Matematička logika i računarstvo

Vedran Čačić <veky@math.hr>
Marko Horvat <mhorvat@math.hr>

(Izvorni autor slajdova: Tin Perkov)

akademska godina 2022./23.

Uvodne informacije

Polaganje:

- predavanja: dva sata tjedno, trideset tjedana
- prvih 15 tjedana Čačić, drugih 15 tjedana Horvat
- četiri domaće zadaće (šalju se e-mailom)
- pristupni ispit (usmeni; prijava mjesec dana ranije!)

Literatura:

- M. Vuković: Primijenjena logika (poslano e-mailom)
- `https://web.math.pmf.unizg.hr/~veky/ml&r/`

Sadržaj kolegija (preciznije na webu — gornji URL):

- teorija modela
- modalna logika
- teorija dokaza
- izračunljivost
- Gödelovi teoremi nepotpunosti
- složenost

Sintaksa logike prvog reda: alfabet

- logički simboli $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\forall$ i $\exists$
- varijable: x, y, z, x_1, x_2, ... (prebrojivo mnogo)
- nelogički simboli:
  - relacijski: P, R, S, R_1, R_2, ... s pridruženom mjesnošću iz $\mathbb{N}_+$
  - funkcijski simboli: f, g, h, f_1, f_2, ... također s mjesnošću
  - konstantski simboli: c, c_1, c_2, ...
- pomoćni simboli: zagrade, zarez

Signatura σ je skup nelogičkih simbola.
Jezik teorije prvog reda zadan je izborom signature.
Signatura sadrži barem jedan dvomjesni relacijski simbol, dok skupovi funkcijskih i konstantskih simbola mogu biti i prazni.

Logika prvog reda je jedna istaknuta teorija prvog reda, čija signatura σ_{FO} ima prebrojivo mnogo relacijskih i funkcijskih simbola mjesnosti k za svaki $k \in \mathbb{N}_+$ i prebrojivo mnogo konstantskih simbola.

Sintaksa logike prvog reda: termi i formule

Neka je σ proizvoljna signatura.

(σ-)**term** je svaka riječ generirana pravilom

$$t \to x \mid c \mid f(t_1, \ldots, t_n)$$

(x je varijabla, c konstantski, a f funkcijski simbol mjesnosti n).

Atomarna formula (At) je riječ oblika $R(t_1, \ldots, t_n)$, gdje je R n-mjesni relacijski simbol, a t_1, ..., t_n su termi. Ako je R dvomjesni relacijski simbol, umjesto $R(t_1, t_2)$ često pišemo $t_1 \ R \ t_2$.

(σ-)**formula** je svaka riječ generirana pravilom

$$F \to At \mid \neg F \mid (F_1 \circ F_2) \mid \forall x\, F \mid \exists x\, F,$$

gdje je $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ binarni logički veznik, a x varijabla.

Složenost formule je broj pojavljivanja logičkih simbola u njoj.

Sintaksa logike prvog reda: slobodne i vezane varijable

U formulama koje sadrže potformulu oblika $\forall x\, F$ ili $\exists x\, F$,
za svaku pojavu x u F kažemo da je u **dosegu kvantifikatora**.
Varijabla x je **slobodna** u G ako se barem jednom pojavljuje u G izvan dosega kvantifikatora; inače je **vezana**.
Otvorena formula je formula bez kvantifikatora.
Zatvorena formula ili **rečenica** je formula bez slobodnih varijabli.
Formulu F u kojoj su sve slobodne varijable među varijablama $x_1, \ldots, x_n$ označavamo s $F(x_1, \ldots, x_n)$ ili kraće $F(\vec{x}\,)$.

Primjer

Teorija grupa je teorija prvog reda čija signatura sadrži jedan dvomjesni relacijski simbol $=$, jedan dvomjesni funkcijski simbol $\cdot$ i jedan konstantski simbol e. Umjesto $\cdot(t_1, t_2)$ pišemo $(t_1 \cdot t_2)$.
Navedimo neke poznate rečenice u jeziku teorije grupa:

- $\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$
- $\forall x (e \cdot x = x \land x \cdot e = x)$
- $\forall x \exists y (x \cdot y = e \land y \cdot x = e)$

Semantika logike prvog reda: σ-strukture

Formule interpretiramo na σ-**strukturama** $\mathfrak{M} = (M, \varphi)$, gdje je $M = |\mathfrak{M}| \neq \emptyset$ **nosač**, a $\varphi \colon \sigma \to M \cup \mathcal{P}(M^*)$ pridružuje svakom:

- n-mjesnom relacijskom simbolu R, relaciju $R^{\mathfrak{M}} \subseteq M^n$;
- n-mjesnom funkcijskom simbolu f, funkciju $f^{\mathfrak{M}} \colon M^n \to M$;
- konstantskom simbolu c, element $c^{\mathfrak{M}} \in M$.

Primjer

Struktura za signaturu teorije grupa (G, φ) nije nužno grupa, jer je

- $=^{\mathfrak{M}}$ binarna relacija na G, ali ne nužno baš jednakost;
- $\cdot^{\mathfrak{M}}$ binarna operacija na G, dakle funkcija $\cdot^{\mathfrak{M}} : G \times G \to G$, ali ne zadovoljava nužno npr. asocijativnost;
- $e^{\mathfrak{M}} \in G$, ali ne mora nužno biti jedinica za operaciju $\cdot^{\mathfrak{M}}$.

Semantika logike prvog reda: valuacija i interpretacija

Za danu σ-strukturu $\mathfrak{M}$, svaku funkciju v
sa skupa varijabli u nosač strukture zovemo **valuacija**.
Valuaciju rekurzivno proširujemo na skup svih σ-terma:

- $v(c) := c^{\mathfrak{M}}$, za svaki konstantski simbol c;
- $v\big(f(t_1, \dots, t_n)\big) = f^{\mathfrak{M}}\big(v(t_1), \dots, v(t_n)\big)$,
  za sve funkcijske simbole f mjesnosti n i terme t_1, ..., t_n.

Koristimo sljedeće oznake:

- za term t, umjesto $v(t)$ pišemo $t^{\mathfrak{M}}[v]$ ili $t^{\mathfrak{M}}[a_1, \dots, a_n]$,
  gdje je $v(x_1) = a_1, \dots, v(x_n) = a_n$, a u t se pojavljuju
  samo varijable (ne nužno sve) iz skupa $\{x_1, \dots, x_n\}$
- za valuaciju v i varijablu x, s v_x označavamo ma koju valuaciju
  koja se podudara s v na svim varijablama osim možda x

Uređeni par $(\mathfrak{M}, v) = (M, \varphi, v)$ zovemo **interpretacija**.

Semantika logike prvog reda: istinitost

Istinitost σ-formule F za danu interpretaciju $(\mathfrak{M}, v)$, u oznaci $\mathfrak{M} \models_v F$, definiramo rekurzivno:

- $\mathfrak{M} \models_v R(t_1, \ldots, t_n)$ znači da je $\left(t_1^{\mathfrak{M}}[v], \ldots, t_n^{\mathfrak{M}}[v]\right) \in R^{\mathfrak{M}}$;
- $\mathfrak{M} \models_v \neg F$ znači da ne vrijedi $\mathfrak{M} \models_v F$ (pišemo $\mathfrak{M} \not\models_v F$);
- $\mathfrak{M} \models_v (F_1 \wedge F_2)$ znači $\mathfrak{M} \models_v F_1$ i $\mathfrak{M} \models_v F_2$;
- $\mathfrak{M} \models_v (F_1 \vee F_2)$ znači $\mathfrak{M} \models_v F_1$ ili $\mathfrak{M} \models_v F_2$;
- $\mathfrak{M} \models_v (F_1 \rightarrow F_2)$ znači $\mathfrak{M} \not\models_v F_1$ ili $\mathfrak{M} \models_v F_2$;
- $\mathfrak{M} \models_v (F_1 \leftrightarrow F_2)$ znači: $\mathfrak{M} \models_v F_1$ ako i samo ako $\mathfrak{M} \models_v F_2$;
- $\mathfrak{M} \models_v \forall x F$ znači da za svaku valuaciju v_x vrijedi $\mathfrak{M} \models_{v_x} F$;
- $\mathfrak{M} \models_v \exists x F$ znači da postoji valuacija v_x takva da $\mathfrak{M} \models_{v_x} F$;

Koristimo sljedeće oznake:

- umjesto $\mathfrak{M} \models_v F(x_1, \ldots, x_n)$ pišemo $\mathfrak{M} \models F[a_1, \ldots, a_n]$, gdje je $a_1 := v(x_1)$, ..., $a_n := v(x_n)$;
- ako je Γ skup formula, oznaka $\mathfrak{M} \models_v \Gamma$ znači da za sve $F \in \Gamma$ vrijedi $\mathfrak{M} \models_v F$.

Semantika logike prvog reda: ispunjivost i valjanost

Kažemo da je formula F:

- **ispunjiva** ako postoji interpretacija $(\mathfrak{M}, v)$ tako da $\mathfrak{M} \models_v F$;
- **oboriva** ako postoji interpretacija $(\mathfrak{M}, v)$ tako da $\mathfrak{M} \not\models_v F$;
- **valjana** ako za svaku interpretaciju vrijedi $\mathfrak{M} \models_v F$.

Kažemo da je σ-struktura $\mathfrak{M}$ **model** za formulu F,
i pišemo $\mathfrak{M} \models F$, ako za svaku valuaciju v vrijedi $\mathfrak{M} \models_v F$.

Primjer

Svaka grupa je model za tri formule navedene u ranijem primjeru.

Za σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su **elementarno ekvivalentne**,
i pišemo $\mathfrak{M} \equiv \mathfrak{N}$, ako za sve rečenice F vrijedi

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

Preslikavanja između struktura: homomorfizam

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. **Homomorfizam** je preslikavanje između njihovih nosača $h\colon M \to N$ takvo da:

- za svaki n-mjesni relacijski simbol $R \in \sigma$ i za sve $(a_1, \ldots, a_n) \in R^{\mathfrak{M}}$ vrijedi $\big(h(a_1), \ldots, h(a_n)\big) \in R^{\mathfrak{N}}$;
- za svaki n-mjesni funkcijski simbol $f \in \sigma$ i sve $a_1, \ldots, a_n \in M$ vrijedi $h\big(f^{\mathfrak{M}}(a_1, \ldots, a_n)\big) = f^{\mathfrak{N}}\big(h(a_1), \ldots, h(a_n)\big)$;
- za svaki konstantski simbol $c \in \sigma$ vrijedi $h(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$.

Primjer

Homomorfizam grupa G i G' zaista je homomorfizam σ-struktura, gdje je σ signatura teorije grupa iz ranijih primjera. Naime, uvjet iz definicije homomorfizma grupa $h(a \cdot b) = h(a) \cdot h(b)$ upravo je uvjet iz definicije homomorfizma σ-struktura za funkcijski simbol $\cdot$. Homomorfizam jedinicu iz G preslikava u jedinicu iz G', što znači da je zadovoljen i uvjet za konstantske simbole, dok je uvjet za relacijski simbol $=$ trivijalno zadovoljen.

Preslikavanja između struktura: jaki homomorfizam

Nažalost, homomorfizam ne čuva nužno istinitost formula.

Primjer

Neka σ sadrži samo $=$ i neka su $\mathfrak{M}$ i $\mathfrak{N}$ strukture s nosačima $\mathbb{Z}$, odnosno $\mathbb{N}$ tako da su $=^{\mathfrak{M}}$ i $=^{\mathfrak{N}}$ odgovarajuće relacije jednakosti. Tada je s $h(x) := |x|$ zadan homomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. No, $\mathfrak{M} \models \neg(x_1 = x_2)[-1, 1]$, ali $\mathfrak{N} \not\models \neg(x_1 = x_2)[h(-1), h(1)]$.

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

$$(a_1, \ldots, a_n) \in R^{\mathfrak{M}} \iff \big(h(a_1), \ldots, h(a_n)\big) \in R^{\mathfrak{N}}.$$

Štoviše, tada je i za svaku otvorenu formulu $F(x_1, \ldots, x_n)$

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

No, za formule s kvantifikatorima to ne mora vrijediti.

Primjer

Inkluzija $h(x) := x$ je jaki homomorfizam struktura $(\mathbb{N}, \leq)$ i $(\mathbb{Z}, \leq)$. No, $\mathbb{N} \models \exists x \forall y (x \leq y)$, ali $\mathbb{Z} \not\models \exists x \forall y (x \leq y)$.

Podmodeli i proširenja

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

- $M := |\mathfrak{M}| \subseteq |\mathfrak{N}|$;
- za svaki n-mjesni relacijski simbol $R \in \sigma$ je $R^{\mathfrak{M}} = R^{\mathfrak{N}} \cap M^n$;
- za svaki n-mjesni funkcijski simbol $f \in \sigma$ je $f^{\mathfrak{M}} = f^{\mathfrak{N}}|_{M^n}$;
- za svaki konstantski simbol $c \in \sigma$ je $c^{\mathfrak{M}} = c^{\mathfrak{N}}$.

Propozicija

Neka $\mathfrak{M}$ podmodel od $\mathfrak{N}$ te v valuacija na $\mathfrak{M}$. Tada:

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

b) *za svaku otvorenu formulu F vrijedi:*

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

Dokaz.

Inkluzija je jaki homomorfizam. $\square$

Preslikavanja između struktura: smještenje i izomorfizam

Jaki homomorfizam koji je injekcija zovemo **smještenje**.
Na normalnim strukturama, svaki jaki homomorfizam je smještenje!
($\mathfrak{M}$ je **normalna** ako je $=^{\mathfrak{M}}$ baš jednakost na $|\mathfrak{M}|$.)

Jaki homomorfizam koji je bijekcija zovemo **izomorfizam**.
Pišemo $\mathfrak{M} \simeq \mathfrak{N}$ ako postoji izomorfizam između $\mathfrak{M}$ i $\mathfrak{N}$.

Propozicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. Sljedeće tvrdnje su ekvivalentne:

a) *postoji smještenje $h\colon M \to N$;*
b) *postoji podmodel od $\mathfrak{N}$ izomorfan s $\mathfrak{M}$.*

Teorem

Ako vrijedi $\mathfrak{M} \simeq \mathfrak{N}$ tada vrijedi i $\mathfrak{M} \equiv \mathfrak{N}$.

Elementarna preslikavanja

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ-strukture. Za preslikavanje $h\colon M \to N$ između njihovih nosača kažemo da je **elementarno preslikavanje** ako za svaku formulu $F(x_1, \ldots, x_n)$ i za sve $a_1, \ldots, a_n \in M$ vrijedi:

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

Iz definicija lako slijedi:

- (jaki) homomorfizam nije nužno elementarno preslikavanje;
- svaki izomorfizam jest elementarno preslikavanje;
- ako između struktura postoji elementarno preslikavanje, onda su one elementarno ekvivalentne;
- elementarno preslikavanje na normalnim strukturama je jaki homomorfizam (normalnost treba za funkcijske i konstantske simbole).

Elementarni podmodel i elementarno proširenje

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

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

Napomena

Na normalnim strukturama, elementarni podmodel je nužno podmodel (ne treba zahtijevati $\mathfrak{M} \subseteq \mathfrak{N}$ u definiciji). Dokaz za konstantske simbole je u skripti.

Propozicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. Tada vrijedi:

- *ako je $\mathfrak{M} \prec \mathfrak{N}$, onda je $\mathfrak{M} \equiv \mathfrak{N}$;*
- *ako je $\mathfrak{M} \prec \mathfrak{N}$, $\mathfrak{M}' \prec \mathfrak{N}$ i $\mathfrak{M} \subseteq \mathfrak{M}'$, onda je $\mathfrak{M} \prec \mathfrak{M}'$.*

Tarski–Vaughtov kriterij za elementarne podmodele

Teorem

Neka je $\mathfrak{M} \subseteq \mathfrak{N}$ *i neka za svaku formulu* $F(x_1, \ldots, x_k, x)$ *i za sve* $a_1, \ldots, a_k \in |\mathfrak{M}|$ *vrijedi: ako* $\mathfrak{N} \models \exists x F[a_1, \ldots, a_k]$*, onda postoji* $a \in |\mathfrak{M}|$ *takav da* $\mathfrak{N} \models F[a_1, \ldots, a_k, a]$*. Tada je* $\mathfrak{M} \prec \mathfrak{N}$*.*

Teorem se dokazuje indukcijom po složenosti formule.

Primjer

Pomoću prethodnog teorema pokazuje se $(\mathbb{Q}, <) \prec (\mathbb{R}, <)$ (uputa u skripti), a onda i $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$.
Dakle, elementarno ekvivalentne strukture nisu nužno izomorfne.
Očita posljedica je da aksiom potpunosti skupa $\mathbb{R}$ ne možemo izraziti nekom rečenicom prvog reda.
Podmodel nije nužno elementarni podmodel:

- $(\mathbb{Z}, 0, +) \subseteq (\mathbb{Q}, 0, +)$, ali $(\mathbb{Z}, 0, +) \not\prec (\mathbb{Q}, 0, +)$;
- polje $\mathbb{Q}$ je podmodel polja $\mathbb{R}$, ali nije elementarni podmodel;
- $(2\mathbb{Z}, 0, +) \subseteq (\mathbb{Z}, 0, +)$, čak je $(2\mathbb{Z}, 0, +) \simeq (\mathbb{Z}, 0, +)$, ali $(2\mathbb{Z}, 0, +) \not\prec (\mathbb{Z}, 0, +)$.

Elementarno smještenje

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

Propozicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ **normalne** *σ-strukture, te $h\colon |\mathfrak{M}| \to |\mathfrak{N}|$. Tada:*

- *h je smještenje ako i samo ako za svaku otvorenu formulu F i svaku valuaciju v na $\mathfrak{M}$ vrijedi da je $\mathfrak{M} \models_v F$ ekvivalentno s $\mathfrak{N} \models_{h \circ v} F$;*
- *h je elementarno smještenje ako i samo ako taj uvjet vrijedi za svaku formulu F.*

Propozicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. Tada postoji elementarno smještenje s $\mathfrak{M}$ u $\mathfrak{N}$ ako i samo ako postoji $\mathfrak{N}' \prec \mathfrak{N}$ takav da je $\mathfrak{M} \simeq \mathfrak{N}'$.

Unija (elementarnog) lanca struktura

Neka je $(I, <)$ linearno uređen skup. 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

Neka je $(I, <)$ linearno uređen skup i $\{\mathfrak{M}_i : i \in I\}$ (elementarni) lanac σ-struktura. Označimo sa $\mathfrak{M} := \bigcup_{i \in I} \mathfrak{M}_i$ σ-strukturu čiji je nosač unija nosača, a interpretacija svakog nelogičkog simbola, unija odgovarajućih intepretacija u danim σ-strukturama. Tada za svaki $i \in I$ vrijedi $\mathfrak{M}_i \subseteq \mathfrak{M}$ $(\mathfrak{M}_i \prec \mathfrak{M})$.

Dokaz.

Za podmodel je trivijalno. Za elementarni podmodel, indukcijom po složenosti formule (zapravo po broju ugniježđenih kvantifikatora) treba provjeriti Tarski–Vaughtov kriterij. $\square$

Parcijalni izomorfizam

Podsjetimo se: izomorfizam povlači elementarnu ekvivalenciju, no obrat ne vrijedi. Stoga je prirodno pitanje postoji li veza među elementarno ekvivalentnim strukturama, analogna izomorfizmu.

Definicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. **Parcijalni izomorfizam** *je svaka parcijalna injekcija $p\colon M \rightharpoonup N$ ($S := Dom(p) \subseteq M$) takva da*

- *za svaki relacijski simbol R i za sve $a_1, \ldots, a_n \in S$ vrijedi $(a_1, \ldots, a_n) \in R^{\mathfrak{M}}$ ako i samo ako $\big(p(a_1), \ldots, p(a_n)\big) \in R^{\mathfrak{N}}$;*
- *za svaki funkcijski simbol f i za sve $a_1, \ldots, a_n \in S$ vrijedi $b := f^{\mathfrak{M}}(a_1, \ldots, a_n) \in S \Longrightarrow p(b) = f^{\mathfrak{N}}\big(p(a_1), \ldots, p(a_n)\big)$;*
- *za svaki konstantski simbol c, $c^{\mathfrak{M}} \in S$ povlači $p(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$.*

Parcijalni izomorfizam nije nužno izomorfizam nekih podmodela, jer S ne mora biti podmodel — ne mora sadržavati interpretaciju svakog konstantskih simbola, niti mora biti zatvoren na interpretaciju svakog funkcijskog simbola.

Parcijalni izomorfizam na relacijskim strukturama

Definicija

Signaturu zovemo **relacijskom** *ako sadrži samo relacijske simbole.*

Lema

Neka je σ relacijska signatura, te neka su $\mathfrak{M}$ i $\mathfrak{N}$ dvije σ-strukture. Neka su $a_1, \ldots, a_n \in M$ i $b_1, \ldots, b_n \in N$. Tada je ekvivalentno:

a) *parcijalna funkcija $p \colon M \rightharpoonup N$ definirana s $p(a_i) = b_i$ za sve i je parcijalni izomorfizam;*

b) *za svaku atomarnu formulu F oblika $R(x_1, \ldots, x_n)$, za sve $i_1, \ldots, i_m \in \{1, \ldots, n\}$ vrijedi*

$$\mathfrak{M} \models F[a_{i_1}, \ldots, a_{i_m}] \text{ ako i samo ako } \mathfrak{N} \models F[b_{i_1}, \ldots, b_{i_m}].$$

Konačno izomorfne strukture

Definicija

σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$ su **konačno izomorfne** *ako postoji niz $(I_n)_{n\in\mathbb{N}}$ nepraznih skupova parcijalnih izomorfizama tako da*

(forth) *za sve $p \in I_{n+1}$ i $a \in M$ postoji $q \in I_n$ koji proširuje p i sadrži a u domeni;*

(back) *za sve $p \in I_{n+1}$ i $b \in N$ postoji $q \in I_n$ koji proširuje p i sadrži b u slici.*

Oznaka: $(I_n)_{n\in\mathbb{N}} : \mathfrak{M} \simeq_f \mathfrak{N}$ ili samo $\mathfrak{M} \simeq_f \mathfrak{N}$.

Uvjeti (forth) i (back) analogni su modernom dokazu teorema o uređajnoj karakterizaciji skupa $\mathbb{Q}$. Definicija konačne izomorfnosti analogna je i definiciji bisimulacije u modalnoj logici.

Teorem (Fraïssé)

Za konačne signature, za **normalne** *strukture $\mathfrak{M}$ i $\mathfrak{N}$, $\mathfrak{M} \equiv \mathfrak{N}$ je ekvivalentno s $\mathfrak{M} \simeq_f \mathfrak{N}$.*

Dokaz: nizom lema. Prvo za relacijsku signaturu. ($\Leftarrow$) je lakše.

Kvantifikatorski rang

Definicija

Svakoj σ-formuli pridružujemo **kvantifikatorski rang** *koji je rekurzivno definiran ovako:*

- $qr(At) := 0$, *ako je* At *atomarna formula*
- $qr(\neg F) := qr(F)$
- $qr(F \circ G) := \max\{qr(F), qr(G)\}$, *gdje je* $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
- $qr(\exists x F) := qr(\forall x F) := qr(F) + 1$

Drugim riječima, kvantifikatorski rang formule je maksimalna dubina ugniježđenih kvantifikatora u njoj.

Konačna izomorfnost povlači elementarnu ekvivalenciju

Neka je σ konačna relacijska signatura i $r \in \mathbb{N}$. Oznakom $L^{\sigma}_{r,n}$ označavamo skup svih σ-formula čije varijable su iz $\{v_1, \ldots, v_r\}$, a kvantifikatorski rang im je manji ili jednak n.

Lema

Neka je $(I_n)_{n\in\mathbb{N}} \colon \mathfrak{M} \simeq_f \mathfrak{N}$; neka su $n, r \in \mathbb{N}$ i $F \in L^{\sigma}_{r,n}$; neka je $p \in I_n$ i $a_1, \ldots, a_r \in Dom(p)$. Tada 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. □

Primjenom leme na zatvorene formule slijedi:

Korolar

Neka je σ konačan skup relacijskih simbola. Za svake dvije σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$ vrijedi: ako $\mathfrak{M} \simeq_f \mathfrak{N}$, tada $\mathfrak{M} \equiv \mathfrak{N}$.

Relacija logičke posljedice i logička ekvivalentnost

Kažemo da σ-formula F **logički slijedi** iz skupa σ-formula S, i pišemo $S \models F$, ako za svaku σ-strukturu $\mathfrak{M}$, iz $\mathfrak{M} \models S$ slijedi $\mathfrak{M} \models F$. Relaciju $\models$ nazivamo **relacija logičke posljedice**.

Za jednočlane skupove, umjesto $\{A\} \models B$ pišemo $A \Rightarrow B$.

Kažemo da su σ-formule F i G **logički ekvivalentne**, i pišemo $F \Leftrightarrow G$, ako vrijedi $F \Rightarrow G$ i $G \Rightarrow F$.

Lema

Neka su $n, r \in \mathbb{N}$ proizvoljni, te σ konačna signatura. Tada je kvocijentni skup $L^{\sigma}_{r,n} \big/_{\Leftrightarrow}$ konačan.

Lema se dokazuje indukcijom po n — važna je konačnost skupa σ.

U skripti je definiran operator zatvorenja skupa formula na logičke veznike i istaknuta su njegova svojstva potrebna u dokazu leme.

Elementarna ekvivalencija povlači konačnu izomorfnost

Lema

Neka je σ konačan skup relacijskih simbola, te neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture. Ako $\mathfrak{M} \equiv \mathfrak{N}$, onda $\mathfrak{M} \simeq_f \mathfrak{N}$.

Dokaz.

Za svaki $n \in \mathbb{N}$ definiramo I_n kao skup parcijalnih izomorfizama $\{(a_1, b_1), \ldots, (a_r, b_r)\}$ takvih da za svaku formulu $F \in L^\sigma_{r,n}$ vrijedi:

$$\mathfrak{M} \models F[a_1, \ldots, a_r] \text{ ako i samo ako } \mathfrak{N} \models F[b_1, \ldots, b_r].$$

Za svaki $n \in \mathbb{N}$ je $I_n \neq \emptyset$, 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 $Dom(p) = \{a_1, \ldots, a_r\}$.
Po prethodnoj lemi, postoji konačan $\{F_1, \ldots, F_s\} \subseteq L^\sigma_{r+1,n}$ takav da za svaku formulu $F \in L^\sigma_{r+1,n}$ postoji $i \in \{1, \ldots, s\}$ tako da vrijedi $F \Leftrightarrow F_i$. . . .

Elementarna ekvivalencija povlači konačnu izomorfnost

Dokaz (nastavak).

Za svaki $i \in \{1, \ldots, s\}$ definiramo formulu G_i ovako:

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

Tada očito

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

te je $qr(\exists v_{r+1}(G_1 \wedge \cdots \wedge G_s)) \leq n + 1$. Iz definicije niza $(I_n)_n$ slijedi $\mathfrak{N} \models \exists v_{r+1}(G_1 \wedge \cdots \wedge G_s)[p(a_1), \ldots, p(a_r)]$, pa postoji $b \in N$ takav da vrijedi

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

...

Elementarna ekvivalencija povlači konačnu izomorfnost

Dokaz (nastavak).

Neka je $F \in L^{\sigma}_{r+1,n}$.
Tada postoji $i \in \{1, \ldots, s\}$ takav da je $F \Leftrightarrow F_i$.
Pretpostavimo sada $\mathfrak{M} \models F[a_1, \ldots, a_r, a]$.
Tada iz $F \Leftrightarrow F_i$ slijedi $\mathfrak{M} \models F_i[a_1, \ldots, a_r, a]$, pa je $G_i = F_i$.
Sada iz $(**)$ posebno slijedi $\mathfrak{N} \models G_i[p(a_1), \ldots, p(a_r), b]$,
odnosno $\mathfrak{N} \models F_i[p(a_1), \ldots, p(a_r), b]$.
Zbog $F \Leftrightarrow F_i$ je $\mathfrak{N} \models F[p(a_1), \ldots, p(a_r), b]$.
Analogno se dokazuje i obrat, pa imamo

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

Treba dokazati da postoji proširenje q od p koje pripada skupu I_n i vrijedi $a \in Dom(q)$. Ako je $a \in Dom(p)$, stavimo $q := p$.
Ako $a \notin Dom(p) = \{a_1, \ldots, a_r\}$, tvrdimo da je
$q := p \cup \{(a, b)\} \in I_n$ traženo proširenje. ...

Elementarna ekvivalencija povlači konačnu izomorfnost

Dokaz (nastavak).

Pokažimo da je q injekcija. Neka je $F := \left(\bigwedge_{i=1}^{r} v_i \neq v_{r+1} \right)$.
Uočimo da je $F \in L^{\sigma}_{r+1,0} \subseteq L^{\sigma}_{r+1,n}$ te vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_r, a]$.
Iz toga i $(***)$ slijedi

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

dakle $b \notin \{p(a_1), \ldots, p(a_r)\}$.
Kako bismo dokazali da funkcija $q = p \cup \{(a, b)\}$ pripada skupu I_n, potrebno je još vidjeti da za svaki k-mjesni relacijski simbol $R \in \sigma$ i sve $c_1, \ldots, c_k \in Dom(p)$ vrijedi:

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

No, to slijedi iz $(***)$ i $Dom(p) = \{a_1, \ldots, a_r\}$. (back) analogno.
Funkcijske (i konstantske) simbole emuliramo relacijskima. $\square$

Parcijalna izomorfnost

Definicija

Za σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$ kažemo da su **parcijalno izomorfne** *ako postoji neprazan skup I parcijalnih izomorfizama koji ima svojstva*

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

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

Oznaka: $I : \mathfrak{M} \simeq_p \mathfrak{N}$ ili samo $\mathfrak{M} \simeq_p \mathfrak{N}$.

Vrijedi:

- $\mathfrak{M} \simeq \mathfrak{N}$ povlači $\mathfrak{M} \simeq_p \mathfrak{N}$, što pak povlači $\mathfrak{M} \simeq_f \mathfrak{N}$;
- ako je struktura $\mathfrak{M}$ konačna, tada $\mathfrak{M} \simeq_f \mathfrak{N}$ povlači $\mathfrak{M} \simeq \mathfrak{N}$;
- Karpov teorem: ako su strukture $\mathfrak{M}$ i $\mathfrak{N}$ prebrojive ili konačne, tada $\mathfrak{M} \simeq_p \mathfrak{N}$ povlači $\mathfrak{M} \simeq \mathfrak{N}$.

Karpov teorem

Dokaz Karpova teorema.

Ideju ste već vidjeli u dokazu uređajne karakterizacije skupa $\mathbb{Q}$.
Neka je $I : \mathfrak{M} \simeq_p \mathfrak{N}$.
Enumerirajmo $|\mathfrak{M}| = \{a_0, a_1, a_2, \dots\}$ i $|\mathfrak{N}| = \{b_0, b_1, b_2, \dots\}$.
Neka je $p_0 \in I$. Primjenom uvjeta (forth) i (back) induktivno konstruiramo niz parcijalnih izomorfizama $(p_n)_n$ u I tako da vrijedi $a_0 \in Dom(p_1)$, $b_0 \in Rng(p_2)$, $a_1 \in Dom(p_3)$, $b_1 \in Rng(p_4)$ i tako dalje. Preciznije, niz (p_n) ima sljedeća svojstva:

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

b) ako je $n = 2r + 1$, onda je $a_r \in Dom(p_n)$;

c) ako je $n = 2r$, onda je $b_r \in Rng(p_n)$.

Iz uvjeta a) slijedi da je dobro definirana funkcija $p := \bigcup_n p_n$, koja je očito parcijalni izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$.

Iz uvjeta b) i c) slijedi redom $Dom(p) = |\mathfrak{M}|$ i $Rng(p) = |\mathfrak{N}|$.
To znači da je p izomorfizam. $\square$

Ispunjivi i konačno ispunjivi skupovi rečenica

Neka je S skup σ-rečenica i $\mathfrak{M}$ σ-struktura.
Pišemo $\mathfrak{M} \models S$ ako za sve $F \in S$ vrijedi $\mathfrak{M} \models F$.
S je **ispunjiv** ako postoji $\mathfrak{M}$ takav da je $\mathfrak{M} \models S$. S je **konačno ispunjiv** ako je svaki njegov konačni podskup ispunjiv.

Ispunjivi i konačno ispunjivi skupovi rečenica

Propozicija

Sljedeće tvrdnje su ekvivalentne:

a) *svaki konačno ispunjiv skup rečenica je ispunjiv;*

b) *za svaki skup rečenica S i svaku rečenicu F takvu da $S \models F$ postoji konačan $S' \subseteq S$ takav da $S' \models F$.*

Dokaz.

$\boxed{\Rightarrow}$ Pretpostavimo suprotno, da za svaki konačan $S' \subseteq S$ postoji $\mathfrak{M}'$ takav da $\mathfrak{M}' \models S' \cup \{\neg F\}$. Iz toga slijedi da je $S \cup \{\neg F\}$ konačno ispunjiv, pa je prema a) ispunjiv: postoji $\mathfrak{M}$ takav da $\mathfrak{M} \models S \cup \{\neg F\}$, što je u kontradikciji s $S \models F$.

$\boxed{\Leftarrow}$ Pretpostavimo suprotno, da postoji konačno ispunjiv S koji nije ispunjiv. Tada trivijalno vrijedi $S \models \neg F$, gdje je F neka valjana rečenica, npr. $\forall x\big(R(x,x) \to R(x,x)\big)$. No, sada iz b) slijedi $S' \models \neg F$ za neki konačan $S' \subseteq S$, što je nemoguće jer je S' ispunjiv, pa postoji $\mathfrak{M}$ takav da $\mathfrak{M} \models S'$, dok $\neg F$ nije ispunjiva, dakle $\mathfrak{M} \not\models F$. $\square$

Lindenbaumova lema

Teorem (Teorem kompaktnosti)

Skup rečenica S je ispunjiv ako i samo ako je svaki konačan podskup od S ispunjiv.

Nužnost očito vrijedi, a dovoljnost dokazujemo nizom lema.
Skup σ-rečenica S je **potpun** ako za svaku σ-rečenicu F vrijedi $S \models F$ ili $S \models \neg F$.

Lema (Lindenbaumova lema)

Svaki konačno ispunjiv skup rečenica
ima konačno ispunjiv potpun nadskup.

Dokaz.

Neka je S konačno ispunjiv, i definiramo
$\mathcal{S} := \{T : S \subseteq T,\ T$ konačno ispunjiv skup rečenica$\} \ni S$.
Unija svakog lanca u $(\mathcal{S}, \subseteq)$ također je u $\mathcal{S}$, pa svaki lanac ima gornju među. Prema Zornovoj lemi $\mathcal{S}$ ima maksimalni element S'.
Lako se vidi da je S' potpun skup rečenica. $\square$

Henkinov skup rečenica i kanonski model

Skup S σ-rečenica je **Henkinov** ako za svaku formulu iz S oblika $\exists x F(x)$ postoji zatvoreni σ-term t takav da vrijedi $F(t/x) \in S$. [$F(t/x)$ označava formulu nastalu supstitucijom svakog slobodnog nastupa varijable x u formuli $F(x)$ termom t.]
Kažemo da je σ-struktura $\mathfrak{M}$ **kanonski model** ako za svaki $a \in |\mathfrak{M}|$ postoji zatvoreni term t tako da vrijedi $t^{\mathfrak{M}} = a$.

Lema

Za svaki potpun konačno ispunjiv Henkinov skup σ-rečenica S postoji kanonski model.

Ideja dokaza.

Za nosač uzmemo skup svih zatvorenih terma i definiramo interpretacije nelogičkih simbola na prirodan način, npr. za n-mjesni relacijski simbol R stavimo $(t_1, \dots, t_n) \in R^{\mathfrak{M}}$ ako i samo ako je $R(t_1, \dots, t_n) \in S$. Indukcijom po složenosti se pokaže da slično vrijedi za sve formule, pa smo dobili model za S. $\square$

Dokaz teorema kompaktnosti

Lema
Svaki konačno ispunjiv skup rečenica S je ispunjiv.

Dokaz.
Simultanom rekurzijom definiramo niz signatura $(\sigma_n)_n$, skupova formula $(T_n)_n$ i skupova rečenica $(S_n)_n$:

$$\begin{aligned}
\sigma_0 &:= \text{skup svih nelogičkih simbola svih rečenica iz } S\\
T_n &:= \text{skup svih } \sigma_n\text{-formula s jednom slobodnom varijablom } x\\
\sigma_{n+1} &:= \sigma_n \mathbin{\dot\cup} \{c_F : F \in T_n\} \ (c_F \text{ su svi novi i međusobno različiti})\\
S_0 &:= S\\
S_{n+1} &:= S_n \cup \{\big(\exists x F(x) \to F(c_F/x)\big) : F \in T_n\}
\end{aligned}$$

Dokažimo indukcijom po n da je svaki skup S_n konačno ispunjiv.

...

Dokaz teorema kompaktnosti

Nastavak dokaza.
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}.
$\Sigma_1 := \Sigma \cap S_n$ je konačan podskup od S_n, pa je ispunjiv:
neka je $\mathfrak{M}$ neki model za Σ_1. Neka su $c_{F_1}, \ldots, c_{F_m}$ svi konstantski simboli iz $\sigma_{n+1} \setminus \sigma_n$ koji se pojavljuju u formulama iz Σ.
Na $\mathfrak{M}$ definiramo interpretaciju konstantskih simbola c_{F_i}:

$$c_{F_i}{}^{\mathfrak{N}} := \begin{cases} a \in |\mathfrak{M}| \text{ takav da } \mathfrak{M} \models F_i[a], & \text{ako takav } a \text{ postoji} \\ \text{proizvoljan } a \in |\mathfrak{M}|, & \text{inače} \end{cases}$$

(formalno, koristimo funkciju izbora na $|\mathfrak{M}|$). Očito $\mathfrak{N} \models \Sigma$.

Neka je S' potpun konačno ispunjiv nadskup od $\bigcup S_n$ (postoji po Lindenbaumovoj lemi). Očito je S' Henkinov skup, pa je ispunjiv.
Redukcijom njegovog modela na σ_0 dobivamo model za S_0. $\square$

Definabilnost u logici prvog reda

Definicija

Za skup σ-formula S, $Mod(S)$ označava klasu svih σ-struktura $\mathfrak{M}$ takvih da $\mathfrak{M} \models S$ (klasu svih modela za S).
Klasa σ-struktura $\mathcal{K}$ je **elementarna** *ako postoji skup σ-formula S takav da je $Mod(S) = \mathcal{K}$.*

Primjer

Neke elementarne klase:

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

Definabilnost konačnim skupom formula

Definicija

Klasa σ-struktura $\mathcal{K}$ je **Δ-elementarna** *ako postoji konačan skup σ-formula S takav da je $Mod(S) = \mathcal{K}$.*

Dokažite da bez smanjenja općenitosti možemo pretpostaviti da je S iz definicije jednočlan: $S = \{F\}$, **te da je F rečenica**.

Propozicija

Neka je S skup σ-formula takav da je $\mathcal{K} = Mod(S)$ Δ-elementarna klasa. Tada postoji konačan $S' \subseteq S$ takav da je $Mod(S') = \mathcal{K}$.

Dokaz.

Neka je $\mathcal{K} = Mod(\{F\})$. Očito je tada $S \models F$.
Zbog kompaktnosti postoji konačan $S' \subseteq S$ takav da $S' \models F$.
Iz $S' \subseteq S$ slijedi $Mod(S') \supseteq Mod(S) = \mathcal{K}$,
a iz $S' \models F$ slijedi $Mod(S') \subseteq Mod(\{F\}) = \mathcal{K}$. $\square$

Karakterizacija Δ-elementarnosti

Lema

Za klasu σ-struktura $\mathcal{K}$, s $\mathcal{K}^c$ (komplement) označimo klasu svih σ-struktura koje ne pripadaju $\mathcal{K}$.
Klasa $\mathcal{K}$ je Δ-elementarna ako i samo ako su $\mathcal{K}$ i $\mathcal{K}^c$ elementarne.

Dokaz.

- $\Rightarrow$ Ako je $\mathcal{K} = Mod(\{F\})$, tada je $\mathcal{K}^c = Mod(\{\neg F\})$.
- $\Leftarrow$ Neka je $\mathcal{K} = Mod(S_1)$ i $\mathcal{K}^c = Mod(S_2)$. Skup $S_1 \cup S_2$ nije ispunjiv, pa iz teorema kompaktnosti slijedi da postoje konačni $S_1' \subseteq S_1$ i $S_2' \subseteq S_2$ takvi da $S_1' \cup S_2'$ nije ispunjiv. Vrijedi $Mod(S_1') \supseteq Mod(S_1) = \mathcal{K}$; dokažimo drugu inkluziju.

  Pretpostavimo suprotno, da je $\mathfrak{M} \in Mod(S_1')$ te $\mathfrak{M} \notin \mathcal{K}$ za neku σ-strukturu $\mathfrak{M}$. Tada $\mathfrak{M} \in \mathcal{K}^c = Mod(S_2) \subseteq Mod(S_2')$, pa bismo imali $\mathfrak{M} \models S_1' \cup S_2'$,
  što je kontradikcija s neispunjivošću od $S_1' \cup S_2'$. $\square$

Primjeri elementarnih klasa koje nisu Δ-elementarne

Primjer

Klasa svih beskonačnih skupova je elementarna, jer je jednaka

$$Mod\left(\left\{\exists y_1 \ldots \exists y_n \bigwedge_{1\le i<j\le n} y_i \neq y_j : n \in \mathbb{N}\setminus\{0,1\}\right\}\right),$$

ali nije Δ-elementarna po prethodnoj propoziciji: za svaki konačni podskup tog skupa formula postoji najveći n, pa bilo koji skup s n elemenata zadovoljava taj podskup (a nije beskonačan).
Po prethodnoj lemi, klasa svih konačnih skupova nije elementarna.

Primjer

Abelova grupa $(G,+)$ je **djeljiva** ako za svaki $n \in \mathbb{N}_+$ i $x \in G$ postoji $y \in G$ takav da je $\underbrace{y + \cdots + y}_{n \text{ puta}} = x$. Dokažite (kao gore):

Klasa svih djeljivih grupa je elementarna, ali nije Δ-elementarna.
Pitanje: Što možemo onda zaključiti o klasi svih nedjeljivih grupa?

Primjeri elementarnih klasa koje nisu Δ-elementarne

Primjer

Klasa $\mathcal{K}_0$ svih polja karakteristike nula je elementarna, ali nije Δ-elementarna. Označimo sa S_0 skup aksioma teorije polja. Za proizvoljni prim-broj p, s $\overline{p}$ označimo term $\underbrace{1 + \cdots + 1}_{p \text{ puta}}$.

Tada za $S := S_0 \cup \{\overline{p} \neq 0 : p \in \mathbb{P}\}$ vrijedi $Mod(S) = \mathcal{K}_0$. Kad bi $\mathcal{K}_0$ bila Δ-elementarna, recimo $\mathcal{K}_0 = Mod(S')$ za konačni skup $S' \subseteq S$, postojalo bi konačno mnogo prim-brojeva $p_1, \ldots, p_k$ takvih da je $(\overline{p_i} \neq 0) \in S'$. Euklidov dokaz kaže da postoji $p \in \mathbb{P}$ različit od svih p_i, pa $\mathbb{Z}_p \models S'$, ali $\mathbb{Z}_p \notin \mathcal{K}_0$.

Također:

- za $p \in \mathbb{P}$, klasa svih polja karakteristike p je Δ-elementarna
- klasa svih polja pozitivne karakteristike nije elementarna
- (slično, ali treba znati algebru) klasa svih algebarski zatvorenih polja je elementarna, ali nije Δ-elementarna

Logika drugog reda

Prethodni primjeri mogu nam poslužiti kao motivacija za razmatranje proširenja logike prvog reda.
U **logici drugog reda** dopuštena je i kvantifikacija po relacijskim i funkcijskim varijablama.
Tako se mogu definirati (bes)konačnost i prebrojivost. Međutim:

Propozicija

Za logiku drugog reda ne vrijedi teorem kompaktnosti.

Dokaz.

Za svaki $n \in \mathbb{N} \setminus \{0, 1\}$ definiramo formulu

$$\psi_{\geq n} := \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j.$$

Također, u logici drugog reda postoji formula φ_{fin} koja izražava svojstvo da je svaka injekcija na proizvoljnom skupu ujedno i surjekcija (napišite ju!). Lako se vidi da $\{\varphi_{fin}, \psi_{\geq 2}, \psi_{\geq 3}, \psi_{\geq 4}, \dots\}$ nema model, ali svaki njegov konačan podskup ima model. $\square$

Logika drugog reda

Napomenimo da za logiku drugog reda ne vrijedi ni jaki teorem potpunosti, kao ni analogon Gödelova teorema potpunosti: skup svih valjanih formula logike drugog reda nije rekurzivno prebrojiv.

Propozicija

Za logiku drugog reda ne vrijedi ni Löwenheim–Skolemov teorem „na dolje".

Dokaz.

Treba definirati formulu koja ima model, ali nema prebrojiv model.

U logici drugog reda (slično kao na prethodnom slajdu) postoji formula $\psi_{fin}(X)$ koja kaže da je interpretacija od X konačna unarna relacija.

Pomoću formule ψ_{fin} nije teško definirati formulu ψ_p koja kaže da postoji uređaj u kojem od svakog elementa postoji samo konačno mnogo manjih elemenata.

Tada vrijedi $\mathfrak{M} \models \neg\psi_p$ ako i samo ako je $|\mathfrak{M}|$ neprebrojiv. $\square$

Beskonačna logika

U **beskonačnoj logici** dopuštene su beskonačne konjunkcije i disjunkcije. Logika $L_{\omega_1\omega}$, uz ostale, ima i sljedeća pravila izgradnje formula: ako je S prebrojiv skup formula, $\bigwedge S$ i $\bigvee S$ su formule.

Simbol $L_{\omega_1\omega}$ označava da je dozvoljeno prebrojivo mnogo ($< \omega_1$) konjunkata i disjunkata, te konačno mnogo ($< \omega$) kvantifikatora.

Za logiku $L_{\omega_1\omega}$ vrijedi Löwenheim–Skolemov teorem „na dolje", ali ne vrijedi teorem kompaktnosti.

Promatraju se i druga proširenja logike prvog reda:

- višesortna logika prvog reda
- slaba logika drugog reda
  (kvantifikacija samo po konačnim podskupovima)
- monadska logika drugog reda
  (kvantifikacija samo po unarnim relacijama)
- logike s dodatnim kvantifikatorima
- ...

Ramseyev teorem

U grupi od $R_3 = 6$ ljudi uvijek postoje 3 koji se međusobno poznaju ili postoji grupa od 3 u kojoj nitko nikog ne poznaje.

Kolika mora biti najmanja grupa ljudi tako da sigurno postoje 4 osobe koje se međusobno poznaju ili postoji grupa od 4 osobe u kojoj nitko nikog ne poznaje? $(R_4 = 18)$ Što je s $n > 4$?

Erdős: if an alien force, vastly more powerful than us, demands the value of R_5 or else they will destroy our planet, we should do everything we can to find it.

But if they ask for R_6, we should attempt to destroy the aliens instead.

Teorem (Ramsey)

Za svaki $n \in \mathbb{N}$ postoji $R_n \in \mathbb{N}$ tako da svaki graf s najmanje R_n čvorova sadrži barem jedan potpuni podgraf s n čvorova ili barem jedan prazan podgraf s n čvorova.

Ramseyev teorem je relativno teško direktno dokazati.

Jednostavnije je dokazati slični rezultat za beskonačne grafove. Nakon toga ćemo relativno jednostavno primjenom tog rezultata i teorema kompaktnosti dokazati Ramseyev teorem.

Beskonačna verzija Ramseyevog teorema

Lema

Svaki beskonačan graf (V, E) sadrži beskonačan potpun podgraf ili beskonačan prazan podgraf.

Dokaz.

Neka je $a_0 \in V$ proizvoljan. Podijelimo $V \setminus \{a_0\}$ u dva dijela:
u $V_{0\top}$ su oni x za koje je $a_0 \; E \; x$, a u $V_{0\bot}$ ostali.
Barem jedan od ta dva dijela je beskonačan.
Definiramo $V_1 := V_{0\top}$ ako je $V_{0\top}$ beskonačan, a $V_1 := V_{0\bot}$ inače.

Sad istu stvar ponovimo s V_1: neka je $a_1 \in V_1$ proizvoljan.
Podijelimo $V_1 \setminus \{a_1\}$ na dva dijela, ovisno o tome jesu li mu elementi u relaciji s a_1 ili nisu. Barem jedan od dijelova je beskonačan, označimo ga s V_2, u njemu odaberemo a_2, ...

Sada elemente od $B := \{a_n : n \in \mathbb{N}\}$ podijelimo u dva dijela, ovisno o tome jesmo li ih odabirali iz skupa $V_{n\top}$ ili $V_{n\bot}$.
Barem jedan od ta dva dijela je beskonačan.
Taj skup vrhova tvori potpun ili prazan podgraf. $\square$

Dokaz Ramseyevog teorema

Pretpostavimo da Ramseyev teorem ne vrijedi, odnosno da postoji $n_0 \in \mathbb{N}$ takav da za svaki $m \in \mathbb{N}$ postoji graf s $p \geq m$ čvorova koji ne sadrži potpuni podgraf s n_0 čvorova ni prazan podgraf s n_0 čvorova. Uvodimo oznake za formule:

$$\varphi_{\text{gr}} := \forall x \neg (x\ E\ x) \wedge \forall x \forall y (x\ E\ y \to y\ E\ x)$$

$$\varphi_{\geq k} := \exists y_1 \cdots \exists y_k \bigwedge_{1 \leq i < j \leq k} \neg (y_i = y_j), \text{ za svaki } k \in \mathbb{N} \setminus \{0, 1\}$$

$$\varphi_{\perp} := \exists y_1 \cdots \exists y_{n_0} \bigwedge_{1 \leq i < j \leq n_0} \big(\neg (y_i = y_j) \wedge \neg (y_i\ E\ y_j) \big)$$

$$\varphi_{\top} := \exists y_1 \cdots \exists y_{n_0} \bigwedge_{1 \leq i < j \leq n_0} \big(\neg (y_i = y_j) \wedge y_i\ E\ y_j \big).$$

Tvrdimo da je konačno ispunjiv skup

$$\Sigma := \{\varphi_{\text{gr}}, \varphi_{\geq 2}, \varphi_{\geq 3}, \varphi_{\geq 4}, \ldots, \neg\varphi_{\perp}, \neg\varphi_{\top}\}.$$

Dokaz Ramseyevog teorema

Neka je Σ_0 proizvoljan konačan podskup od Σ, te $m \in \mathbb{N}$ najveći takav da je $\varphi_{\geq m} \in \Sigma_0$. Iz pretpostavke suprotnog slijedi da postoji $p \geq m$ i graf G s p čvorova koji ne sadrži ni potpun ni prazan podgraf s n_0 čvorova. Iz toga slijedi $G \models \Sigma_0$.

Iz teorema kompaktnosti sada 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 $\mathfrak{M}$ ne može sadržavati ni beskonačni potpuni, ni beskonačni prazni podgraf, što je kontradikcija s beskonačnom verzijom Ramseyevog teorema.

Löwenheim–Skolemovi teoremi

na dolje: svaka teorija prvog reda koja ima beskonačan normalni model ima i prebrojiv normalni model

na gore: svaka teorija prvog reda koja ima beskonačan normalni model (ili proizvoljno velike normalne konačne modele), ima normalni model proizvoljne beskonačne kardinalnosti

U nastavku, signatura σ i skup svih varijabli mogu biti proizvoljne kardinalnosti, s tim da varijabli ima barem prebrojivo mnogo.
S L_σ označavamo uniju skupa svih varijabli i signature σ.
(Dakle L_σ je sigurno beskonačan, a najčešće prebrojiv.)

Löwenheim–Skolemov teorem „na dolje"

Neka je $\mathfrak{M}$ neka σ-struktura, $B \subseteq |\mathfrak{M}|$ i $\operatorname{card} L_\sigma \leq \operatorname{card} |\mathfrak{M}|$.
Tada postoji elementarni podmodel $\mathfrak{N}$ od $\mathfrak{M}$ takav da je $B \subseteq |\mathfrak{N}|$ i $\operatorname{card} |\mathfrak{N}| = \max\{\operatorname{card} B, \operatorname{card} L_\sigma\}$.

Slabi Löwenheim–Skolemov teorem „na dolje"
dobivamo kao posljedicu, za prebrojive L_σ i B.

Podmodel generiran podskupom nosača

Teorem (Knaster–Tarski)

Neka je A proizvoljan skup i $F : \mathcal{P}(A) \to \mathcal{P}(A)$ rastuća funkcija. Tada postoje najmanja i najveća fiksna točka funkcije F.

Neka je $\mathfrak{M}$ σ-struktura i $B \subseteq M$. Definiramo $F : \mathcal{P}(M) \to \mathcal{P}(M)$: $F(X) := B \cup X \cup \{f^{\mathfrak{M}}(a_1, \ldots, a_k) : f \in \sigma, a_1, \ldots, a_k \in B \cup X\} \cup$ $\cup \{c^{\mathfrak{M}} : c \in \sigma\}$. Očito je F rastuća, pa iz Knaster–Tarskijevog teorema slijedi da postoji najmanja fiksna točka X_0. Tada je X_0 nosač podmodela od $\mathfrak{M}$, koji zovemo **podmodel generiran** s B.

Propozicija

Neka je $\operatorname{card} L_\sigma \leq \operatorname{card} B$ *i neka je* $\mathfrak{N}$ *podmodel od* $\mathfrak{M}$ *generiran s* B. *Tada vrijedi* $\operatorname{card} |\mathfrak{N}| = \operatorname{card} B$.

Dokaz.

Svaki element nosača $|\mathfrak{N}|$ je interpretacija nekog σ-terma s parametrima iz skupa B. Svaki element iz $|\mathfrak{N}|$ određuje konačan niz u $B \cup \sigma$, pa je $\operatorname{card} |\mathfrak{N}| \leq \operatorname{card}\big((B \cup \sigma)^*\big) = \operatorname{card} B$. $\square$

Dokaz Löwenheim–Skolemova teorema „na dolje"

Lema

Neka je $\mathfrak{M}$ neka σ-struktura i $B \subseteq \mathfrak{M}$, te neka je μ kardinalni broj između (uključivo) $\max\{\operatorname{card} L_\sigma, \operatorname{card} B\}$ *i* $\operatorname{card} |\mathfrak{M}|$. *Tada postoji podmodel $\mathfrak{N}$ od $\mathfrak{M}$ takav da je $B \subseteq |\mathfrak{N}|$ i* $\operatorname{card} |\mathfrak{N}| = \mu$.

Dokaz.

Zbog uvjeta na μ postoji skup B_0 kardinalnosti μ takav da je $B \subseteq B_0 \subseteq |\mathfrak{M}|$ (dokažite!). Definiramo F kao prije, samo za B_0 umjesto B. Stavimo $B_{n+1} = F(B_n)$, $n \in \mathbb{N}$.
Slično kao u prethodnoj propoziciji, za svaki $n \in \mathbb{N}$ vrijedi $\operatorname{card} B_n = \mu$. Iz teorije skupova znamo: ako je $\aleph_0 \leq \mu$ tada $\aleph_0 \cdot \mu = \mu$. Stoga je $\operatorname{card} B_* = \mu$, za $B_* := \bigcup_{n \in \mathbb{N}} B_n$.
Očito je B_* fiksna točka funkcije F, odnosno B_* je nosač podmodela od $\mathfrak{M}$ čija je kardinalnost μ, a sadrži B. $\square$

Dokaz Löwenheim–Skolemova teorema „na dolje”

Löwenheim–Skolemov teorem „na dolje”

Neka je $\mathfrak{M}$ neka σ-struktura, $B \subseteq |\mathfrak{M}|$ i $\operatorname{card} L_\sigma \leq \operatorname{card} |\mathfrak{M}|$.
Tada postoji elementarni podmodel $\mathfrak{N} \prec \mathfrak{M}$ takav da je
$B \subseteq |\mathfrak{N}|$ i $\operatorname{card} |\mathfrak{N}| = \max \{\operatorname{card} B, \operatorname{card} L_\sigma\}$.

Dokaz.
1° $\operatorname{card} B \geq \operatorname{card} L_\sigma \ (\geq \aleph_0)$ Tada $\max\{\operatorname{card} B, \operatorname{card} L_\sigma\} = \operatorname{card} B$,
pa zbog prethodne leme postoji $\mathfrak{M}' \subseteq \mathfrak{M}$ takav da je $B \subseteq |\mathfrak{M}'|$
i $\operatorname{card} |\mathfrak{M}'| = \operatorname{card} B$. Stavimo $A_0 = |\mathfrak{M}'|$. Pretpostavimo
da smo za neki $i \in \mathbb{N}$ definirali skup A_i i definirajmo A_{i+1}.

Za svaku σ-formulu $F(v_0, v_1, \ldots, v_n)$ i
za sve $\vec{a} = (a_1, \ldots, a_n) \in A_i^n$ takve da $\mathfrak{M} \models \exists v_0 F[\vec{a}]$,
izaberimo $a_{F,\vec{a}} \in |\mathfrak{M}|$ takav da $\mathfrak{M} \models F[a_{F,\vec{a}}, \vec{a}]$.
Neka je A_{i+1} nosač podmodela generiranog s
$A_i \cup \{a_{F,\vec{a}} : F(v_0, v_1, \ldots, v_n) \ \sigma\text{-formula}, \ \vec{a} \in A_i^n, \mathfrak{M} \models F[a_{F,\vec{a}}, \vec{a}]\}$.

...

Dokaz Löwenheim–Skolemova teorema „na dolje"

Nastavak dokaza.
Primijetimo:

- $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$
- $\operatorname{card} A_i = \operatorname{card} A_0$ za svaki $i \in \mathbb{N}$
- $A_* := \bigcup_i A_i$ sadrži sve interpretacije konstantskih simbola i zatvoren je na interpretacije svih funkcijskih simbola iz σ, dakle nosač je nekog podmodela $\mathfrak{N}$
- $\operatorname{card} |\mathfrak{N}| = \sum_i \operatorname{card} A_i = \aleph_0 \cdot \operatorname{card} A_0 = \operatorname{card} A_0 = \operatorname{card} B$

Neka je $F(v_0, \dots, v_n)$ σ-formula i $\vec{a} \in A_*^n$ tako da $\mathfrak{M} \models \exists v_0 F[\vec{a}]$. Tada je $\vec{a} \in A_i^n$ za neki $i \in \mathbb{N}$. No tada je $a_{F,\vec{a}} \in A_{i+1}$, i $\mathfrak{M} \models F[a_{F,\vec{a}}, \vec{a}]$. Iz Tarski–Vaughtova kriterija slijedi $\mathfrak{N} \prec \mathfrak{M}$.

2° $\operatorname{card} B < \operatorname{card} L_\sigma$ Neka je $B' \subseteq |\mathfrak{M}|$ takav da je $B \subseteq B'$ i $\operatorname{card} B' = \operatorname{card} L_\sigma$. Iz prvog slučaja slijedi da postoji $\mathfrak{N}' \prec \mathfrak{M}$ takav da je $B' \subseteq |\mathfrak{N}'|$ i $\operatorname{card} |\mathfrak{N}'| = \operatorname{card} L_\sigma = \max\{\operatorname{card} B', \operatorname{card} L_\sigma\}$. Očito vrijedi $B \subseteq |\mathfrak{N}'|$ i $\operatorname{card} |\mathfrak{N}'| = \max\{\operatorname{card} B, \operatorname{card} L_\sigma\}$. $\square$

Löwenheim–Skolemov teorem „na dolje" — primjeri

Primjer

Postoji prebrojivo polje koje je elementarni podmodel polja $\mathbb{R}$.

Primjer (Skolemov paradoks)

Ako za teoriju skupova ZF postoji model,
onda za nju postoji i prebrojiv model.

S druge strane, u ZF se može dokazati
egzistencija neprebrojivih skupova.

Jednostavni i potpuni dijagram

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

Za skup X i signaturu σ, označimo $\sigma_X := \sigma \dot{\cup} \{\overline{a} : a \in X\}$, gdje su $\overline{a}$ novi konstantski simboli i za $a \neq b$ imamo $\overline{a} \neq \overline{b}$.
Za σ-strukturu $\mathfrak{M}$ takvu da je $X \subseteq |\mathfrak{M}|$, s $\mathfrak{M}_X$ označimo σ_X-strukturu s nosačem $|\mathfrak{M}|$, takvu da je $s^{\mathfrak{M}_X} := s^{\mathfrak{M}}$ za sve $s \in \sigma$ i $\overline{a}^{\mathfrak{M}_X} := a$ za sve $a \in X$.

Definicija

Jednostavni dijagram *σ-strukture $\mathfrak{M}$ je skup $\sigma_{\mathfrak{M}}$-rečenicā*
$\Delta(\mathfrak{M}) = \{G(\overline{a_1}, \ldots, \overline{a_n}) : G(v_1, \ldots, v_n)$ *otvorena σ-formula,*
$a_1, \ldots, a_n \in |\mathfrak{M}|$ *i* $\mathfrak{M} \models G[a_1, \ldots, a_n]\}$.
Potpuni dijagram *strukture $\mathfrak{M}$ je* $\mathcal{D}(\mathfrak{M}) = \{F(\overline{a_1}, \ldots, \overline{a_n}) :$ $F(v_1, \ldots, v_n)$ *σ-formula,* $a_1, \ldots, a_n \in |\mathfrak{M}|$ *i* $\mathfrak{M} \models F[a_1, \ldots, a_n]\}$.

Lema o dijagramu

Lema

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ normalne σ-strukture.
Tada se $\mathfrak{M}$ može smjestiti / elementarno smjestiti u $\mathfrak{N}$ ako i samo ako postoji $\sigma_{\mathfrak{M}}$-ekspanzija od $\mathfrak{N}$ koja je model za jednostavni / potpuni dijagram $\Delta(\mathfrak{M})$.

Dokaz.

$\boxed{\Rightarrow}$ Postoji podmodel $\mathfrak{N}' \subseteq \mathfrak{N}$ takav da je $\mathfrak{M} \simeq \mathfrak{N}'$.
Neka je f izomorfizam $\mathfrak{M}$ i $\mathfrak{N}'$. Neka je $\mathfrak{N}''$ $\sigma_{\mathfrak{M}}$-ekspanzija od $\mathfrak{N}$ takva da je $\overline{a}^{\mathfrak{N}''} = f(a)$. Dokažimo da je $\mathfrak{N}''$ model za $\Delta(\mathfrak{M})$.

Neka je $F(\overline{a_1}, \ldots, \overline{a_n}) \in \Delta(\mathfrak{M})$. Tada je $\mathfrak{M} \models F[a_1, \ldots, a_n]$.
Kako je f izomorfizam $\mathfrak{M}$ i $\mathfrak{N}'$, slijedi $\mathfrak{N}' \models F[f(a_1), \ldots, f(a_n)]$.
Kako je F otvorena formula i $\mathfrak{N}' \subseteq \mathfrak{N}$, imamo
$\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$. Očito slijedi $\mathfrak{N}'' \models F(\overline{a_1}, \ldots, \overline{a_n})$. $\cdots$

Lema o dijagramu

Nastavak dokaza.

$\boxed{\Leftarrow}$ Neka je $\sigma_{\mathfrak{M}}$-ekspanzija $\mathfrak{N}'$ strukture $\mathfrak{N}$ model za jednostavni dijagram $\Delta(\mathfrak{M})$. Definiramo $g : |\mathfrak{M}| \to |\mathfrak{N}|$ s $g(a) := \overline{a}^{\mathfrak{N}'}$. Dokažimo da je g smještenje $\mathfrak{M}$ u $\mathfrak{N}$.

Neka su $a, b \in |\mathfrak{M}|$, $a \neq b$. Tada $\mathfrak{N}' \models \Delta(\mathfrak{M}) \ni (\overline{a} \neq \overline{b})$ znači $\overline{a}^{\mathfrak{N}'} \neq \overline{b}^{\mathfrak{N}'}$, odnosno $g(a) \neq g(b)$. Dakle g je injekcija.

Dokažimo da je g jaki homomorfizam. Neka je $c \in \sigma$ proizvoljni konstantski simbol, i $a := c^{\mathfrak{M}}$. Tada $g(c^{\mathfrak{M}}) = g(a) = \overline{a}^{\mathfrak{N}'} = c^{\mathfrak{N}'}$: zadnja jednakost slijedi iz $\mathfrak{N}' \models \Delta(\mathfrak{M}) \ni (\overline{a} = c)$.
No, $\mathfrak{N}'$ je ekspanzija σ-strukture $\mathfrak{N}$, pa je po definiciji $c^{\mathfrak{N}} = c^{\mathfrak{N}'}$.
Time smo dokazali $g(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$.
Tvrdnja se slično dokazuje za funkcijske i relacijske simbole iz σ.

Tvrdnja s elementarnim smještenjem odnosno potpunim dijagramom dokazuje se slično (raspišite!). $\square$

Metoda dijagrama

Konstrukcija (elementarnog) proširenja zadane strukture pomoću prethodne leme zove se **metoda dijagrama**.

Propozicija

Neka je $\mathfrak{M}$ neka beskonačna normalna σ-struktura. Tada postoji σ-struktura $\mathfrak{N}$ takva da je $\mathfrak{M} \neq \mathfrak{N}$ i $\mathfrak{M} \prec \mathfrak{N}$.

Dokaz.

Neka je c novi konstantski simbol (izvan $\sigma_{\mathfrak{M}}$). Neka je $S := \{c \neq \overline{a} : a \in |\mathfrak{M}|\}$, i $S' \subseteq \mathcal{D}(\mathfrak{M}) \cup S$ konačan. Kako je po pretpostavci $|\mathfrak{M}|$ beskonačan, postoji $a_0 \in |\mathfrak{M}|$ takav da se $\overline{a_0}$ ne pojavljuje ni u jednoj formuli iz S'. Neka je $\sigma' := \sigma_{\mathfrak{M}} \cup \{c\}$ i $\mathfrak{M}'$ σ'-ekspanzija od $\mathfrak{M}_{|\mathfrak{M}|}$ takva da je $c^{\mathfrak{M}'} := a_0$. Očito je $\mathfrak{M}' \models S'$. Po teoremu kompaktnosti postoji model $\mathfrak{N}'$ za $\mathcal{D}(\mathfrak{M}) \cup S$.

Zbog $\mathfrak{N}' \models \mathcal{D}(\mathfrak{M})$, po lemi o dijagramu je $\mathfrak{M}$ moguće elementarno smjestiti u σ-redukciju $\mathfrak{N}$ od $\mathfrak{N}'$. Bez smanjenja općenitosti strukturu $\mathfrak{N}$ možemo promatrati kao elementarno proširenje od $\mathfrak{M}$. Iz $\mathfrak{N}' \models S$ slijedi $c^{\mathfrak{N}'} \in |\mathfrak{N}| \setminus |\mathfrak{M}|$, pa je $|\mathfrak{M}| \neq |\mathfrak{N}|$. $\square$

Dokaz Löwenheim–Skolemova teorema „na gore”

Löwenheim–Skolemov teorem „na gore” [pojačana verzija]

Neka je $\mathfrak{M}$ beskonačna normalna σ-struktura i λ kardinalni broj takav da je $\lambda \geq \max\{\text{card}\,|\mathfrak{M}|, \text{card}\,L_\sigma\}$.

Tada postoji σ-struktura $\mathfrak{N}$ za koju vrijedi $\mathfrak{M} \prec \mathfrak{N}$ i $\text{card}\,|\mathfrak{N}| = \lambda$.

Dokaz.

Najprije dokazujemo da postoji σ-struktura $\mathfrak{M}'$ takva da je $\mathfrak{M} \prec \mathfrak{M}'$ i $\text{card}\,|\mathfrak{M}'| \geq \lambda$. Za svaki ordinalni broj $i < \lambda$ uvodimo novi konstantski simbol $c_i \notin \sigma$ i definiramo skup formula $S = \mathcal{D}(\mathfrak{M}) \cup \{c_i \neq c_j : i < j < \lambda\}$. Slično kao u dokazu prethodne propozicije, svaki konačan podskup od S je ispunjiv. Iz teorema kompaktnosti slijedi da postoji model $\mathfrak{N}'$ za S.

Označimo sa $\mathfrak{M}'$ pripadnu σ-redukciju od $\mathfrak{N}'$. Kako je $\mathfrak{N}'$ model za $\mathcal{D}(\mathfrak{M})$, po lemi o dijagramu $\mathfrak{M}$ možemo smjestiti u $\mathfrak{M}'$. Zato BSOMP $\mathfrak{M} \prec \mathfrak{M}'$. Očito $\text{card}\,|\mathfrak{M}'| = \text{card}\,|\mathfrak{N}'| \geq \lambda$. $\cdots$

Dokaz Löwenheim–Skolemova teorema „na gore"

Nastavak dokaza.

Dokažimo sada tvrdnju teorema. Neka je $\mathfrak{M}'$ elementarno proširenje od $\mathfrak{M}$ takvo da je $\operatorname{card}|\mathfrak{M}'| \geq \lambda$.
Neka je $A \subseteq |\mathfrak{M}'|$ takav da je $|\mathfrak{M}| \subseteq A$ i $\operatorname{card} A = \lambda$.
(Dokažite da takav A postoji!)

Po Löwenheim–Skolemovu teoremu „na dolje",
postoji σ-struktura $\mathfrak{N}$ takva da je $A \subseteq |\mathfrak{N}|$, $\mathfrak{N} \prec \mathfrak{M}'$ i $\operatorname{card}|\mathfrak{N}| = \lambda$.
Sada iz $\mathfrak{M} \prec \mathfrak{M}'$, $\mathfrak{N} \prec \mathfrak{M}'$ i $\mathfrak{M} \subseteq \mathfrak{N}$ slijedi $\mathfrak{M} \prec \mathfrak{N}$. $\square$

Napomena

Ubuduće smatramo da su **sve strukture normalne**.

Kategorične teorije

U nastavku ćemo proizvoljan skup σ-rečenica zvati **teorijom**.

Definicija

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

Iz Löwenheim–Skolemova teorema „na gore” slijedi da niti jedna ispunjiva teorija nije kategorična. Zato promatramo slabiji pojam.

Definicija

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

Primjer

Teorija gustih obostrano neograničenih linearno uređenih skupova je $\aleph_0$-kategorična. (Dokaz: uređajna karakterizacija skupa $\mathbb{Q}$)

Potpune teorije

Za signaturu σ, σ-teorija T je **potpuna** ako
za svaku σ-rečenicu F vrijedi $T \models F$ ili $T \models \neg F$.

Lema

Teorija T je potpuna ako i samo ako su svi modeli od T elementarno ekvivalentni.

Primjer

- teorija grupa nije potpuna: $\mathbb{Z}_2 \not\equiv \mathbb{Z}_3$
- teorija polja karakteristike nula nije potpuna: $\mathbb{C} \not\equiv \mathbb{R}$ ($\mathbb{C}$ je algebarski zatvoreno, a $\mathbb{R}$ nije)
- teorija algebarski zatvorenih polja nije potpuna: $\mathbb{C} \not\equiv \overline{\mathbb{Z}_2}$ (različite su karakteristike)
- teorija algebarski zatvorenih polja karakteristike nula jest potpuna („dokaz” kasnije)

Łoś–Vaughtov test potpunosti — lema

Lema

Neka je $\mathfrak{M}$ beskonačna struktura i λ beskonačni kardinalni broj. Tada postoji $\mathfrak{N}$ takva da je $\mathfrak{M} \equiv \mathfrak{N}$ i $\operatorname{card} |\mathfrak{N}| = \lambda$.

Dokaz.

Kako je $\mathfrak{M}$ beskonačan model za skup rečenicā
$Th(\mathfrak{M}) := \{F : F \text{ je rečenica i } \mathfrak{M} \models F\}$,
po Löwenheim–Skolemovu teoremu „na gore”
postoji model $\mathfrak{N}$ za $Th(\mathfrak{M})$ kardinalnosti nosača λ.
Dakle, $\mathfrak{N} \models Th(\mathfrak{M})$, odnosno $Th(\mathfrak{M}) \subseteq Th(\mathfrak{N})$.

Za dokaz obratne inkluzije, neka je F rečenica takva da $\mathfrak{N} \models F$,
i pretpostavimo $\mathfrak{M} \not\models F$. Tada $\mathfrak{M} \models \neg F$,
odnosno $\neg F \in Th(\mathfrak{M}) \subseteq Th(\mathfrak{N})$, pa $\mathfrak{N} \models \neg F$,
što je u kontradikciji s pretpostavkom $\mathfrak{N} \models F$. $\square$

Łoś–Vaughtov test potpunosti

Teorem (Łoś–Vaught)

Neka je T λ-kategorična teorija za neki beskonačni λ i neka je svaki model od T beskonačan. Tada je T potpuna teorija.

Dokaz.

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ proizvoljni (moraju biti beskonačni) modeli od T. Po prethodnoj lemi, postoje modeli $\mathfrak{M}'$ i $\mathfrak{N}'$ kardinalnosti nosača λ takvi da je $\mathfrak{M} \equiv \mathfrak{M}'$ i $\mathfrak{N} \equiv \mathfrak{N}'$. Zbog λ-kategoričnosti je $\mathfrak{M}' \simeq \mathfrak{N}'$, pa stoga i $\mathfrak{M}' \equiv \mathfrak{N}'$. Jer je $\equiv$ ekvivalencija, imamo $\mathfrak{M} \equiv \mathfrak{N}$. Time smo dokazali da su svaka dva modela od T elementarno ekvivalentna, pa je T potpuna teorija. $\square$

Primjer

Primjenom Łoś–Vaughtova testa pokazuje se da je teorija gustih linearnih uređaja bez krajnjih točaka potpuna.

Ograničenost primjene Łoś–Vaughtova testa

Postoje potpune teorije koje imaju samo beskonačne modele, ali nisu λ-kategorične ni za jedan beskonačni kardinalni broj λ.

Nadalje, vrijedi sljedeći teorem, koji nećemo dokazivati:

Teorem (Morley)

Neka je T potpuna teorija koja je λ-kategorična za neki neprebrojivi kardinalni broj λ, te nema konačnih modela. Tada je T μ-kategorična za svaki neprebrojivi kardinalni broj μ.

Primjena Łoś–Vaughtova testa: algebarski zatvorena polja

S ACF_p označavamo teoriju algebarski zatvorenih polja karakteristike p, gdje je $p \in \mathbb{P} \cup \{0\}$.
Dokazat ćemo da je ACF_p potpuna za svaki p. Iz toga će slijediti verzija *Lefschetzova principa* („ono što je istinito za $\mathbb{C}$, istinito je za svako algebarski zatvoreno polje karakteristike 0").
Signatura teorije polja uz $=$ sadrži binarne funkcijske simbole $+$ i $\cdot$ i dva konstantska simbola 0 i 1. Teorija algebarski zatvorenih polja *ACF* je skup koji sadrži aksiome polja i rečenice (za sve $n \in \mathbb{N}_+$)
$\forall a_0 \cdots \forall a_{n-1} \forall a_n \exists x \, (a_n \neq 0 \to a_n x^n + \cdots + a_1 x + a_0 = 0)$.

Lema

Svako algebarski zatvoreno polje K je beskonačno.

Dokaz.

Pretpostavimo suprotno, $K = \{a_1, \ldots, a_n\}$ za $n \geq 1$.
Promotrimo polinom $f(x) = (x - a_1) \cdots (x - a_n) + 1 \in K[x]$.
Kako je K algebarski zatvoreno i $\partial f \geq 1$, postoji $\alpha \in K$ takav da je $f(\alpha) = 0$. No $\alpha \neq a_i$ za svaki i jer $f(a_i) = 1 \neq 0$. $\square$

Primjena Łoś–Vaughtova testa: algebarski zatvorena polja

Za $p \in \mathbb{P}$, označimo s F_p formulu $\overline{p} = \overbrace{1 + \cdots + 1}^{p \text{ puta}} = 0$.
Označimo $ACF_p := ACF \cup \{F_p\}$; $ACF_0 := ACF \cup \{\neg F_p : p \in \mathbb{P}\}$.

Teorem (Steiniz)

Svaka teorija ACF_p je λ-kategorična za svaki neprebrojivi λ.

Skica dokaza.

Neka je K polje. Za $X \subseteq K$ kažemo da je algebarski nezavisan ako za svaki polinom $q \in K[X_1, \ldots, X_n]$ i za sve međusobno različite $a_1, \ldots, a_n \in X$ iz $q(a_1, \ldots, a_n) = 0$ slijedi $q = 0$ (nulpolinom). Transcendentna baza polja je svaki maksimalan algebarski nezavisan podskup. Stupanj transcendentnosti polja je kardinalnost proizvoljne transcendentne baze. Za dokaz je ključno da su dva algebarski zatvorena polja su izomorfna ako i samo ako su iste karakteristike i imaju isti stupanj transcendentnosti. $\square$

Prethodna lema i Steinizov teorem
povlače potpunost po Łoś–Vaughtovu testu.

Lefschetzov princip

Propozicija

Neka je F rečenica teorije polja. Sljedeće tvrdnje su ekvivalentne:

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

b) *za svako algebarski zatvoreno K karakteristike nula je $K \models F$*

c) *za neko algebarski zatvoreno K karakteristike nula je $K \models F$*

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

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

Lefschetzov princip

Dokaz.

Očito vrijedi $(b) \Rightarrow (a) \Rightarrow (c)$, a zbog potpunosti teorije ACF_0 vrijedi i $(c) \Rightarrow (a)$. Također, očito $(e) \Rightarrow (d)$. Preostaje dokazati npr. $(b) \Rightarrow (e)$ i $(d) \Rightarrow (c)$ (kontrapozicijom $\neg(c) \Rightarrow \neg(d)$).

$\boxed{(b) \Rightarrow (e)}$ Iz teorema kompaktnosti slijedi da postoje $p_1, \ldots, p_n \in \mathbb{P}$ takvi da $ACF \cup \{\neg F_{p_1}, \ldots, \neg F_{p_n}\} \models F$.
Označimo $m := \max\{p_1, \ldots, p_n\}$ i $G := (\neg F_{p_1} \wedge \cdots \wedge \neg F_{p_n})$.
Tada za svako algebarski zatvoreno K karakteristike $p > m \geq p_i$ očito vrijedi $K \models G$, pa i $K \models F$.

$\boxed{\neg(c) \Rightarrow \neg(d)}$ Pretpostavimo da ni u kojem modelu od ACF_0 ne vrijedi F, dakle $ACF_0 \models \neg F$. Po teoremu kompaktnosti postoje $p_1, \ldots, p_n \in \mathbb{P}$ takvi da $ACF \cup \{\neg F_{p_1}, \ldots, \neg F_{p_n}\} \models \neg F$.
Tada (uz oznake kao gore) za svaki $p > m$ vrijedi $ACF_p \models G$,
pa u svakom modelu od ACF_p vrijedi $\neg F$,
odnosno ne postoji takav u kojem vrijedi F. $\square$

Axov teorem

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

Teorem (Ax)

Za $n \in \mathbb{N}_+$ svaka polinomna injekcija $f : \mathbb{C}^n \to \mathbb{C}^n$ je i surjekcija.

Dokaz.

Za sve $n, d \in \mathbb{N}$ neka je $\Phi_{n,d}$ rečenica takva da za svako polje K, $K \models \Phi_{n,d}$ znači da je svaka polinomna injekcija $g : K^n \to K^n$ s koordinatnim funkcijama stupnja najviše d ujedno i surjekcija.

Konkretno, $\Phi_{n,d}$ je univerzalno zatvorenje formule

$$\forall \vec{x} \forall \vec{y} \Big(\bigwedge_{k=1}^{n} p_k(\vec{x}) = p_k(\vec{y}) \to \bigwedge_{k=1}^{n} x_k = y_k \Big) \to \\ \to \forall \vec{y} \, \exists \, \vec{x} \bigwedge_{k=1}^{n} p_k(\vec{x}) = y_k,$$

gdje je $\vec{x}$ pokrata za n varijabli $x_1, \ldots, x_n$,
a $p_k(\vec{x})$ pokrata za term $\sum_{\vec{e} \in [1..d]^n} a_{k,\vec{e}} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$. $\quad \ldots$

Axov teorem

Nastavak dokaza.

Neka je K konačno polje, i $\overline{K}$ njegovo algebarsko zatvorenje. Iz algebre je poznato $\overline{K} = \bigcup_i K_i$, gdje je $(K_i)_i$ rastući niz konačnih polja (dobivenih rekurzivnim dodavanjem nultočaka polinoma).

Neka je $f : \overline{K}^n \to \overline{K}^n$ proizvoljna polinomna injekcija i d najveći stupanj koordinatnog polinoma od f. Za $\vec{y} = (y_1, \ldots, y_n) \in \overline{K}^n$ postoje $i_1, \ldots, i_n \in \mathbb{N}$ takvi da je $y_t \in K_{i_t}$ za sve t.

Jer je $(K_i)_i$ rastući, za $j := \max\{i_1, \ldots, i_n\}$ vrijedi $y_1, \ldots, y_n \in K_j$. Kako je $f|_{K_j^n}$ injekcija i K_j^n konačan, $f|_{K_j^n}$ je i surjekcija, pa za zadani $\vec{y}$ postoji $\vec{x} \in K_j^n \subseteq \overline{K}^n$ takav da je $f(\vec{x}) = \vec{y}$. Slijedi da za svaki $m \in \mathbb{N}$ postoji prosti broj $p > m$ i algebarski zatvoreno polje $\overline{K}$ karakteristike p (konkretno, recimo $\overline{\mathbb{Z}_p}$) u kojem vrijedi $\Phi_{n,d}$.

Iz Lefschetzova principa ($(d) \Rightarrow (a)$) slijedi $\mathbb{C} \models \Phi_{n,d}$.
Zbog proizvoljnosti n i d slijedi tvrdnja teorema. $\square$

Robinsonov teorem konzistentnosti

Teorija T (skup rečenica) je **konzistentna** ako postoji model za T.

U sljedeće dvije leme,
s $\mathfrak{M}^-$ označavamo σ-redukciju σ'-strukture $\mathfrak{M}$ (za $\sigma \subseteq \sigma'$).

Lema

Neka su σ i σ' signature takve da je $\sigma \subseteq \sigma'$.
Neka je T potpuna σ-teorija, a $T' \supseteq T$ konzistentna σ'-teorija.
Tada za svaki $\mathfrak{M} \models T$ postoji $\mathfrak{M}' \models T'$ takav da je $\mathfrak{M} \prec \mathfrak{M}'^-$.

Robinsonov teorem konzistentnosti

Dokaz prve leme.

Prema lemi o dijagramu, dovoljno je dokazati da je $T' \cup \mathcal{D}(\mathfrak{M})$ konzistentna. Pretpostavimo suprotno. Iz teorema kompaktnosti slijedi da postoji konačan $S \subseteq T' \cup \mathcal{D}(\mathfrak{M})$ koji nema model.

Potpuni dijagram je zatvoren na konjunkciju, pa postoji $F(\overline{a_1}, \ldots, \overline{a_n}) \in \mathcal{D}(\mathfrak{M})$ koja je ekvivalentna skupu formula $S \cap \mathcal{D}(\mathfrak{M})$. Kako S nema model, vrijedi $T' \models \neg F(\overline{a_1}, \ldots, \overline{a_n})$, a onda i $T' \models G := \forall v_1 \cdots \forall v_n \neg F(v_1, \ldots, v_n)$, što je σ-rečenica.

Kad bi $T \models \neg G$, tada bi zbog $\sigma \subseteq \sigma'$ i $T \subseteq T'$ vrijedilo $T' \models \neg G$, što je kontradikcija s pretpostavkom da je T' konzistentna.

Dakle, $T \not\models \neg G$. Zbog potpunosti od T je $T \models G$. 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 $\mathfrak{M} \models F[a_1, \ldots, a_n]$. $\square$

Robinsonov teorem konzistentnosti

Lema

Neka su σ i σ' signature takve da je $\sigma \subseteq \sigma'$.
Neka je T potpuna σ-teorija, a $T' \supseteq T$ konzistentna σ'-teorija.
Neka je $\mathfrak{M}$ model za T i $\mathfrak{N}_1$ model za T' takav da je $\mathfrak{N}_1^- \prec \mathfrak{M}$.
Tada postoji model $\mathfrak{N}_2$ za T' takav da je $\mathfrak{N}_1 \prec \mathfrak{N}_2$ i $\mathfrak{M} \prec \mathfrak{N}_2^-$.

Dokaz.

Dovoljno je dokazati da je $T' := \mathcal{D}(\mathfrak{M}) \cup \mathcal{D}(\mathfrak{N}_1)$ konzistentna.
Pretpostavimo suprotno. Primjenom teorema kompaktnosti (slično kao u prethodnoj lemi) slijedi da postoji σ-formula F, $a_1, \dots, a_n \in |\mathfrak{N}_1|$ i $a_{n+1}, \dots, a_{n+p} \in |\mathfrak{M}| \setminus |\mathfrak{N}_1|$ takvi da je $F(\overline{a_1}, \dots, \overline{a_{n+p}}) \in \mathcal{D}(\mathfrak{M})$ i $\mathcal{D}(\mathfrak{N}_1) \models \neg F(\overline{a_1}, \dots, \overline{a_{n+p}})$.
Tada $\mathcal{D}(\mathfrak{N}_1) \models \forall v_1 \cdots \forall v_p \neg F(\overline{a_1}, \dots, \overline{a_n}, v_1, \dots, v_p)$, a onda i $\mathfrak{N}_1 \models \forall v_1 \cdots \forall v_p \neg F[a_1, \dots, a_n]$. No $\mathfrak{M} \models \exists v_1 \cdots \exists v_p F[a_1, \dots, a_n]$, pa je dobivena kontradikcija s pretpostavkom $\mathfrak{N}_1^- \prec \mathfrak{M}$. $\square$

Robinsonov teorem konzistentnosti

Teorem (Robinson)

Neka je T potpuna σ-teorija, te neka su σ_1 i σ_2 signature takve da je $\sigma = \sigma_1 \cap \sigma_2$. Neka su T_1 konzistentna σ_1-teorija i T_2 konzistentna σ_2-teorija takve da je $T \subseteq T_1 \cap T_2$. Tada je teorija $T_1 \cup T_2$ konzistentna.

Dokaz.

Neka je $\mathfrak{N}_1$ model teorije T_1. Kako je $T \subseteq T_1$, očito vrijedi $\mathfrak{N}_1^- \models T$. Prema prvoj lemi, postoji model $\mathfrak{N}_1'$ teorije T_2 takav da je $\mathfrak{N}_1^- \prec \mathfrak{N}_1'^-$ (uzmemo $\mathfrak{M} := \mathfrak{N}_1^-$). Kako je $\mathfrak{N}_1' \models T_2$ i $T \subseteq T_2$, vrijedi $\mathfrak{N}_1'^- \models T$. Primjenom druge leme (za $\mathfrak{M} := \mathfrak{N}_1'^-$) slijedi da postoji model $\mathfrak{N}_2$ teorije T_1 takav da je $\mathfrak{N}_1 \prec \mathfrak{N}_2$ i $\mathfrak{N}_1'^- \prec \mathfrak{N}_2^-$.

Kako je $T \subseteq T_1$, očito $\mathfrak{N}_2^- \models T$. Sada primjenom druge leme (uz $\mathfrak{M} := \mathfrak{N}_2^-$) slijedi da postoji model $\mathfrak{N}_2'$ teorije T_2 takav da je $\mathfrak{N}_1' \prec \mathfrak{N}_2'$ i $\mathfrak{N}_2^- \prec \mathfrak{N}_2'^-$. $\cdots$

Robinsonov teorem konzistentnosti

Nastavak dokaza.

Uzastopnom primjenom druge leme dobivamo niz $(\mathfrak{N}_n)$ modela za T_1 i niz $(\mathfrak{N}'_n)$ modela za T_2 takvih da za svaki $n \in \mathbb{N}$ vrijedi $\mathfrak{N}_n \prec \mathfrak{N}_{n+1}$, $\mathfrak{N}'_n \prec \mathfrak{N}'_{n+1}$, $\mathfrak{N}_n^- \prec \mathfrak{N}_n'^-$ i $\mathfrak{N}_n'^- \prec \mathfrak{N}_{n+1}^-$.

Neka su $\mathfrak{N}$ i $\mathfrak{N}'$ unije tih elementarnih lanaca.
Iz teorema o uniji lanaca imamo posebno $\mathfrak{N}_1 \prec \mathfrak{N}$ i $\mathfrak{N}'_1 \prec \mathfrak{N}'$.

Kako je $\mathfrak{N}_1$ model za T_1, također je i $\mathfrak{N}$ model za T_1.
Iz analognog razloga $\mathfrak{N}'$ je model za T_2. Očito je

$$\mathfrak{N}^- = \bigcup_{n \in \mathbb{N}} \mathfrak{N}_n^- \prec \bigcup_{n \in \mathbb{N}} \mathfrak{N}_n'^- = \mathfrak{N}'^-.$$

Iz toga slijedi da je dobro definirana $(\sigma_1 \cup \sigma_2)$-struktura $\mathfrak{N} \cup \mathfrak{N}'$ koja je očito model teorije $T_1 \cup T_2$.

Time smo dokazali da je teorija $T_1 \cup T_2$ konzistentna. $\square$

Craigova interpolacijska lema

Teorem (Craig)

*Neka su F i G rečenice za koje vrijedi $F \Rightarrow G$. Tada postoji rečenica H (**interpolant** za F i G) takva da vrijedi $F \Rightarrow H \Rightarrow G$ i svaki nelogički simbol (osim možda $=$) iz H je i u F i G.*

Dokaz.

Pretpostavimo suprotno. Želimo konstruirati potpunu teoriju T takvu da su $T \cup \{F\}$ i $T \cup \{\neg G\}$ konzistentne. Tada Robinsonov teorem kaže da je $T \cup \{F, \neg G\}$ konzistentna, što je nemoguće jer $F \Rightarrow G$. Neka je σ_F (σ_G) skup svih nelogičkih simbola iz F (G), te $\sigma := (\sigma_F \cap \sigma_G) \cup \{=\}$ (konačan). Neka je $\{A_n : n \in \mathbb{N}\}$ skup svih σ-rečenica, gdje fiksiramo $A_0 := \forall v_0(v_0 = v_0 \vee v_0 \neq v_0)$.

Konstruirat ćemo niz σ-rečenica $(B_n)_n$ takvih da za sve n:

(i) $B_{n+1} \Rightarrow B_n$;

(ii) $B_n \Rightarrow A_n$ ili $B_n \Rightarrow \neg A_n$;

(iii) ne postoji interpolant za $F \wedge B_n$ i $G \wedge B_n$ $\cdots$

Craigova interpolacijska lema

Nastavak dokaza.

Stavimo $B_0 := A_0$ — lako se vidi da ispunjava (ii) i (iii).

Neka je za neki $n \in \mathbb{N}$ definirano B_n. Tvrdimo da

1. ne postoji interpolant za $F \wedge B_n \wedge A_{n+1}$ i $G \wedge B_n \wedge A_{n+1}$, ili
2. ne postoji interpolant za $F \wedge B_n \wedge \neg A_{n+1}$ i $G \wedge B_n \wedge \neg A_{n+1}$.

U suprotnom bi postojale σ-rečenice H_1 i H_2 takve da

$$F \wedge B_n \wedge \quad A_{n+1} \Rightarrow H_1 \Rightarrow G \wedge B_n \wedge \quad A_{n+1} \text{ i}$$

$$F \wedge B_n \wedge \neg A_{n+1} \Rightarrow H_2 \Rightarrow G \wedge B_n \wedge \neg A_{n+1}, \text{ a stoga i}$$

$$F \wedge B_n \Leftrightarrow (F \wedge B_n \wedge A_{n+1}) \vee (F \wedge B_n \wedge \neg A_{n+1}) \Rightarrow H_1 \vee H_2 \Rightarrow$$
$$\Rightarrow (G \wedge B_n \wedge A_{n+1}) \vee (G \wedge B_n \wedge \neg A_{n+1}) \Leftrightarrow G \wedge B_n,$$

što je nemoguće zbog pretpostavke indukcije (za B_n vrijedi (iii)).

Sada definiramo B_{n+1} kao:

- $B_n \wedge A_{n+1}$, ako vrijedi tvrdnja 1;
- $B_n \wedge \neg A_{n+1}$, inače (tada mora vrijediti tvrdnja 2).

Lako se vidi da B_{n+1} zadovoljava svojstva (i)–(iii). $\cdots$

Craigova interpolacijska lema

Nastavak dokaza.

Neka je $T = \{B_n : n \in \mathbb{N}\}$. Treba dokazati da su $T \cup \{F\}$ i $T \cup \{\neg G\}$ konzistentne i da je T potpuna.

Najprije dokazujemo da je za svaki $n \in \mathbb{N}$ formula $F \wedge B_n$ ispunjiva.
Uočimo da je F ispunjiva (inače bi $\neg A_0$ bio interpolant za F i G).
Kako je $B_0 = A_0$ valjana, očito je $F \wedge B_0$ ispunjiva.

Neka je $n \in \mathbb{N}$: tada za $F \wedge B_{n+1}$ i $G \wedge B_{n+1}$ ne postoji interpolant.
Slično kao gore iz toga zaključujemo da je $F \wedge B_{n+1}$ ispunjiva.
Po teoremu kompaktnosti, dovoljno je dokazati da je svaki konačni podskup od $T \cup \{F\}$ konzistentan.

Neka je $\{B_{i_1}, \dots, B_{i_n}\} \subseteq T$, pri čemu je $i_1 < \cdots < i_n$.
Neka je $\mathfrak{M}$ model za $F \wedge B_{i_n}$. Iz (i) slijedi $\mathfrak{M} \models B_{i_1} \wedge \cdots \wedge B_{i_n}$.
Analogno (raspišite!) se dokazuje da je $T \cup \{\neg G\}$ konzistentna.

Preostaje dokazati da je T potpuna.
Neka je A proizvoljna σ-rečenica. Tada je $A = A_n$ za neki n.
Prema (*ii*), $B_n \Rightarrow A$ ili $B_n \Rightarrow \neg A$, pa i $T \models A$ ili $T \models \neg A$. $\square$

Implicitna definabilnost

Neka je σ signatura i $P \neq P'$ n-mjesni relacijski simboli izvan σ. Neka je $\sigma' := \sigma \cup \{P\}$ te G σ'-formula. S $G_{P'/P}$ označavamo formulu dobivenu iz G zamjenom svakog pojavljivanja P s P'.

Analogno za teorije, definiramo $T_{P'/P} := \{G_{P'/P} : G \in T\}$.

Lema

Ako je F σ-formula takva da $F \Rightarrow G$, onda i $F \Rightarrow G_{P'/P}$.

Definicija

Neka je T σ'-teorija. Kažemo da je n-mjesni relacijski simbol P **implicitno definabilan** *u T ako za svaki n-mjesni relacijski simbol $P' \notin \sigma$ vrijedi $T \cup T_{P'/P} \models P(v_1, \ldots, v_n) \leftrightarrow P'(v_1, \ldots, v_n)$.*

Propozicija

Neka je T σ'-teorija. Tada je P implicitno definabilan u T ako i samo ako za svaku σ-strukturu $\mathfrak{M}$ postoji najviše jedna interpretacija od P takva da je σ'-ekspanzija od $\mathfrak{M}$ model za T.

Eksplicitna definabilnost

Definicija

Neka je T σ'-teorija ($\sigma' := \sigma \dot\cup \{P\}$). Kažemo da je relacijski simbol P **eksplicitno definabilan** *u T ako postoji σ-formula $F(v_1, \ldots, v_n)$ takva da $T \models P(v_1, \ldots, v_n) \leftrightarrow F(v_1, \ldots, v_n)$.*

Propozicija (Padoaova metoda)

Neka je T σ'-teorija. Ako je P eksplicitno definabilan u T, onda je P i implicitno definabilan u T.

Primjer

Neka je $\sigma = \{+, =\}$ i R dvomjesni relacijski simbol. Neka je T skup svih $(\sigma \cup \{R\})$-rečenica koje vrijede u strukturi $(\mathbb{Z}, +, <)$. Tvrdimo da R nije eksplicitno definabilan u T. Naime, $(\mathbb{Z}, +, >)$ je također model za T jer je $(\mathbb{Z}, +, <) \simeq (\mathbb{Z}, + >)$ (po $x \mapsto -x$).
To znači da ne postoji jedinstvena interpretacija od R takva da je $(\sigma \cup \{R\})$-ekspanzija od $(\mathbb{Z}, +)$ model za T.
Dakle, R nije implicitno definabilan u T,
a po prethodnoj propoziciji tada nije ni eksplicitno definabilan u T.

Bethov teorem definabilnosti

Teorem (Beth)

Neka je T $(\sigma \dot\cup \{P\})$-teorija, gdje je P relacijski simbol.
Ako je P implicitno definabilan u T,
onda je i eksplicitno definabilan u T.

Dokaz.
Označimo s n mjesnost relacijskog simbola $P \notin \sigma$.
Neka su $c_1, \ldots, c_n \notin \sigma$ različiti konstantski simboli, te $P' \notin \sigma$ n-mjesni relacijski simbol. Kako je P implicitno definabilan, $T \cup T_{P'/P} \models P(v_1 \ldots, v_n) \leftrightarrow P'(v_1, \ldots, v_n)$. Tada je $T \cup \{P(c_1, \ldots, c_n)\} \cup T_{P'/P} \cup \{\neg P'(c_1, \ldots, c_n)\}$ inkonzistentna.

Po teoremu kompaktnosti, postoje konačni $S \subseteq T$ i $S' \subseteq T_{P'/P}$ takvi da je $S \cup \{P(c_1, \ldots, c_n)\} \cup S' \cup \{\neg P'(c_1, \ldots, c_n)\}$ inkonzistentna. Označimo $F := \bigwedge_{A \in S} A$ i $G := \bigwedge_{B \in S'} B$. Tada formula $F \wedge P(c_1, \ldots, c_n) \wedge G \wedge \neg P'(c_1, \ldots, c_n)$ nije ispunjiva, pa vrijedi $F \wedge P(c_1, \ldots, c_n) \Rightarrow G \rightarrow P'(c_1, \ldots, c_n)$. $\cdots$

Bethov teorem definabilnosti

Nastavak dokaza.

Po Craigovoj interpolacijskoj lemi, postoji interpolant H koji je $(\sigma \cup \{c_1, \ldots, c_n\})$-rečenica. Dakle P i P' se ne pojavljuju u H. Kako je $S \subseteq T$ i $F = \bigwedge_{A \in S} A$, očito je $T \models F$. Sada iz $F \wedge P(c_1, \ldots, c_n) \Rightarrow H$ slijedi $T \models P(c_1, \ldots, c_n) \to H$, odnosno (jer je $\{c_1, \ldots, c_n\} \cap \sigma = \emptyset$) $T \models P(v_1, \ldots, v_n) \to H$.

Kako $T_{P'/P} \models G$ i $H \Rightarrow G \to P'(c_1, \ldots, c_n)$, vrijedi $T_{P'/P} \models H \to P'(c_1, \ldots, c_n)$. Zamjenom unatrag P/P' dobijemo $T \models H \to P(c_1, \ldots, c_n)$ i stoga $T \models H' \to P(v_1, \ldots, v_n)$ (gdje je H' dobivena iz H pisanjem v_i umjesto c_i).

Slično se dobije i drugi smjer.

Dakle, P je eksplicitno definabilan u T. $\square$

Produkti σ-struktura

Kartezijev produkt σ-struktura definiramo na prirodni način — ali produkt modela neke teorije ne mora biti model te teorije.

Primjer

Kartezijev produkt familije grupa je grupa. Preciznije, neka je $\{(G_i, \circ_i) : i \in I\}$ familija grupa. Na Kartezijevom produktu $\prod_{i \in I} G_i = \{(f : I \to \bigcup_{i \in I} G_i) :$ za svaki $i \in I$ vrijedi $f(i) \in G_i\}$ definiramo $(f \circ g)(i) := f(i) \circ_i g(i)$. Tada je je $(\prod_{i \in I} G_i, \circ)$ grupa.

Primjer

Kartezijev produkt polja ne mora biti polje. Neka je $\{F_i := (A_i, +_i, \cdot_i, 0_i, 1_i) : i \in I\}$ familija polja. Operacije $+$ i $\cdot$ na $\prod_{i \in I} A_i$ definiramo kao kod grupa, te definiramo $0 : I \to \bigcup_i A_i$ s $0(i) = 0_i$ i $1 : I \to \bigcup_i A_i$ s $1(i) = 1_i$. Uz tako definirane operacije Kartezijev produkt polja općenito nije polje. Na primjer, $\mathbb{R} \times \mathbb{R}$ nije polje, jer su $(0,1), (1,0) \neq 0$, ali $(0,1) \cdot (1,0) = 0$.

Produkti σ-struktura

Primjer

Kartezijev produkt linearno uređenih skupova općenito nije linearno uređen skup. Neka je $\{(A_i, <_i), i \in I\}$ familija linearno uređenih skupova. Neka je $A = \prod_{i \in I} A_i$. Definiramo relaciju $R \subseteq A \times A$ s $f\,R\,g$ ako za sve $i \in I$ vrijedi $f(i) <_i g(i)$. Tada (A, R) općenito nije linearno uređen. Na primjer, u $\mathbb{R} \times \mathbb{R}$ elementi $(0, 1)$ i $(1, 0)$ nisu usporedivi.

No, moguće je definirati relaciju ekvivalencije na Kartezijevom produktu, tako da promatranjem kvocijentnog skupa dobijemo željena svojstva. Kako bismo definirali odgovarajuću relaciju ekvivalencije, potreban nam je pojam filtera.

Filter

Intuicija: filter nad skupom I je skup „dovoljno velikih" podskupova od I. „Dovoljno veliki skupovi" možemo shvatiti kao „komplementi zanemarivih skupova".

Također možemo shvatiti elemente filtera kao „glasove" za formule: formulu smatramo istinitom ako vrijedi na dovoljno velikom skupu.

Definicija

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

(i) *$I \in F$ (ekvivalentno s $F \neq \emptyset$);*

(ii) *ako su $X, Y \in F$, onda je $X \cap Y \in F$ (zatvorenost na konačne presjeke);*

(iii) *ako je $X \in F$ i $X \subseteq Z \subseteq I$, onda je $Z \in F$ (zatvorenost na nadskupove).*

Primjeri filtera

Primjer (Zadatak: interpretirajte navedene filtere glasački!)

- $\{I\}$ je filter nad I (**trivijalni filter**)
- $\mathcal{P}(I)$ je filter nad I (**nepravi filter**)
- za $X \subseteq I$, $F = \{Y \subseteq I : X \subseteq Y\}$ je filter nad I (**filter generiran skupom** X).
  Specijalno, za $x \in X$, $\{S \subseteq I : x \in S\}$ zovemo **glavni filter**.
- **Fréchetov filter**: za beskonačan skup I, skup svih **kofinitnih** podskupova, $F = \{X \subseteq I : X^c \text{ konačan}\}$, je filter
- skup svih okolina dane točke x topološkog prostora $(X, \mathcal{T})$, $\{Y : Y \subseteq X \wedge (\exists U \in \mathcal{T})(x \in U \subseteq Y)\}$, je filter nad X
- za $E \subseteq \mathcal{P}(I)$, $F = \bigcap\{F' : F' \text{ filter nad } I, E \subseteq F'\}$ je filter (**generiran familijom** E). Druga karakterizacija istog filtera je $F = \{X \subseteq I : (\exists Y_1, \dots, Y_n \in E)(Y_1 \cap \dots \cap Y_n \subseteq X)\}$.

Reducirani produkt skupova

Neka je $\{M_i : i \in I\}$ familija skupova i F filter nad I.
Na Kartezijevom produktu

$$\prod_{i\in I} M_i = \left\{ \left(f : I \to \bigcup_{i\in I} M_i\right) : (\forall I \in I)\big(f(i) \in M_i\big) \right\}$$

definiramo binarnu relaciju $\sim$ ovako:

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

Lako je pokazati da je $\sim_F$ relacija ekvivalencije.
S $[f]_F$ označavamo klasu ekvivalencije kojoj pripada f.

Kvocijentni skup $\prod_i \mathfrak{M}_i \big/_{\sim_F}$ skraćeno označavamo $\prod_F M_i$,
i zovemo ga **reducirani produkt familije skupova** $\{M_i : i \in I\}$.

Reducirani produkt σ-struktura

Definicija

Neka je σ signatura i neka je $\{\mathfrak{M}_i : i \in I\}$ familija σ-struktura. Neka je F proizvoljan filter nad I. Definiramo σ-strukturu $\mathfrak{M}$:

- $|\mathfrak{M}| := \prod_F M_i$
- *za svaki relacijski simbol R definiramo $([f_1]_F, \dots, [f_n]_F) \in R^{\mathfrak{M}}$ ako i samo ako je $\{i \in I : (f_1(i), \dots, f_n(i)) \in R^{\mathfrak{M}_i}\} \in F$;*
- *za svaki funkcijski simbol f definiramo $f^{\mathfrak{M}}([f_1]_F, \dots, [f_n]_F) := \left[\left(f^{\mathfrak{M}_i}(f_1(i), \dots, f_n(i))\right)_{i \in I}\right]_F$;*
- *za svaki konstantski simbol c definiramo $c^{\mathfrak{M}} = [(c^{\mathfrak{M}_i})_{i \in I}]_F$.*

Lako se vidi da definicije ne ovise o izboru reprezentanata.

Struktura $\mathfrak{M}$ zove se **reducirani produkt familije σ-struktura** *i označava $\prod_F \mathfrak{M}_i$. Ako je $\mathfrak{M}_i = \mathfrak{M}$ za sve i, reducirani produkt zovemo* **reduciranom potencijom** *od $\mathfrak{M}$ i označavamo $\prod_F \mathfrak{M}$.*

Valuacija na reduciranom produktu

Neka je $\{\mathfrak{M}_i : i \in I\}$ familija σ-struktura i neka je v_i valuacija na $\mathfrak{M}_i$ za svaki $i \in I$. Kažemo da je valuacija v na reduciranom produktu $\mathfrak{M} = \prod_F \mathfrak{M}_i$ **inducirana familijom valuacija** $\{v_i : i \in I\}$ ako za svaku varijablu x vrijedi $v(x) = \big[\big(v_i(x)\big)_{i \in I}\big]_F$.

Lema

Za svaki σ-term t vrijedi $v(t) = \big[\big(v_i(t)\big)_{i \in I}\big]_F$.

Dokaz.

Indukcijom po t. Za varijable tvrdnja vrijedi po definiciji od v. Za konstantske simbole, $v(c) = c^{\mathfrak{M}} = \big[\big(c^{\mathfrak{M}_i}\big)_{i \in I}\big]_F = \big[\big(v_i(c)\big)_{i \in I}\big]_F$.

Neka tvrdnja vrijedi za $t_1, \ldots, t_k$. Tada je $v\big(f(t_1, \ldots, t_k)\big) =$

$$= f^{\mathfrak{M}}\big(v(t_1), \ldots, v(t_k)\big) = f^{\mathfrak{M}}\big([(v_i(t_1))_{i \in I}]_F, \ldots, [(v_i(t_k))_{i \in I}]_F\big)$$

$$= \big[\big(f^{\mathfrak{M}_i}\big(v_i(t_1), \ldots, v_i(t_k)\big)\big)_{i \in I}\big]_F = \big[\big(v_i(f(t_1, \ldots, t_k))\big)_{i \in I}\big]_F.$$

$\square$

Pravi filter i ultrafilter

Definicija

Za filter F nad skupom I kažemo da je **pravi** *ako je*

(iv) $F \neq \mathcal{P}(I)$ *(što je ekvivalentno s $\emptyset \notin F$).*

Pravi filter F nad I zovemo **ultrafilter** *ako za svaki $X \subseteq I$ vrijedi*

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

Za reducirane produkte / potencije skupova i σ-struktura s obzirom na ultrafilter kažemo da su **ultraprodukti** / **ultrapotencije**.

Svaki glavni filter je ultrafilter. [Ostali primjeri su kompliciraniji.]

Propozicija

Filter generiran s $E \subseteq \mathcal{P}(I)$ je pravi ako i samo ako E ima **svojstvo konačnih presjeka**: *$X_1, \ldots, X_n \in E$ povlači $X_1 \cap \cdots \cap X_n \neq \emptyset$.*

Ultrafilter

Propozicija

Neka je I beskonačan skup. Tada vrijedi:

- *skup svih kofinitnih $S \subseteq I$ ima svojstvo konačnih presjeka*
- *ultrafilter U nad I nije glavni ako i samo ako sadrži samo beskonačne skupove, što vrijedi ako i samo ako sadrži sve kofinitne podskupove od I*
- *svaki ultrafilter nad I ima beskonačno mnogo elemenata*

Propozicija

Neka je F pravi filter nad skupom I. Tada je F ultrafilter ako i samo ako je maksimalan (odnosno, ne postoji pravi filter F' nad I takav da je $F \subset F'$), što je ako i samo ako za sve $X, Y \subseteq I$ vrijedi: $X \cup Y \in F$ ako i samo ako $X \in F$ ili $Y \in F$.

Teorem o ultrafilteru

Teorem

Neka je $I \neq \emptyset$ *i* $E \subseteq \mathcal{P}(I)$ *familija sa svojstvom konačnih presjeka. Tada postoji ultrafilter* U *nad* I *koji je nadskup od* E*.*

Dokaz.

Neka je F_0 presjek svih filtera koji sadrže E. Tada je F_0 pravi filter.
Neka je $\mathcal{F}$ familija svih pravih filtera koji sadrže E. Tada je $\mathcal{F} \neq \emptyset$ jer je $F_0 \in \mathcal{F}$. Neka je $\mathcal{L}$ proizvoljni lanac u $(\mathcal{F}, \subseteq)$.
Lako je provjeriti da je $\bigcup \mathcal{L}$ pravi filter koji sadrži F.
Time smo dokazali da svaki lanac u $\mathcal{F}$ ima gornju među.
Iz Zornove leme slijedi da u $\mathcal{F}$ postoji maksimalni element U.
Iz prethodne propozicije slijedi da je U ultrafilter. $\square$

Korolar (Teorem o ultrafilteru)

Svaki pravi filter F *nad* I *može se proširiti do ultrafiltera nad* I*.*

Primjer

Postoji ultrafilter koji proširuje Fréchetov filter. [On nije glavni.]

Prebrojivo nepotpuni ultrafilteri

Definicija

Za ultrafilter U kažemo da je **prebrojivo potpun** *ako je zatvoren na prebrojive presjeke, dakle ako za svaki niz $(X_n)_n$ u U vrijedi $\bigcap_n X_n \in U$. Inače kažemo da je* **prebrojivo nepotpun**.

Primjer

- Ultrafilter U nad $\mathbb{N}$ koji sadrži Fréchetov filter je prebrojivo nepotpun. Naime, $X_n := \mathbb{N} \setminus \{n\} \in U$, ali $\bigcap_{n\in\mathbb{N}} X_n = \emptyset \notin U$.
- Svaki glavni ultrafilter je prebrojivo potpun.
  Štoviše, očito je zatvoren na proizvoljne presjeke.

Propozicija

Neka je $I \neq \emptyset$ i U ultrafilter nad I. Tada je U prebrojivo nepotpun ako i samo ako postoji padajući niz $(Y_n)_n$ u U takav da je $I = Y_0$ i $\bigcap_n Y_n = \emptyset$, ako i samo ako postoji niz $(Z_n)_n$ u parovima disjunktnih podskupova od I takav da vrijedi $\bigcup_n Z_n = I$, te $Z_n \notin U$ za sve n.

Łośov teorem

Teorem (Łoś)

Neka je $\{\mathfrak{M}_i : i \in I\}$ *familija* σ*-struktura,* U *ultrafilter nad* I *i* v *valuacija na* $\prod_U \mathfrak{M}_i$ *inducirana familijom* $\{v_i : i \in I\}$*.*
Neka je F σ*-formula.*
Tada je $\prod_U \mathfrak{M}_i \models_v F$ *ako i samo ako je* $\{i : \mathfrak{M}_i \models_{v_i} F\} \in U$*.*

Dokaz.

Teorem dokazujemo indukcijom po složenosti formule F.
Neka je F atomarna formula oblika $\boxed{F = R(t_1, \ldots, t_k)}$. Tada:

$$\begin{aligned}\prod\nolimits_U \mathfrak{M}_i \models_v R(t_1, \ldots, t_k) &\iff \big(v(t_1), \ldots, v(t_k)\big) \in R^{\mathfrak{M}} \iff \\ &\iff \big([(v_i(t_1))_{i\in I}]_U, \ldots, [(v_i(t_k))_{i\in I}]_U\big) \in R^{\mathfrak{M}} \iff \\ &\iff \big\{i \in I : \big(v_i(t_1), \ldots, v_i(t_k)\big) \in R^{\mathfrak{M}_i}\big\} \in U \iff \\ &\iff \{i \in I : \mathfrak{M}_i \models_{v_i} R(t_1, \ldots, t_k)\} \in U. \quad \cdots\end{aligned}$$

Łośov teorem

Nastavak dokaza.

Pretpostavimo da tvrdnja vrijedi za svaku formulu složenosti manje od nekog $n > 0$. Neka je F σ-formula složenosti n. Tada je F oblika $\neg G$, $(G \wedge H)$, $(G \vee H)$, $(G \to H)$, $(G \leftrightarrow H)$, $\forall x\, G$ ili $\exists x\, G$, pri čemu su G i H niže složenosti, pa za njih tvrdnja vrijedi.

$\boxed{F = \neg G}$ Vrijede sljedeće ekvivalencije:

$$
\begin{aligned}
\prod\nolimits_U \mathfrak{M}_i \models_v \neg G &\iff \prod\nolimits_U \mathfrak{M}_i \not\models_v G \\
&\iff \{i \in I : \mathfrak{M}_i \models_{v_i} G\} \notin U \\
[\,\text{svojstvo (v)}\,] &\iff I \setminus \{i \in I : \mathfrak{M}_i \models_{v_i} G\} \in U \\
&\iff \{i \in I : \mathfrak{M}_i \not\models_{v_i} G\} \in U \\
&\iff \{i \in I : \mathfrak{M}_i \models_{v_i} \neg G\} \in U. \qquad \cdots
\end{aligned}
$$

Łośov teorem

Nastavak dokaza.

$\boxed{F = \exists x\, G}$ Pretpostavimo $\prod_U \mathfrak{M}_i \models_v \exists x\, G$. Tada postoji v_x takva da je $\prod_U \mathfrak{M}_i \models_{v_x} G$. Lako je vidjeti da vrijedi sljedeće:
$\{i \in I : \mathfrak{M}_i \models_{(v_x)_i} G\} \subseteq \{i \in I : \text{postoji } (v_i)_x; \mathfrak{M}_i \models_{(v_i)_x} G\} =$
$= \{i \in I : \mathfrak{M}_i \models_{v_i} \exists x\, G\} \in U$ zbog zatvorenosti na nadskupove.

Obratno, pretpostavimo $S = \{i : \mathfrak{M}_i \models_{v_i} \exists x\, G\} \in U$. Za svaki $i \in I$, odaberimo $(v_i)_x$ tako da vrijedi $\mathfrak{M}_i \models_{(v_i)_x} G$ ako je $i \in S$, a $(v_i)_x := v_i$ inače. Uočimo da je $S = \{i : \mathfrak{M}_i \models_{(v_i)_x} G\} \in U$.

Neka je v' valuacija inducirana familijom $\{(v_i)_x : i \in I\}$.
Tada je po pretpostavci indukcije $\prod_U \mathfrak{M}_i \models_{v'} G$.

Preostaje dokazati da je $v'(y) = v(y)$ za sve varijable $y \neq x$.
Očito za sve $y \neq x$ vrijedi $\{i : (v_i)_x(y) = v_i(y)\} = I \in U$, dakle
$\left[\big((v_i)_x(y)\big)_{i \in I}\right]_U = \left[\big(v_i(y)\big)_{i \in I}\right]_U$, odnosno $v'(y) = v(y)$. $\cdots$

Łośov teorem

Nastavak dokaza.

$\boxed{F = (G \wedge H)}$ Vrijede sljedeće ekvivalencije:

$$\begin{aligned}
\prod_U \mathfrak{M}_i \models_v (G \wedge H) &\iff \prod_U \mathfrak{M}_i \models_v G \ \text{ i } \prod_U \mathfrak{M}_i \models_v H \\
\text{[pretpostavka]} &\iff \{i : \mathfrak{M}_i \models_{v_i} G\}, \{i : \mathfrak{M}_i \models_{v_i} H\} \in U \\
[A \cap B \subseteq A, B] &\iff \{i : \mathfrak{M}_i \models_{v_i} G\} \cap \{i : \mathfrak{M}_i \models_{v_i} H\} \in U \\
&\iff \{i : \mathfrak{M}_i \models_{v_i} (G \wedge H)\} \in U.
\end{aligned}$$

Ostale slučajeve ne moramo dokazivati — svi ostali veznici i kvantifikatori se mogu napisati ekvivalentno pomoću $\exists$, $\neg$ i $\wedge$. □

Korolar (Łośov osnovni teorem o ultraproduktima)

Za svaku rečenicu F vrijedi:

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

Primjene Łośova teorema

Izravno iz Łośova teorema slijede činjenice poput

- ultraprodukt familije polja je polje,
- ultraprodukt familije linearno uređenih skupova je linearno uređen skup, ...

Dokaz teorema kompaktnosti pomoću ultraprodukata.

Neka je S skup rečenica. Pretpostavimo da svaki konačan podskup od S ima model. Neka je I skup svih konačnih podskupova od S.

Za svaki $i \in I$, neka je $\mathfrak{M}_i$ model za skup formula i. Za svaku $F \in S$, neka je $S_F = \{i \in I : F \in i\}$ i neka je $E = \{S_F : F \in S\}$.

Tada E ima svojstvo konačnih presjeka. Stoga postoji ultrafilter U nad I takav da je $E \subseteq U$. Tvrdimo da je $\prod_U \mathfrak{M}_i$ model za S.

Neka je $F \in S$. Za svaki $i \in S_F$ vrijedi $\mathfrak{M}_i \models i \ni F$, pa posebno $\mathfrak{M}_i \models F$. Dakle, $S_F \subseteq \{i \in I : \mathfrak{M}_i \models F\}$.

Kako je $S_F \in E \subseteq U$, to je $\{i \in I : \mathfrak{M}_i \models F\} \in U$, pa je po Łośovu teoremu $\prod_U \mathfrak{M}_i \models F$. $\square$

Elementarne klase i ultraprodukti

Teorem

Klasa σ-struktura $\mathcal{K}$ je elementarna ako i samo ako je zatvorena na ultraprodukte i elementarnu ekvivalenciju.
Posljedica: *$\mathcal{K}$ je Δ-elementarna ako i samo ako su $\mathcal{K}$ i $\mathcal{K}^c$ zatvorene na ultraprodukte i elementarnu ekvivalenciju.*

Dokaz (samo smjer $\boxed{\Leftarrow}$, jer smjer $\boxed{\Rightarrow}$ očito vrijedi).

Neka je $\mathcal{K}$ klasa σ-struktura zatvorena na ultraprodukte i elementarnu ekvivalenciju. Tvrdimo $\mathcal{K} = Mod\big(Th(\mathcal{K})\big)$. Očito vrijedi $\boxed{\subseteq}$. Neka je $\mathfrak{M} \in Mod(\Sigma)$. Neka je I skup svih konačnih podskupova od $Th(\mathfrak{M})$. Lako se vidi da za svaki $i \in I$ postoji $\mathfrak{M}_i \in \mathcal{K}$ takav da $\mathfrak{M}_i \models i$. Kao u dokazu teorema kompaktnosti, možemo izabrati ultrafilter U nad I za koji $\prod_U \mathfrak{M}_i \models Th(\mathfrak{M})$.

Kako je $\mathcal{K}$ zatvorena na ultraprodukte, slijedi $\prod_U \mathfrak{M}_i \in \mathcal{K}$.
Iz $\prod_U \mathfrak{M}_i \models Th(\mathfrak{M})$ slijedi $\prod_U \mathfrak{M}_i \equiv \mathfrak{M}$.
No $\mathcal{K}$ je zatvorena na elementarnu ekvivalenciju, pa je $\mathfrak{M} \in \mathcal{K}$. $\square$

Univerzalne teorije

Teoremi o očuvanju povezuju sintaksu formula teorije i zatvorenost klase modela teorije u odnosu na neku konstrukciju. Promatrat ćemo teorije čije klase modela su zatvorene redom na podmodele, proširenja, unije lanaca, homomorfizme i reducirane produkte.

Definicija

Formula F je **univerzalna** *ako je oblika*
$F = \forall x_1 \cdots \forall x_n G$ *za neku otvorenu formulu G.*
Univerzalna teorija *je ona koja sadrži samo univerzalne rečenice.*

Primjer

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

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

Teorem očuvanja za podmodele

Teorije T i T' nad istom signaturom su **ekvivalentne** ako je $Mod(T) = Mod(T')$.

T je **očuvana za podmodele** ako $\mathfrak{N} \subseteq \mathfrak{M} \models T$ povlači $\mathfrak{N} \models T$; drugim riječima, ako je klasa $Mod(T)$ zatvorena na podmodele: .

Teorem

Neka je T σ-teorija. Tada je T je očuvana za podmodele ako i samo ako postoji univerzalna σ-teorija T' ekvivalentna s T.

Dokaz.

$\boxed{\Leftarrow}$ Neka je $\mathfrak{M}$ model teorije T i $\mathfrak{N} \subseteq \mathfrak{M}$. $Mod(T) = Mod(T')$ povlači $\mathfrak{M} \models T'$. Indukcijom po broju kvantifikatora univerzalne formule F, lako se dokaže da iz $\mathfrak{M} \models F$ slijedi $\mathfrak{N} \models F$.

Posebno, za sve $F \in T'$ vrijedi $\mathfrak{N} \models F$. Time smo dokazali $\mathfrak{N} \models T'$, a onda iz $Mod(T) = Mod(T')$ slijedi $\mathfrak{N} \models T$. $\cdots$

Teorem očuvanja za podmodele

Nastavak dokaza.

$\boxed{\Rightarrow}$ Definiramo $T' = \{G : G \text{ univerzalna rečenica i } T \models G\}$.
Tvrdimo da su T i T' ekvivalentne. Očito $Mod(T) \subseteq Mod(T')$.

Neka je $\mathfrak{M}$ model za T'. Dovoljno je dokazati da je skup $T \cup \Delta(\mathfrak{M})$ ispunjiv — tada iz leme o dijagramu slijedi da postoji model $\mathfrak{N}$ za T takav da je $\mathfrak{M} \subseteq \mathfrak{N}^- \models T$, pa onda i $\mathfrak{M} \models T$.

Pretpostavka suprotnog bi po teoremu kompaktnosti povlačila da postoje $G_1, \ldots, G_m \in \Delta(\mathfrak{M})$ takve da $T \not\models \bigwedge G_i =: G(\overline{a_1}, \ldots, \overline{a_n})$ (gdje smo s $\overline{a_1}, \ldots, \overline{a_n}$ označili sve nove konstantske simbole koji se pojavljuju u formulama $G_1, \ldots, G_m$).

Očito je $\mathfrak{M} \models G(\overline{a_1}, \ldots, \overline{a_n})$, no $T \models \neg G(\overline{a_1}, \ldots, \overline{a_n})$, a $\{\overline{a_1}, \ldots, \overline{a_n}\} \cap \sigma = \emptyset$, pa je i $T \models \forall x_1 \cdots \forall x_n \neg G(x_1, \ldots, x_n) \in T'$.

Zbog $\mathfrak{M} \models T'$ je posebno $\mathfrak{M} \models \forall x_1 \cdots \forall x_n \neg G(x_1, \ldots, x_n)$, što je u kontradikciji s $\mathfrak{M} \models G[a_1, \ldots, a_n]$. $\square$

Teorem očuvanja za podmodele

Primjer

Može li se teorija grupa aksiomatizirati univerzalnim formulama u signaturi $\sigma = \{\cdot, 1, =\}$?

Neka je $\mathfrak{M} = (\mathbb{Z}, +, 0)$ i $\mathfrak{N} = (\mathbb{N}, +, 0)$. Tada je $\mathfrak{M}$ model teorije grupa i $\mathfrak{N} \subseteq \mathfrak{M}$. No, $\mathfrak{N}$ nije grupa, dakle teorija grupa nije očuvana za podmodele. Iz upravo dokazanog teorema slijedi da teorija grupa nije ekvivalentna nijednoj univerzalnoj teoriji.

U dokazima teorema o očuvanju često koristimo lemu o dijagramu.

Egzistencijalne teorije

Definicija

Formula F je **egzistencijalna** *ako je $F = \exists x_1 \cdots \exists x_n G$ za otvorenu G.* **Egzistencijalna teorija** *sadrži samo egzistencijalne rečenice.*

Teorija T je **očuvana za proširenja modela** *ako $\mathfrak{N} \supseteq \mathfrak{M} \models T$ povlači $\mathfrak{N} \models T$ (klasa $Mod(T)$ je zatvorena na proširenja).*

Teorem

Neka je T σ-teorija. Tada je T je očuvana za proširenja ako i samo ako postoji egzistencijalna σ-teorija T' ekvivalentna s T.

Dokaz.

$\boxed{\Leftarrow}$ Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture takve da je $\mathfrak{M} \subseteq \mathfrak{N}$ i $\mathfrak{M} \models T$.
Pretpostavimo suprotno, da postoji $F \in T'$ takva da $\mathfrak{N} \not\models F$.

F je rečenica, pa $\mathfrak{N} \models \neg F$. Štoviše, $\neg F$ je ekvivalentna univerzalnoj rečenici, pa je teorija $\{\neg F\}$ očuvana za podmodele.

Sada iz $\mathfrak{M} \subseteq \mathfrak{N} \models \neg F$ slijedi $\mathfrak{M} \models \neg F$. No iz $\mathfrak{M} \in Mod(T) = Mod(T')$ slijedi $\mathfrak{M} \models F \in T'$, kontradikcija. $\cdots$

Teorem očuvanja za proširenja

Dokaz.

$\boxed{\Rightarrow}$ Neka je T očuvana za proširenja. Za svaku rečenicu F, neka je $U(F) := \{G : G \text{ univerzalna rečenica i } F \Rightarrow G\}$.

Metodom dijagrama se vidi da $(*)$ za svaki $\mathfrak{M} \models U(F)$ postoji $\mathfrak{N} \supseteq \mathfrak{M}$ takav da je $\mathfrak{N} \models F$ (teorija $\Delta(\mathfrak{M}) \cup \{F\}$ je konzistentna).

Neka je $F \in T$. Prema $(*)$ je teorija $U(\neg F) \cup T$ inkonzistentna, pa iz teorema kompaktnosti slijedi da postoje rečenice $G_1, \ldots, G_n \in U(\neg F)$ takve da je teorija $\{G_1, \ldots, G_n\} \cup T$ inkonzistentna. Neka je $G_F := (G_1 \wedge \cdots \wedge G_n)$. Tada je $T \cup \{G_F\}$ inkonzistentna, pa $T \models \neg G_F$. Kako je svaka G_i univerzalna, postoji egzistencijalna $H_F \Leftrightarrow \neg G_F$, pa je $T' := \{H_F : F \in T\}$ egzistencijalna teorija. Očito, svaki model za T je i model za T'.

Obratno, neka $\mathfrak{M} \models T'$ i $F \in T$. Iz $H_F \Leftrightarrow \neg G_F \Rightarrow F$ (jer su sve $G_i \in U(\neg F)$) i $H_F \in T'$ slijedi $\mathfrak{M} \models F$. $\square$

$\forall\exists$-teorije

Definicija

*Za rečenicu F kažemo da je $\forall\exists$-**formula** ako postoji otvorena formula G takva da je $F = \forall x_1 \cdots \forall x_n \exists x_{n+1} \cdots \exists x_m G$. Za teoriju T kažemo da je $\forall\exists$-**teorija** ako su svi njeni elementi $\forall\exists$-formule.*

Primjer

Teorija obostrano neograničenih gustih linearnih uređaja, teorija grupa i teorija polja su $\forall\exists$-teorije.

Napomena

- univerzalne i egzistencijalne formule su primjeri $\forall\exists$-formula
- konjunkcija/disjunkcija $\forall\exists$-formula ekvivalentna je $\forall\exists$-formuli

Kažemo da je teorija T **očuvana za unije lanaca modela** ako za svaki lanac $\{\mathfrak{M}_i : i \in I\} \subseteq Mod(T)$ vrijedi $\bigcup_{i \in I} \mathfrak{M}_i \in Mod(T)$.

Teorem očuvanja za unije lanaca

Najprije navodimo tri leme (prva se dokazuje indukcijom po broju kvantifikatora, a druga i treća metodom dijagrama).

Za $\mathfrak{M} \subseteq \mathfrak{N}$ kažemo da je $\mathfrak{M}$ **1-elementarni podmodel** od $\mathfrak{N}$, i pišemo $\mathfrak{M} \prec_1 \mathfrak{N}$, ako za svaku univerzalnu formulu $F(v_1, \ldots, v_n)$ i $a_1, \ldots, a_n \in |\mathfrak{M}|$, $\mathfrak{M} \models F[a_1, \ldots, a_n]$ povlači $\mathfrak{N} \models F[a_1, \ldots, a_n]$ (obrnuti smjer vrijedi zbog $\mathfrak{M} \subseteq \mathfrak{N}$).

Lema

1. *Neka je $\mathfrak{M} \prec_1 \mathfrak{M}'$. Tada i za sve egzistencijalne formule F vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$ ako i samo ako $\mathfrak{M}' \models F[a_1, \ldots, a_n]$.*
2. *Ako $\mathfrak{M} \prec_1 \mathfrak{M}'$, tada postoji $\mathfrak{N}$ takav da je $\mathfrak{M} \prec \mathfrak{N}$ i $\mathfrak{M}' \subseteq \mathfrak{N}$.*
3. *Neka je T σ-teorija i $T' = \{G : G \text{ je } \forall\exists\text{-rečenica}, T \models G\}$. Ako $\mathfrak{M} \models T'$, tada postoji $\mathfrak{N}$ takav da $\mathfrak{M} \prec_1 \mathfrak{N} \models T$.*

Teorem očuvanja za unije lanaca

Teorem

Neka je T σ-teorija. Tada je T je očuvana za unije lanaca modela ako i samo ako postoji $\forall\exists$-teorija T' ekvivalentna s T.

Dokaz.

$\boxed{\Leftarrow}$ Treba dokazati da je svaka $\forall\exists$-formula očuvana za unije lanaca modela.

Neka je $F = \forall x_1 \cdots \forall x_n \exists y_1 \cdots \exists y_p H(x_1, \ldots, x_n, y_1, \ldots, y_p)$, pri čemu je H otvorena formula.

Neka je $\{\mathfrak{M}_i : i \in I\}$ lanac modela za F i $\mathfrak{M} = \bigcup_{i \in I} \mathfrak{M}_i$. Treba dokazati $\mathfrak{M} \models F$, što je ekvivalentno s $\mathfrak{M} \models \exists y_1 \cdots \exists y_p H[a_1, \ldots, a_n]$ za proizvoljne $a_1, \ldots, a_n \in |\mathfrak{M}|$.

I je linearno uređen, pa postoji $i \in I$ takav da su $a_1, \ldots, a_n \in |\mathfrak{M}_i|$. Zbog $\mathfrak{M}_i \models F$ postoje $b_1, \ldots, b_p \in |\mathfrak{M}_i|$ takvi da vrijedi $\mathfrak{M}_i \models H[a_1, \ldots, a_n, b_1, \ldots, b_p]$. Kako je $\mathfrak{M}_i \subseteq \mathfrak{M}$ i H otvorena, $\mathfrak{M} \models H[a_1, \ldots, a_n, b_1, \ldots, b_p]$, iz čega slijedi tvrdnja. $\cdots$

Teorem očuvanja za unije lanaca

Dokaz drugog smjera (slično dokazu Robinsonova teorema).

$\boxed{\Rightarrow}$ Neka je teorija T očuvana za unije lanaca modela. Označimo $T' := \{G : G \text{ je } \forall\exists\text{-formula}, T \models G\}$. Očito $Mod(T) \subseteq Mod(T')$, preostaje dokazati obrat. Neka je $\mathfrak{M}_0$ proizvoljni model za T'.

Po lemi 3 postoji model $\mathfrak{M}_1$ za T takav da je $\mathfrak{M}_0 \prec_1 \mathfrak{M}_1$. Po lemi 2 postoji $\mathfrak{M}_2$ tako da $\mathfrak{M}_0 \prec \mathfrak{M}_2$ i $\mathfrak{M}_1 \subseteq \mathfrak{M}_2$. Kako je $\mathfrak{M}_0 \models T'$ i $\mathfrak{M}_0 \prec \mathfrak{M}_2$, također je $\mathfrak{M}_2 \models T'$. Uzastopnom primjenom lema dobivamo lanac modela $\{\mathfrak{M}_k : k \in \mathbb{N}\}$ takvih da je za sve $k \in \mathbb{N}$:

- $\mathfrak{M}_{2k} \models T'$ i $\mathfrak{M}_{2k+1} \models T$
- $\mathfrak{M}_{2k} \prec_1 \mathfrak{M}_{2k+1}$, $\mathfrak{M}_{2k} \prec \mathfrak{M}_{2k+2}$ i $\mathfrak{M}_{2k+1} \subseteq \mathfrak{M}_{2k+2}$

Posebno je $\mathfrak{M}_{2k} \subseteq \mathfrak{M}_{2k+1}$, pa je $(\mathfrak{M}_k)_k$ rastući.

Dakle, za $\mathfrak{M} := \bigcup_k \mathfrak{M}_k$ je $\mathfrak{M} = \bigcup_k \mathfrak{M}_{2k+1} = \bigcup_{k\in\mathbb{N}} \mathfrak{M}_{2k}$.

Za svaki k je $\mathfrak{M}_{2k+1} \models T$, a T je očuvana za unije lanaca, pa je $\mathfrak{M} \models T$. Iz $\mathfrak{M}_{2k} \prec \mathfrak{M}_{2k+2}$ i $\mathfrak{M} = \bigcup_k \mathfrak{M}_{2k}$, po teoremu o uniji elementarnih lanaca slijedi $\mathfrak{M}_0 \prec \mathfrak{M}$, pa je i $\mathfrak{M}_0 \models T$. $\square$

Modelno potpune teorije

Primjer (Teorija koja nije očuvana za unije lanaca)

Neka je T teorija gustih linearnih uređaja s rubovima.

Za svaki $k \in \mathbb{N}$, neka je $\mathfrak{M}_k := ([-k, k], <) \models T$.
No $\bigcup_{k \in \mathbb{N}} \mathfrak{M}_k = (\mathbb{R}, <) \not\models T$: „imati rub" nije $\forall\exists$-formula.

Teorija T je **modelno potpuna** ako
za sve $\mathfrak{M}, \mathfrak{N} \in Mod(T)$, $\mathfrak{M} \subseteq \mathfrak{N}$ povlači $\mathfrak{M} \prec \mathfrak{N}$.

Propozicija

Svaka modelno potpuna teorija je ekvivalentna nekoj $\forall\exists$-teoriji.

Dokaz.

Neka je $\{\mathfrak{M}_i : i \in I\}$ lanac modela za T. Za sve $i, j \in I$,
$i < j$ povlači $\mathfrak{M}_i \subseteq \mathfrak{M}_j$, a onda modelna potpunost daje $\mathfrak{M}_i \prec \mathfrak{M}_j$.
To znači da je $\{\mathfrak{M}_i : i \in I\}$ elementarni lanac modela za T.

Iz teorema o uniji elementarnog lanca slijedi $\bigcup_{i \in I} \mathfrak{M}_i \models T$.
Po prethodnom teoremu T je ekvivalentna nekoj $\forall\exists$-teoriji. $\square$

Pozitivne teorije

Definicija

Kažemo da je formula F **pozitivna** *ako ne sadrži $\neg$, $\rightarrow$ ni $\leftrightarrow$ (izgrađena je od atomarnih formula pomoću $\wedge$, $\vee$, $\exists$ i $\forall$).*

Za neku teoriju kažemo da je **pozitivna teorija** *ako je svaka njena rečenica pozitivna formula.*

Definicija

Za teoriju T kažemo da je **očuvana za homomorfizme** *ako je homomorfna slika svakog modela za T također model za T.*

Kažemo da je σ-formula $F(v_1, \ldots, v_n)$ **očuvana za homomorfizme** *ako za sve σ-strukture $\mathfrak{M}$ i $\mathfrak{N}$, za svaki homomorfizam $h : |\mathfrak{M}| \rightarrow |\mathfrak{N}|$ i za sve $a_1, \ldots, a_n \in |\mathfrak{M}|$ vrijedi: ako $\mathfrak{M} \models F[a_1, \ldots, a_n]$, onda $\mathfrak{N} \models F[h(a_1), \ldots, h(a_n)]$.*

Teorem očuvanja za homomorfizme

Teorem

Neka je T konzistentna σ-teorija. T je očuvana za homorfizme ako i samo ako postoji pozitivna σ-teorija T' ekvivalentna s T.

Napomena

Inkonzistentna teorija je trivijalno zatvorena na homomorfizme (nema modela), no nije ekvivalentna niti jednoj pozitivnoj teoriji, jer svaka pozitivna teorija ima model.

Naime, struktura s nosačem $\{0\}$ u kojoj su svi konstantski simboli interpretirani s 0, svi funkcijski simboli kao konstantne 0-funkcije, a svi relacijski simboli kao $\{(0, \ldots, 0)\}$, model je za svaku pozitivnu formulu nad bilo kojim skupom simbola σ.

Dokaz.

$\boxed{\Leftarrow}$ Dovoljno je dokazati (indukcijom po složenosti formule) da je svaka pozitivna formula očuvana za homomorfizme (onda će i njihove logičke posljedice biti takve). $\cdots$

Teorem očuvanja za homomorfizme

Dokaz.

$\boxed{\Rightarrow}$ Neka je T konzistentna σ-teorija očuvana za homomorfizme. Pišemo $\mathfrak{M} \equiv_p \mathfrak{N}$ ako za svaku pozitivnu σ-rečenicu F vrijedi $\mathfrak{M} \models F$ ako i samo ako $\mathfrak{N} \models F$. Koriste se dvije pomoćne tvrdnje:

1. ako je $\mathfrak{M} \equiv_p \mathfrak{M}'$, onda postoji $\mathfrak{N}$ takva da je $\mathfrak{M}' \prec \mathfrak{N}$ i postoji smještenje $f : |\mathfrak{M}| \to |\mathfrak{N}|$ takvo da je $\mathfrak{M}_{|\mathfrak{M}|} \equiv_p \mathfrak{N}_{|\mathfrak{M}|}$
2. ako je $\mathfrak{N}_0 \equiv_p \mathfrak{M}_0 \models T$, onda je i $\mathfrak{N}_0 \models T$ (pogledati skriptu!)

Neka je $\mathfrak{M}_0$ kanonski model za T. Tada za svaku pozitivnu σ-rečenicu F vrijedi $T \models F$ ako i samo ako $\mathfrak{M}_0 \models F$.

[Pozitivne formule ne mogu biti međusobno kontradiktorne!]

Za $T' = \{F : F \text{ pozitivna}, \mathfrak{M}_0 \models F\}$, svaki model za T ujedno je i model za T'. Obratno, neka je $\mathfrak{N}_0 \models T'$. Tada je $\mathfrak{M}_0 \equiv_p \mathfrak{N}_0$, pa iz 2. tvrdnje slijedi $\mathfrak{N}_0 \models T$. $\square$

Elementarne Hornove formule

Definicija

Elementarna Hornova formula H *je elementarna konjunkcija oblika* $H_1 \vee \cdots \vee H_n$*, gdje je najviše jedan konjunkt* H_i *atomaran, a ostali konjunkti su negacije atomarnih formula.*

Napomena

- ako je $n = 1$, sāma H je atomarna ili negacija atomarne
- ako je $n > 1$ i H_n atomarna, onda je $H_i = \neg G_i$, gdje su $G_1, \ldots, G_{n-1}$ atomarne i $H \Leftrightarrow (G_1 \wedge \cdots \wedge G_{n-1}) \rightarrow H_n$
- ako je $n > 1$ i nijedna H_i nije atomarna, onda je $H_i = \neg G_i$, gdje su $G_1, \ldots, G_n$ atomarne i $H \Leftrightarrow \neg(G_1 \wedge \cdots \wedge G_n)$

Hornove formule

Definicija

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

Napomena

Po teoremu o preneksnoj normalnoj formi, za svaku Hornovu formulu H postoje elementarne Hornove formule $F_1, \ldots, F_n$ takve da je $H \Longleftrightarrow \mathfrak{Q}_1 x_1 \cdots \mathfrak{Q}_m x_m (F_1 \wedge \cdots \wedge F_n)$, gdje su $\mathfrak{Q}_i \in \{\forall, \exists\}$.

Primjer

Teorija grupa i teorija prstena mogu biti aksiomatizirane skupovima Hornovih formula.

Teorija polja ne može, jer njena formula $\forall x \exists y \, (x = 0 \vee x \cdot y = 1)$ nije ekvivalentna niti jednoj Hornovoj formuli.

Očuvanje za reducirane produkte

Za formulu A kažemo da je **očuvana za reducirane produkte** ako za svaku familiju $\{\mathfrak{M}_i : i \in I\}$ σ-struktura i svaki filter F nad I vrijedi: ako $\{i \in I : \mathfrak{M}_i \models A\} \in F$, onda $\prod_F \mathfrak{M}_i \models A$.

Sljedeća propozicija dokazuje se indukcijom po broju koraka u izgradnji Hornove formule.

Propozicija

Hornove formule su očuvane za reducirane produkte.

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

Propozicija

Neka je F zatvorena formula. Ekvivalentno je:

a) *F je ekvivalentna nekoj univerzalnoj Hornovoj formuli*

b) *F je očuvana za podmodele i za reducirane produkte*

c) *F je očuvana za podmodele i za konačne produkte*

Omašivanje tipova

U nastavku T označava proizvoljnu (fiksiranu) potpunu σ-teoriju.

Intuicija: tip je „beskonačna konjunkcija"
(ali s konačno mnogo slobodnih varijabli).

Definicija

*Za $n \in \mathbb{N}$, n-**tip teorije** T je skup σ-formulā S koji je zatvoren na konjunkciju i sve slobodne varijable su mu u skupu $\{x_1, \ldots, x_n\}$.*

Neka je S n-tip od T i $\mathfrak{M} \models T$. **Niz** $a_1, \ldots, a_n \in |\mathfrak{M}|$ **realizira** S *ako za sve $F \in S$ vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$.*

Model $\mathfrak{M}$ **realizira** S *ako postoji niz u $\mathfrak{M}$ koji realizira S.*
U suprotnom kažemo da **model** $\mathfrak{M}$ **omašuje** S.

Napomena

Neka je S tip i neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za T. Tada vrijedi:

- ako $\mathfrak{M} \prec \mathfrak{N}$, te je $a_1, \ldots, a_n$ niz iz $\mathfrak{M}$ koji realizira tip S, tada taj niz realizira tip S i u strukturi $\mathfrak{N}$;
- ako $\mathfrak{M} \simeq \mathfrak{N}$ i $\mathfrak{M}$ realizira/omašuje S, onda to isto čini i $\mathfrak{N}$.

Konzistentni tipovi

Definicija

Kažemo da je n-tip teorije T **konzistentan tip** *ako postoji model $\mathfrak{M}$ za T koji ga realizira.*

Lema

Neka je T potpuna σ-teorija i S n-tip. Tada je S konzistentan ako i samo ako postoji prebrojivi model koji ga realizira, što je ako i samo ako za sve $F \in S$ vrijedi $T \models \exists x_1 \cdots \exists x_n F$.

Dokaz.

Druga tvrdnja očito povlači prvu. Dokažimo da prva tvrdnja povlači treću. Neka je $\mathfrak{M}$ model za T i $a_1, \ldots, a_n \in |\mathfrak{M}|$ takvi da za sve $F \in S$ vrijedi $\mathfrak{M} \models F[a_1, \ldots, a_n]$.
Neka je $\mathfrak{N}$ model za T i neka je $F \in S$. Očito $\mathfrak{M} \models \exists x_1 \cdots \exists x_n F$.
Zbog potpunosti T je $\mathfrak{M} \equiv \mathfrak{N}$, pa i $\mathfrak{N} \models \exists x_1 \cdots \exists x_n F$. $\cdots$

Konzistentni tipovi

Nastavak.

Preostaje dokazati da treća tvrdnja povlači drugu. Neka je $\sigma' = \sigma \cup \{c_1, \ldots, c_n\}$, gdje su $c_1, \ldots, c_n$ novi konstantski simboli (međusobno različiti). Neka je $T' = T \cup \{F(c_1, \ldots, c_n) : F \in S\}$.

Tada je T' konzistentna. Zaista, u suprotnom po teoremu kompaktnosti postoji konačan $S' \subseteq S$ takav da je teorija $T \cup \{F(c_1, \ldots, c_n) : F \in S'\}$ inkonzistentna. Neka je G konjunkcija svih formula iz S'. Po definiciji tipa, S je zatvoren na konjunkcije, pa je $G \in S$. Tada $T \models \neg G(c_1, \ldots, c_n)$ i stoga $T \models \neg \exists x_1 \cdots \exists x_n G(x_1, \ldots, x_n)$, što je kontradikcija s 3. tvrdnjom.

Kako je T' konzistentna, iz Löwenheim–Skolemova teorema „na dolje" slijedi da T' ima prebrojiv model $\mathfrak{M}'$. Sada je σ-redukcija od $\mathfrak{M}'$ prebrojiv model za T, i u njoj niz $c_1^{\mathfrak{M}'}, \ldots, c_n^{\mathfrak{M}'}$ realizira S. $\square$

Konzistentni tipovi

Pomoću leme o dijagramu dokazuje se (skripta!) da su dvije σ-strukture elementarno ekvivalentne ako i samo ako postoji jedna σ-struktura koja je elementarno proširenje „obiju" (preciznije, jedne i izomorfne kopije druge).

$$(\mathfrak{M} \equiv \mathfrak{N}) \iff \exists\, \mathfrak{U}\, \exists\, \mathfrak{N}' \,(\mathfrak{M} \prec \mathfrak{U} \land \mathfrak{N} \simeq \mathfrak{N}' \prec \mathfrak{U})$$

Lema

Neka je T potpuna σ-teorija, $\mathfrak{M}$ model za T i S konzistentan tip.

Tada postoji σ-struktura $\mathfrak{N}$ takva da je $\mathfrak{M} \prec \mathfrak{N}$ i $\mathfrak{N}$ realizira S.

Dokaz.

Neka je $\mathfrak{M}'$ model za T koji realizira S. Kako je T potpuna, vrijedi $\mathfrak{M} \equiv \mathfrak{M}'$. Stoga postoji $\mathfrak{N}$ takav da je $\mathfrak{M} \prec \mathfrak{N}$ i $\mathfrak{M}' \prec \mathfrak{N}$.

Kako $\mathfrak{M}'$ realizira S, to i $\mathfrak{N}$ realizira S. $\square$

Izolirani tipovi

Definicija

Neka je S n-tip i $G(x_1, \ldots, x_n)$ σ-formula. Kažemo da G **izolira** *S ako $T \models \exists x_1 \cdots \exists x_n G$ i za sve $F \in S$ je $T \models \forall x_1 \cdots \forall x_n (G \to F)$.*

Kažemo da je S **izolirani tip** *ako postoji formula koja ga izolira.*

Propozicija

Ako je S izolirani tip, onda svaki model teorije T realizira S.

Posebno, svaki izolirani tip je konzistentan.

Dokaz.

Neka je $G(x_1, \ldots, x_n)$ formula koja izolira S, i neka je $\mathfrak{M}$ model za T. Kako je $T \models \exists x_1 \cdots \exists x_n G$, postoje $a_1, \ldots, a_n \in |\mathfrak{M}|$ takvi da $\mathfrak{M} \models G[a_1, \ldots, a_n]$. Kako je $T \models \forall x_1 \cdots \forall x_n (G \to F)$ za sve $F \in S$, posebno je $\mathfrak{M} \models F[a_1, \ldots, a_n]$. $\square$

Teorem o omašivanju tipova je obrat prethodne propozicije.

Teorem o omašivanju tipova

Teorem

Neka je T potpuna σ-teorija. Ako je S tip koji nije izoliran, onda postoji prebrojivi model teorije T koji omašuje S. Ako T sadrži aksiome jednakosti, postoji takav normalni model.

Dokaz.

Traženi prebrojivi model konstruiramo Henkinovom metodom. Neka je $C = \{c_i : i \in \mathbb{N}\}$ skup novih (međusobno različitih) konstantskih simbola i $\sigma' = \sigma \cup C$. Konstruiramo σ'-teoriju T' takvu da:

1. $T \subseteq T'$
2. T' je potpuna σ'-teorija
3. T' je Henkinova: za svaku σ'-formulu $F(x)$ postoji $i \in \mathbb{N}$ takav da je $\big(\exists x F(x) \to F(c_i/x)\big) \in T'$
4. za svaki $n \in \mathbb{N}_+$ i za sve $d_1, \ldots, d_n \in C$ postoji $F(x_1, \ldots, x_n) \in S$ takav da $\neg F(d_1, \ldots, d_n) \in T'$

Pretpostavimo da je takva teorija konstruirana. $\cdots$

Teorem o omašivanju tipova

Nastavak dokaza.

Ako trebamo normalnu strukturu, na C definiramo
$R(c_i, c_j) :\Leftrightarrow (T' \models c_i = c_j)$ (inače za R stavimo običnu jednakost).
R je relacija ekvivalencije zbog aksiomā jednakosti u $T \subseteq T'$.

Neka je $\overline{c}$ oznaka za klasu ekvivalencije s reprezentantom c. Sad je lako (detalje ispuštamo) definirati σ'-strukturu $\mathfrak{M}'$ s nosačem $C/_R$ takvu da za sve $d_1, \ldots, d_n \in C$ i za svaku σ-formulu $F(x_1, \ldots, x_n)$ vrijedi $\mathfrak{M}' \models F[\overline{d_1}, \ldots, \overline{d_n}]$ ako i samo ako $F(d_1, \ldots, d_n) \in T'$.

Neka je $\mathfrak{M}$ σ-redukcija od $\mathfrak{M}'$. Dokažimo da tada $\mathfrak{M}$ omašuje S. Neka su $d_1, \ldots, d_n \in C$. Prema uvjetu 4, postoji $F(x_1, \ldots, x_n) \in S$ takva da $\mathfrak{M}' \models \neg F[\overline{d_1}, \ldots, \overline{d_n}]$. Dakle, nijedan niz iz $C/_R$ ne realizira S. Očito je $\mathfrak{M}$ model za teoriju T (po uvjetu 1, vrijedi $T \subseteq T'$, a po definiciji je $\mathfrak{M}'$ model za T'), pa slijedi tvrdnja.

Preostaje konstruirati teoriju T'. Neka je $(F_i)_i$ niz svih σ'-rečenica, a $\big(G_i(x)\big)_i$ niz svih σ'-formula s jednom slobodnom varijablom. Neka je $(\gamma_i)_i$ niz svih uređenih n-torki skupa C. $\cdots$

Teorem o omašivanju tipova

Nastavak dokaza.

Indukcijom ćemo definirati niz teorija $(T_k)_k$
takvih da za sve $k \in \mathbb{N}$ vrijede sljedeća svojstva:

(a) T_k je unija skupa T i konačnog skupa rečenica

(b) T_k je konzistentna

(c) $T_k \subseteq T_m$ za $k \leq m$ (dovoljno je tražiti $T_k \subseteq T_{k+1}$)

Tada za $T' := \bigcup_k T_k$ iz (b), (c) i teorema kompaktnosti lako slijedi da je T' konzistentna.

Stavimo $T_0 := T$, te ako imamo T_k, za T_{k+1} stavimo:

- $T_k \cup \{F_i\}$ ako je konzistentna, inače $T_k \cup \{\neg F_i\}$, za $k = 3i$ (time se postiže potpunost);
- $T_k \cup \{\exists x G_i(x) \to G_i(c_j)\}$, gdje c_j nije ni u jednoj formuli iz T_k niti u G_i, za $k = 3i + 1$ (T' mora biti Henkinova). $\cdots$

Teorem o omašivanju tipova

Nastavak dokaza.

Treći slučaj, $k = 3i + 2$, nešto je složeniji.
Želimo postići da $T' = \bigcup_k T_k$ ispunjava uvjet 4.

Neka je $\gamma_i =: (d_1, \ldots, d_n)$. Prema pretpostavci indukcije (svojstvo (a)), postoji σ'-rečenica H takva da je T_k ekvivalentna s $T \cup \{H\}$.

Postoji σ-formula D i $e_1, \ldots, e_m \in C$ takvi da je H ekvivalentna s $D(d_1, \ldots, d_n, e_1, \ldots, e_m)$. Označimo $E := \exists x_{n+1} \cdots \exists x_{n+m} D$.

Kako je T potpuna, vrijedi $T \models \exists x_1 \cdots \exists x_n E$. Kako S nije izoliran, postoji $F(x_1, \ldots, x_n) \in S$ takva da $T \not\models \forall x_1 \cdots \forall x_n (E \to F)$.

Stoga su redom konzistentne teorije:

- $T \cup \{\neg \forall x_1 \cdots \forall x_n (E \to F)\}$
- $T \cup \{\exists x_1 \cdots \exists x_n \exists x_{n+1} \cdots \exists x_{n+m} (D \wedge \neg F)\}$
- $T \cup \{D(d_1, \ldots, d_n, e_1, \ldots, e_m) \wedge \neg F(d_1, \ldots, d_n)\}$

Slijedi da možemo definirati $T_{k+1} := T_k \cup \{\neg F(d_1, \ldots, d_n)\}$. $\square$

Konzistentni tipovi $\aleph_0$-kategoričnih teorija

Korolar

Neka je T potpuna $\aleph_0$-kategorična teorija.
Tada je svaki konzistentni tip izoliran.

Dokaz.

Pretpostavimo suprotno. Neka je S konzistentni neizolirani tip.
Zbog konzistentnosti, neki prebrojivi model $\mathfrak{M}$ za T realizira S.

S druge strane, kako S nije izoliran, po teoremu o omašivanju tipova postoji prebrojivi model $\mathfrak{N}$ za T koji ga omašuje.

Kako su $\mathfrak{M}$ i $\mathfrak{N}$ prebrojivi modeli, a T je $\aleph_0$-kategorična, $\mathfrak{M} \simeq \mathfrak{N}$, što je u kontradikciji s time da $\mathfrak{M}$ realizira S, a $\mathfrak{N}$ ga omašuje. $\square$

Istaknimo bez dokaza da vrijedi i obrat: potpuna teorija je $\aleph_0$-kategorična ako i samo ako je svaki konzistentni tip izoliran.

Potpuni tipovi

Definicija

Za n-tip S kažemo da je **potpuni tip** *ako je konzistentan i za svaku σ-formulu F čije varijable su iz $\{x_1, \ldots, x_n\}$ vrijedi $F \in S$ ili $\neg F \in S$. Skup svih potpunih n-tipova označavamo sa $\mathcal{S}_n$.*

Napomena

- Ako su S_1 i S_2 potpuni n-tipovi i $S_1 \subseteq S_2$, onda je $S_1 = S_2$.
- Ako je $\mathfrak{M}$ model potpune teorije i $\vec{a} \in |\mathfrak{M}|^n$, onda je $t(\vec{a}/\mathfrak{M}) = \{F(x_1, \ldots, x_n) : \mathfrak{M} \models F[\vec{a}]\}$ potpun tip.
- Svaki potpuni tip je oblika $t(\vec{a}/\mathfrak{M})$ za neke $\mathfrak{M}$ i $\vec{a} \in |\mathfrak{M}|^n$.

Propozicija

Ako formula $F(x_1, \ldots, x_n)$ izolira potpuni tip S, onda je $F \in S$.

Dokaz.

Vrijedi $T \models \exists x_1 \cdots \exists x_n F$, pa $T \not\models \forall x_1 \cdots \forall x_n (F \to \neg F)$.
Stoga $\neg F \notin S$. Kako je S potpun, slijedi $F \in S$. $\square$

Potpuni tipovi $\aleph_0$-kategoričnih teorija

Iz prethodnog korolara posebno slijedi da je za potpunu $\aleph_0$-kategoričnu teoriju svaki potpuni tip izoliran.

Vrijedi i obrat (ispuštamo dokaz): potpuna teorija je $\aleph_0$-kategorična ako i samo ako je svaki potpuni tip izoliran.

Korolar

Neka je T potpuna $\aleph_0$-kategorična teorija.
Tada je za svaki $n \in \mathbb{N}$ skup svih potpunih n-tipova $\mathcal{S}_n$ konačan.

Dokaz.

Neka je $n \in \mathbb{N}$. Ako je S potpuni n-tip, onda je S izoliran. Odaberimo formulu $F_S(x_1, \ldots, x_n)$ koja izolira S. Tada je $F_S \in S$.

Ako su $S_1 \neq S_2$ potpuni n-tipovi, lako se vidi $\neg F_{S_1} \in S_2$. Pretpostavimo da postoji $n \in \mathbb{N}$ takav da je skup $\mathcal{S}_n$ beskonačan.

Jeziku teorije T dodajmo skup novih konstantskih simbola $\{c_1, \ldots, c_n\}$. Tada je $T' := T \cup \{\neg F_S(c_1, \ldots, c_n) : S \in \mathcal{S}_n\}$ konzistentna, jer je $T_X = T \cup \{\neg F_S(c_1, \ldots, c_n) : S \in X\}$ konzistentna za svaki konačni $X \subseteq \mathcal{S}_n$. $\cdots$

Potpuni tipovi $\aleph_0$-kategoričnih teorija

Nastavak dokaza.

Zaista, neka je $S_0 \in \mathcal{S}_n \setminus X$, $\mathfrak{M}$ model za T i $\vec{a} \in |\mathfrak{M}|^n$ takvi da je $S_0 = t(\vec{a}/\mathfrak{M})$.

Za svaki $S \in X$ vrijedi $\neg F_S \in S_0$, pa $\mathfrak{M} \models \neg F_S[a_1, \ldots, a_n]$. Dakle, model za teoriju T_X dobivamo tako da svaki konstantski simbol c_i interpretiramo s a_i.

Time je dokazano da je T' konzistentna. Neka je $\mathfrak{N}$ model za T'. Tada postoje $b_1, \ldots, b_n \in |\mathfrak{N}|$ takvi da za svaki $S \in \mathcal{S}_n$ vrijedi $\mathfrak{N} \models \neg F_S[b_1, \ldots, b_n]$. Stoga potpuni n-tip $t(\vec{b}/\mathfrak{N})$ nije u $\mathcal{S}_n$, čime je dobivena kontradikcija. $\square$

I u ovom slučaju vrijedi i obrat: potpuna teorija je $\aleph_0$-kategorična ako i samo ako je za svaki n skup svih potpunih n-tipova konačan (također ispuštamo dokaz).

Eliminacija kvantifikatora

U dokazima potpunosti nekih teorija koristili smo Łoś–Vaughtov test. No, on nije uvijek primjenjiv, jer postoje potpune teorije koje nisu λ-kategorične ni za jedan beskonačni kardinalni broj λ.

U dokazima potpunosti koristi se i eliminacija kvantifikatora.

Definicija

Za teoriju T kažemo da **dopušta eliminaciju kvantifikatora** *ako za svaku formulu $F(x_1, \ldots, x_n)$ postoji otvorena formula $G(x_1, \ldots, x_n)$ koja joj je ekvivalentna u teoriji T, odnosno*

$$T \models \forall x_1 \cdots \forall x_n \big(F(x_1, \ldots, x_n) \leftrightarrow G(x_1, \ldots, x_n) \big).$$

Primitivne egzistencijalne formule

Podsjetimo se, egzistencijalne formule su one koje su u preneksnoj normalnoj formi i sadrže samo egzistencijalne kvantifikatore.

Za egzistencijalnu σ-formulu kažemo da je **primitivna** ako je oblika $\exists x_1 \cdots \exists x_n G(x_1, \ldots, x_n)$, gdje je G elementarna konjukcija — konjunkcija atomarnih i negacijā atomarnih formula.

Lema

Svaka egzistencijalna formula je logički ekvivalentna disjunkciji primitivnih egzistencijalnih formula.

Lema

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.

Primitivne egzistencijalne formule

Dokaz.

$\boxed{\Rightarrow}$ Ako T dopušta eliminaciju kvantifikatora, onda po definiciji tvrdnja vrijedi za sve formule, pa posebno i za primitivne egzistencijalne s jednim kvantifikatorom.

$\boxed{\Leftarrow}$ Dovoljno je dokazati tvrdnju za formule u preneksnoj normalnoj formi. To dokazujemo indukcijom po broju kvantifikatora u F. Baza ima dva slučaja:

$\boxed{F = \exists x G}$ Prema prethodnoj lemi, postoje primitivne egzistencijalne formule $G_1, \ldots, G_m$ takve da $T \models \exists x G \leftrightarrow (G_1 \vee \cdots \vee G_m)$. Po pretpostavci, za svaku formulu G_i postoji otvorena formula F_i takva da $T \models G_i \leftrightarrow F_i$.
Stoga $T \models (G_1 \vee \cdots \vee G_m) \leftrightarrow (F_1 \vee \cdots \vee F_m)$.
Dakle, $T \models F \leftrightarrow (F_1 \vee \cdots \vee F_m)$.

$\boxed{F = \forall x G}$ Prema prethodnom slučaju, postoji otvorena formula F takva da $T \models \exists x \neg G \leftrightarrow F$.
Dakle, $T \models \neg \exists x \neg G \leftrightarrow \neg F$, odnosno $T \models \forall x G \leftrightarrow \neg F$. $\cdots$

Primitivne egzistencijalne formule

Dokaz.

Pretpostavimo da tvrdnja vrijedi za svaku formulu u preneksnoj normalnoj formi s n kvantifikatora. Neka je F formula u preneksnoj normalnoj formi s $n+1$ kvantifikatorom. Imamo dva slučaja:

$\boxed{F = \exists x F'}$ Po pretpostavci indukcije, postoji otvorena formula G' takva da $T \models F' \leftrightarrow G'$. Dakle, $T \models \exists x F' \leftrightarrow \exists x G'$.

Po bazi indukcije, postoji otvorena formula G takva da $T \models \exists x G' \leftrightarrow G$, pa $T \models F \leftrightarrow G$.

$\boxed{F = \forall x F'}$ Analogno. $\square$

Kriterij za eliminaciju kvantifikatora

Teorem

Neka je T σ-teorija i $F(x_1, \ldots, x_n)$ σ-formula. Ekvivalentno je:

a) *Formula F je ekvivalentna u T nekoj otvorenoj formuli.*

b) *Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za teoriju T, $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{N}_0 \subseteq \mathfrak{N}$ takvi da je $\mathfrak{M}_0 \simeq \mathfrak{N}_0$ i neka je $f : |\mathfrak{M}_0| \to |\mathfrak{N}_0|$ izomorfizam. Tada za sve $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ iz $\mathfrak{M} \models F[a_1, \ldots, a_n]$ slijedi $\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$.*

Dokaz.

$\boxed{\Rightarrow}$ Neka je G otvorena takva da $T \models \forall x_1 \cdots \forall x_n(F \leftrightarrow G)$, neka su $\mathfrak{M}, \mathfrak{N}, \mathfrak{M}_0, \mathfrak{N}_0, f$ kao u iskazu i neka su $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ takvi da $\mathfrak{M} \models F[a_1, \ldots, a_n]$. Tada vrijedi i $\mathfrak{M} \models G[a_1, \ldots, a_n]$. Kako je G otvorena i $\mathfrak{M}_0 \subseteq \mathfrak{M}$, vrijedi i $\mathfrak{M}_0 \models G[a_1, \ldots, a_n]$.

Zbog $\mathfrak{M}_0 \simeq \mathfrak{N}_0$ vrijedi i $\mathfrak{N}_0 \models G[f(a_1), \ldots, f(a_n)]$. Sada $\mathfrak{N}_0 \subseteq \mathfrak{N}$ povlači $\mathfrak{N} \models G[f(a_1), \ldots, f(a_n)]$. Iz $\mathfrak{N} \models T \models \forall x_1 \cdots \forall x_n(F \leftrightarrow G)$ zaključujemo $\mathfrak{N} \models F[f(a_1), \ldots, f(a_n)]$. $\cdots$

Kriterij za eliminaciju kvantifikatora

$\boxed{\Leftarrow}$ Koristimo sljedeću pomoćnu tvrdnju (ispuštamo njen dokaz).

Lema

Neka je T σ-teorija zatvorena za relaciju logičke posljedice, $\varphi(x_1, \ldots, x_m)$ σ-formula i S skup σ-formula zatvoren za disjunkciju čije slobodne varijable su iz $\{x_1, \ldots, x_m\}$. Ekvivalentno je:

(1) $T \models \forall x_1 \cdots \forall x_m \, \varphi$ *ili* $T \models \forall x_1 \cdots \forall x_m \, \neg\varphi$ *ili postoje otvorene formule* $\varphi_1, \ldots, \varphi_k \in S$ *takve da* $T \models \forall x_1 \cdots \forall x_m \big(\varphi \leftrightarrow (\varphi_1 \wedge \cdots \wedge \varphi_k)\big)$

(2) *ako su* $\mathfrak{M}$ *i* $\mathfrak{N}$ *modeli za* T, $a_1, \ldots, a_m \in |\mathfrak{M}|$ *i* $b_1, \ldots, b_m \in |\mathfrak{N}|$, *takvi da* $\mathfrak{M} \models \varphi[a_1, \ldots, a_m]$ *i za sve* $F \in S$ *iz* $\mathfrak{M} \models F[a_1, \ldots, a_m]$ *slijedi* $\mathfrak{N} \models F[b_1, \ldots, b_m]$, *onda vrijedi i* $\mathfrak{N} \models \varphi[b_1, \ldots, b_m]$

Kriterij za eliminaciju kvantifikatora

Zatim se dokaže da iz tvrdnje b) teorema slijedi tvrdnja (2) leme.

Za taj dokaz je ključno sljedeće poopćenje leme o dijagramu:

Lema

Neka je $\mathfrak{M}$ σ-struktura i $X \subseteq |\mathfrak{M}|$ koji generira $\mathfrak{M}$. Neka je

$$\Delta_X(\mathfrak{M}) := \{F : F \textit{ otvorena } \sigma_X\textit{-formula}\,,\ \mathfrak{M}_X \models F\}.$$

Tada $\mathfrak{M}$ možemo smjestiti u σ-strukturu $\mathfrak{N}$ ako i samo ako postoji ekspanzija od $\mathfrak{N}$ koja je model za skup formula $\Delta_X(\mathfrak{M})$.

Kriterij za eliminaciju kvantifikatora

Kako iz ranije leme slijedi (1), preostaje dokazati da (1) povlači a).

Promotrimo sva tri slučaja iz (1).

- ako $T \models \forall x_1 \cdots \forall x_n F$, onda za otvorenu formulu $G := (x_1 = x_1)$ vrijedi $T \models \forall x_1 \cdots \forall x_n (F \leftrightarrow G)$
- ako $T \models \forall x_1 \cdots \forall x_n \neg F$, onda za $G := \neg(x_1 = x_1)$ vrijedi $T \models \forall x_1 \cdots \forall x_n (F \leftrightarrow G)$
- ako postoje otvorene formule $\varphi_1, \ldots, \varphi_k \in S$ takve da je $T \models \forall x_1 \cdots \forall x_m \big(F \leftrightarrow (\varphi_1 \wedge \cdots \wedge \varphi_k)\big)$, onda je $(\varphi_1 \wedge \cdots \wedge \varphi_k)$ tražena formula $\square$

Napomena

Uvjet b) iz prethodnog teorema ekvivalentan je s tvrdnjom:

> *ako su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za T, $\mathfrak{M}_0 \subseteq \mathfrak{M}$ i $\mathfrak{M}_0 \subseteq \mathfrak{N}$, onda za sve $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ iz $\mathfrak{M} \models F[a_1, \ldots, a_n]$ slijedi $\mathfrak{N} \models F[a_1, \ldots, a_n]$.*

Eliminacija kvantifikatora i modelna potpunost

Teorem

Ako teorija T dopušta eliminaciju kvantifikatora, onda je ona modelno potpuna.

Dokaz.

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli za T takvi da je $\mathfrak{M} \subseteq \mathfrak{N}$. Treba dokazati $\mathfrak{M} \prec \mathfrak{N}$. Inkluzija $f : |\mathfrak{M}| \to |\mathfrak{N}|$ je injektivni jaki homomorfizam.

Treba još vidjeti da za svaku formulu F i za sve $a_1, \ldots, a_n \in |\mathfrak{M}|$ vrijedi $\mathfrak{M} \models \varphi[a_1, \ldots, a_n]$ ako i samo ako $\mathfrak{N} \models \varphi[a_1, \ldots, a_n]$.

Kako T dopušta eliminaciju kvantifikatora, tvrdnju je dovoljno dokazati za otvorene formule, no za takve formule ona vrijedi jer se radi o jakom homomorfizmu. $\square$

Potpunost i modelna potpunost

Primjer

Teorija gustih linearnih uređaja s rubovima, $Th(\mathbb{N}, s)$, gdje je s funkcija sljedbenika, $Th(\mathbb{N}, <)$ i $Th(\mathbb{N}, 0, s, +, \cdot, <)$ su potpune, ali nisu modelno potpune. S druge strane, dokazat ćemo da je teorija ACF modelno potpuna, a ranije smo vidjeli da nije potpuna.

Definicija

Za model $\mathfrak{B}$ teorije T kažemo da je **osnovni model** *teorije T ako u svakom modelu od T postoji podmodel izomorfan s $\mathfrak{B}$.*

Teorem

Ako je T modelno potpuna i ima osnovni model, onda je potpuna.

Dokaz.

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli teorije T, i $\mathfrak{B}$ njen osnovni model.
Tada postoje $\mathfrak{M}'$ i $\mathfrak{N}'$ takvi da je $\mathfrak{B} \simeq \mathfrak{M}' \subseteq \mathfrak{M}$ i $\mathfrak{B} \simeq \mathfrak{N}' \subseteq \mathfrak{N}$.

Iz modelne potpunosti slijedi $\mathfrak{M}' \prec \mathfrak{M}$ i $\mathfrak{N}' \prec \mathfrak{N}$, pa imamo $\mathfrak{M} \succ \mathfrak{M}' \simeq \mathfrak{B} \simeq \mathfrak{N}' \prec \mathfrak{N}$, odnosno $\mathfrak{M} \equiv \mathfrak{M}' \equiv \mathfrak{B} \equiv \mathfrak{N}' \equiv \mathfrak{N}$. $\square$

Teorija obostrano neograničenih gustih linearnih uređaja

Teorem

Teorija eorija obostrano neograničenih gustih linearnih uređaja (DLO) dopušta eliminaciju kvantifikatora.

Korolar

Teorija DLO je modelno potpuna. Posebno, $\mathbb{Q} \prec \mathbb{R}$.

Podsjetimo se, ranije smo vidjeli da je *DLO* i potpuna.

Teorija algebarski zatvorenih polja

Teorem

Teorija ACF dopušta eliminaciju kvantifikatora.

Dokaz.

Prema ranijoj lemi, dovoljno je dokazati da za svaku primitivnu egzistencijalnu formulu s jednim kvantifikatorom postoji otvorena formula njoj ekvivalentna u ACF. Koristit ćemo napomenu nakon teorema o kriteriju za eliminaciju kvantifikatora. Neka je $\psi(x_1, \ldots, x_n, y)$ konjunkcija atomarnih i negacija atomarnih formula. Neka su $\mathfrak{M}$ i $\mathfrak{N}$ algebarski zatvorena polja i $\mathfrak{M}_0$ podmodel i od $\mathfrak{M}$ i od $\mathfrak{N}$. Neka su $a_1, \ldots, a_n \in |\mathfrak{M}_0|$ takvi da $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$. Treba dokazati $\mathfrak{N} \models \exists y \psi[a_1, \ldots, a_n]$. Ako proširimo signaturu od ACF konstantskim simbolima $\overline{a_1}, \ldots, \overline{a_n}$, termi s jednom slobodnom varijablom su polinomi nad $|\mathfrak{M}_0|$, a atomarne formule su oblika $f(x) = 0$, gdje je f polinom. Formula ψ je elementarna konjunkcija, što znači da je $\psi(\overline{a_1}, \ldots, \overline{a_n}, y) = \left(\bigwedge_{i=1}^{m} f_i(y) = 0 \land \bigwedge_{j=1}^{k} g_j(y) \neq 0\right)$ za neke $f_1, \ldots, f_m, g_1, \ldots, g_k \in \mathfrak{M}_0[X]$. ...

Teorija algebarski zatvorenih polja

Nastavak dokaza.
Neka je $\mathfrak{M}_0'$ algebarsko zatvorenje od $\mathfrak{M}_0$. Tada je $\mathfrak{M}_0' \subseteq \mathfrak{M}$ i $\mathfrak{M}_0' \subseteq \mathfrak{N}$. Promotrimo slučaj kad postoji $i_0 \in \{1, \ldots, m\}$ takav da f_{i_0} nije nul-polinom. Zbog $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$, postoji $b \in |\mathfrak{M}|$ takav da $\mathfrak{M} \models (\bigwedge_{i=1}^{m} f_i(y) = 0 \wedge \bigwedge_{j=1}^{k} g_j(y) \neq 0)[b]$. Posebno, $f_{i_0}(b) = 0$. Stoga je $b \in |\mathfrak{M}_0'|$. Kako je $\mathfrak{M}_0' \subseteq \mathfrak{M}$ i ψ otvorena, vrijedi i $\mathfrak{M}_0' \models \psi[b]$. Kako je $\mathfrak{M}_0' \subseteq \mathfrak{N}$, zaključujemo $b \in |\mathfrak{N}|$ i stoga $\mathfrak{N} \models \psi[b]$ jer je $\mathfrak{M}_0' \subseteq \mathfrak{N}$ i ψ otvorena.

Preostaje slučaj kad su svi f_i nul-polinomi. Iz $\mathfrak{M} \models \exists y \psi[a_1, \ldots, a_n]$ slijedi $\mathfrak{M} \models \exists y (\bigwedge g_j(y) \neq 0)$, pa nijedan g_j nije nul-polinom. Postoji konačan $S \subseteq |\mathfrak{M}_0'|$ koji sadrži sve nultočke svih g_j.

Kako je svako algebarski zatvoreno polje beskonačno, postoji $b \in |\mathfrak{M}_0'| \setminus S$. Posebno, $b \in |\mathfrak{N}|$. Kako je $\mathfrak{M}_0' \models (\bigwedge g_j(y) \neq 0)[b]$, odnosno $\mathfrak{M}_0' \models \psi[b]$, te $\mathfrak{M}_0' \subseteq \mathfrak{N}$ i $\psi(y)$ otvorena, zaključujemo $\mathfrak{N} \models \psi[a_1, \ldots, a_n, b]$. $\square$

Hilbertov Nullstellensatz

Primjenom modelne potpunosti teorije ACF može se dokazati Hilbertov Nullstellensatz. Potrebni pojmovi i rezultati iz algebre:

- ako je R prsten i $I \subseteq R$, kažemo da je I **ideal** ako je $(I, +)$ grupa, $R \cdot I \subseteq I$ i $I \cdot R \subseteq I$
- $\{0\}$ i R su (**trivijalni**) ideali, ostali su **pravi ideali**
- $m\mathbb{Z}$ je ideal u prstenu $\mathbb{Z}$ za svaki $m \in \mathbb{Z}$
- **prosti ideal** je pravi ideal u kojem $x \cdot y \in I \Rightarrow x \in I \vee y \in I$
- ako je R komutativni prsten s jedinicom i $(I, +)$ aditivna podgrupa, onda je I ideal ako i samo ako $I \cdot R = I$
- u prstenu s jedinicom, ideal I je pravi ako i samo ako $1 \notin I$
- pravi ideal I je prost ako i samo ako je $R/_I$ integralna domena
- za pravi ideal I u prstenu R kažemo da je **maksimalni ideal** ako ne postoji pravi ideal I' u R takav da je $I \subset I'$
- svaki maksimalni ideal je prost (obrat općenito ne vrijedi)
- za svaki pravi ideal postoji maksimalni ideal koji ga sadrži

Hilbertov Nullstellensatz

- ako je R komutativan prsten s jedinicom i $a \in R$, $I(a) = \{ax : x \in R\}$ je ideal (**glavni ideal generiran s** a)
- $I(a_1, \ldots, a_n) = \{a_1 x_1 + \cdots + a_n x_n : x_1, \ldots, x_n \in R\}$ je **konačno generiran**: najmanji ideal u R koji je $\supseteq \{a_1, \ldots, a_n\}$
- prsten je **Noetherin** ako mu je svaki ideal konačno generiran
- svako polje je Noetherin prsten
- **Hilbertov teorem o bazi**: ako je R Noetherin prsten, onda je $R[X_1, \ldots, X_n]$ također Noetherin prsten

Primjer

Neka su $f_1, \ldots, f_k \in R := \mathbb{C}[X_1, \ldots, X_n]$. Koji su nužni i dovoljni uvjeti da ti polinomi imaju zajedničku nultočku?
Ako postoje $g_1, \ldots, g_n \in R$ takvi da je $f_1 g_1 + \cdots + f_n g_n = 1$ ($I(f_1, \ldots, f_n) = R$), onda očito ne postoji zajednička nultočka.

Po Hilbertovu Nullstellensatzu, vrijedi i obrat.

Hilbertov Nullstellensatz

Teorem (Hilbertov Nullstellensatz)

Ako je F algebarski zatvoreno polje i $I \subseteq F[X_1, \ldots, X_n]$ pravi ideal, tada postoji $\vec{a} \in F^n$ tako da za svaki $f \in I$ vrijedi $f(\vec{a}) = 0$.

Dokaz.

Neka je $J \subseteq F[X_1, \ldots, X_n]$ maksimalni ideal koji sadrži I. Tada je $F[X_1, \ldots, X_n]/_J$ polje. Neka je K njegovo algebarsko zatvorenje. Identifikacijom $a \mapsto a + J$ možemo smatrati $F \subseteq K$. Kako je ACF modelno potpuna, slijedi $F \prec K$. Iz Hilbertova teorema o bazi slijedi da postoje $g_1, \ldots, g_m \in J$ takvi da je $J = I(g_1, \ldots, g_m)$. Neka je $G := \exists x_1 \cdots \exists x_n \big(\bigwedge_{i=1}^m g_i(x_1, \ldots, x_n) = 0\big)$. Kako za svaki $i \in \{1, \ldots, m\}$ vrijedi $g_i(X_1 + J, \ldots, X_n + J) = g_i + J = 0$, a K je algebarsko zatvorenje od $F[X_1, \ldots, X_n]/_J$, imamo $K \models G$. Sada iz $F \prec K$ slijedi $F \models G$. Neka je $\vec{a} \in F^n$ takva da vrijedi $g_1(\vec{a}) = \cdots = g_m(\vec{a}) = 0$. Svaki $f \in I \subseteq J = I(g_1, \ldots, g_m)$ je oblika $f = g_1 h_1 + \cdots + g_m h_m$ za $h_1, \ldots, h_m \in F[X_1, \ldots, X_n]$. Sada iz $g_1(\vec{a}) = \cdots = g_m(\vec{a}) = 0$ slijedi $f(\vec{a}) = 0$. $\square$

Hilbertov sedamnaesti problem

Za racionalnu funkciju $f = \frac{g}{h}$ nad $\mathbb{R}$ kažemo da je **pozitivno semidefinitna** ako za svaki $x \in \mathbb{R}$ iz $h(x) \neq 0$ slijedi $f(x) \geq 0$.

Hilbertov 17. problem

Može li se svaka pozitivno semidefinitna racionalna funkcija nad $\mathbb{R}$ zapisati kao konačna suma kvadrata racionalnih funkcija?

Primjer (Motzkinov polinom)

Analogni problem za polinome ima negativan odgovor: polinom $p(x,y) := 1 + x^4 \cdot y^2 + x^2 \cdot y^4 - 3x^2 \cdot y^2$ je pozitivno semidefinitan.

Naime, iz nejednakosti aritmetičke i geometrijske sredine slijedi:

$$\frac{1 + x^4 \cdot y^2 + x^2 \cdot y^4}{3} \geq \sqrt[3]{1 \cdot (x^4 y^2) \cdot (x^2 y^4)} = x^2 y^2,$$

pa je $p(x,y) \geq 0$, za sve $x, y \in \mathbb{R}$. No (to nećemo dokazivati!), p se ne može napisati kao konačan zbroj kvadrata polinoma nad $\mathbb{R}$.

Teorija realno zatvorenih uređenih polja

Rješenje 17. Hilbertova problema proizlazi iz činjenice da teorija realno zatvorenih uređenih polja dopušta eliminaciju kvantifikatora. Signaturi teorije polja dodajemo dvomjesni relacijski simbol $<$, a aksiomima polja dodajemo uređajnu linearnost i kompatibilnost s operacijama, čime dobivamo teoriju **uređenih polja**.

Uređeno polje K ima **svojstvo srednje vrijednosti** za polinom $f(X) \in K[X]$ ako za sve $a, b \in K$ takve da je $a < b$ i $f(a) < 0 < f(b)$ postoji $c \in K$ za koji je $a < c < b$ i $f(c) = 0$.

Uređeno polje K je **realno zatvoreno** ako ima svojstvo srednje vrijednosti za svaki polinom $f(X) \in K[X]$.

Primjer

- $\mathbb{R}$ je realno zatvoreno uređeno polje (pišemo $\mathbb{R} \models RCOF$)
- $\mathbb{A} \models RCOF$ ($\mathbb{A}$ je skup algebarskih realnih brojeva)
- $\mathbb{Q} \not\models RCOF$: nema svojstvo srednje vrijednosti za $x^2 - 2$
- $\mathbb{C} \not\models RCOF$ jer uopće nije OF :-) (iako jest CF)

Teorija realno zatvorenih uređenih polja

Zaključujemo rezultatima koje nećemo dokazivati.

Teorem

Teorija realno zatvorenih uređenih polja RCOF dopušta eliminaciju kvantifikatora.

Korolar

RCOF je modelno potpuna.

Teorem (Artinovo rješenje 17. Hilbertova problema)

Neka je F polje $\mathbb{R}$ ili $\mathbb{Q}$.

Tada se svaka pozitivno semidefinitna racionalna funkcija nad F može zapisati kao zbroj kvadrata racionalnih funkcija nad F.

Skup formula konzistentan s teorijom modela

Neke oznake i pojmovi:

- $\Gamma(x)$: 1-tip, odnosno skup formula
  u kojima samo varijabla x može imati slobodan nastup
- za σ-strukturu $\mathfrak{M}$, skup σ-rečenica $Th(\mathfrak{M}) = \{F : \mathfrak{M} \models F\}$
  zovemo **teorija modela** $\mathfrak{M}$
- $\Gamma(x)$ je **konzistentan s** $Th(\mathfrak{M})$ ako postoji σ-struktura
  $\mathfrak{N} \equiv \mathfrak{M}$ i postoji $a \in |\mathfrak{N}|$ takav da vrijedi $\mathfrak{N} \models \Gamma[a]$
  (tip $\Gamma(x)$ je konzistentan u odnosu na potpunu teoriju $Th(\mathfrak{M})$)

Propozicija

$\Gamma(x)$ *je konzistentan s teorijom modela* $\mathfrak{M}$ *ako i samo ako za svaki konačan* $\Delta(x) \subseteq \Gamma(x)$ *postoji* $a \in |\mathfrak{M}|$ *takav da vrijedi* $\mathfrak{M} \models \Delta[a]$.

Saturirana struktura

Neka je $\mathfrak{M}$ σ-struktura i $A \subseteq |\mathfrak{M}|$, te $\sigma_A = \sigma \cup \{\overline{a} : a \in A\}$, tako da $a_1 \neq a_2$ povlači $\overline{a_1} \neq \overline{a_2}$. S $\mathfrak{M}_A$ označavamo σ_A-ekspanziju od $\mathfrak{M}$ takvu da je $\overline{a}$ interpretiran s a za svaki $a \in A$.

Definicija

*Neka je λ kardinalni broj. Kažemo da je σ-struktura $\mathfrak{M}$ λ-**saturirana** ako za svaki $A \subseteq |\mathfrak{M}|$ takav da je $\operatorname{card} A < \lambda$, i za svaki skup σ_A-formula $\Gamma(x)$, vrijedi:*
ako je $\Gamma(x)$ konzistentan s teorijom modela $\mathfrak{M}_A$,
onda postoji $b \in |\mathfrak{M}_A| = |\mathfrak{M}|$ takav da $\mathfrak{M}_A \models \Gamma(x)[b]$
(svaki 1-tip konzistentan u odnosu na $Th(\mathfrak{M}_A)$ je realiziran u $\mathfrak{M}_A$).

Za ω_1-saturiranu σ-strukturu, gdje je ω_1 najmanji neprebrojivi kardinalni broj, kažemo i da je **prebrojivo saturirana**.

Primjeri i protuprimjeri prebrojivo saturiranih struktura

Primjer

Svaka konačna struktura je prebrojivo saturirana
(jer za konačne strukture „$\equiv$" povlači „$\cong$")

Primjer

$(\mathbb{Q}, <, =)$ jest prebrojivo saturiran
(dokaz primjenom teorema o uređajnoj karakterizaciji skupa $\mathbb{Q}$)

Primjer

$(\mathbb{N}, <, =)$ nije prebrojivo saturiran: promotrimo skup formula

$$\begin{aligned}\Gamma(x) := \{&\exists y_1\,(y_1 < x),\\ &\exists y_1\,\exists y_2\,(y_1 < y_2 < x),\\ &\exists y_1\,\exists y_2\,\exists y_3\,(y_1 < y_2 < y_3 < x), \ldots\}.\end{aligned}$$

Svaki je konačan podskup od $\Gamma(x)$ realiziran na $(\mathbb{N}, <, =)$,
no čitav skup $\Gamma(x)$ nije realiziran na $(\mathbb{N}, <, =)$.

Kardinalnost saturiranih struktura

Propozicija

Ne postoji prebrojiva, prebrojivo saturirana σ-struktura.

Dokaz.

Pretpostavimo da je $|\mathfrak{M}|$ prebrojiv.
Tada je svaki konačan podskup od $\Gamma(x) = \{x \neq \bar{a} : a \in |\mathfrak{M}|\}$ realiziran u $\mathfrak{M}_{|\mathfrak{M}|}$.
Po pretpostavci je $|\mathfrak{M}|$ prebrojiv i $\mathfrak{M}$ prebrojivo saturiran, pa je $\Gamma(x)$ realiziran u $\mathfrak{M}_{|\mathfrak{M}|}$, što je očito nemoguće. $\square$

Isti dokaz (za λ umjesto ω_1) pokazuje da vrijedi:

Propozicija

Ako je $\mathfrak{M}$ beskonačna λ-saturirana struktura, onda je $\operatorname{card} \mathfrak{M} \geq \lambda$.

Definicija

„$\mathfrak{M}$ je **saturirana**” *znači da je $\mathfrak{M}$* $(\operatorname{card} |\mathfrak{M}|)$*-saturirana.*

Egzistencija prebrojivo saturiranih struktura

Teorem

Svaki ultraprodukt nad prebrojivo nepotpunim ultrafilterom je prebrojivo saturiran.

Dokaz.

Neka je $\{\mathfrak{M}_i : i \in I\}$ familija σ-struktura i U prebrojivo nepotpun ultrafilter nad I. Neka je $A = \{(a_k)_U : k \in \mathbb{N}\}$ niz u $\prod_U \mathfrak{M}_i$ i $\Gamma(x)$ skup σ_A-formula čiji je svaki konačan podskup realiziran u $(\prod_U \mathfrak{M}_i)_A$. Treba dokazati da je $\Gamma(x)$ realiziran u $(\prod_U \mathfrak{M}_i)_A$.

Označimo $A_i = \{a_k(i) : k \in \mathbb{N}\}$ i uočimo $(\prod_U \mathfrak{M}_i)_A = \prod_U (\mathfrak{M}_i)_{A_i}$. Stoga je dovoljno dokazati: ako je svaki konačan podskup skupa σ_A-formula $\Gamma(x)$ realiziran u σ_A-strukturi $\prod_U \mathfrak{M}_i$, onda je $\Gamma(x)$ realiziran u $\prod_U \mathfrak{M}_i$. Neka je $\Gamma(x) = \{\varphi_1(x), \varphi_2(x), \ldots\}$, i označimo $\psi_n(x) := \bigwedge_{i=1}^n \varphi(x)$ („parcijalne konjunkcije").

Kako je U prebrojivo nepotpun, postoji niz (Y_n) u U takav da je $I = Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq \cdots$ i $\bigcap_n Y_n = \emptyset$. Definiramo niz u $\mathcal{P}(I)$ s $X_0 := I$, te $X_n := \{i \in Y_n : \mathfrak{M}_i \models \exists x \psi_n(x)\}$ za sve $n \in \mathbb{N}_+$. $\cdots$

Egzistencija prebrojivo saturiranih struktura

Nastavak dokaza.
Iz pretpostavke slijedi $\prod_U \mathfrak{M}_i \models \exists x \psi_n(x)$ za svaki $n \in \mathbb{N}_+$. Stoga $\{i \in I : \mathfrak{M}_i \models \exists x \psi_n(x)\} \in U$ (i $Y_n \in U$), pa je (X_n) niz u U.

Očito $\bigcap_n X_n = \emptyset$ i $X_0 \supseteq X_1 \supseteq X_2 \supseteq \ldots$.
Dakle, za svaki $i \in I$ postoji najveći $n(i) \in \mathbb{N}$ takav da je $i \in X_{n(i)}$.

Definiramo $f : I \to \bigcup_i |\mathfrak{M}_i|$ (funkcija izbora!), tako da svaki $i \in I$ preslikamo u neki $a \in |\mathfrak{M}_i|$ takav da $\mathfrak{M}_i \models \psi_{n(i)}(x)[a]$. Specijalno, $\psi_0(x) = \top$, pa ako je $n(i) = 0$ uzmemo bilo koji element od $|\mathfrak{M}_i|$.

Posebno, za svaki $n \in \mathbb{N}_+$ i za svaki $i \in X_n$ vrijedi $\mathfrak{M}_i \models \varphi_n[f(i)]$ (jer ψ_n povlači φ_n). Dakle, $\{i \in I : \mathfrak{M}_i \models \varphi_n[f(i)]\} \supseteq X_n \in U$, pa je $\prod_U \mathfrak{M}_i \models \varphi_n\big[[f]_U\big]$.
Time smo dokazali $\prod_U \mathfrak{M}_i \models \Gamma(x)\big[[f]_U\big]$. $\square$

Teorem o jedinstvenosti za saturirane strukture

Teorem

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ saturirane σ-strukture iste kardinalnosti.

Ako su $\mathfrak{M}$ i $\mathfrak{N}$ elementarno ekvivalentne, onda su i izomorfne.

Dokaz.

Tvrdnju dokazujemo samo za prebrojive $\mathfrak{M}$ i $\mathfrak{N}$. Neka je $|\mathfrak{M}| = \{m_0, m_1, \dots\}$ i $|\mathfrak{N}| = \{n_0, n_1, \dots\}$. Definirat ćemo nizove (a_n) u $|\mathfrak{M}|$ i (b_n) u $|\mathfrak{N}|$. Stavimo $a_0 := m_0$ i promotrimo tip $t(a_0/\mathfrak{M}) = \{F(x) : \mathfrak{M} \models F[a_0]\}$. Kako je $\mathfrak{M} \models t(a_0/\mathfrak{M})[a_0]$ i $\mathfrak{M} \equiv \mathfrak{N}$, tip $t(a_0/\mathfrak{M})$ je konzistentan s teorijom modela $\mathfrak{N}$. Zbog saturiranosti tada postoji $b_0 \in |\mathfrak{N}|$ takav da $\mathfrak{N} \models t(a_0/\mathfrak{M})[b_0]$. $\dots$

Teorem o jedinstvenosti za saturirane strukture

Dokaz.

Lako se vidi $\mathfrak{M}_{\{a_0\}} \equiv \mathfrak{N}_{\{b_0\}}$.

Pretpostavimo da su definirani $a_0, \ldots, a_{n-1}$ i $b_0, \ldots, b_{n-1}$ takvi da je $\mathfrak{M}_{\{a_0,\ldots,a_{n-1}\}} \equiv \mathfrak{N}_{\{b_0,\ldots,b_{n-1}\}}$.

Ako je n paran, a_n i b_n definiramo ovako: neka je $k_0 = \min\big\{k : m_k \in |\mathfrak{M}| \setminus \{a_0, \ldots, a_{n-1}\}\big\}$. Definiramo $a_n = m_{k_0}$.
Tip $T_n = t(a_n/\mathfrak{M}_{\{a_0,\ldots,a_{n-1}\}})$ je očito konzistentan s teorijom ω_1-saturiranog modela $\mathfrak{N}_{\{b_0,\ldots,b_{n-1}\}}$.
Stoga postoji $b_n \in |\mathfrak{N}| \setminus \{b_0, \ldots, b_{n-1}\}$ takav da $\mathfrak{N}_{\{b_0,\ldots,b_{n-1}\}} \models T_n[b_n]$ i $\mathfrak{M}_{\{a_0,\ldots,a_{n-1},a_n\}} \equiv \mathfrak{N}_{\{b_0,\ldots,b_{n-1},b_n\}}$.

U slučaju neparnog n postupa se analogno, s tim da prvo biramo $b_n \in |\mathfrak{N}| \setminus \{b_0, \ldots, b_{n-1}\}$ s najmanjim indeksom, a zatim a_n tako da se realizira odgovarajući tip T'_n.
Lako se vidi da je $\{a_n \mapsto b_n\}_n$ izomorfizam struktura $\mathfrak{M}$ i $\mathfrak{N}$. $\square$

Svojstva *back* i *forth*

Definicija

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ σ-strukture.
Neka je I skup parcijalnih izomorfizama između $\mathfrak{M}$ i $\mathfrak{N}$.
Kažemo da I ima svojstvo:

forth *ako za svaki $p \in I$ i svaki $a \in |\mathfrak{M}|$ postoji $q \in I$ takav da je $p \subseteq q$ i $a \in Dom(q)$;*

back *ako za svaki $p \in I$ i svaki $b \in |\mathfrak{N}|$ postoji $q \in I$ takav da je $p \subseteq q$ i $b \in Rng(q)$.*

Teorem

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 svojstva back i forth.*

Modalna logika: sintaksa

Alfabet modalne logike proširuje alfabet logike sudova:

- prebrojiv skup propozicijskih varijabli $\Phi = \{p, q, p_1, p_2, \dots\}$
- logički veznici $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$ (dovoljno: $\to$)
- logičke konstante $\top$, $\bot$ (dovoljno: $\bot$)
- modalni operatori $\Box$, $\Diamond$ (dovoljno: jedno od to dvoje)

Modalna formula je svaka riječ generirana gramatikom

$$F \to p \mid \top \mid \bot \mid \neg F \mid (F_1 \circ F_2) \mid \Box F \mid \Diamond F,$$

gdje je $p \in \Phi$, a $\circ \in \{\wedge, \vee, \to, \leftrightarrow\}$.
Brojne su intendirane interpretacije formula oblika $\Box A$, primjerice:

- Nužno vrijedi A.
- Agent zna da vrijedi A. (*epistemička logika*)
- Agent vjeruje da vrijedi A.
- Dokazivo je A. (*logika dokazivosti*)

Zadatak: Izrazite sve ostalo pomoću $\to$, $\bot$ i $\Diamond$!

Modalna logika: sistemi

Aksiomi sistema **K** su sve tautologije (u proširenom jeziku! npr. $\Box p \vee \neg \Box p$) i

$$\Box(A \to B) \to (\Box A \to \Box B).$$

Pravila izvoda su modus ponens i generalizacija: iz A zaključi $\Box A$. Skup **teorema** sistema **K** je najmanji skup formulā koji sadrži sve aksiome i zatvoren je na pravila izvoda.

„Formula A je teorem sistema **K**" pišemo $\vdash A$.

Ovisno o intendiranoj interpretaciji, različite modalne sisteme dobivamo dodavanjem jednog ili više drugih aksioma, kao što su:

- $\Box A \to A$ („Ako agent zna A, onda vrijedi A.")
- $\Box A \to \Box\Box A$ (*pozitivna introspekcija*)
- $\neg\Box A \to \Box\neg\Box A$ (*negativna introspekcija*)
- $\Box(\Box A \to A) \to \Box A$ (*Löbova formula*)

Semantika

Kripkeove strukture:

- okvir $\mathfrak{F} = (W, R)$, $W \neq \emptyset$ svjetovi, $R \subseteq W \times W$ dostiživost
- model $\mathfrak{M} = (\mathfrak{F}, V)$, $V : \Phi \to \mathcal{P}(W)$ $[\Vdash \subseteq W \times \Phi]$ valuacija
- točkovni model $(\mathfrak{M}, w)$, gdje je $w \in W$

Istinitost formule u točkovnom modelu:

- $\mathfrak{M}, w \Vdash p$ znači $w \in V(p)$, za sve $p \in \Phi$
- $\mathfrak{M}, w \Vdash \bot$ nikad (pišemo $\mathfrak{M}, w \nVdash \bot$)
- $\mathfrak{M}, w \Vdash (\varphi \to \psi)$ znači da je $\mathfrak{M}, w \nVdash \varphi$ ili $\mathfrak{M}, w \Vdash \psi$
- $\mathfrak{M}, w \Vdash \Diamond\varphi$ znači da postoji v takav da je $w\,R\,v$ i $\mathfrak{M}, v \Vdash \varphi$

Valjanost i ispunjivost:

- globalna istinitost: $\mathfrak{M} \Vdash \varphi$ znači: $\mathfrak{M}, w \Vdash \varphi$ za sve $w \in W$
- valjanost na okviru: $\mathfrak{F} \Vdash \varphi$ znači: $(\mathfrak{F}, V) \Vdash \varphi$ za sve valuacije
- valjanost: $\Vdash \varphi$ znači $\mathfrak{F} \Vdash \varphi$ za svaki okvir $\mathfrak{F}$
- ispunjivost: „φ je ispunjiva" znači da postoji točkovni model $(\mathfrak{M}, w) = (W, R, V, w)$ takav da vrijedi $\mathfrak{M}, w \Vdash \varphi$

Istinitost, valjanost, ispunjivost

Primjer

- $\mathfrak{M}_1 = (\mathbb{N}, <, V_1),\ V_1(p) = \emptyset$ za sve $p \in \Phi$
  - $\mathfrak{M}_1 \Vdash \Diamond\neg p$ za sve $p \in \Phi$
  - $\mathfrak{M}_1 \Vdash \Box\neg p$ za sve $p \in \Phi$
- $\mathfrak{M}_2 = (\mathbb{N}, <, V_2),\ V_2(p_i) = \{i\}$ za sve $p_i \in \Phi$
  - $\mathfrak{M}_2 \Vdash \Diamond\neg p$ za sve $p \in \Phi$
  - $\mathfrak{M}_2, 1 \Vdash \Diamond p_2$
  - $\mathfrak{M}_2, 1 \nVdash \Box\neg p_2$
  - $\mathfrak{M}_2 \nVdash \Box\neg p_2$
  - $\mathfrak{M}_2, i \Vdash \Box\neg p_i$
- $\mathfrak{M} = (W, R, V)$, gdje je
  - $W = \mathcal{P}(\Phi)$ (epistemičke alternative ili moguća stanja stvari)
  - R relacija ekvivalencije na W (*indistinguishability*)
  - $w \in V(p)$ ako i samo ako $p \in w$ (kanonska valuacija)
  - $\mathfrak{M}, \{p\} \Vdash p$
  - $\mathfrak{M} \Vdash p \to \Diamond p$
  - $\mathfrak{M} \Vdash \Diamond\Diamond p \to \Diamond p$

Istinitost, valjanost, ispunjivost

Primjer

Neka je $\mathfrak{F}$ Kripkeov okvir, s relacijom dostiživosti R. Tada:

- $\Vdash \Box(p \to q) \to (\Box p \to \Box q)$
- $\nVdash \Box p \to p$, ali $\mathfrak{F} \Vdash \Box p \to p$ ako je R refleksivna („ako agent zna p, onda vrijedi p");
- $\mathfrak{F} \Vdash \Box p \to \Box\Box p$ ako je R tranzitivna (*pozitivna introspekcija*);
- $\mathfrak{F} \Vdash \neg\Box p \to \Box\neg\Box p$ ako je R euklidska: $w\,R\,u$ i $w\,R\,v$ povlači $u\,R\,v$ (*negativna introspekcija*);
- $\mathfrak{F} \Vdash \Box(\Box p \to p) \to \Box p$ (*Löbova formula*) ako je R tranzitivna i inverzno dobro utemeljena (ne postoji beskonačni lanac $w_1\ R\ w_2\ R\ w_3\ R \cdots$).

Vrijede i obrati, npr. ako $\mathfrak{F} \Vdash \Box p \to p$, onda je R refleksivna. Pritom kažemo da formula $\Box p \to p$ *definira* refleksivnost.

Modalna definabilnost

Neka je Σ skup modalnih formula. Pišemo $\mathfrak{M}, w \Vdash \Sigma$ ako $\mathfrak{M}, w \Vdash \varphi$ za sve $\varphi \in \Sigma$ (slično $\mathfrak{M} \Vdash \Sigma$, ili $\mathfrak{F} \Vdash \Sigma$).

Označimo:

$$
\begin{aligned}
Mod_l(\Sigma) &:= \{(\mathfrak{M}, w) : \mathfrak{M}, w \Vdash \Sigma\} \\
Mod_g(\Sigma) &:= \{\mathfrak{M} : \mathfrak{M} \Vdash \Sigma\} \\
Fr(\Sigma) &:= \{\mathfrak{F} : \mathfrak{F} \Vdash \Sigma\}
\end{aligned}
$$

$Mod_l(\varphi)$ označava $Mod_l(\{\varphi\})$, i analogno za Mod_g i Fr.

Kažemo da Σ **definira** klasu točkovnih modela $\mathcal{K}. := Mod_l(\Sigma)$. Slično, kažemo da Σ definira klasu modela $\mathcal{K} := Mod_g(\Sigma)$, a da Σ definira klasu okvira $\mathcal{K}'$ ako je $\mathcal{K}' = Fr(\Sigma)$.

Modalna definabilnost

Kažemo da Σ definira svojstvo struktura ako definira klasu svih struktura s tim svojstvom (recimo, kažemo da $(\Box p \to p)$ definira refleksivnost jer definira klasu svih refleksivnih okvira).

Definicija

Kažemo da je klasa (svojstvo) struktura **modalno definabilna** *ako postoji skup modalnih formula koji je definira.*

Primjer

- $(\Box p \to p)$ i $(p \to \Diamond p)$ definiraju refleksivnost okvira.
- $(\Box p \to \Box\Box p)$ i $(\Diamond\Diamond p \to \Diamond p)$ definiraju tranzitivnost okvira.
- $(\Diamond p \to \Box\Diamond p)$ definira klasu svih euklidskih okvira.
- Löbova formula $\big(\Box(\Box p \to p) \to \Box p\big)$ definira klasu svih tranzitivnih i inverzno dobro utemeljenih okvira.

Bisimulacija

Bisimulacija je osnovna ekvivalencija među Kripkeovim modelima.

Definicija

Neka su $\mathfrak{M} = (W, R, V)$ *i* $\mathfrak{M}' = (W', R', V')$ *modeli.*
Bisimulacija *je relacija* $Z \subseteq W \times W'$ *koja ima sljedeća svojstva:*

(at) *ako* $w \, Z \, w'$*, onda za sve* $p \in \Phi$ *vrijedi:*
$\mathfrak{M}, w \Vdash p$ *ako i samo ako* $\mathfrak{M}', w' \Vdash p$*;*

(forth) *ako* $w \, Z \, w'$ *i* $w \, R \, v$*, onda*
postoji $v' \in W'$ *za koji vrijedi* $w' \, R' \, v'$ *i* $v \, Z \, v'$*;*

(back) *ako* $w \, Z \, w'$ *i* $w' \, R' \, v'$*, onda*
postoji $v \in W$ *za koji vrijedi* $w \, R \, v$ *i* $v \, Z \, v'$*.*

Propozicija

Ako vrijedi $w \, Z \, w'$*, onda vrijedi* $\mathfrak{M}, w \Vdash \varphi$ *ako i samo ako* $\mathfrak{M}', w' \Vdash \varphi$*, za svaku modalnu formulu* φ*.*

Drugim riječima, bisimulirani svjetovi su modalno ekvivalentni, odnosno modalne formule su invarijantne na bisimulacije.

Dokazivanje nedefinabilnosti

Primjer

Refleksivnost okvira je modalno definabilna, formulom $(\Box p \to p)$.

No, refleksivnost modela nije! Zaista, neka je $\mathcal{K}$ klasa svih modela $\mathfrak{M} = (W, R, V)$ takvih da je R refleksivna. Tada:

- $\mathfrak{M}_1 = (\mathbb{N}, <, V) \notin \mathcal{K}$, gdje je $V(p) = \emptyset$ za sve $p \in \Phi$
- $\mathfrak{M}_2 = \big(\{w\}, \{(w, w)\}, V\big) \in \mathcal{K}$, gdje je V kao gore

No, $\mathbb{N} \times \{w\}$ je očito bisimulacija.

Pretpostavimo da neki skup modalnih formula Σ definira $\mathcal{K}$, odnosno $\mathcal{K} = Mod_g(\Sigma)$. Tada $\mathfrak{M}_2 \Vdash \Sigma$.

No modalne formule su invarijantne na bisimulacije, pa $\mathfrak{M}_1 \Vdash \Sigma$. Dakle, $\mathfrak{M}_1 \in Mod_g(\Sigma) = \mathcal{K}$. Kontradikcija.

Generirani podokvir i generirani podmodel

Definicija

Generirani podmodel *od* $\mathfrak{M} = (W, R, V)$ *je* $\mathfrak{M}' = (W', R', V')$*:*

- $W' \subseteq W$
- $R' = R \cap (W' \times W')$
- $V'(p) = V(p) \cap W'$, *za sve* $p \in \Phi$
- *ako* $w \in W'$ *i* $w \, R \, v$, *onda* $v \in W'$

Generirani podokvir *se definira na isti način, samo bez spominjanja valuacije. Kažemo da je okvir* $\mathfrak{F}$ **generiran svijetom** w *ako je najmanji generirani podokvir od* $\mathfrak{F}$ *koji sadrži* w *upravo* $\mathfrak{F}$*.*

Propozicija

Generirani podmodeli čuvaju istinitost,
a generirani podokviri čuvaju valjanost modalnih formula.

Dokaz.

$\{(w, w) : w \in W'\}$ je bisimulacija između $\mathfrak{M}$ i $\mathfrak{M}'$. $\square$

Disjunktna unija

Definicija

Disjunktna unija *familije modela* $\{\mathfrak{M}_i = (W_i, R_i, V_i) : i \in I\}$ *je model* $\biguplus_{i \in I} \mathfrak{M}_i := (W, R, V)$*, gdje je:*

- $W := \bigcup_{i \in I} W_i \times \{i\}$
- $(w, i)\ R\ (v, j)$ *definirano kao* $i = j \wedge w\ R_i\ v$
- $(w, i) \in V(p)$ *definirano s* $w \in V_i(p)$

Disjunktna unija familije okvira definira se na isti način, samo bez dijela koji se odnosi na valuaciju (treća stavka gore).

Propozicija

Disjunktna unija čuva istinitost i valjanost modalnih formula.

Dokaz.

Neka je $i \in I$. Definiramo $w\ Z_i\ (w, i)$ za sve $w \in W_i$.
Tada je Z_i bisimulacija između $\mathfrak{M}_i$ i $\biguplus_{i \in I} \mathfrak{M}_i$. □

Ograničeni morfizam

Definicija

Neka su $\mathfrak{M} = (W, R, V)$ i $\mathfrak{M}' = (W', R', V')$ modeli.
Ograničeni morfizam *je $f : W \to W'$ koja ima svojstva:*

(at) $\mathfrak{M}, w \Vdash p$ *ako i samo ako* $\mathfrak{M}', f(w) \Vdash p$, *za sve* $p \in \Phi$

(forth) *ako* $w\, R\, v$, *onda* $f(w)\; R'\; f(v)$

(back) *ako* $f(w)\; R'\; v'$, *onda postoji* $v \in W$ *za koji vrijedi* $w\, R\, v$ *i* $f(v) = v'$

Ograničeni morfizam okvira definira se isto, samo bez uvjeta (at).

Propozicija

Surjektivni ograničeni morfizam čuva valjanost modalne formule.

Dokaz.

Graf ograničenog morfizma je bisimulacija. □

Još primjera nedefinabilnosti

Primjer

Nerefleksivnost nije modalno definabilna:
generirani podokvir nerefleksivnog okvira može biti refleksivan.

Primjer

Konačnost nije modalno definabilna: disjunktna unija (beskonačno mnogo) konačnih okvira može biti beskonačna.

Primjer

Irefleksivnost nije modalno definabilna:

- $\mathfrak{F} := \big(\{1,2\},\{(1,2),(2,1)\}\big)$ jest irefleksivan;
- $\mathfrak{F}' := \big(\{3\},\{(3,3)\}\big)$ nije irefleksivan;
- $\{1 \mapsto 3, 2 \mapsto 3\} : \mathfrak{F} \to \mathfrak{F}'$ je surjektivni ograničeni morfizam između njih.

Standardna translacija

Formule modalne logike također se interpretiraju na relacijskim strukturama, nad signaturom $\sigma := \{R^2\} \cup \{P_i^1 : p_i \in \Phi\}$.

Svaki Kripkeov model $\mathfrak{M} = (W, R, V)$ se može shvatiti kao σ-struktura, uz $R^{\mathfrak{M}} = R$ i $P_i^{\mathfrak{M}} = V(p_i)$ za sve $p_i \in \Phi$.

Standardna translacija modalne formule definira se rekurzivno:

- $ST_x(p_i) := P_i(x)$
- $ST_x(\bot) := (x \neq x)$
- $ST_x(\varphi \to \psi) := \big(ST_x(\varphi) \to ST_x(\psi)\big)$
- $ST_x(\Box\varphi) := \forall y\big(x\,R\,y \to ST_y(\varphi)\big)$, gdje je y nova varijabla

Propozicija

- $\mathfrak{M}, w \Vdash \varphi$ *ako i samo ako* $\mathfrak{M} \models ST_x(\varphi)[w]$;
- $\mathfrak{M} \Vdash \varphi$ *ako i samo ako* $\mathfrak{M} \models \forall x\, ST_x(\varphi)$;
- *Svaka modalno definabilna klasa (točkovnih) modela je elementarna.*

Standardna translacija — primjeri

$$ST_x(\Diamond\top) = \exists y\big(x\,R\,y \wedge ST_y(\top)\big) = \exists y\big(x\,R\,y \wedge y = y\big) \Leftrightarrow$$
$$\Leftrightarrow \exists y(x\,R\,y)$$

$$ST_x(\Box p \to p) = \big(ST_x(\Box p) \to ST_x(p)\big) =$$
$$= \big(\forall y\big(x\,R\,y \to ST_y(p)\big) \to Px\big) = \big(\forall y(x\,R\,y \to Py) \to Px\big)$$

$$ST_x\big(\Box(\Box p \to p) \to \Box p\big) = \big(ST_x\big(\Box(\Box p \to p)\big) \to ST_x(\Box p)\big) =$$
$$= \big(\forall y\big(x\,R\,y \to ST_y(\Box p \to p)\big) \to \forall y\big(x\,R\,y \to ST_y(p)\big)\big) =$$
$$= \big(\forall y\big(x\,R\,y \to (ST_y(\Box p) \to ST_y(p))\big) \to \forall y(x\,R\,y \to Py)\big) =$$
$$= \big(\forall y\big(x\,R\,y \to (\forall z(y\,R\,z \to ST_z(p)) \to Py)\big) \to$$
$$\to \forall y(x\,R\,y \to Py)\big) =$$
$$= \big(\forall y\big(x\,R\,y \to (\forall z(y\,R\,z \to Pz) \to Py)\big) \to \forall y(x\,R\,y \to Py)\big)$$

Van Benthemov teorem karakterizacije

Vidjeli smo da svaka modalna formula ima ekvivalentnu formulu prvog reda na modelima i da obrat ne vrijedi (npr. refleksivnost modela je elementarno svojstvo, ali nije modalno definabilna!)

Pitanje: ako ne sve, koje σ-formule imaju modalni ekvivalent?

Modalne formule su invarijantne na bisimulacije. I njihove su standardne translacije onda invarijantne na bisimulacije:

Definicija

Kažemo da je σ-formula $F(x)$ **invarijantna na bisimulacije** *ako za sve točkovne modele $(\mathfrak{M}, w)$ i $(\mathfrak{M}', w')$ vrijedi: ako postoji bisimulacija Z između $\mathfrak{M}$ i $\mathfrak{M}'$ takva da je $w\,Z\,w'$, tada $\mathfrak{M} \models F(x)[w]$ ako i samo ako $\mathfrak{M}' \models F(x)[w']$.*

Istaknimo bez dokaza:

Teorem (van Benthem)

σ-formula $F(x)$ je ekvivalentna standardnoj translaciji neke modalne formule ako i samo ako je invarijantna na bisimulacije.

Ultrafiltersko proširenje

Definicija

Ultrafiltersko proširenje *modela* $\mathfrak{M} = (W, R, V)$ *je model* $\mathfrak{M}^{\mathfrak{u}} := (W^{\mathfrak{u}}, R^{\mathfrak{u}}, V^{\mathfrak{u}})$, *gdje je*

- $W^{\mathfrak{u}}$ *skup svih ultrafiltera nad* W
- $u\, R^{\mathfrak{u}}\, v$ *znači da za sve* $A \in v$ *vrijedi* $m_{\Diamond}(A) := R^{-1}[A] \in u$, *što je ekvivalentno s* $\{A \subseteq W : m_{\Box}(A) \in u\} \subseteq v$, *gdje je* $m_{\Box}(A) := \{w \in W : R[w] \subseteq A\}$
- $u \in V^{\mathfrak{u}}(p)$ *ako i samo ako* $V(p) \in u$

Indukcijom po složenosti formule dokazuje se:

Propozicija

Za sve φ *vrijedi* $\mathfrak{M}^{\mathfrak{u}}, u \Vdash \varphi$ *ako i samo ako* $V(\varphi) := \{w \in W : \mathfrak{M}, w \Vdash \varphi\} \in u$, *odnosno* $u \in V^{\mathfrak{u}}(\varphi)$ *ako i samo ako* $V(\varphi) \in u$.

Posebno, $(\mathfrak{M}, w)$ *i* $(\mathfrak{M}^{\mathfrak{u}}, w^{\mathfrak{u}})$ *su modalno ekvivalentni, gdje je* $w^{\mathfrak{u}}$ *glavni filter generiran s* w.

Još jedan kriterij za dokazivanje nedefinabilnosti

Ultrafiltersko proširenje okvira $\mathfrak{F} = (W, R)$ je $\mathfrak{F}^{\mathfrak{u}} = (W^{\mathfrak{u}}, R^{\mathfrak{u}})$.

Propozicija

Neka je $\mathfrak{F}$ okvir i φ modalna formula. Ako $\mathfrak{F}^{\mathfrak{u}} \Vdash \varphi$, onda $\mathfrak{F} \Vdash \varphi$.

Dokaz.

Neka je $\mathfrak{M} = (\mathfrak{F}, V)$, gdje je V proizvoljna i neka je $w \in W$. Iz pretpostavke je $\mathfrak{M}^{\mathfrak{u}}, w^{\mathfrak{u}} \Vdash \varphi$, što je ekvivalentno s $\mathfrak{M}, w \Vdash \varphi$. $\square$

Primjer

Neka je $\mathcal{K} := Mod\big(\forall x \exists y (x\ R\ y \land y\ R\ y)\big)$ klasa svih okvira u kojima svaki svijet ima refleksivnog sljedbenika. Tada $(\mathbb{N}, <) \notin \mathcal{K}$, ali $(\mathbb{N}^{\mathfrak{u}}, <^{\mathfrak{u}}) \in \mathcal{K}$ (ultrafilter v dobiven iz Fréchetova filtera sadrži samo beskonačne skupove pa vrijedi $u <^{\mathfrak{u}} v <^{\mathfrak{u}} v$ za svaki ultrafilter u), dakle $\mathcal{K}$ nije modalno definabilna.

Ipak, $\mathcal{K}$ *jest* zatvorena na surjektivne ograničene morfizme, generirane podokvire i disjunktne unije!

Goldblatt–Thomasonov teorem

Teorem

Neka je $\mathcal{K}$ elementarna klasa okvira. Tada je $\mathcal{K}$ modalno definabilna ako i samo ako je zatvorena na disjunktne unije, generirane podokvire i surjektivne ograničene morfizme i „obrnuto zatvorena" na ultrafilterska proširenja: $\mathfrak{F}^{\mathfrak{u}} \in \mathcal{K}$ povlači $\mathfrak{F} \in \mathcal{K}$.

Teorem nećemo detaljno dokazivati.

[Diplomski rad Marka Horvata: Goldblatt–Thomasonov teorem.]

Upoznat ćemo *modalnu saturaciju*, koja se koristi u dokazu.

Modalna saturacija

Podsjetimo se, bisimuliranost povlači modalnu ekvivalenciju.

Obrat općenito ne vrijedi, ali vrijedi za saturirane modele.

Definicija

Neka je $\mathfrak{M} = (W, R, V)$ *model. Kažemo da je skup formula* Σ **ispunjiv u podskupu** $W' \subseteq W$ *ako postoji* $v \in W'$ *takav da vrijedi* $\mathfrak{M}, v \Vdash \Sigma$*. Kažemo da je* Σ **konačno ispunjiv u** W' *ako je svaki njegov konačan podskup ispunjiv u* W'*.*

Kažemo da je model $\mathfrak{M}$ **modalno saturiran** *ako za svaki skup formula* Σ *i za svaki* $w \in W$ *vrijedi: ako je* Σ *konačno ispunjiv u* $R[w]$*, onda je* Σ *ispunjiv u* $R[w]$*.*

Propozicija

Neka su $\mathfrak{M}$ *i* $\mathfrak{N}$ *modalno saturirani modeli te* $w \in |\mathfrak{M}|$ *i* $w' \in |\mathfrak{N}|$*.*

Ako su w *i* w' *modalno ekvivalentni, onda su bisimulirani.*

Dokaz.

Modalna ekvivalentnost je bisimulacija. $\square$

Ultrafiltersko proširenje je modalno saturirano

Propozicija

Ultrafiltersko proširenje svakog modela $\mathfrak{M}$ je modalno saturirano.

Dokaz.

Neka je $u \in W^{\mathfrak{u}}$ i neka je Σ skup formula konačno ispunjiv u $R^{\mathfrak{u}}[u]$.

Stavimo $E = \{V(\varphi) : \varphi \in \Sigma\} \cup \{A \subseteq W : m_{\Box}(A) \in u\}$.
Lako se vidi da E ima svojstvo konačnih presjeka,
pa se može proširiti do ultrafiltera $v \in W^{\mathfrak{u}}$.

Jasno, $u\, R^{\mathfrak{u}}\, v$ i $\mathfrak{M}^{\mathfrak{u}}, v \Vdash \Sigma$, pa je Σ ispunjiv u $R^{\mathfrak{u}}[u]$. $\square$

Korolar

Neka su $\mathfrak{M}$ i $\mathfrak{N}$ modeli te neka su $w \in |\mathfrak{M}|$ i $v \in |\mathfrak{N}|$.
Tada vrijedi: w i v su modalno ekvivalentni ako i samo ako postoji bisimulacija Z između $\mathfrak{M}^{\mathfrak{u}}$ i $\mathfrak{N}^{\mathfrak{u}}$ za koju vrijedi $w^{\mathfrak{u}}\, Z\, v^{\mathfrak{u}}$.

Hilbertovski sistemi

Hilbertovski sistemi zadani su **aksiomima** i **pravilima izvoda**.

- **izvod** — konačan niz formula koji sadrži aksiome, formule koje zovemo **pretpostavkama** i formule dobivene primjenom pravila izvoda na formule koje su ranije u nizu
- formula F je **izvediva** iz skupa formula S (oznaka: $S \vdash F$) — F je posljednja formula u izvodu sa skupom pretpostavki S
- **dokaz** — izvod čiji skup pretpostavki je prazan
- **teorem** — posljednja formula u dokazu (oznaka: $\vdash F$)

Primjer

- račun sudova (RS)
- račun predikata (RP)
- sistemi modalne logike (K i njegova proširenja)

Hilbertovski sistemi

Veza sintakse (npr. hilbertovskog sistema) i semantike:

- teorem adekvatnosti: svaki teorem sistema je valjana formula
- teorem potpunosti: svaka valjana formula je teorem sistema
- jaka potpunost: $S \vdash F$ ako i samo ako $S \models F$

Primjer

- Formula logike sudova je teorem sistema RS ako i samo ako je tautologija.
- Formula logike prvog reda je teorem sistema RP ako i samo ako je valjana formula.
- Modalna formula je teorem sistema K ako i samo ako je modalno valjana.

Prednost hilbertovskih sistema: mali broj pravila izvoda i stoga manji broj slučajeva u induktivnim dokazima metateorema.
Mana: neintuitivni dokazi u sistemu (sjećate li se $\vdash A \to A$ u RS?).

Prirodna dedukcija

Sistemi prirodne dedukcije zadani su samo pravilima izvoda, od kojih su neka **hipotetska**: imaju **privremene pretpostavke** koje se **zatvaraju** primjenom hipotetskog pravila. Definiramo:

- **izvod** — konačno stablo čiji listovi su označeni pretpostavkama i privremenim pretpostavkama, a čvorovi formulama dobivenim primjenom pravila izvoda na čvorove potomke
- formula F je **izvediva** iz skupa formula S — F je oznaka korijena stabla izvoda sa skupom pretpostavki S
- **dokaz** — izvod čiji skup pretpostavki je prazan
- **teorem** — formula kojom je označen korijen stabla dokaza

Primjer

Vrijede teoremi adekvatnosti i potpunosti za:

- sistem prirodne dedukcije za logiku sudova (PD)
- sistem prirodne dedukcije za logiku prvog reda

Pravila izvoda prirodne dedukcije za logiku sudova

$$\frac{A \land B}{A}\ (\land \mathrm{E}) \qquad \frac{A \land B}{B}\ (\land \mathrm{E}) \qquad \frac{A \quad B}{A \land B}\ (\land \mathrm{I})$$

$$\frac{A}{A \lor B}\ (\lor \mathrm{I}) \qquad \frac{B}{A \lor B}\ (\lor \mathrm{I}) \qquad \frac{A \lor B \quad \begin{array}{c}\overline{A}^{\,n} \\ \vdots \\ C\end{array} \quad \begin{array}{c}\overline{B}^{\,m} \\ \vdots \\ C\end{array}}{C}\ n,m(\lor \mathrm{E})$$

$$\frac{\begin{array}{c}\overline{A}^{\,n} \\ \vdots \\ \bot\end{array}}{\neg A}\ n(\neg \mathrm{I}) \qquad \frac{A \quad \neg A}{\bot}\ (\neg \mathrm{E}) \qquad \frac{\neg\neg A}{A}\ (\neg\neg \mathrm{E})$$

$$\frac{\begin{array}{c}\overline{A}^{\,n} \\ \vdots \\ B\end{array}}{A \to B}\ n(\to \mathrm{I}) \qquad \frac{A \quad A \to B}{B}\ (\to \mathrm{E})$$

$$\frac{A \leftrightarrow B}{A \to B}\ (\leftrightarrow \mathrm{E}) \qquad \frac{A \leftrightarrow B}{B \to A}\ (\leftrightarrow \mathrm{E}) \qquad \frac{A \to B \quad B \to A}{A \leftrightarrow B}\ (\leftrightarrow \mathrm{I})$$

Dodatna pravila izvoda za logiku prvog reda

$$\frac{A(x)}{\forall x\, A(x)}\ (\forall\, \mathrm{I})$$

gdje x nije slobodna varijabla nijedne nezatvorene privremene pretpostavke o kojoj ovisi izvod formule $A(x)$

$$\frac{\forall x\, A(x)}{A(t/x)}\ (\forall\, \mathrm{E})$$

gdje je t term slobodan za varijablu x u formuli $A(x)$

$$\frac{A(t/x)}{\exists x\, A(x)}\ (\exists\, \mathrm{I})$$

gdje je t term slobodan za varijablu x u formuli $A(x)$

$$\dfrac{\exists x\, A(x) \qquad \begin{array}{c} \overline{A(x)}^{\,n} \\ \vdots \\ B \end{array}}{B}\ n\,(\exists\, \mathrm{E})$$

gdje x nema slobodnih nastupa u formuli B i ni u jednoj pretpostavci u izvodu formule B osim možda u $A(x)$

Primjer dokaza prirodnom dedukcijom

Primjer

Ako x nema slobodnih nastupa u A, onda je

$$\forall x\big(A \to B(x)\big) \to \big(A \to \forall x\, B(x)\big)$$

teorem sistema prirodne dedukcije za logiku prvog reda.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\forall x(A \to B(x))}^{\;1}}{A \to B(x)}\;(\forall\mathrm{E}) \qquad \overline{A}^{\;2}}{B(x)}\;(\to\mathrm{E})}{\forall x B(x)}\;(\forall\mathrm{I})}{A \to \forall x B(x)}\;2(\to\mathrm{I})}{\forall x(A \to B(x)) \to (A \to \forall x B(x))}\;1(\to\mathrm{I})$$

Pitanje: gdje se točno koristi to da x nema slobodnih nastupa u A?

Normalizacija

Primjer

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{1}
\UnaryInfC{$A \wedge C$}
\RightLabel{$(\wedge\mathrm{E})$}
\UnaryInfC{A}
\AxiomC{}
\RightLabel{2}
\UnaryInfC{$A \to B$}
\RightLabel{$(\to\mathrm{E})$}
\BinaryInfC{B}
\AxiomC{}
\RightLabel{1}
\UnaryInfC{$A \wedge C$}
\RightLabel{$(\wedge\mathrm{E})$}
\UnaryInfC{C}
\RightLabel{$(\to\mathrm{I})$}
\UnaryInfC{$B \to C$}
\RightLabel{$(\to\mathrm{E})$}
\BinaryInfC{C}
\RightLabel{$2(\to\mathrm{I})$}
\UnaryInfC{$(A \to B) \to C$}
\RightLabel{$1(\to\mathrm{I})$}
\UnaryInfC{$(A \wedge C) \to ((A \to B) \to C)$}
\end{prooftree}
$$

Uočimo da je $B \to C$ najprije konkluzija jednog pravila introdukcije, a onda odmah premisa pravila eliminacije.

U svakom pravilu eliminacije, premisu koja sadrži nastup veznika koji eliminiramo primjenom pravila zovemo **glavna premisa**.

Kažemo da izvod sadrži **rez** ako postoji
konkluzija nekog pravila introdukcije koja je nakon toga
(ne nužno odmah) glavna premisa pravila eliminacije za isti veznik.

Izvod je u **normalnoj formi** ako ne sadrži nijedan rez.

Normalizacija

Prema teoremu o normalizaciji, svaki izvod može se normalizirati.

Prije skice dokaza, normalizirajmo prethodni primjer.

$$\dfrac{\dfrac{\dfrac{\overline{A \wedge C}^{\;1}}{C}\,(\wedge\mathrm{E})}{(A \to B) \to C}\,(\to\mathrm{I})}{(A \wedge C) \to ((A \to B) \to C)}\,1(\to\mathrm{I})$$

Kako bi bilo manje slučajeva u dokazu teorema normalizacije, pretpostavlja se da su logički simboli u alfabetu samo $\wedge$, $\to$, $\perp$ i $\forall$.

Koristimo $\neg A$ kao pokratu za $A \to \perp$, i druge standardne pokrate. Imamo i jedno dodatno pravilo izvoda i poopćeni $(\forall\mathrm{I})$:

$$\dfrac{\begin{array}{c}\overline{\neg A}^{\;n} \\ \vdots \\ \perp\end{array}}{A}\; n\,(RA) \qquad \dfrac{A}{\forall x A(x/y)}\;(\forall\mathrm{I})$$

pri čemu y nije slobodna ni u jednoj nezatvorenoj privremenoj pretpostavci o kojoj ovisi izvod od $A(x)$ i x je slobodna za y u A

Normalizacija

Nije teško opisati transformacije izvoda
kojima se eliminiraju rezovi za $\wedge$ i $\rightarrow$.

Najveći tehnički problemi u dokazu su sa $\forall$.

Indukcijom po visini izvoda dokazuje se:

Lema

U svakom izvodu vezane varijable se mogu preimenovati tako da nijedna varijabla u izvodu nema i vezane i slobodne nastupe.

Sljedeću lemu samo iskazujemo
bez detalja o transformacijama i bez dokaza.

Lema

Nakon odgovarajućih preimenovanja varijabli transformacijama za $\wedge$, $\rightarrow$ i $\forall$ dobivaju se opet izvodi.

Normalizacija

S $D >_1 D'$ označavamo da je izvod D' transformacija izvoda D.

S $>$ označavamo refleksivno i tranzitivno zatvorenje relacije $>_1$.

Definicija

Izvod D je **normaliziran** *ako ne postoji D' takav da je $D >_1 D'$.*
D je **normalizabilan** *ako postoji normalizirani izvod D' takav da je $D > D'$.*
Sustav je **slabo normalizacijski** *ako je svaki izvod normalizabilan, a* **jako je normalizacijski** *ako je $<$ dobro utemeljena.*

Lema

Pravila izvoda $(\neg I)$ i (RA) se mogu ograničiti samo na slučajeve u kojima je konkluzija atomarna formula.

Normalizacija

Definicija

- **rang reza** *u izvodu D je složenost pripadne formule reza*
- *formulu reza u D koja ima maksimalnu složenost zovemo* **maksimalna formula reza**
- **rang reza izvoda** *je $r(D) = (d, n)$, gdje je d složenost maksimalne formule reza, a n broj maksimalnih formula reza, te $r(D) = (0, 0)$ ako izvod nema rezova*

Ideja dokaza teorema normalizacije je (leksikografski) smanjivati rang reza izvoda dok ne eliminiramo sve rezove.

Lema

Neka je D izvod u kojem nastupa rez na samom kraju, pri čemu je rang tog reza m, a drugih rezova u tom izvodu strogo manji od m.

Tada transformacijom izvoda D na tom rezu dobivamo izvod čiji svi rezovi imaju rang strogo manji od m.

Normalizacija

Lema
Neka je D izvod. Ako je $r(d) > (0,0)$,
onda postoji izvod D' za koji je $D >_1 D'$ i $r(D) < r(D')$.

Teorem (slaba normalizacija)
Svaki izvod se može normalizirati.

Teorem (svojstvo podformulnosti)
Neka je D normalizirani izvod koji pokazuje $S \vdash F$. Tada je svaka formula u izvodu D podformula od F, od neke formule iz S, ili neke pretpostavke koja je poništena primjenom pravila (RA).

Pažnja! Podformula ne znači nužno „kraća formula":
$A(t|x)$ je podformula od $\forall x\, A$, t može biti dugačak.

Teorem (jaka normalizacija)
Svaki niz transformacija vodi na normalni oblik.

Modificirana sintaksa

Kod prirodne dedukcije ponekad može biti zamorno provjeriti je li neka formula pretpostavka, privremena pretpostavka ili zatvorena privremena pretpostavka. Kod sistema sekvenata pretpostavke se stalno prepisuju. Podsjetimo se leme o preimenovanju koja je omogućila da slobodne i vezane varijable kod prirodne dedukcije mogu biti različite. Ovdje taj problem izbjegavamo tako da definiramo da su u alfabetu dvije vrste varijabli. Također, osim terma i formula, koristimo i pseudoterme i pseudoformule.
Time se izbjegava pojam terma slobodnog za varijablu u formuli.

- **slobodne varijable** $(a, b, c, \dots)$ — ne mogu se kvantificirati
- **vezane varijable** $(x, y, z, \dots)$ — ne mogu nastupiti slobodno
- **termi** se grade od slobodnih varijabli i funkcijskih simbola
- **pseudotermi** mogu imati i vezane varijable
- **pseudoformula** može imati slobodne nastupe vezanih varijabli
- **atomarne formule** sadrže samo terme
- ako je $F(x)$ pseudoformula (koja može sadržavati pseudoterme s varijablom x), onda su $\forall x F(x)$ i $\exists x F(x)$ formule

Sistem sekvenata

S Γ i Δ označavamo konačne nizove formula, a s A i B formule.
S Δ, A označavamo niz koji nakon formula niza Δ sadrži i A.

Izraze oblika $\Gamma \vdash \Delta$ zovemo **sekvente**.
Intuitivno, $\Gamma \vdash \Delta$ znači: „$\bigwedge \Gamma$ povlači $\bigvee \Delta$".

Gentzenov klasični sistem sekvenata LK zadan je s tri grupe pravila. **Strukturna pravila** su:

- **slabljenje**: $\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}$
- **kontrakcija**: $\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}$
- **permutacija**: $\dfrac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2}$

Sistem sekvenata

Pravila o identitetu su:

- **aksiom**: $\dfrac{}{A \vdash A}$
- **rez**: $\dfrac{\Gamma_1, A \vdash \Delta_1 \quad \Gamma_2 \vdash A, \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}$ (A je **formula reza**)

Logička pravila su:

- **negacija**: $\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \qquad \dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}$

  ($\neg A$ je **glavna formula**, a A je **pomoćna formula**)

- **konjunkcija**:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}$$

(Za binarne veznike $\circ$, $A \circ B$ je glavna, a A i B pomoćne.)

Sistem sekvenata

- **disjunkcija**:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \lor B, \Delta} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \lor B, \Delta} \qquad \frac{\Gamma_1, A \vdash \Delta_1 \quad \Gamma_2, B \to \Delta_2}{\Gamma_1, \Gamma_2, A \lor B \vdash \Delta_1, \Delta_2}$$

- **kondicional**:

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2, B \vdash \Delta_2}{\Gamma_1, \Gamma_2, A \to B \vdash \Delta_1, \Delta_2}$$

- **univerzalni kvantifikator**:

$$\frac{\Gamma \vdash A(a), \Delta}{\Gamma \vdash \forall x\, A(x), \Delta}$$

gdje a (**svojstvena varijabla**) ne nastupa u donjoj sekventi

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x\, A(x) \vdash \Delta}$$

(formula $\forall x\, A$ je **glavna**, a $A(a)$ i $A(t)$ su **pomoćne**)

Sistem sekvenata

- **egzistencijalni kvantifikator**: $\dfrac{\Gamma, A(a) \vdash \Delta}{\Gamma, \exists x\, A(x) \vdash \Delta}$

  gdje a (**svojstvena varijabla**) ne nastupa u donjoj sekventi

  $\dfrac{\Gamma \vdash A(t), \Delta}{\Gamma \vdash \exists x\, A(x), \Delta}$ (formula $\exists x\, A$ je **glavna**, a $A(a)$ i $A(t)$ su **pomoćne**)

Izvod D u sistemu LK je stablo sekventi takvo da

- polazne sekvente su aksiomi
- svaka sekventa u D osim najdonje (**krajnje**) je gornja sekventa nekog pravila čija donja sekventa je također u D

Izvod D s krajnjom sekventom S zovemo **izvod za sekventu** S.
Ako je $S = (\Gamma \vdash \Delta)$, pišemo $D : \Gamma \vdash \Delta$.
Kažemo da je formula A **dokaziva** ako postoji izvod za $\vdash A$.

Vrijedi jaka potpunost: A je logička posljedica skupa Γ ako i samo ako postoji izvod za sekventu $\Gamma \vdash A$.

Primjer dokaza u sistemu sekvanata

Primjer

Prirodnom dedukcijom smo dokazali

$$\forall x\big(A \to B(x)\big) \to \big(A \to \forall x B(x)\big),$$

gdje x nema slobodnih nastupa u A.
Evo i dokaza u sistemu sekvenata:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{A \vdash A \quad B(a) \vdash B(a)}{A, A \to B(a) \vdash B(a)}}{A, \forall x(A \to B(x)) \vdash B(a)}}{\forall x(A \to B(x)), A \vdash B(a)}}{\forall x(A \to B(x)), A \vdash \forall x B(x)}}{\forall x(A \to B(x)) \vdash (A \to \forall x B(x))}}{\vdash \forall x(A \to B(x)) \to (A \to \forall x B(x))}$$

Eliminacija reza

Primjer

$$\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, A \to B \vdash B} \quad \dfrac{B \vdash B \quad C \vdash C}{B \to C, B \vdash C}}{A \to B, B \to C, A \vdash C}}{A \to B, B \to C \vdash A \to C}$$

Bez reza:

$$\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, A \to B \vdash B} \quad C \vdash C}{A \to B, B \to C, A \vdash C}}{A \to B, B \to C \vdash A \to C}$$

Eliminacija reza

S $h(\Pi)$ označavamo visinu stabla Π, s $\partial(A)$ **rang formule** A:

- $\partial(At) := 1$, ako je At atomarna formula
- $\partial(A \circ B) := \max\{\partial A, \partial B\} + 1$, gdje je $\circ$ binarni logički veznik
- $\partial(\forall x A) := \partial(\exists x A) := \partial(\neg A) := \partial A + 1$

te s $d(\Pi)$ **rang izvoda** Π, tj. maksimalni rang formule reza u Π.
Dokaz sljedeće tehničke leme ispuštamo.

Lema

Neka je $\Pi : \Gamma \vdash \Delta$, neka je a varijabla i t term.
Označimo s $\Pi(t/a)$ stablo dobiveno tako da se u izvodu Π svaki nastup varijable a zamijeni s t. Tada je $\Pi(t/a) : \Gamma(t/a) \vdash \Delta(t/a)$.

Glavna lema

Lema

Neka je A formula čiji je rang $\partial A = d > 0$. Neka su $\Pi_1 : \Gamma_1 \vdash \Delta_1$ i $\Pi_2 : \Gamma_2 \vdash \Delta_2$ izvodi rangova manjih od d. Tada postoji izvod $\Pi : \Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2$ čiji je rang također manji od d.

Dokaz.

Indukcijom po $h(\Pi_1) + h(\Pi_2)$. Baza: $h(\Pi_1) = h(\Pi_2) = 1$. Tada Π_1 i Π_2 sadrže samo aksiome: $\Pi_1 = (B \vdash B)$ i $\Pi_2 = (C \vdash C)$ za neke formule B i C. Tada imamo sljedeće slučajeve:

$\boxed{B = A, C \neq A}$ Traženi izvod $\Pi : \Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2$:

$$\dfrac{\dfrac{C \vdash C}{C, A \vdash C}}{A, C \vdash C} \qquad \text{Pritom je } d(\Pi) = 0 < d.$$

$\boxed{B \neq A, C = A}$ Analogno.

$\boxed{B = A, C = A}$ Traženi izvod je $\Pi := (A \vdash A)$, ranga $0 < d$. $\cdots$

Glavna lema

Nastavak.

$\boxed{B \neq A, C \neq A}$ Traženi izvod Π:

$$\cfrac{\cfrac{\cfrac{B \vdash B}{B, C \vdash B}}{B, C \vdash C, B}}{B, C \vdash B, C}$$

I ovdje je očito $d(\Pi) = 0 < d$.

Pretpostavka: neka je $n \in \mathbb{N}$ takav da za sve izvode Π_1' i Π_2' takve da je $h(\Pi_1') + h(\Pi_2') < n$ vrijedi tvrdnja.

Korak: neka je $\Pi_1 : \Gamma_1 \vdash \Delta_1$ i $\Pi_2 : \Gamma_1 \vdash \Delta_2$ takvi da je $h(\Pi_1) + h(\Pi_2) = n$, i A formula za koju je $\partial A = d > d(\Pi_1), d(\Pi_2)$.

Neka je r_i posljednje pravilo primijenjeno u Π_i. Slučajevi:

1. barem jedan od izvoda Π_1, Π_2 je visine jedan
2. barem jedno od pravila r_1, r_2 je strukturno
3. barem jedno od pravila r_1, r_2 je pravilo reza
4. oba pravila r_1, r_2 su logička, a u barem jednom A nije glavna
5. oba pravila r_1, r_2 su logička i A je glavna formula u oba $\cdots$

Glavna lema

Nastavak.

$\boxed{1.}$ BSOMP $h(\Pi_1) = 1$. Imamo dva podslučaja:

$\boxed{1.1.}$ $\Pi_1 = (A \vdash A)$. Traženi izvod (točkice su Π_2):

$$\dfrac{\begin{array}{c}\vdots \\ \Gamma_2 \vdash \Delta_2\end{array}}{A, \Gamma_2 \setminus \{A\} \vdash \Delta_2} \qquad \text{Očito je } d(\Pi) = d(\Pi_2) < d.$$

$\boxed{1.2.}$ $\Pi_1 = (B \vdash B)$ za $B \neq A$

(točkice su slabljenja i permutacije):

$$\begin{array}{c} B \vdash B \\ \vdots \\ B, \Gamma_2 \setminus \{A\} \vdash B, \Delta_2 \end{array} \qquad \text{Pritom je } d(\Pi) = 0 < d. \qquad \cdots$$

Glavna lema

Nastavak.

$\boxed{2.}$ BSOMP r_1 je strukturno pravilo.

$\boxed{2.1.}$ r_1 je slabljenje (BSOMP lijevo). Tada je Π_1 oblika:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_1' \vdash \Delta_1\end{array}}{\Gamma_1', B \vdash \Delta_1}$$

pri čemu točkice predstavljaju izvod $\Pi_1' : \Gamma_1' \vdash \Delta_1$. Kako je $h(\Pi_1') + h(\Pi_2) < n$, na Π_1' i Π_2 možemo primijeniti pretpostavku indukcije, pa postoji izvod $\Pi' : \Gamma_1', \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2$ takav da je $d(\Pi') < d$. Primjenom jednog lijevog slabljenja dobivamo traženi izvod Π i očito je $d(\Pi) = d(\Pi') < d$. $\cdots$

Glavna lema

Nastavak.

$\boxed{2.2.}$ r_1 je kontrakcija (BSOMP lijeva). Tada je Π_1 oblika:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_1', B, B \vdash \Delta_1\end{array}}{\Gamma_1', B \vdash \Delta_1}$$

pri čemu točkice predstavljaju izvod $\Pi_1' : \Gamma_1', B, B \vdash \Delta_1$. Kako je $h(\Pi_1') + h(\Pi_2) < n$, na Π_1' i Π_2 možemo primijeniti pretpostavku indukcije, pa postoji izvod $\Pi' : \Gamma_1', B, B, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2$ takav da je $d(\Pi') < d$. Primjenom jedne lijeve kontrakcije dobivamo traženi izvod Π, i očito je $d(\Pi) = d(\Pi') < d$. $\cdots$

Glavna lema

Nastavak.

$\boxed{3.}$ BSOMP r_2 je rez. Kako je $d(\Pi_2) < d$, formula reza u r_2 nije A. Izvod Π_2 je oblika:

$$\dfrac{\begin{matrix}\vdots \\ \Gamma_{21} \vdash B, \Delta_{21}\end{matrix} \quad \begin{matrix}\vdots \\ B, \Gamma_{22} \vdash \Delta_{22}\end{matrix}}{\Gamma_{21}, \Gamma_{22} \vdash \Delta_{21}, \Delta_{22}}$$

pri čemu su točkice izvodi koje označimo s Π_{21}, odnosno Π_{22}.

Kako je $h(\Pi_1) + h(\Pi_{21}) < n$ i $h(\Pi_1) + h(\Pi_{22}) < n$, po pretpostavci indukcije postoje izvodi ranga manjeg od d:

- $\Pi_3 : \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, B, \Delta_{21}$
- $\Pi_4 : \Gamma_1, B, \Gamma_{22} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{22}$

$\cdots$

Glavna lema

Nastavak.

Traženi izvod:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, B, \Delta_{21}\end{array} \quad \begin{array}{c}\vdots\\ \Gamma_1, B, \Gamma_{22} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{22}\end{array}}{\Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2}$$

pri čemu točkice predstavljaju Π_3 i Π_4.

Zadnje primijenjeno pravilo je rez po B, a B je formula reza u Π_2, pa vrijedi $\partial B \leq d(\Pi_2) < d$, a onda je i $d(\Pi) < d$. $\cdots$

Glavna lema

Nastavak.

$\boxed{4.}$ oba pravila r_1, r_2 su logička,
a A u barem jednom (BSOMP u r_2) nije glavna formula.

$\boxed{4.1.}$ r_2 ima jednu premisu. Izvod Π_2 je oblika

$$\dfrac{\begin{matrix}\vdots \\ \Gamma_{21} \vdash \Delta_{21}\end{matrix}}{\Gamma_2 \vdash \Delta_2}$$

Iz pretpostavke indukcije slijedi da postoji izvod
$\Pi_3 : \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{21}$ ranga manjeg od d.

Traženi izvod je:

$$\dfrac{\begin{matrix}\vdots \\ \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{21}\end{matrix}}{\Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2}$$

pri čemu je posljednje primijenjeno pravilo r_2. $\cdots$

Glavna lema

Nastavak: $\boxed{4.2.}$ r_2 ima dvije premise. Izvod Π_2 je oblika

$$\dfrac{\begin{array}{c}\vdots \\ \Gamma_{21} \vdash \Delta_{21}\end{array} \quad \begin{array}{c}\vdots \\ \Gamma_{22} \vdash \Delta_{22}\end{array}}{\Gamma_2 \vdash \Delta_2}$$

pri čemu su točkice izvodi koje označimo s Π_{21}, odnosno Π_{22}.
Primjenom pretpostavke indukcije na Π_1 i Π_{21},
odnosno na Π_1 i Π_{22}, postoje izvodi ranga manjeg od d:

- $\Pi_3 : \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{21}$
- $\Pi_4 : \Gamma_1, \Gamma_{22} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{22}$

Traženi izvod (posljednje primijenjeno pravilo je r_2):

$$\dfrac{\begin{array}{c}\vdots \\ \Gamma_1, \Gamma_{21} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{21}\end{array} \quad \begin{array}{c}\vdots \\ \Gamma_1, \Gamma_{22} \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_{22}\end{array}}{\Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2}$$

Glavna lema

Nastavak.

$\boxed{5.}$ oba pravila r_1, r_2 su logička i A je glavna formula u oba.

$\boxed{5.1.\ A = \neg B}$ r_1 i r_2 su pravila negacije (BSOMP r_1 desno).

Izvod Π_1 je oblika:

$$\dfrac{\begin{array}{c}\vdots \\ \Gamma_1, B \vdash \Delta_{11}\end{array}}{\Gamma_1 \vdash \neg B, \Delta_{11}}$$

Označimo $\Pi_{11} : \Gamma_1, B \vdash \Delta_{11}$, i uočimo $\Delta_{11} = \Delta_1 \setminus \{\neg B\}$.
Primjenom pretpostavke indukcije na Π_{11} i Π_2 dobivamo izvod:

$$\dfrac{\begin{array}{c}\vdots \\ \Gamma_1, B, \Gamma_2 \setminus \{\neg B\} \vdash \Delta_{11} \setminus \{\neg B\}, \Delta_2\end{array}}{\Gamma_1, \Gamma_2 \setminus \{\neg B\} \vdash \Delta_1 \setminus \{\neg B\}, \Delta_2}$$

koristeći desno pravilo negacije u zadnjem koraku. $\cdots$

Glavna lema

Nastavak.

$\boxed{5.2.\ A = (B \wedge C)}$ BSOMP r_1 je desno, a r_2 lijevo pravilo konjunkcije. Izvod Π_1 je oblika:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_{11} \vdash B, \Delta_{11}\end{array} \quad \begin{array}{c}\vdots\\ \Gamma_{12} \vdash C, \Delta_{12}\end{array}}{\Gamma_{11}, \Gamma_{12} \vdash B \wedge C, \Delta_{11}, \Delta_{12}}$$

pri čemu točkice predstavljaju izvode koje označimo s Π_{11}, odnosno Π_{12}. Izvod Π_2 je oblika:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_{21}, B \vdash \Delta_2\end{array}}{\Gamma_{21}, B \wedge C \vdash \Delta_2}$$

pri čemu točkice predstavljaju izvod koji označimo s Π_{21}. $\cdots$

Glavna lema

Nastavak.
Primijenimo pretpostavku indukcije na Π_{11} i Π_2, te na Π_1 i Π_{21}.

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma_{11}, \Gamma_2 \setminus \{A\} \vdash B, \Delta_{11} \setminus \{A\}, \Delta_2\end{array} \quad \begin{array}{c}\vdots\\ \Gamma_1, \Gamma_{21} \setminus \{A\}, B \vdash \Delta_{11}, \Delta_{12}, \Delta_2\end{array}}{\Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2}$$

koristeći rez po B u zadnjem koraku,
što ne kvari rang izvoda jer je $\partial B < \partial A$.

$\boxed{5.3.\ A = (B \vee C)}$ slično prethodnom slučaju (raspišite!)

$\boxed{5.4.\ A = (B \to C)}$ slično prethodnim slučajevima $\cdots$

Glavna lema

Nastavak.

$\boxed{5.5.\ A = \exists x\, B}$ BSOMP r_1 je desno, a r_2 lijevo pravilo za egzistencijalni kvantifikator. Izvodi Π_1 i Π_2 su redom oblika:

$$\dfrac{\begin{matrix}\vdots\\ \Gamma_1 \vdash \Delta_{11}, B(t)\end{matrix}}{\Gamma_1 \vdash \Delta_{11}, \exists x B(x)} \qquad \dfrac{\begin{matrix}\vdots\\ \Gamma_{22}, B(a) \vdash \Delta_2\end{matrix}}{\Gamma_{22}, \exists x B(x) \vdash \Delta_2}$$

Označimo točkice s $\Pi_{11} : \Gamma_1 \vdash \Delta_{11}, B(t)$ i $\Pi_{22} : \Gamma_{22}, B(a) \vdash \Delta_2$. Koristimo pretpostavku indukcije za Π_1 i Π_{22}, odnosno Π_{11} i Π_2.

...

Glavna lema

Nastavak.

Traženi izvod je:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma_1, \Gamma_{22} \setminus \{A\}, B(a) \vdash \Delta_1 \setminus \{A\}, \Delta_2\end{array}}{\Gamma_1, \Gamma_{22} \setminus \{A\}, B(t) \vdash \Delta_1 \setminus \{A\}, \Delta_2} \quad \begin{array}{c}\vdots\\ \Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_{11} \setminus \{A\}, B(t), \Delta_2\end{array}}{\Gamma_1, \Gamma_2 \setminus \{A\} \vdash \Delta_1 \setminus \{A\}, \Delta_2}$$

pri čemu je zadnji korak rez po $B(t)$,
a prije toga u lijevom podstablu primjena tehničke leme.

$\boxed{5.6.\ A = \forall x\, B}$ slično prethodnom slučaju (raspišite!) $\square$

Lema

Za svaki izvod ranga $d > 0$ postoji izvod iste sekvente nižeg ranga.

Gentzenov teorem i posljedice

Teorem (Gentzenov *Hauptsatz* za sistem LK)

Za svaki izvod postoji izvod iste sekvente bez reza.

Korolar (podformulnost)

Ako je neka formula F dokaziva u sistemu LK, onda za nju postoji izvod u kojem se upotrebljavaju samo podformule od F.

Korolar (konzistentnost)

U sistemu LK ne postoji izvod za praznu sekventu $\vdash$.

Korolar (Gentzenov teorem o midsekventi)

*Neka je S sekventa koja ima izvod u LK, a sadrži samo formule u preneksnoj normalnoj formi. Tada postoji izvod od S bez reza koji sadrži sekventu M (**midsekventu**) tako da su sve formule iz M otvorene, svako pravilo izvoda iznad M je strukturno ili propozicijsko, a svako ispod M strukturno ili kvantifikatorsko.*

Izračunljive funkcije

Intuitivno, funkcija $f : S \subseteq \mathbb{N}^k \to \mathbb{N}$ (skraćeno $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$) je **izračunljiva** ako postoji algoritam $\mathcal{A}$ koji je računa: za sve $\vec{x} \in \mathbb{N}^k$, $\mathcal{A}$-izračunavanje s $\vec{x}$ stane ako i samo ako je $x \in Dom(f) = S$, i u tom slučaju izlazni podatak mu je upravo $f(x)$.

Prema Church–Turingovoj tezi,
sve izračunljive funkcije su parcijalno rekurzivne.

Definicija

Inicijalne funkcije *su:*

- $Z : \mathbb{N} \to \mathbb{N}$ *definirana sa* $Z(x) := 0$ *(***nul-funkcija***)*
- $Sc : \mathbb{N} \to \mathbb{N}$ *definirana sa* $Sc(x) := x + 1$ *(***sljedbenik***)*
- *za* $n \in \mathbb{N}, k \in \{1, \ldots, n\}$, $I_k^n : \mathbb{N}^n \to \mathbb{N}$ *definirana s* $I_k^n(x_1, \ldots, x_n) := x_k$ *(***koordinatna projekcija***)*

Definirani i nedefinirani izrazi

Promatrat ćemo i funkcije koje nisu totalne,
odnosno izraze koji za neke prirodne brojeve nisu definirani.
Ako je f k-mjesna parcijalna funkcija i $\vec{x} \in \mathbb{N}^k$,

- pišemo $f(\vec{x}) \uparrow$ ako $\vec{x} \notin Dom(f)$
- pišemo $f(\vec{x}) \downarrow$ ako $\vec{x} \in Dom(f)$

Pišemo $f(\vec{x}) \simeq g(\vec{x})$ ako za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:

- $f(\vec{x}) \downarrow$, $g(\vec{x}) \downarrow$ i $f(\vec{x}) = g(\vec{x})$, ili
- $f(\vec{x}) \uparrow$ i $g(\vec{x}) \uparrow$.

Definicija

Neka su $H, G_1, \ldots, G_n$ funkcije. Neka je funkcija F definirana s

$$F(\vec{x}) \simeq H\big(G_1(\vec{x}), \ldots, G_n(\vec{x})\big).$$

Kažemo da je funkcija F definirana **kompozicijom**.

Primitivna rekurzija

Definicija

Neka je G totalna k-mjesna funkcija i H totalna $(k+2)$-mjesna funkcija. Neka je $(k+1)$-mjesna funkcija F definirana s

$$F(\vec{x}, 0) := G(\vec{x}),$$
$$F(\vec{x}, y+1) := H\big(\vec{x}, y, F(\vec{x}, y)\big).$$

Kažemo da je funkcija F definirana **primitivnom rekurzijom.**
Za $k = 0$, definicija (degeneriranom) primitivnom rekurzijom je

$$F(0) := a \qquad (a \in \mathbb{N})$$
$$F(n+1) := H(n, F(n))$$

Najmanji skup funkcija koji sadrži inicijalne funkcije i zatvoren je na kompoziciju i na primitivnu rekurziju, zove se skup **primitivno rekurzivnih funkcija***. Relacija je* **primitivno rekurzivna** *ako joj je karakteristična funkcija takva.*

Minimizacija

Inicijalne funkcije, kompozicija i primitivna rekurzija nisu dovoljne da bi se definirala svaka izračunljiva funkcija (npr. Ackermanova funkcija nije primitivno rekurzivna). Stoga se definira operator minimizacije μ i tako dobiva skup parcijalno rekurzivnih funkcija.

Definicija

Neka je $f = \chi_R$ *karakteristična funkcija (s kodomenom* $\{0, 1\}$*).*

S $\mu y\, R(\vec{x}, y)$ *označavamo najmanji* y *takav da vrijedi* $R(\vec{x}, y)$*, odnosno* $f(\vec{x}, y) = 1$ *(nedefinirano ako takav ne postoji).*

S μR *(ili* μf*) označavamo funkciju definiranu na projekciji od* R*, pravilom* $\vec{x} \mapsto \mu y R(\vec{x}, y)$*.*

Kažemo da je funkcija $\mu R = \mu f$ *definirana* **minimizacijom** *relacije* R*, odnosno njene karakteristične funkcije* f*.*

Parcijalno rekurzivne funkcije

Definicija

Najmanji skup funkcija koja sadrži sve inicijalne funkcije i zatvoren je na kompoziciju, primitivnu rekurziju i minimizaciju, zove se skupom **parcijalno rekurzivnih funkcija***.*

Za parcijalno rekurzivnu funkciju koja je totalna kažemo da je **rekurzivna** *funkcija.*

Za relaciju na $\mathbb{N}^k$ kažemo da je **rekurzivna relacija** *(ili* **skup***) ako je njena karakteristična funkcija rekurzivna.*

Propozicija

Komplement rekurzivnog skupa (relacije), presjek i unija konačno mnogo rekurzivnih skupova (relacija) su rekurzivni.

Primjer

Relacije uspoređivanja $=$, $\neq$, $\leq$, $\geq$, $<$ i $>$ su primitivno rekurzivne.

Definicija funkcije po slučajevima

Propozicija

Neka su $R_1, \ldots, R_n$ u parovima disjunktne (primitivno) rekurzivne relacije, te G_0, G_1, ..., G_n (primitivno) rekurzivne funkcije.

Tada je (primitivno) rekurzivna i funkcija $F : \mathbb{N}^k \to \mathbb{N}$ definirana s

$$F(\vec{x}) = \begin{cases} G_1(\vec{x}), & R_1(\vec{x}) \\ G_2(\vec{x}), & R_2(\vec{x}) \\ & \vdots \\ G_n(\vec{x}), & R_n(\vec{x}) \\ G_0(\vec{x}), & \textit{inače} \end{cases}$$

Propozicija

Neka je F (primitivno) rekurzivna, a G totalna funkcija takva da je $G(\vec{x}) = F(\vec{x})$ osim za konačno mnogo $\vec{x}$.

Tada je G također (primitivno) rekurzivna.

Korolar: Svaki konačni skup je primitivno rekurzivan.

Kleenejev teorem o normalnoj formi

Teorem

Postoji primitivno rekurzivna funkcija U takva da za svaki $k \in \mathbb{N}_+$ postoji primitivno rekurzivna relacija T_k takva da za svaku k-mjesnu parcijalno rekurzivnu funkciju φ^k postoji **indeks** *$e \in \mathbb{N}$ takav da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi:*

- $\varphi(\vec{x}) \downarrow \iff \exists y T_k(\vec{x}, e, y)$
- $\varphi(\vec{x}) \simeq U\big(\mu y T_k(\vec{x}, e, y)\big)$

Definicija

Za sve $e \in \mathbb{N}$, $k \in \mathbb{N}_+$, definiramo k-mjesnu funkciju $\{e\}$ ovako:

$$\{e\}(\vec{x}) :\simeq U\big(\mu y T_k(\vec{x}, e, y)\big).$$

Teorem

Funkcija $\varphi : \mathbb{N}^k \rightharpoonup \mathbb{N}$ je parcijalno rekurzivna ako i samo ako ima indeks ($\exists e(\varphi = \{e\}^k)$).

Posljedice Kleenejevog teorema

Teorem (Definicija funkcije po slučajevima — druga verzija)

Neka su $R_1, \ldots, R_n$ u parovima disjunktne k-mjesne rekurzivne relacije i $F_1, \ldots, F_n$ k-mjesne parcijalno rekurzivne funkcije. Tad je

$$F(\vec{x}) \simeq \begin{cases} F_1(\vec{x}), & \text{ako vrijedi } R_1(\vec{x}) \\ & \vdots \\ F_n(\vec{x}), & \text{ako vrijedi } R_n(\vec{x}) \end{cases}$$

parcijalno rekurzivna.

Teorem

Svaka parcijalno rekurzivna funkcija može se definirati tako da se minimizacija upotrijebi najviše jednom.

Teorem o parametru ili S_{mn}-teorem

Za $m,n \in \mathbb{N}_+$ postoji rekurzivna funkcija $S_{mn} : \mathbb{N}^{m+1} \to \mathbb{N}$ takva da za sve $e \in \mathbb{N}, \vec{x} \in \mathbb{N}^n, \vec{y} \in \mathbb{N}^m$ vrijedi $\{S_{mn}(\vec{y}, e)\}(\vec{x}) \simeq \{e\}(\vec{x}, \vec{y})$.

Posljedice Kleenejevog teorema

Dijagonalna lema

Za svaki $k \in \mathbb{N}_+$ postoji rekurzivna funkcija D_k takva da je za svaki $e \in \mathbb{N}$, $\{D_k(e)\}^k(\vec{x}) \simeq \{e\}(\vec{x}, e)$.

Teorem rekurzije

Neka je G $(k+1)$-mjesna parcijalno rekurzivna funkcija. Tada postoji $e \in \mathbb{N}$ takav da za sve $\vec{x} \in \mathbb{N}^k$ vrijedi

$$\{e\}^k(\vec{x}) \simeq G(\vec{x}, e).$$

Teorem o fiksnoj točki

Za svaku unarnu rekurzivnu funkciju F, i za svaki $k \in \mathbb{N}_+$, postoji $e \in \mathbb{N}$ takav da su funkcije $\{e\}^k$ i $\{F(e)\}^k$ jednake.

Teorem (Rice)

Neka je $k \in \mathbb{N}_+$ i $S \subseteq \mathbb{N}$ rekurzivan skup takav da za sve $i, j \in \mathbb{N}$ iz $i \in S$ i $\{i\}^k = \{j\}^k$ slijedi $j \in S$. Tada je $S = \emptyset$ ili $S = \mathbb{N}$.

Church–Turingova teza

Smatramo da je svaka parcijalno rekurzivna funkcija izračunljiva.

Church–Turingova teza je da vrijedi i obrat:
Svaka izračunljiva funkcija je parcijalno rekurzivna.

Kako je izračunljivost intuitivan pojam (nije strogo definiran) nemoguće je dati dokaz Church–Turingove teze. [Dershowitz!]

Oboriti je, značilo bi naći funkciju koja nije parcijalno rekurzivna, a koju bismo smatrali izračunljivom (što do sada nije učinjeno).

Najvažniji argumenti u prilog Church–Turingovoj tezi:

- razni načini definiranja novih funkcija pomoću već danih parcijalno rekurzivnih funkcija (npr. simultana rekurzija, rekurzija s poviješću, definicija funkcija po slučajevima) ponovo daju parcijalno rekurzivne funkcije
- sve do sada poznate definicije kojima je cilj opisati klasu izračunljivih funkcija (npr. parcijalno rekurzivne funkcije, RAM-izračunljive funkcije, Turing-izračunljive funkcije, ...) definiraju istu klasu funkcija

Church–Turingova teza

Church–Turingova teza se primjenjuje prilikom dokaza nepostojanja algoritma za rješavanje nekog problema.

Primjer

Postoji funkcija koja nije izračunljiva. Naime, promotrimo funkciju

$$F(x) := \begin{cases} \{x\}(x) + 1, & \{x\}(x)\downarrow \\ 0, & \text{inače.} \end{cases}$$

Lako je vidjeti da ni za koji $e \in \mathbb{N}$ ne vrijedi $F = \{e\}$.
(Tada bi bilo $\{e\}(e) = F(e) = \{e\}(e) + 1$.)

To znači da za funkciju F ne postoji indeks,
a tada znamo da funkcija F nije parcijalno rekurzivna.
Primjenom Church–Turingove teze, funkcija F nije izračunljiva.

Aritmetička hijerarhija

Definicija

Kažemo da je relacija $R \subseteq \mathbb{N}^k$ **aritmetička** *ako postoji rekurzivna relacija* $P \subseteq \mathbb{N}^{k+n}$ *takva da za sve* $\vec{x}$ *vrijedi*

$$R(\vec{x}) \text{ ako i samo ako } \mathfrak{Q}_1 y_1 \cdots \mathfrak{Q}_n y_n P(\vec{x}, y_1, \ldots, y_n),$$

gdje je $\mathfrak{Q}_i$ *simbol* $\forall$ *ili* $\exists$*. Podriječ* $\mathfrak{Q}_1 y_1 \cdots \mathfrak{Q}_n y_n$ *zovemo* **prefiks***.*

Propozicija

Za svaku rekurzivnu relaciju R *mjesnosti* $k+2$ *postoji rekurzivna relacija* $\hat{R}$ *mjesnosti* $k+1$ *takva da za sve* $\vec{x} \in \mathbb{N}^k$ *vrijedi:*

- $\forall y\, \forall z\, R(\vec{x}, y, z)$ *ako i samo ako* $\forall u\, \hat{R}(\vec{x}, u)$
- $\exists y\, \exists z\, R(\vec{x}, y, z)$ *ako i samo ako* $\exists u\, \hat{R}(\vec{x}, u)$

Dakle, možemo *kontrahirati* istovrsne uzastopne kvantifikatore, dobivši tako **alternirajući prefiks** koji ne sadrži dva uzastopna egzistencijalna ili univerzalna kvantifikatora.

Aritmetička hijerarhija

Definicija

Neka je $n \in \mathbb{N}_+$. Definiramo sljedeće oznake i pojmove:

- *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 $\exists$*
- *za relaciju R kažemo da je Π_n^0-relacija (pišemo $R \in \Pi_n^0$) ako postoji rekurzivna relacija P i Π_n^0 prefiks $\mathfrak{Q}_1 y_1 \ldots \mathfrak{Q}_n y_n$ takvi da vrijedi $R(\vec{x})$ ako i samo ako $\mathfrak{Q}_1 y_1 \cdots \mathfrak{Q}_n y_n P(\vec{x}, y_1, \ldots, y_n)$*
- *analogno definiramo pojam Σ_n^0-relacije*
- *kažemo da je relacija Δ_n^0 ako je istovremeno Π_n^0 i Σ_n^0*
- $\Pi_0^0 = \Sigma_0^0 = \Delta_0^0$ *označava klasu svih rekurzivnih relacija*

Gornji indeks (0) označava da se radi o relacijama na brojevima.

Oznaka poput Π_n^1 odnosila bi se na relacije na skupovima brojeva (koje nećemo razmatrati; njima se bavi *analitička* hijerarhija).

Aritmetička hijerarhija

Iz prethodne propozicije odmah slijedi:

Propozicija

Svaka aritmetička relacija je Π^0_n *ili* Σ^0_n *za neki* $n \in \mathbb{N}$.

Kako uvijek možemo dodati irelevantne kvantifikatore, očito vrijedi:

Propozicija

Ako je $k > n$, *tada je* $\Pi^0_n \cup \Sigma^0_n \subseteq \Delta^0_k$.

Međutim, mnogo je zanimljivije da vrijedi i sljedeće:

Teorem o aritmetičkoj hijerarhiji

Za svaki $n \in \mathbb{N}_+$ postoji Π^0_n-relacija koja nije Σ^0_n
te postoji Σ^0_n-relacija koja nije Π^0_n.

Korolar

Za sve $i, j \in \mathbb{N}$ *takve da je* $i < j$ *vrijedi* $\Pi^0_i \cup \Sigma^0_i \subset \Delta^0_j$.

Rekurzivno prebrojivi skupovi

Intuitivno, skup je odlučiv ili rekurzivan ako postoji algoritam koji za svaki prirodan broj može odrediti pripada li tom skupu.

Skup (jednomjesnu relaciju) S smatramo rekurzivno prebrojivim ako postoji algoritam koji za svaki prirodni broj kao ulazni podatak algoritma, kao izlazni podatak daje neki element skupa, te će se na taj način iscrpiti svi elementi od S.

No, budući da želimo pokriti i višemjesne relacije, definicija je drugačija (a može se pokazati da je za jednomjesne relacije ekvivalentna gornjoj).

Definicija

Kažemo da je relacija $R \subseteq \mathbb{N}^k$ **rekurzivno prebrojiva (RE)** *ako je R domena neke parcijalno rekurzivne funkcije.*

Propozicija

Relacija je RE ako i samo ako je Σ_1^0-relacija.

Teorem

Postoji RE skup koji nije rekurzivan.

Rekurzivno prebrojivi skupovi

Primjer

Promotrimo diofantsku jednadžbu $p(\vec{x}, y) = q(\vec{x}, y)$,
gdje su p i q polinomi s varijablama $\vec{x}$ i y s koeficijentima iz $\mathbb{Z}$.
Skup D definiran s $y \in D :\Longleftrightarrow \exists \vec{x}\big(p(\vec{x}, y) = q(\vec{x}, y)\big)$ je RE.

Rješenjem desetog Hilbertova problema dokazan je obrat:
svaki RE skup je projekcija skupa rješenja diofantske jednadžbe.

Definicija

Neka je F k-mjesna funkcija. **Graf** *od F je $(k+1)$-mjesna relacija Gr_F definirana s $Gr_F(\vec{x}, y) :\Longleftrightarrow \vec{x} \in Dom(F) \land F(\vec{x}) = y$.*

Teorem o grafu

Neka je $F : S \subseteq \mathbb{N}^k \to \mathbb{N}$ proizvoljna funkcija. Tada vrijedi:

- F je parcijalno rekurzivna ako i samo ako je Gr_F RE;
- **totalna** F je rekurzivna ako i samo ako je Gr_F rekurzivan.

Rekurzivno prebrojivi skupovi

Propozicija (Definicija funkcije po slučajevima – treća verzija)

Neka su $R_1, \ldots, R_n$ u parovima disjunktne RE relacije, te $G_1, \ldots, G_n$ parcijalno rekurzivne funkcije.

Tada je parcijalno rekurzivna i funkcija F zadana s

$$F(\vec{x}) \simeq \begin{cases} G_1(\vec{x}), & \text{ako vrijedi } R_1(\vec{x}) \\ & \vdots \\ G_n(\vec{x}), & \text{ako vrijedi } R_n(\vec{x}) \end{cases}$$

Teorem (Post)

R je rekurzivna ako i samo ako su R i R^c RE.

Propozicija

Podskup od $\mathbb{N}$ je RE ako i samo ako je slika neke parcijalno rekurzivne injekcije. Podskup od $\mathbb{N}$ je beskonačan i RE ako i samo ako je slika neke rekurzivne injekcije.

Turingovi strojevi

Intuitivno, Turingov stroj je automat s konačno mnogo stanja,
i trakom neomeđenom zdesna, shvaćenom kao niz ćelijā.
U svakoj ćeliji je zapisan jedan simbol fiksirane konačne abecede.

U jednom trenutku stroj može čitati i pisati u jednu ćeliju.

Definicija

Turingov stroj *je struktura* $(\mathcal{S}, \Sigma, \Gamma, s_0, q_0, q_{DA}, q_{NE}, \Pi)$, *gdje je:*

- $\mathcal{S}$ *konačan skup* **stanja**
- $\Gamma \supset \Sigma$ *konačna* **radna abeceda**
- $s_0 \in \Gamma \setminus \Sigma$ **prazni simbol**
- $q_0 \in \mathcal{S}$ **početno stanje**
- q_{DA} *završno* **stanje prihvaćanja**
- q_{NE} *završno* **stanje odbijanja**
- $\Pi : \Gamma \times (\mathcal{S} \setminus \{q_{DA}, q_{NE}\}) \to \Gamma \times \{L, D\} \times \mathcal{S}$ **funkcija prijelaza** *(L/D znače da će se glava za čitanje pomaknuti lijevo/desno)*

Turingovi strojevi

Razmatramo samo Turingove strojeve koji imaju točno dva (različita) završna stanja q_{DA} i q_{NE}.

Definicija

Kažemo da Turingov stroj nad Σ **prihvaća riječ** *$w \in \Sigma^*$ ako T stane u konačno mnogo koraka u stanju q_{DA} pod pretpostavkom da je na početku rada stroja na traci zapisana samo riječ w.*

S $L(T)$ označavamo skup svih riječi koje T prihvaća.
Kažemo da T **prepoznaje jezik** *$L \subseteq \Sigma^*$ ako je $L = L(T)$.*

Jezik L je **Turing-prepoznatljiv** *ako postoji Turingov stroj koji ga prepoznaje, a* **Turing-odlučiv** *je ako uz to taj stroj za svaku riječ $w \in \Sigma^* \setminus L$ stane u stanju q_{NE}. Dva Turingova stroja nad istom abecedom su* **ekvivalentni** *ako prepoznaju isti jezik.*

Teorem (Post)

Jezik $L \subseteq \Sigma^*$ je Turing-odlučiv ako i samo ako su jezici L i $\Sigma^* \setminus L$ Turing-prepoznatljivi.

Turingovi strojevi s više traka

Turingov stroj s više traka ima sve dijelove kao i Turingov stroj, ali ima više (konačno mnogo) trakā za obradu podataka.

Svaka traka ima svoju glavu. Ulazni podatak sprema se na prvu traku, a ostale su trake na početku rada prazne.

Dozvoljeno je čitanje, pisanje i pomicanje glava na nekim ili na svim trakama simultano: funkcija prijelaza Turingova stroja s k traka je $\Pi : \Gamma^k \times (\mathcal{S} \setminus \{q_{DA}, q_{NE}\}) \to \Gamma^k \times \{L, D, H\}^k \times \mathcal{S}$ (pri čemu H znači ostajanje glave na mjestu).

Teorem

Svaki Turingov stroj s više traka ekvivalentan je nekom Turingovu stroju s jednom trakom.

U nastavku promatramo Turingove strojeve s tri trake:

- na **ulaznoj traci** su na početku rada zapisani ulazni podaci
- druga je **radna traka**
- na **izlaznu traku** se zapisuje izlazni podatak

Turing-izračunljivost

Neka je T Turingov stroj s tri trake i $\vec{x} \in \mathbb{N}^k$.

Rad stroja T kod kojeg je na ulaznoj traci zapisan ulazni podatak $\vec{x}$ zovemo T-**izračunavanje** s $\vec{x}$.

Definicija

Turingov stroj T **računa funkciju** $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *ako za sve $\vec{x} \in \mathbb{N}^k$ T-izračunavanje s $\vec{x}$ stane ako i samo ako $\vec{x} \in Dom(f)$, i tada je na izlaznoj traci zapisan broj $f(\vec{x})$.*

Funkcija je **Turing-izračunljiva** *ako je računa neki Turingov stroj.*

Teorem

Funkcija $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ je Turing-izračunljiva ako i samo ako je parcijalno rekurzivna.

Nedeterministični Turingovi strojevi

Turingove strojeve koje smo do sada razmatrali zovemo i **determinističnim Turingovim strojevima**.

Nedeterministični Turingovi strojevi umjesto funkcije prijelaza imaju *relaciju* prijelaza: $\Pi \subseteq \Gamma \times \mathcal{S} \times \Gamma \times \{L, D\} \times \mathcal{S}$.

Za nedeterministične strojeve izračunavanje nije nužno niz, već *stablo* konfiguracija.

Definicija

Kažemo da nedeterministični Turingov stroj T **prihvaća riječ** *$w \in \Sigma^*$ ako T s ulaznim podatkom w ima svojstvo da barem jedna grana stane nakon konačno mnogo koraka u stanju q_{DA}.*

Teorem

Za svaki nedeterministični Turingov stoj postoji neki deterministični Turingov stroj koji mu je ekvivalentan.

Problem zaustavljanja (*Halting problem*)

Svakom Turingovu stroju T možemo pridružiti kōd $\langle T \rangle$.

Halting problem

Postoji li algoritam koji će za svaki Turingov stroj T i za svaki ulazni podatak odrediti hoće li T s tim ulaznim podatkom stati?

Dokazano je da takav algoritam ne postoji:

Teorem

Jezik $A_{TM} = \{\langle T, w \rangle : T$ *Turingov stroj,* $w \in L(T)\}$ *nije odlučiv.*

Korolar

Komplement jezika A_{TM} *nije Turing-prepoznatljiv.*

Aritmetizacija

Aritmetizacija je funkcija koja najprije svakom simbolu alfabeta, a zatim svakoj riječi, pridružuje prirodni **Gödelov broj**.

Aritmetizacija mora biti efektivna injekcija s efektivnim inverzom.

Alfabet logike prvog reda sadrži:

- logičke simbole $\neg$, $\vee$ i $\exists$
- dvomjesni relacijski simbol $=$
- pomoćne simbole (zagrade i zarez)
- prebrojivo mnogo varijabli $v_i, i \in \mathbb{N}$
- prebrojivo mnogo relacijskih simbola $A_i^j, i \in \mathbb{N}$, za svaku mjesnost $j \in \mathbb{N}_+$
- prebrojivo mnogo funkcijskih simbola f_i^j, $i \in \mathbb{N}$, za svaku mjesnost $j \in \mathbb{N}$ (konstantski simboli su 0-mjesni funkcijski)

U nastavku pod **teorijom** podrazumijevamo svaki skup rečenica zatvoren na relaciju logičke posljedice.

Ipak, najčešće ćemo ih zadavati navođenjem aksioma (kao što vektorske prostore zadajemo navođenjem izvodnica).

Aritmetizacija

Gödelovi brojevi simbola koji čine formule logike prvog reda:

$'$	v	R	$\rightarrow$	$\forall$	f	(	$\neg$	,	)
0	1	2	3	4	5	6	7	8	9

Formulu čitamo kao broj čije su dekadske znamenke gornji simboli. (Formula ne može početi znakom $'$.)
Mjesnost zaključujemo brojeći zareze između zagrada.
Konstantske simbole shvaćamo kao funkcijske simbole mjesnosti 0.
Relacijske (uključivo $=$) i funkcijske simbole pišemo prefiksno.
Redni broj simbola pišemo ponavljanjem simbola $'$: $R_3 = R'''$.
Ostale binarne veznike zapisujemo pomoću negacije i kondicionala, a egzistencijalnu kvantifikaciju negiranjem univerzalne.

Uobičajene aritmetičke simbole shvaćamo kao $0 = f_0^0()$, $x = v_0$, $y = v_1$, $z = v_2$, $s = f_0^1$, $(+) = f_0^2$, $(\cdot) = f_1^2$, $(=) = R_0^2$, $(<) = R_1^2$.

Aritmetizacija

Smatrat ćemo da se u jeziku aritmetike relacijski i funkcijski simboli koriste na sljedeći način:

- $t_1 + t_2$, $t_1 \cdot t_2$ umjesto $+(t_1, t_2)$, $\cdot(t_1, t_2)$
- $t_1 = t_2$, $t_1 < t_2$ umjesto $=(t_1, t_2)$, $<(t_1, t_2)$
- t' ($t + 0'$ ako postoji opasnost od zabune) umjesto $s(t)$

Strukturu $(\mathbb{N}, 0, s, +, \cdot, <)$ nazivamo **standardni model**.
Za svaki $n \in \mathbb{N}$ definiramo **numeral** $\overline{n}$ kao pokratu za $0'''^{\cdots}$, gdje se $'$ pojavljuje n puta (npr. $\overline{3}$ je pokrata za $0'''$).
Za kodiranje riječi koristimo konkatenaciju.
Neka je e kod riječi E, a d kod riječi D; kod riječi ED tada je $e * d = e \cdot 10^{\lfloor \log d \rfloor + 1} + d$. Očito je $*$ rekurzivna funkcija.

Propozicija

Primjene logičkih veznika i kvantifikacije, gledane kao funkcije na kodovima formula, su rekurzivne.

Aritmetizacija

Propozicija

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.

Propozicija

Ako je Γ rekurzivan skup rečenica, onda je sljedeća relacija rekurzivna: „Σ je izvod rečenice D iz skupa Γ".

Korolar

Neka je Γ rekurzivan skup rečenica.
Tada je $[\Gamma]$, skup svih rečenica izvedivih iz Γ, rekurzivno prebrojiv.

Korolar (Gödelov teorem potpunosti — apstraktni oblik)

Skup svih valjanih formula logike prvog reda je rekurzivno prebrojiv.

Dokaz.

Po Gödelovu teoremu potpunosti, taj je skup jednak $[\emptyset]$. $\square$

Aritmetizacija

Kažemo da je teorija T:

- **aksiomatizabilna** ako postoji rekurzivan skup rečenica Γ takav da je $\Gamma \vdash F$ ako i samo ako $F \in T$ za svaku rečenicu F
- **potpuna** ako za svaku rečenicu F vrijedi $\Gamma \vdash F$ ili $\Gamma \vdash \neg F$
- **konzistentna** ako postoji rečenica F takva da $F \notin T$

Za skup rečenica Γ kažemo da je **odlučiv** ako je
skup svih rečenica koje se mogu izvesti iz Γ rekurzivan.

Uočimo: teorija T je odlučiva ako i samo ako je rekurzivna.

Aritmetizacija

Teorem

Svaka aksiomatizabilna i potpuna teorija T je odlučiva.

Dokaz.

S T^* označimo skup Gödelovih brojeva rečenica iz T.
Iz ranijeg korolara znamo da je T^* rekurzivno prebrojiv.

1° Ako je T inkonzistentna, $T = [T]$ je zapravo skup svih rečenica pripadnog jezika, koji je rekurzivan.

2° Ako je T konzistentna, označimo s X skup svih prirodnih brojeva koji nisu kodovi rečenica, a s Y skup svih kodova rečenica koje nisu u T. Tada je $\mathbb{N} \setminus T^* = X \cup Y$.

X je rekurzivan kao komplement skupa kodova svih rečenica.

Kako je T potpuna, Y je jednak skupu svih kodova rečenica čije negacije su u T, dakle $Y := \{n \in \mathbb{N} : neg(n) \in T^*\} = neg^{-1}[T^*]$.
T^* je rekurzivno prebrojiv, pa je i Y takav (dokažite!).

Stoga je $\mathbb{N} \setminus T^*$ rekurzivno prebrojiv, pa je T^* rekurzivan. $\square$

Definabilnost i reprezentabilnost

Definicija

Za rečenicu F u jeziku aritmetike kažemo da je **točna** *(correct) ako je istinita u standardnom modelu.*

Definicija

Skup $S \subseteq \mathbb{N}$ je **aritmetički definiran** *formulom $D(x)$*
(u jeziku aritmetike, s jednom slobodnom varijablom x)
ako za sve $n \in \mathbb{N}$ vrijedi: $n \in S$ ako i samo ako je $D(\overline{n})$ točna.

S je **aritmetički** *ako postoji formula koja ga definira.*

Ovi pojmovi analogno se definiraju i za višemjesne relacije.

Funkcija $f : \mathbb{N}^k \to \mathbb{N}$ je **aritmetička** *ako je Gr_F aritmetički.*

Primjer

Inicijalne funkcije su aritmetičke:

Gr_Z je definiran s $(x = x \wedge y = 0)$, Gr_{Sc} s $y = x'$,
a $Gr_{I_n^k}$ s $(x_1 = x_1 \wedge \cdots \wedge y = x_n \wedge \cdots \wedge x_k = x_k)$.

Definabilnost i reprezentabilnost

Također, skup aritmetičkih funkcija je zatvoren na kompoziciju (dokažite!). Za primitivnu rekurziju trebamo kompliciranije alate.

Sljedeća lema, koja omogućuje kodiranje konačnih nizova prirodnih brojeva, dokazuje se pomoću kineskog teorema o ostacima.

Lema (o Gödelovoj funkciji β)

Za svaki $k \in \mathbb{N}$ i za sve $a_0, a_1, \ldots, a_{k-1} \in \mathbb{N}$ postoje $s, t \in \mathbb{N}$ takvi da za svaki $i < k$ vrijedi $a_i = \beta(s, t, i) := s \bmod (i't)'$.

Primjenom leme možemo definirati kod konačnog niza $(a_0, a_1, \ldots, a_{k-1})$ kao uređeni par (s, t).
Pomoću funkcije β je definirano dekodiranje.

Definabilnost i reprezentabilnost

Lema

Svaka rekurzivna funkcija je aritmetička.

Svaki rekurzivni skup je aritmetički.

To je semantička veza rekurzivnih funkcija i aritmetičkih teorija (formula koja definira funkciju je istinita u standardnom modelu).

Cilj nam je odrediti čisto sintaksnu vezu:

- otkriti sintaksu formula koje definiraju rekurzivne funkcije
- za posebnu klasu formula koje su i točne dokazati da su teoremi aritmetičkih teorija

Definicija

Formula je **rudimentarna** *ako u njoj nema neograničenih kvantifikatora. Formula je* $\exists$-**rudimentarna** *ako je oblika* $\exists x\varphi$*, gdje je* φ *rudimentarna. Analogno:* $\forall$-**rudimentarna**, *oblika* $\forall x\varphi$.

Iako su rudimentarne formule slabije od Δ_0^0-formulā, $\exists$-rudimentarne su Σ_1^0, a $\forall$-rudimentarne Π_1^0 (teško je dokazati).

Definabilnost i reprezentabilnost

Propozicija

Svaka rekurzivna funkcija je definabilna,
i definirana je nekom $\exists$-rudimentarnom formulom.

Definicija

Neka je T konzistentna teorija u jeziku aritmetike i $D(x)$ formula od T s jednom slobodnom varijablom x. Kažemo da je skup $S \subseteq \mathbb{N}$ **definiran** *formulom $D(x)$ u teoriji T ako vrijedi:*

- *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 višemjesne relacije.

Primijetimo da je aritmetička definabilnost zapravo definabilnost u teoriji koja sadrži sve točne rečenice.

Definabilnost i reprezentabilnost

Pojmovi s prethodnog slajda mogu se generalizirati i na funkcije, no za njih nam često treba jače svojstvo.

Definicija

Neka je $f : \mathbb{N}^k \to \mathbb{N}$ funkcija i $F(x_1, \ldots, x_k, y)$ formula u jeziku aritmetike, s točno $k+1$ slobodnih varijabli.

*Kažemo da je f **reprezentirana** u teoriji T formulom F ako za sve $n_1, \ldots, n_k \in \mathbb{N}$ vrijedi*

$$\forall y\big(F(\overline{n_1}, \ldots, \overline{n_k}, y) \leftrightarrow y = \overline{f(n_1, \ldots, n_k)}\big) \in T.$$

*Kažemo da je funkcija **reprezentabilna** u teoriji T ako je reprezentirana nekom formulom.*

Minimalna aritmetika

Minimalna aritmetika Q zadana je sljedećim (konačnim!) skupom nelogičkih aksioma:

(Q1) $\neg(x' = 0)$

(Q2) $x' = y' \to x = y$

(Q3) $x + 0 = x$

(Q4) $x + y' = (x + y)'$

(Q5) $x \cdot 0 = 0$

(Q6) $x \cdot y' = (x \cdot y) + x$

(Q7) $\neg(x < 0)$

(Q8) $x < y' \leftrightarrow (x < y \lor x = y)$

(Q9) $x < y \lor x = y \lor y < x$

Minimalna aritmetika

Teorem (Σ^0_1-potpunost teorije Q)

Neka je F proizvoljna $\exists$-rudimentarna rečenica.
Tada je F točna ako i samo ako je dokaziva u teoriji Q.

Dokaz.

$\boxed{\Leftarrow}$ Svaki aksiom od Q je točna rečenica, a pravila izvoda čuvaju točnost, pa su svi teoremi od Q točne rečenice.

$\boxed{\Rightarrow}$ Indukcijom po složenosti. Za atomarne rečenice oblika $\overline{m} = \overline{n}$, točnost povlači $m = n$, pa su $\overline{m}$ i $\overline{n}$ jednaki termi.
Koristeći aksiom za jednakost $x = x$ lako slijedi $Q \vdash \overline{m} = \overline{m}$.

Za točne atomarne rečenice oblika $\overline{n} < \overline{m}$, mora biti $m = k + 1$ za neki k, a $Q \vdash x < \overline{k+1} \leftrightarrow (x = 0 \lor x = \overline{1} \lor \cdots \lor x = \overline{k})$ lako slijedi iz (Q8). Iz toga slijedi da $n < m$ povlači $Q \vdash \overline{n} < \overline{m}$.

Za općenite atomarne rečenice ($t = s$ i $t < s$; t i s zatvoreni termi) tvrdnja slijedi iz činjenice da se svaki zatvoreni term t može *izračunati* (postoji $k \in \mathbb{N}$ takav da $Q \vdash t = \overline{k}$), koja se dokazuje indukcijom po duljini terma. $\cdots$

Minimalna aritmetika

Nastavak dokaza.

Slučajeve s logičkim veznicima je lako raspisati; pogledajmo kvantifikatore. Sve varijable moraju biti vezane, i svi kvantifikatori (osim egzistencijalnog na početku formule) su ograničeni.
To znači da nam varijable i ne trebaju, jer se svaka ograničena kvantifikacija može zapisati kao konačna konjunkcija/disjunkcija.

Npr. ako je t zatvoreni term takav da $Q \vdash t = \overline{k+1}$, onda za svaku formulu $A(x)$ vrijedi

$$Q \vdash \big((\forall x < t)A(x) \leftrightarrow \big(A(0) \land A(\overline{1}) \land \cdots \land A(\overline{k})\big)\big).$$

Naravno, ako $Q \vdash t = 0$, tada $Q \vdash (\forall x < t)A(x)$.

Na kraju (zapravo na početku!) ni varijabla po kojoj egzistencijalno neograničeno kvantificiramo na početku formule nije potrebna.

Naime, ako je $\exists x\, A(x)$ točna, postoji $k \in \mathbb{N}$ takav da je $A(\overline{k})$ točna, pa je po prepostavci indukcije dokaziva u Q.
Stoga je očito u Q dokaziva i formula $\exists x\, A(x)$. $\square$

Minimalna aritmetika

Prethodni teorem ne vrijedi za proizvoljne formule. Npr. ako je $\forall x\, A(x)$ točna $\forall$-rudimentarna rečenica, možemo zaključiti da su $A(0), A(\overline{1}), A(\overline{2}), \ldots$ točne rudimentarne rečenice, i time dokazive u Q, ali iz toga ne možemo zaključiti da je $\forall x\, A(x)$ dokaziva u Q.

Kontraprimjer je **aritmetika ordinalnih brojeva** koja jest model za teoriju Q, ali u tom modelu ne vrijede neke univerzalne točne rečenice poput komutativnosti zbrajanja.

Teorem

- *Svaka rekurzivna funkcija je reprezentabilna u Q;*
  štoviše, reprezentirana je nekom $\exists$-rudimentarnom formulom.
- *Svaka rekurzivna relacija je definabilna u Q;*
  štoviše, definirana je nekom $\exists$-rudimentarnom formulom.

Dijagonalna lema

Neka je A riječ nad alfabetom jezika aritmetike i k njen Gödelov broj. Numeral $\overline{k}$ zovemo **Gödelov kod** od A i označavamo $\lceil A \rceil$.

Riječ $\neg\forall x(x = \lceil A \rceil \rightarrow \neg A)$ zovemo **dijagonalizacijom** od A. [Dijagonalizacija formule $A(x)$ je ekvivalentna rečenici $A(\lceil A \rceil)$.]

Dijagonalna lema

Neka je T teorija u jeziku aritmetike koja proširuje Q. Za svaku formulu $B(x)$ postoji rečenica G takva da $T \vdash \big(G \leftrightarrow B(\lceil G \rceil)\big)$.

Dokaz.

Lako se vidi da postoji primitivno rekurzivna funkcija $diag : \mathbb{N} \rightarrow \mathbb{N}$ takva da vrijedi: ako je n Gödelov broj riječi A,
onda je $diag(n)$ Gödelov broj dijagonalizacije od A.

Kako T proširuje Q, funkcija $diag$ je reprezentabilna u T.
Neka je $Diag(x, y)$ formula koja reprezentira $diag$; to znači da za sve $n \in \mathbb{N}$ vrijedi $T \vdash \forall y\big(Diag(\overline{n}, y) \leftrightarrow y = \overline{diag(n)}\big)$.

Lako se vidi (raspišite!) da je dijagonalizacija formule $A(x) := \exists y\big(Diag(x, y) \wedge B(y)\big)$ tražena rečenica G. $\square$

„Russellov paradoks" na Gödelov način

Lema

Neka je T konzistentna teorija koja proširuje Q.

Skup T^* Gödelovih brojeva svih teorema od T nije definabilan u T.

Dokaz.

Pretpostavimo suprotno, da postoji formula $F(x)$ takva da:

(1) ako $n \in T^*$ onda $T \vdash F(\overline{n})$;

(2) ako $n \notin T^*$ onda $T \vdash \neg F(\overline{n})$.

Iz dijagonalne leme postoji rečenica G za koju $T \vdash G \leftrightarrow \neg F(\lceil G \rceil)$. Neka je g Gödelov broj od G. Pretpostavimo $T \nvdash G$; tada $g \notin T^*$.

Iz (2) slijedi $T \vdash \neg F(\overline{g})$, tj. $T \vdash \neg F(\lceil G \rceil)$ i stoga $T \vdash G$, čime je dobivena kontradikcija. Dakle, mora vrijediti $T \vdash G$ i zato $g \in T^*$.

Iz (1) slijedi $T \vdash F(\overline{g})$, dakle $T \vdash \neg G$. Time smo dobili da je teorija T inkonzistentna, suprotno pretpostavci leme. $\square$

Nedefinabilnost aritmetike

Skup svih točnih rečenica zovemo **aritmetika** i označavamo s $\mathcal{A}$.

Teorem Tarskog o nedefinabilnosti aritmetike

Skup $\mathcal{A}^*$ Gödelovih brojeva svih točnih rečenica nije definabilan.

Dokaz.

Slijedi iz leme, jer je $\mathcal{A}$ konzistentno proširenje od Q. $\square$

Teorem

Skup Gödelovih brojeva svih točnih rečenica nije rekurzivan.

Dokaz.

„Dokazali" smo da su rekurzivni skupovi definabilni, pa je pretpostavka suprotnog u kontradikciji s teoremom Tarskog. $\square$

Teorem (Bitna neodlučivost teorije Q)

Niti jedno konzistentno proširenje T teorije Q nije odlučivo.

Dokaz.

T^* nije definabilan u T, pa nije rekurzivan, pa T nije odlučiva. $\square$

Neodlučivost logike prvog reda

Teorem (Church)

Skup svih valjanih rečenica logike prvog reda nije odlučiv.

Dokaz.

Neka je C konjunkcija svih univerzalnih zatvorenjā aksiomā teorije Q, i c Gödelov broj od C. Tada za svaku rečenicu A u jeziku aritmetike vrijedi $Q \vdash A$ ako i samo ako $C \vdash_{RP} A$, što vrijedi ako i samo ako je formula $(C \to A)$ valjana.

Neka je Λ^* skup Gödelovih brojeva svih valjanih rečenica logike prvog reda i Q^* skup Gödelovih brojeva svih teorema od Q.

S $f(n) := \begin{cases} cond(c, n) := 6 * c * 3 * n * 9, & isSentence(n) \\ \ulcorner\neg\forall x(x = x)\urcorner^{\mathbb{N}} = 741\,261\,819, & \text{inače} \end{cases}$

je zadana rekurzivna funkcija s $\mathbb{N}$ u $\mathbb{N}$.

Prvi odlomak dokaza pokazuje da za svaki $n \in \mathbb{N}$ vrijedi $n \in Q^*$ ako i samo ako $f(n) \in \Lambda^*$, odnosno $\chi_{Q^*} = \chi_{\Lambda^*} \circ f$. Kako je f rekurzivna, iz rekurzivnosti Λ^* bi slijedila rekurzivnost skupa Q^*. No, po prethodnom teoremu, Q^* nije rekurzivan. $\square$

Gödelov prvi teorem nepotpunosti

Teorem (Gödel)

Ne postoji konzistentno, potpuno i aksiomatizabilno proširenje teorije Q.

Dokaz.

Svaka potpuna i aksiomatizabilna teorija je odlučiva, pa tvrdnja slijedi iz bitne neodlučivosti od Q. $\square$

Korolar

Aritmetika nije aksiomatizabilna.

Dokaz.

Aritmetika (skup svih točnih rečenica) jest konzistentno i potpuno proširenje od Q. $\square$

Gödelova i Rosserova rečenica

Neka je T aksiomatizabilno proširenje od Q. Skup svih rečenica dokazivih u T i skup svih rečenica čije su negacije dokazive u T su rekurzivno prebrojivi.

Svaki rekurzivan skup definabilan je u T $\exists$-rudimentarnom formulom. Slijedi da postoje $\exists$-rudimentarne formule
$Prv_T(x) = \exists y\, Prf_T(x, y)$ i $Prv_T\big(neg(x)\big)$,
pri čemu je $Prf_T(x, y)$ rudimentarna, tako da za sve rečenice A:

- $T \vdash A$ ako i samo ako je $Prf_T(\ulcorner A \urcorner, \overline{b})$ točna za neki $b \in \mathbb{N}$ (i isto tako za rečenice oblika $\neg A$)

Prema dijagonalnoj lemi, postoje rečenice G_T i R_T takve da

- $T \vdash \big(G_T \leftrightarrow \neg Prv_T(\ulcorner G_T \urcorner)\big)$
- $T \vdash \big(R_T \leftrightarrow \forall y \big(Prf_T(\ulcorner R_T \urcorner, y) \rightarrow (\exists z < y) Prf_T(\ulcorner \neg R_T \urcorner, z)\big)\big)$

Rečenicu G_T zovemo **Gödelovom rečenicom** za teoriju T, a R_T **Rosserovom rečenicom** za T.

Gödelova i Rosserova rečenica

Za rečenicu F kažemo da je **neodlučiva** u teoriji T ako ne vrijedi niti $T \vdash F$ niti $T \vdash \neg F$.

Gödelov prvi teorem nepotpunosti u Rosserovu obliku

Neka je T konzistentno i aksiomatizabilno proširenje od Q.

Tada je Rosserova rečenica R_T neodlučiva za teoriju T.

Teorija T u jeziku aritmetike je ω-**inkonzistentna** ako postoji formula $F(x)$ takva da $T \vdash \exists x F(x)$, ali $T \vdash \neg F(\overline{n})$ za svaki $n \in \mathbb{N}$. Inače je ω-**konzistentna**. Svaka ω-konzistentna teorija je konzistentna, ali obrat ne vrijedi općenito.

Gödelov prvi teorem nepotpunosti u originalnom obliku

Neka je T konzistentno i aksiomatizabilno proširenje od Q.

Tada je Gödelova rečenica G_T nedokaziva u T. Ako je teorija T ω-konzistentna, onda ni rečenica $\neg G_T$ nije dokaziva u T.

Peanova aritmetika

Sistem PA uz prvih šest aksioma minimalne aritmetike

(Q1) $\neg(x' = 0)$

(Q2) $x' = y' \to x = y$

(Q3) $x + 0 = x$

(Q4) $x + y' = (x + y)'$

(Q5) $x \cdot 0 = 0$

(Q6) $x \cdot y' = (x \cdot y) + x$

sadrži i shemu aksioma indukcije (F je proizvoljna formula):

$$\big(F(0) \land \forall x(F(x) \to F(x'))\big) \to \forall x\, F(x)\,.$$

[Ovdje jezik ne sadrži simbol $<$, no možemo
$x < y$ shvatiti kao pokratu za $\exists z(x + z' = y)$.]

U tom smislu, i koristeći indukciju (i ostale aksiome),
mogu se dokazati (Q7), (Q8) i (Q9),
pa Peanovu artimetiku PA možemo smatrati proširenjem teorije Q.

Konzistentnost

Neka je T proširenje od Q.
Teorija T je konzistentna ako i samo ako postoji rečenica koja iz nje nije izvediva — ili ekvivalentno, ako i samo ako postoji rečenica F takva da F i $\neg F$ nisu istovremeno teoremi od T.

Iz aksioma (Q1) slijedi $T \vdash 0' \neq 0$. Dakle, T je konzistentna ako i samo ako $T \nvdash \lightning := (0' = 0)$. Označimo

$$Con_T := \neg Prv_T(\ulcorner \lightning \urcorner) = \neg Prv_T(\overline{2\,656\,569\,985\,699}).$$

Za općenite teorije može biti netrivijalno pitanje koja formula „dobro izražava" njihovu konzistentnost, ali kao što vidimo, za *aritmetičke* teorije (u jeziku aritmetike) to je pitanje bitno lakše.

Hilbert–Bernaysovi uvjeti

Definicija

Za teoriju T, **predikat dokazivosti** *je formula $B(x)$ s jednom slobodnom varijablom koja zadovoljava uvjete:*

(P1) *ako* $T \vdash A$*, onda* $T \vdash B(\ulcorner A \urcorner)$

(P2) $T \vdash B(\ulcorner A \to A' \urcorner) \to \big(B(\ulcorner A \urcorner) \to B(\ulcorner A' \urcorner)\big)$

(P3) $T \vdash B(\ulcorner A \urcorner) \to B\big(\ulcorner B(\ulcorner A \urcorner) \urcorner\big)$

(za sve rečenice A i A' u jeziku teorije T).

Pravi predikat dokazivosti *zadovoljava i obrat svojstva* (P1).

[Primjer: $x = x$ jest predikat dokazivosti, ali nije pravi.]

Lema (Hilbert–Bernays)

Neka je T konzistentno i aksiomatizabilno proširenje od PA. Tada je $Prv_T(x)$ predikat dokazivosti za T. Ako je T ω-konzistentna, onda je to pravi predikat dokazivosti.

Dokaz ispuštamo, uz naglasak da ovdje nije dovoljno da T proširuje Q, jer se u dokazu koristi i shema aksioma indukcije.

Drugi dokaz prvog Gödelova teorema

Gödelov prvi teorem nepotpunosti može se dokazati
i primjenom Hilbert–Bernaysovih uvjeta izvedivosti.

Neka je T aksiomatizabilno i ω-konzistentno proširenje od PA.

Prema dijagonalnoj lemi, postoji rečenica G_T
takva da $T \vdash G_T \leftrightarrow \neg Prv_T(\ulcorner G_T \urcorner)$.

Pretpostavimo $T \vdash G_T$. Iz gornjeg tada slijedi $T \vdash \neg Prv_T(\ulcorner G_T \urcorner)$.

S druge strane, iz pretpostavke $T \vdash G_T$ i uvjeta (P1) slijedi
$T \vdash Prv_T(\ulcorner G_T \urcorner)$. Time smo dobili da je T inkonzistentna,
suprotno početnoj pretpostavci. Dakle, mora vrijediti $T \nvdash G_T$.

Iz obrata (P1) slijedi $T \nvdash Prv_T(\ulcorner G_T \urcorner)$. Dakle, $T \nvdash \neg G_T$.

Logika dokazivosti

Pišući $\Box A$ umjesto $Prv_T(\lceil A \rceil)$, Hilbert–Bernaysovi uvjeti postaju:

(P1) ako $\vdash A$, onda $\vdash \Box A$ — pravilo izvoda u modalnoj logici

(P2) $\vdash \big(\Box(A \to A') \to (\Box A \to \Box A')\big)$ — aksiom **K**

(P3) $\vdash (\Box A \to \Box\Box A)$ — tranzitivnost (što s (P2) zovemo **K4**)

Za proširenje sistema **K4** *Löbovom formulom*

$$\big(\Box(\Box A \to A) \to \Box A\big),$$

koje zovemo **sistem GL** (Gödel–Löb),
vrijede teoremi adekvatnosti i potpunosti u odnosu na klasu svih tranzitivnih i inverzno dobro utemeljenih Kripkeovih okvira.

Löbova formula *nije* posljedica samo Hilbert–Bernaysovih uvjeta, ali jest posljedica dijagonalne leme, odnosno postojanja *fiksnih točaka* odgovarajućih modalnih formula.

Gödelov drugi teorem nepotpunosti

Teorem (Gödel)

Neka je T konzistentno i aksiomatizabilno proširenje teorije PA.

Tada vrijedi: $T \vdash (Con_T \to G_T)$.

U dokazu koristimo modalnu notaciju s prethodnog slajda.
Također, pišemo $\vdash A$ umjesto $T \vdash A$, i G umjesto G_T.

Dokaz.

Iz (P1) i (P2) slijedi da za sve rečenice A i B vrijedi: ako $\vdash A \to B$, onda $\vdash \Box A \to \Box B$. No $\vdash G \leftrightarrow \neg\Box G$, pa onda i $\vdash \neg G \leftrightarrow \Box G$, iz čega slijedi $\vdash \Box\neg G \leftrightarrow \Box\Box G$.

Prema (P3) je $\vdash \Box G \to \Box\Box G$, pa je $\vdash \Box G \to \Box\neg G$.

Očito $\vdash G \to (\neg G \to \lightning)$ (jer je to sudovno valjana formula).

Slijedi $\vdash \Box G \to (\Box\neg G \to \Box\lightning)$. Iz prethodnog (po logičkom aksiomu (A2)) je $\vdash \Box G \to \Box\lightning$, dakle $\vdash \neg\Box\lightning \to \neg\Box G$.

Sada iz $\vdash \neg\Box G \leftrightarrow G$ slijedi tvrdnja. $\Box$

Iz prvog i drugog Gödelova teorema slijedi $T \nvdash Con_T$.

Löbov teorem

Gödelova rečenica je fiksna točka formule $\neg Prv_T(x)$.

Prema dijagonalnoj lemi, postoji i fiksna točka formule $Prv_T(x)$ (kao i mnoge druge fiksne točke):
Henkinova rečenica H takva da $T \vdash H \leftrightarrow Prv_T(\ulcorner H \urcorner)$.

Je li ona dokaziva? **Jest**, što slijedi iz sljedećeg teorema.

Teorem (Löb)

Neka je T konzistentno i aksiomatizabilno proširenje teorije PA. Tada za svaku rečenicu A vrijedi

$$T \vdash Prv_T(\ulcorner A \urcorner) \to A \quad \textit{ako i samo ako} \quad T \vdash A\,.$$

Dokaz Löbova teorema sasvim je analogan dokazu drugog Gödelova teorema (s prethodnog slajda), samo što umjesto konkretne fiksne točke G_T trebamo općenitu fiksnu točku Ψ takvu da $T \vdash \Psi \leftrightarrow \big(Prv_T(\ulcorner \Psi \urcorner) \to A\big)$, koja postoji po dijagonalnoj lemi ($\Psi = G_T$ se dobije za $A := \lightning$).

Aritmetička potpunost

Definicija

Aritmetička interpretacija *je funkcija* * *koja svakoj modalnoj formuli pridružuje rečenicu jezika aritmetike tako da vrijedi:*

- $\perp^* = \lightning$
- $(A \to B)^* = (A^* \to B^*)$
- $(\Box A)^* = Prv_{PA}(\ulcorner A \urcorner)$

(Aritmetička interpretacija je zadana svojim djelovanjem na propozicijskim varijablama.)

Teorem (Solovay)

Za svaku modalnu formulu F *vrijedi:* F *je teorem sistema* **GL** *ako i samo ako* $PA \vdash F^*$ *za svaku aritmetičku interpretaciju* *.

Vremenska složenost

Za svaki algoritam važno je koliko vremenskih i prostornih resursa treba za njegov rad. Vremenska i prostorna složenost iskazuju se kao funkcije veličine ulaznih podataka za algoritam.

Teorija složenosti ne bavi se prvenstveno proučavanjem potrebnih resursa za pojedini algoritam, već razmatra odnos među klasama algoritama „iste" složenosti.

Definicija

Vremenska složenost determinističnog Turingova stroja T *je funkcija* $time_T : \mathbb{N} \to \mathbb{N}$, *gdje je* $time_T(n)$ *maksimalni broj koraka koje stroj* T *napravi za svaki ulazni podatak duljine* n.

Vremenska složenost nedeterminističnog Turingova stroja N *je funkcija* $time_N : \mathbb{N} \to \mathbb{N}$, *gdje je* $time_N(n)$ *maksimalni broj koraka (uzimajući u obzir sve grane) koje stroj* N *napravi za svaki ulazni podatak duljine* n.

Prostorna složenost

Definicija

Prostorna složenost determinističnog Turingova stroja T *je funkcija* $space_T : \mathbb{N} \to \mathbb{N}$, *gdje je* $space_T(n)$ *maksimalni broj ćelija (uzimajući u obzir sve trake) po kojima stroj* T *čita i piše, za svaki uzlazni podatak duljine* n.

Prostorna složenost nedeterminističnog Turingova stroja N *je funkcija* $space_N : \mathbb{N} \to \mathbb{N}$, *gdje je* $space_N(n)$ *maksimalni broj ćelija (uzimajući u obzir sve trake i sve grane) po kojima stroj* N *čita i piše, za svaki ulazni podatak duljine* n.

Asimptotska analiza

Točno vrijeme/prostor potreban za rad stroja je teško ili nemoguće izračunati, a i nije prikladno za razmatranje odnosa među različitim algoritmima. Stoga ga procjenjujemo **za velike ulazne podatke**.

U takvoj **asimptotskoj analizi**, npr. ako promatramo polinom, bitan je samo vodeći član — ostale zanemarujemo jer vodeći član dominira nad ostalim članovima za ulazne podatke velike duljine.

Štoviše, asimptotska analiza zanemaruje čak i koeficijent uz vodeći član, ostavljajući samo stupanj polinoma kao bitni podatak.

Mi ćemo ići i dalje, tako što će nam svi polinomi predstavljati istu klasu složenosti.

$\mathcal{O}$-notacija

Definicija

Neka su $f, g : \mathbb{N} \to \mathbb{R}_{0+} := \{x \in \mathbb{R} : x \geq 0\}$ *proizvoljne funkcije.*

Pišemo $f(n) = \mathcal{O}\big(g(n)\big)$, *odnosno kratko* $f = \mathcal{O}(g)$,
ako postoje prirodni brojevi c *i* n_0 *takvi da*
za svaki prirodan broj $n \geq n_0$ *vrijedi* $f(n) \leq c \cdot g(n)$.

Definicija

(Ne)deterministički Turingov stroj T *je:*

- **polinoman** *ako je* $time_T(n) = \mathcal{O}\big(p(n)\big)$ *(za neki polinom* p*)*
- **eksponencijalan** *ako je* $time_T(n) = \mathcal{O}\big(2^{p(n)}\big)$
- **prostorno polinoman** *ako je* $space_T(n) = \mathcal{O}\big(p(n)\big)$
- **prostorno eksponencijalan** *ako je* $space_T(n) = \mathcal{O}\big(2^{p(n)}\big)$

Problem SAT

Problem SAT: odrediti je li zadana formula logike sudova ispunjiva

Semantičke tablice su jedan algoritam koji rješava problem SAT, ali za formulu s n propozicijskih varijabli u najgorem slučaju treba $\mathcal{O}(2^n)$ koraka, dakle semantičke tablice su eksponencijalni (nepolinomni) algoritam.

Problem SAT se obično promatra za formule u konjunktivnoj normalnoj formi, jer je tako jednostavnije, a *za svaku formulu logike sudova se može u polinomnom vremenu odrediti konjunktivna normalna forma koja je ispunjiva ako i samo ako je početna formula ispunjiva* (Cejtinov algoritam).

Ako svaka elementarna disjunkcija sadrži najviše n literala, govorimo o problemu n-SAT.

Trošak simulacije višetračnih/nedeterminističnih strojeva

Teorem (simulacija višetračnog stroja jednotračnim)

Neka je $f : \mathbb{N} \to \mathbb{R}_{0+}$ funkcija takva da je $f(n) \geq n$ za svaki $n \in \mathbb{N}$. Tada za svaki Turingov stroj s više traka vremenske složenosti $f(n)$ postoji ekvivalentni Turingov stroj s jednom trakom, vremenske složenosti $\mathcal{O}\big(f^2(n)\big)$.

Teorem (simulacija nedeterminističnog stroja determinističnim)

Neka je $f : \mathbb{N} \to \mathbb{R}_{0+}$ funkcija takva da je $f(n) \geq n$ za svaki $n \in \mathbb{N}$. Tada za svaki nedeterministični Turingov stroj vremenske složenosti $f(n)$ postoji ekvivalentni deterministični Turingov stroj vremenske složenosti $2^{\mathcal{O}(f(n))}$.

Klase složenosti

Definicija

Neka je $f : \mathbb{N} \to \mathbb{R}_{0+}$ *proizvoljna funkcija. Klasa* $DTIME\big(f(n)\big)$ *je skup svih jezika (nad fiksiranom abecedom) koji su odlučivi nekim* $\mathcal{O}(f)$*-vremenski složenim determinističnim Turingovim strojem.*

Klasa $NTIME\big(f(n)\big)$ *je skup svih jezika (nad fiksiranom abecedom) koji su odlučivi nekim* $\mathcal{O}(f)$*-vremenski složenim nedeterminističnim Turingovim strojem.*

$$P := \bigcup_{k \in \mathbb{N}} DTIME(n^k) \qquad NP := \bigcup_{k \in \mathbb{N}} NTIME(n^k)$$

Polinomna svedivost (reducibilnost)

Definicija

Neka su Σ_1 *i* Σ_2 *proizvoljne abecede. Funkcija* $f : \Sigma_1^* \to \Sigma_2^*$ *je* **vremenski polinomno izračunljiva** *ako postoji polinomno vremenski složen Turingov stroj koji za svaku* $w \in \Sigma_1^*$ *kao ulazni podatak na izlaznoj traci u završnom stanju ima* $f(w)$*.*

Jezik $L_1 \subseteq \Sigma_1^*$ *je* **polinomno svediv** *na jezik* $L_2 \subseteq \Sigma_2^*$ *ako postoji polinomno vremenski izračunljiva funkcija* $f : \Sigma_1^* \to \Sigma_2^*$ *takva da za svaku* $w \in \Sigma_1^*$ *vrijedi:* $w \in L_1$ *ako i samo ako* $f(w) \in L_2$*.*

Propozicija

Relacija „biti polinomno svediv na" je tranzitivna.

Propozicija

Ako jezik pripada klasi P (odnosno NP), onda i svaki jezik polinomno svediv na njega također pripada klasi P (odnosno NP).

NP-teški problemi

Definicija

Za problem S kažemo da je **NP-težak**
ako je svaki problem iz NP polinomno svediv na S.

Primjer

Neka je $D := \{p \in \mathbb{Z}[X_1, \ldots, X_n] : p \text{ ima cjelobrojnu nultočku}\}$.

Iz Matijasevičevog rješenja desetog Hilbertova problema znamo da je jezik D neodlučiv: ne postoji nikakav Turingov stroj koji ga odlučuje, pa posebno $D \notin$ NP.

No, može se pokazati da je D NP-težak jezik.

Iz tog primjera vidimo da problemi mogu biti NP-„preteški"; takvi nam obično nisu zanimljivi.

Zanimljivi su oni koji su „taman dovoljno teški" za klasu NP.

NP-potpunost

Definicija

Kažemo da je jezik L **NP-potpun** *ako vrijedi:*

- *L pripada klasi NP, i*
- *L je NP-težak.*

Propozicija

Neka je L_1 NP-težak jezik i $L_2 \in NP$.

Ako je L_1 polinomno svediv na L_2, onda su L_1 i L_2 NP-potpuni.

Teorem (Cook–Levin)

Problem SAT je NP-potpun. (Štoviše, 3-SAT je NP-potpun.)

Napomena

Kad bi postojao polinomni algoritam koji rješava neki NP-potpun problem, u polinomnom bi vremenu bili rješivi svi NP problemi.

Klase prostorne složenosti

Definicija

Neka je $f : \mathbb{N} \to \mathbb{R}_{0+}$ proizvoljna funkcija. Definiramo:

- **DSPACE**$\big(f(n)\big) := \{L : L$ *je jezik odlučiv nekim* $\mathcal{O}\big(f(n)\big)$ *prostorno složenim determinističnim Turingovim strojem*$\}$
- **NSPACE**$\big(f(n)\big) := \{L : L$ *je jezik odlučiv nekim* $\mathcal{O}\big(f(n)\big)$ *prostorno složenim nedeterminističnim Turingovim strojem*$\}$
- **PSPACE** $:= \bigcup_{k\in\mathbb{N}} DSPACE(n^k)$,
  NPSPACE $:= \bigcup_{k\in\mathbb{N}} NSPACE(n^k)$

Kažemo da je $f : \mathbb{N} \to \mathbb{N}$ **dobro izračunljiva** *ako postoji deterministični stroj T koji izračunava f u vremenu $\mathcal{O}\big(f(n)\big)$.*

Teorem (Savitch)

Ako je $f : \mathbb{N} \to \mathbb{N}$ dobro izračunljiva funkcija i za svaki $n \in \mathbb{N}$ vrijedi $f(n) \geq \log n$, onda je $NSPACE\big(f(n)\big) \subseteq DSPACE\big(f^2(n)\big)$.

Korolar

$PSPACE = NPSPACE$.

λ-račun: motivacija

Vidjeli smo (grubu skicu) kako izgleda funkcijsko programiranje na brojevima (parcijalno rekurzivne funkcije), i imperativno programiranje na riječima (Turingovi strojevi).

Prirodno je zapitati se kako bi izgledalo funkcijsko programiranje na riječima.

Odgovor daje *λ-račun* A. Churcha, izvorno osmišljen kao primarna formalizacija koncepta izračunljivosti.

> [Ipak, Turingovi strojevi su bolje odgovarali intuiciji.]
>
> Gödel: *"The correct definition of mechanical computability was established beyond any doubt by Turing."*

No, Turingovi strojevi su prilično teški za programiranje netrivijalnih algoritama, jer su preniske razine apstrakcije.

λ-račun je (programski) jezik mnogo više razine.

[Sandro Lovnički: pLam]

λ-račun: jezik

Jezik λ-računa čine:

- prebrojivo mnogo varijabli: $Var := \{x_i : i \in \mathbb{N}\}$.
  Varijable označavamo malim slovima: često u, v, x, y, z.
- apstraktor λ, točka . i zagrade ().

λ-izrazi su nizovi gornjih simbola koji se definiraju rekurzivno:

varijabla Svaka varijabla je λ-izraz.

aplikacija Ako su M i N λ-izrazi, tada je i (MN) λ-izraz.

apstrakcija Ako je M λ-izraz i x varijabla, tada je $\lambda x.M$ λ-izraz.

Intendirana interpretacija: λ-izrazi predstavljaju funkcije (koje preslikavaju λ-izraze u λ-izraze, jer jedino takvi objekti ovdje postoje). Aplikacija je primjena funkcije M na N, a apstrakcija je konstrukcija funkcije koja svoj argument nazvan x preslikava u M (supstituirajući argument umjesto varijable x u izrazu M). Standardni zapisi su $M(N)$ i $x \mapsto M$.

λ-račun: konvencije

Zagrade u aplikaciji ne pišemo uvijek. Smatramo da aplikacija veže jače nego apstrakcija [$\lambda x.MN$ je $\lambda x.(MN)$, ne $(\lambda x.M)N$], te je asocirana ulijevo [$M_1 M_2 M_3$ je $(M_1 M_2) M_3$, ne $M_1(M_2 M_3)$].

Više ugniježđenih apstrakcija pišemo zajedno: $\lambda xy.M$ je $\lambda x.\lambda y.M$. Tako reprezentiramo funkcije više argumenata (*currying*).

Zasad su λ-izrazi samo statični nizovi znakova. Da bismo računali s njima, opisat ćemo *konverzije*, kojima možemo pretvoriti jedan λ-izraz u drugi, (na neki način) ekvivalentni.

Varijabla x je *vezana* ako je u dosegu apstraktora λx, a *slobodna* inače. (Naravno, zapravo treba govoriti o *pojavama* varijabli.)

Konverzija α je odabir nove, još nekorištene varijable, i zamjena svih (vezanih) pojava jedne vezane varijable tom novom varijablom. Tako postižemo da su vezane varijable disjunktne sa slobodnima.

$$(\lambda x_1.x_1)x_1 \overset{\alpha}{\Rightarrow} (\lambda x_2.x_2)x_1$$

Računanje u λ-računu

Konverzija β se odnosi na *redekse*: podizraze oblika $(\lambda x.M)N$. Takav podizraz se *reducira*: zamjenjuje izrazom dobivenim iz M zamjenom svih slobodnih (u M!) pojava od x s izrazom N. Pritom ćemo (konverzijom α) osigurati da M nema *vezanih* pojava varijable x, niti ikoje varijable koja je slobodna u N.

$$\big(\lambda x_1 x_2.x_2(\lambda x_1.x_1)x_1\big)(x_2x_4) \overset{\alpha}{\Rightarrow} \big(\lambda x_1.\lambda x_2.x_2(\lambda x_3.x_3)x_1\big)(x_2x_4) \overset{\alpha}{\Rightarrow}$$
$$\overset{\alpha}{\Rightarrow} \big(\lambda x_1.\lambda x_5.x_5(\lambda x_3.x_3)x_1\big)(x_2x_4) \overset{\beta}{\Rightarrow} \lambda x_5.x_5(\lambda x_3.x_3)(x_2x_4)$$

Konverzija η je „pojednostavljivanje" podizraza oblika $\lambda x.Mx$ u M, pod uvjetom da M ne sadrži slobodnu pojavu varijable x.

$$\lambda x_1x_2.x_1x_2 = \lambda x_1.(\lambda x_2.x_1x_2) \overset{\eta}{\Rightarrow} \lambda x_1.x_1 =: \mathtt{I}$$

Jedna zabavna interpretacija — aligatori i njihova jaja:
`http://worrydream.com/AlligatorEggs/`

Normalne forme i kombinatori

λ-izraz bez slobodnih varijabli zovemo *kombinator*,
a za onaj bez redeksa kažemo da je u *normalnoj formi*.
Kombinatori u normalnoj formi su „izračunati do kraja".
(Možda se još mogu pojednostaviti konverzijom η.)

Oznakom $\Rightarrow^*$ označavamo refleksivno i tranzitivno zatvorenje unije konverzija α i β (kao binarnih relacija na λ-izrazima).

Teorem (Church–Rosser, o konfluentnosti λ-računa)

*Ako su M_1, M_2 i M_3 λ-izrazi takvi da $M_1 \Rightarrow^* M_2$ i $M_1 \Rightarrow^* M_3$,
tada postoji λ-izraz M_4 takav da $M_2 \Rightarrow^* M_4$ i $M_3 \Rightarrow^* M_4$.*

Korolar

Normalna forma λ-izraza, ako postoji, jedinstvena je — i dobije se **standardnim** *računanjem, koje uvijek reducira prvi vanjski redeks.*

Primjer

Postoje λ-izrazi, čak i kombinatori, *bez* normalne forme:
najjednostavniji je $\omega := (\lambda x.xx)(\lambda x.xx)$.

Reprezentacija vrijednosti u λ-računu

Kako samo pomoću funkcija reprezentirati statične objekte?
Ideja: apstrakcijom „prizovemo u postojanje” objekte koje želimo.

Najjednostavnije je ako trebamo reprezentirati elemente nekog konačnog skupa. Uzmimo za primjer $bool = \{\mathtt{T}, \mathtt{F}\}$.

Tehnika „*wishful thinking*”: *kad bismo imali* neka dva objekta t i f, *mogli bismo* $\mathtt{T}$ definirati kao t, a $\mathtt{F}$ kao f.

No možemo ih „imati” tako da ih apstrahiramo.

$$\mathtt{T} := \lambda t\,f.t$$
$$\mathtt{F} := \lambda t\,f.f$$

Drugim riječima, logička vrijednost je selekcija, od dva argumenta, prvog ili drugog. To zapravo znači da ako je b tipa *bool*, bMN prelazi u M ako je b istina, a u N ako je b laž (ternarni operator).

Sad je lako napraviti i logičke „veznike”: npr. $\mathtt{not} := \lambda b.b\,\mathtt{F}\,\mathtt{T}$, $\mathtt{or} := \lambda xy.xxy \overset{\eta}{\Rightarrow} \lambda x.xx$, a iz ta dva se mogu dobiti svi ostali.

Churchovi numerali

Prirodne brojeve (tip *nat*) možemo vrlo slično reprezentirati.

Kad bismo imali neka dva objekta z (nulu) i s (sljedbenik), *mogli bismo* prirodni broj n dobiti n-strukom primjenom s na z.

$$n := \lambda s\,z.s(s(\cdots s(z)\cdots))$$

Konkretno $\mathtt{0} := \lambda sz.z \overset{\alpha}{\Rightarrow} \mathtt{F}$, $\mathtt{1} := \lambda sz.sz \overset{\eta\alpha}{\Longrightarrow} \mathtt{I}$, $2 := \lambda sz.s(sz)$ itd.

To zapravo znači da ako je n tipa *nat*, $n\,f\,x$ znači „n puta primijeni f na x" (ograničena petlja).

Opet, nije problem napraviti aritmetičke operacije:
$\mathtt{add} := \lambda xysz.xs(ysz)$, $\mathtt{mul} := \lambda xysz.x(ys)z \overset{\eta}{\Rightarrow} \lambda xys.x(ys)$.

Sljedbenik je jasan, $\mathtt{Sc} := \lambda nsz.s(nsz)$, no što je prethodnik?

Primitivna rekurzija

U teoriji izračunljivosti, prethodnik se definira degeneriranom primitivnom rekurzijom:

$$pd(0) := 0,$$
$$pd(n+1) := n.$$

Usporedimo običnu iteraciju i (malo modificiranu) degeneriranu primitivnu rekurziju:

$$\begin{aligned} 0\,h\,a &\Rightarrow^* a & \qquad pr\,0\,h\,a &\Rightarrow^* a \\ (\mathtt{Sc}\,n)\,h\,a &\Rightarrow^* h\,(n\,h\,a) & \qquad pr\,(\mathtt{Sc}\,n)\,h\,a &\Rightarrow^* h\,(pr\,n\,h\,a, n) \end{aligned}$$

Vidimo da pored prethodne vrijednosti, funkcija h mora primiti još jedan argument: „kontrolnu varijablu" koja označava u kojem smo prolasku. Zato moramo kodirati *parove*. (*Currying* ne funkcionira jer iteracija zahtijeva da se oba argumenta prenesu odjednom.)

Parovi

Uređene parove možemo predstaviti kao funkcije s domenom *bool*.

$$\langle x, y\rangle := \lambda b.b\,x\,y \qquad\qquad \mathtt{fst} := \lambda p.p\,\mathtt{T}$$
$$\mathtt{pair} := \lambda xy.\langle x, y\rangle \qquad\qquad \mathtt{snd} := \lambda p.p\,\mathtt{F}$$

Sada možemo i reprezentirati funkcije dviju varijabli
na tradicionalniji način: uvodimo pokratu

$$\lambda\langle x, y\rangle.M := \lambda p.(\lambda xy.M)(\mathtt{fst}p)(\mathtt{snd}p)$$

Pomoću toga lako simuliramo primitivnu rekurziju,
„unaprijeđujući" f tako da vodi računa i o broju koraka:

$$\tilde{f} := \lambda\langle z, n\rangle.\langle f\,z\,n, \mathtt{Sc}\,n\rangle$$
$$\mathtt{pr} := \lambda nfx.\mathtt{fst}(n\,\tilde{f}\,\langle x, 0\rangle)$$

Zadatak: Isprogramirajte faktorijel pomoću kombinatora $\mathtt{pr}$.

Kompliciranije strukture

Sada je lako isprogramirati prethodnik: da bismo izračunali prethodnik od n, n puta na 0 primijenimo funkciju koja prima prethodno izračunatu vrijednost prethodnika i broj prolazaka, te vraća broj prolazaka.

$$\mathtt{pd} := \lambda n.\, \mathtt{pr}\, n\, (\lambda zb.b)\, 0$$

Analogno tipu *bool* možemo reprezentirati sve konačne tipove, pa tako i konačne nizove, kao što smo ovdje učinili s parovima.

Pomoću prirodnih brojeva i konačnih nizova možemo reprezentirati („kodirati") razne diskretne matematičke strukture.

Primjerice, konačni usmjereni graf možemo kodirati tako da vrhove predstavimo prirodnim brojevima, a bridove parovima brojeva.

Sada možemo implementirati sve algoritme s ograničenim petljama na takvim strukturama. No što je s *neograničenim* petljama?

Pseudoλ

λ-izraze možemo shvatiti kao jednostavne programe.

def f x y z: return M	$\leftrightsquigarrow$	$f = \lambda x\, y\, z.M$

def f x y z:
    $a = N_1$
    $b = N_2$
    return M
	$\leftrightsquigarrow$	$f = \lambda x\, y\, z.\big(\lambda a.$
		$(\lambda b.M)N_2$
		$\big)N_1$

def f x y z:
    if N_1: return M_1
    elif N_2: return M_2
    else: return M_0
	$\leftrightsquigarrow$	$f = \lambda x\, y\, z.$
		$N_1 M_1 (N_2 M_2 M_0)$

Petlju for (ograničenu) smo vidjeli na slajdu „primitivna rekurzija”.
Za neograničene petlje trebaju nam općenite rekurzije.

Kombinator $\mathtt{Y}$

def rec *fakt* *n*:
    if *n* == 0: return 1
    else: return *n*∗*fakt*(*n*−1)

$\leftrightsquigarrow$

$$rec = \lambda\, fakt\, n.\, 0?\, n\, 1\, (\mathtt{mul}\, n(fakt(\mathtt{pd}(\mathtt{n}))))$$

(sami napišite 0? pomoću $\mathtt{pr}$ — može se i jednostavnije!)

Ključno je prenijeti funkciju *fakt* kao jedan od argumenata, da bi bila dostupna unutar tijela *rec*. Sad je *fakt* **fiksna točka** od *rec*:

$$fakt \Rightarrow^* rec\ fakt$$

(pazite na smjer!) To postižemo s $fakt := \mathtt{Y}\, rec$, gdje je

$$\mathtt{Y} := \lambda\, rec.\big(\lambda x.\, rec(x\,x)\big)\big(\lambda x.\, rec(x\,x)\big).$$

Zadatak: Dokažite da je svaka parcijalno rekurzivna funkcija prikaziva nekim kombinatorom (na Churchovim numeralima).