedi da je U ultrafiltar. □

Teorem 1.101. (Teorem o ultrafiltru).
Svaki pravi filtar F nad I može biti proširen do ultrafiltra nad I.

Dokaz. Iz propozicije 1.97. znamo da svaki pravi filtar ima svojstvo konačnih presjeka. Iz prethodnog teorema slijedi tražena tvrdnja. □

Propozicija 1.102. *Neka je U ultrafiltar nad skupom I, te $X \in U$ proizvoljan. Tada je $U \cap \mathcal{P}(X)$ ultrafiltar.*

Propozicija 1.103. *Neka je U ultrafiltar nad skupom I, te neka je $I = A_1 \cup \ldots \cup A_n$. Tada postoji i takav da je $A_i \in U$. Ako su skupovi A_i u parovima disjunktni tada postoji točno jedan i takav da je $A_i \in U$.*

Dokaz. Ako $A_i \notin U$ tada je $A_i^c \in U$. Pošto je

$$\emptyset = I^c = (A_1 \cup \ldots \cup A_n)^c = A_1^c \cap \ldots \cap A_n^c$$

tada je nemoguće da za svaki i vrijedi $A_i \notin U$ (svaki ultrafiltar ima svojstvo konačnih presjeka). Ako su skupovi u A_i u parovima disjunktni tada je nemoguće $A_i, A_j \in U$, opet zbog svojstva konačnih presjeka svakog ultrafiltra. □

Propozicija 1.104. *Neka je U ultrafiltar nad skupom I, takav da postoji konačan skup $A = \{a_1, \ldots, a_n\}$ za kojeg vrijedi $A \in U$. Tada je U glavni ultrafiltar.*

Dokaz. Očito $I = A^c \cup \{a_1\} \cup \ldots \cup \{a_n\}$. Iz prethodne propozicije slijedi da postoji i takav da je $\{a_i\} \in U$. Tada je $U = \{X \subseteq I : a_i \in X\}$. □

Propozicija 1.105. *Neka je S skup podskupova nekog skupa I takav da za sve $X_1, \ldots, X_n \in S$ vrijedi da je $X_1 \cap \ldots \cap X_n$ beskonačan skup. Tada je skup S sadržan u nekom ultrafiltru nad I koji nije glavni.*

Dokaz. Označimo sa $\mathcal{F}$ Fréchetov filtar nad skupom I. Očito skup $S \cup \mathcal{F}$ ima svojstvo konačnih presjeka. Iz teorema o ultrafiltru slijedi da postoji ultrafiltar U tako da je $S \cup \mathcal{F} \subseteq U$. Iz propozicije 1.104. slijedi da ultrafiltar U nije glavni. □

Koristeći pojam ultrafiltara sada ćemo definirati pojam ultraprodukta. Prvo ćemo definirati pojam ultraprodukta familije skupova, a nakon toga pojam ultraprodukta familije proizvoljnih struktura iste signature.

Definicija 1.106. *Neka je* $\{M_i : i \in I\}$ *proizvoljna familija skupova, te* U *proizvoljan ultrafiltar nad* I*. Na Kartezijevom produktu familije skupova* $\{M_i : i \in I\}$*, tj. na skupu*

$$\prod_{i\in I} M_i = \{f \mid f : I \to \cup_{i\in I} M_i \ \text{ tako da je za svaki } \ i \in I \ \text{ ispunjeno } \ f(i) \in M_i\}$$

definiramo binarnu relaciju $\sim$ *ovako:*

$$f \sim g \ \text{ ako i samo ako } \ \{i \in I : f(i) = g(i)\} \in U$$

Lako je pokazati da je relacija $\sim$ *jedna relacija ekvivalencije. Za* $f \in \prod_{i\in I} M_i$ *sa* f_U *označavamo pripadnu klasu ekvivalencije. Skup svih klasa ekvivalencije nazivamo* **ultraprodukt familije skupova** $\{M_i : i \in I\}$*, te ga označavamo sa* $\prod_U M_i$*.*

Definicija 1.107. *Neka je* σ *proizvoljna signatura, te neka je* $\{\mathfrak{M}_i = (M_i, \varphi_i) : i \in I\}$ *neka familija* σ*–struktura. Neka je* U *proizvoljan ultrafiltar nad skupom* I*. Definiramo* σ*–strukturu* $\mathfrak{M} = (M, \varphi)$ *na sljedeći način:*

$$M = \prod_U M_i$$

za relacijski simbol $R^n \in \sigma$ *definiramo:*
$$((f_1)_U, \ldots, (f_n)_U) \in \varphi(R) \quad \text{ako i samo ako} \quad \{i : (f_1(i), \ldots, f_n(i)) \in \varphi_i(R)\} \in U$$

za funkcijski simbol $f^n \in \sigma$ *definiramo:*
$$\varphi(f^n)((f_1)_U, \ldots, (f_n)_U) = \Big(\ i \mapsto \varphi_i(f^n)(f_1(i), \ldots, f_n(i)) \ \Big)_U$$

za konstantski simbol $c \in \sigma$ *definiramo* $\varphi(c) = \Big(i \mapsto \varphi_i(c)\Big)_U$

Upravo definirana struktura se naziva **ultraprodukt familije struktura** $\{\mathfrak{M} : i \in I\}$ *i označavamo je sa* $\prod_U \mathfrak{M}_i$*.*

Ako su sve strukture $\mathfrak{M}_i$ *međusobno jednake, tj.* $\mathfrak{M}_i = \mathfrak{N}$*, za svaki* $i \in I$*, tada pripadni ultraprodukt nazivamo* **ultrapotencija** *strukture* $\mathfrak{N}$*.*

Propozicija 1.108. *Definicija ultraprodukta ne ovisi o izboru reprezentanata. Točnije, ako* $I \neq \emptyset$*,* $\{\mathfrak{M}_i = (M_i, \varphi_i) : i \in I\}$ *familija* σ*–struktura,* U *ultrafiltar nad* I*, te*

$$f_1, \ldots, f_n, \ g_1, \ldots, g_n \in \prod_{i\in I} M_i \ \text{ tako da vrijedi } \ f_1 \sim g_1, \quad \ldots \quad f_n \sim g_n,$$

tada vrijedi:

a) $\{i : (f_1(i), \ldots, f_n(i)) \in \varphi_i(R)\} \in U$ *ako i samo ako* $\{i : (g_1(i), \ldots, g_n(i)) \in \varphi_i(R)\} \in U$;

b) $\Big(i \mapsto \varphi_i(f_1(i), \ldots, f_n(i))\ \Big) \ \sim \ \Big(i \mapsto \varphi_i(g_1(i), \ldots, g_n(i))\ \Big)$

Napomena 1.109. *Neka je* $\{\mathfrak{M}_i : i \in I\}$ *neka familija* σ*–struktura. Ako je* F *filtar nad skupom tada je relacija* $\sim$ *na* $\prod_{i\in I} M_i$ *također relacija ekvivalencije. To znači da možemo promatrati kvocijentni skup* $\prod_{i\in I} M_i/\sim$ *. Interpretacije nelogičkih simbola definiramo isto kao i u definiciji ultraprodukta. Tako definiranu* σ*–strukturu nazivamo* **reducirani produkt**.

Neka je $I \neq \emptyset$, U neki ultrafiltar nad skupom I, $\{\mathfrak{M}_i : i \in I\}$ familija σ–struktura, $\{v_i : i \in I\}$ familija valuacija (v_i je valuacija na strukturi $\mathfrak{M}_i$). Kažemo da je valuacija v na ultraproduktu $\mathfrak{M} = \prod_U \mathfrak{M}_i$ **inducirana familijom valuacija** $\{v_i : i \in I\}$ ako za svaku individualnu varijablu x vrijedi $v(x) = (i \mapsto v_i(x))_U$.

Lema 1.110. *Neka je* $I \neq \emptyset$, U *neki ultrafiltar nad skupom* I, $\{\mathfrak{M}_i : i \in I\}$ *neka familija* σ*–struktura,* $\{v_i : i \in I\}$ *familija valuacija (*v_i *je valuacija na strukturi* $\mathfrak{M}_i$ *),* v *valuacija na ultraproduktu* $\mathfrak{M} = \prod_U \mathfrak{M}_i$ *koja je inducirana familijom valuacija* $\{v_i : i \in I\}$*. Tada za svaki* σ*–term* t *vrijedi*

$$v(t) = (i \mapsto v_i(t))_U.$$

Dokaz. Indukcijom po duljini terma t dokazujemo danu tvrdnju. Neka je term t jednak nekom konstantskom simbolu c. Tada imamo:

$$\begin{array}{rcl} v(c) & = & \text{(definicija proširenja valuacije na terme)} \ = \ c^{\mathfrak{M}} \\ & = & \text{(definicija interpretacije)} \ = \ (i \mapsto c^{\mathfrak{M}_i})_U \\ & = & (i \mapsto v_i(c))_U \end{array}$$

Ako je term t jednak individualnoj varijabli tada tražena jedankost slijedi iz definicije valuacije v.

Neka je $n \in \mathbb{N} \setminus \{0\}$ takav da za svaki term t' čija je duljina strogo manja od n vrijedi tražena tvrdnja. Neka je t proizvoljan term duljine n. Pošto je $n > 0$ tada je $t \equiv f(t_1, \ldots, t_k)$ za neki funkcijski simbol f i terme $t_1, \ldots, t_k$, čija je duljina strogo manja od n. Tada redom imamo:

$$\begin{aligned} v(t) &= v(f(t_1,\ldots,t_k)) = \\ &= \text{(definicija proširenja valuacije na terme)} \\ &= f^{\mathfrak{M}}(v(t_1),\ldots,v(t_k)) = \text{(pretpostavka indukcije)} \\ &= f^{\mathfrak{M}}((i\mapsto v_i(t_1))_U,\ldots,(i\mapsto v_i(t_k))_U) \\ &= \text{(definicija interpretacije na ultraproduktu)} \\ &= \Big(i\mapsto f^{\mathfrak{M}_i}(v_i(t_1),\ldots,v_i(t_k))\Big)_U \\ &= \text{(definicija proširenja valuacije)} \\ &= (i\mapsto v_i(f(t_1,\ldots,t_k)))_U = (i\mapsto v_i(t))_U \end{aligned}$$

□

Teorem 1.111. *Neka je $I\neq\emptyset$, U neki ultrafiltar nad skupom I, $\{\mathfrak{M}_i : i\in I\}$ familija σ–struktura, $\{v_i : i\in I\}$ familija valuacija (v_i je valuacija na strukturi $\mathfrak{M}_i$), te v valuacija na ultraproduktu $\prod_U \mathfrak{M}_i$ koja je inducirana familijom valuacija $\{v_i : i\in I\}$. Neka je F neka σ–formula. Tada vrijedi:*

$$\prod_U \mathfrak{M}_i \models_v F \quad \textit{ako i samo ako} \qquad \{i : \mathfrak{M}_i \models_{v_i} F\}\in U$$

Dokaz. Indukcijom po složenosti formuli F dokazujemo danu tvrdnju. Promotrimo prvo slučaj kada je F atomarna formula, tj. $F\equiv R(t_1,\ldots,t_k)$, gdje je R neki k–mjesni relacijski simbol, a $t_1,\ldots,t_k$ su σ–termi. Tada redom vrijedi:

$$\begin{aligned} \textstyle\prod_U \mathfrak{M}_i \models_v F \Leftrightarrow\ & \textstyle\prod_U \mathfrak{M}_i \models_v R(t_1,\ldots,t_k) \\ \Leftrightarrow\ & (v(t_1),\ldots,v(t_k))\in R^{\mathfrak{M}} \\ \Leftrightarrow\ & \Big((i\mapsto v_i(t_1))_U,\ldots,(i\mapsto v_i(t_k))_U\Big)\in R^{\mathfrak{M}} \\ \Leftrightarrow\ & \{i : (v_i(t_1),\ldots,v_i(t_k))\in R^{\mathfrak{M}_i}\}\in U \\ \Leftrightarrow\ & \{i : \mathfrak{M}_i \models_{v_i} R(t_1,\ldots,t_k)\}\in U \end{aligned}$$

Pretpostavimo sada da tvrdnja vrijedi za svaku formulu čija je složenost strogo manja od nekog $n\in\mathbb{N}\setminus\{0\}$ i svaku familiju valuacija $\{v_i : i\in I\}$. Neka je F proizvoljna σ–formula složenosti n. Promatramo slučajeve obzirom na oblik formule F.

Promotrimo prvo slučaj kada je F oblika $\neg G$. Tada redom vrijede sljedeće ekvivalencije:

$$\begin{aligned} \textstyle\prod_U \mathfrak{M}_i \models_v F \Leftrightarrow\ & \textstyle\prod_U \mathfrak{M}_i \models_v \neg G \ \Leftrightarrow\ \prod_U \mathfrak{M}_i \not\models_v G \\ & \text{(pretpostavka indukcije)} \\ \Leftrightarrow\ & \{i\in I : \mathfrak{M}_i \models_{v_i} G\}\notin U \\ & \text{(uvjet (v) iz definicije ultrafiltra)} \\ \Leftrightarrow\ & I\setminus\{i\in I : \mathfrak{M}_i \models_{v_i} G\}\in U \\ \Leftrightarrow\ & \{i\in I : \mathfrak{M}_i \not\models_{v_i} G\}\in U \\ \Leftrightarrow\ & \{i\in I : \mathfrak{M}_i \models_{v_i} \neg G\}\in U \end{aligned}$$

Promotrimo sada slučaj kada je formula F oblika $G \wedge H$. Redom vrijede sljedeće ekvivalencije:

$$\begin{aligned}
\prod_U \mathfrak{M}_i \models_v F \Leftrightarrow\ & \prod_U \mathfrak{M}_i \models_v G \wedge H \\
\Leftrightarrow\ & \prod_U \mathfrak{M}_i \models_v G \ \text{ i } \ \prod_U \mathfrak{M}_i \models_v H \\
& \text{(pretpostavka indukcije)} \\
\Leftrightarrow\ & \{i : \mathfrak{M}_i \models_{v_i} G\} \in U \ \text{ i } \ \{i : \mathfrak{M}_i \models_{v_i} H\} \in U \\
& ((\Rightarrow) \text{ slijedi zbog zatvorenosti ultrafiltra na presjeke}) \\
& ((\Leftarrow) \text{ slijedi zbog zatvorenosti ultrafiltra na nadskupove}) \\
& \Leftrightarrow \{i : \mathfrak{M}_i \models_{v_i} G\} \cap \{i : \mathfrak{M}_i \models_{v_i} H\} \in U \\
& \Leftrightarrow \{i : \mathfrak{M}_i \models_{v_i} G \wedge H\} \in U
\end{aligned}$$

Na kraju razmatramo slučaj kada je $F \equiv \exists x G(x)$. Pretpostavimo prvo da vrijedi $\prod_U \mathfrak{M}_i \models \exists x G(x)$. Tada iz definicije istinitosti slijedi da postoji valuacija $v_x : Var \to \prod_U M_i$ tako da vrijedi $v_x(y) = v(y)$ za svaku varijablu y različitu od x, te imamo $\prod_U \mathfrak{M}_i \models_{v_x} G(x)$. Lako je vidjeti da vrijedi

$$\begin{aligned}
\{i \ :\ & \mathfrak{M}_i \ \models_{(v_x)_i} G(x)\} \\
\subseteq\ & \{i \ :\ \text{postoji valuacija } (v_i)_x \text{ tako da } \mathfrak{M}_i \models_{(v_i)_x} G(x)\} \\
=\ & \{i \ :\ \mathfrak{M}_i \models_{v_i} \exists x G(x)\}
\end{aligned}$$

(Pazite! Valucije $(v_x)_i$ i $(v_i)_x$ općenito nisu iste.) Iz uvjeta zatvorenosti na nadskupove iz definicije ultrafiltra slijedi $\{i \ :\ \mathfrak{M}_i \models_{v_i} \exists x G(x)\} \in U$.

Dokažimo sada obrat. Pretpostavimo da vrijedi $S = \{i \ :\ \mathfrak{M}_i \models_{v_i} \exists x G(x)\} \in U$. Tada za svaki $i \in I$ postoji valuacija $(v_i)_x$ tako da vrijedi:

$$\left.\begin{array}{l} v_i(y) = (v_i)_x(y), \quad \text{za svaku varijablu } y \text{ različitu od } x \\ \mathfrak{M}_i \models_{(v_i)_x} G(x) \end{array}\right\} (*)$$

Neka je za svaki $i \in I$ valuacija $(v_i)_x$ fiksirana (aksiom izbora!). Pošto je očito ispunjeno $S = \{i : \models_{(v_i)_x} G(x)\}$, tada iz pretpostavke $S \in U$ slijedi i

$$\{i : \mathfrak{M}_i \models_{(v_i)_x} G(x)\} \in U \qquad (**)$$

Označimo $u \in \prod_{i \in I} M_i$ tako da za svaki $i \in S$ vrijedi $u(i) = (v_i)_x(x)$. Za svaki $i \in I \setminus S$ sa $(v_i)_x$ označimo valuaciju na $\mathfrak{M}_i$ koja je na svim varijablama y definirana sa: $(v_i)_x(y) = u(i)$. Neka je sa v' označena valuacija na ultraproduktu

koja je inducirana familijom valuacija $\{(v_i)_x : i \in I\}$. Iz $(**)$ i pretpostavke indukcije slijedi

$$\prod_U \mathfrak{M}_i \models_{v'} G(x) \qquad (***)$$

Iz $(*)$ slijedi da za svaku varijablu $y \neq x$ vrijedi $S \subseteq \{i \ : \ (v_i)_x(y) = v_i(y)\}$. Pošto je $S \in U$ tada iz uvjeta nadskupa iz definicije ultrafiltra očito slijedi da vrijedi $\{i \ : \ (v_i)_x(y) = v_i(y)\} \in U$. Iz ovog posljednjeg slijedi $(i \mapsto (v_i)_x(y))_U = (i \mapsto v_i(y))_U$, tj. $v'(y) = v(y)$, za svaku varijablu $y \neq x$. Sada iz $(***)$ i definicije istinitosti konačno dobivamo $\prod_U \mathfrak{M}_i \models_v \exists x G(x)$. □

Sljedeći teorem je direktna posljedica teorema 1.111.

Teorem 1.112. *(Łosov osnovni teorem o ultraproduktima)*
Neka je $I \neq \emptyset$, $\{\mathfrak{M}_i : i \in I\}$ proizvoljna familija σ–struktura i U proizvoljan ultrafiltar nad I. Tada za svaku zatvorenu formulu F vrijedi:

$$\prod_U \mathfrak{M}_i \models F \quad \textit{ako i samo ako} \quad \{i \in I : \mathfrak{M}_i \models F\} \in U.$$

Napomena 1.113. *Lako je pokazati da je ultraprodukt proizvoljne familije polja ponovno polje (nad proizvoljnim ultrafiltrom). Zatim, ultraprodukt familije linearno uređenih skupova je linearno uređen skup. No, sve te tvrdnje direktno slijede iz sljedećeg Łosovog teorema.*

Sada dajemo još jedan dokaz teorema kompaknosti.

Teorem 1.114. *(Teorem kompaktnosti)*
Neka je S proizvoljan skup zatvorenih formula. Za skup S postoji model ako i samo ako za svaki konačan podskup od S postoji model.

Dokaz. Pretpostavimo da za svaki konačan podskup od S postoji model. Označimo sa I skup svih konačnih podskupova skupa S. Za svaki $i \in I$ neka je sa $\mathfrak{M}_i$ označen neki model za skup formula i. Za svaki $F \in S$ označimo $S_F = \{i \in I : F \in i\}$, te $E = \{S_F : F \in S\}$. Lako je dokazati da skup E ima svojstvo konačnih presjeka. Iz teorema 1.100. slijedi da postoji ultrafiltar U nad I takav da je $E \subseteq U$. Dokažimo da je ultraprodukt $\prod_U \mathfrak{M}_i$ model za skup rečenica S. Neka je $F \in S$ proizvoljna rečenica. Za svaki $i \in S_F$ očito vrijedi $\mathfrak{M}_i \models i$, te $F \in i$. Tada očito za svaki $i \in S_F$ vrijedi $\mathfrak{M}_i \models F$. Iz toga slijedi: $S_F \subseteq \{i \in I : \mathfrak{M}_i \models F\}$. Pošto je po definiciji $S_F \in E$, te je $E \subseteq U$, tada imamo $S_F \in U$, a onda i $\{i \in I : \mathfrak{M}_i \models F\} \in U$. Iz Łosovog teorema sada slijedi $\prod_U \mathfrak{M}_i \models F$. □

Za ultrafiltar U kažemo da je **prebrojivo nepotpun** *ako nije zatvoren za prebrojive presjeke, tj. postoji niz $(X_n) \subseteq U$ takav da $\cap X_n \notin U$.*

Primjer 1.115. *Ultrafiltar nad $\mathbb{N}$ koji sadrži Fréchetov filtar je prebrojivo nepotpun. Neka je $X_n = \mathbb{N} \setminus \{n\}$. Pošto je svaki skup kofinitan tada je $X_n \in U$. Očito je $\cap_n X_n = \emptyset$. Svaki glavni ultrafiltar je prebrojivo potpun. Ako je $U = \{X \subseteq I : a \in X\}$ neki glavni filtar, te $(X_n) \subseteq U$, tada je očito $a \in \cap X_n$. Iz toga odmah slijedi $\cap X_n \in U$, tj. glavni ultrafiltar U je prebrojivo potpun.*

Propozicija 1.116. *Neka je $I \neq \emptyset$ i U ultrafiltar nad I. Tada su sljedeće tvrdnje ekvivalentne:*

a) ultrafiltar U je prebrojivo nepotpun;

b) postoji niz $(Y_n) \subseteq U$ takav da vrijedi

$$\cap Y_n = \emptyset \quad i \quad I = Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq \dots$$

c) postoji niz $(Z_n) \subseteq \mathcal{P}(I)$ takav da za svaki $n \in \mathbb{N}$ vrijedi $Z_n \notin U$, a za sve $n \neq m$ vrijedi

$$Z_n \cap Z_m = \emptyset \quad i \quad \cup Z_n = I$$

Napomena 1.117. *Ultrapotencija nad glavnim ultrafiltrom je elementarno ekvivalentna početnom modelu, pa takve konstrukcije nisu zanimljive. Točnije: ako je $I \neq \emptyset$, $a \in I$ i $U = \{X \subseteq I \ : \ a \in X\}$, te $\mathfrak{M}$ neka σ–struktura, tada vrijedi $\prod_U \mathfrak{M} \equiv \mathfrak{M}$.*

Teorem 1.118. *Neka je $\mathcal{K}$ neka klasa σ–struktura. Tada vrijedi:*

(a) klasa $\mathcal{K}$ je elementarna ako i samo ako klasa $\mathcal{K}$ je zatvorena za ultraprodukte i elementarnu ekvivalenciju.

(b) klasa $\mathcal{K}$ je Δ–elementarna ako i samo ako klase $\mathcal{K}$ i $\mathcal{K}^c$ su zatvorene za ultraprodukte i elementarnu ekvivalenciju.

Dokaz a). Pretpostavimo prvo da je klasa $\mathcal{K}$ elementarna, tj. da postoji skup formula Σ tako da vrijedi $\mathcal{K} = Mod(\Sigma)$. Svaka elementarna klasa je očito zatvorena za elementarnu ekvivalenciju. Neka je $\{\mathfrak{M}_i : i \in I\}$ neka podklasa od $\mathcal{K}$, te U neki ultrafiltar nad I. Pošto za svaki $i \in I$ vrijedi $\mathfrak{M}_i \models \Sigma$, tada iz Łosovog teorema slijedi $\prod_U \mathfrak{M}_i \models \Sigma$, a onda i $\prod_U \mathfrak{M}_i \in \mathcal{K}$.

Dokažimo sada obrat u tvrdnji a). Neka je $\mathcal{K}$ proizvoljna klasa σ–struktura koja je zatvorena za ultraprodukte i elementarnu ekvivalenciju. Neka je $\Sigma = \{F : \mathcal{K} \models F\}$. Tvrdimo da vrijedi $\mathcal{K} = Mod(\Sigma)$. Očito je $\mathcal{K} \subseteq Mod(\Sigma)$. Dokažimo obratnu inkluziju. Neka je $\mathfrak{N} \in Mod(\Sigma)$. Neka je I skup svih konačnih podskupova skupa $Th(\mathfrak{N})$ $(= \{G : \mathfrak{N} \models G\}$). Lako je provjeriti da za svaki $i \in I$ postoji σ–struktura $\mathfrak{M}_i$ tako da vrijedi $\mathfrak{M}_i \models i$. Na isti način kao u dokazu teorema kompaktnosti možemo izabrati ultrafiltar U nad skupom I tako da vrijedi $\prod_U \mathfrak{M}_i \models Th(\mathfrak{N})$. Pošto je po pretpostavci klasa $\mathcal{K}$ zatvorena za ultraprodukte tada je $\prod_U \mathfrak{M}_i \in \mathcal{K}$. Iz $\prod_U \mathfrak{M}_i \models Th(\mathfrak{N})$ lako slijedi $\prod_U \mathfrak{M}_i \equiv \mathfrak{N}$. Pošto je po pretpostavci klasa $\mathcal{K}$ zatvorena za elementarnu ekvivalenciju tada imamo $\mathfrak{N} \in \mathcal{K}$.

Tvrdnja b) teorema slijedi iz upravo dokazane tvrdnje a) i propozicije koja govori da je neka klasa $\mathcal{K}$ Δ–elementarna ako i samo ako su klase $\mathcal{K}$ i $\mathcal{K}^c$ elementarne. □

Bez dokaza ovdje ističemo pojačanu verziju prethodnog teorema (vidi npr. [6]).

Teorem 1.119. *Neka je $\mathcal{K}$ neka klasa σ–struktura. Tada je ekvivalentno:*

(i) klasa $\mathcal{K}$ je elementarna;

(ii) klasa $\mathcal{K}$ je zatvorena za ultraprodukte i izomorfizme, a klasa $\mathcal{K}^c$ je zatvorena za ultraprotencije.

1.11 Teoremi o očuvanju

Teoremi o očuvanju dovode u vezu sintaktičku formu teorije (tj. njenih formula) i zatvorenosti klase svih modela teorije u odnosu na neko svojstvo. Mi ćemo promatrati teorije čije klase modela su redom zatvorene na: podmodele, proširenja modela, unije lanaca modela, homomorfizme i reducirane produkte.

Za formulu F kažemo da je **univerzalna formula** ako postoji otvorena formula G tako da vrijedi: $F \equiv \forall x_1 \ldots \forall x_n G$. Za teoriju T kažemo da je **univerzalna teorija** ako sadrži samo univerzalne rečenice.

Teorija linearnih uređaja je univerzalna teorija. Teorija grupa je također univerzalna teorija ako uz simbole $\cdot, 1$ i $=$ uvedemo i jednomjesni funkcijski simbol $^{-1}$, te umjesto rečenice $\forall x \exists y (x \cdot y = y \cdot x = 1)$ stavimo $\forall x (x \cdot x^{-1} = x^{-1} \cdot x = 1)$.

Primijetimo da konjunkcija dvije univerzalne formule nije univerzalna formula, ali je konjunkcija univerzalnih formula logički ekvivalentna univerzalnoj formuli.

Ako je T neka teorija tada sa $Mod(T)$ označavamo klasu svih modela teorije T. Kažemo da su dvije σ–teorije T i T' ekvivalentne ako vrijedi $Mod(T) = Mod(T')$.

Za teoriju T kažemo da je **očuvana za podmodele** ako za svaki model $\mathfrak{M}$ teorije T i svaki podmodel $\mathfrak{N}$ od $\mathfrak{M}$ vrijedi da je $\mathfrak{N}$ također model od T. (Odnosno, klasa $Mod(T)$ je zatvorena za podmodele).

Teorem 1.120. *Neka je T neka σ–teorija. Ekvivalentno je:*

a) teorija T je očuvana za podmodele

b) postoji univerzalna σ–teorija T' koja je ekvivalentna s teorijom T.

Dokaz. Dokažimo prvo da b) povlači a). Neka je $\mathfrak{M}$ proizvoljni model teorije T i $\mathfrak{N} \subseteq \mathfrak{M}$. Pošto je $Mod(T) = Mod(T')$ tada očito vrijedi $\mathfrak{M} \models T'$. Indukcijom po broju kvantifikatora formule oblika $\forall x_1 \ldots \forall x_n G$, gdje je G otvorena formula, lako je dokazati da vrijedi:

$$\text{ako} \quad \mathfrak{M} \models \forall x_1 \ldots \forall x_n G \quad \text{tada} \quad \mathfrak{N} \models \forall x_1 \ldots \forall x_n G$$

Sada posebno za svaku univerzalnu rečenicu $F \in T'$ vrijedi $\mathfrak{N} \models F$. Time smo dokazali $\mathfrak{N} \models T'$, a onda iz $Mod(T) = Mod(T')$ slijedi $\mathfrak{N} \models T$.

Dokažimo sada obrat, tj. a)⇒b). Definiramo teoriju $T' = \{G : G \text{ je univerzalna rečenica i } T \models G\}$. Tvrdimo da su teorije T i T' ekvivalentne. Očito $T \models T'$.

Za dokaz ekvivalentnosti teorija T i T' treba još samo dokazati da za svaku formulu $F \in T$ vrijedi $T' \models F$. Neka je $\mathfrak{M}$ proizvoljan model za teoriju T'. Dokazujemo da je teorija $T \cup \Delta(\mathfrak{M})$ konzistentna. (Uočimo da tada iz leme o dijagramu slijedi da tada postoji model $\mathfrak{N}$ za $T \cup \Delta(\mathfrak{M})$, tako da vrijedi $\mathfrak{M} \subseteq \mathfrak{N}^-$. Tada iz pretpostavke da je teorija T očuvana za podmodele slijedi $\mathfrak{M} \models T$). Pretpostavimo suprotno, tj. da je teorija $T \cup \Delta(\mathfrak{M})$ inkonzistentna. Tada iz **teorema kompaktnosti** slijedi da postoji skup $\{G_1, \ldots, G_m\} \subseteq \Delta(\mathfrak{M})$ i skup $\{H_1, \ldots, H_p\} \subseteq T$ tako da skup formula $\{G_1, \ldots, G_m, H_1, \ldots, H_p\}$ nije ispunjiv. Neka su $a_1, \ldots, a_n \in |\mathfrak{M}|$ takvi da su $\overline{a_1}, \ldots, \overline{a_n}$ svi konstantski simboli koji se pojavljuju u nekoj od formula $G_1, \ldots, G_m$. Iz definicije dijagrama slijedi da je skup $\Delta(\mathfrak{M})$ zatvoren za konjunkcije. Iz toga slijedi da je $G_1 \wedge \ldots \wedge G_m \in \Delta(\mathfrak{M})$. Označimo $G(\overline{a_1}, \ldots, \overline{a_n}) \equiv G_1 \wedge \ldots \wedge G_m$. Tada vrijedi $T \models \neg G(\overline{a_1}, \ldots, \overline{a_n}) \wedge H_1 \wedge \ldots \wedge H_p$. Pošto je $G(\overline{a_1}, \ldots, \overline{a_n}) \in \Delta(\mathfrak{M})$ tada po definiciji vrijedi:

$$\mathfrak{M} \models G[a_1, \ldots, a_n] \qquad (*)$$

Iz $T \models \neg G(\overline{a_1}, \ldots, \overline{a_n})$ i činjenice $\{\overline{a_1}, \ldots, \overline{a_n}\} \cap \sigma = \emptyset$, slijedi da tada vrijedi i $T \models \forall x_1 \ldots \forall x_n \neg G(x_1, \ldots, x_n)$. Iz definicije teorije T' slijedi da joj formula $\forall x_1 \ldots \forall x_n \neg G(x_1, \ldots, x_n)$ pripada. Pošto je $\mathfrak{M}$ model za teoriju T' tada posebno vrijedi $\mathfrak{M} \models \forall x_1 \ldots \forall x_n \neg G(x_1, \ldots, x_n)$, što je kontradikcija sa $(*)$. □

Primjer 1.121. *Već smo bili istaknuli da za signaturu $\sigma = \{\cdot, 1, =\}$ teorija grupa nije univerzalna teorija. Postavlja se pitanje postoji li univerzalna teorija (iste signature!) koja je ekvivalentna teoriji grupa. U tu svrhu primijenimo prethodni teorem. Neka je $\mathfrak{M} = (\mathbb{Z}, +)$ i $\mathfrak{N} = (\mathbb{N}, +)$. Struktura $\mathfrak{M}$ je model teorije grupa, te vrijedi $\mathfrak{N} \subseteq \mathfrak{M}$. No, pošto $\mathfrak{N}$ nije grupa, tada teorija grupa nije očuvana za podmodele. Iz prethodnog teorema slijedi da teorija grupa nije ekvivalentna nekoj univerzalnoj teoriji. To možemo interpretirati i na sljedeći način: ne postoji aksiomatizacija teorije grupa u signaturi σ koja sadrži samo univerzalne formule.*

Za formulu F kažemo da je **egzistencijalna formula** ako postoji otvorena formula G tako da vrijedi: $F \equiv \exists x_1 \ldots \exists x_n G$. Za teoriju T kažemo da je **egzistencijalna teorija** ako sadrži samo egzistencijalne rečenice. Za teoriju T kažemo da je **očuvana za proširenja modela** ako za svaki model $\mathfrak{M}$ teorije T i svako proširenje $\mathfrak{N}$ od $\mathfrak{M}$ vrijedi da je $\mathfrak{N}$ također model od T. (Odnosno, klasa $Mod(T)$ je zatvorena za proširenja modela).

Teorem 1.122. *Neka je T neka σ–teorija. Ekvivalentno je:*

a) teorija T je očuvana za proširenja

b) postoji egzistencijalna σ–teorija T' koja je ekvivalentna s teorijom T.

Dokaz. Dokažimo prvo da vrijedi b) $\Rightarrow$ a). Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture takve da $\mathfrak{M} \subseteq \mathfrak{N}$ i $\mathfrak{M} \models T$. Pretpostavimo da postoji $F \in T'$ takva da $\mathfrak{N} \not\models F$. Pošto je F rečenica tada vrijedi $\mathfrak{N} \models \neg F$. Pošto je rečenica $\neg F$ ekvivalentna univerzalnoj rečenici tada iz teorema 1.120. slijedi da je teorija $\{\neg F\}$ očuvana za podmodele. Sada iz $\mathfrak{M} \subseteq \mathfrak{N}$ i $\mathfrak{N} \models \neg F$ slijedi $\mathfrak{M} \models \neg F$. U drugu ruku iz $\mathfrak{M} \models T$, $F \in T'$ i $Mod(T) = Mod(T')$, imamo $\mathfrak{M} \models F$. Time je dobivena kontradikcija. To znači da je $\mathfrak{N}$ model za teoriju T'. Pošto $Mod(T) = Mod(T')$, tada je $\mathfrak{N}$ model i za teoriju T, pa smo dokazali da je teorija T očuvana za proširenja.
Dokažimo obrat. Neka je teorija T očuvana za proširenja. Za svaku zatvorenu formulu F označimo:

$$U(F) := \{G \ : \ G \ \text{ je univerzalna rečenica, } \ F \to G \text{ je valjana}\}$$

Primjenom metode dijagrama lako je dokazati da je za svaku rečenicu F teorija $\Delta(\mathfrak{M}) \cup \{F\}$ konzistentna. Tada očito vrijedi sljedeća tvrdnja, koju označavamo sa $(*)$:

> za svaku rečenicu F i svaki model $\mathfrak{M}$ za teoriju $U(F)$ postoji model $\mathfrak{N}$ za F koji je proširenje strukture $\mathfrak{M}$.

Primjenom pomoćne tvdnje $(*)$ lako se dobiva da vrijedi:

> za svaku rečenicu $F \in T$ teorija $U(\neg F) \cup T$ je inkonzistentna

Neka je $F \in T$ proizvoljna. Iz prethodne tvrdnje i **teorema kompaktnosti** slijedi da postoje rečenice $G_1, \ldots, G_n \in U(\neg F)$ tako da je teorija $\{G_1, \ldots, G_n\} \cup T$ inkonzistentna. Neka je $G_F \equiv G_1 \wedge \ldots \wedge G_n$. Pošto je svaka rečenica G_i univerzalna formula, tada bez smanjenja općenitosti možemo pretpostaviti da je i formula G_F univerzalna formula. Pošto je očito teorija $T \cup \{G_F\}$ inkonzistentna, tada vrijedi:

$$T \models \neg G_F \qquad (**)$$

Neka je $T' := \{\neg G_F \ : \ F \in T\}$. Bili smo primijetili da je svaka formula G_F univerzalna, pa je formula $\neg G_F$ ekvivalentna egzistencijalnoj formuli. Bez smanjenja općenitosti možemo pretpostaviti da je svaka formula $\neg G_F$ egzistencijalna, tj. da je teorija T' egzistencijalna. Iz $(**)$ slijedi $T \models T'$. Dokažimo obrat. Neka je $\mathfrak{M}$ proizvoljan model za teoriju T', i $F \in T$. Pošto je formula $\neg G_F \to F$ valjana, te je $\neg G_F \in T'$, tada $\mathfrak{M} \models F$. □

Za rečenicu F kažemo da je $\forall\exists$–**formula** ako postoji otvorena formula G tako da vrijedi $F \equiv \forall x_1 \ldots \forall x_n \exists x_{n+1} \ldots \exists x_m \ G$, pri čemu dopuštamo da je $n = 0$ ili

$m = 0$ (može i oboje). Za teoriju T kažemo da je $\forall\exists$–**teorija** ako su svi njeni elementi $\forall\exists$–formule.

Primijetimo da su univerzalane i egzistencijalne formule posebni primjeri upravo definiranih $\forall\exists$–formula. Primijetimo, zatim, da su konjunkcija i disjunkcija $\forall\exists$–formula ekvivalentne nekoj $\forall\exists$–formuli (potrebno je samo preimenovati vezane varijable).

Kažemo da je neka teorija T **očuvana za unije lanaca modela** ako za svaku familiju $\{\mathfrak{M}_i : i \in I\}$ modela teorije T takvu da je $(I, <)$ linerano uređen skup, te za sve $i < j$ imamo $\mathfrak{M}_i \subseteq \mathfrak{M}_j$, vrijedi da je $\cup_{i\in I}\mathfrak{M}_i$ model teorije T.

Cilj nam je dokazati teorem koji govori da je teorija očuvana za unije lanaca modela ako i samo ako je ta teorija ekvivalentna nekoj $\forall\exists$–teoriji. No, prije toga iskazujemo tri leme. Neka $\mathfrak{M} \subseteq \mathfrak{N}$. Kažemo da je $\mathfrak{M}$ jedan 1–**elementarni podmodel** od $\mathfrak{N}$ ako za svaku univerzalnu formulu $F(v_1, \ldots, v_n)$ i sve $a_1, \ldots, a_n$ iz $|\mathfrak{M}|$ vrijedi da $\mathfrak{M} \models F[a_1, \ldots, a_n]$ povlači $\mathfrak{N} \models F[a_1, \ldots, a_n]$. Ako je $\mathfrak{M}$ neki 1–elementarni podmodel od $\mathfrak{N}$ tada to označavamo sa $\mathfrak{M} \prec_1 \mathfrak{N}$. Sljedeću lemu je jednostavno dokazati indukcijom po broju kvantifikatora formule F.

Lema 1.123. *Neka $\mathfrak{M} \prec_1 \mathfrak{N}$. Tada za sve univerzalne i egzistencijalne formule F vrijedi*

$$\mathfrak{M} \models F[a_1, \ldots, a_n] \qquad \textit{ako i samo ako} \qquad \mathfrak{N} \models F[a_1, \ldots, a_n]$$

Sljedeće dvije leme se na standardni način dokazuju metodom dijagrama.

Lema 1.124. *Neka $\mathfrak{M} \prec_1 \mathfrak{N}$. Tada postoji struktura $\mathfrak{A}$ tako da je $\mathfrak{M} \prec \mathfrak{A}$ i $\mathfrak{N} \subseteq \mathfrak{A}$.*

Lema 1.125. *Neka je T neka σ–teorija. Označimo:*

$$T' := \{G : G \text{ je } \forall\exists\textit{–rečenica, } T \models G\}.$$

Neka je $\mathfrak{M}$ neki model za teoriju T'. Tada postoji struktura $\mathfrak{N}$ tako da vrijedi:

$$\mathfrak{M} \prec_1 \mathfrak{N} \quad i \quad \mathfrak{N} \models T$$

Teorem 1.126. *Neka je T neka σ–teorija. Ekvivalentno je:*

a) teorija T je očuvana za unije lanaca modela

b) postoji $\forall\exists$–teorija T' koja je ekvivalentna s teorijom T.

Dokaz. Primjenom teorema o uniji lanaca modela lako je dokazati da je svaka $\forall\exists$–formula očuvana za unije lanaca modela.
Dokažimo obrat. Neka je teorija T očuvana za unije lanaca modela. Označimo: $T' := \{G \ : \ G \ \text{ je } \ \forall\exists\text{–formula}, \ T \models G\}$. Očito $T \models T'$. Dokažimo da vrijedi i obratno. Neka je $\mathfrak{M}_0$ proizvoljan model za teoriju T'. Iz leme 1.125. slijedi da postoji model $\mathfrak{M}_1$ za teoriju T tako da vrijedi $\mathfrak{M}_0 \prec_1 \mathfrak{M}_1$. Sada iz leme 1.124. slijedi da postoji struktura $\mathfrak{M}_2$ tako da vrijedi $\mathfrak{M}_0 \prec \mathfrak{M}_2$ i $\mathfrak{M}_1 \subseteq \mathfrak{M}_2$. (Pošto $\mathfrak{M}_0 \models T'$ i $\mathfrak{M}_0 \prec \mathfrak{M}_2$ tada $\mathfrak{M}_2 \models T'$). Uzastopnom primjenom lema dobivamo lanac modela $\{\mathfrak{M}_k : k \in \mathbb{N}\}$ tako da za svaki $k \in \mathbb{N}$ vrijedi:

$$\begin{array}{l} \mathfrak{M}_{2k} \models T' \quad \text{i} \quad \mathfrak{M}_{2k+1} \models T; \\ \mathfrak{M}_{2k} \prec_1 \mathfrak{M}_{2k+1}, \quad \mathfrak{M}_{2k} \prec \mathfrak{M}_{2k+2} \quad \text{i} \quad \mathfrak{M}_{2k+1} \subseteq \mathfrak{M}_{2k+2} \end{array}$$

Iz gornjeg posebno slijedi da za svaki $k \in \mathbb{N}$ vrijedi $\mathfrak{M}_{2k} \subseteq \mathfrak{M}_{2k+1}$. Iz ovog posljednjeg i $\mathfrak{M}_{2k+1} \subseteq \mathfrak{M}_{2k+2}$, slijedi da za svaki $k \in \mathbb{N}$ vrijedi $\mathfrak{M}_k \subseteq \mathfrak{M}_{k+1}$. Označimo $\mathfrak{M} := \cup_{k\in\mathbb{N}}\mathfrak{M}_k$. Uočimo da je $\mathfrak{M} := \cup_{k\in\mathbb{N}}\mathfrak{M}_{2k+1}$. Pošto za svaki $k \in \mathbb{N}$ vrijedi $\mathfrak{M}_{2k+1} \models T$, te je po pretpostavci teorija T očuvana za unije lanaca tada imamo $\mathfrak{M} \models T$. Pošto $\mathfrak{M}_{2k} \prec \mathfrak{M}_{2k+2}$ i $\mathfrak{M} = \cup_k\mathfrak{M}_{2k}$ tada iz teorema o uniji elementarnih lanaca slijedi $\mathfrak{M}_0 \prec \mathfrak{M}$. Sada iz $\mathfrak{M} \models T$ slijedi $\mathfrak{M}_0 \models T$. □

Primjeri nekih $\forall\exists$–teorija su: teorija grupa, teorija polja i teorija gustih linearnih uređaja bez rubnih točaka.

Za teoriju T kažemo da je **modelno potpuna** ako za svaka dva modela $\mathfrak{M}$ i $\mathfrak{N}$ teorije T, takve da je $\mathfrak{M} \subseteq \mathfrak{N}$, vrijedi $\mathfrak{M} \prec \mathfrak{N}$.

Propozicija 1.127. *Svaka modelno potpuna teorija je ekvivalentna nekoj $\forall\exists$–teoriji.*

Dokaz. Neka je $\{\mathfrak{M}_i : i \in I\}$ neki lanac modela za teoriju T. Neka su $i, j \in I$ takvi da je $i < j$. Tada imamo $\mathfrak{M}_i \subseteq \mathfrak{M}_j$, a onda iz modelne potpunosti teorije T slijedi $\mathfrak{M}_i \prec \mathfrak{M}_j$. To znači da je $\{\mathfrak{M}_i : i \in I\}$ elementarni lanac modela za teoriju T. Iz teorema o uniji elementarnih lanaca slijedi da je $\cup\mathfrak{M}_i$ model za teoriju T. Iz prethodnog teorema slijedi da je teorija T ekvivalentna nekoj $\forall\exists$–teoriji. □

Primjer 1.128. *Navodimo jedan primjer teorije koja nije očuvana za unije lanaca modela. Neka je T teorija gustih linearnioh uređaja s rubovima. Za svaki $k \in \mathbb{N}$ neka je $\mathfrak{M}_k := ([-k, k], <)$. Tada očito za svaki $k \in \mathbb{N}$ vrijedi $\mathfrak{M}_k \models T$. No, pošto je očito $\cup_k\mathfrak{M}_k = \mathbb{R}$, tada $\cup_k\mathfrak{M}_k \not\models T$.*

Kažemo da je neka formula φ **pozitivna** ako je izgrađena iz atomarnih formula samo pomoću veznika $\wedge$ i $\vee$, te pomoću kvantifikatora $\exists$ i $\forall$ (dakle, u sebi ne sadrži negaciju, kondicional, a ni bikondicional). Za neku teoriju kažemo da je **pozitivna teorija** ako je svaka njena rečenica pozitivna formula.
Kažemo da je neka σ–**formula** $\varphi(v_1, \ldots, v_n)$ **očuvana za homomorfizme** ako za sve σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$, te za svaki homomorfizam $h : \mathfrak{M} \to \mathfrak{N}$ i sve $a_1, \ldots, a_n$ iz $|\mathfrak{M}|$, vrijedi

$$\text{ako} \quad \mathfrak{M} \models \varphi[a_1, \ldots, a_n] \quad \text{tada} \quad \mathfrak{N} \models \varphi[h(a_1), \ldots, h(a_n)]$$

Kažemo da je **teorija očuvana za homomorfizme** ako je svaka njena formula očuvana za homomorfizme.

Teorem 1.129. *Neka je T neka konzistentna σ–teorija. Ekvivalentno je:*

a) teorija T je očuvana za homorfizme

b) postoji pozitivna σ–teorija T' koja je ekvivalentna s teorijom T.

Dokaz. Prvo, primijetimo da je bitan zahtjev na konzistentnost. Naime, inkonzistentna teorija je trivijalno zatvorena za homomorfizme (jer nema modela), no nije ekvivalentna niti jednoj pozitivnoj teoriji, jer je kontradikciju nemoguće zapisati kao pozitivnu formulu. U drugu ruku, primijetimo da struktura $\{0\}$, u kojoj su svi konstantski simboli interpretirani s 0, svi funkcijski simboli kao konstantne 0–funkcije, a svi relacijski simboli kao $\{(0, \ldots, 0)\}$, je model za svaku pozitivnu formulu nad bilo kojim skupom simbola σ. Dakle, za svaku pozitivnu teoriju postoji model.

Za jedan smjer, da ekvivalentnost s pozitivnom teorijom povlači zatvorenost za homomorfizme, dovoljno je vidjeti da je svaka pozitivna formula očuvana za homomorfizme (onda će i njihove logičke posljedice biti takve). No to je jednostavno dokazati indukcijom po složenosti formule. Uočimo da su otvorene pozitivne formule dobivene pomoću konjunkcije i disjunkcije iz atomarnih, koje su pak očuvane za homomorfizme po definiciji.

Dokažimo drugi smjer, odnosno da zatvorenost za homomorfizme povlači ekvivalentnost s nekom pozitivnom teorijom (i konzistentnom). Neka je T konzistentna σ–teorija koja je zatvorena za homomorfizme. Na proizvoljnim σ–strukturama definirajmo binarnu relaciju $\equiv_p$ ovako:

$$\begin{aligned} &\mathfrak{M} \equiv_p \mathfrak{N} \quad \text{ako i samo ako} \\ &\quad (\forall F \ \text{ pozitivnu } \sigma\text{–rečenicu}) \ (\mathfrak{M} \models F \ \text{ ako i samo ako } \ \mathfrak{N} \models F) \end{aligned}$$

Sada nam trebaju dvije leme.

Lema 1.130. *Neka su* $\mathfrak{M}$ *i* $\mathfrak{N}$ *proizvoljne* σ*–strukture. Ako* $\mathfrak{M} \equiv_p \mathfrak{N}$ *tada postoji* σ*–struktura* $\mathfrak{A}$*, takva da vrijedi:*

(i) $\mathfrak{N} \prec \mathfrak{A}$

(ii) postoji smještenje $f : \mathfrak{M} \to \mathfrak{A}$ *takvo da* $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|} \equiv_p (\mathfrak{A}, f(a))_{a\in|\mathfrak{M}|}$.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da su strukture $\mathfrak{M}$ i $\mathfrak{N}$ disjunktne (inače uzmemo njihove izomorfne kopije). Dokaz provodimo metodom "pozitivnog" dijagrama. U tu svrhu definiramo dvije nove teorije ("pozitivni dijagrami"):

$$T_{\mathfrak{M}} := \{F \,:\, F \text{ je pozitivna } \sigma_{|\mathfrak{M}|}\text{–rečenica, } (\mathfrak{M}, a)_{a\in|\mathfrak{M}|} \models F\}$$

$$T_{\mathfrak{N}} := \{F \,:\, F \text{ je pozitivna } \sigma_{|\mathfrak{N}|}\text{–rečenica, } (\mathfrak{N}, a)_{a\in|\mathfrak{N}|} \models F\}$$

Naravno, $T_{\mathfrak{M}}$ je $\sigma_{\mathfrak{M}}$–teorija, a $T_{\mathfrak{N}}$ je $\sigma_{\mathfrak{N}}$–teorija. No, obje teorije se mogu promatrati i kao $\sigma_{\mathfrak{M}} \cup \sigma_{\mathfrak{N}}$–teorije. Označimo $T' := T_{\mathfrak{M}} \cup T_{\mathfrak{N}}$. Teorija T' je konzistentna (prije smo bili primijetili da to vrijedi za svaku pozitivnu teoriju). Štoviše, pošto vrijedi $\mathfrak{M} \equiv_p \mathfrak{N}$ i $|\mathfrak{M}| \cap |\mathfrak{N}| = \emptyset$, tada postoji model $\mathfrak{B}$ za teoriju T' koji je oblika $(\mathfrak{A}, a', b)_{a\in|\mathfrak{M}|\wedge b\in|\mathfrak{N}|}$, gdje je $\mathfrak{A}$ σ-struktura. Opišimo malo preciznije konstrukciju modela $\mathfrak{B}$. Za svaki konačan podskup od T', označimo s $F_1, \ldots, F_k$ sve njegove elemente iz $T_{\mathfrak{M}}$, a s $G_1, \ldots, G_l$ sve njegove (preostale) elemente iz $T_{\mathfrak{N}}$. Konjunkcija svih F_i, $F := \bigwedge_{i=1}^{k} F_i$, je također pozitivna $\sigma_{|\mathfrak{M}|}$-rečenica, koja je istinita na $(\mathfrak{M}, a)_{a\in|\mathfrak{M}|}$, te je $F \in T_{\mathfrak{M}}$. Jednako tako je $G := \bigwedge_{j=1}^{l} G_j \in T_{\mathfrak{N}}$. Model za formule F i G bit će model i za početni konačan podskup od T'. Model za F i G postoji unutar $|\mathfrak{N}|$, samo što ćemo za $a \in |\mathfrak{N}|$, morati $\overline{a}$ interpretirati s nekim $a' \in |\mathfrak{N}|$. Iz $\mathfrak{B} \models T_{\mathfrak{N}}$ zaključujemo $\mathfrak{N} \equiv \mathfrak{A}$, a budući da je i $|\mathfrak{N}| \subseteq |\mathfrak{A}|$, imamo $\mathfrak{N} \prec \mathfrak{A}$. Jednako tako iz $\mathfrak{B} \models T_{\mathfrak{M}}$ slijedi drugi dio leme. □

Zamjenom uloga struktura $\mathfrak{M}$ i $\mathfrak{N}$ u iskazu prethodne leme dobivamo sljedeću lemu.

Lema 1.131. *Neka su* $\mathfrak{M}$ *i* $\mathfrak{N}$ *proizvoljne* σ*–strukture. Ako* $\mathfrak{M} \equiv_p \mathfrak{N}$*, tada postoji* σ*-struktura* $\mathfrak{A}$*, takva da vrijedi:*

(i) $\mathfrak{M} \prec \mathfrak{A}$

(ii) postoji smještenje $g : \mathfrak{N} \to \mathfrak{A}$ *takvo da* $(\mathfrak{A}, g(b))_{a\in|\mathfrak{N}|} \equiv_p (\mathfrak{N}, b)_{b\in|\mathfrak{N}|}$.

Iz prethodne dvije leme možemo dobiti da za našu teoriju T vrijedi sljedeće:

Propozicija 1.132. *Neka je T konzistentna σ-teorija koja je zatvorena za homomorfizme, te neka su $\mathfrak{M}_0$ i $\mathfrak{N}_0$ dvije proizvoljne σ–strukture. Ako vrijedi $\mathfrak{M}_0 \equiv_p \mathfrak{N}_0$ i $\mathfrak{M}_0 \models T$, tada imamo i $\mathfrak{N}_0 \models T$.*

Dokaz. Prvo na strukture $\mathfrak{M}_0$ i $\mathfrak{N}_0$ primijenimo lemu 1.130. Dobijemo strukturu, koju označimo sa $\mathfrak{N}_1$, i homomorfizam $f_0 : \mathfrak{M}_0 \to \mathfrak{N}_1$, takve da vrijedi

$$\mathfrak{N}_0 \prec \mathfrak{N}_1 \quad \text{i} \quad (\mathfrak{M}_0, a)_{a\in|\mathfrak{M}_0|} \equiv_p (\mathfrak{N}_1, f_0(a))_{a\in|\mathfrak{M}_0|}$$

Sada, primijenimo li lemu 1.131. na modele $\mathfrak{M}_0$ i $\mathfrak{N}_1$ (točnije, na strukture $(\mathfrak{M}_0, a)_{a\in|\mathfrak{M}_0|}$ i $(\mathfrak{N}_1, f_0(a))_{a\in|\mathfrak{M}_0|}$), dobijemo strukturu $\mathfrak{M}_1$ i homomorfizam $g_1 : \mathfrak{N}_1 \to \mathfrak{M}_1$, takve da je

$$\mathfrak{M}_0 \prec \mathfrak{M}_1 \qquad \text{i}$$
$$(\mathfrak{M}_1, a, g_1(b))_{a\in|\mathfrak{M}_0|\wedge b\in|\mathfrak{N}_1|} \equiv_p (\mathfrak{N}_1, b)_{b\in|\mathfrak{N}_1|} = (\mathfrak{N}_0, f_0(a), b)_{a\in|\mathfrak{M}_0|\wedge b\in|\mathfrak{N}_1|}$$

Sada imamo strukture $\mathfrak{M}_1$ i $\mathfrak{N}_1$, na odgovarajući način proširene, između kojih vrijedi relacija $\equiv_p$, pa na njih ponovo možemo primijeniti lemu 1.130. Dobit ćemo strukturu $\mathfrak{N}_2$ i homomorfizam f_1, no iz dokaza leme 1.130. se vidi da možemo uzeti f_1 kao proširenje od f_0. Jednako tako ćemo u sljedećem koraku dobiti strukturu $\mathfrak{M}_2$ i homomorfizam g_2, i tako dalje. Uzastopnom primjenom lema 1.130. i 1.131. dobivamo dva elementarna lanca struktura, u kojima je svaka elementarno proširenje one prethodne, te homomorfizme među njima koji također čine rastući niz:

$$\begin{array}{l}\text{za svaki } n \in \mathbb{N} \text{ je } f_n : \mathfrak{M}_n \to \mathfrak{N}_{n+1} \text{ homomorfizam,}\\ \text{te vrijedi } f_n \subseteq f_{n+1}\end{array}$$

To znači da ako napravimo unije lanaca:

$$\mathfrak{M}_\omega := \bigcup_{n\in\omega} \mathfrak{M}_n \quad \text{i} \quad \mathfrak{N}_\omega := \bigcup_{n\in\omega} \mathfrak{N}_n,$$

tada će unija homomorfizama, $f_\omega := \bigcup_{n\in\omega} f_n$, biti homomorfizam između $\mathfrak{M}_\omega$ i $\mathfrak{N}_\omega$ (svaka formula u sebi sadrži samo konačno mogo varijabli, te ako su parametri a_i iz pojedinih $|\mathfrak{M}_{j_i}|$, od svih j_i postoji najveći, $j_{\max}$. Sada jednostavno iskoristimo činjenicu da je $f_{j_{\max}}$ homomorfizam).
Iz **teorema o uniji elementarnih lanaca** slijedi da je svaka struktura $\mathfrak{M}_i$ elementarna podstruktura od $\mathfrak{M}_\omega$. Specijalno vrijedi $\mathfrak{M}_0 \prec \mathfrak{M}_\omega$. Jednako tako je i $\mathfrak{N}_0 \prec \mathfrak{N}_\omega$. No ako je $\mathfrak{M}_0$ model za T, tada je zbog $\mathfrak{M}_0 \prec \mathfrak{M}_\omega$ i $\mathfrak{M}_\omega$ također model za T. Sada napokon iskoristimo da je T zatvorena na homomorfizme:

$\mathfrak{N}_\omega$ je homomorfna slika od $\mathfrak{M}_\omega$ (po homomorfizmu f_ω), te je i $\mathfrak{N}_\omega$ model za T. I natrag, jer je $\mathfrak{N}_0 \prec \mathfrak{N}_\omega$, dobivamo da je $\mathfrak{N}_0$ model za T, što smo i trebali dokazati. □

Sada upravo dokazanu propoziciju iskoristimo za dokazivanje da je teorija T ekvivalentna nekoj pozitivnoj teoriji. Neka je $\mathfrak{M}_0$ kanonski model za teoriju T (tada za svaku σ-rečenicu F vrijedi: $T \models F$ ako i samo ako $\mathfrak{M}_0 \models F$). Po uzoru na prije provedene dokaze drugih teorema o očuvanju, logičan izbor za ekvivalentnu pozitivnu teoriju je:

$$T' := \{F \,:\, F \text{ je pozitivna } \sigma\text{-rečenica, } \mathfrak{M}_0 \models F\}$$

Očito $T \models T'$ ($\mathfrak{M}_0$ je kanonski model za T). Dokažimo suprotni smjer. U tu svrhu neka je $\mathfrak{N}_0$ proizvoljni model za T'. Po definiciji skupa T' svaka pozitivna σ–rečenica koja vrijedi u $\mathfrak{M}_0$, vrijedi i u $\mathfrak{N}_0$. To znači da vrijedi $\mathfrak{M}_0 \equiv_p \mathfrak{N}_0$, te budući da je $\mathfrak{M}_0$ model za T, imamo iz propozicije 1.132. da je i $\mathfrak{N}_0$ model za T. □

Elementarna Hornova formula H je formula oblika $H_1 \vee \ldots \vee H_n$, gdje je najviše jedna formula H_i atomarna, a ostale formule H_i su negacije atomarnih.

Napomena 1.133. *Ako je $n = 1$ tada je elementarna Hornova formula H neka atomarna formula ili negacija atomarne formule. Ako je $n > 1$, te je upravo formula H_n atomarna, a za svaki $i \in \{1, \ldots, n-1\}$ imamo $H_i \equiv \neg G_i$, gdje su $G_1, \ldots, G_{n-1}$ atomarne formule, tada imamo:*

$$\begin{aligned} H \equiv\ & \neg G_1 \vee \ldots \vee G_{n-1} \vee H_n \\ \Leftrightarrow\ & \neg(G_1 \wedge \ldots \wedge G_{n-1}) \vee H_n \\ \Leftrightarrow\ & (G_1 \wedge \ldots \wedge G_{n-1}) \rightarrow H_n \end{aligned}$$

Ako je $n > 1$, te niti jedna formula H_i nije atomarna, tj. za svaki $i \in \{1, \ldots, n\}$ imamo $H_i \equiv \neg G_i$, gdje su $G_1, \ldots, G_n$ atomarne formule, tada vrijedi:

$$\begin{aligned} H \equiv\ & \neg G_1 \vee \ldots \vee G_n \\ \Leftrightarrow\ & \neg(G_1 \wedge \ldots \wedge G_n) \vee \bot \\ \Leftrightarrow\ & (G_1 \wedge \ldots \wedge G_n) \rightarrow \bot \end{aligned}$$

Za formulu kažemo da je **Hornova formula** ako je dobivena iz nekih elementarnih Hornovih formula samo pomoću veznika $\wedge$ i kvantifikatora $\forall$ i $\exists$.

Napomena 1.134. *Primjenom teorema o preneksnoj normalnoj formi slijedi da za svaku Hornovu formulu H postoje elementarne Hornove formule $F_1, \ldots, F_n$ tako da vrijedi $H \equiv Q_1 x_1 \ldots Q_m x_m \ (F_1 \ \wedge \ \ldots \ \wedge \ F_n)$, gdje su $Q_i \in \{\forall, \exists\}$.*

Teorija grupa i teorija prstena mogu biti aksiomatizirane samo sa skupom Hornovih formula. Teorija polja ne može biti aksiomatizirana s Hornovim formulama. Aksiom $\forall x \exists y (x \neq 0 \to x \cdot y = 1)$ nije ekvivalentan niti jednoj Hornovoj formuli.

Neka je $I \neq \emptyset$ i F proizvoljan filtar nad I. Neka je $\{\mathfrak{M}_i : i \in\}$ neka familija σ–struktura. Na Kartezijovom produktu $\prod_{i \in I} |\mathfrak{M}_i|$ definiramo relaciju $\sim_F$ sa:

$$f \sim_F g \qquad \text{ako i samo ako} \qquad \{i : f(i) = g(i)\} \in F$$

Lako je provjeriti da je relacija $\sim_F$ relacija ekvivalencije. Za $f \in \prod_{i \in I} |\mathfrak{M}_i|$ pripadnu klasu ekvivalencije označavamo sa $\overline{f}$. Na skupu $\prod_{i \in I} |\mathfrak{M}_i| / \sim_F$ definiramo interpretacije nelogičkih simbola iz σ na isti način kao kod definicije ultraprodukta struktura. Na primjer za k–mjesni relacijski simbol R definiramo interpretaciju $R^{\mathfrak{M}}$ sa:

$$(\overline{f_1}, \ldots, \overline{f_k}) \in R^{\mathfrak{M}} \qquad \text{ako i samo ako} \qquad \{i : (f_1(i), \ldots, f_k(i)) \in R^{\mathfrak{M}_i}\} \in F$$

Tako definiranu σ–strukturu $\mathfrak{M}$ nazivamo **reducirani produkt** familije σ–struktura $\{\mathfrak{M}_i : i \in I\}$, te ga označavamo sa $\prod_{i \in I} \mathfrak{M}_i / F$.

Za formulu φ kažemo da je to **formula očuvana za reducirane produkte** ako za svaku familiju $\{\mathfrak{M}_i : i \in I\}$ σ–struktura i svaki filtar F nad skupom I vrijedi:

$$\text{ako} \quad \{i : \mathfrak{M}_i \models \varphi\} \in F \qquad \text{tada} \qquad \prod_{i \in I} \mathfrak{M}_i / F \models \varphi$$

Propozicija 1.135. *Hornove formule su očuvane za reducirane produkte.*

Dokaz se provodi indukcijom po broju koraka koji su potrebni za izgradnju Hornove formule.

Univerzalna Hornova formula je formula oblika $\forall x_1 \ldots \forall x_n (H_1 \wedge \ldots \wedge H_n)$, gdje su H_i elementarne Hornove formule.

Propozicija 1.136. *Neka je F neka zatvorena formula. Ekvivalentno je:*

a) formula F je ekvivalentna nekoj univerzalnoj Hornovoj formuli;

b) formula F je očuvana za reducirane produkte i podmodele;

c) formula F je očuvana za konačne produkte i podmodele.

1.12 Tipovi

Tipovi su jedan od centralnih pojmova teorije modela. Mi ćemo uvesti osnovne pojmove u vezi tipova. Glavni cilj nam je dokazati teorem o omašivanju tipova, te dati primjenu tipova na $\aleph_0$–kategorične teorije. U čitavom ovom poglavlju T označava proizvoljnu, ali fiksiranu, potpunu σ–teoriju.

Definicija 1.137. *Neka je $n \in \mathbb{N}$ proizvoljan. Svaki skup S nekih σ–formula koji je zatvoren za konjunkciju, te je skup svih slobodnih varijabli koje nastupaju u formulama od S podskup od $\{x_1, \ldots, x_n\}$, nazivamo n–***tip** teorije T.*

Umjesto "n–tip teorije T" govorit ćemo najčešće samo "n–tip", odnosno "tip", kada neće biti nužno isticati teoriju, odnosno n.

Definicija 1.138. *Neka je S neki n–tip, $\mathfrak{M}$ neki model za teoriju T i $a_1, \ldots, a_n$ neki elementi od $\mid \mathfrak{M} \mid$. Kažemo da* **niz** $a_1, \ldots, a_n$ **realizira tip** *S ako za svaku formulu $F \in S$ vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$. Kažemo da* **model** $\mathfrak{M}$ *teorije T* **realizira tip** *S ako postoji niz u $\mathfrak{M}$ koji realizira S. Ako neki model $\mathfrak{M}$ teorije T ne realizira tip S tada kažemo da* **model** $\mathfrak{M}$ **omašuje tip**.

Napomena 1.139. *Neka je S neki tip, te neka su $\mathfrak{M}$ i $\mathfrak{N}$ dva modela teorije T. Tada vrijedi:*

a) ako $\mathfrak{M} \prec \mathfrak{N}$, te je $a_1, \ldots, a_n$ niz iz $\mathfrak{M}$ koji realizira tip S, tada taj isti niz realizira tip S u strukturi $\mathfrak{N}$

b) ako $\mathfrak{M} \simeq \mathfrak{N}$ i model $\mathfrak{M}$ realizira tip S, tada i model $\mathfrak{N}$ realizira tip S.

Definicija 1.140. *Za tip kažemo da je* **konzistentan tip** *ako postoji model $\mathfrak{M}$ za teoriju T koji ga realizira.*

U sljedećeoj lemi dajemo karakterizaciju konzistentnih tipova.

Lema 1.141. *Neka je T neka potpuna σ–teorija, te neka je S neki n–tip. Ekvivalentno je:*

a) postoji prebrojiv model $\mathfrak{M}$ za teoriju T koji realizira tip S

b) postoji neki model za teoriju T koji realizira tip S

c) za svaku formulu $F \in S$ vrijedi $T \models \exists x_1 \ldots \exists x_n F$

Dokaz. Implikacija a) $\Rightarrow$ b) je očita. Dokazujemo b) $\Rightarrow$ c). Neka je $\mathfrak{M}$ model za teoriju T i $a_1, \ldots, a_n$ niz u $\mathfrak{M}$ tako da za svaki $F \in S$ vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$. Neka je $\mathfrak{N}$ proizvoljan model za teoriju T i $F \in S$ proizvoljna formula. Pošto $\mathfrak{M} \models F[a_1, \ldots, a_n]$ tada očito $\mathfrak{M} \models \exists x_1 \ldots x_n F$ Pošto je po pretpostavci T potpuna teorija tada vrijedi $\mathfrak{M} \equiv \mathfrak{N}$, pa imamo $\mathfrak{N} \models \exists x_1 \ldots x_n F$.
Dokažimo sada c) $\Rightarrow$ a). Pretpostavimo da vrijedi tvrdnja c). Neka je $\sigma' = \sigma \cup \{c_1, \ldots, c_n\}$, gdje su $c_1, \ldots, c_n$ novi konstantski simboli (međusobno različiti). Neka je $T' = T \cup \{F(c_1, \ldots, c_n) : F \in S\}$. Tvrdimo da je teorija T' konzistentna. Pretpostavimo suprotno. Iz **teorema kompaktnosti** slijedi da postoji konačan podskup S' od S tako da je teorija $T \cup \{F(c_1, \ldots, c_n) : F \in S'\}$ inkonzistentna. Neka je sa G označena konjunkcija formula iz skupa S'. Iz definicije tipa znamo da je skup S zatvoren za konjunkciju, pa vrijedi $G \in S$. Iz inkonzistentnosti teorije $T \cup \{F(c_1, \ldots, c_n) : F \in S'\}$ očito slijedi $T \models \neg G(c_1, \ldots, c_n)$. Pošto $c_1, \ldots, c_n \notin \sigma$ tada imamo $T \models \neg \exists x_1 \ldots \exists x_n G(x_1, \ldots, x_n)$. Time je dobivena kontradikcija, jer smo bili pretpostavili da vrijedi tvrdnja c) iz leme. Pošto je teorija T' konzistentna, tada iz Löwenheim–Skolemovog teorema "na dolje" slijedi da za teoriju T' postoji prebrojiv model $\mathfrak{M}'$. Za svaki $i \in \{1, \ldots, n\}$ označimo $a_i = c_i^{\mathfrak{M}'}$. Označimo sa $\mathfrak{M}$ σ–redukciju modela $\mathfrak{M}'$. Očito je $\mathfrak{M}$ prebrojiv model teorije T čiji niz $a_1, \ldots, a_n$ realizira tip S. □

Lema 1.142. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Ekvivalentno je:*

(i) $\mathfrak{M} \equiv \mathfrak{N}$

(ii) postoji σ–struktura $\mathfrak{A}$ tako da vrijedi $\mathfrak{M} \prec \mathfrak{A}$ i $\mathfrak{N} \prec \mathfrak{A}$.

Dokaz. Implikacija b) $\Rightarrow$ a) lako slijedi iz činjenice da općenito $\mathfrak{K} \prec \mathfrak{L}$ povlači $\mathfrak{K} \equiv \mathfrak{L}$.
Dokažimo obrat. Pretpostavimo da vrijedi $\mathfrak{M} \equiv \mathfrak{N}$. Bez smanjenja općenitosti možemo pretpostaviti da su strukture $\mathfrak{M}$ i $\mathfrak{N}$ disjunktne (inače uzmemo neke njihove disjunktne izomorfne kopije). Dokazujemo da je teorija $T' = \mathcal{D}(\mathfrak{M}) \cup \mathcal{D}(\mathfrak{N})$ konzistentna. Pretpostavimo suprotno, tj. da je teorija T' inkonzistentna. Iz **teorema kompaktnosti** slijedi da postoji konačni $S_1 \subseteq \mathcal{D}(\mathfrak{M})$ tako da je skup $S_1 \cup \mathcal{D}(\mathfrak{N})$ inkonzistentan. Označimo sa $F(x_1, \ldots, x_n)$ onu σ–formulu koja ima svojstvo da je $F(\overline{a_1}, \ldots, \overline{a_n})$ konjunkcija svih formula iz S_1. Pošto je očito svaki potpuni dijagram zatvoren za konjunkciju, tada imamo $F(\overline{a_1}, \ldots, \overline{a_n}) \in \mathcal{D}(\mathfrak{M})$. Iz inkonzistentnosti skupa formula $S_1 \cup \mathcal{D}(\mathfrak{N})$ lako slijedi da vrijedi $\mathcal{D}(\mathfrak{N}) \models \neg F(\overline{a_1}, \ldots, \overline{a_n})$. Pošto konstantski simboli $\overline{a_1}, \ldots, \overline{a_n}$ ne nastupaju niti u jednoj formuli iz $\mathcal{D}(\mathfrak{N})$ tada iz posljednjeg očito slijedi

$$\mathcal{D}(\mathfrak{N}) \models \forall x_1 \ldots \forall x_n \neg F(x_1, \ldots, x_n)$$

No, $\forall x_1 \ldots \forall x_n \neg F(x_1, \ldots, x_n)$ je σ–formula, pa imamo i

$$\mathfrak{N} \models \forall x_1 \ldots \forall x_n \neg F(x_1, \ldots, x_n)$$

Iz pretpostavke $\mathfrak{M} \equiv \mathfrak{N}$ tada slijedi i $\mathfrak{M} \models \forall x_1 \ldots \forall x_n \neg F(x_1, \ldots, x_n)$. Time je dobivena kontradikcija s $\mathfrak{M} \models F[a_1, \ldots, a_n]$ (jer je $F(\overline{a_1}, \ldots, \overline{a_n}) \in \mathcal{D}(\mathfrak{M})$). Time smo dokazali da je teorija T' konzistentna. Iz leme o dijagramu slijedi da postoji σ–struktura $\mathfrak{A}$ tako da vrijedi $\mathfrak{M} \prec \mathfrak{A}$ i $\mathfrak{N} \prec \mathfrak{A}$. □

Lema 1.143. *Neka je T potpuna σ–teorija, $\mathfrak{M}$ model za T i S neki konzistentan tip. Tada postoji σ–struktura $\mathfrak{A}$ tako da vrijedi $\mathfrak{M} \prec \mathfrak{A}$ i model $\mathfrak{A}$ realizira tip S.*

Dokaz. Neka je $\mathfrak{N}$ model za teoriju T koji realizira tip S. Pošto je po pretpostavci leme T potpuna teorija tada vrijedi $\mathfrak{M} \equiv \mathfrak{N}$. Iz leme 1.142. slijedi da postoji struktura $\mathfrak{A}$ tako da vrijedi $\mathfrak{M} \prec \mathfrak{A}$ i $\mathfrak{N} \prec \mathfrak{A}$. Pošto struktura $\mathfrak{N}$ realizira tip S tada i strukutra $\mathfrak{A}$ realizira tip S. □

Definicija 1.144. *Neka je S neki n–tip i $G(x_1, \ldots, x_n)$ neka σ–formula. Kažemo da formula G* **izolira** *tip S ako vrijedi:*

a) $T \models \exists x_1 \ldots x_n G$

b) za svaku formulu $F \in S$ *vrijedi* $T \models \forall x_1 \ldots \forall x_n (G \to F)$

Za tip S kažemo da je **izolirani tip** *ako postoji formula koja ga izolira.*

Propozicija 1.145. *Ako je S izolirani tip tada svaki model teorije T realizira tip S. Svaki izolirani tip je konzistentan.*

Dokaz. Neka je $G(x_1, \ldots, x_n)$ formula koja izolira tip S. Neka je $\mathfrak{M}$ neki model za teoriju T. Pošto po pretpostavci vrijedi $T \models \exists x_1 \ldots x_n G$, tada postoje $a_1, \ldots, a_n$ iz $\mid \mathfrak{M} \mid$ tako da vrijedi $\mathfrak{M} \models G[a_1, \ldots, a_n]$. Pošto $T \models \forall x_1 \ldots \forall x_n (G \to F)$, za svaku formulu $F \in S$, tada posebno $\mathfrak{M} \models F[a_1, \ldots, a_n]$. □

Osnovni teorem o tipovima je obrat prethodne napomene. Iskazujemo ga u formi obrata po kontrapoziciji.

Teorem 1.146. (Teorem o omašivanju tipova)
Neka je T potpuna σ–teorija. Ako je S tip koji nije izoliran tada postoji prebrojivi model teorije T koji omašuje tip S.

Dokaz. Traženi prebrojivi model teorije T ćemo konstruirati primjenjujući **Henkinovu metodu** koju smo koristili na početku ovog kolegija za dokaz teorema kompaktnosti, odnosno na dodiplomskom studiju za dokaz generaliziranog teorema potpunosti za teorije prvog reda. Neka je $C = \{c_i : i \in \mathbb{N}\}$ prebrojiv skup novih, međusobno različitih, konstantskih simbola. Neka je $\sigma' = \sigma \cup C$. Konstruirat ćemo σ'–teoriju T' koja će imati sljedeća svojstva:

(1) $T \subseteq T'$

(2) T' je potpuna σ'–teorija

(3) T' je **Henkinova teorija**, tj. ako je $F(x)$ neka σ'–formula, tada postoji $i \in \mathbb{N}$ tako da $\exists x F(x) \to F(c_i/x) \in T'$

(4) za svaki $n \in \mathbb{N} \setminus \{0\}$ i sve $d_1, \ldots, d_n \in C$ postoji formula $F(x_1, \ldots, x_n) \in S$ tako da vrijedi $\neg F(d_1, \ldots, d_n) \in T'$

Pretpostavimo, za tren, da smo uspjeli konstruirati teoriju T' koja ima svojstva (1)–(4). Tada na skupu C novih konstantskih simbola definiramo binarnu relaciju R ovako:

$$R(c_i, c_j) \qquad \text{ako i samo ako} \qquad T' \models c_i = c_j$$

Lako je provjeriti da je R relacija ekvivalencije (prepostavljamo da svaka teorija sadrži aksiome jednakosti!) Za $c \in C$ sa $\overline{c}$ ćemo označavati pripadnu klasu ekvivalencije. Lako je sada definirati σ'–strukturu $\mathfrak{M}'$ čiji je nosač C/R, te tako da za sve $d_1, \ldots, d_n \in C$ i svaku σ–formulu $F(x_1, \ldots, x_n)$ vrijedi:

$$\mathfrak{M}' \models F[\overline{d_1}, \ldots, \overline{d_n}] \qquad \text{ako i samo ako} \qquad F(d_1, \ldots, d_n) \in T'$$

(Prvo bi se definirala interpretacija relacijskih simbola kako je gore zapisano, a onda bi trebalo indukcijom po složenosti formule dokazati da tvrdnja vrijedi za sve formule. Prilikom definicije interpretacije trebalo bi dokazati i neovisnost o izboru reprezentanata.)

Označimo sa $\mathfrak{M}$ σ–redukciju strukture $\mathfrak{M}'$. Tvrdimo da strukutra $\mathfrak{M}$ omašuje tip S. Neka su $d_1, \ldots, d_n \in C$ proizvoljni. Iz uvjeta (4) na teoriju T' slijedi da postoji formula $F(x_1, \ldots, x_n) \in S$ tako da je $\neg F(d_1, \ldots, d_n) \in T'$. Iz svojstva stukture $\mathfrak{M}'$ imamo $\mathfrak{M}' \models \neg F[\overline{d_1}, \ldots, \overline{d_n}]$. To znači da niti jedan niz iz C/R ne realizira tip S. (Primijetimo još samo da je $\mathfrak{M}$ model za teoriju T, jer po (1) imamo $T \subseteq T'$, te po osnovnom svojstvu strukture $\mathfrak{M}'$ imamo da je $\mathfrak{M}'$ model za teoriju T'.)

Preostaje konstruirati teoriju T'. Neka je $(F_i : i \in \mathbb{N})$ niz koji sadrži sve zatvorene σ'–formula. Neka je $(G_i(x) : i \in \mathbb{N})$ niz svih σ'–formula s jednom slobodnom varijablom. Neka je $(\gamma_i : i \in \mathbb{N})$ niz svih uređenih n–torki skupa C (pošto je S jedan n–tip, tada ovdje promatramo baš n–torke). Indukcijom ćemo definirati niz teorija $(T_k : k \in \mathbb{N})$ koji ima sljedeća svojstva:

(a) $T_k = T \cup$ neki konačan skup σ'–rečenica

(b) T_k je konzistentna teorija za svaki $k \in \mathbb{N}$

(c) $T_k \subseteq T_m$, za sve $k \leq m$

Nakon toga ćemo definirati $T' = \cup T_k$. Primjenom uvjeta (b) i (c), te **teorema kompaktnosti** na standradni način lako slijedi da je T' konzistetna teorija.

Sada indukcijom definiramo niz teorija (T_k). Neka je $T_0 = T$. Neka je $k \in \mathbb{N}$ takav da je za svaki $m \leq k$ teorija T_m definirana. Prilikom definicije teorije T_{k+1} razlikujemo tri slučaja:

$k = 3i$

$$T_{k+1} = \begin{cases} T_k \cup \{F_i\}, & \text{ako je teorija } T_k \cup \{F_i\} \text{ konzistentna} \\ T_k \cup \{\neg F_i\}, & \text{inače} \end{cases}$$

(Uočite da ovime postižemo da je teorija $\cup T_k$ potpuna).

$k = 3i + 1$

Neka je $j \in \mathbb{N}$ takav da c_j ne nastupa niti u jednoj formuli teorije T_k, a ni u formuli G_i. Tada definiramo:
$T_{k+1} = T_k \cup \{\exists x G_i(x) \to G_i(c_j)\}$

(Time postižemo da je teorija $\cup T_k$ Henkinova teorija.)

Slučaj $k = 3i + 2$ je nešto kompliciraniji. Ovdje želimo da teorija $\cup T_k$ ispunjava uvjet (4) koji smo prije naveli. Neka su $d_1, \ldots, d_n \in C$ takvi da je $\gamma_i = (d_1, \ldots, d_n)$. Iz pretpostavke indukcije znamo da postoji neka zatvorena σ'–formula H tako da je teorija T_k ekvivalentna s teorijom $T \cup \{H\}$. Neka je D neka σ–formula, te $e_1, \ldots, e_m \in C$ tako da vrijedi $H \equiv D(d_1, \ldots, d_n, e_1, \ldots, e_m)$. Neka je $E \equiv \exists x_{n+1} \ldots \exists x_{n+m} D$. Pošto je $\exists x_1 \ldots \exists x_n E$ jedna σ–rečenica, te je po pretpostavci teorema T potpuna teorija, tada vrijedi $T \models \exists x_1 \ldots \exists x_n E$. Po pretpostavci teorema S je n–tip koji nije izoliran. Tada posebno za formulu E

postoji formula $F(x_1, \ldots, x_n) \in S$ tako da vrijedi $T \not\models \forall x_1 \ldots \forall x_n(E \to F)$. Iz ovog posljednjeg slijedi da je teorija $T \cup \{\neg\forall x_1 \ldots \forall x_n(E \to F)\}$ konzistentna. Tada je i teorija $T \cup \{\exists x_1 \ldots \exists x_n(\exists x_{n+1} \ldots \exists x_{n+m} D \wedge \neg F)\}$ konzistentna, odnosno, teorija $T \cup \{\exists x_1 \ldots \exists x_n \exists x_{n+1} \ldots \exists x_{n+m}(D \wedge \neg F)\}$ je konzistentna. Pošto konstantski simboli iz skupa C ne nastupaju u toj teoriji, tada slijedi da je konzistentna i teorija $T \cup \{D(d_1, \ldots, d_n, e_1, \ldots, e_m) \wedge \neg F(d_1, \ldots, d_n)\}$. Iz toga slijedi da možemo definirati $T_{k+1} = T \cup \{\neg F(d_1, \ldots, d_n)\}$. □

1.12.1 $\aleph_0$–kategorične teorije

Prisjetimo se prvo definicije $\aleph_0$–kategorične teorije. Za teoriju T kažemo da je $\aleph_0$–kategorična ako ima barem jedan model kardinalnosti $\aleph_0$, te su svi njeni modeli kardinalnosti $\aleph_0$ međusobno izomorfni.

Korolar 1.147. *Neka je T potpuna $\aleph_0$–kategorična teorija. Svaki konzistentan tip je izoliran.*

Dokaz. Pretpostavimo da postoji konzistentan tip S koji nije izoliran. Iz definicije konzistentnog tipa slijedi da postoji prebrojivi model $\mathfrak{M}$ za teoriju T koji realizira tip S. Iz teorema o omašivanju tipova slijedi da za neizolirani tip S postoji prebrojivi model $\mathfrak{N}$ za T koji omašuje tip S. Pošto su $\mathfrak{M}$ i $\mathfrak{N}$ prebrojivi modeli od T tada mora vrijediti $\mathfrak{M} \simeq \mathfrak{N}$. No, to je u kontradikciji s činjenicom da jedan model realizira S, a drugi ga omašuje. □

Definicija 1.148. *Za n–tip S kažemo da je* **potpuni tip** *ako je konzistentan, te za svaku σ–formulu vrijedi: $F \in S$ ili $\neg F \in S$. Skup svih potpunih n–tipova označavamo sa S_n.*

Napomena 1.149. *Ako su S_1 i S_2 potpuni n–tipovi, te je $S_1 \subseteq S_2$, tada vrijedi $S_1 = S_2$. Ako je $\mathfrak{M}$ neki model potpune teorije, i $\vec{a} \in |\mathfrak{M}|^n$, tada je*

$$t(\vec{a}/\mathfrak{M}) = \{F(x_1, \ldots, x_n) : \mathfrak{M} \models F[\vec{a}]\}$$

primjer jednog potpunog tipa. Svaki potpuni tip je oblika $t(\vec{a}/\mathfrak{M})$ za neki model $\mathfrak{M}$ i neki $\vec{a} \in |\mathfrak{M}|^n$.

Propozicija 1.150. *Ako formula $F(x_1, \ldots, x_n)$ izolira potpuni tip S tada vrijedi $F \in S$.*

Dokaz. Pošto F izolira tip S tada posebno vrijedi $T \models \exists x_1 \ldots x_n F$. Tada posebno $T \not\models \forall x_1 \ldots \forall x_n(F \to \neg F)$. Pošto F izolira tip S tada po definiciji slijedi $\neg F \notin S$. No, S je potpuni tip, pa je $F \in S$. □

Korolar 1.151. *Neka je T neka potpuna $\aleph_0$–kategorična teorija. Tada je za svaki $n \in \mathbb{N}$ skup S_n svih potpunih n–tipova konačan.*

Dokaz. Neka je $n \in \mathbb{N}$ proizvoljan. Ako je S neki potpuni n–tip tada iz korolara 1.147. slijedi da je S izoliran tip. Neka je $F_S(x_1, \ldots, x_n)$ neka formula koja izolira tip S. Iz propozicije 1.150. slijedi $F_s \in S$. Ako su S_1 i S_2 dva različita potpuna n–tipa lako je vidjeti da je tada $\neg F_{S_1} \in S_2$. Pretpostavimo da postoji $n \in \mathbb{N}$ takav da je skup S_n beskonačan. Jeziku teorije T dodajmo skup novih konstantskih simbola $\{c_1, \ldots, c_n\}$. Neka je $T' = T \cup \{\neg F_S : S \in S_n\}$. Tvrdimo da je teorija T' konzistentna. Neka je X proizvoljan konačan podskup od S_n. Dokazujemo da je teorija $T_X = T \cup \{\neg F_S : S \in X\}$ konzistentna. Neka je $S_0 \subseteq S_n \setminus X$ proizvoljan. Iz napomene 1.149. slijedi da postoji model $\mathfrak{M}$ za teoriju T i $\vec{a} \in |\mathfrak{M}|^n$ tako da vrijedi $S_0 = t(\vec{a}/\mathfrak{M})$. Na početku ovog dokaza smo bili dokazali da za svaki $S \in X$ vrijedi $\neg F_S \in S_0$. Iz ovog posljednjeg, i $S_0 = t(\vec{a}/\mathfrak{M})$, slijedi da za svaki $S \in X$ vrijedi $\mathfrak{M} \models \neg F_S[a_1, \ldots, a_n]$. Kako bi dobili model za teoriju T_X dovoljno je svaki konstantski simbol c_i interpretirati sa a_i. Iz **teorema kompaktnosti** slijedi da je teorija T' konzistentna. Neka je $\mathfrak{A}$ neki model za teoriju T'.

Neka su $b_1, \ldots, b_n \in |\mathfrak{A}|$ takvi da vrijedi $\mathfrak{A} \models T'[b_1, \ldots, b_n]$. Posebno imamo da za svaki $S \in S_n$ vrijedi $\mathfrak{A} \models \neg F_S[b_1, \ldots, b_n]$. Tada iz propozicije 1.150. slijedi da potpuni n–tip $t(\vec{a}/\mathfrak{M})$ ne pripada skupu S_n, čime je dobivena kontradikcija. □

U sljedećem teoremu ističemo da vrijedi i obrat korolara 1.147..

Teorem 1.152. *Neka je T neka potpuna teorija, te neka je za svaki $n \in \mathbb{N}$ svaki potpuni n–tip izoliran. Tada je teorija T $\aleph_0$–kategorična.*

Dokaz teorema lako slijedi primjenom sljedeće dvije leme.

Lema 1.153. *Neka je za svaki $n \in \mathbb{N}$ svaki potpuni n–tip izoliran. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli teorije T, te $\vec{a} \in |\mathfrak{M}|^n$ i $\vec{b} \in |\mathfrak{N}|^n$ takvi da je $t(\vec{a}/\mathfrak{M}) = t(\vec{b}/\mathfrak{N})$. Tada za svaki $a \in |\mathfrak{M}|$ postoji $b \in |\mathfrak{N}|$ tako da vrijedi $t(\vec{a}, a/\mathfrak{M}) = t(\vec{b}, b/\mathfrak{N})$.*

Lema 1.154. *Neka je T neka potpuna teorija. Neka je za svaki $n \in \mathbb{N}$ svaki potpuni n-tip izoliran. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dva prebrojiva modela teorije T, te $\vec{a} \in |\mathfrak{M}|^n$ i $\vec{b} \in |\mathfrak{N}|^n$ tako da vrijedi $t(\vec{a}/\mathfrak{M}) = t(\vec{b}/\mathfrak{N})$. Tada postoji izomorfizam $f : \mathfrak{M} \simeq \mathfrak{N}$ tako da za svaki $i \in \{1, \ldots, n\}$ vrijedi $f(a_i) = b_i$.*

Za $n \in \mathbb{N}$ neka je sa $Lind_n$ označena Lindenbaumova algebra nad skupom svih formula čija slobodne varijable pripadaju skupu $\{x_1, \ldots, x_n\}$. U sljedećem teoremu rezimiramo sve veze $\aleph_0$–kategoričnih teorija i potpunih tipova.

Teorem 1.155. *Neka je T potpuna teorija. Sljedeće tvrdnje su ekvivalentne:*

a) teorija T je $\aleph_0$–kategorična

b) za svaki $n \in \mathbb{N}$ svaki konzistentan n–tip je izoliran

c) za svaki $n \in \mathbb{N}$ svaki potpuni n–tip je izoliran

d) za svaki $n \in \mathbb{N}$ skup S_n je konačan

e) za svaki $n \in \mathbb{N}$ skup $Lind_n$ je konačan

1.13 Eliminacija kvantifikatora

Za dokaz potpunosti neke teorije koristili smo sljedeći Łos–Vaughtov test:

> *ako neka teorija T nema konačnih modela, te je λ–kategorična za neki beskonačni kardinalni broj λ, tada je T potpuna teorija.*

Primjenom Łos–Vaughtovog testa bili smo dokazali da su teorija gustih linearnih uređaja bez krajnjih točaka (tj. DLO), te teorija algebarski zatvorenih polja dane karakteristike (tj. ACF_p), potpune teorije. Bili smo već naveli da se Vaughtov test ne može uvijek primijeniti za dokaz potpunosti, jer postoje potpune teorije koje nisu λ–kategorične niti za jedan beskonačni kardinalni broj λ. Metoda eliminacije kvantifikatora često omogućava dokaz potpunosti teorije. Dokazat ćemo da teorija ACF dopušta eliminaciju kvantifikatora, pa ćemo kao posljedicu dobiti Hilbertov Nullstellensatz. Zatim, opisat ćemo kako eliminirati kvantifikatore u teoriji realnih zatvorenih uređenih polja, te kako iz toga dobiti Robinsonovo rješenje Hilbertovog 17. problema.

Definicija 1.156. *Za teoriju T kažemo da dopušta eliminaciju kvantifikatora ako za svaku formulu $F(x_1, \ldots, x_n)$, $n \geq 1$, postoji formula $G(x_1, \ldots, x_n)$ bez kvantifikatora takva da*

$$T \models \forall x_1 \ldots \forall x_n (F(x_1, \ldots, x_n) \leftrightarrow G(x_1, \ldots, x_n)).$$

Sljedećom definicijom i lemama opisujemo pojam egzistencijalne formule koji će nam koristiti u dokazu kriterija kojim teorija dopušta eliminaciju kvantifikatora.

Definicija 1.157. *Za neku σ–formulu kažemo da je* **egzistencijalna formula** *ako je u preneksnoj formi koja sadrži jedino egzistencijalne kvantifikartore u svom prefiksu. Za egzistencijalnu σ—formulu kažemo da je* **primitivna** *ako je oblika $\exists x_1 \ldots \exists x_n G(x_1, \ldots, x_n)$, pri čemu je G elementarna konjukcija, tj. G je konjunkcija atomarnih i negacije atomarnih formula.*

Lema 1.158. *Svaka egzistencijalna formula je logički ekvivalentna disjunkciji primitivnih egzistencijalnih formula.*

Lema 1.159. *Teorija T dopušta eliminaciju kvantifikatora ako i samo ako je svaka primitivna egzistencijalna formula sa samo jednim egzistencijalnim kvantifikatorom ekvivalentna u teoriji T nekoj formuli bez kvantifikatora.*

Dokaz. Pretpostavimo da teorija T dopušta eliminaciju kvantifikatora. To po definiciji znači da za svaku σ–formulu $F(x_1, \ldots, x_n)$ postoji neka σ–formula $G(x_1, \ldots, x_n)$ bez kvantifikatora takva da vrijedi $T \models \forall x_1 \ldots \forall x_n (F \leftrightarrow G)$. Posebno, gornja tvrdnja vrijedi za svaku primitivnu egzistencijalnu formulu koja ima samo jedan egzistencijalan kvatifikator.

Dokažimo obrat. Pretpostavimo da je svaka primitivna egzistencijalna formula sa samo jednim egzistencijalnim kvantifikatorom ekvivalentna u teoriji T nekoj formuli bez kvantifikatora. Iz teorema o preneksnoj normalnoj formi slijedi da za svaku formulu teorije T postoji formula u preneksnoj normalnoj formi koja joj je ekvivalentna. Odavde slijedi da je dovoljno dokazati da je svaka formula teorije T, koja je u preneksnoj normalnoj formi, ekvivalentna nekoj formuli bez kvantifikatora. Ovu tvrdnju dokazujemo indukcijom po broju kvantifikatora formule u preneksnoj normalnoj formi. Neka je F formula u preneksnoj normalnoj formi koja sadrži točno jedan kvantifikator.

1. slučaj: formula F je oblika $\exists x G$, gdje je G otvorena formula.
Tada iz leme 1.158. slijedi da postoje neke primitivne egzistencijalne formule $G_1, \ldots, G_m$ takve da $T \models \exists x G \leftrightarrow (G_1 \vee \ldots \vee G_m)$. Po pretpostavci vrijedi da za svaku formulu G_i postoji otvorena formula F_i takva da vrijedi $T \models G_i \leftrightarrow F_i$, za svaki $i = 1, \ldots, m$. Odavde očito slijedi $T \models (G_1 \vee \ldots \vee G_m) \leftrightarrow (F_1 \vee \ldots \vee F_m)$, odnosno $T \models F \leftrightarrow (F_1 \vee \ldots \vee F_m)$. Formula $F_1 \vee \ldots \vee F_m$ je otvorena, pa je ovaj slučaj dokazan.

2. slučaj: formula F je oblika $\forall x G$, gdje je G otvorena formula.
Po De Morganovim pravilima vrijedi $\models \forall x G \leftrightarrow \neg \exists x \neg G$. Iz upravo razmatranog 1. slučaja slijedi da postoji otvorena formula F takva da vrijedi $T \models \exists x \neg G \leftrightarrow F$. Odavde slijedi $T \models \neg \exists x \neg G \leftrightarrow \neg F$, odnosno $T \models \forall x G \leftrightarrow \neg F$. Formula $\neg F$ je otvorena, pa smo dokazali tvrdnju i za ovaj slučaj.

Pretpostavimo da tvrdnja vrijedi za svaku formulu G u preneksnoj normalnoj formi koja ima n kvantifikatora. Neka je F formula u preneksnoj normalnoj formi čiji prefiks sadrži točno $n + 1$ kvantifikator. Promatramo dva slučaja obzirom na prvi lijevi kvantifikator.

1. slučaj: neka je F oblika $\exists x F'$ gdje je F' formula u preneksnom obliku čiji prefiks sadrži točno n kvantifikatora.
Po pretpostavci indukcije postoji otvorena formula G' takva da $T \models F' \leftrightarrow G'$. Tada očito vrijedi i $T \models \exists x F' \leftrightarrow \exists x G'$. Na isti način kao u bazi indukcije može se pokazati da postoji otvorena formula G takva da $T \models G \leftrightarrow \exists x G'$, odnosno $T \models F \leftrightarrow G$.

2. slučaj: neka je F oblika $\forall x F'$, gdje je F' formula u preneksnom obliku čiji prefiks sadrži točno n kvantifikatora.
Iz pretpostavke indukcije slijedi da postoji otvorena formula G' takva da vrijedi $T \models F' \leftrightarrow G'$. Tada očito vrijedi i $T \models \forall x F' \leftrightarrow \forall x G'$. Analogno kao u bazi indukcije možemo pokazati da postoji neka otvorena formula G takva da vrijedi $T \models G \leftrightarrow \forall x G'$. □

Sljedeći teorem daje jedan kriterij za eliminaciju kvantifikatora.

Teorem 1.160. *Neka je T neka σ–teorija i F proizvoljna σ–formula. Sljedeće tvrdnje su ekvivalentne:*

a) Formula F je ekvivalentna u teoriji T nekoj formuli bez kvantifikatora

b) Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za teoriju T, $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{N}_0 \subseteq \mathfrak{N}$, te neka je $f : \mathfrak{M}_0 \simeq \mathfrak{N}_0$. Tada za sve $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ vrijedi da $\mathfrak{M} \models F[a_1, \ldots, a_n]$ povlači $\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$.

Dokaz. Pretpostavimo prvo da vrijedi tvrdnja a). Tada postoji formula G bez kvantifikatora tako da vrijedi $T \models \forall x_1 \ldots \forall x_n (F \leftrightarrow G)$. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za teoriju T, $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{N}_0 \subseteq \mathfrak{N}$, te neka je $f : \mathfrak{M}_0 \simeq \mathfrak{N}_0$. Neka su $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ tako da vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$. Tada vrijedi i $\mathfrak{M} \models G[a_1, \ldots, a_n]$. Pošto je G formula bez kvantifikatora, te $\mathfrak{M}_0 \subseteq \mathfrak{M}$, tada vrijedi i $\mathfrak{M}_0 \models G[a_1, \ldots, a_n]$. Pošto $f : \mathfrak{M}_0 \simeq \mathfrak{N}_0$ tada $\mathfrak{N}_0 \models G[f(a_1), \ldots, f(a_n)]$. Sada iz $\mathfrak{N}_0 \subseteq \mathfrak{N}$ slijedi $\mathfrak{N} \models G[f(a_1), \ldots, f(a_n)]$. Pošto je $\mathfrak{N}$ model teorije T, te vrijedi $T \models \forall x_1 \ldots \forall x_n (F \leftrightarrow G)$, tada iz tog i posljednjeg slijedi konačno $\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$.

Dokaz obrata je deleko kompliciraniji. Ovdje ćemo navesti samo glavne crte dokaza. Prvo se dokaže sljedeća pomoćna tvrdnja $(*)$:

Neka je T neka σ–teorija koja je zatvorena za relaciju logičke posljedice, te neka je $\varphi(x_1, \ldots, x_m)$ neka σ–formula. Neka je S neki skup σ–formula koji je zatvoren za disjunkciju, i čije slobodne varijable pripadaju skupu $\{x_1, \ldots, x_m\}$. Ekvivalentno je:

(1) $T \models \forall x_1 \ldots \forall x_m \varphi$ ili $T \models \forall x_1 \ldots \forall x_m \neg\varphi$ ili postoje formule $\varphi_1, \ldots, \varphi_k \in S$ tako da vrijedi $T \models \forall x_1 \ldots \forall x_m (\varphi \leftrightarrow \varphi_1 \wedge \ldots \wedge \varphi_k)$

(2) Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli teorije T, $a_1, \ldots, a_m \in |\mathfrak{M}|$, $b_1, \ldots, b_m \in |\mathfrak{N}|$, te neka $\mathfrak{M} \models \varphi[a_1, \ldots, a_m]$. Zatim, neka za svaku formulu $F \in S$ vrijedi da ako $\mathfrak{M} \models F[a_1, \ldots, a_m]$ tada $\mathfrak{N} \models F[b_1, \ldots, b_m]$. Tada imamo da vrijedi $\mathfrak{N} \models \varphi[b_1, \ldots, b_m]$.

Zatim se dokaže da iz tvrdnje b) teorema slijedi tvrdnja (2) prethodne pomoćne tvrdnje. Za taj dokaz je ključno sljedeće poopćenje leme o dijagramu:

Neka je $\mathfrak{M}$ neka σ–struktura i $X \subseteq |\mathfrak{M}|$. Označimo:

$$\Delta_X(\mathfrak{M}) = \{F : \begin{array}{l} F \text{ je otvorena } \sigma \cup \{\overline{a} : a \in X\}\text{–formula} \\ \text{takva da } (\mathfrak{M}, a)_{a\in X} \models F\} \end{array}$$

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ–strukture i $X \subseteq |\mathfrak{M}|$ skup generatora za strukturu $\mathfrak{M}$. Tada vrijedi:

strukutru $\mathfrak{M}$ možemo smjestiti u strukturu $\mathfrak{N}$ ako i samo ako postoji ekspanzija strukture $\mathfrak{N}$ koja je model za skup formulu $\Delta_X(\mathfrak{M})$.

Iz pomoćne tvrdnje $(*)$ slijedi da vrijedi (1). Promotrimo posebno svaki od tri slučaja koji su navedeni u (1).

Ako vrijedi $T \models \forall x_1 \ldots \forall x_n F$ tada npr. za otvorenu formulu $G \equiv x_1 = x_2$ vrijedi $T \models \forall x_1 \ldots \forall x_n (F \leftrightarrow G)$.

Ako vrijedi $T \models \forall x_1 \ldots \forall x_n \neg F$ tada npr. za otvorenu formulu $G \equiv \neg(x_1 = x_2)$ vrijedi $T \models \forall x_1 \ldots \forall x_n (F \leftrightarrow G)$.

Promotrimo još situaciju kada postoje otvorene formule $\varphi_1, \ldots, \varphi_k \in S$ tako da vrijedi $T \models \forall x_1 \ldots \forall x_m (F \leftrightarrow \varphi_1 \wedge \ldots \wedge \varphi_k)$. Tada je očito $G \equiv \varphi_1 \wedge \ldots \wedge \varphi_k$ jedna tražena formula. □

Napomena 1.161. *Uvjet b) iz prethodnog teorema 1.160. ekvivalentan je sa sljedećom tvrdnjom:*

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli teorije T, te $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{M}_0 \subseteq \mathfrak{N}$. Tada za sve $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ takve da $\mathfrak{M} \models F[a_1, \ldots, a_n]$ vrijedi $\mathfrak{N} \models F[a_1, \ldots, a_n]$.

Teorem 1.162. *Neka je T neka σ–teorija. Ekvivalentno je:*

a) teorija T dopušta eliminaciju kvantifikatora

b) Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli teorije T, te $\mathfrak{M}_0 \subseteq \mathfrak{M}$ konačno generirani podmodel. Neka je $f : |\mathfrak{M}_0| \to |\mathfrak{M}|$ smještenje. Tada za svaki $b \in |\mathfrak{M}|$ postoji elementarno proširenje $\mathfrak{N}'$ od $\mathfrak{N}$ i smještenje $f : |\mathfrak{M}'_0| \to |\mathfrak{N}'|$ koja je proširenje funkcije f, a sa $\mathfrak{M}'_0$ je označen podmodel od $\mathfrak{M}$ koji je generiran sa $|\mathfrak{M}_0| \cup \{b\}$.

Definicija 1.163. *Za teoriju T kažemo da je* **modelno potpuna** *ako za svaka dva modela $\mathfrak{M}$ i $\mathfrak{N}$ teorije T, takva da je $\mathfrak{M} \subseteq \mathfrak{N}$, vrijedi $\mathfrak{M} \prec \mathfrak{N}$.*

Teorem 1.164. *Ako teorija T dopušta eliminaciju kvantifikatora tada je ona modelno potpuna.*

Dokaz. Neka $\mathfrak{M}, \mathfrak{N} \models T$ tako da $\mathfrak{M} \subseteq \mathfrak{N}$. Preslikavanje $f : |\mathfrak{M}| \to |\mathfrak{N}|$, definirano sa $f(x) = x$, je injektivni jaki homomorfizam. Treba samo još vidjeti da za svaku formulu φ i sve $a_1, \ldots, a_n \in |\mathfrak{M}|$ vrijedi:

$$\mathfrak{M} \models \varphi[a_1, \ldots, a_n] \qquad \text{ako i samo ako} \qquad \mathfrak{N} \models \varphi[a_1, \ldots, a_n] \qquad (*)$$

Pošto po pretpostavci teorija T dopušta eliminaciju kvantifikatora, tada je prethodnu tvrdnju dovoljno dokazati za otvorene formule. No, znamo da tvrdnja $(*)$ vrijedi za otvorene formule kada se radi o jakom homomorfizmu. □

Napomena 1.165. *Pojam modelno potpune teorije je već definiran prilikom razmatranja teorema o očuvanju na unije lanaca. Dokazano je da je svaka modelno potpuna teorija ekvivalentna nekoj $\forall\exists$–teoriji. Ne postoji direktna veza između potpunih i modelno potpunih teorija. Sljedeće teorije su potpune, ali nisu modelno potpune: teorija gustih lineranih uređaja s rubovima, $Th(\mathbb{N}, Sc)$, $Th(\mathbb{N}, <)$ i $Th(\mathbb{N}, 0, Sc, +, \cdot, <)$. Dokazat ćemo da je teorija ACF modelno potpuna, a bili smo prije primijetili da teorija ACF nije potpuna.*

Definicija 1.166. *Za model $\mathfrak{P}$ teorije T kažemo da je* **osnovni model** *teorije T ako za svaki model $\mathfrak{M}$ od T postoji $\mathfrak{N} \subseteq \mathfrak{M}$ tako da vrijedi $\mathfrak{N} \simeq \mathfrak{P}$.*

Teorem 1.167. *Neka je T modelno potpuna teorija za koju postoji osnovni model. Tada je T potpuna teorija.*

Dokaz. Dokazujemo da su svaka dva modela $\mathfrak{M}$ i $\mathfrak{N}$ od T elementarno ekvivalentni. Neka je $\mathfrak{P}$ osnovni model za teoriju T. Bez smanjena općenitosti možemo pretpostaviti da vrijedi $\mathfrak{P} \subseteq \mathfrak{M}$ i $\mathfrak{P} \subseteq \mathfrak{N}$. Pošto je po pretpostavci teorema teorija T modelno potpuna tada vrijedi $\mathfrak{P} \prec \mathfrak{M}$ i $\mathfrak{P} \prec \mathfrak{N}$. Iz ovog posljednjeg lako slijedi $\mathfrak{M} \equiv \mathfrak{N}$. □

Neka je $\sigma_{DLO} = \{<, =\}$. Aksiomi teorije gustih linearnih uređaja bez krajnjih točaka, kratko DLO (eng. dense linear ordering), su sljedeći:

$(A0)$ aksiomi jednakosti

$(A1)$ $\neg(x < x)$

$(A2)$ $x < y \ \wedge \ y < z \ \rightarrow \ x < z$

$(A3)$ $x < y \ \vee \ x = y \ \vee \ y < x$

$(A4)$ $x < y \ \rightarrow \ \exists z(x < z < y)$

$(A5)$ $\neg\exists x \forall y(x < y \ \vee \ x = y)$

$(A6)$ $\neg\exists x \forall y(y < x \ \vee \ x = y)$

Teorem 1.168. *Teorija DLO dopušta eliminaciju kvantifiaktora.*

Dokaz. Primjena teorema 1.162.

Korolar 1.169. *Teorija DLO je potpuna. Teorija DLO je modelno potpuna. Posebno iz* $\mathbb{Q} \subseteq \mathbb{R}$ *slijedi* $\mathbb{Q} \prec \mathbb{R}$.

Sa ACF označavamo teoriju algebarski zatvorenih polja. Tu teoriju već smo razmatrali prilikom dokaza Axovog teorema.

Teorem 1.170. *Teorija ACF dopušta eliminaciju kvantifikatora.*

Dokaz. Iz leme 1.159. slijedi da je dovoljno dokazati da za svaku primitivnu egzistencijalnu formulu s jednim egzistencijalnim kvantifikatorom postoji otvorena formula koja joj je ekvivalentna u teoriji ACF. Neka je $\psi(\vec{x}, y)$ neka konjunkcija atomarnih i negacije atomarnih formula. Sada koristimo napomenu 1.161., odnosno teorem 1.160.. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ neka algebarski zatvorena polja, te $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{M}_0 \subseteq \mathfrak{N}$. (Uočite da je tada nužno $\mathfrak{M}_0$ polje, ali nije nužno algebarski zatvoreno). Zatim, neka su $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ takvi da vrijedi $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$. Želimo dokazati da postoji $b \in |\mathfrak{N}|$ tako da vrijedi $\mathfrak{N} \models \exists y \psi[a_1, \ldots, a_n, b]$. Uočimo da su termi s jednom slobodnom varijablom jezika $\sigma_{ACF} \cup \{\overline{a_1}, \ldots, \overline{a_n}\}$ zapravo polinomi nad skupom $|\mathfrak{M}_0|$, a atomarne formule su oblika $f(x) = 0$ gdje je f polinom. Pošto je $\psi(y, \overline{a_1}, \ldots, \overline{a_n})$ konjunkcija

atomarnih i negacije atomarnih formula, te sadrži samo jednu slobodnu varijablu, tada postoji polinomi $f_1, \ldots, f_m \in \mathfrak{M}_0[X]$ i $g_1, \ldots, g_k \in \mathfrak{M}_0[X]$, tako da vrijedi

$$\psi(y, \overline{a_1}, \ldots, \overline{a_n}) \equiv \bigwedge_{i=1}^{m} f_i(y) = 0 \wedge \bigwedge_{j=1}^{k} g_j(y) \neq 0$$

Neka je $\mathfrak{A}$ algebarsko zatvorenje polja $\mathfrak{M}_0$. Tada vrijedi $\mathfrak{A} \subseteq \mathfrak{M}$ i $\mathfrak{A} \subseteq \mathfrak{N}$. Sada promatramo dva slučaja:

a) postoji $i_0 \in \{1, \ldots, m\}$ tako da f_{i_0} nije nul–polinom

b) za svaki $i \in \{1, \ldots, m\}$ f_i je nul–polinom

Promotrimo prvo slučaj a). Iz pretpostavke $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$ slijedi da postoji $b \in |\mathfrak{N}|$ tako da vrijedi $\mathfrak{M} \models \psi[a_1, \ldots, a_n, b]$. To znači da vrijedi

$$\mathfrak{M} \models \Big(\bigwedge_{i=1}^{m} f_i(y) = 0 \wedge \bigwedge_{j=1}^{k} g_j(y) \neq 0 \Big)[b]$$

Posebno imamo $f_{i_0}(b) = 0$. Iz definicije polja $\mathfrak{A}$ slijedi $b \in |\mathfrak{A}|$ (pošto je $\mathfrak{A}$ algebarsko zatvorenje polja $\mathfrak{M}_0$ tada $\mathfrak{A}$ sadrži nul–točku svakog polinoma s koeficijentima iz $|\mathfrak{M}_0|$). Iz činjenice $\mathfrak{A} \subseteq \mathfrak{M}$ i pošto je formula ψ otvorena, tada vrijedi i $\mathfrak{A} \models \psi[b]$. Pošto je $\mathfrak{A} \subseteq \mathfrak{N}$ tada je $b \in |\mathfrak{N}|$. Konačno, iz $\mathfrak{A} \models \psi[b]$, $\mathfrak{A} \subseteq \mathfrak{N}$ i činjenice da je ψ otvorena formula, imamo $\mathfrak{N} \models \psi[b]$.

Sada razmatramo slučaj b), tj. slučaj kada su svi polinomi $f_1, \ldots, f_m$ nul–polinomi. Iz pretpostavke $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$ tada slijedi $\mathfrak{M} \models \exists y(\bigwedge g_j(y) \neq 0)$. Iz ovog posljednjeg slijedi da niti za jedan $j \in \{1, \ldots, k\}$ polinom g_j nije nul–polinom. Pošto $g_j \in \mathfrak{M}_0[X]$, za svaki $j \in \{1, \ldots, k\}$, te je $\mathfrak{A}$ algebarski zatvorenje od $\mathfrak{M}_0$, tada postoji konačan $S \subseteq |\mathfrak{A}|$ koji sadrži sve nul–točke svih polinoma g_j. Iz leme 1.65. znamo da je svako algebarski zatvoreno polje beskonačno. Tada postoji $b \in |\mathfrak{A}| \setminus S$. Iz $\mathfrak{A} \subseteq \mathfrak{N}$ slijedi $b \in |\mathfrak{N}|$. Očito vrijedi $\mathfrak{A} \models \Big(\bigwedge g_j(y) \neq 0 \Big)[b]$, tj. $\mathfrak{A} \models \psi[b]$. Pošto $\mathfrak{A} \subseteq \mathfrak{N}$, te je formula $\psi(y)$ je otvorena, $\mathfrak{A} \models \psi[b]$, i $a_1, \ldots, a_n, b \in |\mathfrak{N}|$, tada $\mathfrak{N} \models \psi[a_1, \ldots, a_n, b]$. □

Sada ćemo primjenom modelne potpunusti teorije ACF dati dokaz Hilbertovog Nullstellensatza. Prvo navodimo pojmove i činjenice iz algebre koji su nam potrebni. Neka je R neki prsten i $I \subseteq R$. Kažemo da je I **ideal** ako je $(I, +)$ grupa, te vrijedi $R \cdot I \subseteq I$ i $I \cdot R \subseteq I$. Svaki prsten ima barem dva ideala. To su $\{0\}$ i R. Nazivamo ih **trivijalni ideali**. Sve druge ideale nazivamo **pravi ideali**. U prstenu $\mathbb{Z}$ za svaki $m \in \mathbb{Z}$ je $m\mathbb{Z}$ ideal. Za pravi ideal $I \subseteq R$ kažemo

da je **prosti ideal** ako za svaki $x, y \in R$ vrijedi da $x \notin I$ i $y \notin I$ povlači $x \cdot y \notin I$.

Propozicija 1.171. *Neka je R prsten. Tada vrijedi:*

a) Neka je R komutativan prsten s jedinicom i $(I, +)$ aditivna podgrupa. Tada je I ideal ako i samo ako $I \cdot R = I$.

b) Neka je R prsten s jedinicom. Ideal I je pravi ako i samo ako $1 \notin I$.

c) Pravi ideal I je prosti ideal ako i samo ako R/I je integralna domena.

Za pravi ideal I u prstenu R kažemo da je **maksimalni ideal** ako ne postoji pravi ideal I' u R tako da vrijedi $I \subset I'$. Svaki maksimalni ideal je prosti ideal. Obrat općenito ne vrijedi.

Teorem o maksimalnom idealu
Neka je R prsten i I pravi ideal. Tada postoji maksimalni ideal J koji sadrži ideal I.

Ako je R prsten i $n \in \mathbb{N} \setminus \{0\}$ tada sa $R[X_1, \ldots, X_n]$ označavamo prsten svih polinoma s koeficijenima iz R sa n varijabli.

Neka je R komutativan prsten s jedinicom i $a \in R$ proizvoljan. Označimo $I(a) = \{ax : x \in R\}$. Lako je vidjeti da je za svaki $a \in R$ skup $I(a)$ ideal u prstenu R. Nazivamo ga **glavni ideal generiran s elementom** a. Ako je $\{a_1, \ldots, a_n\} \subseteq R$ tada $I(a_1, \ldots, a_n)$ definiramo kao najmanji ideal u prstenu R koji sadrži skup $\{a_1, \ldots, a_n\}$. Nije teško vidjeti da vrijedi $I(a_1, \ldots, a_n) = \{a_1x_1 + \ldots + a_nx_n \ : \ x_i \in R\}$.

Za ideal I kažemo da je **konačno generirani ideal** ako postoje $a_1, \ldots, a_n \in R$ tako da vrijedi $I = I(a_1, \ldots, a_n)$. Za prsten kažemo da je **Noetherin prsten** ako je svaki ideal u prstenu konačno generiran. Svako polje je Noetherin prsten.

Hilbertov teorem o bazi
Neka je R Noetherin prsten. Tada je $R[X_1, \ldots, X_n]$ također Noetherin prsten.

Primjer 1.172. *Neka su $f_1, \ldots, f_k$ proizvoljni polinomi iz $\mathbb{C}[X_1, \ldots, X_n]$. Koji su nužni i dovoljni uvjeti da ti polinomi imaju zajedničku nul–točku?*

Ako postoje polinomi $g_1, \ldots, g_n \in \mathbb{C}[X_1, \ldots, X_n]$ tako da vrijedi $f_1g_1 + \ldots + f_ng_n = 1$ (tj. ideal $I(f_1, \ldots, f_n)$ je nepravi), tada očito ne postoji zajednička nul–točka.

Hilbertov Nullstellensatz jednostavno govori da vrijedi i obrat.

Teorem 1.173. *(***Hilbertov Nullstellensatz***)*
Neka je F neko algebarski zatvoreno polje, te $I \subseteq F[X_1, \ldots, X_n]$ neki pravi ideal. Tada postoji $\vec{a} \in F^n$ tako da za svaki $f \in I$ vrijedi $f(\vec{a}) = 0$.

Dokaz. Iz teorema o maksimalnom idealu slijedi da postoji maksimalni ideal $J \subseteq F[X_1, \ldots, X_n]$ tako da vrijedi $I \subseteq J$. Tada je $F[X_1, \ldots, X_n]/J$ polje. Neka je K algebarsko zatvorenje polja $F[X_1, \ldots, X_n]/J$. Svaki element $a \in F$ možemo poistovjetiti s klasom $a + J$, pri čemu element a poistovjetimo s konstantnim polinomom $(x_1, \ldots, x_n) \mapsto a$, pa imamo $F \subseteq K$. Iz teorema 1.170. znamo da teorija ACF dopušta eliminaciju kvantifikatora, a onda iz teorema 1.164. slijedi da je teorija ACF modelno potpuna. Pošto su F i K modeli teorije ACF, te vrijedi $F \subseteq K$ tada imamo $F \prec K$. Pošto je svako polje posebno Noetherin prsten tada iz Hilbertovog teorema o bazi slijedi da postoje $g_1, \ldots, g_m \in J$ tako da vrijedi $J = I(g_1, \ldots, g_m)$. Označimo $G \equiv \exists x_1 \ldots \exists x_n \Big(\bigwedge_{i=1}^{m} g_i(x_1, \ldots, x_n) = 0 \Big)$. Pošto za svaki $i \in \{1, \ldots, m\}$ vrijedi $g_i(X_1 + J, \ldots, X_n + J) = g_i + J = 0$, te je K algebarsko zatvorenje polja $F[X_1, \ldots, X_n]/J$, tada imamo $K \models G$. Iz ovog posljednjeg, te $F \prec K$, slijedi $F \models G$. Neka je $\vec{a} \in F^n$ takav da vrijedi $g_1(\vec{a}) = \ldots = g_m(\vec{a}) = 0$. Neka je $f \in I$ proizvoljan polinom. Iz $I \subseteq J$ slijedi $f \in J$. Pošto $J = I(g_1, \ldots, g_m)$ tada postoje $h_1, \ldots, h_m \in F[X_1, \ldots, X_n]$ tako da vrijedi $f = g_1h_1 + \ldots + g_mh_m$. Sada iz ovog posljednjeg i $g_1(\vec{a}) = \ldots = g_m(\vec{a}) = 0$ očito slijedi $f(\vec{a}) = 0$. □

Za racionalnu funkciju $f = g/h$ nad poljem realnih brojeva kažemo da je **pozitivno semidefinitna** ako vrijedi: $(\forall x \in \mathbb{R})(h(x) \neq 0 \to f(x) \geq 0)$.

Hilbertov sedamnaesti problem glasi:

> *Ako je f pozitivno semidefinitna racionalna funkcija nad poljem $\mathbb{R}$ može li se f napisati kao konačna suma kvadrata racionalnih funkcija?*

Prvo rješenje sedamnaestog problema, koje je dao Artin 1927. godine, bilo je sasvim algebarsko, bez logičkih metoda. "Logičko" rješenje ovog problema dao je Robinson 1955., i ono predstavlja jednu od prvih primjena teorije modela u algebri. Ovaj se problem može formulirati i za polinome. Hilbert je 1888. godine dokazao da postoje pozitivno semidefinitni polinomi nad poljem realnih

brojeva koji nisu konačne sume kvadrata polinoma. Taj Hilbertov dokaz nije bio konstruktivan, odnosno Hilbert nije dao neki konkretan primjer polinoma takve vrste. Sada navodimo primjer takvog polinoma kojeg je 1966. godine dao Motzkin. Polinom $p(x,y) = 1 + x^4 \cdot y^2 + x^2 \cdot y^4 - 3x^2 \cdot y^2$ je pozitivno semidefinitan, ali se ne može napisati kao konačan zbroj kvadrata polinoma nad $\mathbb{R}$. Iz AG–nejednakosti (aritmetička sredina je uvijek veća od geometrijske) slijedi:

$$\frac{1 + x^4 \cdot y^2 + x^2 \cdot y^4}{3} \geq \sqrt[3]{1 \cdot (x^4y^2) \cdot (x^2y^4)} = x^2y^2,$$

pa je $p(x,y) \geq 0$, za sve $x, y \in \mathbb{R}$. Dokaz da se polinom p ne može napisati kao suma kvadrata polinoma je nešto složeniji, pa ga ovdje ispuštamo.

Rješenje 17. Hilbertovog problema slijedi iz činjenice da teorija realnih zatvorenih uređenih polja dopušta eliminaciju kvantifikatora. Kako bismo definirali pojam realnog zatvorenog uređenog polja skupu nelogičkih simbola teorije polja dodajemo još i dvomjesni relacijski simbol kojeg ćemo označavati sa $<$, te aksiomima polja dodajemo još i sljedeće aksiome:

Aksiomi teorije linearnih uređaja su:

$$x < y \ \wedge \ y < z \ \rightarrow x < z$$

$$x < y \ \rightarrow \ x \neq y$$

$$x < y \ \vee \ x = y \ \vee \ y < x$$

Aksiomi o kompatiblnosti uređaja i operacija

$$x < y \ \rightarrow \ x + z < y + z$$

$$0 < x \ \wedge \ 0 < y \ \rightarrow \ 0 < xy$$

Polje koje zadovoljava sve navedene aksiome naziva se **uređeno polje**.

Neka je F neko uređeno polje i $f \in F[X]$ proizvoljan polinom. Kažemo da polje F ima **svojstvo srednje vrijednosti** u odnosu na polinom f ako za sve $a, b \in F$, takve da je $a < b$ i $f(a) < 0 < f(b)$, postoji $c \in F$ tako da je $a < c < b$ i $f(c) = 0$. Za uređeno polje F kažemo da je **realno zatvoreno uređeno polje** ako ima svojstvo srednje vrijednosti za svaki polinom $f \in F[X]$.

Polje realnih brojeva je realno zatvoreno uređeno polje. Polje racionalnih brojeva nije realno zatvoreno uređeno polje, jer nema svojstvo srednje vrijednosti u odnosu na polinom $f(x) = x^2 - 2$. Polje kompleksnih brojeva nije realno zatvoreno uređeno polje jer na $\mathbb{C}$ ne možemo definirati uređaj koji bi bio kompatibilan s operacijama.

Teoriju realnih zatvorenih uređenih polja kratko označavamo sa **RCOF** (eng. real closed order fields).

Teorem 1.174. *Teorija RCOF dopušta eliminaciju kvantifikatora. Teorija RCOF je modelno potpuna.*

Korolar 1.175. *Neka je S neki konačan sustav jednadžbi i nejednadžbi s koeficijentima u nekom uređenom polju F. Ako sustav S ima rješenje u nekom uređenom proširenju od F, tada sustav S ima rješenje i u realnom uređenom zatvorenju $\overline{F}$ od F.*

Dokaz. Primijetimo prvo da u iskazu korolara koristimo činjenicu da za svako uređeno polje F postoji realno zatvoreno uređeno proširenje $\overline{F}$. Neka je G neko uređeno proširenje od F u kojem sustav S ima rješenje. Znamo (!) da u realnom uređenom zatvorenju $\overline{G}$ od G postoji potpolje koje je izomorfno zatvorenju $\overline{F}$. Bez smanjenja općenitosti možemo pretpostaviti (!) da vrijedi $\overline{F} \subseteq \overline{G}$. Pošto je teorija RCOF modelno potpuna, te su $\overline{F}$ i $\overline{G}$ realno zatvorena uređena polja takva da je $\overline{F} \subseteq \overline{G}$, tada vrijedi $\overline{F} \prec \overline{G}$. Pošto sustav S ima rješenje u polju G, te je $G \subseteq \overline{G}$, tada sustav ima rješenje i u polju $\overline{G}$. Očito je sustav S ekvivalentan nekoj formuli oblika $\exists x_1 \ldots \exists x_n \varphi$. To znači da vrijedi $\overline{G} \models \exists x_1 \ldots \exists x_n \varphi$. Iz ovog posljednjeg i $\overline{F} \prec \overline{G}$ slijedi $\overline{F} \models \exists x_1 \ldots \exists x_n \varphi$. □

Lagrangeov teorem. Za svaki pozitivan racionalan broj q postoje $a, b, c, d \in \mathbb{Q}$ takvi da je $q = a^2 + b^2 + c^2 + d^2$.

Teorem 1.176. *(**Artinovo rješenje 17. Hilbertovog problema**)*
Neka je F polje realnih ili racionalnih brojeva. Neka je $f \in F(x_1, \ldots, x_n)$ pozitivno semidefinitna racionalna funkcija. Tada postoje polinomi $g_1, \ldots, g_k \in F[X_1, \ldots, X_n]$ tako da vrijedi: $f = \sum_{i=1}^{k} g_i^2$

Detaljno rješenje Hilbertovog 17. problema možete vidjeti u [14], [18], [22] i [31].

1.14 Saturacija

Saturirani ili "zasićeni" modeli su modeli koji imaju "maksimalna" svojstva. Za svaki kardinalni broj λ mogu se razmatrati λ–saturirani modeli. Kao glavni alat za konstrukciju saturiranih modela poslužit će nam ultraprodukti. Prije definicije λ–saturiranog modela moramo uvesti još neke pojmove.
Sa $\Gamma(x)$ označavamo skup FO–formula u kojima samo varijabla x može imati slobodni nastup. Ako je $\mathfrak{M}$ neki σ–model tada skup σ–rečenica $Th(\mathfrak{M}) = \{F : \mathfrak{M} \models F\}$ nazivamo **teorija modela** $\mathfrak{M}$.

Neka je $\mathfrak{M}$ neka σ–struktura i $\Gamma(x)$ skup σ–formula. Kažemo da je neki skup σ–formula $\Gamma(x)$ **konzistentan s teorijom modela** $\mathfrak{M}$ ako postoji σ–model $\mathfrak{N}$ tako da vrijedi:

a) $\mathfrak{M} \equiv \mathfrak{N}$

b) postoji $a \in |\mathfrak{N}|$ tako da vrijedi $\mathfrak{N} \models \Gamma(x)[a]$.

(Odnosno, skup formula $\Gamma(x)$ je konzistentan 1–tip u odnosu na potpunu teoriju $Th(\mathfrak{M})$.)

Propozicija 1.177. *Neka je $\mathfrak{M}$ neka σ–struktura i $\Gamma(x)$ skup σ–formula. Sljedeće tvrdnje su ekvivalentne:*

a) skup $\Gamma(x)$ je konzistentan s teorijom modela $\mathfrak{M}$

b) za svaki konačan podskup $\Delta(x)$ od $\Gamma(x)$ postoji $a \in |\mathfrak{M}|$ tako da vrijedi $\mathfrak{M} \models \Delta(x)[a]$

Neka je $\mathfrak{M}$ neka σ–struktura. Za svaki $A \subseteq |\mathfrak{M}|$ neka je $\sigma_A = \sigma \cup \{\overline{a} : a \in A\}$, gdje je za svaki $a \in A$ novi konstantski simbol, te za $a_1 \neq a_2$ vrijedi $\overline{a_1} \neq \overline{a_2}$. Sa $\mathfrak{M}_A$ označavamo σ_A–ekspanziju modela $\mathfrak{M}$, gdje je za svaki $a \in A$ konstantski simbol $\overline{a}$ interpretiran sa a.

Definicija 1.178. *Neka je λ proizvoljan kardinalni broj. Kažemo da je neki σ–model $\mathfrak{M}$ λ–***saturiran** *ako za svaki $A \subseteq |\mathfrak{M}|$, takav da je $kard(A) < \lambda$, i svaki skup σ_A–formula $\Gamma(x)$ za koji postoji σ_A–model $\mathfrak{N}$ takav da:*

$$\mathfrak{M}_A \equiv \mathfrak{N} \quad \textit{i postoji} \quad a \in |\mathfrak{N}| \quad \textit{takav da} \quad \mathfrak{N} \models \Gamma(a),$$

imamo da postoji $b \in |\mathfrak{M}_A|$ tako da vrijedi $\mathfrak{M}_A \models \Gamma(x)[b]$.

Napomena 1.179. *Model $\mathfrak{M}$ je λ–saturiran ako je za svaki $A \subseteq |\mathfrak{M}|$ kardinalnosti strogo manje od λ svaki 1–tip, koji je konzistentan u odnosu na potpunu teoriju $Th(\mathfrak{M}_A)$, realiziran u modelu $\mathfrak{M}_A$.*

Model koji je ω_1–saturiran nazivamo i **prebrojivo saturiran model**. (Sa ω_1 je označen prvi neprebrojivi kardinalni broj).

Primjer 1.180. *a) Svaki konačan model je prebrojivo saturiran.*
Dokaz. Neka je $\mathfrak{M}$ neka konačna σ–struktura. Neka je $A \subseteq |\mathfrak{M}|$ proizvoljan. Neka je $\Gamma(x)$ tip koji je konzistentan u odnosu na teoriju $Th(\mathfrak{M}_A)$. Tada postoji σ_A–struktura $\mathfrak{N}$ i $b \in |\mathfrak{N}|$ tako da vrijedi $\mathfrak{N} \equiv \mathfrak{M}_A$, te imamo $\mathfrak{N} \models \Gamma(x)[b]$. Pošto je $\mathfrak{M}_A$ konačna struktura, te vrijedi $\mathfrak{N} \equiv \mathfrak{M}_A$ tada postoji izomorfizam $f : \mathfrak{N} \simeq \mathfrak{M}_A$. Tada očito vrijedi $\mathfrak{M}_A \models \Gamma(x)[f(b)]$.

b) Model $(\mathbb{Q}, <, =)$ je ω–saturiran.
(Za dokaz primijenite Cantorov teorem o uređanoj karakteristici skupa $\mathbb{Q}$.)

c) Model $(\mathbb{N}, <, =)$ nije prebrojivo saturiran.
Kako bi to dokazali definiramo skup formula:

$$\Gamma(x) = \{ \quad \exists y_1(y_1 < x),\ \exists y_1 \exists y_2(y_1 < y_2 < x),$$

$$\exists y_1 \exists y_2 \exists y_3(y_1 < y_2 < y_3 < x) \ \ldots, \}$$

Očito je svaki konačan podskup od $\Gamma(x)$ ispunjiv na $(\mathbb{N}, <, =)$, te skup $\Gamma(x)$ nije ispunjiv na $(\mathbb{N}, <, =)$.

Propozicija 1.181. *Svaki beskonačan ω_1–saturiran model je neprebrojiv.*

Dokaz. Neka je $\mathfrak{M}$ beskonačan ω_1–saturiran model. Pretpostavimo da je $\mathfrak{M}$ prebrojiv σ–model. Neka je $\Gamma(x) = \{x \neq \overline{a} : a \in |\mathfrak{M}|\}$. Neka $b \notin |\mathfrak{M}|$ proizvoljna, te označimo $|\mathfrak{N}| = |\mathfrak{M}| \cup \{x_0\}$. Definiramo interpretaciju nelogičkih simbola kako bismo dobili $\sigma_{\mathfrak{M}}$–strukturu $\mathfrak{N}$. Za svaki nelogički simbol $s \in \sigma$ neka je $s^{\mathfrak{N}} = s^{\mathfrak{M}}$. Zatim, za svaki $a \in |\mathfrak{M}|$ definiramo $\overline{a}^{\mathfrak{N}} = a$. Očito tada vrijedi $\mathfrak{N} \equiv (\mathfrak{M}, a)_{a \in |\mathfrak{M}|}$, te $\mathfrak{N} \models \Gamma(x)[b]$. Pošto je po pretpostavci skup $|\mathfrak{M}| \subseteq |\mathfrak{N}|$ prebrojiv, tada je $\Gamma(x)$ prebrojiv skup $\sigma_{\mathfrak{M}}$–formula koji je konzistentan s teorijom modela $(\mathfrak{M}, a)_{a \in |\mathfrak{M}|}$. Pošto je po pretpostavci model $\mathfrak{M}$ ω_1–saturiran tada bi posebno skup formula $\Gamma(x)$ trebao biti ispunjiv u modelu $(\mathfrak{M}, a)_{a \in |\mathfrak{M}|}$, što očito nije. □

Propozicija 1.182. *Ako je $\mathfrak{M}$ neki λ–saturirani model tada je model $\mathfrak{M}$ konačan ili pak je kardinalnosti veće ili jednake od λ.*

Sljedeći teorem govori o egzistenciji ω_1–saturiranih modela. Pojam prebrojivo nepotpunog ultrafiltra je definiran na strani 61.

Teorem 1.183. *Neka je $\{\mathfrak{M}_i : i \in I\}$ neka familija σ–struktura. Neka je U proizvoljan prebrojivo nepotpun ultrafiltar nad I. Tada je ultraprodukt $\prod_U \mathfrak{M}_i$ prebrojivo saturiran.*
(Kratko: **svaki ultraprodukt nad prebrojivo nepotpunim ultrafiltrom je ω_1–saturiran**.*)*

Dokaz. Iz propozicije 1.177. slijedi da je dovoljno dokazati da za svaki niz elemenata $A = (a_m)$ od $\prod_U \mathfrak{M}_i$ i svaki skup σ_A–formula $\Gamma(x)$ čiji je svaki konačan podskup ispunjiv u $(\prod_U \mathfrak{M}_i, a_m)_{m\in\mathbb{N}}$, vrijedi da je skup $\Gamma(x)$ ispunjiv u $(\prod_U \mathfrak{M}_i, a_m)_{m\in\mathbb{N}}$. Ako za svaki $k \in \mathbb{N}$ izaberemo $b_k \in \prod_{i\in\mathbb{N}} \mathfrak{M}_i$ t.d. $a_k = (b_k)_U$, primijetimo da vrijedi

$$(\prod_U \mathfrak{M}_i, a_k)_{k\in\mathbb{N}} = \prod_U ((\mathfrak{M}_i, b_k(i))_{k\in\mathbb{N}})$$

Budući da jezik određen sa σ proizvoljan prebrojiv jezik, te je jezik određen sa σ_A također prebrojiv, dovoljno je dokazati sljedeću tvrdnju:

> *Ako je skup $\Gamma(x)$ nekih σ_A–formula konačno ispunjiv u σ_A–strukturi $\prod_U \mathfrak{M}_i$, tada je on i ispunjiv u toj strukturi.*

Neka je $\Gamma(x) = \{\varphi_1(x), \varphi_2(x), \ldots\}$ proizvoljan konačno ispunjiv skup σ_A–formula u $\prod_U \mathfrak{M}_i$. Budući da je U prebrojivo nepotpun ultrafiltar tada iz propozicije 1.116. slijedi da postoji niz $(Y_n) \subseteq U$ sa svojstvom

$$I = Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq \ldots, \qquad \text{i} \quad \bigcap_{n\in\mathbb{N}} Y_n = \emptyset.$$

Definiramo niz podskupova (X_n) od I na sljedeći način:

$$X_0 = I$$

$$X_n = Y_n \cap \{i \in I \mid \mathfrak{M}_i \models \exists x(\varphi_1(x) \wedge \ldots \wedge \varphi_n(x))\}, \quad \text{za} \quad n > 0$$

Budući da je po pretpostavci skup formula $\Gamma(x)$ konačno ispunjiv u modelu $\prod_U \mathfrak{M}_i$, tada posebno za svaki $n > 0$ vrijedi:

$$\prod_U \mathfrak{M}_i \models \exists x(\varphi_1(x) \wedge \ldots \wedge \varphi_n(x))$$

Iz Łosovog teorema stoga slijedi da za svaki $n > 0$ vrijedi:

$$\{i \in I \mid \mathfrak{M}_i \models \exists x(\varphi_1(x) \wedge \ldots \wedge \varphi_n(x))\} \in U$$

Sada iz definicije skupova X_n slijedi da za svaki $n \in \mathbb{N}$ vrijedi $X_n \in U$.
Iz $\bigcap X_n \subseteq \bigcap I_n = \emptyset$ posebno slijedi $\bigcap X_n = \emptyset$, te očito za svaki $n \in \mathbb{N}$ vrijedi $X_n \supseteq X_{n+1}$. Prema tome, za svaki $i \in I$ postoji najveći $n(i) \in \mathbb{N}$ takav da $i \in X_{n(i)}$. Primijetimo da za slučaj $n(i) > 0$ vrijedi:

$$i \in X_{n(i)} \subseteq \ldots \subseteq X_1 \subseteq X_0,$$

a onda očito slijedi $\mathfrak{M}_i \models \exists x(\varphi_1(x) \wedge \ldots \wedge \varphi_{n(i)}(x))$. Iz posljednjeg slijedi da za svaki $i \in I$ postoji $f(i) \in \mathfrak{M}_i$ takav da $\mathfrak{M}_i \models (\varphi_1(x) \wedge \ldots \wedge \varphi_{n(i)}(x))[f(i)]$. Definiramo funkciju $f : I \to \bigcup \mathfrak{M}_i$ ovako:

ako je n(i)=0 neka je $f(i) \in \mathfrak{M}_i$ proizvoljan.

ako je $n(i) > 0$, biramo $f(i)$ tako da vrijedi

$$\mathfrak{M}_i \models (\varphi_1(x) \wedge \ldots \wedge \varphi_{n(i)}(x))[f(i)].$$

Za svaki $n > 0$ i svaki $i \in X_n$ očito je $n \leq n(i)$, pa posebno vrijedi i $\mathfrak{M}_i \models \varphi_n[f(i)]$. Dakle, vrijedi $\{i \in I \mid \mathfrak{M}_i \models \varphi_n[f(i)]\} \supseteq X_n \in U$. Sada iz Łosovog teorema slijedi da za svaki $n \in \mathbb{N}$ vrijedi $\prod_U \mathfrak{M}_i \models \varphi_n[f_U]$, i time smo dokazali:

$$\prod_U \mathfrak{M}_i \models \Gamma(x)[f_U].$$

□

Definicija 1.184. *Za strukturu $\mathfrak{M}$ kažemo da je* **saturirana struktura** *ako je kard($\mathfrak{M}$)–saturirana.*

Teorem 1.185. *(***Teorem o jedinstvenosti za saturirane modele***)*
Neka su $\mathfrak{M}$ i $\mathfrak{N}$ saturirane σ–strukture iste kardinalnosti. Ako su strukture $\mathfrak{M}$ i $\mathfrak{N}$ elementarno ekvivalentne tada su one i izomorfne.

Dokaz provodimo samo za slučaj kada su $\mathfrak{M}$ i $\mathfrak{N}$ prebrojive strukture. Sasvim analogno se dokazuje za općeniti slučaj. Detalje možete vidjeti npr. u skripti [22].

Neka je $M = \{m_0, m_1, \ldots\}$ i $N = \{n_0, n_1, \ldots, \}$. Induktivno definiramo nizove $(a_n) \subseteq M$ i $(b_n) \subseteq N$. Neka je $a_0 := m_0$, te promotrimo njegov pripadni tip $t(a_0/\mathfrak{M}) = \{F(x) : \mathfrak{M} \models F[a_0]\}$. Očito vrijedi $\mathfrak{M} \models t(a_0/\mathfrak{M})[a_0]$, pa zbog $\mathfrak{M} \equiv \mathfrak{N}$ vrijedi da je tip $t(a_0/\mathfrak{M})$ konzistentan s teorijom modela $\mathfrak{N}$. Pošto je

po pretpostavci model $\mathfrak{N}$ ω_1–saturiran tada slijedi da postoji $b_0 \in N$ takav da $\mathfrak{N} \models \Gamma(x)[b_0]$. Lako je vidjeti da vrijedi $(\mathfrak{M}, a_0) \equiv (\mathfrak{N}, b_0)$.

Pretpostavimo da smo za neki $n \in \mathbb{N}$, $n > 0$, definirali skupove $\{a_0, \ldots, a_{n-1}\}$ i $\{b_0, \ldots, b_{n-1}\}$, tako da vrijedi: $(\mathfrak{M}, a_0, \ldots, a_{n-1}) \equiv (\mathfrak{N}, b_0, \ldots, b_{n-1})$. Pri definiciji elemenata a_n i b_n razlikujemo dva slučaja: n je paran i n je neparan. Promotrimo prvo slučaj kada je n paran. Neka je $k_0 = \min\{k : m_k \in M \setminus \{a_0, \ldots, a_{n-1}\}\}$. Tada definiramo $a_n := m_{k_0}$.
Pošto je tip $T_n := t(a_n/(\mathfrak{M}, a_0, \ldots, a_{n-1}))$ očito konzistentan s teorijom modela $(\mathfrak{N}, b_0, \ldots, b_{n-1})$, te je model $(\mathfrak{N}, b_0, \ldots, b_{n-1})$ također ω_1–saturiran, tada postoji $b_n \in N \setminus \{b_0, \ldots, b_{n-1}\}$ tako da vrijedi:

$$(\mathfrak{N}, b_0, \ldots, b_{n-1}) \models T_n[b_n] \quad \text{i}$$

$$(\mathfrak{M}, a_0, \ldots, a_{n-1}, a_n) \equiv (\mathfrak{N}, b_0, \ldots, b_{n-1}, b_n)$$

U slučaju kada je n neparan prvo biramo $b_n \in N \setminus \{b_0, \ldots, b_{n-1}\}$ s najmanjim indeksom. Tada sasvim analogno kao za slučaj kada je n paran izaberemo a_n kao što smo tamo birali b_n, pri čemu element a_n realizira odgovarajući tip T_n'.
Ovakvim postupkom naizmjeničnog uzimanja elemenata oba skupa (tzv. **back and forth** konstrukcija) dobivamo nizove $a_0, a_1, \ldots$ i $b_0, b_1, \ldots$ takve da za svaki $n \in \mathbb{N}$ element a_n realizira odgovarajući tip T_n' u $(\mathfrak{M}, a_0, \ldots, a_{n-1})$, te b_n realizira tip T_n u $(\mathfrak{N}, b_0, \ldots, b_{n-1})$. Zatim, vrijedi $(\mathfrak{M}, a_0, a_1, \ldots) \equiv (\mathfrak{N}, b_0, b_1, \ldots)$. Sada je lako provjeriti da je preslikavanje $a_n \mapsto b_n$ izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. □

Kako bi mogli izreći sljedeći teorem koji povezuje eliminaciju kvantifikatora i saturirane modele, prvo definiramo posebnu vrstu skupova parcijalnih izomorfizama.

Definicija 1.186. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Neka je I neki skup parcijalnih izomorfizama između $\mathfrak{M}$ i $\mathfrak{N}$. Kažemo da skup I ima* **back-and-forth** *svojstvo ako vrijedi:*

a) za svaki $p \in I$ i svaki $a \in |\mathfrak{M}|$ postoji $q \in I$ tako da vrijedi $p \subseteq q$ i $a \in Dom(q)$

b) za svaki $p \in I$ i svaki $b \in |\mathfrak{N}|$ postoji $q \in I$ tako da vrijedi $p \subseteq q$ i $b \in Rng(q)$

Teorem 1.187. *Neka je T neka σ–teorija. Sljedeće tvrdnje su ekvivalentne:*

a) teorija T dopušta eliminaciju kvantifikatora

b) ako su $\mathfrak{M}$ i $\mathfrak{N}$ dva ω_1–saturirana modela teorije T tada skup svih konačnih parcijalnih izomorfizama između modela $\mathfrak{M}$ i $\mathfrak{N}$ ima back-and-fort svojstvo

U skripti [22] možete vidjeti i Vaughtov teorem o egzistenciji saturiranog modela koji je prebrojiv, odnosno Morley, Vaughtov teorem o egzistenciji neprebrojivog saturiranog modela.

1.15 Apstraktna teorija modela

Lindströmov prvi teorem osigurava posebno mjesto logici prvog reda među svim logičkim sistemima. Naime, logika prvog reda je najizražajniji logički sistem u kojem vrijedi Löwenheim–Skolemov teorem i teorem kompaktnosti. Drugim riječima, ne postoji "moćnija" logika s gore navedenim svojstvima od logike prvog reda.

Eliminacija funkcijskih i konstatnskih simbola u FO

Često se javlja potreba da se skup nelogičkih simbola zamijeni sa skupom nelogičkih simbola koji sadrži samo relacijske simbole. Prirodni način da se to napravi je da se promatraju grafovi funkcija. Za skup nelogičkih simbola kažemo da je **relacijski** ako sadrži samo relacijske simbole.

Neka je σ neki skup nelogičkih simbola. Za svaki n–mjesni funkcijski simbol $f \in \sigma$ neka je F novi $(n+1)$–mjesni relacijski simbol. Za svaki konstantski simbol $c \in \sigma$ neka je C novi jednosmjesni relacijski simbol. Neka se σ^r sastoji od relacijskih simbola od σ i novih relacijskih simbola kako smo upravo definirali.

Svakoj σ–strukturi $\mathfrak{M}$ pridružujemo σ^r–strukturu $\mathfrak{M}^r$ koja je definirana na sljedeći način:

a) $|\mathfrak{M}^r| = |\mathfrak{M}|$

b) za svaki relacijski simbol $R \in \sigma$ definiramo $R^{\mathfrak{M}^r} = R^{\mathfrak{M}}$

c) za svaki n–mjesni funkcijski simbol $f \in \sigma$ neka je interpretacija novog relacijskog simbola F definirana kao graf funkcije $f^{\mathfrak{M}}$, tj. za sve $a_1, \ldots, a_n, a_{n+1} \in |\mathfrak{M}|$ definiramo:

$$(a_1, \ldots, a_n, a_{n+1}) \in R^{\mathfrak{M}^r} \quad \text{ako i samo ako} \quad f^{\mathfrak{M}}(a_1, \ldots, a_n) = a_{n+1}$$

d) za svaki konstantski simbol $c \in \sigma$ interpretaciju novog jednomjesnog relacijskog simbola C definiramo pomoću grafa konstantne funkcije $a \mapsto c^{\mathfrak{M}}$, tj. točnije za svaki $a \in |\mathfrak{M}|$ definiramo:

$$a \in C^{\mathfrak{M}^r} \quad \text{ako i samo ako} \quad c^{\mathfrak{M}} = a$$

Svaku σ–formulu transformiramo u σ^r–formulu zamjenjujući sve potformule oblika:

a) $A(\ldots f(\vec{x}) \ldots)$ sa $F(\vec{x}, y) \to A(\ldots y/f(\vec{x}) \ldots)$,

b) $A(\ldots c \ldots)$ sa $C(x) \to A(\ldots x/c \ldots)$.

Ako je G neka σ–formula tada sa G^r označavamo σ^r–formulu koja je dobivena iz formule F eliminacijom svih funkcijskih i konstantskih simbola.

Teorem 1.188. *Za svaku σ–formulu G i svaku σ–strukturu $\mathfrak{M}$ vrijedi:*

$$\mathfrak{M} \models G \quad \textit{ako i samo ako} \quad \mathfrak{M}^r \models G^r$$

Dokaz se provodi indukcijom po složenosti formule, a onda indukcijom po broju pojavljivanja funkcijskih i konstantskih simbola u formuli G.

Korolar 1.189. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Tada vrijedi:*

$$\mathfrak{M} \equiv \mathfrak{N} \quad \textit{ako i samo ako} \quad \mathfrak{M}^r \equiv \mathfrak{N}^r$$

Neka je $\mathfrak{M}$ neka σ–struktura. Za neprazan skup $S \subseteq |\mathfrak{M}|$ kažemo da je σ–**zatvoren skup** u strukturi $\mathfrak{M}$ ako vrijedi:

a) za svaki konstantski simbol $c \in \sigma$ vrijedi $c^{\mathfrak{M}} \in S$

b) za svaki funkcijski simbol $f^n \in \sigma$ i sve elemente $a_1, \ldots, a_n \in S$ vrijedi $f^{\mathfrak{M}}(a_1, \ldots, a_n) \in S$.

Ako je $\mathfrak{M} \subseteq \mathfrak{N}$ tada je skup $|\mathfrak{M}|$ jedan σ–zatvoren skup u strukturi $\mathfrak{N}$. Očito svaki σ–zatvoren skup S definira jedinstveni podmodel zadane strukture $\mathfrak{M}$. Taj podmodel označavamo sa $[S]^{\mathfrak{M}}$.

Relativizacija u FO.

Definicija 1.190. *Neka je σ neki skup nelogičkih simbola, te U jednomjesni relacijski simbol takav da $U \notin \sigma$. Za svaku σ–formulu φ induktivno definiramo $\sigma \cup \{U\}$–formulu φ^U, koju nazivamo U–relativizacija od φ, ovako:*

a) $\varphi^U \equiv \varphi$, *ako je φ neka elementarna formula,*

b) $(\neg\varphi)^U \equiv \neg\varphi^U$

c) $(\varphi \vee \psi)^U \equiv \varphi^U \vee \psi^U$

d) $(\exists x\varphi)^U \equiv \exists x(U(x) \wedge \varphi)$

Lema 1.191. *(Lema o relativizaciji)*
Neka je $\mathfrak{M}$ neka $\sigma \cup \{U\}$–struktura, gdje je U jednomjesni relacijski simbol takav da $U \notin \sigma$), te je $U^{\mathfrak{M}}$ neki σ–zatvoren skup. Tada za svaku σ–rečenicu φ vrijedi:

$$[U^{\mathfrak{M}}]^{\mathfrak{M}} \models \varphi \quad \textit{ako i samo ako} \quad \mathfrak{M} \models \varphi^U$$

Primjeri logičkih sistema

Prilikom razmatranja primjena teorema kompaktnosti bili smo naveli da u **logici drugog reda**, koju ovdje označavamo sa L_{II}, ne vrijedi teorem kompaktnosti, a ni Löwenheim–Skolemov teorem "na dolje".

Slaba logika drugog reda, tj. logika koju označavamo sa L_{II}^{W}, razlikuje se od logike drugog reda L_{II} samo u definiciji istinitosti formula oblika $\exists X\varphi$. Neka je $\mathfrak{M}$ neka σ–struktura, te v neka valuacija (za L_{II}) na $\mathfrak{M}$. Neka je X proizvoljna n–mjesna relacijska varijabla, te neka je φ neka formula logike drugog reda. Tada za logiku L_{II}^{W} definiramo:

$$\mathfrak{M} \models_v \exists X\varphi \quad \text{ako i samo ako} \quad \text{postoji konačan } S \subseteq |\mathfrak{M}|^n \text{ tako da } \mathfrak{M} \models_v \varphi[S]$$

Za logiku L_{II}^{W} ne vrijedi teorem kompaktnosti, ali vrijedi Löwenheim–Skolemov teorem.

Bili smo definirali i **beskonačnu logiku** $L_{\omega_1\omega}$. Podsjetit ćemo da je u logici $L_{\omega_1\omega}$ dopuštena i sljedeće pravilo izgradnje formula:

ako je S prebrojiv skup formula tada su $\bigwedge S$ i $\bigvee S$ također formule.

Löweinheim–Skolemov teorem vrijedi za logiku $L_{\omega_1\omega}$, a teorem kompaktnosti ne. Sada to dokazujemo u sljedeće dvije propozicije.

Propozicija 1.192. *(Za logiku $L_{\omega_1\omega}$ ne vrijedi teorem kompaktnosti) Postoji skup formula logike $L_{\omega_1\omega}$ koji je konačno ispunjiv, ali nije ispunjiv.*

Dokaz. Za svaki $n \in \mathbb{N} \setminus \{0, 1\}$ definiramo rečenicu sa:

$$\varphi_{\geq n} \equiv \bigwedge_{0 \leq i < j \leq n} x_i \neq x_j$$

Zatim, neka je $\varphi_{fin} \equiv \bigvee\{\neg\varphi_{\geq n} : n \geq 2\}$. Tada za svaku normalnu strukturu $\mathfrak{M}$ očito vrijedi:

$$\mathfrak{M} \models \varphi_{fin} \quad \text{ako i samo ako} \quad \mathfrak{M} \text{ je konačna struktura}$$

Svaki konačan podskup od $\{\varphi_{fin}\} \cup \{\varphi_{\geq n} : n \geq 2\}$ ima model, ali za sam skup ne postoji model. □

Lema 1.193. *Neka je σ najviše prebrojiv skup nelogičkih simbola. Zatim, neka je φ neka $L_{\omega_1\omega}$ formula, te neka je $\mathfrak{M}$ neki model za formulu φ. Tada postoji konačan ili prebrojiv normalan podmodel $\mathfrak{N}$ od $\mathfrak{M}$ koji je model za formulu φ.*

Skica dokaza. Definira se najviše prebrojiv podskup od $|\mathfrak{M}|$ koji je σ–zatvoren, te sadrži sve "svjedoke istinitosti" egzistencijalnih potformula od φ.

Tvrdnja sljedeće propozicije slijedi direktno iz prethodne leme.

Propozicija 1.194. *(Za $L_{\omega_1\omega}$ vrijedi Löwenheim–Skolemov teorem)*
Svaki skup rečenica logike $L_{\omega_1\omega}$ koji ima model ima i konačan ili prebrojiv model.

Logički sistem L_Q^N dobivamo dodavanjem alfabetu logike prvog reda novog kvantifikatora Qx, te je interpretacija formule oblika $Qx\varphi$ definirana sa: "postoji neprebrojivo mnogo x koji zadovoljavaju formulu φ." Logički sistem L_Q^N je izražajniji od logike prvog reda. Npr. pojam "najviše prebrojiv" možemo definirati formulom $\neg Qx(x = x)$.

Propozicija 1.195. *(Za logiku L_Q^N ne vrijedi Löwenheim–Skolemov teorem)*
Postoji formula logike L_Q^N koja ima model, ali nema konačan, a ni prebrojiv model.

Dokaz. Formula $Qx(x = x)$ ima neprebrojiv model, ali nema konačan, a ni prebrojiv model.

Teorem kompaktnosti vrijedi za sistem L_Q^N ako je skup nelogičkih simbola najviše prebrojiv, ali ne vrijedi općenito.

Propozicija 1.196. *(Teorem kompaktnosti ne vrijedi za sistem L_Q^N)*
Neka je σ neprebrojiv skup nelogičkih simbola. Tada postoji skup formula logike L_Q^N koji je konačno ispunjiv, ali on sam nije ispunjiv.

Dokaz. Neka je $\Phi = \{\neg(c = d) : c, d \in \sigma,\ c \neq d\} \cup \{\neg Qx(x = x)\}$. Lako je vidjeti da svaki konačan podskup od Φ ima model, ali za skup Φ ne postoji model. □

Logički sistem L_Q^P dobivamo dodavanjem alfabetu logike prvog reda novog kvantifikatora Qx. Interpretacija formule oblika $Qx\varphi$ je definirana sa: "postoji prebrojivo mnogo x koji zadovoljavaju formulu φ." Za logiku L_Q^P ne vrijedi teorem kompaktnosti, ali vrijedi Löwenheim–Skolemov teorem.

Kod logičkog sistema L_Q^K interpretacija formule oblika $Qx\varphi$ je definirana sa: "postoji samo konačno mnogo x koji zadovoljavaju formulu φ." Za sistem L_Q^K ne vrijedi teorem kompaktnosti, ali vrijedi Löwenheim–Skolemov teorem.

Kod logičkog sistema L_Q^D interpretacija formule oblika $Qx\varphi$ je definirana sa: "postoje barem dva različita x koji zadovoljavaju formulu φ." Za sistem L_Q^D ne vrijedi teorem kompaktnosti, a ni Löwenheim–Skolemov teorem.

Rezimirajmo u sljedećoj tablici rezultate o logičkim sistemima koje smo bili naveli.

Logički sistem	Löwenheim–Skolemov teorem	Teorem kompaktnosti	
		Općenito	za prebrojive skupove formula
FO	+	+	+
L_{II}	–	–	–
L_{II}^{W}	+	–	–
$L_{\omega_1\omega}$	+	–	–
L_Q^N	–	–	+
L_Q^P	+	–	–
L_Q^K	+	–	–
L_Q^D	–	–	–

Prirodno se postavlja pitanje postoji li izražajniji logički sistem od logike prvog reda za kojeg bi vrijedili teorem kompaktnosti i Löwenheim–Skolemov teorem.

Svaki skup nelogičkih simbola može sadržavati proizvoljan broj relacijskih, funkcijskih i konstantskih simbola. Intuitivno, na logički sistem možemo gledati kao na način pridruživanja nekog nelogičkog skupa simbola i skupa rečenica stvorenih od tih simbola zajedno s relacijom koja određuje istinitost rečenice. Primjerice, kod logike prvog reda skupu nelogičkih simbola σ pridružuje se skup σ–rečenica prvog reda, a relacija istinitosti je uobičajena relacija $\models$ između interpretacije i formula.

Definicija 1.197. Logički sistem $\mathfrak{L}$ *sastoji se od funkcije* L *i binarne relacije* $\models_{\mathfrak{L}}$. *Funkcija* L *svakom skupu nelogičkih simbola* σ *pridružuje neki skup* $L(\sigma)$, *koji nazivamo skup* σ*–rečenica, pri čemu vrijedi:*

(a) Ako je $\sigma \subseteq \sigma'$ *tada je* $L(\sigma) \subseteq L(\sigma')$

(b) Ako su $\mathfrak{M}$ *i* φ *u relaciji* $\models_{\mathfrak{L}}$, *što kratko označavamo sa* $\mathfrak{M} \models_{\mathfrak{L}} \varphi$ *tada postoji skup* σ *takav da je* $\mathfrak{M}$ *neka* σ*–struktura i* $\varphi \in L(\sigma)$

(c) Ako vrijedi $\mathfrak{M} \models_{\mathfrak{L}} \varphi$ *i* $\mathfrak{M} \simeq \mathfrak{N}$ *tada vrijedi i* $\mathfrak{N} \models_{\mathfrak{L}} \varphi$

(d) Ako je $\sigma \subseteq \sigma'$, $\varphi \in L(\sigma)$ *i* $\mathfrak{M}$ *je* σ'*–struktura, tada vrijedi:*

$$\mathfrak{M} \models_{\mathfrak{L}} \varphi \qquad \textit{ako i samo ako} \qquad \mathfrak{M} \restriction \sigma \models_{\mathfrak{L}} \varphi,$$

gdje je sa $\mathfrak{M} \restriction \sigma$ *označena* σ*–redukcija od* $\mathfrak{M}$.

Neka je $\mathfrak{L}$ neki logički sistem i $\varphi \in L(\sigma)$. Označimo sa $Mod(\sigma, \mathfrak{L})(\varphi)$ skup svih modela za rečenicu φ, tj. $Mod(\sigma, \mathfrak{L})(\varphi) = \{\mathfrak{M} : \mathfrak{M}$ je σ–struktura i $\mathfrak{M} \models_{\mathfrak{L}} \varphi\}$.

Definicija 1.198. *(a) Kažemo da je logički sistem* $\mathfrak{L}'$ **izražajan barem** *kao logički sistem* $\mathfrak{L}$*, i pišemo* $\mathfrak{L} \leq \mathfrak{L}'$*, ako za svaki skup* σ *i za svaku rečenicu* $\varphi \in L(\sigma)$ *postoji* $\psi \in L'(\sigma)$ *tako da vrijedi* $Mod(\sigma, \mathfrak{L})(\varphi) = Mod(\sigma, \mathfrak{L}')(\psi)$.

(b) Kažemo da su logički sistemi $\mathfrak{L}$ *i* $\mathfrak{L}'$ **jednako izražajni**, *i pišemo* $\mathfrak{L} \sim \mathfrak{L}'$*, ako vrijedi* $\mathfrak{L} \leq \mathfrak{L}'$ *i* $\mathfrak{L}' \leq \mathfrak{L}$.

Primjer 1.199. *Redom imamo:*

(i) $FO \leq L_{II}^{\mathrm{W}}$; $FO \leq L_{II}$; $FO \leq L_{Q}^{N}$; $FO \leq L_{\omega_1\omega}$

(ii) $L_{II}^{\mathrm{W}} \leq L_{II}$; *ne vrijedi* $L_{II} \leq L_{II}^{\mathrm{W}}$

(iii) ne vrijedi: $L_{II} \leq FO$; $L_{Q} \leq FO$; $L_{\omega_1\omega} \leq FO$

Definicija 1.200. *Kažemo da je* **logički sistem zatvoren za bulovske veznike**, *te pišemo* $Boole(\mathfrak{L})$*, ako vrijedi:*

(a) Za svaki skup σ *i svaku rečenicu* $\varphi \in L(\sigma)$ *postoji rečenica* $\psi \in L(\sigma)$ *takva da za svaku* σ*–strukturu* $\mathfrak{M}$ *vrijedi:*

$$\mathfrak{M} \models_{\mathfrak{L}} \psi \quad \textit{ako i samo ako} \quad \mathfrak{M} \not\models_{\mathfrak{L}} \varphi$$

(b) Za svaki skup σ*, te* $\varphi, \psi \in L(\sigma)$ *postoji rečenica* $\chi \in L(\sigma)$ *tako da za svaku* σ*–strukturu* $\mathfrak{M}$ *vrijedi:*

$$\mathfrak{M} \models_{\mathfrak{L}} \chi \quad \textit{ako i samo ako} \quad \mathfrak{M} \models_{\mathfrak{L}} \varphi \;\; i \;\; \mathfrak{M} \models_{\mathfrak{L}} \psi$$

Ako vrijedi svojstvo $Boole(\mathfrak{L})$ tada ćemo sa $\neg\varphi$ označavati rečenicu ψ iz uvjeta (a) iz prethodne definicije, odnosno sa $\varphi \wedge \psi$ ćemo označavati rečenicu χ iz uvjeta (b). Analogno bi mogli definirati rečenice $\varphi \vee \psi$, $\varphi \to \psi$ i $\varphi \leftrightarrow \psi$.

Neka je $\mathfrak{M}$ proizvoljna σ–struktura, te neka je U jednomjesni relacijski simbol tako da $U \notin \sigma$. Prisjetimo se: ako je $U^{\mathfrak{M}}$ σ–zatvoren skup u strukturi $\mathfrak{M}$ tada sa $[U^{\mathfrak{M}}]^{\mathfrak{M}}$ označavamo podmodel od $\mathfrak{M}$ s nosačem $U^{\mathfrak{M}}$. Sa $(\mathfrak{M}, U^{\mathfrak{M}})$ označavamo $\sigma \cup \{U\}$–strukturu kod koje je $U^{\mathfrak{M}}$ σ–zatvoren skup u strukturi $\mathfrak{M}$.

Definicija 1.201. *Kažemo da* **logički sistem** $\mathfrak{L}$ **dopušta relativizaciju**, *i pišemo* $Rel(\mathfrak{L})$*, ako za svaki skup* σ*, svaku rečenicu* $\varphi \in L(\sigma)$ *i svaki jednomjesni relacijski simbol* $U \notin \sigma$ *postoji neka rečenica* $\psi \in L(\sigma \cup \{U\})$ *takva da za svaku* σ*–strukturu* $\mathfrak{M}$ *i svaki* σ*–zatvoreni skup* $U^{\mathfrak{M}}$ *strukture* $\mathfrak{M}$ *vrijedi:*

$$(\mathfrak{M}, U^{\mathfrak{M}}) \models_{\mathfrak{L}} \psi \quad \textit{ako i samo ako} \quad [U^{\mathfrak{M}}]^{\mathfrak{M}} \models_{\mathfrak{L}} \varphi$$

Ako vrijedi $Rel(\mathfrak{L})$ tada sa φ^U označavamo rečenicu ψ iz prethodne definicije.

Definicija 1.202. *Kažemo da* **logički sistem $\mathfrak{L}$ dopušta eliminaciju** *funkcijskih i konstantskih simbola, tj. njihovu zamjenu novim relacijskim simbolima, i pišemo $Elim(\mathfrak{L})$, ako za svaki skup σ nelogičkih simbola i za svaku rečenicu $\varphi \in L(\sigma)$ postoji rečenica $\psi \in L(\sigma^r)$ takva da za svaku σ–strukturu $\mathfrak{M}$ vrijedi: $\mathfrak{M} \models_{\mathfrak{L}} \varphi$ ako i samo ako $\mathfrak{M}^r \models_{\mathfrak{L}} \psi$.*

Ako vrijedi $Elim(\mathfrak{L})$, tada sa φ^r označavamo rečenicu ψ iz prethodne definicije.

Definicija 1.203. *Za logički sistem $\mathfrak{L}$ kažemo da je* **regularan logički sistem** *ako za njega vrijede svojstva $Boole(\mathfrak{L})$, $Rel(\mathfrak{L})$ i $Elim(\mathfrak{L})$.*

Logika prvog reda je regularan sistem. (Jasno je da vrijedi $Boole(FO)$. Iz teorema 1.188. slijedi da vrijedi $Rel(FO)$, a iz leme 1.191. slijedi da vrijedi $Elim(FO)$).
Uvedimo sljedeće oznake:

a) *LöSko*($\mathfrak{L}$) označava činjenicu da za logički sistem $\mathfrak{L}$ vrijedi Löwenheim–Skolemov teorem, tj. da za svaku ispunjivu rečenicu iz $\mathfrak{L}$ postoji konačan ili prebrojiv normalan model.

b) *Comp*($\mathfrak{L}$) označava činjenicu da za logički sistem $\mathfrak{L}$ vrijedi teorem kompaktnosti, tj. ako je S skup rečenica iz $\mathfrak{L}$ takav da je svaki konačan podskup od S ispunjiv, tada je i S ispunjiv.

Teorem 1.204. *(Lindströmov prvi teorem)*
Neka je $\mathfrak{L}$ regularan logički sistem za koji vrijedi $FO \leq \mathfrak{L}$, te vrijedi Comp($\mathfrak{L}$) i LöSko($\mathfrak{L}$). Tada imamo $\mathfrak{L} \sim FO$.

Prije dokaza prvog Lindströmovog teorema navodimo tri leme, te definiramo pojam parcijalno izomorfnih strukutra i navodimo osnovna svojstva.

Neka je $\mathfrak{L}$ logički sistem i σ skup nelogičkih simbola. Neka je $\Phi \cup \{\varphi\} \subseteq L(\sigma)$. Kažemo da rečenica φ **logički slijedi** iz skupa rečenica Φ, i pišemo $\Phi \models_{\mathfrak{L}} \varphi$, ako za svaku σ–strukturu $\mathfrak{M}$ za koju vrijedi $\mathfrak{M} \models_{\mathfrak{L}} \Phi$, vrijedi i $\mathfrak{M} \models_{\mathfrak{L}} \varphi$.

Lema 1.205. *Neka je $\mathfrak{L}$ neki regularni logički sistem takav da vrijedi Comp($\mathfrak{L}$). Zatim, neka je σ neki skup nelogičkih simbola, te $\Phi \cup \{\varphi\} \subseteq L(\sigma)$ tako da vrijedi $\Phi \models_{\mathfrak{L}} \varphi$. Tada postoji konačan $\Phi_0 \subseteq \Phi$ tako da vrijedi $\Phi_0 \models_{\mathfrak{L}} \varphi$.*

Lema 1.206. *Neka je $\mathfrak{L}$ neki regularni logički sistem takav da vrijedi Comp($\mathfrak{L}$), te FO $\leq \mathfrak{L}$. Zatim, neka je σ neki skup nelogičkih simbola, te $\psi \in L(\sigma)$. Tada postoji konačan $\sigma_0 \subseteq \sigma$ tako da sve σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$ vrijedi da činjenica $\mathfrak{M} \restriction \sigma_0 \simeq \mathfrak{N} \restriction \sigma_0$ povlači $\mathfrak{M} \models_{\mathfrak{L}} \psi$ ako i samo ako $\mathfrak{N} \models_{\mathfrak{L}} \psi$.*

(Sa $\mathfrak{M} \restriction \sigma_0$ je označena σ_0–redukcija strukture $\mathfrak{M}$).

Lema 1.207. *Neka je $\mathfrak{L}$ neki regularni logički sistem takav da vrijedi Comp($\mathfrak{L}$), te FO $\leq \mathfrak{L}$. Neka za svaki skup σ, te za sve σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ za koje vrijedi $\mathfrak{M} \equiv_{FO} \mathfrak{N}$, imamo i $\mathfrak{M} \equiv_{\mathfrak{L}} \mathfrak{N}$. Tada vrijedi FO $\sim \mathfrak{L}$.*

Sada slijedi skica dokaza prvog Lindströmovog teorema.

Iz leme 1.207. slijedi da je za FO $\sim \mathfrak{L}$ dovoljno dokazati da za svaki skup nelogičkih simbola σ, te sve σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ vrijedi:

$$\text{ako } \mathfrak{M} \equiv_{FO} \mathfrak{N} \quad \text{tada} \quad \mathfrak{M} \equiv_{\mathfrak{L}} \mathfrak{N} \qquad (+)$$

Pošto je po pretpostavci $\mathfrak{L}$ regularni logički sistem, te posebno vrijedi $Elim(\mathfrak{L})$, tada je lako vidjeti da je tvrdnju (+) dovoljno dokazati za relacijske skupove nelogičkih simbola.

Neka je σ neki relacijski skup nelogičkih simbola. Pretpostavimo da ne vrijedi (+), tj. da postoje σ–strukutre $\mathfrak{M}$ i $\mathfrak{N}$, te da postoji rečenica $\psi \in L(\sigma)$ tako da vrijedi

$$\mathfrak{M} \equiv_{FO} \mathfrak{N}, \qquad \mathfrak{M} \models_{\mathfrak{L}} \psi \quad \text{i} \quad \mathfrak{N} \models_{\mathfrak{L}} \neg\psi \qquad (1)$$

Iz leme 1.206. slijedi da postoji konačan $\sigma_0 \subseteq \sigma$ tako da za sve σ–strukture $\mathfrak{M}_1$ i $\mathfrak{N}_1$ vrijedi:

$$(*) \begin{cases} \text{ako } \mathfrak{M}_1 \restriction \sigma_0 \simeq \mathfrak{N}_1 \restriction \sigma_0 \quad \text{tada} \\ \qquad\qquad\qquad\qquad \mathfrak{M}_1 \models_{\mathfrak{L}} \psi \text{ ako i samo ako } \mathfrak{N}_1 \models_{\mathfrak{L}} \psi \end{cases}$$

Iz (1) imamo $\mathfrak{M} \equiv_{FO} \mathfrak{N}$, a onda posebno i $\mathfrak{M} \restriction \sigma_0 \equiv_{FO} \mathfrak{N} \restriction \sigma_0$. Sada iz Fraissévog teorema slijedi da postoji niz (I_n) skupova parcijalnih izomorfizama tako da vrijedi:

$$(I_n) : \mathfrak{M} \restriction \sigma_0 \simeq_f \mathfrak{N} \restriction \sigma_0 \qquad (2)$$

Ključno je dokazati sljedeću tvrdnju (i najviše je posla).

Tvrdnja (3)

postoje σ–strukture $\mathfrak{M}'$ i $\mathfrak{N}'$ koje su najviše prebrojive i za koje vrijedi

$$\mathfrak{M}' \restriction \sigma_0 \simeq_p \mathfrak{N}' \restriction \sigma_0, \qquad \mathfrak{M}' \models_{\mathfrak{L}} \psi \text{ i } \mathfrak{N}' \models_{\mathfrak{L}} \neg\psi$$

Sada iz Karpovog teorema (vidi lemu 1.32.) slijedi da vrijedi $\mathfrak{M}' \restriction \sigma_0 \simeq \mathfrak{N}' \restriction \sigma_0$. Iz tvrdnje $(*)$ slijedi da vrijedi: $\mathfrak{M}' \models_{\mathfrak{L}} \psi$ ako i samo ako $\mathfrak{N}' \models_{\mathfrak{L}} \psi$, što je kontradikcija s tvrdnjom (3).

Lindströmov drugi teorem

Naglasimo neka svojstva logike prvog reda kako bi bila jasnija definicija tih pojmova za proizvoljan logički sistem. Kada kažemo **odlučiv skup** tada mislimo na neki skup riječi nad zadanim alfabetom za koji postoji algoritam (odnosno, Turingov stroj) koji za svaku riječ alfabeta kao ulazni podatak korektno odlučuje radi li se o riječi iz početnog skupa riječi. Ako je σ **odlučiv skup** nelogičkih simbola tada je i skup svih σ–rečenica odlučiv, tj. postoji algoritam koji za svaki konačan niz simbola alfabeta može odrediti je li to σ–rečenica. Operacije kao što su negacija formule, relativizacija, te eliminacija funkcijskih simbola, mogu biti **efektivno provedene**. Postoji adekvatan dokazni račun takav da je skup svih valjanih σ–rečenica **rekurzivno prebrojiv**.

Definicija 1.208. *Neka je $\mathfrak{L}$ neki logički sistem. Kažemo da je* **$\mathfrak{L}$ efektivan logički sistem** *ako je za svaki odlučiv skup σ nelogičkih simbola skup $L(\sigma)$ odlučiv, te za svaku σ–rečenicu $\varphi \in L(\sigma)$ postoji konačan $\sigma_0 \subseteq \sigma$ tako da vrijedi $\varphi \in L(\sigma_0)$.*

Logički sistemi FO, L_{II}, L_{II}^{W} i L_Q su efektivni, a $L_{\omega_1\omega}$ nije.

Definicija 1.209. *Neka su $\mathfrak{L}$ i $\mathfrak{L}'$ neki efektivni logički sistemi.*

a) $\mathfrak{L} \leq_{eff} \mathfrak{L}'$ *ako i samo ako za svaki odlučivi skup σ postoji izračunljiva funkcija $*$ koja svakoj rečenici $\varphi \in L(\sigma)$ pridružuje neku rečenicu $\varphi^* \in L'(\sigma)$ tako da vrijedi*

$$Mod(\sigma, \mathfrak{L})(\varphi) = Mod(\sigma, \mathfrak{L}')(\varphi^*)$$

b) $\mathfrak{L} \sim_{eff} \mathfrak{L}'$ *ako i samo ako* $\mathfrak{L} \leq_{eff} \mathfrak{L}'$ *i* $\mathfrak{L}' \leq_{eff} \mathfrak{L}$

Definicija 1.210. *Neka je $\mathfrak{L}$ neki logički sistem. Kažemo da je* **$\mathfrak{L}$ efektivno regularan logički sistem** *ako je efektivan i ako za svaki odlučiv skup σ nelogičkih simbola vrijedi:*

a) postoji izračunljiva funkcija koja svakoj rečenici $\varphi \in L(\sigma)$ pridružuje neku rečenicu $\neg\varphi$ tako da za svaku σ–strukturu $\mathfrak{M}$ vrijedi:

$$\models_{\mathfrak{L}} \neg\varphi \quad \textit{ako i samo ako} \quad \mathfrak{M} \not\models_{\mathfrak{L}} \varphi$$

Postoji izračunljiva funkcija koja svim parovima rečenica $\varphi, \psi \in L(\sigma)$ pridružuje neku rečenicu $\varphi \wedge \psi \in L(\sigma)$ tako da za svaku σ–strukturu $\mathfrak{M}$ vrijedi:

$$\mathfrak{M} \models_{\mathfrak{L}} \varphi \wedge \psi \quad \textit{ako i samo ako} \quad \mathfrak{M} \models_{\mathfrak{L}} \varphi \textit{ i } \mathfrak{M} \models_{\mathfrak{L}} \psi$$

b) Za svaki unarni relacijski simbol U, takav da $U \notin \sigma$, postoji izračunljiva funkcija koja svakoj rečenici $\varphi \in L(\sigma)$ pridružuje rečenicu $\varphi^U \in L(\sigma)$ tako da za svaku σ–strukturu $\mathfrak{M}$ i svaki σ–zatvoreni skup $U^{\mathfrak{M}}$ vrijedi:

$$(\mathfrak{M}, U^{\mathfrak{M}}) \models_{\mathfrak{L}} \varphi^U \quad \textit{ako i samo ako} \quad [U^{\mathfrak{M}}]^{\mathfrak{M}} \models_{\mathfrak{L}} \varphi$$

c) Postoji izračunljiva funkcija koja svakoj rečenici $\varphi \in L(\sigma)$ pridružuje rečenicu $\varphi^r \in L(\sigma^r)$ tako da za svaku σ–strukturu $\mathfrak{M}$ vrijedi:

$$\mathfrak{M} \models_{\mathfrak{L}} \varphi \quad \textit{ako i samo ako} \quad \mathfrak{M}^r \models_{\mathfrak{L}} \varphi^r$$

Definicija 1.211. *Neka je $\mathfrak{L}$ neki efektivno regularan logički sistem. Kažemo da je $\mathfrak{L}$* **rekurzivno prebrojiv za valjanost** *ako je za svaki odlučiv skup σ nelogičkih simbola skup svih valjanih σ–rečenica rekurzivno prebrojiv.*

Teorem 1.212. *(Lindströmov drugi teorem)*
Neka je $\mathfrak{L}$ neki efektivno regularan logički sistem takav da vrijedi $FO \leq_{eff} \mathfrak{L}$. Ako vrijedi LöSko($\mathfrak{L}$), te je $\mathfrak{L}$ rekurzivno prebrojiv za valjanost, tada $FO \sim_{eff} \mathfrak{L}$.

Ova predavanja su napisana koristeći isključivo knjigu [8]. U knjigama [6], [12] i [13] su dani također dokazi Lindströmovih teorema.

1.16 Teorija konačnih modela

U ovoj točki glavni nam je cilj dati motivaciju za proučavanje teorije konačnih modela. (Klasična) teorija modela uglavnom proučava beskonačne modele. Teorija konačnih modela - skraćeno FMT (eng. Finite Model Theory), uključuje:

- **klasičnu teoriju modela**,

- **kombinatoriku**

- **teoriju složenosti**.

Neki dijelovi FMT jako su povezani s računarstvom, posebno **deskriptvna teorija složenosti**. Zapravo, smatra se da bi FMT trebala biti logika za računarstvo. Osnove o teoriji složenosti, te Turingovi strojevi, dani su u Dodatku.

Dokazano je da mnogi klasični rezultati teorije modela ne vrijede na klasi svih konačnih struktura. Tu posebno treba istaknuti teoreme kompaktnosti i potpunosti, te mnoge teoreme o očuvanju i lemu interpolacije. Nevaženje teorema kompaktnosti povlači da standardni dokazi mnogih teorema ne mogu više biti provedeni u okviru FMT. U ovom trenutku (osim npr. Rosenovog teorema iz 2002) nije poznat niti jedan primjer nekog klasičnog teorema iz teorije modela koji ostaje vrijediti nad konačnim strukturama. Vjerojatno bi neki takav rezultat trebao biti dokazan nekim sasvim novim metodama. Iz tog razloga se smatra da je logika prvog reda "loša logika" za FMT.

Iz perspektive izražajne snage logike prvog reda se također ponaša loše: u nekim slučajevima je preslaba, a u nekima prejaka. Preslaba je jer mnoga prirodna svojstva, kao što su npr. da struktura ima točno paran broj elementa ili da je graf povezan, ne mogu biti definirana s jednom rečenicom. U drugu ruku, logika prvog reda je prejaka jer svaka klasa konačnih struktura nad konačnom signaturom može biti definirana s nekim beskonačnim skupom rečenica logike prvog reda. Čak i gore, svaka konačna struktura (nad konačnom signaturom bez funkcijskih simbola) može biti definirana s jednom rečenicom do na izomorfizam. Današnja teorija modela uglavnom razmatra potpune teorije prvog reda koje su u FMT sasvim trivijalne. Ako je teorija T potpuna tada su svi njeni modeli elementarno ekvivalentni. To znači da ako postoji konačan model $\mathfrak{M}$ za T, te je $\mathfrak{N}$ neki drugi model za T tada $\mathfrak{M} \equiv \mathfrak{N}$, a onda $\mathfrak{M} \simeq \mathfrak{N}$.

Nevaženje nekih teorema iz klasične teorije modela

Teorem kompaktnosti ne vrijedi za FMT, tj.

> *postoji skup S rečenica logike prvog reda čiji svaki konačan podskup ima konačan model, ali za S ne postoji konačan model.*

Skica dokaza:

$$\varphi_n \equiv \text{kardinalni broj nosača strukture je različit od } n$$

$$T = \{\varphi_n : n \in \mathbb{N}\}$$

Svaki konačan podskup T' od T ima konačan model (ako $\varphi_n \in T \setminus T'$ tada je svaka struktura s točno n elemenata model za T').

Teorem potpunosti ne vrijedi za FMT.

Iz teorema potpunosti za logiku prvog reda slijedi da je skup V svih valjanih rečenica rekurzivno prebrojiv. Nevaženje teorema potpunosti za FMT slijedi iz Trachtenbrotovog teorema.

Teorem 1.213. (Trachtenbrotov teorem)
Skup V_{fin} svih rečenica koje su istinite na svim konačnim strukturama nije rekurzivno prebrojiv.

Skica dokaza. Označimo:

$$S_{fin} = \text{skup svih rečenica za koje } \underline{\text{postoji}} \text{ konačan model}$$

Lako je dokazati da je skup S_{fin} rekurzivno prebrojiv. Iz nerješivosti **halting problema** slijedi da skup

$$\{T \ : \ T \ \text{ je Turingov stroj koji staje}\}$$

nije rekurzivan. Za svaki Turingov stroj T moguće je konstruirati rečenicu φ_T takva da vrijedi:

$$\text{Turingov stroj } T \text{ staje ako i samo ako } \varphi_T \in S_{fin}$$

Iz toga slijedi da skup S_{fin} nije rekurzivan. Očito vrijedi: $S^c_{fin} = \{\varphi : \neg\varphi \in V_{fin}\}$ Pretpostavimo da je skup V_{fin} rekurzivno prebrojiv. Tada je očito skup S^c_{fin} rekurzivno prebrojiv. Iz Postovog teorema slijedi da je skup S_{fin} rekurzivan, čime je dobivena kontradikcija. □

Löwenheim–Skolemovi teoremi nemaju smisla nad konačnim strukturama.

Sljedeći korolar Trachtenbrotovog teorema govori da ne postoje nikakve smislene analogije Löwenheim–Skolemovog teorema za FMT.

Korolar 1.214. *Ne postoji rekurzivna funkcija* $f : \mathbb{N} \to \mathbb{N}$ *takva da ako neka rečenica* φ *logike prvog reda ima model, tada mora imati model kardinalnosti manje od* $f(\lceil\varphi\rceil)$.

(Sa $\lceil\varphi\rceil$ smo označili kod formule φ, odnosno Gödelov broj – o tome više prilikom razmatranja Gödelovih teorema nepotpunosti).

Bethov teorem o definabilnosti ne vrijedi za FMT, tj.

> *postoji unarni relacijski simbol koji implicitno definabilan, ali nije eksplicitno definabilan.*

Craigova interpolacijska lema ne vrijedi za FMT, tj.

> *ako je* $\sigma = \{<, c\}$, *te* P *i* P' *neki unarni relacijski simboli, tada postoje* $\sigma \cup \{P\}$*–rečenica* A *i* $\sigma \cup \{P'\}$*–rečenica* B *tako da vrijedi* $A \models_{fin} B$, *ali ne postoji* σ*–rečenica* C *tako da vrijedi* $A \models_{fin} C$ *i* $C \models_{fin} B$.

Łos, Tarskijev teorem ne vrijedi za FMT, tj.

> *postoji rečenica koja je očuvana za podmodele (na konačnim strukturama!) a nije ekvivalentna (na konačnim strukturama!) univerzalnoj rečenici.*

Gurevich i Shelah su dali prvi primjer jedne takve rečenice. Andréka, van Benthem i Németi su 1995. dokazali da Łos, Tarskijev teorem ne vrijedi za FO^s, za $s \geq 3$. Grädel i Rosen su 1999. dokazali da Łos, Tarskijev teorem ne vrijedi za FO^2.

Birkhoffov teorem ne vrijedi za FMT. Za logiku prvog reda on glasi:

> *Neka je σ neka signatura i $\mathcal{K}$ neka klasa σ–struktura. Tada je ekvivalentno:*
>
> *a) klasa $\mathcal{K}$ je zatvorena za Kartezijeve produkte, podmodele i homomorfne slike;*
> *(odnosno, $\mathcal{K}$ je mnogostrukost, tj. $\mathcal{K} = HSP(\mathcal{K})$).*
>
> *b) klasa $\mathcal{K}$ je definabilna sa skupom rečenica oblika $\forall\vec{x}\varphi$, gdje je φ atomarna formula.*

(Primijetimo: ako σ sadrži samo funkcijske simbole tada tvrdnja b) zapravo govori da je klasu struktura $\mathcal{K}$ moguće definirati pomoću nekog skupa jednakosti). Interesantno je primijetiti da se ne zahtijeva da je klasa $\mathcal{K}$ definabilna u logici prvog reda. Zatim, Birkhoffov dokaz ne koristi teorem kompaktnosti.

Ehrenfeuchtove igre

Znamo da općenito vrijedi da $\mathfrak{M} \simeq \mathfrak{N}$ povlači $\mathfrak{M} \equiv \mathfrak{N}$, te da obrat ne vrijedi (npr. $(\mathbb{R}, <) \equiv (\mathbb{Q}, <)$.) Pokušava se "što više izvući" iz činjenice $\mathfrak{M} \equiv \mathfrak{N}$. Iz tog razloga se definiraju razne vrste oslabljenih izomorfizama i oslabljenih verzija elementarne ekvivalencije. Ponekad je teško opisati relaciju elementarne ekvivalencije, tj. ispitati vrijedi li $\mathfrak{M} \equiv \mathfrak{N}$. Iz tog razloga promatraju se Ehrenfeuchtove igre.
Radi jednostavnijeg izlaganja i zapisa sada promatramo signaturu σ koja od nelogičkih simbola sadrži samo simbol za jednakost i jedan dvomjesni relacijski simbol R.
Zatim, pretpostavljamo da su sve promatrane strukture **normalne**.

Neka su $\mathfrak{M} = (M, R_M)$ i $\mathfrak{N} = (N, R_N)$ dvije σ–strukture. Svaku konačnu injekciju iz M u N koja čuva relacije R_M i R_N nazivamo **lokalni izomorfizam**.

Propozicija 1.215. *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture. Neka je $f : S \subseteq M \to N$ proizvoljna funkcija. Sljedeće tvrdnje su ekvivalentne:*

a) funkcija f je lokalni izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$

b) za svaku atomarnu formulu $A(x_1, \ldots, x_n)$ i sve $s_1, \ldots, s_n \in S$ vrijedi:

$$\mathfrak{M} \models A[s_1, \ldots, s_n] \text{ ako i samo ako } \mathfrak{N} \models A[f(s_1), \ldots, f(s_n)]$$

(naveli smo općeniti slučaj; u našem slučaju jedine atomarne formule su oblika $R(x_i, x_j)$ i $x_i = x_j$)

c) za svaku otvorenu formulu $F(x_1, \ldots, x_n)$ i sve $s_1, \ldots, s_n \in S$ vrijedi:

$$\mathfrak{M} \models F[s_1, \ldots, s_n] \text{ ako i samo ako } \mathfrak{N} \models F[f(s_1), \ldots, f(s_n)]$$

d) f je izomorfizam podmodela od $\mathfrak{M}$ koji je generiran sa S i podmodela od $\mathfrak{N}$ koji je generiran sa $Rng(f)$.

Napomena 1.216. *a) prazno preslikavanje je lokalni izomorfizam (signatura ne smije sadržavati konstantske simbole!);*

b) svaki konačni dio izomorfizma je lokalni izomorfizam;

c) kompozicija lokalnih izomorfizama je lokalni izomorfizam.

Definicija 1.217. *(***Ehrenfeuchtova igra***)*
Svake dvije σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ zajedno s prirodnim brojem $n \in \mathbb{N}$ određuju Ehrenfeuchtovu igru duljine n između struktura $\mathfrak{M}$ i $\mathfrak{N}$. Eherenfeuchtovu igru između struktrua $\mathfrak{M}$ i $\mathfrak{N}$ igraju dva igrača, **Spoiler** *i* **Duplikator** *naizmjence, dok svaki ne napravi n poteza. Na početku Spoiler bira jedan element iz jednog od modela, i nakon njega Duplikator bira jedan element iz drugog modela. Ta dva elementa čine jedan par. Nakon toga ponavlja se postupak. Spoiler bira iz jednog od modela i za njim i Duplikator, i tako sve dok ne naprave n poteza, odnosno dok ne odrede n parova (ne nužno međusobno različitih). Na kraju igre, tih n parova čine konačnu relaciju između modela $\mathfrak{M}$ i $\mathfrak{N}$. Duplikator pobjeđuje u igri ako je dobivena relacija lokalni izomorfizam. U suprotnom definiramo da pobjeđuje Spoiler.*

Primijetimo: Spoiler pokušava u n poteza naglasiti razliku između struktura, a Duplikator pokušava te razlike "sakriti".

Napomena 1.218. *1. Ponavljanje poteza nije zabranjeno, ali za Spoilera nije pametno.*

2. Nekad je vidljivo da je Spoiler pobijedio i prije kraja igre. No, da bi Duplikator pobijedio u nekoj igri moraju se odigrati svi potezi.

3. Igra se može igrati i ako je jedna od struktura prazna. U tom slučaju igrač koji nema što izabrati gubi.

Primjer 1.219. *1.* $\mathfrak{M} = (\mathbb{Z}, <)$ *i* $\mathfrak{N} = (\mathbb{R}, <)$, *te je* $n = 3$. *Igra je zadana sljedećom tablicom*

	Spoiler	*Duplikator*	*Spoiler*	*Duplikator*	*Spoiler*	*Duplikator*
$\mathbb{Z}$		*2*	*0*			*5*
$\mathbb{R}$	*e*			*3*	π	

Primijetite da je već nakon drugog poteza jasno da je Spoiler pobijedio, jer imamo: $0 < 2$ *i* $3 = f(0) > f(2) = e$.

2. Opet neka je $\mathfrak{M} = (\mathbb{Z}, <)$ *i* $\mathfrak{N} = (\mathbb{R}, <)$, *te je* $n = 3$. *Igra je zadana sljedećom tablicom*

	Spoiler	*Duplikator*	*Spoiler*	*Duplikator*	*Spoiler*	*Duplikator*
$\mathbb{Z}$		*2*	*0*			*5*
$\mathbb{R}$	*e*			*0*	π	

U ovoj igri je Duplikator pobijedio.

3. U svakoj igri duljine nula pobjeđuje Duplikator (nema konstantskih simbola!).

Strategija za nekog igrača je pravilo koje mu govori koji potez odigrati u svakom trenutku igre kada je njegov red za potez. **Pobjednička strategija** za nekog igrača za zadane strukture i broj poteza, je strategija koja ga vodi do pobjede u svakoj igri između tih struktura u danom broju poteza.

Oznake:

a) $D(\mathfrak{M}, \mathfrak{N}, n)$ označava da u svakoj igri s n poteza između struktura $\mathfrak{M}$ i $\mathfrak{N}$ Duplikator ima pobjedničku strategiju

b) $S(\mathfrak{M}, \mathfrak{N}, n)$ označava da u svakoj igri s n poteza između struktura $\mathfrak{M}$ i $\mathfrak{N}$ Spoiler ima pobjedničku strategiju

Lema 1.220. *Neka su* $\mathfrak{M}, \mathfrak{N}$ *i* $\mathfrak{A}$ *neke* σ*–strukture, te neka je* $n \in \mathbb{N}$ *proizvoljan. Tada vrijedi:*

a) ako $D(\mathfrak{M}, \mathfrak{N}, n)$ *tada za svaki* $m \leq n$ *vrijedi* $D(\mathfrak{M}, \mathfrak{N}, m)$

b) ako $D(\mathfrak{M}, \mathfrak{N}, n)$ *tada* $D(\mathfrak{N}, \mathfrak{M}, n)$

c) ako $\mathfrak{M} \simeq \mathfrak{N}$ *tada za svaki* $m \in \mathbb{N}$ *vrijedi* $D(\mathfrak{M}, \mathfrak{N}, m)$

d) ako $D(\mathfrak{M}, \mathfrak{N}, n)$ *i* $D(\mathfrak{N}, \mathfrak{A}, n)$ *tada* $D(\mathfrak{M}, \mathfrak{A}, n)$

Propozicija 1.221. *Neka struktura $\mathfrak{M}$ ima točno n $(n \in \mathbb{N})$ elemenata, te neka je $\mathfrak{N}$ proizvoljna struktura. Tada vrijedi:*

a) ako $D(\mathfrak{M}, \mathfrak{N}, n)$ tada je strukturu $\mathfrak{M}$ moguće smjestiti u strukturu $\mathfrak{N}$

b) ako $D(\mathfrak{M}, \mathfrak{N}, n+1)$ tada $\mathfrak{M} \simeq \mathfrak{N}$

Determinirane igre su one igre u kojima uvijek neki igrač mora pobijediti.

Teorem o determiniranosti Ehrenfeuchtovih igara.
Za svake dvije σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$, te svaki $n \in \mathbb{N}$, postoji pobjednička strategija za jednog igrača za svaku Ehrenfeuchtovu igru između struktura $\mathfrak{M}$ i $\mathfrak{N}$ u n poteza.

Primjer 1.222. *Promotrimo opet $\mathfrak{M} = (\mathbb{Z}, <)$ i $\mathfrak{N} = (\mathbb{R}, <)$, te je $n = 3$. Igra je zadana sljedećom tablicom*

	Spoiler	*Duplikator*	*Spoiler*	*Duplikator*	*Spoiler*	*Duplikator*
$\mathbb{Z}$		*2*	*1*			*???*
$\mathbb{R}$	e			x	$x < y < e$	

Spoiler je u drugom potezu izabrao broj $1 \in \mathbb{Z}$ čime je osigurao pobjedu. Duplikator u drugom potezu mora birati neki broj $x \in \mathbb{R}$ koji je manji od e. Tada u trećem potezu Spoiler bira neki broj $y \in \mathbb{R}$ koji je između x i e. Pošto ne postoji cijeli broj između 1 i 2, Duplikator u trećem potezu više ne može sačuvati lokalni izomorfizam. Dakle, vrijedi $S(\mathfrak{M}, \mathfrak{N}, 3)$.

Kako bismo dali još neke primjere igara u kojima pojedini igrač ima pobjedničku strategiju, uvodimo sljedeće oznake za linearno uređene skupove: $L_k = (\{1, \ldots, k\}, <$), za svaki $k \in \mathbb{N}$, $\omega = (\mathbb{N}, <)$, $\zeta = (\mathbb{Z}, <)$, $\eta = (\mathbb{Q}, <)$ i $\lambda = (\mathbb{R}, <)$.

Primjer 1.223. *Vrijedi:*

- $S(\omega, \zeta, 3)$ *(jer $\mathbb{N}$ ima najmanji element, a $\mathbb{Z}$ nema)*
- $S(\omega, \eta, 3)$ *(jer je skup $\mathbb{Q}$ je gust)*
- $D(\omega, \omega + \omega, 3)$; $S(L_6, L_7, 3)$
- $S(\omega + L_1 + \omega^*, \omega + L_2 + \omega^*, 3)$
- $D(L_7, \omega + \omega^*, 3)$; $D(\omega, \omega + \zeta, 3)$
- *Za svaki $n \in \mathbb{N}$ vrijedi $D(\lambda, \eta, n)$*

- *Ako su A i B beskonačni skupovi tada za svaki $n \in \mathbb{N}$ vrijedi $D(\mathcal{P}(A), \mathcal{P}(B), n)$*
- *Ako $|A|,\ |B| \geq 2^n$ tada $D(\mathcal{P}(A), \mathcal{P}(B), n)$*
- *Ako $k, m \geq 2^n - 1$ tada vrijedi $D(L_k, L_m, n)$*

Za dokaz Ehrenfeuchtovog teorema ključna je lema o raslojavanju. Ako je $\mathfrak{M}$ neka σ–struktura i $a \in |\mathfrak{M}|$ proizvoljan, tada s $(\mathfrak{M}, a)$ označavamo $\sigma \cup \{\overline{a}\}$–ekspanziju strukture $\mathfrak{M}$ ($\overline{a}$ je novi konstantski simbol), kod koje je interpretacija od $\overline{a}$ jednaka a.
U lemi koja slijedi, te u Ehrenfeuchtovom teoremu promatramo igre između struktura oblika $(\mathfrak{M}, a)$ i $(\mathfrak{N}, b)$. Važno je samo napomenuti da svaki lokalni izomorfizam između takvih struktura mora element a preslikavati u b (jer su to interpretacije istog (!) konstantskog simbola).

Lema 1.224. *(***Lema o raslojavanju***)*
Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ–strukture, te $n \in \mathbb{N}$ proizvoljan. Tada vrijedi:

$$D(\mathfrak{M}, \mathfrak{N}, n+1) \quad \textit{ako i samo ako} \quad \begin{cases} (\forall a \in M)(\exists b \in N)\ D((\mathfrak{M}, a),\ (\mathfrak{N}, b), n) \\ (\forall b \in N)(\exists a \in M)\ D((\mathfrak{M}, a),\ (\mathfrak{N}, b), n) \end{cases}$$

Kvantifikatorski rang formule, u oznaci $qr(F)$, definirali smo kao maksimalan broj uklopljenih kvantifikatora (vidi definiciju 1.24. na strani 13).

U lemi 1.28. dokazali smo da ako imamo fiksirani konačan skup varijabli, tada za svaki $n \in \mathbb{N}$ postoji samo konačno mnogo, do na logičku ekvivalenciju, rečenica čiji je kvantifikatorski rang manji od n.
Za σ–strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su n–**elementarno ekvivalentne**, te pišemo $\mathfrak{M} \equiv_n \mathfrak{N}$, ako za sve σ–rečenice F, za koje imamo $qr(F) \leq n$, vrijedi: $\mathfrak{M} \models F$ ako i samo ako $\mathfrak{N} \models F$.

Teorem 1.225. *(***Ehrenfeuchtov teorem***)*
Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ–strukture, te $n \in \mathbb{N}$ proizvoljan. Tada vrijedi:

$$D(\mathfrak{M}, \mathfrak{N}, n) \textit{ ako i samo ako } \mathfrak{M} \equiv_n \mathfrak{N}.$$

Fraisséov teorem (vidi teorem 1.30. na strani 16) je zapravo algebarska verzija Ehrenfeuchtovog teorema. Razmatraju se i druge igre: igre s kamenčićima, igre dostiživosti, igre parnosti, ...

Deskriptivna teorija složenosti

Teorija deskriptivne složenosti omogućava definicije klasa složenosti koje su nezavisne o izboru modela izračunavanja ili programskog jezika. Centralni program deskriptivne teorije složenosti jest uspostava veze između računske složenosti i logičke definabilnosti. Pokazuje se kako je ta veza daleko dublja od one koju možemo dobiti samom analizom složenosti algoritama za verifikaciju modela za pojedinu logiku. Osnovni cilj u toj analizi jest povezati istaknute klase složenosti s logikom (ili logikama) čija se izražajna moć (na svim konačnim strukturama ili nekoj drugoj klasi konačni struktura) u određenom smislu podudara upravo s danom klasom složenosti.

Problem ispunjivosti za neku logiku $\mathcal{L}$ na nekoj klasi $\mathcal{D}$ struktura (ne nužno iste signature) definiran je na slijedeći način:

> *Za danu rečenicu ψ logike $\mathcal{L}$ potrebno je odrediti postoji li struktura $\mathfrak{A} \in \mathcal{D}$ takva da vrijedi $\mathfrak{A} \models \psi$.*

Problemi SAT i TQBF su primjeri problema ispunjivosti. Pokazalo se da problemi ispunjivosti nisu najvažniji u teoriji konačnih modela.

Središnje mjesto u teoriji konačnih modela zauzima problem verifikacije modela kojeg opisujemo sljedećom definicijom. **Problem verifikacije modela** za logiku $\mathcal{L}$ i klasu struktura $\mathcal{D}$ definiran je na slijedeći način:

> *Za danu rečenicu ψ logike $\mathcal{L}$ i strukturu $\mathfrak{A} \in \mathcal{D}$ potrebno je odrediti vrijedi li $\mathfrak{A} \models \psi$.*

Neka je $\mathcal{L}$ neka logika, $\mathcal{C}$ neka klasa računske složenosti i $\mathcal{D}$ neka klasa konačnih struktura. Kažemo da **logika $\mathcal{L}$ hvata klasu složenosti $\mathcal{C}$ na klasi struktura** $\mathcal{D}$ ako za svaku signaturu σ vrijedi:

1. Za svaku rečenicu $\psi \in \mathcal{L}[\sigma]$ problem verifikacije modela za ψ na $\mathcal{D}[\sigma]$ nalazi se u klasi složenosti $\mathcal{C}$.

2. Za svaku klasu struktura $\mathcal{K} \subseteq \mathcal{D}[\sigma]$ koja se nalazi u klasi složenosti $\mathcal{C}$ postoji rečenica $\psi \in \mathcal{L}[\sigma]$ takva da je

$$\mathcal{K} = \{\mathfrak{M} \in \mathcal{D}[\sigma] : \mathfrak{A} \models \psi\}$$

Pojam logike je definiran u poglavlju *Apstraktna teorija modela*. Tamo su i uvedene oznake $L[\sigma]$ i $\mathcal{D}[\sigma]$.

Egzistencijalna formula logike drugog reda, tj. Σ^1_1–formula, je formula oblika

$$\exists R_1 \dots \exists R_n \exists f_1 \dots \exists f_m \ \varphi,$$

gdje je φ formula logike prvog reda.

Primjeri Σ^1_1–formula:

3–obojiv graf:

$$\begin{aligned}\exists R \exists B \exists G \Big(\quad & \forall x (Rx \vee Bx \vee Gx) \wedge \\ & \forall x \Big(\neg(Rx \wedge Bx) \ \wedge \ \neg(Bx \wedge Gx) \wedge \\ & \neg(Rx \wedge Gx) \Big) \wedge \\ & \forall x \forall y \Big(Exy \to (\neg(Rx \wedge Ry) \wedge \\ & \neg(Bx \wedge By) \ \wedge \ \neg(Gx \wedge Gy) \Big) \Big)\end{aligned}$$

Hamiltonov graf:

$$\begin{aligned}\exists R \Big(\quad & R \text{ je linearni uređaj } \wedge \\ & \forall x E(x, x+1) \wedge E(max, min) \Big)\end{aligned}$$

Teorem 1.226. *(***Fagin, 1974.***)*
Logika Σ^1_1 hvata klasu NP na klasi svih konačnih struktura.

Uobičajno je Faginov teorem jednostavno iskazivati u obliku: $\Sigma^1_1 = NP$

Cook, Levinov teorem o NP–potpunosti problema SAT moguće je dobiti kao posljedicu Faginovog teorema.

Korolar 1.227. *Logika Π^1_1 hvata klasu* co*–NP na klasi svih konačnih struktura.*

Korolar 1.228. *Vrijedi: NP=*co*–NP ako i samo ako $\Sigma^1_1 = \Pi^1_1$.*

Teorem 1.229. *(***Grädel***)*
Logike SO–HORN i Σ_1^1–HORN hvataju klasu P na klasi svih uređenih konačnih struktura.

Teorem 1.230. *(***Immerman, Vardi***)*
Logika najmanje fiksne točke LFP hvata klasu P na klasi svih uređenih konačnih struktura.

Teorem 1.231. *(***Abiteboul–Vianu, Vardi***)*
Logika parcijalne fiksne točke PFP hvata klasu PSPACE na klasi svih uređenih konačnih struktura.

Otvoreni problem: Postoji li logika koja hvata klasu P na klasi svih konačnih struktura?
(Ukoliko je odgovor na prethodno pitanje "ne" tada $P \neq NP$)

Dokazi svih navedenih teorema iz teorije konačnih modela, te više detalja i primjera, možete vidjeti u knjigama [9], [11] i [17]. O ovoj temi svakako je zanimljiv članak E. Rosen, *Some aspects of model theory*, Bulletin of Symbolic Logic, 8 (2002). Deskriptivnoj teoriji složenosti posvećena je knjiga [15].

Poglavlje 2

Teorija dokaza

Teorija dokaza ne izučava samo teoreme nekih teorija, odnosno što znamo u toj teoriji, već i kako dolazimo do tih teorema. Najvažnije teme izučavanja (opće) teorije dokaza su:

1. Definicija pojma dokaza
2. Istraživanje strukture dokaza, što uključuje i pitanje egzistencije normalnih formi
3. Način predstavljanja dokaza formalnim zapisima
4. Primjena uvida u strukturu dokaza na druga logička pitanja

Neki istaknuti dijelovi teorije dokaza:

- sistemi prirodne dedukcije
- sistemi sekventi
- rezolucija
- Herbrandov teorem (logičko programiranje)

Mi ćemo se baviti analiziranjem dokaza logike prvog reda, tj. prezentirat ćemo Gentzenov rad iz 1935. godine. Gentzen je dao odgovor u dva koraka:

- prvom analizom Gentzen je pokazao kako se pojam dokaza može definirati uz pomoć formalnog sistema
- dubljom analizom strukture dokaza pokazao je da ih je moguće napisati u vrlo posebnom obliku

2.1 Prirodna dedukcija. Normalizacija

Napomene o pojedinom pravilu sistema prirodne dedukcije i druge detalje možete pročitati u skripti [28].

Definicija 2.1. *Sistem prirodne dedukcije PD klasične logike sudova zadan je sljedećim pravilima izvoda:*

$$\frac{A \wedge B}{A}\ (\wedge E) \qquad \frac{A \wedge B}{B}\ (\wedge E) \qquad \frac{A \quad B}{A \wedge B}\ (\wedge I)$$

$$\frac{A \vee B \quad \begin{array}{c}\overline{A}^{\,n}\\ \vdots\\ C\end{array} \quad \begin{array}{c}\overline{B}^{\,m}\\ \vdots\\ C\end{array}}{C}\ {}_{n,m}(\vee E) \qquad \frac{A}{A \vee B}\ (\vee I) \qquad \frac{B}{A \vee B}\ (\vee I)$$

$$\frac{A \quad \neg A}{\bot}\ (\neg E) \qquad \frac{\neg\neg A}{A}\ (DN) \qquad \frac{\begin{array}{c}\overline{A}^{\,n}\\ \vdots\\ \bot\end{array}}{\neg A}\ {}_{n}(\neg I)$$

$$\frac{A \quad A \to B}{B}\ (\to E) \qquad \frac{\begin{array}{c}\overline{A}^{\,n}\\ \vdots\\ B\end{array}}{A \to B}\ {}_{n}(\to I)$$

$$\frac{A \leftrightarrow B}{A \to B}\ (\leftrightarrow E) \qquad \frac{A \leftrightarrow B}{B \to A}\ (\leftrightarrow E)$$

$$\frac{A \to B \qquad B \to A}{B \leftrightarrow A}\ (\leftrightarrow I)$$

Definicija 2.2. Stablo *je konačan parcijalno uređen skup $(S, <)$ (tj. binarna relacija $<$ je irefleksivna i tranzitivna) koji ima sljedeća dva svojstva:*

a) postoji najmanji element $s_0 \in S$ (taj element nazivamo **korijen***);*

b) za svaki $s \in S$, $s \neq s_0$, postoji jedinstveni konačni niz $s_1, \ldots, s_n \in S$, tako da vrijedi

$$s_0 < s_1 < s_2 < \ldots < s_n = s,$$

te za svaki $i \in \{0, \ldots, n-1\}$ vrijedi da je s_{i+1} neposredni sljedbenik od s_i. (Za $y \in S$ kažemo da je neposredni sljedbenik elementa $x \in S$ ako vrijedi $x < y$ i ne postoji $z \in S$ takav da vrijedi $x < z < y$).

Elemente stabla obično nazivamo **čvorovi**. **Put** je svaki niz čvorova $s_1, \ldots, s_n$ pri čemu je za svaki
$i \in \{1, \ldots, n-1\}$ čvor s_{i+1} neposredni sljedbenik od s_i. Za svaki $s \in S$ parcijalno uređen skup $\{x \in S : s \leq x\}$ nazivamo **podstablo**.

Po definiciji smatramo da je **visina** korijena jednaka jedan. **Visina čvora** s je duljina jedinstvenog puta od s do korijena. **Visina stabla** je maksimum skupa svih visina čvorova, odnosno duljina najdužeg puta u stablu. Neka je S' podstablo od S, te neka je s_0' korijen od S', a s_0 korijen od S. Kažemo da je S' **neposredno podstablo** od S ako je s_0' neposredni sljedbenik od s_0.

Definicija 2.3. Označeno stablo *je uređena trojka $(S, <, f)$ gdje je $(S, <)$ stablo, a*

$$f : S \ \rightarrow \ \mathcal{F} \cup \{\overline{F}^n : F \in \mathcal{F}, \ n \in \mathbb{N}\} \cup \{\bot\}$$

(Sa $\mathcal{F}$ smo označili skup svih formula logike sudova).
Funkciju f nazivamo funkcija označavanja, i govorimo da je čvor $s \in S$ označen sa $f(s)$.

Pojmovi vezani uz stabla kao što su: korijen, list, put, podstablo, visina čvora, visina stabla, neposedno podstablo, ... koriste se i za označena stabla. Tako npr. korijen označenog stabla $(S, <, f)$ je onaj čvor koji je korijen stabla $(S, <)$.

Sada nam je prvi cilj definirati pojam izvoda u sistemu PD. Kako bismo mogli navesti definiciju izvoda u sistemu prirodne dedukcije moramo prvo vrlo pažljivo **uvesti oznake koje ćemo koristiti za označena stabla**. Najčešće ćemo označena stabla označavati sa D, D' i D''. Ako je A formula i $n \in \mathbb{N}$ tada oznake A i $\overline{A}^n$ označavaju stabla koja se sastoje samo od jednog čvora. Sada redom navodimo oznake za označena stabla i pripadna objašnjenja.

D
A

Ovu oznaku koristimo za označeno stablo čiji korijen je označen s formulom A. Smatrat ćemo da ova oznaka i oznaka D označavaju isto označeno stablo. Razlika je jedino što navedena oznaka, za razliku od oznake D, ističe da je korijen označen sa A.

$$\begin{array}{c} D \\ A \\ \hline B \end{array}$$

Ovu oznaku koristimo za označeno stablo čiji je korijen označen sa B, te je jedino neposredno podstablo označeno sa $\frac{D}{A}$.

$$\begin{array}{cc} D & D' \\ A & B \\ \hline \multicolumn{2}{c}{C} \end{array}$$

Ovu oznaku koristimo za označeno stablo s korijenom označenim formulom C, te ima točno dva neposredna podstabla koja su označena sa $\frac{D}{A}$ i $\frac{D'}{B}$.

$$\begin{array}{ccc} D & D' & D'' \\ A & B & C \\ \hline \multicolumn{3}{c}{F} \end{array}$$

Ovo je oznaka za označeno stablo s korijenom označenim formulom F, te ima točno tri neposredna podstabla koja su označena sa $\frac{D}{A}$, $\frac{D'}{B}$ i $\frac{D''}{C}$.

A
D
B

Ovo je oznaka za označeno stablo s korijenom označenim s formulom B, koje može, ali ne mora, imati jedan ili više listova označenih formulom A. Smatrat ćemo da ova oznaka i oznaka D označavaju isto označeno stablo.

$$\begin{array}{c} A \\ D \\ B \\ \\ \hline C \end{array}$$

Ovu oznaku koristimo za označeno stablo čiji je korijen označen sa C, te ima jedno neposredno podstablo. Neki listovi (mo-žda niti jedan, a možda svi) su označeni formulom A.

$$\begin{array}{c} \overline{A}^n \\ D \\ B \\ \hline C \end{array}$$

Ovu oznaku koristimo za označeno stablo koje je kao stablo jednako onom koje smo označili s prethodno navedenom oznakom. Razlika je samo da su neki listovi (možda niti jedan, a možda svi) označeni formulom $\overline{A}^n$.

Definicija 2.4. *Skup X svih izvoda sistema prirodne dedukcije je najmanji skup koji sadrži sva označena stabla s točno jednim čvorom, te je skup X zatvoren*

na sljedeće operacije:

(1) $\overset{D}{A}$ *i* $\overset{D'}{B}$ *pripadaju* X*, tada i označeno stablo*

$$\dfrac{\overset{D}{A} \qquad \overset{D'}{B}}{A \wedge B}$$

pripada skupu X*.*

(2) $\overset{D}{A \wedge B}$ *pripada* X*, tada i označena stabla*

$$\dfrac{\overset{D}{A \wedge B}}{A} \quad i \quad \dfrac{\overset{D}{A \wedge B}}{B}$$

pripadaju skupu X*;*

(3) *Ako označeno stablo* $\overset{D}{A}$ *pripada* X*, tada i* $\dfrac{\overset{D}{A}}{A \vee B}$ *pripada* X*.*

Ako označeno stablo $\overset{D}{B}$ *pripada* X*, tada i* $\dfrac{\overset{D}{B}}{A \vee B}$ *pripada* X*.*

(4) Ako označena stabla

$$\begin{array}{lll} \overset{D}{A \vee B}, & \overset{A}{\underset{C}{D'}}, & \overset{B}{\underset{C}{D''}} \end{array}$$

pripadaju skupu X

tada i označeno stablo

$$\dfrac{\overset{D}{A \vee B} \qquad \overset{\overline{A}^n}{\underset{C}{D'}} \qquad \overset{\overline{B}^m}{\underset{C}{D''}}}{C}$$

pripada skupu X*;*

(5) *Ako označena stabla* $\overset{D}{A}$ *i* $\overset{D'}{A \to B}$ *pripadaju skupu* X *tada i*

$$\dfrac{\overset{D}{A} \qquad \overset{D'}{A \to B}}{B}$$

pripada skupu X*;*

(6) Ako označeno stablo

$$\begin{array}{l} A \\ D \\ B \end{array} \quad \textit{pripada skupu } X \textit{ tada i } \quad \dfrac{\begin{array}{c}\overline{A}^n \\ D \\ B\end{array}}{A \to B} \quad \textit{pripada skupu } X;$$

(7) $$\textit{Ako } \begin{array}{c} D \\ \neg\neg A \end{array} \quad \textit{pripada } X \textit{ tada i } \quad \dfrac{\begin{array}{c} D \\ \neg\neg A \end{array}}{A} \quad \textit{pripada skupu } X;$$

(8) $$\textit{Ako } \begin{array}{c} D \\ A \end{array} \; i \; \begin{array}{c} D' \\ \neg A \end{array} \textit{ pripadaju } X \textit{ tada i}$$

$$\dfrac{\begin{array}{c} D \\ A \end{array} \qquad \begin{array}{c} D' \\ \neg A \end{array}}{\bot} \quad \textit{pripada } X;$$

(9) $$\textit{Ako } \begin{array}{l} A \\ D \\ \bot \end{array} \textit{ pripada } X \textit{ tada i } \dfrac{\begin{array}{c}\overline{A}^n \\ D \\ \bot\end{array}}{\neg A} \textit{ pripada } X;$$

(10) $$\textit{Ako } \begin{array}{c} D \\ A \leftrightarrow B \end{array} \textit{ pripada } X \textit{ tada i } \dfrac{\begin{array}{c} D \\ A \leftrightarrow B \end{array}}{A \to B} \; i \; \dfrac{\begin{array}{c} D \\ A \leftrightarrow B \end{array}}{B \to A} \textit{ pripadaju } X;$$

(11) $$\textit{Ako } \begin{array}{c} D \\ A \to B \end{array} \; i \; \begin{array}{c} D' \\ B \to A \end{array} \textit{ pripadaju } X \textit{ tada i}$$

$$\dfrac{\begin{array}{c} D \\ A \to B \end{array} \quad \begin{array}{c} D' \\ B \to A \end{array}}{A \leftrightarrow B} \quad \textit{pripada skupu } X.$$

Svako označeno stablo $D \in X$ nazivamo **izvod**. *Skup S svih formula kojima su označeni listovi izvoda D, koje nisu privremene pretpostavke zatvorene nekim hipotetičkim pravilom, nazivamo* **skup pretpostavki** *izvoda D. Ako je korijen izvoda D označen s formulom F, a S je skup pretpostavki, tada govorimo još da je* **formula** F **izvediva iz skupa pretpostavki** S. *To označavamo sa $S \vdash_{PD} F$. Obično ćemo kratko pisati $S \vdash F$ ako nema mogućnosti zabune. Ako vrijedi $S \vdash F$, te je S' neki* **nadskup od** S **tada po definiciji smatramo** *da vrijedi $S' \vdash F$. Za formulu F kažemo da je* **teorem** *sistema prirodne dedukcije ako je izvediva iz praznog skupa. To ćemo zapisivati kao $\vdash_{PD} F$, tj. kratko $\vdash F$. Tada dani izvod nazivamo i* **dokaz** *u sistemu prirodne dedukcije.*

Napomena 2.5. *Ako prilikom korištenja nekog hipotetičkog pravila zatvaramo neku privremenu pretpostavku nije nužno zahtijevati da je neki list izvoda označen s tom privremenom pretpostavkom. Promotrimo tu situaciju prilikom korištenja pravila* $(\to I)$*. Neka je* $\frac{D}{B}$ *neki izvod formule* B *iz skupa pretpostavki* S*. Pomoću tog izvoda možemo konstruirati izvod za formulu* $A \to B$ *iz skupa* S*. Neka je* n *najmanji prirodan broj koji je veći od svih brojeva koji označavaju privremene pretpostavke u izvodu* D*. U izvodu* D *uz korijen* B *dodajemo sljedeće:*

$$\dfrac{\dfrac{\dfrac{\overline{A}^{\,n} \qquad B}{A \wedge B}(\wedge I)}{B}(\wedge E)}{A \to B}{}_{n}(\to I)$$

Ovaj primjer nam ilustrira da je u izvodima dozvoljeno zatvaranje privremene pretpostavke iako ta pretpostavka nije prije uvedena. Odnosno navedeni izvod možemo kraće zapisati kao:

$$\dfrac{\begin{array}{c} D \\ B \end{array}}{A \to B}$$

Na analogan način bi postupili i kod preostala dva hipotetička pravila, tj. kod $(\vee E)$ *i* $(\neg I)$*.*

Teorem 2.6. *(Teorem adekvatnosti za sistem prirodne dedukcije)*
Neka je S *skup formula, i* F *neka formula. Ako vrijedi* $S \vdash_{PD} F$ *tada vrijedi* $S \models F$*. Posebno imamo da je svaki teorem sistema prirodne dedukcije valjana formula.*

Teorem adekvatnosti se standardno dokazuje indukcijom po visini stabla izvoda.

Korolar 2.7. *Sistem prirodne dedukcije je konzistentan, tj. ne postoji formula* A *tako da su* A *i* $\neg A$ *teoremi sistema prirodne dedukcije.*

Teorem 2.8. *(Teorem potpunosti za sistem* PD*)*
Ako je A *valjana formula tada je* A *teorem sistema* PD*.*

Ovaj teorem se standardno dokazuje primjenom Lindenbaumove leme i leme o istinitosti.

Sistem prirodne dedukcije za logiku prvog reda dobivamo dodavanjem sistemu PD pravila za kvantifikatiore.

$$\frac{A(x)}{\forall x A(x)}\ (\forall I)$$ pri čemu x nije slobodna varijabla niti jedne nezatvorene privremene pretpostavke o kojoj ovisi izvod formule $A(x)$;

$$\frac{\forall x A(x)}{A(t/x)}\ (\forall E)$$ gdje je t proizvoljan term koji je slobodan za varijablu x u formuli $A(x)$;

$$\frac{A(t/x)}{\exists x A(x)}\ (\exists I)$$ gdje je t proizvoljan term koji je slobodan za varijablu x u formuli $A(x)$;

$$\frac{\exists x A(x) \qquad \begin{array}{c}\overline{A(x)}^{n}\\ \vdots \\ B\end{array}}{B}\ (\exists E)$$ pri čemu varijabla x nema slobodnih nastupa u formuli B, te niti u jednoj pretpostavci u izvodu formule B, osim možda u formuli $A(x)$.

Na analogan način bi se proširile definicije pojmova iz logike sudova kao što su označeno stablo i izvod.

Primjer 2.9. *Neka je A formula koja ne sadrži slobodnih nastupa varijable x. Za ilustraciju ćemo dokazati da je formula*

$$\forall x(A \to B(x)) \to (A \to \forall x B(x))$$

teorem sistema prirodne dedukcije logike prvog reda.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\forall x(A \to B(x))}^{1}}{A \to B(x)}(\forall E) \qquad \overline{A}^{2}}{B(x)}(\to E)}{\forall x B(x)}(\forall I)}{A \to \forall x B(x)}(\to I)}{\forall x(A \to B(x)) \to (A \to \forall x B(x))}(\to I)$$

Za **sistem prirodne dedukcije logike prvog reda vrijedi teorem adekvatnosti**, tj. svaki teorem je valjana formula. Može se dokazati da vrijedi i obrat, tj. **teorem potpunosti**. Sada ćemo se baviti **normalizacijom izvoda** sistema prirodne dedukcije. Sve ispuštene detalje o normalizaciji možete pročitati u knjizi [27].

Promotrimo prvo sljedeći izvod.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{A\wedge C}^{1}}{A}(\wedge E) \quad \dfrac{\overline{A\to B}^{2}}{B}(\to E) \quad \dfrac{\overline{A\wedge C}^{1}}{C}(\wedge E)}{B\to C}(\to I)}{C}(\to E)}{(A\to B)\to C}(\to I)}{(A\wedge C)\to((A\to B)\to C)}(\to I)$$

Posebno uočite formulu $B \to C$ u prethodnom izvodu. Ta formula je prvo konkluzija jednog pravila introdukcije, a onda je odmah premisa pravila eliminacije. Takve situacije bi svakako željeli izbjeći u izvodima.

Formule napisane iznad crte u nekom pravilu izvoda nazivamo **premise**, a formulu napisanu neposredno ispod crte nazivamo **konkluzija**. U svakom pravilu eliminacije veznika premisu koja sadrži veznik na koji primjenjujemo pravilo eliminacije (i to baš onaj nastup veznika koji eliminiramo) nazivamo **glavna premisa**, a ostale premise nazivamo sporedne premise. Kao primjer promotrimo pravilo $(\to I)$.

$$\dfrac{A \quad A \to B}{B}\ (\to E)$$

Formula $A \to B$ je glavna premisa, a A je sporedna premisa (ako čak i sadrži veznik $\to$).

Formulu φ u nekom izvodu nazivamo **formulom reza** ako je φ prvo konkluzija nekog pravila introdukcije za neki veznik V, a nakon toga (ne nužno odmah) glavna premisa nekog pravila eliminacije za isti veznik V. Kažemo da se u nekom izvodu pojavljuje **rez** ako postoji u tom izvodu barem jedna formula reza. Za izvod D kažemo da je u **normalnoj formi** ako ne sadrži niti jedan rez. **Teorem o normalizaciji** govori da se svaki izvod može normalizirati. Posljedica toga je da za svaki izvod postoji jedinstvena normalna forma. Iako se na prvi pogled tvrdnja teorema normalizacije može činiti očita, njen dokaz je relativno zahtjevan.

Jedan izvod formule $(A \wedge C) \to ((A \to B) \to C)$ može se bez reza zapisati ovako:

$$\dfrac{\dfrac{\dfrac{\overline{A \wedge C}^{1}}{C}(\wedge E)}{(A \to B) \to C}(\to I)}{(A \wedge C) \to ((A \to B) \to C)}(\to I)$$

Uočite da nismo naveli da je formula $A \to B$ privremena pretpostavka, iako smo je koristilli prilikom prve primjene pravila $(\to I)$. U napomeni prije smo bili naveli zašto tako možemo postupati.

Sada nam je cilj opisati skicu dokaza teorema normalizacije. U tu svrhu promatrat ćemo logiku prvog reda koja od logičkih simbola sadrži samo

$$\wedge,\ \to,\ \bot,\ \forall$$

Simbol negacije $\neg$ koristimo kao pokratu, tj. formula $\neg A$ je pokrata za $A \to \bot$. U tom smislu koristimo i sljedeće pravilo koje označavamo sa (RAA).

$$\dfrac{\begin{array}{c}\overline{\neg A}^{\,n}\\ \vdots \\ \bot\end{array}}{A}\ {}_{n}(RAA)$$

Umjesto već navedenog pravila $(\forall I)$ koristit ćemo sljedeće pravilo:

$$\dfrac{A}{\forall x A(x/y)}(\forall I)$$

pri čemu y nije slobodna varijabla niti jedne nezatvorene privremene pretpostavke o kojoj ovisi izvod formule $A(x)$, te je varijabla x slobodna za varijablu y u formuli A.

Lako je vidjeti da je "staro" pravilo introdukcije kvantifikatora $\forall$ specijalan slučaj upravo navedenog.

Umjesto "eliminacijom reza izvod prevodimo" koristit ćemo samo kratko riječ "transformacijom". Lako je opisati sve moguće slučajeve transformacija: za veznik $\wedge$, za veznik $\rightarrow$ i kvantifikator $\forall$. Nije odmah jasno da je transformacija s kvantifikatorom dozvoljena. Tu se kriju najveći tehnički problemi prilikom dokaza teorem normalizacije.

$$\text{Ako je } \begin{array}{c} D \\ A \end{array} \text{ neki izvod tada općenito } \begin{array}{c} D(y/x) \\ A(y/x) \end{array} \text{ ne mora biti izvod.}$$

Lema 2.10. *U svakom izvodu vezane varijable se mogu preimenovati tako da niti jedna varijabla u izvodu ne nastupa istovremeno kao vezana i kao slobodna.*

Dokaz se provodi indukcijom po visini izvoda.

Lema 2.11. *Nakon odgovarajućih preimenovanja varijabli transformacije na veznicima $\wedge$ i $\rightarrow$, te na kvantifikatoru $\forall$ daju kao rezultat opet izvode.*

Ako su D i D' izvodi tada sa $D >_1 D'$ označavamo da je izvod D' transformacija izvoda D. Sa $D > D'$ označavamo činjenicu da postoji konačan niz izvoda $D_0, D_1, \ldots, D_n$ tako da vrijedi

$$D = D_0 >_1 D_1 >_1 \ldots >_1 D_n = D'$$

Definicija 2.12. *Neka je D neki izvod. Ako ne postoji izvod D' tako da vrijedi $D >_1 D'$ tada kažemo da je D* **normalizirani izvod**. *Za izvod D kažemo da se* **može normalizirati** *ako postoji normalizirani izvod D' tako da vrijedi $D > D'$. Kažemo da relacija $>$ ima* **jako normalizacijsko svojstvo** *ako ne postoji beskonačan niz transformacija za neki izvod. Kažemo da relacija $>$ ima* **slabo normalizacijsko svojstvo** *ako se svaki izvod može normalizirati.*

Lema 2.13. *Pravila izvoda $(\neg I)$ i (RAA) se mogu ograničiti samo na slučajeve u kojima je konkluzija atomarna formula.*

Dokaz se provodi indukcijom po visini stabla izvoda. U koraku indukcije promatraju se svi oblici formula koje mogu biti konkluzije pravila $(\neg I)$, odnosno (RAA).

Definicija 2.14. *Neka je D neki izvod.*

a) **Rang reza** *u izvodu D je složenost pripadne formule reza.*

b) Formulu reza u izvodu D koja ima maksimalnu složenost nazivamo **maksimalna formula reza**.

Uvodimo sljedeće oznake:

- *Ako je φ neka formula tada sa $k(\varphi)$ označavamo njenu složenost.*
- $d = \max\{k(\varphi) : \varphi$ *je formula reza u izvodu* $D\}$, *pri čemu definiramo* $\max \emptyset = 0$
- $n =$ *broj maksimalnih formula reza*
- $r(D) = (d, n)$, *te* $r(D)$ *nazivamo rang reza izvoda* D

Ako izvod nema rezova tada je $r(D) = (0, 0)$. Ideja dokaza teorema normalizacije je sistematski smanjivati rang izvoda dok ne eliminiramo sve rezove. Uređaj na rangu reza izvoda definiran je **leksikografski**, tj.

$$(d, n) < (d', n') \Leftrightarrow d < d' \vee (d = d' \wedge n = n')$$

Lema 2.15. *Neka je D izvod u kojem nastupa rez na samom kraju. Neka je rang tog reza jednak m, a rangovi drugih reza u tom izvodu neka su strogo manji od m. Tada transfomacijom izvoda D na tom rezu dobivamo izvod čiji svi rezovi imaju rang strogo manji od m.*

Lema 2.16. *Neka je D neki izvod. Ako je $r(d) > (0, 0)$ tada postoji izvod D' takav da je $D' >_1 D$ i $r(D) < r(D')$.*

Teorem 2.17. *(***Slaba normalizacija***)*
Svaki se izvod može normalizirati.

Teorem 2.18. *(***Svojstvo podformulnosti***)*
Neka je D normalizirani izvod za $\Gamma \vdash \varphi$. Tada za svaku formulu ψ u izvodu D vrijedi barem jedno od sljedećeg:

- *ψ je neka podformula od φ*
- *ψ je podformula neke formule iz skupa Γ*
- *podformula neke pretpostavke koja je poništena primjenom pravila (RAA)*

Korolar 2.19. *Logika prvog reda je konzistentna, tj. ne postoji izvod za $\perp$.*

Teorem 2.20. *(***Jaka normalizacija***)*
Svaki niz transformacija vodi na normalni oblik.

Teorem 2.21. *(***Church–Rosserovo svojstvo***)*
Ako $D \geq D_1$ i $D \geq D_2$ tada postoji izvod D_3 tako da vrijedi $D_1 \geq D_3$ i $D_2 \geq D_3$.

2.2 Sistem sekvenata

Ako je stablo izvoda u sistemu prirodne dedukcije veliko ponekad može biti vrlo zamorno provjeriti je li neka formula pretpostavka, "otvorena" privremena pretpostavka ili pak je zatvorena privremena pretpostavka. Iz tog razloga promatra se sistem kod kojeg se **stalno prepisuju pretpostavke**.

Već kod sistema prirodne dedukcije bili smo naglasili da ako je D neki izvod tada općenito $D(t/x)$ ne mora biti izvod. Iz tog razloga definiramo da alfabet logike prvog reda sadrži dvije vrste varijabli:

- $a, b, c, \ldots$ slobodne varijable
- $x, y, z, \ldots$ vezane varijable

(Slobodne varijable se ne mogu kvantificirati, a vezane varijable ne mogu nastupiti slobodno u formulama). Tada se **termi** mogu graditi samo iz slobodnih varijabli i funkcijskih simbola. **Pseudotermi** se grade pomoću slobodnih i vezanih varijabli, te funkcijskih simbola. Kod **pseudoformula** i vezane varijable mogu nastupiti slobodne. Prilikom definicije **formule** zahtijeva se da atomarne fomule sadrže samo terme, te ako je $F(x)$ pseudoformula (koja može sadržavati i pseudoterme s varijablom x) tada su $\forall x F(x)$ i $\exists x F(x)$ formule. Uočite da je ovakvim razlikovanjem varijabli nepotrebno razmatrati je li term slobodan za neku varijablu u formuli. Mi se nećemo detaljnije baviti problem kada iz izvoda D supstitucijom varijable ponovno dobivamo izvod. Želimo samo naglasiti da ako ne razlikujemo varijable tada postoje valjane formule za koje na postoji izvod bez reza (Fefermanov primjer: $P(x, y) \to \exists y \exists x P(y, x)$.)

Sa Γ i Δ označavamo konačne nizove formula. Ako je A neka formula tada sa Δ, A kratko označavamo niz koji osim formula niza Δ sadrži i formulu A. Izraze oblika $\Gamma \to \Delta$ nazivamo **sekvente**. Intuitivno $\Gamma \to \Delta$ znači da "$\bigwedge \Gamma$ povlači $\bigvee \Delta$".

Gentzenov klasični sistem sekvenata LK zadan je s tri grupe pravila:

- strukturna pravila
- pravila o identitetu
- logička pravila

Strukturna pravila sistema LK:

- **slabljenje**

$$\frac{\Gamma \to \Delta}{\Gamma \to A, \Delta} \qquad \frac{\Gamma \to \Delta}{\Gamma, A \to \Delta}$$

- **kontrakcija**

$$\frac{\Gamma, A, A \to \Delta}{\Gamma, A \to \Delta} \qquad \frac{\Gamma \to A, A, \Delta}{\Gamma \to A, \Delta}$$

- **permutacija**

$$\frac{\Gamma_1, A, B, \Gamma_2 \to \Delta}{\Gamma_1, B, A, \Gamma_2 \to \Delta} \qquad \frac{\Gamma \to \Delta_1, A, B, \Delta_2}{\Gamma \to \Delta_1, B, A, \Delta_2}$$

Pravila o identitetu sistema LK

- aksiom $A \to A$
- **rez**

$$\frac{\Gamma_1, A \to \Delta_1 \qquad \Gamma_2 \to A, \Delta_2}{\Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2}$$

Formulu A nazivamo **formulu reza**.

Logička pravila sistema LK

- negacija

$$\frac{\Gamma, A \to \Delta}{\Gamma \to \neg A, \Delta} \qquad \frac{\Gamma \to A, \Delta}{\Gamma, \neg A \to \Delta}$$

  Formulu A nazivamo **pomoćna formula**, a formulu $\neg A$ **glavna formula** izvoda.

- konjunkcija

$$\frac{\Gamma_1 \to A, \Delta_1 \qquad \Gamma_2 \to B, \Delta_2}{\Gamma_1, \Gamma_2 \to A \wedge B, \Delta_1, \Delta_2}$$

$$\frac{\Gamma, A \to \Delta}{\Gamma, A \wedge B \to \Delta} \qquad \frac{\Gamma, B \to \Delta}{\Gamma, A \wedge B \to \Delta}$$

  Formule A i B nazivamo **pomoćne formule**, a formulu $A \wedge B$ **glavna formula** izvoda.

- disjunkcija

$$\frac{\Gamma \to A, \Delta}{\Gamma \to A \vee B, \Delta} \qquad \frac{\Gamma \to B, \Delta}{\Gamma \to A \vee B, \Delta}$$

$$\frac{\Gamma_1, A \to \Delta_1 \qquad \Gamma_2, B \to \Delta_2}{\Gamma_1, \Gamma_2, A \vee B \to \Delta_1, \Delta_2}$$

  Formule A i B nazivamo **pomoćne formule**, a formulu $A \vee B$ **glavna formula** izvoda.

- kondicional

$$\frac{\Gamma, A \to B, \Delta}{\Gamma \to A \Rightarrow B, \Delta}$$

$$\frac{\Gamma_1 \to A, \Delta_1 \qquad \Gamma_2, B \to \Delta_2}{\Gamma_1, \Gamma_2, A \Rightarrow B \to \Delta_1, \Delta_2}$$

  Formule A i B nazivamo **pomoćne formule**, a formulu $A \Rightarrow B$ **glavna formula** izvoda.[1]

- univerzalni kvantifikator

$$\frac{\Gamma \to A(a), \Delta}{\Gamma \to \forall x A, \Delta}$$

  pri čemu se varijabla a ne pojavljuje u donjoj sekventi. Varijabla a se naziva **svojstvena varijabla**.

$$\frac{\Gamma, A(t) \to \Delta}{\Gamma, \forall x A \to \Delta}$$

  Formule $A(a)$ i $A(t)$ nazivamo **pomoćne formule**, a formulu $\forall x A$ **glavna formula** izvoda.

- egzistencijalni kvantifikator

$$\frac{\Gamma \to A(t), \Delta}{\Gamma \to \exists x A, \Delta}$$

$$\frac{\Gamma, A(a) \to \Delta}{\Gamma, \exists x A \to \Delta}$$

  pri čemu se varijabla a ne pojavljuje u donjoj sekventi. Varijabla a se naziva **svojstvena varijabla**.

[1] U ovoj točki kondicional označavamo sa $\Rightarrow$. Razlog tome je što simbol $\to$ koristimo za zapis sekventi.

Definicija 2.22. *Izvod D u sistemu LK je stablo sekventi pri čemu su zadovoljeni sljedeći uvjeti:*

- *polazne sekvente su aksiomi*
- *svaka sekventa u D, osim najdonje, je gornja sekventa nekog pravila čija donja sekventa je također u D.*

Najdonju sekventu u izvodu nazivamo **krajnja sekventa** *izvoda. Izvod D s krajnjom sekventom S nazivamo* **izvod za sekventu** *S. Kažemo da je* **formula** *A* **dokaziva** *u sistemu LK ako postoji izvod za sekventu $\to A$.*

Prvo uvodimo neke oznake:

- $h(\Pi)$ je oznaka za visinu stabla Π
- $\partial(A)$ je oznaka za rang formule, pri čemu definiramo:
  a) $\partial(\text{atomarna formula})=1$
  b) $\partial(A \circ B) = \max\{\partial A, \partial B\} + 1$
  c) $\partial(\forall x A) = \partial(\exists x A) = \partial(\neg A) = \partial(A) + 1$
- $d(\Pi)$ nazivamo rang izvoda Π, pri čemu je to maksimalni rang formule reza koja nastupa u izvodu Π.

Lema 2.23. ("Tehnička lema") *Neka je Π izvod sekvente $\Gamma \to \Delta$, te neka je a neka varijabla i t neki term. Označimo sa $\Pi(t/a)$ stablo koje smo dobili tako da smo u izvodu Π svaki nastup varijable a zamijenili s termom t. Tada je $\Pi(t/a)$ izvod sekvente $\Gamma(t/a) \to \Delta(t/a)$.*

Lema 2.24. (Glavna lema) *Neka je A formula takva da je $\partial(A) = d > 0$. Neka je Π_1 izvod sekvente $\Gamma_1 \to \Delta_1$, a Π_2 izvod sekvente $\Gamma_2 \to \Delta_2$, pri čemu je $d(\Pi_1) < d$ i $d(\Pi_2) < d$. Tada postoji izvod Π sekvente $\Gamma_1, \Gamma_2 \setminus \{A\} \to \Delta_1 \setminus \{A\}, \Gamma_2$, pri čemu je $d(\Pi) < d$. Sa $\Gamma_2 \setminus \{A\}$, odnosno $\Delta_1 \setminus \{A\}$, označavamo niz formula iz kojeg smo maknuli formulu A.*

Dokaz. Dokaz provodimo indukcijom po $h(\Pi_1) + h(\Pi_2)$. Promotrimo prvo bazu indukcije. Tada imamo $h(\Pi_1) = h(\Pi_2) = 1$. Tada izvodi Π_1 i Π_2 sadrže samo aksiome, tj. $\Pi_1 ... B \to B$ i $\Pi_2 ... C \to C$. Razmatramo četiri slučaja obzirom na to je li neka od formula B ili C jednaka formuli A. Ako je $B \equiv A$ i $C \not\equiv A$ tada jedan traženi izvod sekvente $\Gamma_1, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$ izgleda:

$$\Pi \begin{cases} \dfrac{C \to C}{C, A \to C} \\ \dfrac{}{A, C \to C} \end{cases}$$

Koristili smo pravila slabljenja i permutacije. Uočite da je u ovom slučaju $\Gamma_1 = \{A\}$, $\Delta_1 = \{A\}$, $\Gamma_2 = \{C\}$ i $\Delta_2 = \{C\}$, pa je $\Gamma_2 \setminus A = \{C\}$ i $\Delta_1 \setminus A = \emptyset$. Iz toga slijedi da je u ovom slučaju sekventa $\Gamma_1, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$ jednaka $A, C \to C$. Primijetimo još da je $d(\Pi) = 0 < d$. Slučaj $B \not\equiv A$ i $C \equiv A$ je sasvim analogan prethodnom slučaju, pa ga nećemo raspisivati. Ako je $B \equiv A$ i $C \equiv A$ tada jedan traženi izvod Π izgleda: $A \to A$. Ako je $B \not\equiv A$ i $C \not\equiv A$ tada jedan traženi izvod izgleda:

$$\Pi \begin{cases} \dfrac{B \to B}{B, C \to B} \\ \dfrac{}{B, C \to C, B} \\ \dfrac{}{B, C \to B, C} \end{cases}$$

U prethodnom izvodu koristili smo samo pravila slabljenja i permutacije. Uočimo da je tada $d(\Pi) = 0 < d$. Ovdje imamo $\Gamma_1 = \{B\}$, $\Delta_1 = \{B\}$, $\Gamma_2 = \{C\}$ i $\Delta_2 = \{C\}$. Tada je $\Gamma_2 \setminus A = \{C\}$ i $\Delta_1 \setminus A = \{B\}$.

Posvetimo se sada koraku indukcije. Neka je $n \in \mathbb{N}$ tako da za sve izvode Π_1' i Π_2', za koje je $h(\Pi_1') + h(\Pi_2') < n$, vrijedi tvrdnja. Neka je Π_1 izvod sekvente $\Gamma_1 \to \Delta_1$, Π_2 izvod sekvente $\Gamma_1 \to \Delta_2$, tako da je $h(\Pi_1) + h(\Pi_2) = n$. Neka je A formula za koju vrijedi $\partial A = d$, te $d(\Pi_1),\ d(\Pi_2) < d$. Promatramo slučajeve obzirom na zadnje pravilo izvoda u Π_1, odnosno Π_2. Pravilo u izvodu Π_1 koje je primjenjeno posljednje označavamo sa r_1, odnosno sa r_2 u izvodu Π_2. Korak indukcije dijelimo na sljedećih pet slučaja:

1. Barem jedan od izvoda Π_1 i Π_2 je visine jedan.

2. Barem u jednom izvodu Π_1 i Π_2 posljednje primijenjeno pravilo izvoda je neko strukturno pravilo.

3. Barem u jednom izvodu Π_1 i Π_2 posljednje primijenjeno pravilo izvoda je pravilo reza.

4. Oba pravila r_1 i r_2 su logička pravila i formula A nije glavna formula barem u jednom pravilu r_i.

5. Oba pravila r_1 i r_2 su logička pravila i formula A je glavna formula u oba pravila.

Promotrimo prvo slučaj kada je neki od izvoda Π_1 i Π_2 visine jedan, tj. sastoji se samo od jednog aksioma. Radi određenosti neka je to izvod Π_1. Tu imamo dva podslučaja: $\Pi_1 ... A \to A$ i $\Pi_1 ... B \to B$, gdje je $B \not\equiv A$. Za slučaj $\Pi_1 ... A \to A$ jedan traženi izvod Π je sljedećeg oblika:

$$\Pi \left\{ \begin{array}{l} \Pi_2 \left\{ \begin{array}{c} \vdots \\ \Gamma_2 \to \Delta_2 \end{array} \right. \\ \hline A, \Gamma_2 \setminus A \to \Delta_2 \end{array} \right.$$

Očito je $\Gamma_1 = \Delta_1 = \{A\}$, pa je $\Delta_1 \setminus A = \emptyset$. Zatim, očito je $A, \Gamma_2 \setminus A = \Gamma_2$, te $d(\Pi) = d(\Pi_2) < d$. Za slučaj kada je $\Pi_1 ... B \to B$, gdje je $B \not\equiv A$, jedan traženi izvod Π izgleda ovako:

$$\Pi \left\{ \begin{array}{l} \dfrac{B \to B}{\dfrac{}{B, \Gamma_2 \setminus A \to B, \Delta_2}} \end{array} \right.$$

S dvije crte smo označili da koristimo slabljenje i permutaciju koliko puta treba. Uočite da je u ovom slučaju $\Gamma_1 = \Delta_1 = \{B\}$, pa je $\Delta_1 \setminus A = B$. Zatim, vrijedi $d(\Pi) = 0 < d$.

Promotrimo sada drugi slučaj kada je barem u jednom izvodu Π_1 i Π_2 posljednje primijenjeno pravilo neko strukturno pravilo. Radi određenosti neka je pravilo r_1 u izvodu Π_1 strukturno. Tu promatramo četiri podslučaja.

2a) pravilo r_1 je slabljanje slijeva. Tada postoji formula B tako da je izvod Π_1 oblika:

$$\Pi_1 \left\{ \begin{array}{l} \Pi_1' \left\{ \begin{array}{c} \vdots \\ \Gamma_1' \to \Delta_1 \end{array} \right. \\ \hline \Gamma_1', B \to \Delta_1 \end{array} \right.$$

Pošto je $h(\Pi_1') + h(\Pi_2) < n$ tada na izvode Π_1' i Π_2 možemo primijeniti pretpostavku indukcije. Tada postoji izvod Π' sekvente $\Gamma_1', \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$ takav da je $d(\Pi') < d$. Primjenom jednog slabljenja slijeva dobivamo jedan traženi izvod Π za sekventu $\Gamma_1', B, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$, koja je zapravo jednaka traženoj sekventi $\Gamma_1, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$.

2b) pravilo r_1 je slabljenje zdesna. Ovaj slučaj je sasvim analogan prethodnom slučaju a).

2c) pravilo r_1 je kontrakcija slijeva. Tada postoji formula B tako da je izvod Π_1 oblika:

$$\Pi_1 \left\{ \begin{array}{l} \Pi_1' \left\{ \begin{array}{l} \vdots \\ \Gamma_1', B, B \to \Delta_1 \end{array} \right. \\ \hline \Gamma_1', B \to \Delta_1 \end{array} \right.$$

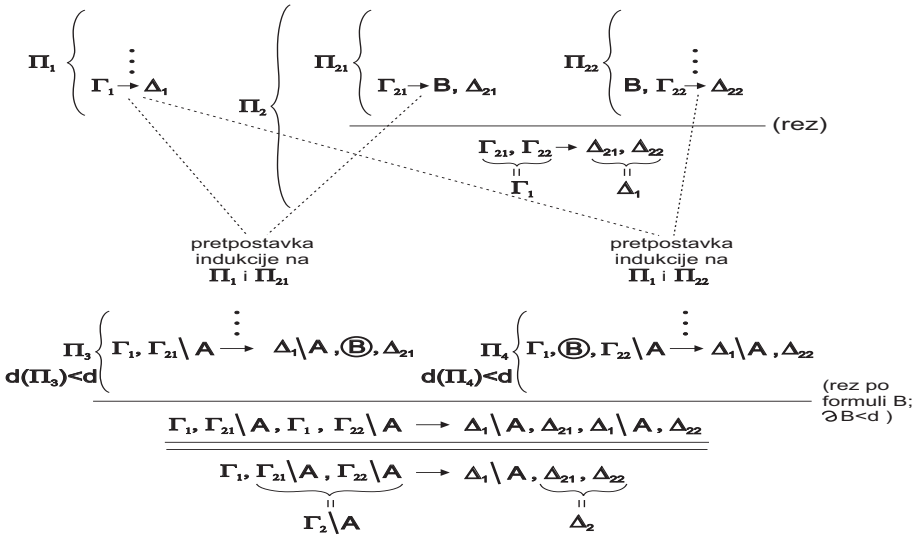
Pošto je $h(\Pi_1') + h(\Pi_2) < n$ tada na izvode Π_1' i Π_2 možemo primijeniti pretpostavku indukcije. Tada postoji izvod Π' sekvente $\Gamma_1', B, B, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$ takav da je $d(\Pi') < d$ (razmatramo samo slučaj kada je formula B različita od formule A; slučaj kada je $B \equiv A$ je sasvim analogan). Primjenom kontrakcije slijeva dobivamo jedan traženi izvod Π za sekventu $\Gamma_1', B, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$, koja je zapravo jednaka traženoj sekventi $\Gamma_1, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$.

2d) pravilo r_1 je kontrakcija zdesna. Ovaj slučaj je sasvim analogan prethodnom slučaju c).

Promotrimo sada treći slučaj kada je barem jedno pravilo r_1 ili r_2 rez. Radi određnosti neka je pravilo r_2 rez. Pošto je $d(\Pi_2) < d$, tada je r_2 rez nižeg ranga od d. Iz toga slijedi da je formula reza u pravilu r_2 različita od formule A. Oblik izvoda Π_2 možemo skicirati na sljedeći način:

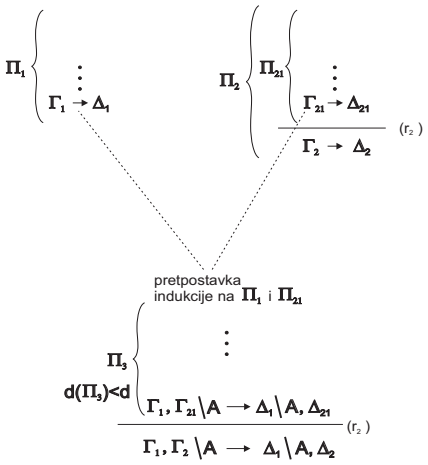
$$\Pi_2 \left\{ \begin{array}{l} \Pi_{21} \left\{ \begin{array}{l} \vdots \\ \Gamma_{21} \to B, \Delta_{21} \end{array} \right. \quad \Pi_{22} \left\{ \begin{array}{l} \vdots \\ B, \Gamma_{22} \to \Delta_{22} \end{array} \right. \\ \hline \Gamma_{21}, \Gamma_{22} \to \Delta_{21}, \Delta_{22} \end{array} \right.$$

Primijetimo: $\Gamma_2 = \Gamma_{21}, \Gamma_{22}$ i $\Delta_2 = \Delta_{21}, \Delta_{22}$. Pošto je $h(\Pi_1) + h(\Pi_{21}) < n$, te je $d(\Pi_1),\ d(\Pi_{21}) < d$, tada na te izvode možemo primijeniti pretpostavku indukcije: postoji izvod Π_3 sekvente $\Gamma_1, \Gamma_{21} \setminus A \to \Delta_1 \setminus A, B, \Delta_{21}$, tako da je $d(\Pi_3) < d$. Analogno, pošto je $h(\Pi_1) + h(\Pi_{22}) < n$, te je $d(\Pi_1),\ d(\Pi_{22}) < d$, tada na te izvode možemo primijeniti pretpostavku indukcije: postoji izvod Π_4 sekvente $\Gamma_1, B, \Gamma_{22} \setminus A \to \Delta_1 \setminus A, \Delta_{22}$, tako da je $d(\Pi_4) < d$. Skicu jednog traženog izvoda Π dajemo na sljedećoj slici.

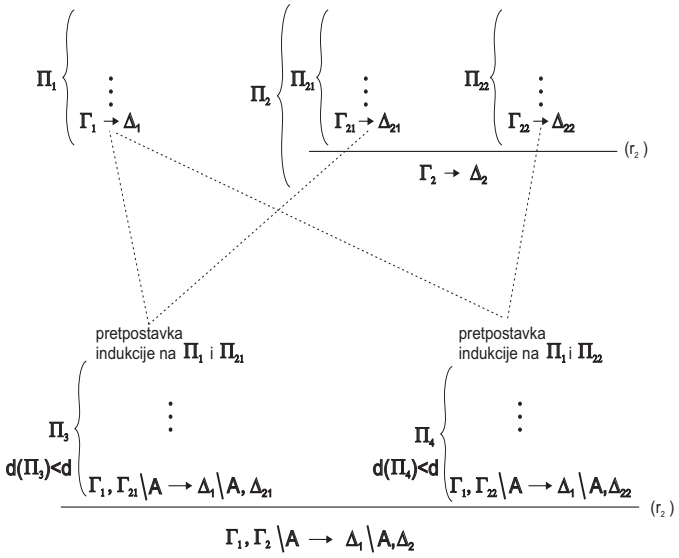


Uočimo da je $d(\Pi) < d$, jer je $d(\Pi_1) < d$ i $d(\Pi_2) < d$, te je $\partial B < d$.

Četvrti slučaj koji promatramo je situacija kada su oba pravila r_1 i r_2 logička pravila, te formula A nije glavna formula barem jednog pravila. Radi određenosti, bez smanjenja općenitosti, možemo pretpostaviti da formula A nije glavna formula pravila r_2. Prvo promatramo slučaj kada pravilo r_2 ima jednu premisu. Ilustraciju kontstrukcije jednog traženog izvoda Π sekvente $\Gamma_1, \Gamma \setminus A \to \Delta_1 \setminus A, \Delta_2$ dajemo na sljedećoj slici.



Sada promatramo podslučaj četvrtog slučaja kada pravilo r_2 ima dvije premise. Ilustraciju kontstrukcije jednog traženog izvoda Π sekvente $\Gamma_1, \Gamma \setminus A \to \Delta_1 \setminus A, \Delta_2$ dajemo na sljedećoj slici.

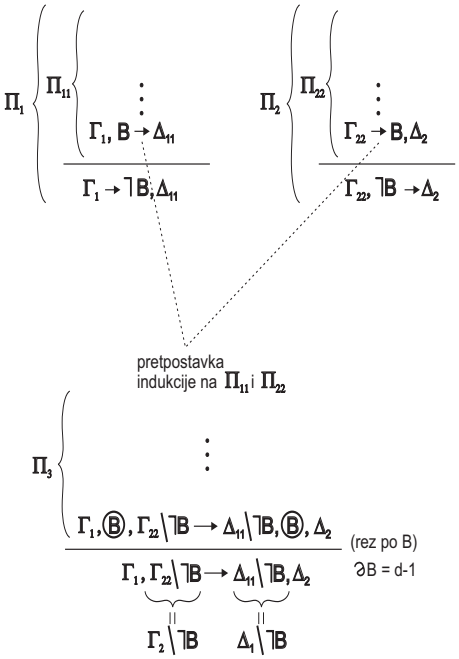


Peti, i posljednji, slučaj u koraku indukcije je situacija kada su oba pravila r_1 i r_2 logička pravila, te je formula A glavna formula u oba pravila. Tu promatramo podslučaje obzirom na vrstu logičkih pravila.

Ako je formula A oblika $\neg B$ tada je r_1 pravilo introdukcije negacije zdesna, a r_2 pravilo introdukcije negacije slijeva (ili obratno). Na sljedećoj slici ilustriramo izgled izvoda Π_1 i Π_2.

$$\Pi_1 \left\{ \dfrac{\Pi_{11} \left\{ \begin{array}{c} \vdots \\ \Gamma_1, B, \to \Delta_{11} \end{array} \right.}{\Gamma_1, \to \neg B, \Delta_{11}} \right. \qquad \Pi_2 \left\{ \dfrac{\Pi_{22} \left\{ \begin{array}{c} \vdots \\ \Gamma_{22} \to B, \Delta_2 \end{array} \right.}{\Gamma_2, \neg B \to \Delta_2} \right.$$

Primjenom pretpostavke indukcije na izvode Π_{11} i Π_{22} lako dobivamo jedan traženi izvod Π kojeg ilustriramo na sljedećoj slici.

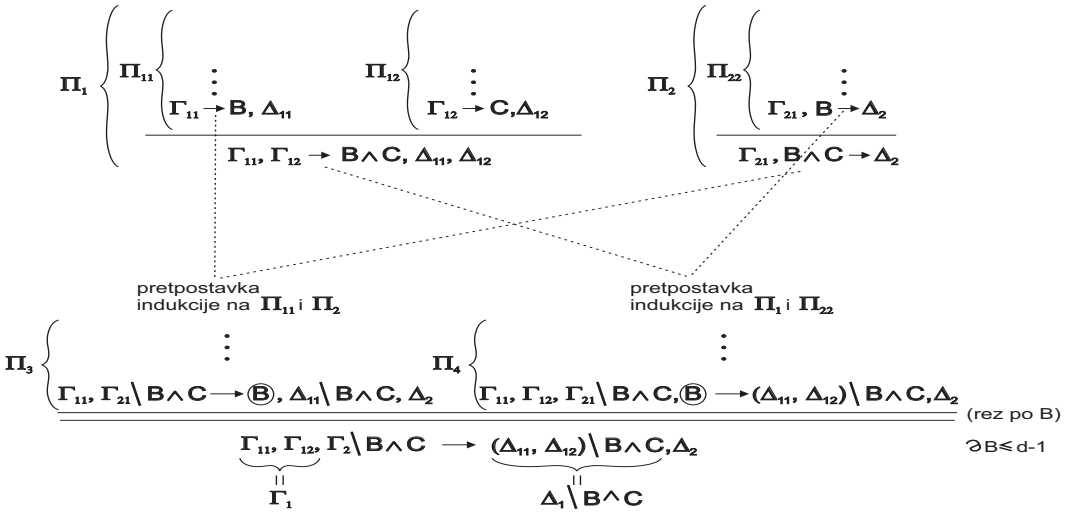


Ako je formula A oblika $B \wedge C$, tada jedno pravilo r_i mora biti pravilo introdukcije konjunkcije zdesna, a drugo pravilo r_i mora biti pravilo introduckije slijeva. Ako je pravilo r_1 "konjunkcija zdesna", a pravilo r_2 "konjunkcija slijeva", tada je izgled izvoda Π_1 i Π_2 dan na sljedećoj slici.

$$\Pi_1 \left\{ \dfrac{\Pi_{11} \left\{ \begin{array}{c} \vdots \\ \Gamma_{11}, \to B, \Delta_{11} \end{array} \right. \qquad \Pi_{12} \left\{ \begin{array}{c} \vdots \\ \Gamma_{12} \to C, \Delta_{12} \end{array} \right.}{\Gamma_{11}, \Gamma_{12} \to B \wedge C, \Delta_{11}, \Delta_{12}} \right.$$

$$\Pi_2 \left\{ \dfrac{\Pi_{22} \left\{ \begin{array}{c} \vdots \\ \Gamma_{21}, B \to \Delta_2 \end{array} \right.}{\Gamma_{21}, B \wedge C \to \Delta_2} \right.$$

Pošto je očito $h(\Pi_{11}) + h(\Pi_2) < n$ i $h(\Pi_1) + h(\Pi_{22}) < n$, tada na te izvode možemo primijeniti pretpostavku indukcije. Ilustracija konstrukcije jednog traženog izvoda Π dana je na sljedećoj slici.

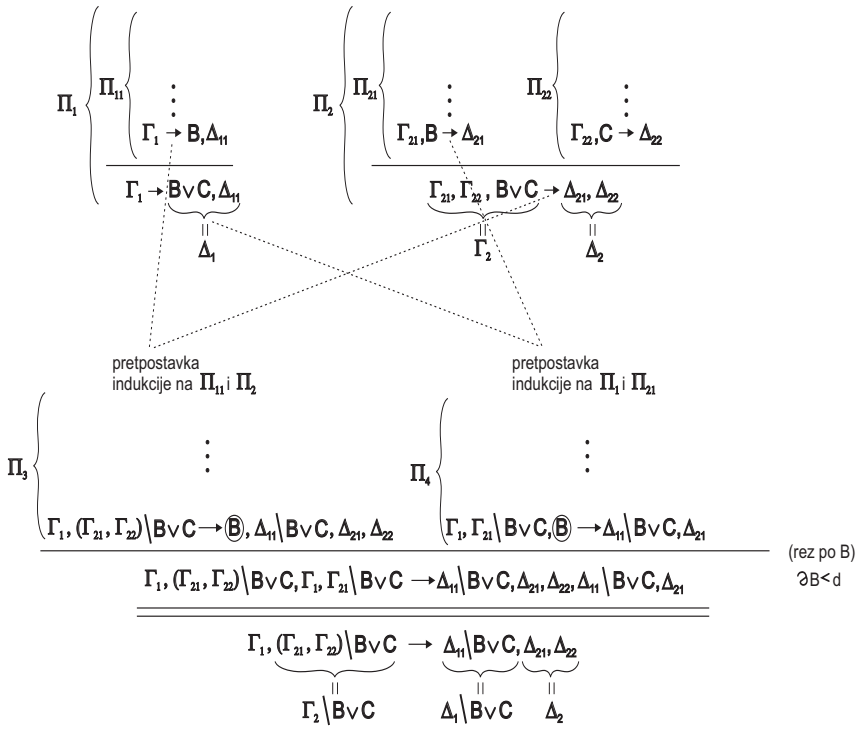


Ako je formula A oblika $B \vee C$ tada bez smanjenja općenitosti možemo pretpostaviti da je r_1 pravilo introdukcije disjunkcije zdesna, a r_2 je pravilo introdukcije disjunkcije slijeva. Na sljedećoj slici ilustriramo izgled izvoda Π_1 i Π_2.

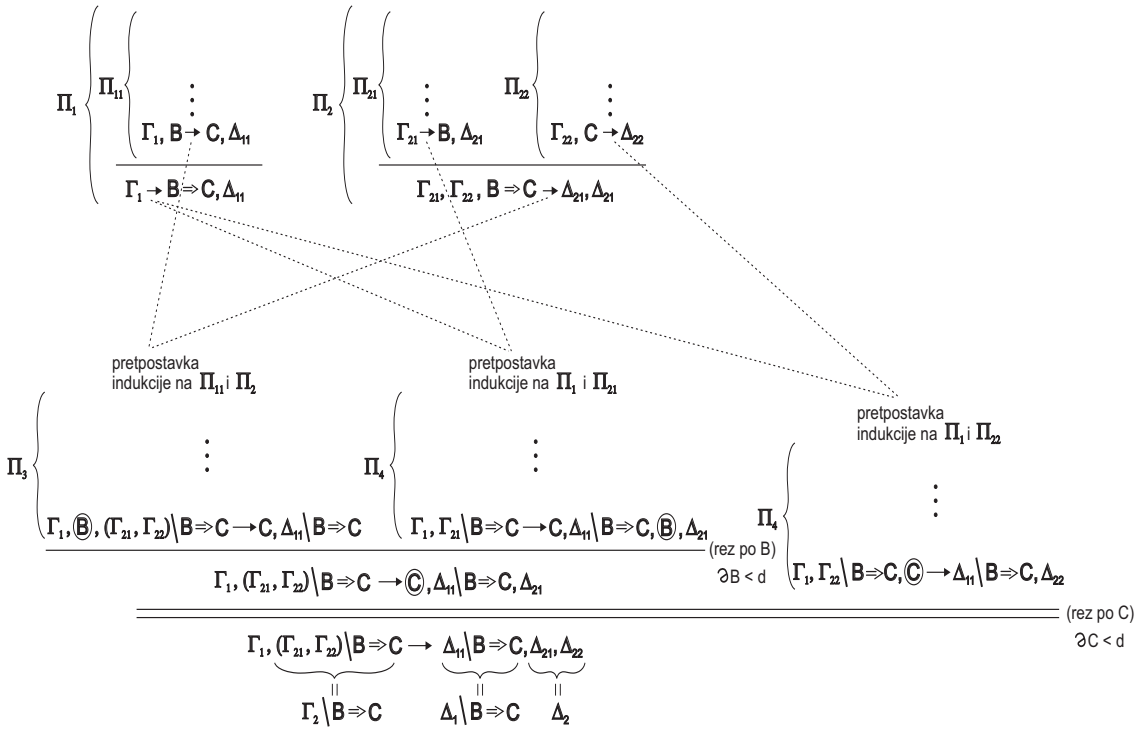
$$\Pi_1 \left\{ \dfrac{\Pi_{11} \left\{ \begin{array}{c} \vdots \\ \Gamma_1, B \to \Delta_{11} \end{array} \right.}{\Gamma_1 \to B \vee C, \Delta_{11}} \right.$$

$$\Pi_2 \left\{ \dfrac{\Pi_{21} \left\{ \begin{array}{c} \vdots \\ \Gamma_{21}, B \to \Delta_{21} \end{array} \right. \qquad \Pi_{22} \left\{ \begin{array}{c} \vdots \\ \Gamma_{22}, C \to \Delta_{22} \end{array} \right.}{\Gamma_{21}, \Gamma_{22}, B \vee C \to \Delta_{21}, \Delta_{22}} \right.$$

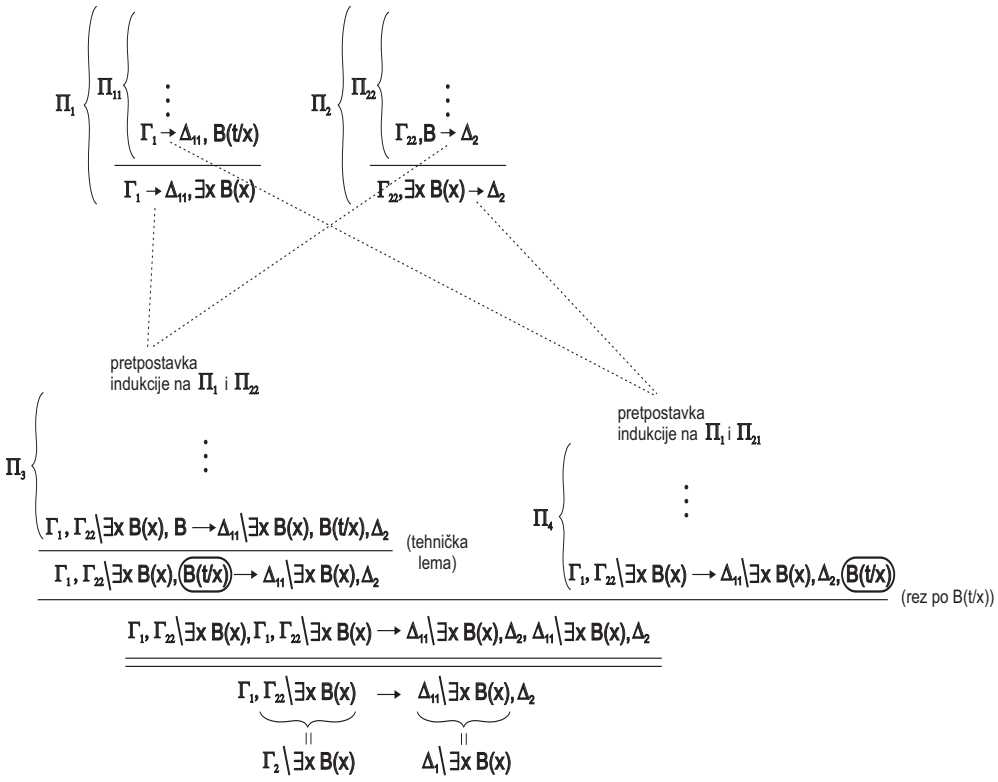
Na izvode Π_{11} i Π_{22} primijenimo pretpostavku indukcije. Pošto je $A \equiv B \vee C$ tada je $\partial B < d$. To znači da formula B ne može biti formula reza ranga d, odnosno primjenom pravila reza na formulu B i izvode čiji je rang strogo manji od d dobivamo izvod čiji je rang strogo manji od d. To sve ilustriramo na sljedećoj slici



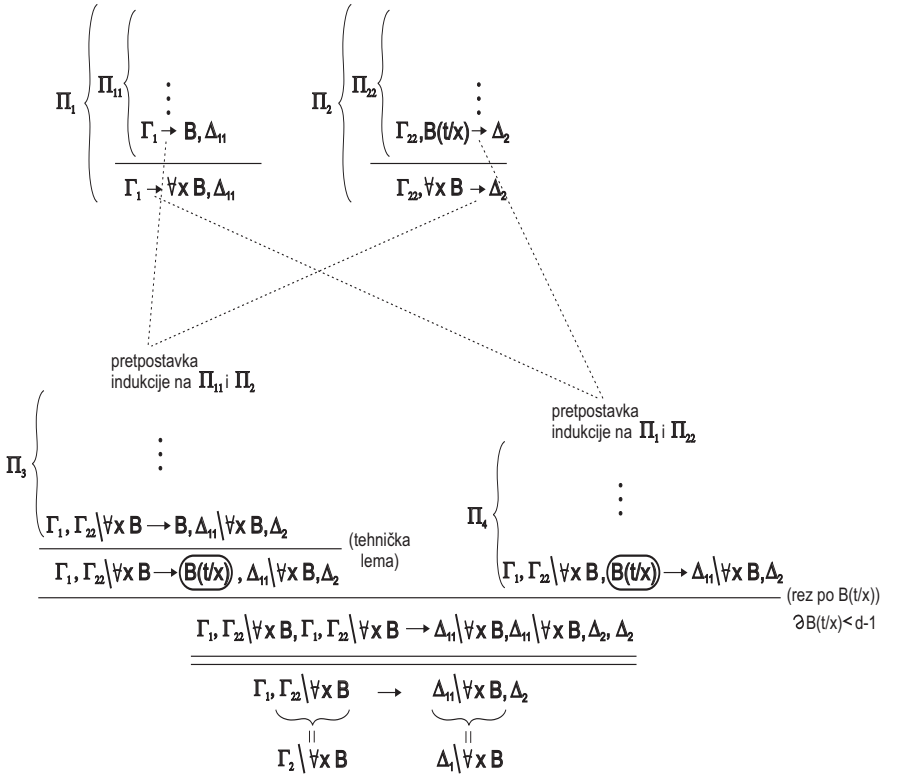
Ako je formula A oblika $B \Rightarrow C$ tada možemo bez smanjenja općenitosti pretpostaviti da je r_1 pravilo introdukcije kondicional zdesna, a r_2 je pravilo introdukcije kondicional slijeva. Tu situaciju, zajedno s ilustracijom jednog traženog izvoda Π sekvente $\Gamma_1, \Gamma_2 \setminus A \to \Delta_1 \setminus A, \Delta_2$ dajemo na sljedećoj slici.



Na sljedećoj slici je ilustrirana situacija kada je formula A oblika $\exists x B$.



Na kraju na sljedećoj slici ilustriramo situaciju ako je formula A oblika $\forall x B$.



Time je glavna lema potpuno dokazana. Q.E.D.

Lema 2.25. *Neka je* Π *izvod sekvente* $\Gamma \to \Delta$ *i* $d(\Pi) = d > 0$. *Tada postoji izvod* Π' *iste sekvente tako da je* $d(\Pi') < d$.

Dokaz. Dokaz provodimo indukcijom po visini stabla Π, tj. $h(\Pi)$. Promotrimo prvu bazu indukcije. Neka je Π izvod za koji je $h(\Pi) = 2$. Primijetimo da zbog uvjeta leme $d(\Pi) > 0$, ne može vrijediti $h(\Pi) = 1$. Tada je izvod Π sljedećeg oblika:

$$\Pi \left\{ \begin{array}{c} \dfrac{\Gamma_1 \to A, \Delta_1 \qquad \Gamma_2, A \to \Delta_2}{\Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2} \end{array} \right.$$

pri čemu je $\partial A = d$. Iz uvjeta $h(\Pi) = 2$, slijedi da premise tj. sekvente $\Gamma_1 \to A$, Δ_1 i Γ_2, $A \to \Delta_2$, moraju biti aksiomi sistema LK. Time imamo da je izvod Π zapravo oblika:

$$\Pi \left\{ \begin{array}{c} \dfrac{A \to A \qquad A \to A}{A \to A} \end{array} \right.$$

Uzmemo li za Π' upravo sekventu $A \to A$, koja je aksiom, imamo traženi izvod sekvnete za koji je rang strogo manji od d.

Promotrimo sada korak indukcije. Neka je $n \in \mathbb{N},\ n > 2$, takav da za sve izvode $\overline{\Pi}$, za koje je $h(\overline{\Pi}) < n$, vrijedi tvrdnja leme. Neka je Π neki izvod čija ja visina jednka n. Označimo sa r pravilo izvoda koje je posljednje primijenjeno u izvodu Π. Sva pravila izvoda sistema LK imaju kao premise najviše dvije sekvente. To znači da izvod Π može biti jednog od sljedeća dva oblika:

$$\Pi \left\{ \begin{array}{c} \vdots \\ \dfrac{\Gamma_1 \to \Delta_1}{\Gamma \to \Delta} \end{array} \right. \qquad \text{ili} \qquad \Pi \left\{ \begin{array}{c} \vdots \qquad\qquad \vdots \\ \dfrac{\Gamma_1 \to \Delta_1 \qquad \Gamma_2 \to \Delta_2}{\Gamma \to \Delta} \end{array} \right.$$

Označimo s Π_i podstablo izvoda Π, koje je izvod za sekventu $\Gamma_i \to \Delta_i$, pri čemu je $i = 1$ ili $i \in \{1, 2\}$ (ovisi o tome koliko premisa ima pravilo r).
Sada razlikujemo dva slučaja: pravilo r je pravilo reza, te pravilo r nije pravilo reza. Razmotrimo svaki slučaj posebno.

Neka je r neko pravilo izvoda sistema LK koje nije pravilo reza. Radi određenosti promatramo samo slučaj kada pravilo r ima dvije premise. Iz pretpostavke indukcije slijedi da postoje izvodi Π_i' sekvenata $\Gamma_i \to \Delta_i$, za $i = 1, 2$, pri čemu je $d(\Pi_i') < d$. Sada traženi izvod Π' konstruiramo na sljedeći način:

$$\Pi' \left\{ \begin{array}{c} \dfrac{\Pi_1' \left\{ \begin{array}{c} \vdots \\ \Gamma_1 \to \Delta_1 \end{array} \right. \qquad \Pi_2' \left\{ \begin{array}{c} \vdots \\ \Gamma_2 \to \Delta_2 \end{array} \right.}{\Gamma \to \Delta} \end{array} \right.$$

Očito je $d(\Pi') < d$.

Sada razmatramo slučaj u koraku indukcije kada je pravilo r upravo pravilo reza ranga d. Tada pravilo r ima dvije premise koje su oblika: $\Gamma_1 \to \Delta_1, A$ i $A, \Gamma_2 \to \Delta_2$. Pošto je $h(\Pi_i) < n$, za $i = 1, 2$, tada iz pretpostavke indukcije slijedi da postoji izvod Π_1' za sekventu $\Gamma_1 \to \Delta_1, A$, te izvod Π_2' za sekventu $A, \Gamma_2 \to \Delta_2$, tako da je $d(\Pi_i') < d$. Tada imamo izvode Π_1' i Π_2', te formulu A tako da vrijedi:

$$\Pi_1' \left\{ \begin{array}{c} \vdots \\ \Gamma_1 \to \Delta_1, A \end{array} \right. \qquad \Pi_2' \left\{ \begin{array}{c} \vdots \\ A,\ \Gamma_2 \to \Delta_2 \end{array} \right.$$

te $d(\Pi_1') < d$, $d(\Pi_2') < d$ i $\partial A = d$. Primjenom glavne leme slijedi da postoji izvod Π' sekvente $\Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2$, tako da vrijedi $d(\Pi') < d$. Q.E.D.

Iz prethodne leme direktno slijedi sljedeći teorem.

Teorem 2.26. (Gentzenov Hauptsatz za sistem LK) *Pravilo reza je redundantno, tj. za svaki izvod neke sekvente $\Gamma \to \Delta$ postoji izvod iste sekvente u kojem se ne koristi pravilo reza.*

Sada navodimo neke najvažnije posljedice Gentzenovog Hauptsatza.

Korolar 2.27. (Svojstvo podformulnosti) *Ako je neka formula F dokaziva u sistemu LK tada postoji izvod u kojem se upotrebljavaju samo podformule od F.*

Dokaz. Iz Gentzenovog Hauptsatza slijedi da za formulu F postoji izvod u kojem se ne koristi pravilo reza. U svakom pravilu izvoda sistema LK, osim pravila reza, svaka formula koja se pojavljuje u gornjoj sekventi je podformula neke formule koja se pojavljuje u donjoj sekventi. Dakle, svaki izvod bez reza sadrži samo podformule krajnje sekvente. □

Korolar 2.28. *Sistem LK je konzistentan, tj. u sistemu LK ne postoji izvod za praznu sekventu $\to$.*

Dokaz. Pretpostavimo da je prazna sekventa $\to$ dokaziva u LK. Tada iz Gentzenovog Hauptsatza slijedi da za praznu sekventu $\to$ postoji izvod u LK bez reza. No, to je nemoguće zbog svojstva podformulnosti. □

Korolar 2.29. (Gentzenov teorem o midsekventi) *Neka je S neka sekventa koja se sastoji samo od formula u preneksnoj normalnoj formi, te neka je sekventa S dokaziva u sistemu LK. Tada postoji dokaz bez reza sekvente S koji sadrži sekventu S', koju zovemo* **midsekventa**, *za koju vrijedi:*

- *formule sekvente S' ne sadrže kvantifikatore*
- *svako pravilo izvoda iznad S' je strukturno ili propozicionalno*
- *svako pravilo izvoda ispod S' je strukturno ili pak je pravilo izvoda s kvantifikatorima.*

Dakle, midsekventa dijeli izvod na gornji dio u kojem se ne koriste pravila izvoda za kvantifikatore, i donji izvod u kojem se ne koriste pravila izvoda za logičke veznike.

Teorem 2.30. (Craigova interpolacijska lema) *Neka je $A \to B$ dokaziva formula u sistemu LK. Ako obje formule A i B sadrže barem jedan isti relacijski simbol, tada postoji formula C tako da su formule $A \to C$ i $C \to B$ dokazive u sistemu LK, te formula C sadrži samo one nelogičke simbole koji su zajednički formulama A i B. Ako formule A i B ne sadrže niti jedan zajednički relacijski simbol tada je barem jedna od sekventi $A \to$ i $\to B$ dokaziva u sistemu LK.*

Teorem 2.31. (Bethov teorem o definabilnosti za sistem LK) *Ako je relacijski simbol R moguće implicitno definirati u sistemu LK tada se taj simbol R može definirati i eksplicitno.*

Poglavlje 3

Gödelovi teoremi nepotpunosti

Na početku želimo istaknuti neke povijesne okolnosti koje su prethodile otkriću Gödelovih teorema. Krajem 19. stoljeća G. Cantor je zasnovao novu teoriju – teoriju skupova. U kratkom vremenu postignuti su mnogi značajni rezultati. No, osim novih velikih otkrića dogodilo se još nešto – u novoj teoriji otkriveni su paradoksi. (npr. Russellov, Cantorov i Burali–Fortijev paradoks; vidi [29]). Činilo se da je matematika u velikoj krizi. Iz tog razloga pojačana su istraživanja iz osnova matematike. Dobiveni su rezultati o relativnoj konzistentnosti, tj. dokazano je da konzistentnost aritmetike povlači konzistentnost analize, a pretpostavka o konzistentnosti analize da povlači konzistentnost geometrije.

U svom poznatom popisu problema iz 1900. godine D. Hilbert je drugi problem formulirao ovako: *Dokazati konzistentnost aritmetike.* Štoviše, Hilbert se zalagao za "čišćenje" matematike u sljedećem smislu:

> *Točno odrediti dijelove matematike u kojima se svi dokazi mogu izvršiti na formalan i konačan način, odnosno naglasiti dijelove gdje su mogući problemi.*

Ta Hilbertova nastojanja se nazivaju Hilbertov program. Svrha velikog i ambicioznog Hilbertovog programa bila je postaviti aksiomatske osnove na kojima bi se moglo temeljiti svako istraživanje Nemogućnost ostvarenja Hilbertovog programa slijedi iz Gödelovih teorema nepotpunosti iz 1931. godine. Ovdje ih iskazujemo.

Gödelov prvi teorem nepotpunosti

> *Ne postoji konzistentno potpuno i aksiomatizabilno proširenje teorije Q.*

Gödelov drugi teorem nepotpunosti

> *Neka je T konzistentno i aksiomatizabilno proširenje Peanove aritmetike. Tada rečenica Con_T nije dokaziva u teoriji T.*

(Sve pojmove i oznake koji su navedni u iskazima Gödelovih teorema definirat ćemo kasnije).

Ovdje ističemo najvažnije dijelove dokaza Gödelovih teorema:

1. Aritmetizacija (gedelizacija) jezika
2. Reprezentabilnost rekurzivnih funkcija
3. Dijagonalna lema
4. Tarskijev teorem o nedefinabilnosti aritmetičke istine
5. Dokaz Gödelovog prvog teorema
6. Predikat dokazivosti. Hilbert–Bernaysovi uvjeti.
7. Dokaz Gödelovog drugog teorema. Löbov teorem.

Želimo istaknuti da dokaz Gödelovih teorema, koji ovdje prezentiramo, većinom prati tekst knjige [5].

3.1 Aritmetizacija

Pod aritmetizacijom podrazumijevamo preslikavanje kojim prvo svakom simbolu alfabeta pridružujemo neki prirodan broj, a nakon toga svakom konačnom nizu simbola pridružujemo prirodan broj. Obično se kodovi simbola, odnosno konačnih nizova simbola, nazivaju **Gödelovi brojevi**. No, postupak aritmetizacije ne završava pukim pridruživanjem Gödelovih brojeva. Potrebno je i dokazati da definirano preslikavanje ima dobro svojstva (injektivnost; efektivno je, te je i dekodiranje efektivno). Krenimo redom. Pošto ćemo zapravo definirati aritmetizaciju općenite teorije prvog reda, navodimo prvo alfabet logike prvog reda:

$$\{\neg,\ \vee,\ \exists\} \cup \{=\} \cup \{(),\} \cup \{v_i : i \in \mathbb{N}\} \cup \{A_i^j : i, j \in \mathbb{N}\} \cup \{f_i^j : i, j \in \mathbb{N}\}$$

Sa A_i^j je označen i–ti j–mjesni relacijski simbol, odnosno sa f_i^j je označen i–ti j–mjesni funkcijski simbol. Konstanstki simboli su nul–mjesni funkcijski

simboli. U ovom trenutku nije važno koji konkretni aksiomatski sistem za logiku prvog reda promatramo. U trenutku kada će nam to biti važno, istaknut ćemo koja svojstva aksiomatski sistem za logiku prvog reda treba imati. Zatim ćemo samo kratko primijetiti da npr. sistem RP iz skripte [28], ima tražena svojstva. U daljenjem tekstu pod **teorijom** smatramo svaki skup rečenica zatvoren za relaciju izvedivosti.
Sada definiramo Gödelove brojeve svakog simbola logike prvog reda na način da u prvoj tablici navodimo simbole, a u drugoj pridružene Gödelove brojeve.

(	$\neg$	$\exists$	$=$	v_0	A_0^0	A_0^1	A_0^2	...	f_0^0	f_0^1	...
)	$\vee$			v_1	A_1^0	A_1^1	A_1^2	...	f_1^0	f_1^1	...
,				v_2	A_2^0	A_2^1	A_2^2	...	f_2^0	f_2^1	...
				v_3	A_3^0	A_3^1	A_3^2	...	f_3^0	f_3^1	...
				$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$	...

1	2	3	4	5	6	68	688	...	7	78	...
19	29			59	69	689	6889	...	79	789	...
199				599	699	6899	68899	...	799	7899	...
				5999	6999	68999	688999	...	7999	78999	...
				$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$	...

Jezik aritmetike pored dvomjesnog relacijskog simbola = ima i sljedeće nelogičke simbole (u zagradama iza svakog simbola je navedena njegova intendirana interpretacija):

- konstantski simbol 0 (prirodni broj 0);
- unarni funkcijski simbol ' (funkcija sljedbenika, koju označavamo sa s);
- binarni funkcijski simbol + (zbrajanje prirodnih brojeva);
- binarni funkcijski simbol $\cdot$ (množenje prirodnih brojeva);
- binarni relacijski simbol $<$ (uređaj na prirodnim brojevima).

Strukturu $(\mathbb{N}, 0, s, +, \cdot, <)$ nazivamo **standardni model**.

Za svaki prirodni broj n definiramo **numeral** $\overline{n}$ kao pokratu za niz simbola u kojem je prvi znak konstantski simbol 0, a nakon toga dolazi n nastupa funkcijskog simbola $'$. Na primjer, $\overline{3}$ nam je pokrata za $0'''$. Uzevši u obzir prije navedenu intendiranu interpretaciju, numerali zapravo predstavljaju prirodna imena za brojeve. Primijetimo da su nelogičkim simbolima aritmetičkih teorija pridruženi redom sljedeći kodovi:

$<$ (to je relacijski simbol A_0^2) $\mapsto$ 688

0 (to je konstanski simbol f_0^0) $\mapsto$ 7

$'$ (to je funkcijski simbol f_0^1) $\mapsto$ 78

$+$ (to je funkcijski simbol f_0^2) $\mapsto$ 788

$\cdot$ (to je funkcijski simbol f_1^2) $\mapsto$ 7889

Za kodiranje konačnih nizova simbola koristimo konkatenaciju. Npr. promotrimo sljedeći konačan niz simbola: $(0 = 0 \ \vee \ \neg 0 = 0)$. Ispod svakog simbola navednog konačnog niza pišemo pripadni kod:

$$\begin{array}{ccccccccccc} (& 0 & = & 0 & \vee & \neg & 0 & = & 0 &) \\ 1 & 7 & 4 & 7 & 29 & 2 & 7 & 4 & 7 & 19 \end{array}$$

To znači da konačnom nizu simbola $(0 = 0 \ \vee \ \neg 0 = 0)$ pridružujemo prirodan broj 174 729 274 719.

Neka je e kod nekog izraza E, a d kod nekog izraza D. Tada je kod izraza ED dan sa:

$$e * d \;=\; e \cdot 10^{lg(d)+1} \;+\; d,$$

gdje je s $lg(d)$ označeno najveće cijelo od $\log(d)$. Očito je $*$ jedna dvomjesna rekuzivna funkcija.

Propozicija 3.1. *Logičke operacije negacije, disjunkcije, egzistencijalne kvantifikacije i susptitucija terma u formulu, su rekurzivne funkcije.*

Dokaz. Neka je $neg : \mathbb{N} \to \mathbb{N}$ funkcija definirana sa $neg(x) = 2 * x$. Očito je neg rekurzivna funkcija. Neka je $disj : \mathbb{N} \to \mathbb{N}$ funkcija definirana sa

$$disj(x, y) = 1 * x * 29 * y * 199$$

Očito je funkcija $disj$ rekurzivna. Za supstituciju terma u formulu dokaz je dosta kompliciraniji, pa ga ovdje ispuštamo (nećemo niti koristiti tu operaciju u daljnjim razmatranjima).

Propozicija 3.2. *Skup svih formula logike prvog reda je rekurzivan. Skup svih formula svake teorije u jeziku aritmetike je rekurzivan. Skup svih rečenica svake teorije u jeziku aritmetike je rekurzivan.*

Skica dokaza. Označimo sa Var skup svih varijabli logike prvog reda, a sa Var^* skup svih pripadnih Gödelovih brojeva. Očito vrijedi:

$$n \in Var^* \;\Leftrightarrow\; n = 5 \;\vee\; n = 59 \;\vee\; n = 599 \;\vee\; \ldots$$

Rekurzivnost skupa Var^* slijedi iz sljedeće ekvivalencije:

$$n \in Var^* \;\Leftrightarrow\; (\exists k < n)\; (n = 5 * \underbrace{9 \;\ldots\; 9}_{k\text{–puta}})$$

(Lako je vidjeti da je funkcija $f : \mathbb{N} \to \mathbb{N}$, koja je definirana sa $f(k) = \underbrace{9 \;\ldots\; 9}_{k-puta}$, rekurzivna).
Označimo sa $Term$ skup svih termi logike prvog reda, a s $Term^*$ skup svih pripadnih Gödelovih brojeva. Očito vrijedi:

$$n \in Term^* \;\Leftrightarrow\; n \in Var^* \;\vee\; (\exists k < n)\; (n = 7 * \underbrace{9 \;\ldots\; 9}_{k\text{–puta}} \;\vee$$

$$(\exists i, j < n)(\; n = 78 * \underbrace{8 \;\ldots\; 8}_{i\text{–puta}} * \underbrace{9 \;\ldots\; 9}_{j\text{–puta}} * 1 * t_1 * 199 * \ldots * 199 * t_i * 19),$$

gdje su $t_1, \ldots, t_i \in Term^*$. Iz posljednje ekvivalencije ne možemo još zaključiti da je skup $Term^*$ rekurzivan, jer s desne strane imamo "rekurzivno" pozivanje na skup $Term^*$. Kako bismo vidjeli da je skup $Term^*$ rekurzivan uvodi se pojam "niz izgradnje terma".
Označimo sa $Atom$ skup svih atomarnih fromula logike prvog reda, a sa $Atom^*$ označimo skup svih pripadnih Gödelovih brojeva. Očito vrijedi:

$$n \in Atom^* \Leftrightarrow (\exists i < n)(\exists j < n) \quad (i \in Term^* \ \wedge \ j \in Term^* \wedge \\ (n = i * 4 * j \ \vee \ n = i * 688 * j))$$

Iz posljednje ekvivalencije slijedi da je skup $Atom^*$ rekurzivan. Označimo sa $Form$ skup svih formula logike prvog reda, a sa $Form^*$ skup Gödelovih brojeva elemenata iz $Form$. Za dokaz rekurzivnosti skupa $Form^*$ treba definirati "niz izgradnje formule".

Propozicija 3.3. *Ako je Γ rekurzivan skup rečenica tada je sljedeća relacija rekurzivna: "Σ je izvod rečenice D iz skupa Γ".*

Korolar 3.4. *Neka je Γ neki rekurzivan skup rečenica. Skup svih rečenica koje su izvedive iz Γ je rekurzivno prebrojiv.*

Korolar 3.5. *(Gödelov teorem potpunosti – apstraktna forma)*
Skup svih valjanih formula logike prvog reda je rekurzivno prebrojiv.

Dokaz. Iz Gödelovog teorema potpunosti slijedi da je skup svih valjanih rečenica logike prvog reda jednak skupu svih rečenica koje su izvedive iz praznog skupa. Pošto je prazan skup rekurzivan tada tvrdnja slijedi iz prethodnog korolara. □

Ako postoji rekurzivan skup rečenica Γ tako da za svaku rečenicu F vrijedi:

$$\Gamma \vdash F \qquad \text{ako i samo ako} \qquad F \in T,$$

tada kažemo da je teorija T **aksiomatizabilna**.

Kažemo da je skup rečnica Γ **potpun** ako za svaku rečenicu F vrijedi:

$$\Gamma \vdash F \qquad \text{ili} \qquad \Gamma \vdash \neg F$$

Analogno definiramo pojam **potpune teorije**. Kažemo da je teorija T **konzistentna** ako postoji rečenica F tako da vrijedi $F \notin T$.

Za skup rečenica Γ kažemo da je **odlučiv** ako je skup svih logičkih posljedica od Γ (odnosno, ekvivalentno: skup svih rečenica koje se mogu izvesti iz Γ) rekurzivan. Posebno, teorija T je **odlučiva** ako i samo ako je rekurzivna.

Teorem 3.6. *Svaka aksiomatizabilna i potpuna teorija T je odlučiva.*

Dokaz. Sa T^* označimo skup Gödelovih brojeva rečenica iz T. Iz korolara 3.4. znamo da je skup T^* rekurzivno prebrojiv. Ako je T inkonzistentna teorija tada je teorija T jednaka skupu svih rečenica pripadnog jezika. Iz propozicije 3.2. posebno slijedi da je skup svih rečenica rekurzivan. Dakle, ako je T inkonzistentna teorija tada je ona rekurzivna.
Promotrimo sada slučaj kada je T konzistentna teorija. Označimo sa X skup svih prirodnih brojeva koji nisu kodovi rečenica. Označimo sa Y skup svih kodova rečenica koje nisu teoremi iz T (odnosno ne pripadaju skupu T.) Očito vrijedi $\mathbb{N} \setminus T^* = X \cup Y$. Iz propozicije 3.2. posebno slijedi da je skup $Sent^*$, koji sadrži kodove svih rečenica, rekurzivan. Pošto je $X = \mathbb{N} \setminus Sent^*$ tada je i skup X rekurzivan. Teorija T je potpuna, pa je skup Y zapravo jednak skupu svih kodova rečenica čije negacije su teoremi od T. Pošto je skup T^* rekurzivno prebrojiv, te pošto za svaki $n \in \mathbb{N}$ vrijedi:

$$n \in Y \qquad \text{ako i samo ako} \qquad neg(n) \in T^*,$$

tada je i skup Y rekurzivno prebrojiv. Sada iz $\mathbb{N} \setminus T^* = X \cup Y$, te rekurzivnosti skupa X i rekurzivne prebrojivosti skupa Y, slijedi da je i skup $\mathbb{N} \setminus T^*$ rekurzivno prebrojiv. Rezimirajmo: skupovi T^* i $\mathbb{N} \setminus T^*$ su rekurzivno prebrojivi. Iz teorema 4.50. slijedi da je skup T^* rekurzivan. □

Za dokaz Gödelovog prvog teorema nepotpunosti dovoljno je dokazati da niti jedno konzistentno proširenje minimalne aritmetike Q (ubrzo ćemo je točno definirati) nije odlučivo.

3.2 Definabilnost skupova i reprezentabilnost funkcija

Reprezentabilnost je široki logički pojam koji se odnosi na mogućnost prikazivanja nekih vanjskih objekata (najčešće relacija i funkcija) u logičkim teorijama. Nas će zanimati reprezentabilnost u tzv. minimalnoj aritmetici, logičkoj teoriji prvog reda s jednakošću koja predstavlja u nekom smislu najmanju aproksimaciju aritmetike prirodnih brojeva sa zbrajanjem i množenjem kao operacijama.

Definicija 3.7. *Za rečenicu F u jeziku aritmetike reći ćemo da je* **korektna** *ako je istinita na standardnom modelu.*

Definicija 3.8. *Neka je $D(x)$ neka formula u jeziku aritmetike s jednom slobodnom varijablom x. Kažemo da je neki skup prirodnih brojeva $S \subseteq \mathbb{N}$ aritmetički definiran formulom $D(x)$ u teoriji T ako za svaki $n \in \mathbb{N}$ vrijedi:*

$$n \in S \qquad \textit{ako i samo ako} \qquad \textit{rečenica } D(\overline{n}) \textit{ je korektna}$$

Kažemo da je **skup** S **aritmetički definabilan u teoriji** T, *ako postoji formula koja ga definira. U daljnjem tekstu umjesto "aritmetički definabilan skup" kratko ćemo govoriti samo "***aritmetički skup***".*

Ti pojmovi prirodno se generaliziraju i na k–arne relacije za $k > 1$ (formula D tada treba imati k slobodnih varijabli).

Definicija 3.9. *Za funkciju $f : \mathbb{N}^k \to \mathbb{N}$ kažemo da je* **aritmetička funkcija** *ako je njen graf aritmetički skup.*

Primjer 3.10. *Inicijalne primitivno rekurzivne funkcije su aritmetičke. Nul–funkcija (tj. njen graf) je definirana s formulom $x = x \wedge y = 0$. Projekcija $I_k^n(x_1, \ldots, x_n) = x_k$ je definirana s formulom $x_1 = x_1 \wedge \ldots \wedge x_n = x_n \wedge y = x_k$. Funkcija sljedbenika $Sc : \mathbb{N} \to \mathbb{N}$, zadana sa $Sc(n) = n + 1$, je definirana s formulom $x = x \wedge y = x'$.*

Problem nastupa kada treba u jeziku aritmetike definirati eksponencijalnu funkciju koja je važna za kodiranje konačnih nizova prirodnih brojeva. U tu svrhu se dokazuje sljedeća lema o Gödelovoj β–funkciji.

Lema 3.11. *Za svaki $k \in \mathbb{N}$ i sve $a_0, a_1, \ldots, a_k \in \mathbb{N}$ postoje $s, t \in \mathbb{N}$ takvi da za svaki $i \in \{0, 1, \ldots, k\}$ vrijedi $a_i = rem(s, t(i + 1) + 1)$.*

Funkcija rem je definirana kao ostatak pri dijeljenju. Funkcija $\beta : \mathbb{N}^3 \to \mathbb{N}$ definira se sa: $\beta(s, t, i) = rem(s, t(i+1)+1)$. Primjenom leme o β–funkciji možemo definirati kod konačnog niza $a_0, a_1, \ldots, a_k$ kao uređeni par (s, t). Pomoću β funkcije je definirano dekodiranje. Lema o β funkciji se dokazuje primjenom kineskog teorema o ostacima.

Lema 3.12. *Svaka rekurzivna funkcija je aritmetička. Svaki rekurzivni skup je aritmetički.*

Prethodna lema daje važnu vezu rekurzivnih funkcija i aritmetičkih teorija. No, primijetimo da je ta veza u biti semantička (formula koja definira funkciju je istinita na standardnom modelu). Željeli bi da veza rekurzivnih funkcija i aritmetičkih teorija bude čisto sintaktička. Prethodna lema nam daje sljedeće smjernice što moramo učiniti:

- otkriti sinaktičku formu formula koje definiraju rekurzivne funkcije

- za posebnu klasu formula koje su i korektne dokazati da su teoremi aritmetičkih teorija

Definicija 3.13. *Za formulu kažemo da je* **rudimentarna formula** *ako u njoj nema neograničenih kvantifikatora (može biti proizvoljno mnogo ograničenih kvantifikatora). Za formulu kažemo da je* $\exists$**–rudimentarna formula** *ako je oblika* $\exists x\varphi$*, gdje je* φ *rudimentarna formula. Za formulu kažemo da je* $\forall$**–rudimentarna formula** *ako je oblika* $\forall x\varphi$*, gdje je* φ *rudimentarna formula.*

Uočite da su rudimentarne formule zapravo Δ_0^0–formule, $\exists$–rudimentarne formule su Σ_1^0–formula, a $\forall$–rudimentarne formule su Π_1^0–formule.

Propozicija 3.14. *Svaka rekurzivna funkcija je definabilna s nekom* $\exists$*–rudimentarnom formulom.*

U knjizi [5] definiraju se i opće $\exists$–rudimentarne formule. Pokazuje se da je svaka opća $\exists$–rudimentarna formula ekvivalentna nekoj $\exists$–rudimentarnoj formuli. O tom dokazu smo govorili prilikom razmatranja aritmetičke hijerarhije, tj. Σ_1^0–formula.

Definicija 3.15. *Neka je* T *konzistentna teorija u jeziku aritmetike, te* $D(x)$ *neka formula od* T *s jednom slobodnom varijablom* x*. Kažemo da je neki skup prirodnih brojeva* S *definiran formulom* $D(x)$ *u teoriji* T *ako vrijede sljedeća dva uvjeta:*

- *za svaki* $n \in S$ *formula* $D(\overline{n})$ *je teorem od* T;
- *za svaki* $n \in \mathbb{N} \setminus S$ *formula* $\neg D(\overline{n})$ *je teorem od* T*.*

Kažemo da je skup S **definabilan** *u teoriji* T*, ako postoji formula* $D(x)$ *kojom je definiran.*

Ti pojmovi prirodno se generaliziraju i na k–mjesne relacije za $k > 1$. Primijetimo da je aritmetička definabilnost zapravo definabilnost u teoriji koja sadrži sve korektne rečenice. No, iako se pojmovi mogu generalizirati i na funkcije, pokazuje se da nam za funkcije često treba jače svojstvo.

Definicija 3.16. *Neka je* $f : \mathbb{N}^k \to \mathbb{N}$ *neka funkcija i* $F(x_1, \ldots, x_k, y)$ *formula u jeziku aritmetike s točno* $(k+1)$*–jednom slobodnom varijablom. Kažemo da je funkcija* f *reprezentirana u teoriji* T *formulom* $F(\vec{x}, y)$ *ako za sve* $n_1, \ldots, n_k \in \mathbb{N}$ *vrijedi:*

$$\forall y(F(\overline{n_1}, \ldots, \overline{n_k}, y) \leftrightarrow y = \overline{m}) \in T, \quad \textit{gdje je} \quad m = f(n_1, \ldots, n_k)$$

Kažemo da je funkcija f **reprezentabilna** *u teoriji* T *ako postoji formula koja je reprezentira.*

Minimalna aritmetika, koju označavamo sa Q, zadana je sljedećim konačnim skupom nelogičkih aksioma:

$$(Q1) \quad 0 \neq x'$$

$$(Q2) \quad x' = y' \ \rightarrow \ x = y$$

$$(Q3) \quad x + 0 = x$$

$$(Q4) \quad x + y' = (x + y)'$$

$$(Q5) \quad x \cdot 0 = 0$$

$$(Q6) \quad x \cdot y' = (x \cdot y) + x$$

$$(Q7) \quad \neg(x < 0)$$

$$(Q8) \quad x < y' \ \rightarrow \ (x < y \vee x = y)$$

$$(Q9) \quad x < y \ \vee \ x = y \ \vee \ y < x$$

Teorija Q je dovoljno jaka da se dokažu glavni teoremi teorije brojeva. No, važnije je da je teorija Q dovoljno jaka da se dokažu sve korektne $\exists$–rudimentarne rečenice.

Teorem 3.17. . *(Σ_1^0–potpunost teorije Q)*
Neka je F proizvoljna $\exists$–rudimentarna rečenica. Tada vrijedi:

rečenica F je korektna ako i samo ako je dokaziva u teoriji Q.

Dokaz. Svaki aksiom od Q je korektna rečenica i pravila izvoda čuvaju korektnost. Iz toga slijedi da su svi teoremi od Q korektne rečenice.

Obrat se dokazuje indukcijom po složenosti korektnih $\exists$–rudimentarnih formula. Za ilustraciju prvo promotrimo rečnice oblika $\overline{m} = \overline{n}$. Ako je takva rečenica korektna, mora biti $m = n$. Tada su termi $\overline{m}$ i $\overline{n}$ sintaktički jednaki, te je aksiom $x = x$ (pretpostavljamo da svaka teorija koju razmatramo sadrži aksiome za jednakost!) dovoljan da zaključimo da je formula teorem od Q.

Promotrimo sada korektne atomarne rečenice oblika $\overline{n} < \overline{m}$ Primjenom aksioma $(Q8)$ nije teško dokazati da za svaki $m = k + 1 \in \mathbb{N}$ vrijedi:

$$x < \overline{m} \rightarrow \ (x = 0 \ \vee \ x = \overline{1} \ \vee \ \ldots \ \vee \ x = \overline{k})$$

Iz ovog posljednjeg nije teško dokazati da za sve $n, m \in \mathbb{N}$ za koje vrijedi $n < m$ imamo $Q \vdash \overline{n} < \overline{m}$. Primijetimo da atomarne rečenice općenito mogu biti oblika $t = s$ i $t < s$, gdje su t i s proizvoljni zatvoreni termi.

Nije teško dokazati indukcijom po duljini terma da za svaki zatvoreni term t postoji prirodan broj k takav da se u Q može dokazati $t = \overline{k}$. Iz toga slijedi da je na primjer atomarna formula $t < s$ u Q ekvivalentno s $\overline{k} < \overline{j}$, što ako je korektno znamo dokazati u Q kao što smo vidjeli prije. Time smo riješili atomarne formule.

Slučajeve s logičkim veznicima je lako raspisati. No što je s varijablama? Kako radimo s rečenicama, svaka varijabla je vezana, odnosno u dosegu nekog kvantifikatora. Osim onog egzistencijalnog na početku formule, svi ti kvantifikatori su ograničeni. No to znači da nam varijable i ne trebaju, jer se svaka ograničena kvantifikacija može zapisati pomoću konačne konjunkcije ili disjunkcije. Na primjer, ako je t zatvoreni term čija je "vrijednost" prirodni broj $k + 1$, tada za svaku formulu $A(x)$ vrijedi

$$Q \vdash (\forall x < t)A(x) \leftrightarrow \Big(A(0) \wedge A(\overline{1}) \ \wedge \ldots \wedge A(\overline{k}) \Big)$$

Naravno, ako je vrijednost od t jednaka 0, ograničena kvantifikacija do t je logička konstanta. I za kraj, niti varijabla po kojoj egzistencijalno neograničeno kvantificiramo na početku formule nam ne treba. Ako je formula $\exists x A(x)$ korektna tada postoji prirodan broj k takav da je rečnica $A(\overline{k})$ korektna. Pošto je $A(\overline{k})$ korektna rudimentarna rečenica, i složenosti je manje od $A(x)$ tada iz prepostavke indukcije slijedi da je dokaziva u Q. Onda je očito u Q dokaziva i formula $\exists x A(x)$. □

Naravno, teorem ne vrijedi za proizvoljne formule. Na primjer, ako je $\forall x A(x)$ korektna $\forall$–rudimentarna rečenica, sve što možemo zaključiti je da su $A(0)$, $A(\overline{1})$, $A(\overline{2}), \ldots$ korektne rudimentarne rečenice, i time dokazive u Q. Međutim iz toga ne možemo zaključiti da je $\forall x A(x)$ dokaziva u Q. Jedan od lijepih kontraprimjera je aritmetika ordinalnih brojeva koja je model za teoriju Q. No, u tom modelu ne vrijede neke univerzalne rečenice poput komutativnosti zbrajanja.

Teorem 3.18. *1. Svaka rekurzivna funkcija je reprezentabilna u Q, i to $\exists$–rudimentarnom formulom.*

2. Svaka rekurzivna relacija je definabilna u Q, i to $\exists$–rudimentarnom formulom.

3.3 Dijagonalna lema

Bilo smo za svaki niz simbola A jezika aritmetike definirali njegov Gödelov broj k. Pripadni numeral $\overline{k}$ nazivamo **Gödelov kod izraza** A, i označavamo ga s $\ulcorner A \urcorner$. Za svaki izraz A riječ $\exists x(x = \ulcorner A \urcorner \ \wedge A)$ nazivamo **dijagonalizacija izraza** A. Primijetimo: ako je $A(x)$ formula tada je rečenica $\exists x(x = \ulcorner A \urcorner \ \wedge A)$ ekvivalentna s rečenicom $A(\ulcorner A \urcorner)$. Uvođenjem dijagonalizacije izraza izbjegli smo supstituciju terma u formulu.

Lema 3.19. *(Dijagonalna lema)*
Neka je T teorija u jeziku aritmetike koja proširuje Q. Za svaku formulu B postoji rečenica G tako da vrijedi: $\vdash_T G \leftrightarrow B(\ulcorner G \urcorner)$.

Dokaz. Lako je vidjeti da postoji primitivno rekurzivna funkcija $diag : \mathbb{N} \to \mathbb{N}$ koja ima sljedećo svojstvo:

> ako je n Gödelov broj nekog izraza A tada je $diag(n)$ jednak Gödelovom broju dijagonalizacije izraza A.

Pošto je T teorija koja proširuje Q tada je rekurzivna funkcija $diag$ reprezentabilna u teoriji T. Neka je $Diag(x, y)$ formula koja reprezentira funkciju $diag$, tj. neka za sve $m, n \in \mathbb{N}$, takve da je $m = diag(n)$, vrijedi:

$$\vdash_T \forall y(Diag(\overline{n}, y) \leftrightarrow y = \overline{m})$$

Neka je $A(x) \equiv \exists y(Diag(x, y) \ \wedge \ B(y))$. Neka je a Gödelov broj formule $A(x)$. Konačno definiramo traženu rečenicu G sa:

$$G \equiv \exists x\Big(\ x = \overline{a} \ \wedge \ A(x) \ \Big)$$

Primijetimo da je rečenica G ekvivalentna rečenici $A(\ulcorner A \urcorner)$, tj. $\exists y(Diag(\ulcorner A \urcorner, y) \wedge B(y))$. Nije teško dokazati da vrijedi $\vdash_T G \leftrightarrow B(\ulcorner G \urcorner)$. □

Lema 3.20. *Neka je T konzistentna teorija koja proširuje teoriju Q. Skup Gödelovih brojeva svih teorema od T nije definabilan u teoriji T.*

Dokaz. Označimo sa T^* skup Gödelovih brojeva svih teorema od T. Pretpostavimo da je skup T^* definabilan u teoriji T, tj. da postoji formula $F(x)$ tako da vrijedi

$$\text{ako} \ \ n \in T^* \ \ \text{tada} \ \ \vdash_T F(\overline{n}) \qquad (*)$$

$$\text{ako} \ \ n \notin T^* \ \ \text{tada} \ \ \vdash_T \neg F(\overline{n}) \qquad (**)$$

Iz dijagonalne leme slijedi da postoji rečenica G tako da vrijedi:

$$\vdash_T G \leftrightarrow \neg F(\ulcorner G \urcorner)$$

Označimo sa g Gödelov broj rečnice G. Iz prethodnog očito slijedi

$$\vdash G \leftrightarrow \neg F(\overline{g}) \qquad (***)$$

Pretpostavimo $\nvdash_T G$. Tada $g \notin T^*$. Iz $(**)$ slijedi $\vdash_T \neg F(\overline{g})$, a onda iz $(***)$ imamo $\vdash_T G$, čime je dobivena kontradikcija. Zaključujemo da mora vrijediti $\vdash_T G$. Iz $\vdash_T G$ slijedi $g \in T^*$. Tada iz $(*)$ slijedi $\vdash_T F(\overline{g})$, a onda iz $(***)$ slijedi $\vdash_T \neg G$. Time smo dobili da je teorija T inkonzistentna, što je suprotno pretpostavci leme. Dakle, pretpostavka da je skup T^* definabilan vodi na kontradikciju. □

Skup svih korektnih rečenica nazivamo **aritmetika**. U daljnjem izlaganju označavat ćemo tu teoriju sa $\mathcal{A}$.

Teorem 3.21. *(Teorem Tarskog o nedefinabilnosti aritmetike)*
Skup Gödelovih brojeva svih korektnih rečenica nije definabilan.

Dokaz. Očito je aritmetika $\mathcal{A}$ konzistentno proširenje teorije Q. Iz leme 3.20. slijedi da skup Gödelovih brojeva teorema od $\mathcal{A}$ nije definabilan. □

Teorem 3.22. *Skup Gödelovih brojeva svih korektnih rečenica nije rekurzivan.*

Dokaz. Pretpostavimo li da je skup Gödelovih brojeva svih korektnih rečenica rekurzivan tada iz leme 3.12. slijedi da je definabilan. No, to je nemoguće po prethodnom teoremu. □

Teorem 3.23. *(Bitna neodlučivost teorije Q)*
Niti jedno konzistentno proširenje teorije Q nije odlučivo.

Dokaz. Neka je teorija T konzistentno proširenje teorije Q. Označimo s T^* skup Gödelovih brojeva teorema teorije T. Iz leme 3.20. slijedi da skup T^* nije definabilan u teoriji T. Sada iz leme 3.12. slijedi da skup T^* nije rekurzivan. To znači da teorija T nije odlučiva. □

Teorem 3.24. *(Churchov teorem)*
Skup svih valjanih rečenica logike prvog reda nije odlučiv.

Dokaz. Označimo sa C konjunkciju aksioma teorije Q, te sa c označimo Gödelov broj rečenice C. Tada za svaku rečenicu A u jeziku aritmetike vrijedi:

$$\vdash_Q A \qquad \text{ako i samo ako} \qquad C \vdash_{FO} A$$

$$\text{ako i samo ako rečenica } \neg C \vee A \text{ je valjana}$$

Neka je $f : \mathbb{N} \to \mathbb{N}$ definirana sa $f(n) = disj(neg(c), n)$. Iz propozicije 3.1. slijedi da je funkcija f rekurzivna. Sa Λ^* označimo skup Gödelovih brojeva svih valjanih FO–rečenica, a sa Q^* skup Gödelovih brojeva svih teorema teorije Q. Iz prethodnih razmatranja imamo da za svaki $n \in \mathbb{N}$ vrijedi:

$$n \in Q^* \qquad \text{ako i samo ako} \qquad f(n) \in \Lambda^*$$

Pošto je funkcija f rekurzivna tada vrijedi:

skup Q^* je rekurzivan ako i samo ako skup Λ^* je rekurzivan.

Iz teorema 3.23. znamo da skup Q^* nije rekurzivan. □

Teorem 3.25. *(Gödelov prvi teorem nepotpunosti)*
Ne postoji konzistentno, potpuno i aksiomatizabilno proširenje teorije Q.

Dokaz. Iz teorema 3.6. znamo da je svako potpuno i aksiomatizabilno proširenje od Q odlučivo. No, iz teorema 3.23. znamo da niti jedno konzistentno proširenje od Q nije odlučivo. □

Korolar 3.26. *Aritmetika nije aksiomatizabilna.*

Dokaz. Aritmetika, tj. skup svih korektnih rečenica, je konzistentno i potpuno proširenje od Q. Iz Gödelovog prvog teorema nepotpunosti slijedi da aritmetika nije aksiomatizabilna. □

3.4 Gödelova i Rosserova rečenica

Neka je teorija T neko aksiomatizabilno proširenje od Q. Znamo da je skup svih rečenica koje su dokazive u T, a i skup svih rečenica čije su negacije dokazive u T, rekurzivno prebrojiv (vidi korolar 3.4.). Zatim, znamo da je svaki rekurzivan skup definabilan u teoriji T s rudimentarnom formulom. Iz toga slijedi da postoje rudimentarne formule $Prf_T(x, y)$ i $Disprf_T(x, y)$ tako da za sve rečenice A vrijedi:

$$\vdash_T A \quad \text{ako i samo ako} \quad \text{postoji } b \in \mathbb{N} \text{ tako da je rečenica } Prf_T(\lceil A \rceil, \overline{b}) \text{ korektna}$$

$$\vdash_T \neg A \quad \text{ako i samo ako} \quad \text{postoji } b \in \mathbb{N} \text{ tako da je rečenica } Disprf_T(\lceil \neg A \rceil, \overline{b}) \text{ korektna}$$

Označimo:

$$Prv_T(x) \quad \text{ako i samo ako} \quad \exists y Prf_T(x, y)$$

$$Disprv_T(x) \quad \text{ako i samo ako} \quad \exists y Disprf_T(x, y)$$

Očito su Prv_T i $Disprv_T$ $\exists$–rudimentarne formule. Iz dijagonalne leme slijedi da postoje rečenice G_T i R_T za koje vrijedi:

$$\vdash_T G_T \leftrightarrow \neg \exists y Prf_T(\lceil G_T \rceil, y)$$

$$\vdash_T R_T \leftrightarrow \forall y (Prf_T(\lceil R_T \rceil, y) \rightarrow \exists z < y Disprf(\lceil R_T \rceil, z))$$

Rečenicu G_T nazivamo **Gödelova rečenica** za teoriju T, a rečenicu R_T nazivamo **Rosserova rečenica** za teoriju T.
Za rečenicu F kažemo da je **neodlučiva** u teoriji T ako ne vrijedi $\vdash_T F$, a ni $\vdash_T \neg F$.

Teorem 3.27. *(Gödelov prvi teorem nepotpunosti u Rooserovoj formi)*
Neka je T konzistentno i aksiomatizabilno proširenje teorije Q. Tada je Rosserova rečenica R_T neodlučiva za teoriju T.

Za teoriju T u jeziku aritmetike kažemo da je ω–**inkonzistentna** ako postoji formula $F(x)$ tako da vrijedi $\vdash_T \exists x F(x)$, te za svaki $n \in \mathbb{N}$ vrijedi $\vdash_T \neg F(\overline{n})$. Inače kažemo da je teorija T ω–konzistentna. Svaka ω–konzistentna teorija je konzistentna, ali obrat ne vrijedi općenito.

Teorem 3.28. *(Gödelov prvi teorem nepotpunosti – orginalna forma)*
Neka je T konzistentno i aksiomatizabilno proširenje od Q. Tada je Gödelova rečenica G_T nedokaziva u T. Ako je teorija T ω–konzistentna tada ni rečenica $\neg G_T$ nije dokaziva u teoriji T.

Napomena 3.29. *Do sada smo kao osnovnu aritmetičku teoriju razmatrali minimalnu aritmetiku Q. Prisjetimo se aksioma Peanove aritmetike PA, te istaknimo vezu teorija Q i PA. Nelogički aksiomi od PA uz aksiome za jednakost su sljedeći:*

(1) $0 \neq x'$
(2) $x' = y' \rightarrow x = y$
(3) $x + 0 = x$
(4) $x + y' = (x + y)'$
(5) $x \cdot 0 = 0$
(6) $x \cdot y' = (x \cdot y) + x$

i shema aksioma indukcije

$$\Big(F(0) \ \wedge \ \forall x(F(x) \rightarrow F(x'))\Big) \ \rightarrow \ \forall x F,$$

gdje je F proizvoljna formula.

Prvo primijetimo da za razliku od teorije Q jezik od PA ne sadrži dvomjesni relacijski simbol $<$. No, to nije problem, jer u PA možemo uvesti pokratu: $x < y$ znači $\exists z(x + z' = y)$. Primjenom sheme aksioma indukcije mogu se dokazati svojstva relacije $<$ koja su iskazana u zadnja tri aksioma teorije Q. Dakle, Peanovu artimetiku možemo smatrati proširenjem teorije Q.

Goodsteinov teorem je jedna određena neodlučiva aritmetička istina. O tome možete čitati u [29]. O verzijima Ramseyevog teorema koje su neodlučive u PA možete čitati u [1].

3.5 Gödelov drugi teorem nepotpunosti

Neka je T neko proširenje teorije Q. Bilo smo definirali da je teorija T konzistentna ako iz nje nije izvediva barem jedna formula. Lako je vidjeti da je to ekvivalentno sa činjenicom da postoji rečenica F tako da F i $\neg F$ nisu istovremeno teoremi teorije T. Iz aksioma $(Q1)$ posebno slijedi $\vdash_T 0 \neq 1$. Iz toga slijedi da je teorija T konzistentna ako i samo ako $\nvdash_T 0 = 1$. Označimo:

$$Con_T \ \equiv \ \neg \ Prv_T(\ulcorner 0 = 1 \urcorner)$$

Lema 3.30. *(Hilbert–Bernaysovi uvjeti izvedivosti)*
Neka je T konzistentno i aksiomatizabilno proširenje od PA. Formulu $Prv_T(x)$ označavamo ovdje kratko sa $B(x)$. Za sve rečenice A, A_1 i A_2 vrijedi:

$(P1)$ *ako* $\vdash_T A$ *tada* $\vdash_T B(\ulcorner A \urcorner)$

$(P2)$ $\vdash_T B(\ulcorner A_1 \rightarrow A_2 \urcorner) \rightarrow \Big(B(\ulcorner A_1 \urcorner) \ \rightarrow B(\ulcorner A_2 \urcorner)\Big)$

$(P3)$ $\vdash_T B(\ulcorner A \urcorner) \ \rightarrow \ B(\ulcorner B(\ulcorner A \urcorner) \urcorner)$

Ovdje nije dovoljno da je teorija T proširenje teorije Q, jer se za dokaz nekih svojstva koristi i aksiom indukcije. Svaka formula $B(x)$ koja zadovljava uvjete $(P1)$–$(P3)$ naziva se **predikat dokazivosti** za teoriju T. (Lako je vidjeti da i npr. formula $B(x) \equiv x = x$ zadovoljava uvjete $(P1)$–$(P3)$.)
Ako je teorija T ω–konzistentna tada predikat dokazivosti $Prv_T(x)$ ima i sljedeće svojstvo:

$$(P4) \qquad \text{ako} \quad \vdash_T Prv_T(\lceil A \rceil) \quad \text{tada} \quad \vdash_T A$$

Teorem 3.31. *(Gödelov drugi teorem nepotpunosti)*
Neka je T konzistentno i aksiomatizabilno proširenje teorije PA. Tada vrijedi: $\vdash_T Con_T \rightarrow G_T$.

Dokaz. Sa $B(x)$ ćemo označavati predikat dokazivosti $Prv_T(x)$. Iz uvjeta izvedivosti $(P1)$ i $(P2)$ lako slijedi da za sve rečenice A_1 i A_2 vrijedi:

$$\text{ako} \quad \vdash_T A_1 \rightarrow A_2 \quad \text{tada} \quad \vdash_T B(\lceil A_1 \rceil) \rightarrow B(\lceil A_2 \rceil) \qquad (*)$$

Iz dijagonalne leme imamo da za Gödelovu rečenicu G_T za teoriju T vrijedi $\vdash_T G_T \leftrightarrow \neg B(\lceil G_T \rceil)$, tj.

$$\vdash_T \neg G_T \leftrightarrow B(\lceil G_T \rceil)$$

Iz ovog posljednjeg i $(*)$ slijedi

$$\vdash_T B(\lceil \neg G_T \rceil) \leftrightarrow B(\lceil B(\lceil G_T \rceil) \rceil) \qquad (**)$$

Iz uvjeta $(P3)$ znamo $\vdash_T B(\lceil G_T \rceil) \rightarrow B(\lceil B(\lceil G_T \rceil) \rceil)$. Iz ovog posljednjeg i $(**)$ slijedi da vrijedi

$$\vdash_T B(\lceil G_T \rceil) \rightarrow B(\lceil \neg G_T \rceil) \qquad (***)$$

Formula $G_T \rightarrow (\neg G_T \rightarrow 0 = 1)$ je valjana, pa posebno vrijedi
$\vdash_T G_T \rightarrow (\neg G_T \rightarrow 0 = 1)$. Sada iz $(*)$ slijedi

$$\vdash_T B(\lceil G_T \rceil) \rightarrow \Big(B(\lceil \neg G_T \rceil) \rightarrow B(\lceil 0 = 1 \rceil) \Big)$$

Iz ovog posljednjeg i $(***)$ lako je vidjeti da vrijedi

$$\vdash_T B(\lceil G_T \rceil) \rightarrow B(\lceil 0 = 1 \rceil)$$

Primjenom kontrapozicije dobivamo

$$\vdash_T \neg B(\lceil 0 = 1 \rceil) \ \rightarrow \ \neg B(\lceil G_T \rceil)$$

Pošto vrijedi $\vdash_T \neg B(\lceil G_T \rceil) \leftrightarrow G_T$, tada imamo

$$\vdash_T Con_T \ \rightarrow \ G_T. \qquad \square$$

Primijetimo da iz prvog i drugog Gödelovog teorema slijedi $\nvdash_T Con_T$.

Napomena 3.32. *Gödelov prvi teorem nepotpunosti dobili smo kao posljedicu sljedeća dva teorema:*

- *Svako aksiomatizabilno i potpuno proširenje od Q je odlučivo.*
- *Svako konzistentno proširenje od Q je neodlučivo.*

Sada ćemo dati dokaz Gödelovog prvog teorema nepotpunosti primjenom Hilbert–Bernaysovih uvjeta izvedivosti. Neka je T aksiomatizabilno i ω–konzistentno proširenje od PA. Iz dijagonalne leme slijedi da postoji rečenica G_T tako da vrijedi:

$$\vdash_T G_T \ \leftrightarrow \ \neg Prv_T(\lceil G_T \rceil) \qquad (*)$$

Pretpostavimo da vrijedi $\vdash_T G_T$. Iz $(*)$ slijedi da vrijedi $\vdash_T \neg Prv_T(\lceil G_T \rceil)$. U drugu ruku iz pretpostavke $\vdash_T G_T$ i uvjeta izvedivosti $(P1)$ slijedi $\vdash_T Prv_T(\lceil G_T \rceil)$. Time smo dobili da je teorija T inkonzistentna, što je suprotno početnoj pretpostavci. Dakle, mora vrijediti $\nvdash_T G_T$. Tada iz uvjeta izvedivosti $(P4)$ slijedi $\nvdash_T Prv_T(\lceil G_T \rceil)$. Iz $(*)$ slijedi $\nvdash_T \neg G_T$.

3.6 Löbov teorem

Gödelova rečenica je "fiksna točka" formule $\neg Prv_T(x)$. Iz dijagonalne leme slijedi da postoji i fiksna točka formule $Prv_T(x)$, tj. postoji rečenica H za koju vrijedi:

$$\vdash_T H \leftrightarrow Prv_T(\lceil H \rceil)$$

Rečenica H se naziva **Henkinova rečenica** za teoriju T. Postavlja se pitanje što je s dokazivošću Henkinove rečenice. O tome govori sljedeći Löbov teorem.

Teorem 3.33. *(Löbov teorem)*
Neka je T konzistentno i aksiomatizabilno proširenje teorije PA. Tada za svaku rečenicu A vrijedi:

$$\vdash_T Prv_T(\lceil A \rceil) \to A \qquad \textit{ako i samo ako} \qquad \vdash_T A$$

Dokaz. Očito $\vdash_T A$ povlači $\vdash_T Prv_T(\lceil A \rceil) \to A$. Za dokaz obrata promatra se fiksna točka formule $Prv_T(x) \to A$.

Iz Löbovog teorema slijedi odmah rješenje Henkinovog teorema:

$$\text{ako} \qquad \vdash_T H \leftrightarrow Prv_T(\lceil H \rceil) \quad \text{tada} \quad \vdash_T H$$

Napomena 3.34. *Lako je vidjeti da iz Löbovog teorema slijedi Gödelov drugi teorem nepotpunosti. S. Kripke je pokazao da vrijedi i obrat.*

Poglavlje 4

Dodatak: Izračunljivost

4.1 Teorija rekurzije

Smatramo (intuitivno) da je neka funkcija $f : S \subseteq \mathbb{N} \to \mathbb{N}$ **izračunljiva** ako postoji algoritam koji je izračunava. Smatramo da algoritam A izračunava funkciju $f : S \subseteq \mathbb{N} \to \mathbb{N}$ ako za svaki $\vec{x}$ vrijedi:

> algoritam A s ulaznim podatkom $\vec{x}$ stane, i kao izlazni podatak daje $f(\vec{x})$ ako i samo ako $\vec{x} \in S$.

Rekurzivne funkcije su jedan način formalne definicije izračunljive funkcije. Sve detalje o ovim temama, te sve dokaze možete vidjeti u skripti [30].

Rekurzivne funkcije i skupovi

Definicija 4.1. *Funkciju $Z : \mathbb{N} \to \mathbb{N}$ definiranu s $Z(x) = 0$ nazivamo* **nul–funkcija.** *Funkciju $Sc : \mathbb{N} \to \mathbb{N}$ definiranu sa $Sc(x) = x+1$ nazivamo* **funkcija sljedbenika** *(eng. successor). Neka je $n \in \mathbb{N}$ i $k \in \{1, \ldots, n\}$. Funkciju $I_k^n : \mathbb{N}^n \to \mathbb{N}$ definiranu s $I_k^n(x_1, \ldots, x_n) = x_k$ nazivamo* **projekcija.**
Funkcije Z, Sc i I_k^n $(n \in \mathbb{N},\ k \leq n)$ nazivamo **inicijalne funkcije**.

Uočite da je svaka inicijalna funkcija totalna.

U daljnjim izlaganjima promatrat ćemo i funkcije koje nisu totalne, pa ćemo se često susretati s izrazima koji za neke prirodne brojeve nisu definirani. Npr. izraz $\frac{x^2-4}{x-2}$ je nedefiniran za $x = 2$, a za sve ostale $x \in \mathbb{N}$ vrijednost izraza je prirodan broj. Važno je naglasiti da mi promatramo samo izraze i funkcije koji uvrštavanjem prirodnih brojeva poprimaju vrijednost koja je prirodan broj ili pak su nedefinirani. Ako je izraz X nedefiniran za neki $\vec{x} \in \mathbb{N}^k$ tada pišemo $X(\vec{x}) \uparrow$, a inače $X(\vec{x}) \downarrow$. Analogno, ako je f parcijalna funkcija, te $\vec{x} \in \mathbb{N}^k$ koji

nije u domeni funkcije f, tada to kratko označavamo s $f(\vec{x})\uparrow$. Ako pak je $\vec{x}$ u domeni funkcije tada to kratko označavamo s $f(\vec{x})\downarrow$.

Posebno nam je važna relacija jednakosti na izrazima, odnosno između parcijalnih funkcija. Neka su X i Y neki izrazi. Sa $X \simeq Y$ označavamo činjenicu da za svaku uređenu k–torku prirodnih brojeva vrijedi:

$$\begin{array}{l} X(\vec{x})\downarrow,\ Y(\vec{x})\downarrow \quad \text{i} \quad X(\vec{x}) = Y(\vec{x}); \\ \qquad\qquad\qquad \text{ili} \\ X(\vec{x})\uparrow \quad \text{i} \quad Y(\vec{x})\uparrow \end{array}$$

Kako bi definirali pojam rekurzivne funkcije moramo definirati još tri operacije: kompoziciju, primitivnu rekurziju i μ-operator.

Definicija 4.2. *Neka su G, $H_1, \ldots H_n$ funkcije. Neka je funkcija F definirana sa:*

$$F(\vec{x}) \simeq G(H_1(\vec{x}), \ldots, H_n(\vec{x})).$$

Tada kažemo da je funkcija F definirana pomoću **kompozicije** *funkcija.*

Definicija 4.3. *Neka je G totalna k–mjesna funkcija, H $(k+2)$-mjesna totalna funkcija. Neka je $(k+1)$-mjesna funkcija F definirana na sljedeći način:*

$$\begin{array}{rcl} F(0,\vec{x}) & = & G(\vec{x}) \\ F(y+1,\vec{x}) & = & H(F(y,\vec{x}), y, \vec{x}) \end{array}$$

Tada kažemo da je funkcija F definirana pomoću **primitivne rekurzije.** *Ako je $k = 0$ tada definicija funkcije F pomoću primitivne rekurzije izgleda:*

$$\begin{array}{rcl} F(0) & = & a \qquad (a \in \mathbb{N}) \\ F(y+1) & = & H(F(y), y) \end{array}$$

Definicija 4.4. *Najmanja klasa totalnih funkcija koja sadrži inicijalne funkcije, te je zatvorena za kompoziciju i primitivnu rekurziju, naziva se* **klasa primitivno rekurzivnih funkcija.**

Uočeno je da inicijalne funkcije, te kompozicija i primitivna rekurzija, nisu dovoljni kako bi se definirala svaka izračunljiva funkcija. Jedan primjer izračunljive funkcije koja nije primitivno rekurzivna je **Ackermanova funkcija**.

Kako bismo intutivno opisali tu funkciju, promotrimo prvotnu Ackermanovu definiciju te funkciju s tri argumenta. Tada definiramo $A(m,n,0) = m+n$. Za $p = 1$ imamo da je $A(m,n,1)$ jednako m^n. Za $p = 2$ imamo da je $A(m,n,2)$ jednako

$$m^{m^{\cdots^m}} \qquad (n \text{ nivoa broja } m)$$

Kako bi formalno definirali Ackermanovu funkciju prvo definiramo funkciju $sg : \mathbb{N} \to \mathbb{N}$ ovako:

$$sg(x) = \begin{cases} 0, & \text{ako je } x = 0; \\ 1, & \text{inače.} \end{cases}$$

Neka je funkcija $B : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definirana pomoću primitivne rekurzije na sljedeći način:

$$\begin{aligned} B(0, y) &= 2 + y \\ B(x + 1, 0) &= sg(x) \\ B(x + 1, y + 1) &= B(x, B(x + 1, y)) \end{aligned}$$

Sada Ackermanovu funkciju A definiramo sa $A(x) = B(x, x)$.

Želimo istaknuti da Ackermannova funkcija vrlo brzo raste. Npr. $B(4, 2)$ je jednako oko $2 \cdot 10^{19728}$, a vrijedonost $B(4, 3)$ je veća od procijenjenog broja atoma čitavog svemira.

Sljedeća propozicija govori o "virtualnim" varijablama.

Propozicija 4.5. *Neka je g primitivno rekurzivna k–mjesna funkcija, te x_1, $\ldots$, x_n različite varijable. Neka je za svaki i, gdje je $1 \leq i \leq k$, z_i jedna od varijabli $x_1, \ldots, x_n$. Neka je funkcija f definirana s $f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k)$. Tada je funkcija f primitivno rekurzivna.*

Primjenom prethodne propozicije odmah slijedi rekurzivnost nul–funkcije proizvoljne mjesnosti.

Propozicija 4.6. *Za sve prirodne brojeve k i n nul–funkcija N, koja je definirana sa $N(x_1, \ldots, x_k) = 0$, i konstantna funkcija C_n, koja je definirana sa $C_n(x_1, \ldots, x_k) = n$, su primitivno rekurzivne.*

Propozicija 4.7. *Sljedeće funkcije su primitivno rekurzivne:*

$$\begin{aligned} &(x, y) \mapsto x + y \\ &(x, y) \mapsto x \cdot y \\ &x \mapsto x! \\ &(x, y) \mapsto x^y \end{aligned}$$

(Po dogovoru stavljamo $0^0 = 1$, kako bi funkcija potenciranja bila totalna).

Sada definiramo μ–operator na funkcijama, te tako dobivamo klasu parcijalno rekurzivnih funkcija. Kao što smo prije već bili spomenuli, svaka izračunljiva funkcija nije primitivno rekurzivna. Upravo je μ–operator ta bitna razlika između primitivno rekurzivnih i izračunljivih funkcija.

Definicija 4.8.
Neka je f neka funkcija. Sa $\mu y(f(\vec{x},y) \simeq 0)$ označavamo funkciju definiranu na sljedeći način:

$$\mu y(f(\vec{x},y) \simeq 0) \simeq \begin{cases} z, & \text{najmanji } z, \text{ ako postoji, takav da je} \\ & f(\vec{x},y)\downarrow, \quad \text{za svaki } y < z, \\ & \text{te je} \quad f(\vec{x},z) = 0; \\ \\ \uparrow, & \text{inače} \end{cases}$$

*Tada kažemo da je funkcija $\mu y(f(\vec{x},y) \simeq 0)$ definirana pomoću μ–***operatora**.

Definicija 4.9. *Najmanja klasa funkcija koja sadrži sve inicijalne funkcije, te je zatvorena za kompoziciju, primitivnu rekurziju i μ-operator, naziva se klasa* **parcijalno rekurzivnih funkcija.** *Funkcija iz klase parcijalno rekurzivnih funkcija koja je totalna naziva se i* **rekurzivna funkcija**. *Kažemo da je* **relacija rekurzivna** *ako je njena karakteristična funkcija rekurzivna. Analogno, kažemo da je* **skup rekurzivan** *ako je njegova karakteristična funkcija rekurzivna.*

Iz definicija slijedi da je svaka primitivno rekurzivna funkcija ujedno i rekurzivna, a onda i parcijalno rekurzivna.

Oduzimanje nije totalna funkcija na skupu $\mathbb{N}$. Iz tog razloga definiramo sljedeću funkciju (**modificiranog oduzimanja**).

$$x \dot{-} y = \begin{cases} x - y, & \text{ako je} \quad x \geq y; \\ 0, & \text{inače.} \end{cases}$$

Da bismo dokazali da je funkcija $\dot{-}$ primitivno rekurzivna prvo definiramo funkciju pr (**funkcija prethodnik**) pomoću primitivne rekurzije ovako:

$$\begin{aligned} pr(0) &= 0 \\ pr(x+1) &= x \end{aligned}$$

Sada funkciju $\dot{-}$ možemo definirati pomoću primitivne rekurzije ovako:

$$\begin{aligned} x \dot{-} 0 &= x \\ x \dot{-} (y+1) &= pr(x \dot{-} y) \end{aligned}$$

Napomena 4.10. *U daljnjim razmatranjima koristit ćemo i sljedeću definiciju funkcije pomoću μ–operatora i relacije. Neka je R $(k+1)$-mjesna relacija. Sa $\mu y R(\vec{x}, y)$ označavamo funkciju definiranu na sljedeći način:*

$$\mu y R(\vec{x}, y) \simeq \begin{cases} \text{najmanji } z \text{ tako da vrijedi } \neg R(\vec{x}, y), \\ \text{za svaki } y < z \text{ i vrijedi } R(\vec{x}, z), \\ \text{ako takav postoji;} \\ \\ \uparrow, \text{ inače.} \end{cases}$$

Lako je vidjeti da time nismo proširili klasu parcijalno rekurzivnih funkciju jer za svaku relaciju R vrijedi:

$$\mu y R(\vec{x}, y) \simeq \mu y \Big(1 \dot{-} \chi_R(\vec{x}, y) \simeq 0 \Big)$$

Sljedeća napomena je jako važna jer naglašava grešku koja se često radi prilikom definicije μ–operatora.

Napomena 4.11. *Neka je $f(\vec{x}, y)$ parcijalno rekurzivna funkcija. Zatim, neka je s M označen operator definiran sa:*

$$M(f)(\vec{x}) = \begin{cases} \text{najmanji } z \text{ takav da je } f(\vec{x}, z) = 0, \\ \text{ako takav } z \text{ postoji;} \\ \\ \uparrow, \quad \text{inače} \end{cases}$$

Uočite da se operator M razlikuje od μ-operatora u tome što nema zahtjeva da je vrijednost funkcije f definirana na svim vrijednostima y koje su manje od z. Može se pokazati da klasa parcijalno rekurzivnih funkcija nije zatvorena za operator M.

Sada navodimo primjere primitivno rekurzivnih funkcija koje ćemo kasnije koristiti. Prilikom defincije Ackermanove funkcije naveli smo definiciju funkcije signum. Pošto funkciju sg možemo definirati pomoću primitivne rekurzije na sljedeći način:

$$\begin{aligned} sg(0) &= 0 \\ sg(x+1) &= 1 \end{aligned}$$

tada slijedi da je funkcija signum primitivno rekurzivna. Označimo sa $\overline{sg}$ funkciju definiranu sa:

$$\overline{sg}(x) = \begin{cases} 1, & \text{ako je } x = 0; \\ 0, & \text{inače.} \end{cases}$$

Očito vrijedi $\overline{sg}(x) = 1 \dot{-} sg(x)$, pa je funkcija $\overline{sg}$ primitivno rekurzivna.

Propozicija 4.12. *Neka su R i P (primitivno) rekurzivne relacije. Tada su i relacije $\neg R$, $R \wedge P$, $R \vee P$, $R \to P$ i $R \leftrightarrow P$ (primitivno) rekurzivne.*

Korolar 4.13. *Neka su A i B rekurzivni skupovi. Tada su i A^c, $A \cap B$ i $A \cup B$ rekurzivni skupovi. Presjek, odnosno unija, konačno mnogo rekurzivnih skupova je rekurzivan skup.*

Propozicija 4.14. *Relacije $\leq$, $\geq$, $<$, $>$ i $=$ su primitivno rekurzivne.*

Propozicija 4.15. *(Definicija funkcije po slučajevima – verzija 1)*
Neka su $R_1, \ldots R_n$ (primitivno) rekurzivne relacije koje imaju svojstvo da za sve $\vec{x}$ postoji točno jedan $i \in \{1, \ldots, n\}$ tako da vrijedi $R_i(\vec{x})$. Neka su $F_1, \ldots, F_n$ (primitivno) rekurzivne funkcije. Tada je funkcija $F : \mathbb{N}^k \to \mathbb{N}$ definirana sa:

$$F(\vec{x}) = \begin{cases} F_1(\vec{x}), & \text{ako vrijedi } R_1(\vec{x}), \\ \vdots & \\ F_n(\vec{x}), & \text{ako vrijedi } R_n(\vec{x}) \end{cases}$$

također (primitivno) rekurzivna.

Propozicija 4.16. *Neka je F (primitivno) rekurzivna funkcija, a G totalna funkcija koja ima svojstvo da vrijedi $G(\vec{x}) = F(\vec{x})$, osim možda za konačno mnogo $\vec{x}$. Tada je funkcija G također (primitivno) rekurzivna.*

Korolar 4.17. *Neka je R relacija za koju postoji najviše konačno mnogo $\vec{x}$ takvih da vrijedi $R(\vec{x})$. Tada je relacija R primitivno rekurzivna.*

Korolar 4.18. *Svaki konačan skup je primitivno rekurzivan.*

Propozicija 4.19. *(Ograničene sume)*
Neka su g, α i β (primitivno) rekurzivne funkcije. Tada su (primitivno) rekurzivne i sljedeće funkcije:

$$a) \quad f(\vec{x}, y) = \sum_{i=0}^{y} g(\vec{x}, i).$$

$$b) \quad f(\vec{x}, y, z) = \begin{cases} \sum_{i=y}^{z} g(\vec{x}, i), & \textit{ako je} \quad y \leq z; \\ \\ 0, & \textit{inače.} \end{cases}$$

$$c) \quad f(\vec{x}) = \begin{cases} \sum_{i=\alpha(\vec{x})}^{\beta(\vec{x})} g(\vec{x}, i), & \textit{ako je} \quad \alpha(\vec{x}) \leq \beta(\vec{x}); \\ \\ 0, & \textit{inače.} \end{cases}$$

Propozicija 4.20. *(Ograničeni produkti)*
Neka su g, α i β (primitivno) rekurzivne funkcije. Tada su (primitivno) rekurzivne i sljedeće funkcije:

$$a) \quad f(\vec{x}, y) = \prod_{i=0}^{y} g(\vec{x}, i).$$

$$b) \quad f(\vec{x}, y, z) = \begin{cases} \prod_{i=y}^{z} g(\vec{x}, i), & \textit{ako je} \quad y \leq z; \\ \\ 1, & \textit{inače.} \end{cases}$$

$$c) \quad f(\vec{x}) = \begin{cases} \prod_{i=\alpha(\vec{x})}^{\beta(\vec{x})} g(\vec{x}, i), & \textit{ako je} \quad \alpha(\vec{x}) \leq \beta(\vec{x}); \\ \\ 1, & \textit{inače.} \end{cases}$$

(Uočite da je definirano da su "prazni" produkti jednaki 1).

Ako je $R(\vec{x}, y)$ rekurzivna relacija tada općenito relacije $\exists y R(\vec{x}, y)$ i $\forall y R(\vec{x}, y)$ ne moraju biti rekurzivne. Nije teško dokazati da je primjenom ograničene kvantifikacije sačuvana rekurzivnost. To ističemo u sljedećoj propoziciji.

Propozicija 4.21. *Neka je R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:*

$$\exists y < z \ R(\vec{x}, y)$$
$$\exists y \leq z \ R(\vec{x}, y)$$
$$\forall y < z \ R(\vec{x}, y)$$
$$\forall y \leq z \ R(\vec{x}, y)$$

Korolar 4.22. *Neka je R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:*

$$\exists y_{z_1<y<z_2} \ R(\vec{x}, y)$$
$$\exists y_{z_1\leq y\leq z_2} \ R(\vec{x}, y)$$
$$\forall y_{z_1<y<z_2} \ R(\vec{x}, y)$$
$$\forall y_{z_1\leq y\leq z_2} \ R(\vec{x}, y)$$

Korolar 4.23. *Neka su α i β (primitivno) rekurzivne funkcije, a R (primitivno) rekurzivna relacija. Tada su (primitivno) rekurzivne i sljedeće relacije:*

$$\exists y_{\alpha(\vec{x})<y<\beta(\vec{x})} \ R(\vec{x}, y)$$
$$\exists y_{\alpha(\vec{x})\leq y\leq\beta(\vec{x})} \ R(\vec{x}, y)$$
$$\forall y_{\alpha(\vec{x})<y<\beta(\vec{x})} \ R(\vec{x}, y)$$
$$\forall y_{\alpha(\vec{x})\leq y\leq\beta(\vec{x})} \ R(\vec{x}, y)$$

Sljedeća propozicija govori da primjenom "ograničenog" μ-operatora na rekurzivnu relaciju dobivamo rekurzivnu (totalnu!) funkciju.

Propozicija 4.24. *Neka je R (primitivno) rekurzivna relacija. Neka je funkcija $f : \mathbb{N}^k \to \mathbb{N}$ definirana sa:*

$$f(\vec{x}) = \begin{cases} \text{najmanji } y \text{ takav da vrijedi } R(\vec{x}, y) \ \ i \ \ y < z, \\ \text{ako takav } y \text{ postoji}; \\ \\ z, \ \text{inače}, \end{cases}$$

(primitivno) rekurzivna. Obično se tako definirana funkcija f označava i sa $\mu y < z \ R(\vec{x}, y)$

Korolar 4.25. *Neka su α i β (primitivno) rekurzivne funkcije, a R (primitivno) rekurzivna relacija. Neka je funkcija $f : \mathbb{N}^k \to \mathbb{N}$ definirana s:*

$$f(\vec{x}) = \begin{cases} \text{najmanji } \ y \ \text{ takav da vrijedi } \ R(\vec{x}, y) \ \ i \ \ \alpha(\vec{x}) < y < \beta(\vec{x}), \\ \text{ako takav } \ y \ \text{ postoji;} \\ \\ \beta(\vec{x}), \quad \text{inače} \end{cases}$$

Ovako definiranu funkciju f obično označavamo s

$$\mu y_{\alpha(\vec{x})<y<\beta(\vec{x})}\ R(\vec{x},y)$$

Analogno se definiraju i funkcije:

$$\mu y_{\alpha(\vec{x})\leq y\leq\beta(\vec{x})}\ R(\vec{x},y)$$
$$\mu y_{\alpha(\vec{x})<y\leq\beta(\vec{x})}\ R(\vec{x},y)$$
$$\mu y_{\alpha(\vec{x})\leq y<\beta(\vec{x})}\ R(\vec{x},y)$$

Sve te funkcije su (primitivno) rekurzivne.

Kleenijev teorem i posljedice

Sada navodimo osnovne teoreme iz teorije rekurzije. To je prije svega Kleenijev teorem o normalnoj formi.

Teorem 4.26. *(Kleenijev teorem o normalnoj formi)*
Postoji primitivno rekurzivna funkcija U, i za svaki $k \geq 1$ postoji primitivno rekurzivna relacija T_k tako da za svaku k–mjesnu parcijalno rekurzivnu funkciju φ postoji $e \in \mathbb{N}$ tako da vrijede sljedeće tvrdnje:

a) $\varphi(\vec{x})\downarrow$ *ako i samo ako postoji y tako da vrijedi $T_k(e,\vec{x},y)$;*

b) $\varphi(\vec{x}) \simeq U(\mu y T_k(e,\vec{x},y))$

Broj e iz iskaza Kleenijevog teorema naziva se **indeks** funkcije φ.

Definicija 4.27. *Za svaki $e,k \in \mathbb{N}$ definiramo k–mjesnu funkciju $\{e\}$ ovako:*

$$\{e\}(\vec{x}) \simeq U(\mu y T_k(e,\vec{x},y))$$

Neka je $\varphi : S \subseteq \mathbb{N}^k \to \mathbb{N}$ neka funkcija. Kažemo da za funkciju φ postoji **indeks** *ako postoji $e \in \mathbb{N}$ takav da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi $\varphi(\vec{x}) \simeq \{e\}(\vec{x})$.*

Teorem 4.28. *Funkcija $\varphi : S \subseteq \mathbb{N}^k \to \mathbb{N}$ je parcijalno rekurzivna ako i samo ako postoji indeks za f.*

Teorem 4.29. *(Definicija funkcije po slučajevima – verzija 2)*
Neka su $R_1, \ldots, R_n$ rekurzivne relacije koje imaju svojstvo da za svaki $\vec{x} \in \mathbb{N}^k$ postoji najviše jedan $i \in \{1,\ldots,n\}$ za kojeg vrijedi $R_i(\vec{x})$. Neka su $F_1, \ldots, F_n$ neke k–mjesne parcijalno rekurzivne funkcije. Funkciju F definiramo po slučajevima ovako:

$$F(\vec{x}) \simeq \begin{cases} F_1(\vec{x}), & \text{ako vrijedi } R_1(\vec{x}); \\ \vdots & \\ F_n(\vec{x}), & \text{ako vrijedi } R_n(\vec{x}). \end{cases}$$

Tada je funkcija F parcijalno rekurzivna.

Teorem 4.30. *Za svaku parcijalno rekurzivnu funkciju φ postoji definicija u kojoj se μ-operator pojavljuje najviše jednom.*

Teorem 4.31. *(Teorem o parametru ili S_n^m–teorem)*
Neka su m i n prirodni brojevi različiti od nule. Tada postoji rekurzivna funkcija $S_n^m : \mathbb{N}^{m+1} \to \mathbb{N}$ tako da za sve $e \in \mathbb{N}$, $\vec{x} \in \mathbb{N}^n$ i $\vec{y} \in \mathbb{N}^m$ vrijedi

$$\{S_n^m(e, \vec{y})\}(\vec{x}) \simeq \{e\}(\vec{y}, \vec{x})$$

Teorem 4.32. *(Teorem rekurzije)*
Neka je G neka $(k+1)$–mjesna parcijalno rekurzivna funkcija. Tada postoji $e \in \mathbb{N}$ tako da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi

$$\{e\}^k(\vec{x}) \simeq G(e, \vec{x}).$$

Teorem 4.33. *(Teorem o fiksnoj točki)*
Za svaku unarnu parcijalnu rekurzivnu funkciju F postoji $e \in \mathbb{N}$ tako da vrijedi $\{e\} \simeq \{F(e)\}$.

Teorem 4.34. *(Riceov teorem)*
Neka je S rekurzivan podskup od $\mathbb{N}$ koji ima svojstvo da za sve $i, j \in \mathbb{N}$, takve da je $i \in S$ i $\{i\} \simeq \{j\}$ slijedi $j \in S$. Tada je $S = \emptyset$ ili $S = \mathbb{N}$.

Churhova teza

Smatramo da je svaka parcijalno rekurzivna funkcija izračunljiva (u intuitivnom smislu koji smo opisali na samom uvodu). Alonso Church je 1936. godine postavio tezu da vrijedi i obrat. Zbog važnosti sada je posebno ističemo.

Churchova teza:

svaka izračunljiva funkcija je parcijalno rekurzivna.

Pošto je pojam izračunljive funkcije intuitivan pojam, tj. nije strogo definiran, nemoguće je dati dokaz Churchove teze. Oboriti pak Churchovu tezu značilo bi odrediti funkciju za koju bi se svi složili da je izračunljiva, a istovremeno bi dokazali da nije parcijalno rekurzivna. No, to do sada nije učinjeno. Ovdje navodimo dvije važne činjenice zbog kojih Churchovu tezu smatramo istinitu.

1. Razni načini definiranja novih funkcija pomoću već danih parcijalno rekurzivnih funkcija (npr. simultana rekurzija, povratna rekurzija, definicija funkcija po slučajevima, ...) daju ponovno parcijalno rekurzivne funkcije.

2. Sve do sada poznate definicije koje imaju za cilj opisati klasu izračunljivih funkcija (parcijalno rekurzivne funkcije, RAM–izračunljive funkcije, Turing–izračunljive, ABAK–izračunljive, ...) definiraju istu klasu funkcija.

Važnost Churchove teze je vrlo velika. Ona se primjenjuje uvijek prilikom dokaza nepostojanja algoritma za rješavanje nekog problema (tj. nerješivosti problema). Sada dajemo jedan primjer takvog problema.

Primjer 4.35. Postoji funkcija koja nije izračunljiva
U svrhu dokaza gornje tvrdnje definiramo funkciju F na sljedeći način:

$$F(x) \simeq \begin{cases} \{x\}(x)+1, & \textit{ako je } \{x\}(x) \downarrow; \\ 0, & \textit{inače.} \end{cases}$$

Lako je vidjeti da niti za jedan $e \in \mathbb{N}$ ne vrijedi $F \simeq \{e\}$. To znači da za funkciju F ne postoji indeks, a tada znamo da funkcija F nije parcijalno rekurzivna. Primjenom Churchove teze slijedi da funkcija F nije izračunljiva.

Aritmetička hijerarhija

Sada ćemo proučavati što se događa s relacijom kada je kvantificiramo s neograničenim kvantifikatorima. Prisjetimo se: ako je relacija R (primitivno) rekurzivna relacija tada su i relacije $(\forall z < y)R(\vec{x}, z)$ i $(\exists z < y)R(\vec{x}, z)$ (primitivno) rekurzivne.

Definicija 4.36. *Kažemo da je relacija $R \subseteq \mathbb{N}^k$* **aritmetička** *ako postoji rekurzivna relacija P tako da vrijedi:*

$$R(\vec{x}) \quad \textit{ako i samo ako} \quad Q_1 y_1 \ldots Q_n y_n P(\vec{x}, y_1, \ldots, y_n),$$

gdje je Q_i simbol $\forall$ ili $\exists$. Riječ $Q_1 y_1 \ldots Q_n y_n$ nazivamo **prefiks**.

Sada nam je cilj pokazati da svaka aritmetička relacija može biti prikazana u vrlo jednostavnom obliku, tj. da njen prefiks možemo zapisati u ekvivalentnom "standardnom" obliku. U tu svrhu prvo istićemo sljedeću propoziciju.

Propozicija 4.37. *Neka je R rekurzivna relacija. Tada postoje rekurzivne relacije P i Q tako da vrijedi:*

$$\forall y \forall z R(\vec{x}, y, z) \quad \textit{ako i samo ako} \quad \forall u P(\vec{x}, u), \quad i$$

$$\exists y \exists z R(\vec{x}, y, z) \quad \textit{ako i samo ako} \quad \exists u Q(\vec{x}, u).$$

Primjenom prethodne propozicije slijedi da uvijek možemo vršiti **kontrakciju** istovrsnih kvantifikatora. Kažemo da je prefiks **alternirajući** ako ne sadrži dva uzastopna egzistencijalna ili univerzalna kvantifikatora.

Definicija 4.38. *Neka je $n > 0$. Kažemo da je prefiks Π_n^0 ako je alternirajući, sadrži n kvantifikatora i prvi kvantifikator slijeva je $\forall$.*
Kažemo da je prefiks Σ_n^0 ako je alternirajući, sadrži n kvantifikatora i prvi kvantifikator slijeva je $\exists$.
Kažemo da je relacija R jedna Π_n^0 relacija ako postoji rekurzivna relacija P i prefiks $Q_1 y_1 \dots Q_n y_n$, koji je Π_n^0, tako da vrijedi

$$R(\vec{x}) \quad \textit{ako i samo ako} \quad Q_1 y_1 \dots Q_n y_n P(\vec{x}, y_1, \dots, y_n).$$

Ponekad ćemo pisati $R \in \Pi_n^0$, te govoriti da je Π_n^0 oznaka klase svih Π_n^0 relacija. Slično definiramo pojam Σ_n^0 relacije.
Kažemo da je relacija Δ_n^0 ako je istovremeno Π_n^0 i Σ_n^0.
Bilo koji od simbola Π_0^0, Σ_0^0 i Δ_0^0 nam označava klasu svih rekurzivnih relacija.

Jasna je uloga donjeg indeksa u oznakama Π_n^0, Σ_n^0 i Δ_n^0. Gornji indeks, tj. nula, označava da se radi o relacijama "na brojevima". Relacija koja bi bila npr. Π_n^1 djelovala bi na skupovima brojeva.

Očito je svaka rekurzivna relacija Δ_n^0, za sve $n \in \mathbb{N}$ (kao prefiks možemo staviti irelevantne kvantifikatore). To znači da su npr. relacije $=$, $\leq$ i $>$ primjeri Δ_7^0 relacija. Relacija $\exists x \forall y (x = y \wedge x < z)$ je jedna Σ_2^0 relacija, dok je $\forall x \exists z \forall y (x \cdot y < z)$ jedna Π_3^0 relacija.

Iz propozicije 4.37. slijedi da prefiks svake aritmetičke relacije možemo napisati u alternirajućem obliku iz čega odmah slijedi tvrdnja sljedeće propozicije, jer svakoj relaciji možemo dodati irelevantne kvantifikatore.

Propozicija 4.39. *Svaka aritmetička relacija je Π_n^0 ili Σ_n^0, za neki $n \in \mathbb{N}$.*

Propozicija 4.40. *Ako je* $R \in \Pi^0_n$ *ili* $R \in \Sigma^0_n$, *za neki* $n \in \mathbb{N}$, *tada je* $R \in \Delta^0_k$ *za svaki* $k > n$. *Za svaki* $k \in \mathbb{N}$ *vrijedi* $\Pi^0_k \subseteq \Pi^0_{k+1}$, *odnosno* $\Sigma^0_k \subseteq \Sigma^0_{k+1}$.

Neka su P i R aritmetičke relacije proizvoljne mjesnosti, a Q neka je simbol $\forall$ ili $\exists$. Tada iz sljedeće tablice čitamo djelovanje logičkih veznika i kvantifikatore na dane relacije.

P, R	$\neg P$	$P \vee R$	$P \wedge R$	$\forall x P$	$\exists x P$	$(Qx < y)P$
Π^0_n	Σ^0_n	Π^0_n	Π^0_n	Π^0_n	Σ^0_{n+1}	Π^0_n
Σ^0_n	Π^0_n	Σ^0_n	Σ^0_n	Π^0_{n+1}	Σ^0_n	Σ^0_n
Δ^0_n	Δ^0_n	Δ^0_n	Δ^0_n	Π^0_n	Σ^0_n	Δ^0_n

Klasifikaciju aritmetičkih relacija na Π^0_n i Σ^0_n relacije nazivamo **aritmetička hijerarhija.**

Teorem 4.41. *(Teorem o aritmetičkoj hijerarhiji)*
Za svaki $n > 0$ *postoji* Π^0_n *relacija koja nije* Σ^0_n, *te postoji* Σ^0_n *relacija koja nije* Π^0_n.

Korolar 4.42. *a) Za sve* $i < j$ *vrijedi:*

$$\Pi^0_i \subset \Sigma^0_j, \qquad \Pi^0_i \subset \Pi^0_j, \qquad \Sigma^0_i \subset \Pi^0_j \qquad i \qquad \Sigma^0_i \subset \Sigma^0_j$$

b) Za svaki $i \in \mathbb{N}$ *vrijedi:*

$$\Pi^0_i \cup \Sigma^0_i \subset \Pi^0_{i+1} \cap \Sigma^0_{i+1}$$

Rekurzivno prebrojivi skupovi

Intuitivno, neki skup smatramo odlučiv ili rekurzivan ako postoji algoritam koji za svaki prirodan broj može odrediti pripada li skupu. Neki skup smatramo rekurzivno prebrojivim ako postoji algoritam koji za svaki prirodan broj, kao ulazni podatak algoritma, kao izlazni podatak daje neki element skupa, te će primjenom algoritma svaki element skupa biti dobiven kao izlazni rezultat.

Definicija 4.43. *Kažemo da je neka relacija $R \subseteq \mathbb{N}^k$* **rekurzivno prebrojiva** *ako je R domena neke parcijalno rekurzivne funkcije. Kratko ćemo reći da je to RE relacija (recursively enumerable).*

Skupovi $\mathbb{N}$ i $\emptyset$ su rekurzivno prebrojivi. Svaki rekurzivan skup S je rekurzivno prebrojiv, jer je S domena sljedeće parcijalno rekurzivne funkcije

$$f(x) \simeq \begin{cases} 1, & \text{ako je } \ x \in S \\ \uparrow, & \text{inače} \end{cases}$$

Propozicija 4.44. *Relacija R je rekurzivno prebrojiva ako i samo ako je R jedna Σ_1^0 relacija.*

Teorem 4.45.
Postoji RE skup koji nije rekurzivan.

Dokaz. Iz teorema o aritmetičkoj hijerahiji slijedi da postoji *RE* skup S (tj. unarna Σ_1^0 relacija) koji nije Π_1^0. Pretpostavimo da je S rekurzivan skup. Znamo da je tada i skup S^c rekurzivan. To znači da je i S^c jedna *RE* skup. Tada slijedi da je skup $(S^c)^c$, tj. S, jedan Π_1^0 skup, što je kontradikcija. □

Primjer 4.46. *Promotrimo diofantsku jednadžbu $p(\vec{x}, y) = q(\vec{x}, y)$, gdje su p i q polinomi s varijablama $\vec{x}$ i y, te s koeficijentima iz skupa $\mathbb{Z}$. Neka je D skup definiran sa:*

$$y \in D \text{ ako i samo ako } \exists \vec{x}(p(\vec{x}, y) = q(\vec{x}, y))$$

Lako je vidjeti da je D jedan RE skup. Prilikom rješavanja desetog Hilbertovog problema dokazano je da vrijedi i obrat, tj. svaki RE skup je skup rješenja neke diofantske jednadžbe.

Definicija 4.47. *Neka je F neka k–mjesna funkcija.* **Graf** *od F je $(k+1)$–mjesna relacija G_F definirana sa:*

$$G_F(\vec{x}, y) \ \text{ ako i samo ako } \ F(\vec{x}) \simeq y.$$

Teorem 4.48. *(Teorem o grafu)*
Neka je $F : S \subseteq \mathbb{N}^k \to \mathbb{N}$ proizvoljna funkcija. Tada vrijede sljedeće tvrdnje:

a) funkcija F je parcijalno rekurzivna ako i samo ako je graf od F jedna RE relacija;

b) funkcija F je rekurzivna ako i samo ako je graf od F rekurzivna relacija.

Propozicija 4.49. *(Definicija funkcije po slučajevima – verzija 3)*
Neka su $R_1, \ldots, R_n$ neke RE relacije koje imaju svojstvo da za svaki $\vec{x} \in \mathbb{N}^k$ postoji najviše jedan $i \in \{1, \ldots, n\}$ tako da vrijedi $R_i(\vec{x})$. Neka su $F_1, \ldots, F_n$ proizvoljne parcijalno rekurzivne funkcije. Definiramo funkciju F na sljedeći način:

$$F(\vec{x}) \simeq \begin{cases} F_1(\vec{x}), & \text{ako vrijedi } R_1(\vec{x}); \\ \quad \vdots & \\ F_n(\vec{x}), & \text{ako vrijedi } R_n(\vec{x}), \end{cases}$$

gdje se podrazumijeva da $F(\vec{x})$ nije definirano ako niti za jedan $i \in \{1, \ldots, n\}$ nije ispunjeno $R_i(\vec{x})$. Tada je funkcija F parcijalno rekurzivna.

Teorem 4.50. *Relacija R je rekurzivna ako i samo ako su relacije R i $\neg R$ rekurzivno prebrojive.*

Propozicija 4.51. *Neka je A neprazan podskup od $\mathbb{N}$. Tada vrijede sljedeće tvrdnje:*

a) skup A je rekurzivno prebrojiv ako i samo ako je skup A slika neke parcijalno rekurzivne funkcije;

b) beskonačan skup A je rekurzivno prebrojiv ako i samo ako je skup A slika neke parcijalno rekurzivne funkcije koja je injekcija.

4.2 Turingovi strojevi

Pošto ćemo u daljnjem tekstu često koristiti pojmove vezane uz proizvoljnoe alfabete, prvo ćemo ovdje navesti pojmove s time u vezi.

Alfabet je proizvoljan neprazan skup. Svaki element alfabeta nazivamo **simbol** ili **znak. Riječ** alfabeta je svaki konačan niz danog alfabeta. **Duljina riječi** je broj simbola koji dolaze u riječi. Duljinu riječi w označavamo sa $|w$. Ako je sa A označen neki alfabet tada se skup svih riječi obično označava sa A^*. Po dogovoru smatramo da skup svih riječi proizvoljnog alfabeta sadrži **praznu riječ**, tj. prazan niz simbola. Najvažnija operacija na skupu riječi je **konkatenacija.** Konkatenacija je binarna operacija na A^*, koja je definirana na sljedeći način: ako su a i b riječi (bolje reći oznake za riječi!) tada kažemo da je riječ

ab nastala konkatenacijom riječi a i b. Kažemo da je b **podriječ** riječi a ako postoje riječi c i d tako da je riječ a nastala konkatenacijom riječi c, b i d, tj. a je jednaka cbd.

Navodimo neke primjere alfabeta. Neka je $A_1 = \{\alpha, \beta\}$. Neke riječi tog alfabeta su npr. $\alpha\alpha\alpha$, $\alpha\beta\alpha\beta\beta\beta$, $\alpha\alpha\beta\beta\alpha\alpha\beta$. Iz riječi $\alpha\alpha\beta\beta$ i $\beta\beta\alpha\beta$ konkatenacijom dobivamo riječ $\alpha\alpha\beta\beta\beta\beta\alpha\beta$.

Neka je, zatim, $A_2 = \{+, \cdot, s, 0, =\} \cup \{x_n : n \in \mathbb{N}\}$. Tada su riječi alfabeta A_2 npr. $x_1 + x_2 = x_2$, $x_1 \cdot x_4 + 0 = x_5$, ali i $++\cdot x_4 ===$.

Propozicija 4.52. *Skup svih riječi konačnog ili prebrojivog alfabeta je prebrojiv.*

Pojam Turingovog stroja definirali su manje–više istovremeno 1936. godine Alan Turing (1912.–1954.) i Emil Post (1897.–1954.). Intuitivno, Turingov stroj je automat koji manipulira simbolima na beskonačnoj traci koja je neomeđena slijeva i zdesna, pri čemu su ti simboli iz fiksiranog konačnog alfabeta. Traka je podijeljena u **registre** (kao filmska traka). U svakom registru može biti zapisan samo jedan simbol. U jednom trenutku glava čitača može promatrati samo jedan registar. Turingov stroj ima samo konačan broj **stanja**.

Turingov stroj može izvršavati četiri akcije:

a) pomaknuti glavu čitača za jedan registar lijevo;

b) pomaknuti glavu čitača za jedan registar desno;

c) pročitati simbol iz registra kojeg promatra;

d) napisati simbol (iz danog skupa simbola) u registar (odnosno, izbrisati postojeći simbol i napisati novi).

Sada dajemo formalnu definiciju Turingovog stroja.

Definicija 4.53. Turingov stroj *je uređena šestorka* $(\mathcal{S}, \Gamma, q_0, s_0, F, \Pi)$, *gdje je redom:*

- $\mathcal{S}$ *konačan skup, čije elemente nazivamo* **stanja**;
- Γ *je konačan skup, kojeg nazivamo* **alfabet**;
- q_0 *je element iz* $\mathcal{S}$ *i nazivamo ga* **početno stanje**;

- s_0 *je element od* Γ *i nazivamo ga* **prazni simbol**;
- F *je podskup od* $\mathcal{S}$ *i njegove elemente nazivamo* **završna stanja**;
- Π *je proizvoljna funkcija sa* $\Gamma \times \mathcal{S}$ *u skup* $\Gamma \times \{L, D, H\} \times \mathcal{S}$ *i nazivamo je* **funkcija prijelaza**.

  (Simboli L i D znači da će se glava za čitanje pomaknuti lijevo, odnosno desno, a simbol H znači da glava za čitanje ostaje na mjestu).

Primjer 4.54. *Na traci se nalazi zapisan prirodan broj veći od nule u unarnom zapisu (npr. broj 5 je zapisan kao IIIII). Definirat ćemo Turingov stroj koji određuje binarni zapis tog broja. Glava čitača se na početku nalazi na krajnjem lijevom znaku. Prvo dajemo opis rada stroja po koracima, a onda ćemo ga točno zadati tablicom.*

1) pomak na zadnji desni znak I;

2) obrisati zadnji desni znak I;

3) pomak na prvo lijevo prazno mjesto;

4) na prazno mjesto pišemo 1;

5) pomak na zadnji desni znak I;

6) obrisati zadnji desni znak I;

7) pomak lijevo do prve znamenke zdesna;

8) ako je znamenka 0 tada je treba obrisati i napisati 1, te primijenimo korak 10); ako je znamenka 1 tada je treba obrisati i napisati 0, te pomaknuti se jedno mjesto lijevo;

9) ako je opet pročitana neka znamenka (0 ili 1) tada se vratimo na korak 8);

10) vraćamo se na korak 5) ako još ima znakova I, a inače stroj stane.

Sada traženi Turingov stroj zadajemo tablicom.

	q_0	q_1	q_2
0	$0Dq_0$	$0Hq_{STOP}$	$1Dq_0$
1	$1Dq_0$	$1Hq_{STOP}$	$0Lq_2$
s_0	s_0Lq_1	s_0Hq_{STOP}	$1Dq_0$
I	IDq_0	s_0Lq_2	ILq_2

Dakle, dani Turingov stroj ima četiri moguća stanja: $q_0,\ q_1,\ q_2$ *i* q_{STOP} *(završno stanje). Skup dozvoljenih simbola je* $\{s_0, I, 0, 1\}$.

Sada razmatramo Turingove strojeve koji imaju točno dva različita završna stanja koja označavamo sa q_{DA} i q_{NE}.

Definicija 4.55. *Kažemo da Turingov stroj* $T = (\mathcal{S}, \Gamma, q_0, s_0, \{q_{DA}, q_{NE}\}, \Pi)$ **prepoznaje riječ** $w \in \Gamma^*$ *ako taj Turingov stroj staje u konačno mnogo koraka u završnom stanju* q_{DA} *kada je na početku rada stroja na traci zapisana samo riječ* w. *Za proizvoljan Turingov stroj* T *sa* $L(T)$ *označavamo skup svih riječi koji* T *prepoznaje. Svaki podskup skupa* Γ^* *svih riječi nazivamo* **jezik**. *Kažemo da neki Turingov stroj* T **prepoznaje jezik** L *ako vrijedi* $L = L(T)$. *Za neki jezik* L *kažemo da je* **Turing–prepoznatljiv** *ako postoji Turingov stroj koji ga prepoznaje.*

Primijetimo: ako Turingov stroj T prepoznaje jezik L, te je $w \in \Gamma^* \setminus L$, tada Turingov stroj T koji na početku kao ulazni podatak ima na traci zapisanu riječ w uopće ne mora stati, tj. ne mora nužno završiti sa stanjem q_{NE}.

Definicija 4.56. *Za neki jezik* L *kažemo da je* **Turing–odlučiv** *ako postoji Turingov stroj* T *koji ga prepoznaje, te za svaku riječ* $w \in \Gamma^* \setminus L$ *stoj staje u završnom stanju* q_{NE}.

Teorem 4.57. *Jezik* $L \subseteq \Gamma^*$ *je Turing–odlučiv ako i samo ako su jezici* L *i* $\Gamma^* \setminus L$ *Turing–prepoznatljivi.*

Definicija 4.58. *Kažemo da su dva Turingova stroja* **ekvivalentna** *ako prepoznaju iste jezike.*

Turingov stroj s više traka

Turingov stroj s više traka ima sve dijelove kao i (običan) Turingov stroj, ali ima više traka (konačno mnogo!) za obradu podataka. Svaka traka ima svoju glavu za čitanje i pisanje. Ulazni podatak sprema se na prvu traku, a ostale su trake su na početku rada prazne. Sada funkcija prijelaza nema viqv se istu domenu, a ni kodomenu. Dozvoljene je čitanje, pisanje i pomicanje svih glava na nekim ili na svim trakama simultano. Formalno, funkcija prijelaza k–tračnog Turingovog stroja je svaka funkcija

$$\Pi : Q \times \Gamma^k \to Q \times \Gamma^k \times \{L, D, H\}^k$$

gdje je k broj traka. Izraz $\Pi(q_i, a_1, ..., a_k) = (q_j, b_1, ..., b_k, L, D, ..., L)$ znači ako je stroj u stanju q_i i glave od 1 do k čitaju redom simbole a_1 do a_k, tada stroj prelazi u stanje q_j, piše simbole b_1 do b_k, i pomiče glave za čitanje i pisanje, ili ulijevo, ili udesno ili ostaje na istom polozaju, ovisno kako je određeno za koju traku. Turingov stroj s više traka izgleda moćnije od originalnog Turingovog stroja, ali može se pokazati da su iste snage.

Teorem 4.59. *Svaki Turingov stroj s više traka ekvivalentan je nekom Turingovom stroju s jednom trakom.*

Kako bi definirali pojam Turing–izračunljive funkcije promatramo Turingove strojeve koje imaju tri trake:

- jednu traku na koju su na početku zapisani samo ulazni podaci (tzv. input traka),
- jednu pomoćnu "radnu" traku,
- jednu traku na koju se zapisuje izlazni rezultat (tzv. output traka).

Neka je T neki Turingov stroj s tri trake i $\vec{x} \in \mathbb{N}^k$. Rad stroja T kod kojeg je na input traci zapisano $\vec{x}$ kao ulazni podatak, nazivamo T–**izračunavanje** sa $\vec{x}$. Primijetimo da svako T–izračunavanje sa $\vec{x}$ ne mora stati.

Definicija 4.60. *Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ proizvoljna funkcija i T neki Turingov stroj. Kažemo da Turingov stroj T izračunava funkciju f ako za svaki $\vec{x} \in \mathbb{N}^k$ vrijedi:*

$$T\text{–izračunavanje sa } \vec{x} \text{ stane, i na output traci je zapisan broj } f(\vec{x})$$

$$\text{ako i samo ako } \vec{x} \in S$$

Za funkciju $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ kažemo da je **Turing–izračunljiva** *ako postoji Turingov stroj koji je izračunava.*

Teorem 4.61. *Funkcija $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ je Turing–izračunljiva ako i samo ako je funkcija f parcijalno rekurzivna.*

Nedeterministički Turingovi strojevi

Turingove strojeve koje smo do sada razmatrali nazivamo **deterministički Turingovi strojevi**. Kod nedeterminističkih Turingovih strojeva funkcija prijelaza poprima vrijednosti u partitivnom skupu.

Definicija 4.62. Nedeterministički Turingov stroj *je uređena šestorka $(\mathcal{S}, \Gamma, q_0, s_0, \{q_{DA}, q_{NE}\}, \delta)$, gdje simboli $\mathcal{S}, \Gamma, q_0, s_0, q_{DA}$ i q_{NE} imaju isto značenje kao kod determinističkih Turingovih strojeva. No, sada je funkcija prijelaza proizvoljna funkcija $\delta : \Gamma \times \mathcal{S} \to \mathcal{P}(\Gamma \times \{L, D, H\} \times \mathcal{S})$.*

Nedeterminizam se najbolje očituje u tome što stroj s istim ulazom i istom stanju može postupati na bitno različite načine. Najbolje je mogućnost postupanja na različite načine zamišljati kao grananja.

Definicija 4.63. *Kažemo da nedeterministički Turingov stroj T* **prihvaća riječ** *$w \in \Gamma^*$ ako taj stroj s ulaznim podatkom w ima svojstvo da barem jedna grana stane u konačno mnogo koraka u završnom stanju q_{DA}.*

Teorem 4.64. *Za svaki nedeterministički Turingov stoj postoji neki deterministički Turingov stroj koji mu je ekvivalentan.*

Problem zaustavljanja ili halting problem

Svakom Turingovom stroju možemo pridružiti kod (konkatenaciju svih konfiguracija ili pak neki prirodan broj). Kod Turingovog stroja T označavamo sa $\overline{T}$.

Halting problem glasi:

> *Postoji li algoritam koji će za svaki Turingov stroj T i za svaki ulazni podatak odrediti hoće li stroj T s tim ulaznim podacima stati?*

Odgovor je da ne postoji. Formalni odgovor o halting problemu izriće sljedeći teorem.

Teorem 4.65. *Neka je jezik L zadan sa:*

$$L = \{(\overline{T}, w) : T \text{ je Turingov stroj i } T \text{ prepoznaje ulazni podatak } w\}$$

Jezik L nije odlučiv.

Korolar 4.66. *Komplement jezika iz prethodnog teorema nije Turing–prepoznatljiv.*

Churchov teorem

Sada ćemo dati dokaz Churchovog teorema, tj. da je logika prvog reda neodlučiva. U tu svrhu ćemo prvo definirati pojam RAM–stroja.

RAM–stroj je idealizirano računalo s beskonačno velikom memorijom koje nikad ne radi greške. Definicija RAM–stroja, koja slijedi, je opisna. Mogli bismo dati definiciju koja bi bila stroža ("RAM–stroj je uređena n-torka ...") i "više" matematička, ali smatramo da tada taj pojam ne bi bio toliko jasan.

Definicija 4.67. *Osnovni dijelovi RAM–stroja su:*

- *registri;*
- *spremnik za program;*
- *brojač.*

Za svaki prirodan broj k stroj ima registar koji označavamo s $\mathcal{R}_k$. U svakom trenutku rada stroja svaki registar $\mathcal{R}_k$ sadrži neki prirodan broj.

U spremniku za program je smješten program. Program je konačan niz instrukcija. Ako je n broj instrukcija u programu tada su one numerirane s 1., 2., $\ldots$, n.

U brojaču se u svakom trenutku rada RAM–stroja nalazi redni broj instrukcije koja se izvršava.
Postoje četiri tipa instrukcija:

- *INC $\mathcal{R}_k$*
  Kada stroj izvodi tu instrukciju tada povećava broj u registru $\mathcal{R}_k$ za jedan, te broj u brojaču poveća za jedan.

- *DEC* $\mathcal{R}_k$, m.
  Broj m *je obavezno redni broj neke instrukcije u programu. Ako je broj u registru* $\mathcal{R}_k$ *različit od nule tada se prilikom izvršenja navedene instrukcije broj u* $\mathcal{R}_k$ *smanji za jedan, a broj u brojaču se poveća za jedan. Ako je broj u registru* $\mathcal{R}_k$ *jednak nuli tada se prilikom izvršenja navedene instrukcije samo broj u brojaču promijeni u* m.

- *GO TO* m
  Broj m *je obavezno redni broj neke instrukcije u programu.*
  Kada stroj izvodi tu instrukciju on jednostavno broj u brojaču mijenja u m.

- *STOP*
  Kada stroj dođe na tu instrukciju tada izračunavanje bezuvjetno stane.

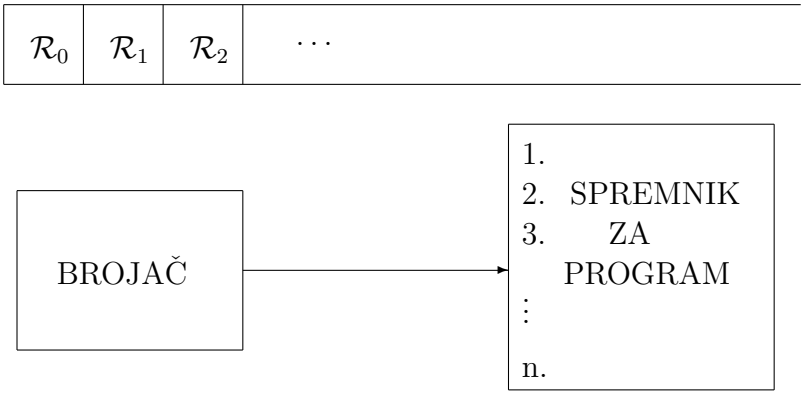
Za primjenu stroja prvo stavljamo program u spremnik programa. Zatim upisujemo odgovarajuće brojeve u registre (ulazni podaci). Ako se radi o programu s k *ulaznih podataka, tada smatramo da su oni redom zapisani u registrima* $\mathcal{R}_1$, $\ldots$, $\mathcal{R}_k$. *U brojaču je na početku broj* 1 *(to znači da se svaki program počinje izvršavati od prve instrukcije). Tada startamo stroj.*

Stroj tada počinje izvršavati instrukcije. U svakom koraku stroj izvršava instrukciju u programu čiji je redni broj u brojaču. Na kraju izvršenja instrukcije mijenja se broj u brojaču.

Ako je izračunavanje došlo na instrukciju STOP, ili pak je broj u brojaču veći od svakog rednog broja instrukcija u programu, tada stroj staje. U tom slučaju je izlazni rezultat zapisan u registru $\mathcal{R}_0$. *Ako se to nikad ne dogodi stroj radi "vječno".*

Napomena 4.68. *Na početku smo rekli da je RAM–stroj neka vrsta idealiziranog računala koja nikad ne griješi. Ako stroj nikad ne stane prilikom izvršenja nekog programa to ne znači da stroj griješi, već je program takav. (Sjetimo se samo koliko puta su nam probleme stvarale beskonačne petlje koje se znaju dogoditi prilikom nepažljivog programiranja.) Beskonačni rad stroja ne dopuštamo samo kako bismo mogli opravdati grešku u programu, već će nam ta neodređenost biti oznaka za jedno svojstvo funkcije čija se vrijednost izračunava.*

Sljedećom slikom dajemo skicu RAM–stroja.



Definicija 4.69. *Za svaki program P za RAM–stroj i svaki $k \in \mathbb{N}$ uređeni par (P, k) nazivamo* **algoritam**, *te označavamo sa A_k^P.*

*Ako je A_k^P neki algoritam i $\vec{x} \in \mathbb{N}^k$ tada rad RAM–stroja s programom P u spremniku i ulaznim podacima $\vec{x}$ nazivamo P–***izračunavanje s** $\vec{x}$.

Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ i A_k^P neki algoritam. Kažemo da algoritam A_k^P **izračunava** *funkciju f ako za sve prirodne brojeve $x_1, \ldots, x_k$ vrijedi da je $(x_1, \ldots, x_k) \in S$ ako i samo ako RAM–stroj s programom P u spremniku i s $(x_1, \ldots, x_k)$ kao ulaznim podacima stane, i u tom slučaju je na kraju rada stroja u registru $\mathcal{R}_0$ zapisan broj $f(x_1, \ldots, x_k)$. Često ćemo i reći da program P izračunava funkciju f, i to u situacijama kada nije potrebno naglašavati mjesnost ulaznih podataka.*

Kažemo da je **funkcija** f **RAM–izračunljiva** *ako postoji algoritam A_k^P koji je izračunava.*

Teorem 4.70. *Neka je $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ proizvoljna funkcija. Funkcija f je RAM–izračunljiva ako i samo ako funkcija f je Turing–izračunljiva.*

Sada dojemo dokaz Churchovog teorema. Za svaki program P^k za RAM–stroj i ulazne podatke $\vec{x} = (m_1, \ldots, m_k)$ definiramo rečenicu logike prvog reda $\varphi_{\vec{x}}^P$ tako da vrijedi

P–izračunavanje sa $\vec{x}$ stane ako i samo ako je formula $\varphi_{\vec{x}}^P$ valjana $(*)$

Primijetimo da primjenom nerješivosti halting problema odavde odmah slijedi da ne postoji algoritam za ispitivanje valjanosti formula logike prvog reda, tj. Churchov teorem.

Sada ćemo opisati konstrukciju tražene formule $\varphi_{\vec{x}}^P$. Neka su $I_1, \ldots, I_n$ instrukcije koje čine program P. Neka su $\mathcal{R}_0, \ldots, \mathcal{R}_m$ svi registri koji se pojavljuju u programu P.

Sada definiramo alfabet σ za rečenicu $\varphi_{\vec{x}}^P$. Neka je $\sigma = \{0,\ s,\ R\}$, gdje su redom:

- 0 je konstantski simbol
- s je jednosmjesni funkcijski simbol
- R je $m+1$ mjesni relacijski simbol

Za svaki prirodan broj $n \neq 0$ sa $s^n(0)$ označavamo term $s(s(\ldots s(0)\ldots)$, gdje se simbol s pojavljuje točno n puta u termu.

Radi lakšeg snalaženja navodimo intendirane interpretacije uvedenih simbola. Intendirana interpretacija terma $s^n(0)$ je prirodan broj n. Zatim, smatramo da je atomarna formula

$$R(s^{n_1}(0), \ldots, s^{n_m}(0), s^k(0))$$

istinita ako i samo ako u nekom trenutku rada RAM–stroja (u spremniku je program P, a $\vec{x}$ su ulazni podaci) za svaki $i = 1, \ldots, m$ u registru $\mathcal{R}_i$ je zapisan prirodan broj n_i, a redni broj sljedeće instrukcije je k.

Za svaki $j = 1, \ldots, n$ (tj. za svaku instrukciju $I_1, \ldots, I_n$) definiramo formulu φ_j na sljedeći način:

- ako je I_j instrukcija oblika $INC\ \mathcal{R}_l$, pri čemu je $l \in \{1, \ldots, m\}$, tada definiramo:

$$\begin{aligned}\varphi_j \ \equiv\ \forall x_1 \ldots \forall x_m \Big(& R(x_1, \ldots, x_m, s^j(0)) \rightarrow \\ & R(x_1, \ldots, x_{l-1}, s(x_l), x_{l+1}, \ldots, x_m, s^{j+1}(0)) \Big)\end{aligned}$$

- ako je I_j oblika $DEC\ \mathcal{R}_p, q$ tada definiramo:

$$\begin{aligned}\varphi_j \ \equiv\ \forall x_1 \ldots \forall x_m \Big(& R(x_1, \ldots, x_m, s^j(0)) \rightarrow \\ & \forall y (x_p = s(y) \rightarrow R(x_1, \ldots, x_{p-1}, y, x_{p+1}, \ldots, x_m, s^{j+1}(0)) \wedge \\ & (x_p = 0 \rightarrow R(x_1, \ldots, x_m, s^q(0))) \Big)\end{aligned}$$

- ako je instrukcija I_j oblika $GO\ TO\ p$ tada definiramo:

$$\varphi_j \ \equiv\ \forall x_1 \ldots \forall x_m \Big(R(x_1, \ldots, x_m, s^j(0)) \rightarrow R(x_1, \ldots, x_m, s^p(0)) \Big)$$

- ako je instrukcija I_j oblika $STOP$ tada definiramo:

$$\varphi_j \equiv \forall x_1 \ldots \forall x_m \Big(R(x_1, \ldots, x_m, s^j(0)) \to R(x_1, \ldots, x_m, s^{n+1}(0)) \Big)$$

Sada konačno definiramo traženu formulu $\varphi_{\vec{x}}^P$ sa:

$$\Big(R(s^{m_1}(0), \ldots, s^{m_k}(0), 0 \ldots, 0) \quad \wedge \varphi_1 \ \wedge \ \ldots \ \wedge \ \varphi_n \Big) \ \to$$
$$\exists x_1 \ldots \exists x_m R(x_1, \ldots, x_m, s^{n+1}(0))$$

Iz njene definicije odmah slijedi da ima traženo svojstvo $(*)$. Q.E.D.

4.3 Teorija složenosti

Za svaki algoritam važno je koliko vremenskih i prostornih resursa treba za njegov rad. Vremenska, odnosno prostorna, složenost iskazuje se kao funkcija veličine ulaznih podataka za algoritam. Teorija složenosti ne bavi se prevenstveno proučavanjem potrebnih resursa za pojedini algoritam, već razmatra odnos među klasama algoritama iste složnosti.

Definicija 4.71. Vremenska složenost determinističkog *stroja T je funkcija $time_T : \mathbb{N} \to \mathbb{N}$, gdje je $time_T(n)$ maksimalan broj koraka koje stroj T napravi za svaki ulazni podatak duljine n.*

Vremenska složenost nedeterminističkog *stroja T je funkcija $time_T : \mathbb{N} \to \mathbb{N}$, gdje je $time_T(n)$ maksimalan broj koraka (uzimajući u obzir sve grane) koje stroj T napravi za svaki ulazni podatak duljine n.*

Ako je $time_T$ vremenska složenost stroja T (determinističkog ili nedeterminističkog) tada kažemo da stroj T radi u vremenu $time_T$, tj. da je T $time_T$– **vremenski složen Turingov stroj**.

Definicija 4.72. Prostorna složenost determinističkog *Turingovog stroja T je funkcija $space_T : \mathbb{N} \to \mathbb{N}$, gdje je $space_T(n)$ maksimalan broj lokacija (uzimajući u obzir sve trake) po kojima stroj T pretražuje za svaki uzlazni podatak duljine n.*

Prostorna složenost nedeterminističkog *Turingovog stroja T je funkcija $space_T : \mathbb{N} \to \mathbb{N}$, gdje je $space_T(n)$ maksimalan broj lokacija (uzimajući u obzir sve trake i sve grane) po kojima stroj T čita i piše, za svaki ulazni podatak duljine n.*

Ako je $space_T$ prostorna složenost stroja T (determinističkog ili nedeterminističkog) tada kažemo da stroj T treba prostor $space_T$, tj. da je T $space_T$– **prostorno složen Turingov stroj**.

Točno vrijeme trajanja rada stroja i prostora je unaprijed nemoguće izračunati, stoga ga procjenjujemo. Jedan prikladan oblik procjene u kojem pokušavamo ocijeniti vrijeme trajanja rada stroja je trajanje rada za velike ulazne podatke, koji zovemo **asimptotska analiza**. U asimptotskoj analizi, ako promatramo polinom, bitan je samo član s najvećom potencijom, dok ostale zanemarujemo, s tim da zanemarimo i koeficijent uz vodeći član, jer član s najvećom potencijom dominira nad ostalim članovima pri ulaznim podacima velike duljine. Primijetimo, ako stroj nikad ne stane za neki podatak duljine n, onda je $time_T(n) = \infty$.

Definicija 4.73. *(big-o-notation)*
Označimo sa $\mathbb{R}^+$ skup nenegativnih realnih brojeva. Neka su $f, g : \mathbb{N} \to \mathbb{R}^+$ proizvoljne funkcije. Pišemo $f(n) = O(g(n))$, odnosno kratko $f = O(g)$, ako postoje prirodni brojevi c i n_0 takvi da za svaki prirodan broj $n \geq n_0$ vrijedi

$$f(n) \leq c \cdot g(n)$$

Primjer 4.74. *1. Ako je polinom P stupnja k tada vrijedi $P(n) = O(n^k)$.*
Dokaz. Neka je $P(x) = a_0 + a_1x + \ldots + a_kx^k$. Neka je $b_i = |a_i|$. Tada za svaki $x \geq 1$ imamo

$$\begin{aligned} |P(x)| &\leq b_0 + b_1x + \ldots + b_kx^k \\ &\left(\tfrac{b_0}{x^k} + \tfrac{b_1}{x^{k-1}} + \ldots + b_k\right)x^k \\ &\leq (b_0 + b_1 + \ldots + b_k)x^k = Mx^k \end{aligned}$$

gdje je $M = b_0 + b_1 + \ldots + b_k$ Iz posljednjeg očito slijedi $P(n) = O(n^k)$.

2. *Ako je $c > 1$ proizvoljan realan broj i P neki polinom tada vrijedi $P(n) = O(c^n)$.*

3. *Vrijedi $\log n = O(n)$. Štoviše, za svaki $k \in \mathbb{N}$ vrijedi $(\log n)^k = O(n)$.*

Definicija 4.75. *Neka je T Turingov stroj (deterministički ili nedeterministički). Kažemo da je stroj T:*

- **(vremenski) polinoman** *ako postoji neki polinom f tako da vrijedi $time_T = O(f)$.*

- **(vremenski) eksponencijalan** *ako postoji eksponencijalna funkcija g tako da vrijedi $time_T = O(g)$.*
- **prostorno polinoman** *ako postoji polinom f tako da vrijedi $space_T = O(f)$.*
- **prostorno eksponencijalan** *ako postoji eksponencijalna funkcija g tako da vrijedi $space_T = O(g)$.*

U istom smislu ćemo koristiti nazive "polinomni" i "eksponencijalni" (vremenski) algoritam.

Napomena 4.76. *Kada govorimo o rješivosti nekog problema na Turingovim strojevima tada pod pripadnim jezikom podrazumijevamo skup svih rješenja tog problema. U daljnjem tekstu govorit ćemo da je neki problem rješiv u polinomnom/eksponencijalnom vremenu, odnosno s polinomnim/eksponencijalnim prostorom, na (ne)determinističkom Turingovom stroju, ako je pripadni jezik takav.*

Primjer 4.77. *Ako su prirodni brojevi a i b zapisani u binarnom obliku, te ako je duljina zapisa n, standardni algoritmi* **zbrajanja** *i* **oduzimanja** *zahtijevaju* $\mathbf{O}(n)$ *vremena.*

Kako bi to dokazali promatramo Turingov stroj s 3 trake. Na traci broj 2 i 3 neka se nalaze sumandi, a traka 1 neka bude na početku prazna (na njoj će Turingov stroj ispisati rezultat zbrajanja). Bez smanjenja općenitosti možemo pretpostaviti da su oba sumanda duljine n (ako je jedan od sumanada manje duljine Turingov stroj ga može dopuniti do duljine n s vodećim nulama u jednom prolazu, dakle u vremenu $O(n)$). Neka su glave na počeku rada stroja na trakama 2 i 3 na posljednjim (desnim) znamenkama sumanada. Lako je konstruirati Turingov stroj T koji će u jednom prolazu obavljati zbrajanje (najviše $n+1$ korak) stoga je $time_T(n) = n+1$, dakle $time_T(n) = O(n)$.
Množenje i dijeljenje s ostatkom zahtijeva $O(n^2)$ **vremena**.

Primjer 4.78. Euklidov algoritam
Podsjetimo se koji su koraci Euklidovog algoritma za određivanje najvećeg zajedničkog djelitelja dvaju prirodnih brojeva a i b (oznaka $nzm(a,b)$). Bez smanjenja općenitosti možemo pretpostaviti da je $a \leq b$. Koraci algoritma:

1. *Ako je $a = 0$ tada je $nzm(a,b) = b$.*
2. *Ako je $a > 0$, tada (teorem o dijeljenju s ostatkom) postoje prirodni brojevi $q \geq 1$ i $0 \leq r < a$ tako da vrijedi $b = q \cdot a + r$. Tada je $nzm(a,b) = nzm(a,r)$. Definiramo $b := a$ i $a := r$, te se vratimo na korak 1.*

Kako vidimo, algoritam je dan rekurzivno, a pošto je $r < a$ očito je da završava u konačno mnogo koraka. Euklidov algoritam je vremenski polinoman. Točnije, **zahtijeva** $O(\log_2 a + \log_2 b)$ **aritmetičkih operacija**.

Primjer 4.79. Množenje matrica
Neka su $A = [a_{ij}]$ i $B = [b_{ij}]$ dvije matrice reda n. Ako označimo $A \cdot B = [c_{ij}]$ tada je $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. Uočimo da je veličina ulaznog podatka $2n^2$. Standardni algoratam za množenje matrica, tj. ako jednostavno množimo matrice koristeći definiciju, treba nam $O(n^3)$ množenja. Postoje brži algoritmi za množenje matrica (npr. Strassenov algoritam; vidi [24]).

Primjer 4.80. Problem SAT *(eng. satisfiability) glasi:*

> *odrediti je li zadana formula logike sudova ispunjiva.*

Semantičke tablice su jedan algoritam koji rješava problem SAT, ali općenito za formulu sa n varijabli treba više od 2^n koraka. Iz tog razloga kažemo da su semantičke tablice **eksponencijalni algoritam**. *Semantička stabla (ili metoda tableauxa) su također jedan potpun i korektan test za ispitivanje ispunjivosti formula. Koja je njihova vremenska složenost? Problem SAT se obično promatra za formule u konjunktivnoj normalnoj formi, jer se za svaku formulu logike sudova može u polinomnom vremenu odrediti konjunktivna normalna forma. Ako svaka elementarna disjunkcija sadrži najviše n literala tada govorimo o n–SAT problemu.*

Primjer 4.81. Problem trgovačkog putnika – TSP *(eng. Traveling Salesman problem)*
Zadan je **neusmjereni potpun** *graf $G = (V, E)$ s n vrhova, tj.*

$$V = \{v_1, \ldots, v_n\} \quad i \quad E = \{\{v_i, v_j\} \ : \ i < j\}$$

Neka su zadani brojevi $d_{ij} = d_{ji} > 0$, koji predstavljaju udaljenost između vrhova v_i i v_j. Treba naći zatvoreni put koji prolazi kroz sve vrhove grafa, a ima minimalnu duljinu. Drugim riječima, treba naći cikličku permutaciju π od n elemenata, takvu da je suma $\sum_{j=1}^{n} d_{j\pi(j)}$ minimalna, gdje je $v_{\pi(j)}$ vrh u koji dolazimo iz vrha v_j. (U praksi se pojavljuju problemi s 50 i više gradova, čije bi egzaktno rješavanje na današnjim računalima trajalo milijardama godina).

Složenost poznatih algoritama za pretraživanje i sortiranje je sljedeća:

1. Linearno pretraživanje: $O(n)$
2. Binarno pretraživanje: $O(\log_n)$
3. Bubble sort: $O(n^2)$
4. Merge-sort: $O(n \log n)$

Definicije i detalje o navedenim algoritmima možete vidjeti u skripti [23].

Teorem 4.82. *(O redukciji višetračnog Turingovog stroja na jednotračni)*
Neka je $f : \mathbb{N} \to \mathbb{R}^+$ funkcija takva da je $f(n) \geq n$, za svaki $n \in \mathbb{N}$. Tada za svaki Turingov stroj vremenske složenosti $f(n)$ s više traka postoji ekvivalentan $O(f^2(n))$–vremenski složen Turingov stroj s jednom trakom.

Teorem 4.83. *(O redukciji nedeterminističkog Turingovog stroja na deterministički)*
Neka je $f : \mathbb{N} \to \mathbb{R}^+$ funkcija takva da je $f(n) \geq n$, za svaki $n \in \mathbb{N}$. Za svaki nedeterministički Turingov stroj vremenske složenosti $f(n)$ postoji ekvivalentan $O(2^{f(n)})$–vremenski složen deterministički Turingov stroj.

Definicija 4.84. *Neka je $f : \mathbb{N} \to \mathbb{R}^+$ proizvoljna funkcija. Klasa vremenske složenosti* **DTIME**(f) *je skup svih jezika koji su odlučivi s nekim $O(f)$–vremenski složenim deterministićkim Turingovim strojem. Klasa vremenske složenosti* **NTIME**(f) *je skup svih jezika koji su odlučivi s nekim $O(f)$–vremenski složenim nedeterminističkim Turingovim strojem.*

Definicija 4.85. *S* **PTIME***, ili samo kratko s* **P***, označavamo klasu svih jezika koji su odlučivi na nekom deterministićkom Turingovom stroju vremenske složenosti $O(n^k)$, za neki $k \in \mathbb{N}$. Dakle, vrijedi*

$$P = \bigcup_{k \in \mathbb{N}} DTIME(n^k)$$

S **NPTIME***, ili samo kratko s* **NP***, označavamo klasu svih jezika koji su odlučivi na nekom nedeterminističkom Turingovom stroju vremenske složenosti $O(n^k)$, za neki $k \in \mathbb{N}$. Dakle, vrijedi*

$$NP = \bigcup_{k \in \mathbb{N}} NTIME(n^k)$$

Napomena 4.86. *Za svaki jezik α vrijedi:*

$$\alpha \in NP \Leftrightarrow \ (\exists R(x,y) \in P)(\exists \ \ polinom \ \ p)$$
$$\alpha = \{x : (\exists y, \ |y| \leq p(|x|))R(x,y)\}$$

(O definiciji klase NP pomoću polinomnog verifikatora vidi npr. [25]).

Primjeri problema koji pripadaju klasi P:

1. zbrajanje, oduzimanje, množenje i dijeljenje s ostatkom prirodnih brojeva
2. određivanje najveće zajedničke mjere dvaju prirodnih brojeva
3. ispitivanje povezanosti grafa; traženje najkraćeg puta u grafu
4. 2–SAT
5. SAT–Horn (problem ispunjivosti Hornovih formula)
6. problem egzistencije rješenja sistema linearnih algebarskih jednadžbi
7. problem ispitivanja prostosti prirodnog broja

Primjeri problema koji pripadaju klasi NP

1. problem ispunjivosti formula logike sudova, tj. problem SAT
2. problem trgovačkog putnika (TSP)
3. problem faktorizacije prirodnih brojeva
4. problem cjelobrojnog linearnog programiranja
5. određivanje da li je graf 3–obojiv
6. Hamiltonov put (put koji sadrži sve vrhove u grafu)
7. Nezavisan skup u grafu (potpuno nepovezan podgraf)
8. Klika u grafu (potpuno povezan podgraf)
9. Minesweeper, potapanje brodova; tetris; igra gomilice; Sokoban
   (vidi V. Kojić, Minesweeper problem je NP–potpun, math.e, 12 (2008); http://e.math.hr)

Neka su Γ_1 i Γ_2 proizvoljni alfabeti.

Definicija 4.87. *Kažemo da je neka funkcija $f : \Gamma_1^* \to \Gamma_2^*$* **vremenski polinomno izračunljiva** *ako postoji polinomno vremenski složen Turingov stroj koji za svaki $w \in \Gamma_1^*$ kao ulazni podatak na traku ispisuje $f(w)$.*

Definicija 4.88. *Kažemo da je jezik $\alpha_1 \subseteq \Gamma_1^*$* **polinomno reducibilan** *u odnosu na jezik $\alpha_2 \subseteq \Gamma_2^*$, ako postoji vremenski polinomno izračunljiva funkcija $f : \Gamma_1^* \to \Gamma_2^*$ takva da za svaki $w \in \alpha_1$ vrijedi: $w \in \alpha_1$ ako i samo ako $f(w) \in \alpha_2$.*

Primjer 4.89. *Funkcija $f : \mathbb{N} \to \{0,1\}^*$ koja prirodnom broju pridružuje njegov binarni zapis je vremenski polinomno izračunljiva, pa su i ta dva jezika polinomno reducibilna.*

Propozicija 4.90. *Ako je jezik $\alpha_1 \subseteq \Gamma_1^*$ polinomno reducibilan u odnosu na jezik $\alpha_2 \subseteq \Gamma_2^*$, a jezik α_2 je polinomno reducibilan u odnosu na jezik $\alpha_3 \subseteq \Gamma_3^*$ tada je i jezik α_1 polinomno reducibilan u odnosu na jezik α_3.*

Propozicija 4.91. *Ako neki jezik pripada klasi P (odnosno NP) tada i svaki jezik koji je polinomno reducibilan u odnosu na njega također pripada klasi P (odnosno NP).*

Definicija 4.92. *Kažemo da je neki jezik α* **NP–potpun** *ako zadovoljava sljedeća dva uvjeta:*

a) jezik α pripada klasi NP

b) svaki jezik $\beta \in NP$ je polinomno reducibilan u odnosu na α.

NP–potpuni problemi su najteži u klasi NP. Riječ potpun trebala bi asocirati da algoritamskim rješenjem ovih problema dolazimo na neki način i do rješenja svih ostalih NP problema.

Propozicija 4.93. *Neka je α neki NP–potpun jezik i $\beta \in NP$. Ako je α polinomno reducibilan u odnosu na β tada je i jezik β NP–potpun.*

Teorem 4.94. *(***Cook, Levinov teorem, 1971.***)*
Problem SAT je NP–potpun.

Skica dokaza. Kako bi dokazali da je SAT∈NP opisujemo algoritam na nedeterminističkom stroju koji u polinomnom vremenu za zadanu formulu F u konjunktivnoj normalnoj formi ispituje je li ispunjiva. Algoritam se sastoji od dva dijela. Prvo na sve moguće načine pridružimo 0 i 1 literalima u formuli F. (Zbog nedeterminizma to možemo napraviti u polinomnom vremenu). U drugom dijelu algoritma računamo istinosnu vrijednost formule F za svaku definiranu interpretaciju. Za to nam treba $O(n)$ koraka, jer to radimo jednim prolaskom kroz formulu.

Preostalo je dokazati kako se proizvoljan jezik $\alpha \in NP$ može polinomno reducirati u odnosu na problem SAT. Neka je $\alpha \in NP$ proizvoljan jezik, te neka je T Turingov stroj koji odlučuje jezik α u vremenu $O(n^c)$, za neki $c \in \mathbb{N}$. Označimo sa $\mathcal{S}$ skup svih stanja, sa Γ alfabet, te sa Π funkciju prijelaza stroja T. Formulama logike sudova opisat ćemo rad Turingov stroja T. Neka je $w = h_1 \dots h_n$ proizvoljna riječ alfabeta Γ. Tada postoji $c_1 \in \mathbb{R}$ tako da stroj T odlučuje u $N = \lceil c_1 n^c \rceil$ koraka pripada li riječ w jeziku α.

Uvodimo oznake za propozicionalne varijable:

a) $X_{k,s}$, za svaki $k \in \{0, \dots, N\}$, i svako stanje $s \in \mathcal{S}$

b) $Y_{k,i}$, za svaki $k \in \{0, \dots, N\}$, i svaki $i \in \{-N, \dots, 0, \dots, N\}$

c) $Z_{k,i,h}$, za svaki $k \in \{0, \dots, N\}$, svaki $i \in \{-N, \dots, 0, \dots, N\}$, te svaki $h \in \Gamma$

Prateći postupak rada stroja T varijablama pridružujemo vrijednosti ovako:

$X_{k,s} = 1$ ako se nakon k–tog koraka stroj T nalazi u stanju s

$Y_{k,i} = 1$ ako se nakon k–tog koraka glava stroja nalazi na i–toj lokaciji

$Z_{k,i,h} = 1$ ako je nakon k–tog koraka u i–toj čeliji zapisan simbol h

(Uočite da nismo uveli nikakvu oznaku za interpretaciju, već za svaku propozicionalnu varijablu p pišemo $p = 1$ ili $p = 0$).

Sada redom definiramo formule koje opisuju potpuno rad stroja.

(1) $\bigvee_{s \in \mathcal{S}} X_{k,s}$, za svaki $k \in \{0, \ldots, N\}$

Ova formula jednostavno izriče da se stroj T u svakom koraku svog rada nalazi u nekom stanju $s \in \mathcal{S}$

(2) $\neg X_{k,s_1} \vee \neg X_{k,s_2})$ za svaki $k \in \{0, \ldots, N\}$, te svaka dva stanja $s_1 \neq s_2$

Ova formula izriče da se stroj T u svakom koraku svog rada nalazi točno u jednom stanju. Analogno definiramo formule od (3) do (7) (vidi npr. [10]).

Navodimo još posljednju formulu.

(8) $(Y_{k,i} \vee Z_{k,i,h} \vee \neg Z_{k+1,i,h}) \wedge (Y_{k,i} \vee \neg Z_{k,i,h} \vee Z_{k+1,i,h})$,
za svaki $k \in \{0, \ldots, N\}$, za svaki $i \in \{-N \ldots, 0, \ldots, N\}$, te za svaki $h \in \Gamma$

Ova formula izriče da tamo gdje nije glava stroja sadržaj čelije se ne mijenja. Označimo sa F_w konjunkciju formula (1)–(8). Lako je vidjeti da vrijedi:

$w \in \alpha$ ako i samo ako $F_w \in SAT$

Zatim, pažljivom analizom definicija formula (1)–(8) može se pokazati da je za svaku riječ $w \in \Gamma^*$ formulu F_w moguće konstruirati u polinomnom vremenu. To znači da je svaki jezik $\alpha \in NP$ polinomno reducibilan u odnosu na SAT. □

Karp je 1972. dokazao da je čitav niz kombinatornih problema, među kojima i TSP, NP–potpun. Do danas je poznato nekoliko tisuća NP–potpunih problema. Klasa NP–potpunih problema ima dva interesantna svojstva:

1. Niti za jedan NP–potpun problem do danas nije poznat polinomni algoritam koji ga rješava.

2. Ako je u polinomnom vremenu rješiv bilo koji od tih problema, onda se u polinomnom vremenu rješivi svi NP problemi.

Na temelju ovih svojstva, mnogi matematičari smatraju da ne postoji polinomni algoritam za bilo koji NP–potpun problem, tj. da je P≠NP.

Teorem 4.95. *Problem 3–SAT je NP–potpun.*

Dokaz. Pošto je 3–SAT specijalni slučaj problema SAT očito vrijedi 3–SAT∈NP. Za dokaz NP–potpunosti problema 3–SAT dokazat ćemo da je problem SAT polinomno reducibilan u odnosu na problem 3–SAT. Neka je $F(P_1, \ldots, P_n)$ proizvoljna formula logike sudova. Dokazujemo da postoji konjunktivna normalna forma $F'(P_1, \ldots, P_n, Q_1, \ldots, Q_m)$ $(m \geq 0)$ tako da svaka elementarna disjunkcija sadrži točno tri literala, te za svaku parcijalnu interpretaciju $I : \{P_1, \ldots, P_n\} \to \{0, 1\}$ vrijedi:

$I(F) = 1$ ako i samo ako postoji proširenje I' od I tako da $I'(F') = 1$.

Primijetimo da iz ove tvrdnje posebno slijedi da za svaku formulu F postoji 3–knf F' tako da vrijedi:

formula F je ispunjiva ako i samo ako F' je ispunjiva.

Prvo ćemo dokazati tvrdnju zadatka za jedan specijalan slučaj, tj. za formulu koja je elementarna disjunkcija. Neka je C proizvoljna elementarna disjunkcija. Tvrdimo da postoji konjunktivna normalna forma C' koja ima sljedeća svojstva:

(i) svaka elementarna disjunkcija od C' sadrži točno tri literala;

(ii) za sve parcijalne interpretacije $I : Var(C) \to \{0, 1\}$ vrijedi: $I(C) = 1$ ako i samo ako postoji proširenje I' od I tako da vrijedi $I'(C') = 1$.

Varijable koje dolaze u formuli C označimo sa P_1, P_2, ..., a novo uvedene varijable u C' ćemo označavati sa Q_1, Q_2, ... Neka je $C \equiv A_1 \vee \ldots \vee A_l$, gdje su A_i literali. Promatramo slučajeve obzirom na broj l.

(a) $l = 1$, tj. $C \equiv A_1$.
Tada definiramo da je formula C' jednaka

$$(A_1 \vee Q_1 \vee Q_2) \wedge (A_1 \vee \neg Q_1 \vee Q_2) \wedge (A_1 \vee Q_1 \vee \neg Q_2) \wedge (A_1 \vee \neg Q_1 \vee \neg Q_2)$$

(b) $l = 2$, tj. $C \equiv A_1 \vee A_2$.
Tada definiramo

$$C' \equiv (A_1 \vee A_2 \vee Q_1) \wedge (A_1 \vee A_2 \vee \neg Q_1).$$

(c) $l = 3$
Tada neka je jednostavno C' upravo formula C.

(d) $l > 3$
Neka je

$$C' \equiv (A_1 \vee A_2 \vee Q_1) \wedge \bigwedge_{i=1}^{l-4} (\neg Q_i \vee A_{i+2} \vee Q_{i+1}) \wedge (\neg Q_{l-3} \vee A_{l-1} \vee A_l).$$

(Ako je $l = 4$ tada u C' imamo "praznu" konjunkciju, tj. konjunkciju oblika $\bigwedge_{i=1}^{0}$. Po definiciji smatramo da je takva konjunkcija jednaka tautologiji $Q_1 \vee \neg Q_1$. Odnosno, za slučaj $l = 4$ definiramo da je $C' \equiv (A_1 \vee A_2 \vee Q_1) \wedge (\neg Q_1 \vee A_3 \vee A_4)$.)

Preostalo je dokazati tvrdnju (ii). U slučaju c) to je trivijalno. Lako je vidjeti da za slučajeve a) i b) možemo uzeti proizvoljna proširenja I'. Preostalo je jedino razmotriti slučaj d). Pretpostavimo prvo da vrijedi $I(C) = 1$. Tada postoji literal A_p tako da je $I(A_p) = 1$. Proširenje I' od I definiramo po slučajevima obzirom na p.

(d_1) ako je $p = 1$ ili $p = 2$ tada definiramo $I'(Q_1) = \ldots = I'(Q_{l-3}) = 0$.

(d_2) ako je $p = l - 1$ ili $p = l$ tada definiramo $I'(Q_1) = \ldots = I'(Q_{l-3}) = 1$.

(d_3) Za broj p, za koji vrijedi $3 \leq p \leq l - 2$, definiramo

$$I'(Q_1) = \ldots = I'(Q_{p-2}) = 1, \qquad I'(Q_{p-1}) = \ldots = I'(Q_{l-3}) = 0.$$

Lako je provjeriti da u svim slučajevima vrijedi $I'(C') = 1$. Obrat tvrdnje dokazujemo obratom po kontrapoziciji. Neka je I interpretacija za koju vrijedi $I(C) = 0$, tj. $I(A_1) = \ldots = I(A_l) = 0$. Ako je I' proširenje od I tako da je $I'(C') = 1$ tada mora biti $I'(Q_1) = \ldots = I'(Q_{l-3}) = 1$. No, tada je i $I'(\neg Q_{l-3} \vee A_{l-1} \vee A_l) = 0$, što povlači $I'(C') = 0$. Time je tvrdnja zadatka potpuno dokazana za slučaj kada je F elementarna disjunkcija.
Promotrimo sada općenit slučaj, tj. kada je F proizvoljna formula. Označimo sa F_1 konjunktivnu normalnu formu za F, tj. neka je $F_1 \equiv C_1 \wedge \ldots \wedge C_s$, gdje su C_i elementarne disjunkcije. Konstruiramo formule C_i' kao prije. (Konstrukcije možemo provesti tako da su skupovi novo uvedenih varijabli međusobno disjunktni). Tada definiramo $F' \equiv C_1' \wedge \ldots \wedge C_s'$. Lako je provjeriti da formula F' ima tražena svojstva. Time smo dokazali da se svaka zadaća iz SAT transformira u neku zadaću iz 3–SAT. Nije teško vidjeti da se ova transfomacija može realizirati u polinomnom vremenu. □

Definicija 4.96. *Za neki problem S kažemo da je* **NP–težak** *ako je svaki NP–problem polinomno reducibilan u odnosu na problem S.*

Primjer 4.97. *Neka je*

$$D = \{p : p \in \mathbb{Z}[X_1, \ldots, X_n] \text{ koji ima cjelobrojnu nultočku } \}$$

Iz Matijasevičevog rješenja 10.–tog Hilbertovog problema znamo da je jezik (!) D neodlučiv (to znači da ne postoji nikakav Turingov stroj koji ga odlučuje, pa posebno $D \notin NP$). Može se pokazati da je jezik D jedan NP–težak jezik.

Definicija 4.98. *Neka je $f : \mathbb{N} \to \mathbb{R}^+$ proizvoljna funkcija. Klase prostorne složenosti $SPACE(f))$ i $NSPACE(f)$ definiramo ovako:*

DSPACE$(f) = \{L : L$ *je jezik odlučiv na nekom $O(f)$ prostorno složenim determinističkim Turingovim strojem* $\}$

NSPACE$(f) = \{L : L$ *je jezik odlučiv na nekom $O(f)$ prostorno složenim nedeterminističkim Turingovim strojem* $\}$

Sada definiramo:

$$\textbf{PSPACE} = \bigcup_{k \in \mathbb{N}} DSPACE(n^k)$$

$$\textbf{NPSPACE} = \bigcup_{k \in \mathbb{N}} NSPACE(n^k)$$

Definicija 4.99. *Kažemo da je funkcija $f : \mathbb{N} \to \mathbb{N}$* **dobro izračunljiva** *ako postoji deterministički Turingov stroj T koji izračunava funkciju f u vremenu $O(f)$.*

Teorem 4.100. *(Savitchev teorem)*
Ako je $f : \mathbb{N} \to \mathbb{N}$ dobro izračunljiva funkcija takva da za svaki $n \in \mathbb{N}$ vrijedi $f(n) \geq \log n$, tada imamo

$$NSPACE(f(n)) \subseteq DSPACE(f^2(n))$$

Korolar 4.101. *Vrijedi: $PSPACE = NSPACE$.*

Definirajmo još neke klase složenosti. Za svaku funkciju $f : \mathbb{N} \to \mathbb{R}^+$ označimo:

$$Time(f) = \{\alpha : \quad \text{jezik } \alpha \text{ je odlučiv na nekom}$$
$$f - \text{vremenski složenim Turingovim strojem}\}$$

$$Space(f) = \{\alpha : \quad \text{jezik } \alpha \text{ je odlučiv na nekom}$$
$$f - \text{prostorno složenim Turingovim strojem}\}$$

$LinTime = \bigcup_{c\in\mathbb{N}} Time(cn)$ Linear Time

$E = \bigcup_{c\in\mathbb{N}} Time(c^n)$

$ExpTime = \bigcup_{c\in\mathbb{N}} Time(2^{n^c})$ Exponential Time

$LogSpace = \bigcup_{c\in\mathbb{N}} Space(c \cdot \log n)$ Logaritmic Space

$LinSpace = \bigcup_{c\in\mathbb{N}} Space(c \cdot n)$ Linear Space

Očito vrijede sljedeće inkluzije:

$$LinTime \subseteq P \subseteq E \subseteq ExpTime$$

$$LogSpace \subseteq LinSpace \subseteq PSPACE$$

Važno je istaknuti da su sve navedene inkluzije prave. Zanimljiva posljedica inkluzije $LogSpace \subset PSPACE$ je da je najmanja jedna od sljedećih inkluzija prava:

$$LogSpace \subseteq P \subseteq NP \subseteq PSPACE$$

Jasno je da vrijedi P⊆NP. Opće prihvaćena slutnja je da vrijedi P≠NP. To se smatra jednim od najvažnijih matematičkih problema i spada među sedam *Millenium Prize Problems*, za čije je rješenje Clay Mathematics Institute raspisao nagradu od milijun dolara.

Kako bi dokazali da vrijedi PTIME ⊆ PSPACE navodimo prvo neke činjenice.

Teorem 4.102. *(Linear Speed Up)*
Neka je α proizvoljan odlučiv jezik. Za svaki Turingov stroj T koji odlučuje jezik α i realan broj $c > 0$ postoji Turingov stroj S koji također odlučuje jezik α, te za svaki $n \in \mathbb{N}$ vrijedi

$$time_S(n) \leq c \cdot time_T(n) + n$$

Teorem 4.103. *(Linear Speed Up – "prostorna" verzija)*
Neka je α proizvoljan odlučiv jezik. Za svaki Turingov stroj T koji odlučuje jezik α i realan broj $c > 0$ postoji Turingov stroj S koji također odlučuje jezik α, te za svaki $n \in \mathbb{N}$ vrijedi

$$space_S(n) \leq c \cdot space_T(n) + n$$

Propozicija 4.104. *Neka je $f : \mathbb{N} \to \mathbb{R}$ proizvoljna funkcija, tako da za svaki $n \in \mathbb{N}$ vrijedi $f(n) > n$. Tada vrijedi $DTIME(f) \subseteq DSPACE(f)$.*

Dokaz. Neka $\alpha \in DTIME(f)$ proizvoljan jezik. Tada postoji k–tračni Turingov stroj T vremenske složenosti f koji odlučuje α. Tada očito $\alpha \in DSPACE(k \cdot f)$ (u jednom koraku stroj T može promijeniti najviše k lokacija). Iz posljednjeg slijedi da je za dokaz propozicije dovoljno dokazati da za svaki $k \in \mathbb{N}$ vrijedi

$$DSPACE(k \cdot f) \subseteq DSPACE(f)$$

Neka je $\beta \in DSPACE(k \cdot f)$ proizvoljan jezik. Tada postoji deterministički Turingov stroj T' prostorne složenosti $k \cdot f$ koji odlučuje jezik β. Iz Linear Speed Up teorema "prostorna" verzija (za $c = 1/k$) slijedi da postoji Turingov stroj S prostorne složenosti najviše $c \cdot k \cdot f(n) + n = f(n) + n$ koji odlučuje jezik β. Pošto po pretpostavci teorema vrijedi $f(n) > n$, tada imamo $f(n) + n < 2f(n) = O(f(n))$. To znači da je stroj S zapravo prostorne složenosti f. □

Korolar 4.105. *Vrijedi $P \subseteq PSPACE$.*

Dokaz. Neka je $\alpha \in P$ proizvoljan jezik. Tada postoji $k \in \mathbb{N}$ tako da je $\alpha \in DTIME(n^k)$. Iz prethodne propozicije slijedi $\alpha \in DSPACE(n^k)$. □

Propozicija 4.106. *Vrijedi* $NP \subseteq NPSPACE$.

Propozicija 4.107. *Vrijedi* $NPSPACE \subseteq EXPTIME$

Definicija 4.108. *Za jezik* α *kažemo da je* **PSPACE–potpun** *ako vrijedi:*

a) jezik α *pripada klasi PSPACE*

b) svaki jezik $\beta \in$*PSPACE je vremenski polinomno reducibilan u odnosu na jezik* α

Za jezik α *kažemo da je PSPACE–težak ako ispunjava prethodni uvjet b).*

(U [25] možete pročitati napomenu zašto se razmatra vremenska polinomna reducibilnost, a ne prostorna).

Formule kvantifikacijske propozicionalne logike $TQBF$ definiramo ovako:

$$p \mid \neg F \mid F \wedge G \mid F \vee G \mid F \to G \mid F \leftrightarrow G \mid \forall pF \mid \exists pF$$

Formula $\forall pF$ je oznaka za formulu $F(\bot/p) \wedge F(\top/p)$, a formula $\exists pF$ je oznaka za formulu $F(\bot/p) \vee F(\top/p)$. (Dakle, logika $TQBF$ se može svesti na klasičnu logiku, ali za to treba eksponencijalno vrijeme! Zašto?) Za neku $TQBF$–formulu kažemo da je zatvorena ako je svaka njena propozicionalna varijabla u dosegu nekog kvantifikatora.

Teorem 4.109. *(Stockmayer, 1974.)*
Problem određivanja istinitosti zatvorenih formula logike $TQBF$ *je PSPACE–potpun.*

Za jezik $\alpha \subseteq \Gamma^*$ označimo s $\overline{\alpha}$ njegov komplement $\Gamma^* \setminus \alpha$. Za svaku klasu složenosti $\mathcal{C}$ možemo definirati klasu co–$\mathcal{C}$ kao $\{\overline{\alpha} \mid \alpha \in \mathcal{C}\}$. Lako se vidi da za sve klase složenosti $\mathcal{C}$ definirane determinističkim Turingovim strojevima vrijedi $\mathcal{C} =$ co–$\mathcal{C}$, a također se može pokazati da ista tvrdnja vrijedi i za sve klase složenosti definirane nedeterminističkim prostorno omeđenim Turingovim strojevima. Ova tvrdnja posljedica je Immerman–Szelepscényjevog teorema koji govori o jednakosti klasa NLOGSPACE i co–NLOGSPACE. Otvoreni je problem da li su klase složenosti definirane nedeterminističkim vremenski omeđenim Turingovim strojevima zatvorene na komplement. Specijalno, pitanje o jednakosti klasa NP i co–NP predstavlja jedno od najpoznatijih otvorenih problema teorije računske složenosti.

Napomena 4.110. *Postavljena je hipoteza da ne postoji polinomni algoritam koji odlučuje* **Hilbertov Nullstellensatz** *nad* $\mathbb{C}$.

Prisjetimo se ukratko o čemu govori taj Hilbertov teorem. Neka su $f_1, \ldots, f_k$ *proizvoljni polinomi iz* $\mathbb{C}[X_1, \ldots, X_n]$. *Koji su nužni i dovoljni uvjeti da ti polinomi imaju zajedničku nul–točku? Odgovor na to pitanje daje Hilbertov Nullstellensatz:*

> *Skup polinoma* $\{f_1, \ldots, f_k\}$ *ima zajedničku nul–točku ako i samo ako ne postoje polinomi* $g_1, \ldots, g_k \in \mathbb{C}[X_1, \ldots, X_k]$ *tako da vrijedi* $\sum_{i=1}^{k} g_i \cdot f_i = 1$.

Odnosno, postoji nul–točka ako i samo ako je ideal $I = I(f_1, \ldots, f_k)$ *pravi ideal. (Ako postoje polinomi* $g_1, \ldots, g_k$ *takvi da je* $\sum g_i \cdot f_i = 1$, *tada pošto iz definicije ideala vrijedi* $I \cdot \mathbb{C}[X_1, \ldots, X_n] \subseteq I$, *tada imamo* $1 \in I$. *Tada je* $I = \mathbb{C}[X_1, \ldots, X_k]$).

Uočite da baš nema smisla pričati o Turingovim strojevima koji operiraju s kompleksnim brojevima! Definiraju se posebni strojevi koji operiraju s kompleksnim brojevima.

Bibliografija

[1] K. J. Barwise (ed.), *Handbook of math. logic, I–IV,* North–Holland, Amsterdam, 1977.

[2] J. L. Bell, A. B. Slomson, *Models and ultraproducts*, Dover Publications, Inc., Mineola, New York, 2006.

[3] P. Blackburn, M. de Rijke, Y. Venema, *Modal Logic,* Springer–Verlag, 2001.

[4] F. M. Brückler, V. Čačić, M. Doko, M. Vuković, *Zbirka zadataka iz teorije skupova*, web–izdanje, PMF–MO, Zagreb, 2008.
URL: web.math.hr/∼vukovic/dodiplomska_nastava.htm

[5] G. S. Boolos, J. P. Burgess, R. C. Jeffrey, *Computability and logic*, Fourth edition, Cambridge University Press, 2002.

[6] C. C. Chang, H. J. Keisler, *Model theory*, North–Holland, Amsterdam, 1997.

[7] R. Cori, D. Lascar, *Mathematical Logic I, II*, Oxford University Press, 2000.

[8] H.–D. Ebbinghaus, J. Flum, W. Thomas, *Mathematical logic*, Springer–Verlag, 1984.

[9] H.–D. Ebbinghaus, J. Flum, *Finite model theory*, Springer, 1999.

[10] P. Gács, L. Lovász, *Complexity of algorithms*, skripta, 1999.
URL: research.microsoft.com/users/lovasz/notes.htm

[11] E. Grädel i dr., *Finite model theory and its applications*, Springer, 2007.

[12] S. Hedman, *A First Course in Logic*, Oxford University Press, 2008.

[13] P. G. Hinman, *Fundamentals of Mathematical Logic*, A. K. Peters, 2005.

[14] C. W. Henson, *Model Theory*, Mathematics Department University of Illinois, 1998.
URL: www.math.uiuc.edu/%7Ehenson/papers/411notes.ps

[15] N. Immerman, *Descriptive Compexity*, Springer, 1999.

[16] T. Jech, *Set Theory*, The Third Millennium Edition, Revised and Expanded, Springer, 2002.

[17] L. Libkin, *Elements of Finite Model Theory*, Springer, 2004.

[18] D. Marker, *Model Theory: An Introduction*, Springer–Verlag, 2002.

[19] A. Marcja, C. Toffalori, *A guide to classical and modern model theory*, Kluwer Academic Publishers, 2003.

[20] B. Poizat, *A course in model theory*, Springer–Verlag, 2000.

[21] D. Prawitz, *Natural Deduction*, Almqvist&Wiksell, Stockholm, 1964.

[22] S. G. Simpson, *Model Theory*, Department of Mathematics The Pennsylvania State University, 1998.
URL: www.math.psu.edu/simpson/courses/math563

[23] S. Singer, *Složenost algoritama*, skripta, PMF-MO, Zagreb, 2005.
URL: web.math.hr/∼singer

[24] S. Singer, *Algoritmi u aritmetici i algebri*, skripta, PMF-MO, Zagreb, 2007., URL: web.math.hr/∼singer

[25] M. Sipser, *Introduction to the Theory of Computation*, PWS Publishing Company, 1996.

[26] G. Takeuti, *Proof theory*, North–Holland, Amsterdam, 1975.

[27] D. van Dalen, *Logic and structures*, Springer–Verlag, 1997.

[28] M. Vuković, *Matematička logika*, Element, 2009.

[29] M. Vuković, *Teorija skupova*, predavanja, PMF–MO, Zagreb, 2006.
URL: web.math.hr/∼vukovic/dodiplomska_nastava.htm

[30] M. Vuković, *Izračunljivost*, skripta, PMF–MO, Zagreb, 2007.
URL: web.math.hr/∼vukovic/dodiplomska_nastava.htm

[31] W. Weiss, C. D'Mello, *Fundamentals of Model Theory*, Department of Mathematics University of Toronto, 1997.
URL: www.math.uwo.ca/ mdawes/courses/420/mod_th.pdf

Indeks