Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odjel

Tajana Ban Kirigin

Logika višeg reda i sustav Isabelle

Magistarski rad

Zagreb, 2004.

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odjel

Tajana Ban Kirigin

Logika višeg reda i sustav Isabelle

Magistarski rad

Voditelj rada:
prof.dr.sc. Dean Rosenzweig

Zagreb, 2004.

Sadržaj

Uvod

Predikatska logika ili logika prvog reda javlja se kao razvijena logička teorija oko 1930. godine kada su dokazana neka meta-svojstva kao što su potpunost, kompaktnost i Skolem-Löwenheim teoremi. Teorije višeg reda sustavnije se proučavaju od šezdesetih godina prošlog stoljeća. Motivacija za to proučavanje pronalazi se u ograničenjima logike prvog reda. Formulama prvog reda ne mogu se iskazati neki standardni matematički pojmovi kao što su konačnost ili pak prebrojivost skupa. Nemoguće je kategorički karakterizirati skup prirodnih brojeva.
Ti se skupovi mogu okarakterizirati jezikom logike drugog reda. Ona je proširenje logike prvog reda koje se dobije uvođenjem relacijskih i funkcijskih varijabli. Nedostatak je ove logike što za nju ne važi teorem potpunosti, kompaktnosti, niti Skolem-Löwenheimovi teoremi.

Isabelle je interaktivni dokazivatelj teorema. To je generički sistem za implementaciju raznih logičkih formalizama. Te tzv. objektne logike formalizirane su njenom meta-logikom. *Isabelle/HOL* je specijalizacija Isabelle za logiku višeg reda (HOL-Higer Order Logic) ili simple type theory, a bazira se na tipiziranom λ računu. Meta-logiku čine formule koje predstavljaju pravila. Kombinacijom pravila grade se dedukcije u meta-logici, meta-dokazi. Oni reprezentiraju dokaze iz objektne logike. Smisleno je stoga da je reprezentacija korektna i potpuna.

Ovaj je rad podijeljen u dva dijela. Prvi se odnosi na logiku drugog reda. Drugi dio odnosi se na Isabelle, generički dokazivatelj teorema koji implementira logiku višeg reda.
U 1. poglavlju uvodi se sintaksa, a u 2. standardna semantika logike drugog reda. U 3. poglavlju pokazuje se gubitak najvećih rezultata koji vrijede za logiku prvog reda. U 4. poglavlju prezentiraju se deduktivni sustavi pomoću kojih se upoznajemo s dokazivanjem. U 5. poglavlju uvodi se nestandardna semantika logike drugog reda, Henkinova semantika, te se pokazuje da osnovni rezultati logike prvog reda vrijede u ovoj semantici. U 6. poglavlju pokazuje se odnos logike višeg reda i logike drugog reda.
U 7. poglavlju uvodi se sintaksa i semantika meta-logike. U 8. poglavlju formalizira se logika prvog reda, te se pokazuje korektnost i potpunost reprezentacije te objektne logike. U 9. poglavlju prelazi se na dokazivanje pomoću Isabelle opisujući metodu dokazivanja unatrag. Konačno, u 10. poglavlju prezentira se osnovna interakcija s Isabelle, te deduktivne metode.

Zahvaljujem voditelju magistarske radnje, dr.sc. Deanu Rosenzweigu, na interesantnoj temi, te svemu što me naučio.
Posebno se želim zahvaliti mr.sc. Paoli Glavan na svesrdnoj pomoći pri izradi ove radnje.
Svim kolegama i prijateljima sa Seminara za teorijsko računarstvo i Seminara za osnove matematike i matematičku logiku, te s Filozofskog Fakulteta u Rijeci hvala na razumijevanju i pruženoj pomoći.

Tajana Ban Kirigin

Dio I
Logika drugog reda

Logika drugog reda proširenje je logike prvog reda. Ono se sastoji u tome da se osim kvantifikacije po elementima domene, dozvoli i kvantifikacija po relacijama i funkcijama na domeni.

Ne proširuje se skup nelogičkih simbola, tj. signatura. Stoga se ne mijenja pojam jezika niti interpretacija: jezik je zadan prebrojivim skupom nelogičkih simbola, a interpretaciju jezika čine domena i funkcija koja svakom nelogičkom simbolu pridružuje njegovu denotaciju.
Uvode se novi tipovi varijabli: relacijske i funkcijske varijable (te kvantifikacija po njima). Varijable logike prvog reda nazivat ćemo individualnim varijablama. Ono što treba proširiti je definicija formule i definicija istinitosti, tj. što to znači da je formula istinita u nekoj interpretaciji.

Logika se može dalje proširiti uvođenjem varijabli koje su relacije relacija, funkcije na relacijama, funkcije na funkcijama itd. To bi bile varijable trećeg reda. Jezik bismo mogli proširiti i nelogičkim simbolima, npr. konstantom koja je relacija među funkcijama na funkcijama.
Proširenja mogu ići dalje na varijable četvrtog reda: npr. varijable koje su relacije među funkcijama na relacijama. I tako dalje.
Ako jezik sadrži varijable n-tog reda, za svaki prirodni broj n, kažemo da je jezik reda ω.
Pokazuje se, međutim, da višim logikama ne dobivamo na izražajnosti, pa je u tom smislu dovoljna logika drugog reda.

1 Sintaksa logike drugog reda

Jezik logike drugog reda zadan je znakovima tj. alfabetom i pravilima kako se iz znakova grade formule. Time je određeno koje konačne nizove znakova, odnosno riječi smatramo formulama logike drugug reda.

Definicija 1. Alfabet *logike drugog reda sastoji se od logičkih simbola:*

logički veznici $\neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow$

kvantifikatori $\forall \quad \exists$

pomoćni simboli $(\quad) \quad ,$

individualne varijable $x, y, z, ..., x_1, x_2, ...$

funkcijske varijable $f, g^2, ..., f_1, f_2, ...$

relacijske varijable $P, R, ..., R_1, R_2^3, ...$

i nelogičkih simbola:

konstantski simboli $a, b, c, ..., c_1, c_2, ...$

funkcijski simboli $f, g, ..., g_1, g_2, ...$

relacijski simboli $P, Q, ..., R_1, R_2^3, ...$

logičke konstante $\top$ *istina i* $\bot$ *laž*

Funkcijske i relacijske varijable i simboli mogu biti unarni, binarni i općenito n-arni što označavamo npr. f^2, R^3, a izostavljamo ako je iz konteksta jasno o kojoj se mjesnosti radi.
Podrazumijeva se, osim toga, i da se istim znakom ne označavaju različiti tipovi varijabli i simbola.

Posebno ćemo promatrati znak jednakosti $=$. Njega možemo smatrati ili logičkim simbolom ili 2-mjesnim relacijskim simbolom.

Možemo reći da smo zadali jezik ako smo zadali pripadni skup nelogičkih simbola K (signaturu).

Definicija 2. Term *logike drugog reda je riječ definirana sljedećom induktivnom definicijom:*

- *svaka individualna varijabla i konstantski simbol je term;*
- *ako je* f^n *n-mjesni funkcijski simbol, a* $t_1, ..., t_n$ *termi, tada je* $\mathsf{f}^n(t_1, ..., t_n)$ *term;*
- *ako je* f^n *n-mjesna funkcijska varijabla, a* $t_1, ..., t_n$ *termi, tada je* $f^n(t_1, ..., t_n)$ *term;*
- *riječ je term logike drugog reda ako i samo ako je nastala pomoću konačno mnogo primjena navedenih pravila.*

Term logike drugog reda je term logike prvog reda ako u njemu ne nastupaju funkcijske varijable.

Definicija 3. Formula *logike drugog reda je riječ definirana sljedećom induktivnom definicijom:*

- *ako je* R *n-mjesni relacijski simbol ili relacijska varijabla, a* $t_1, ..., t_n$ *termi, tada je* $R(t_1, ..., t_n)$ *atomarna formula; logičke konstante* $\top$ *i* $\bot$ *su atomarne formule; svaka atomarna formula je formula;*
- *ako su* A *i* B *formule, tada su* $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$ *i* $A \leftrightarrow B$ *također formule;*
- *ako je* A *formula, a* x *individualna varijabla, tada su* $\forall x\ A$ *i* $\exists x\ A$ *također formule;*
- *ako je* A *formula, a* R *relacijska varijabla, tada su* $\forall R\ A$ *i* $\exists R\ A$ *također formule;*
- *ako je* A *formula, a* f *funkcijska varijabla, tada su* $\forall f\ A$ *i* $\exists f\ A$ *također formule;*
- *riječ je formula logike drugog reda ako i samo ako je nastala pomoću konačno mnogo primjena navedenih pravila.*

Primjer: U logici prvog reda mogli smo izreći svojstvo da, ako su dvije individualne varijable semantički jednake, onda moraju obje zadovoljavati ili obje ne zadovoljavati određeno svojstvo:

$$c = d \rightarrow (Pc \leftrightarrow Pd)$$

U logici drugog reda jednakost se može definirati *Leibnitzovim zakonom o jednakosti nerazlučivih:*

$$c = d \leftrightarrow \forall X(Xc \leftrightarrow Xd)$$

Nastupi svih vrsta varijabli mogu biti slobodni i vezani.

Definicija 4. *Nastup svake varijable u atomarnoj formuli je slobodan. U formulama tipa* $\forall xA, \forall RA, \forall fA$ *svaki nastup individualne varijable* x*, relacijske varijable* R*, odnosno funkcijske varijable* f *je vezan. Ako varijabla* x*,* R *odnosno* f *ima slobodan (vezan) nastup u formuli* A*, tada je taj nastup varijable* x*,* R*, odnosno* f *slobodan (vezan) i u formulama* $\neg A$*,* $A \wedge B$*,* $B \wedge A$*,* $A \vee B$*,* $B \vee A$*,* $A \rightarrow B$*,* $B \rightarrow A$*,* $A \leftrightarrow B$*,* $B \leftrightarrow A$*,* $\forall yA$ *i* $\exists yA$ *gdje je* B *proizvoljna formula, a* y *varijabla različita od varijable* x, R*, odnosno* f*.*
Varijabla *je* slobodna *u formuli* A *ako postoji barem jedan njezin slobodan nastup u formuli* A*. U protivnom je* varijabla vezana *u formuli* A*.*
Formula koja nema slobodnih varijabli naziva se zatvorena formula *ili rečenica.*

Konvencijom o varijablama sve su vezane varijable u svakom kontekstu različite od svih slobodnih varijabli. Nadalje, vezane varijable možemo preimenovati.

Definicija 5. Supstitucijom *varijable* x *termom* t *unutar formule* A *smatramo zamjenu svakog slobodnog nastupa varijable* x *termom* t*, u oznaci* $A(t/x)$*,* $A[t/x]$ *ili* $A(t)$ *ako je iz konteksta jasno o kojoj se supstituciji radi.*

Konvencija o varijablama osigurava da supstitucijom nije moguće vezati slobodnu varijablu.

2 Standardna semantika logike drugog reda

Neka je S neprazan skup nelogičkih simbola jezika logike drugog reda.

Definicija 6. *S-*struktura *je uređeni par $\mathcal{M} = (M, i)$ nepraznog skupa M kojeg nazivamo* domena, nosač *ili* univerzum *i preslikavanja i definiranog na skupu nelogičkih simbola koje ima svojstva:*

- *svakom konstantskom simbolu c_k iz S pridružuje se neki element $i(c_k)$ iz M (također u oznaci $\boldsymbol{c}_k^{\mathcal{M}}$);*
- *svakom funkcijskom simbolu $\mathsf{f}_k^{m_k}$ iz S pridružuje se m_k-mjesna funkcija $i(\mathsf{f}_k^{m_k}) : M^{m_k} \to M$ (također u oznaci $\boldsymbol{f_k}^{\mathcal{M}}$);*
- *svakom relacijskom simbolu $\mathsf{R}_k^{n_k}$ iz S pridružuje se n_k-mjesna relacija $i(\mathsf{R}_k^{n_k})$ na M (također u oznaci $\boldsymbol{R}_k^{\mathcal{M}}$);*
- *logičkoj konstanti $\top$ pridružuje se 1 (istina), a $\bot$ 0 (laž).*

$\mathcal{M} = (M, i)$ *je* struktura za formulu A *ako je funkcija i definirana za svaki nelogički simbol koji nastupa u formuli A.*
$\mathcal{M}$ *je* stuktura za skup formula Γ *ako je $\mathcal{M}$ struktura za svaku formulu iz Γ.*

Definicija 7. *Za danu S-strukturu $\mathcal{M} = (M, i)$* valuacija *v je funkcija koja:*

- *svakoj individualnoj varijabli x pridružuje element domene $v(x)$*
- *svakoj funkcijskoj varijabli f^m pridružuje funkciju $v(f) : M^m \to M$*
- *svakoj relacijskoj varijabli R^n pridružuje n-mjesnu relaciju na M $v(R^n)$, tj. podskup $v(R^n) \subseteq M^n$.*

Definicija 8. *S-*interpretacija *je uređeni par S-strukture $\mathcal{M} = (M, i)$ i valuacije v na M.*

Interpretacijom $I = (\mathcal{M}, v)$ jednoznačno je određena denotacijska funkcija koja je definirana za svaki term logike drugog reda.

Definicija 9. Denotacija *je proširenje valuacije sa skupa varijabli na sve terme:*

$$d(x) = v(x) \quad d(f) = v(f) \quad d(R) = v(R)$$
$$d(c) = i(c) = \boldsymbol{c}^{\mathcal{M}}$$
$$d(\mathsf{f}(\overrightarrow{t})) = i(\mathsf{f})(d(\overrightarrow{t})) = \boldsymbol{f}^{\mathcal{M}}(d(\overrightarrow{t}))$$
$$d(f(\overrightarrow{t})) = d(f)(d(\overrightarrow{t}))$$

Nadalje, za standardnu semantiku, možemo smatrati da je valuacija definirana na skupu svih terama logike drugog reda, na upravo navedeni način.

Definicija 10. *Neka je $I = (\mathcal{M}, v)$ S-interpretacija gdje je $\mathcal{M} = (M, i)$ i v valuacija na $\mathcal{M}$, te neka je F formula izgrađena od simbola iz S.*
Istinitost formule F u interpretaciji I *(u oznaci: $I(F) = 1$, $\mathcal{M} \models_v F$ ili $\mathcal{M}, v \models F$) definiramo induktivno po složenosti formule F:*

- *ako je F atomarna formula oblika $\mathsf{R}(t_1, ..., t_n)$ gdje je R relacijski simbol, tada $\mathcal{M}, v \models F$ ako i samo ako $(v(t_1), ..., v(t_n)) \in i(\mathsf{R}) = \boldsymbol{R}^{\mathcal{M}}$;*
- *ako je F atomarna formula oblika $R(t_1, ..., t_n)$ gdje je R relacijska varijabla, tada $\mathcal{M}, v \models F$ ako i samo ako $(v(t_1), ..., v(t_n)) \in v(R)$;*
- *ako je F logička konstanta, tada $\mathcal{M}, v \models \top$, a nije $\mathcal{M}, v \models \bot$;*
- *ako je F formula oblika $\neg G$, tada $\mathcal{M}, v \models F$ ako i samo ako nije $\mathcal{M}, v \models G$;*
- *ako je F formula oblika $A \wedge B$, tada $\mathcal{M}, v \models F$ ako i samo ako $\mathcal{M}, v \models A$ i $\mathcal{M}, v \models B$;*
- *ako je F formula oblika $A \vee B$, tada $\mathcal{M}, v \models F$ ako i samo ako $\mathcal{M}, v \models A$ ili $\mathcal{M}, v \models B$;*
- *ako je F formula oblika $A \rightarrow B$, tada $\mathcal{M}, v \models F$ ako i samo ako nije $\mathcal{M}, v \models A$ ili je $\mathcal{M}, v \models B$;*
- *ako je F formula oblika $A \leftrightarrow B$, tada $\mathcal{M}, v \models F$ ako i samo ako je $\mathcal{M}, v \models A$ onda i samo onda kad $\mathcal{M}, v \models B$;*
- *ako je F formula oblika $\forall w\, G$, gdje je w individualna varijabla x, funkcijska varijabla f, odnosno relacijska varijabla R, tada $\mathcal{M}, v \models F$ ako i samo ako $\mathcal{M}, v_w \models G$ za svaku valuaciju v_w koja se podudara s valuacijom v na svim varijablama osim možda na varijabli w ;*
- *ako je F formula oblika $\exists w\, G$ gdje je w individualna varijabla x, funkcijska varijabla f, odnosno relacijska varijabla R, tada $\mathcal{M}, v \models F$ ako i samo ako $\mathcal{M}, v_w \models G$ za neku valuaciju v_w koja se podudara s valuacijom v na svim varijablama osim možda na varijabli w.*

Posebno je za terme logike prvog reda t_1i t_2 definirana jednakost:
$\mathcal{M} \models_v t_1 = t_2$ ako i samo ako $v(t_1) = v(t_2)$.

Međutim, jednakost terama logike prvog reda može se u logici drugog reda definirati *Leibnitzovim zakonom o jednakosti nerazlučivih:*

$$t_1 = t_2 := \forall X(Xt_1 \leftrightarrow Xt_2)$$

Jednakost se može definirati i još jednostavnije (nije potreban bikondicional) *Whitehead-Russel definicijom jednakosti*:

$$c = d \leftrightarrow \forall X(Xc \rightarrow Xd)$$

Dokaz. Formula $Pc \rightarrow Pd$ ekvivalentna je formuli $\neg Pc \vee Pd$. Obje su istinite u nekoj interpretaciji onda i samo onda kada skup koji je denotacija od P ne sadrži denotaciju od c ili sadrži denotaciju od d. Stoga je formula $\forall X(Xc \rightarrow Xd)$ istinita ako i samo ako za svaki skup vrijedi da ne sadrži denotaciju od c ili sadrži denotaciju od d. Ako su denotacije terama c i d jednake, to vrijedi za svaki skup; skup ili sadrži ili ne sadrži taj element domene. Ako denotacije terama c i d nisu jednake, tada ta formula nije istinita, budući da npr. skup koji sadrži samo denotaciju od c nema traženo svojstvo. Stoga je formula $\forall X(Xc \rightarrow Xd)$ istinita ako i samo ako termi c i d imaju jednake denotacije. □

Moguće je definirati i jednakost između relacija i funkcija za relacijske varijable P i Q, odnosno funkcijske varijable f i g na svakoj n-torki terama prvog reda: (*pricip ekstenzionalnosti*)

$$P = Q \ := \ \forall \overrightarrow{x} \, (P \overrightarrow{x} \leftrightarrow Q \overrightarrow{x})$$

$$f = g \ := \ \forall \overrightarrow{x} \, (f \overrightarrow{x} = g \overrightarrow{x})$$

Upotreba istog simbola = može se dozvoliti jer će iz konteksta biti jasno o kojoj se jednakosti radi.

Definicija 11. *Formula F logike drugog reda je* ispunjiva *ako postoji interpretacija I u kojoj je formula F istinita. Tada za interpretaciju I kažemo da zadovoljava formulu F ili da je* model *od F.*
Skup formula Γ je ispunjiv ako je svaka formula iz skupa Γ ispunjiva.
Interpretacija I je model skupa formula Γ ako je model svake formule iz skupa Γ.

Definicija 12. *Formula F logike drugog reda je* valjana *ako je istinita u svakoj interpretaciji. U oznaci:* $\models F$.

Definicija 13. *Formula logike drugog reda* F_1 implicira *formulu logike drugog reda* F_2 *ako je za svaku interpretaciju* I *u kojoj je formula* F_1 *istinita i formula* F_2 *istinita. Kaže se da je formula* F_2 *logička posljedica formule* F_1.
U oznaci: $F_1 \Rightarrow F_2$ *ili* $F_1 \models F_2$.
Skup formula logike drugog reda Γ *implicira formulu logike drugog reda* F *ako je svaki model od* Γ *model formule* F.
Kažemo još da je formula F *logička je posljedica od* Γ.
U oznaci: $\Gamma \models F$.

Vrijedi: $F_1 \Rightarrow F_2$ ako i samo ako $\models F_1 \rightarrow F_2$.

Definicija 14. *Formula logike drugog reda* F_1 logički *je* ekvivalentna *formuli logike drugog reda* F_2 *ako i samo ako je za svaku interpretaciju* I *u kojoj je formula* F_1 *istinita i formula* F_2 *istinita. U oznaci:* $F_1 \Leftrightarrow F_2$.

Vrijedi: $F_1 \Leftrightarrow F_2$ ako i samo ako $\models F_1 \leftrightarrow F_2$.

Definicija 15. *S-struktura* $\mathcal{N} = (N, j)$ *je* podstruktura *S-strukture* $\mathcal{M} = (M, i)$ *ako vrijedi:*

- $N \subseteq M$;
- $j(R^n) = i(R^n) \mid_{N^n}$ *za sve relacijske simbole* R^n *iz* S ;
- $j(f^n) = i(f^n) \mid_{N^n}$ *za sve funkcijske simbole* f^n *iz* S ;
- $j(c_k) = i(c_k)$ *za sve konstantske simbole* c_k *iz* S.

Definicija 16. *S-strukture* $\mathcal{M} = (M, i)$ *i* $\mathcal{N} = (N, j)$ *su* homomorfne *ako postoji funkcija* $F : M \rightarrow N$ (homomorfizam struktura) *takva da vrijedi:*

- $(a_1, a_2, ...a_n) \in i(R^n)$ *ako i samo ako* $(F(a_1), F(a_2), ...F(a_n)) \in j(R^n)$ *za sve relacijske simbole* R^n *iz* S *i sve* $a_1, a_2, ...a_n$ *iz* M ;
- $F(i(f^n(a_1, a_2, ...a_n))) = j(f^n(F(a_1), F(a_2), ...F(a_n)))$ *za sve funkcijske simbole* f^n *iz* S *i sve* $a_1, a_2, ...a_n$ *iz* M ;
- $F(i(c_k)) = j(c_k)$ *za sve konstantske simbole* c_k *iz* S.

Ove uvjete možemo kraće zapisati:

- $\overrightarrow{a} \,\epsilon\, \boldsymbol{R}^{\mathcal{M}}$ ako i samo ako $F(\overrightarrow{a}) \,\epsilon\, \boldsymbol{R}^{\mathcal{N}}$;
- $F(\boldsymbol{f}^{\mathcal{M}}(\overrightarrow{a})) = \boldsymbol{f}^{\mathcal{N}}(F(\overrightarrow{a}))$;
- $F(\boldsymbol{c}^{\mathcal{M}}) = \boldsymbol{c}^{\mathcal{N}}$

ili :

- $\langle a \rangle_n \,\epsilon\, \boldsymbol{R}^{\mathcal{M}}$ ako i samo ako $F(\langle a \rangle_n) \,\epsilon\, \boldsymbol{R}^{\mathcal{N}}$;
- $F(\boldsymbol{f}^{\mathcal{M}}(\langle a \rangle_n)) = \boldsymbol{f}^{\mathcal{N}}(F(\langle a \rangle_n))$;
- $F(\boldsymbol{c}^{\mathcal{M}}) = \boldsymbol{c}^{\mathcal{N}}$.

Definicija 17. *Ako je homomorfizam ujedno i bijekcija, tada se on naziva* izomorfizmom*, a strukture* izomorfnim stukturama*.*

3 Neki rezultati za logiku drugog reda

Najvažniji rezultati za logiku prvog reda uz standardnu semantiku formulirani su sljedećim teoremima.

Teorem kompaktnosti: Ako svaki konačan podskup skupa formula ima model, onda cijeli skup ima model.

Löwenheim-Skolem teorem na dolje: Ako skup formula ima model, onda taj skup formula ima i prebrojiv model.

Löwenheim-Skolem teorem na gore: Ako skup formula ima beskonačan model, onda taj skup formula ima i model proizvoljno velike kardinalnosti .

Gödelov teorem potpunosti: Skup valjanih rečenica je rekurzivno prebrojiv.

Promotrimo što se s tim rezultatima događa prijeđemo li na logiku drugog reda.
Prema Löwenheim-Skolem teoremima skup formula koji ima beskonačni model ima i beskonačne modele proizvoljne kardinalnosti. Iz toga slijedi da se jezikom logike prvog reda ne mogu kategorički karakterizirati beskonačne strukture.
Logika drugog reda sa stadardnom semantikom ne dijeli to svojstvo. Mnoge se strukture mogu kategorički karakterizirati u logici drugog reda, npr. skup prirodnih brojeva.
Varijante spomenutih teorema, međutim, vrijede za jezike drugog reda uz Henkinovu semantiku. U tom je smislu ta logika poput logike prvog reda.

Napomena: Teoremi i primjeri koji slijede odnose se na logiku drugog reda uz standardnu semantiku. Smatramo da se nadalje podrazumijeva standardna semantika pa to nećemo navoditi u formulacijama tvrdnji.

3.1 Aksiom prebrojivosti i aksiom beskonačnosti

Označimo sljedeću rečenicu s *Enum*:

$$\exists z \exists u \forall X((Xz \wedge \forall x(Xx \rightarrow Xu(x))) \rightarrow \forall x Xx)$$

Propozicija 1. *Enum je istinita u nekoj interpretaciji ako i samo ako je domena prebrojiva.*

Dokaz. Pretpostavimo da je *Enum* istinita u interpretaciji $\mathcal{M}$. To znači da postoji element a domene $|\mathcal{M}| = M$ i jednomjesna funkcija f na M koji zadovoljavaju formulu

$$\forall X((Xa \wedge \forall x(Xx \to Xf(x))) \to \forall x Xx)$$

Označimo sa 0 konstantu čija je denotacija a, i sa $'$ jednomjesni funkcijski simbol čija je denotacija funkcija f (koristimo notaciju $'(x) = x'$). Formula

$$\forall X((X0 \wedge \forall x(Xx \to Xx')) \to \forall x Xx)$$

je istinita, što znači da svaki podskup A domene M zadovoljava formulu

$$(X0 \wedge \forall x(Xx \to Xx')) \to \forall x Xx$$

kao denotacija od X. Posebno to vrijedi za prebrojiv podskup A domene M čiji su elementi a, $f(a)$, $f(f(a))$, $f(f(f(a)))$ itd. Označimo s N jednomjesni predikat čija je denotacija skup A. Tada je formula

$$(\mathsf{N}0 \wedge \forall x(\mathsf{N}x \to \mathsf{N}x')) \to \forall x \mathsf{N}x$$

istinita. $\mathsf{N}0$ je istinito, jer je a denotacija od 0, A denotacija od N pa je a element skupa A. Zatim je i $\forall x(\mathsf{N}x \to \mathsf{N}x'))$ istinito, jer je za svaki element od A, onaj element koji se dobije aplikacijom funkcije $'$ (čija je denotacija f) na taj element, opet u skupu A. Stoga $\forall x \mathsf{N}x$ mora biti istinito, tj. svaki element domene mora biti u A. Kako je A prebrojiv, i domena mora biti prebrojiva.

Obrnuto, pretpostavimo da je domena interpretacije $\mathcal{M}$ prebrojiva, $|\mathcal{M}| = M = \{m_0, m_1, m_2, ...\}$. Neka je $a = m_0$ i f funkcija koja argumentu m_i pridružuje m_{i+1}, te neka je 0 konstanta i $'$ jednomjesni funkcijski simbol čije su denotacije a i f. Neka je A proizvoljni podskup domene M. Označimo s N jednomjesni predikat čija je denotacija skup A. Tada, ako je $\mathsf{N}0$ istinito, $m_0 = a$ je element od A, i ako je $\forall x(\mathsf{N}x \to \mathsf{N}x')$ istinito, tada za svaki m_i element iz A je i $f(m_i) = m_{i+1}$ element iz A. Dakle, ako je

$$\mathsf{N}0 \wedge \forall x(\mathsf{N}x \to \mathsf{N}x')$$

istinito, svaki element $m_0, m_1, m_2, ...$ domene je iz A, pa je i $\forall x \mathsf{N}x$ istinito. Stoga je

$$(\mathsf{N}0 \wedge \forall x(\mathsf{N}x \to \mathsf{N}x')) \to \forall x \mathsf{N}x$$

istinito, gdje je N jednomjesni predikat čija je denotacija A, odnosno A zadovoljava formulu

$$(X0 \wedge \forall x(Xx \to Xx')) \to \forall x Xx$$

Kako je to istinito za proizvoljni A podskup domene,

$$\forall X((X0 \wedge \forall x(Xx \to Xx')) \to \forall x Xx)$$

je istinito, pa je formula *Enum*

$$\exists z \exists u \forall X((Xz \wedge \forall x(Xx \to Xu(x))) \to \forall x Xx)$$

istinita u $\mathcal{M}$. □

Označimo sljedeću rečenicu s Inf:

$$\exists z \exists u(\forall x(z \neq u(x)) \wedge \forall x \forall y(u(x) = u(y) \to x = y))$$

Propozicija 2. *Formula Inf istinita u nekoj interpretaciji ako i samo ako je domena beskonačna.*

Dokaz. Formulom Inf izažava se egzistencija funkcije u na domeni koja je injekcija, a nije surjekcija. Takva funkcija u nužno zahtjeva beskonačnu domenu. □

3.2 Aritmetika drugog reda

Neka je P^{II} konjunkcija aksioma aritmetike

1. $\forall x \forall y\,(x' = y' \to x = y)$
2. $\forall x\,(\mathbf{0} \neq x')$
3. $\forall x\,(x \neq \mathbf{0} \to \exists y\,(x = y'))$
4. $\forall x\,(x + \mathbf{0} = x)$
5. $\forall x \forall y\,(x + y' = (x + y)')$
6. $\forall x\,(x \cdot \mathbf{0} = \mathbf{0})$
7. $\forall x \forall y\,(x \cdot y' = (x \cdot y) + x)$

i aksioma indukcije Ind:

$$\forall X((X\mathbf{0} \wedge \forall x(Xx \to Xx')) \to \forall x Xx)$$

Propozicija 3. *Interpretacija jezika aritmetike je model od P^{II} ako i samo ako je izomorfna sa standardnom interpretacijom aritmetike.*

Dokaz. U dokazu za aksiom prebrojivosti pokazali smo da se svaki model od Ind sastoji od denotacija terama 0, $0'$, $0''$,... odnosno numerala $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$,... kako ih obično označavamo. U aritmetici prvog reda Q pokazuje se da za prirodne brojeve m, n i p vrijedi:

$$\begin{aligned} m \neq n &\Rightarrow \mathbf{m} \neq \mathbf{n} \\ m < n &\Rightarrow \mathbf{m} < \mathbf{n} \\ m \geq n &\Rightarrow \neg(\mathbf{m} < \mathbf{n}) \\ m + n = p &\Rightarrow \mathbf{m} + \mathbf{n} = \mathbf{p} \\ m + n \neq p &\Rightarrow \mathbf{m} + \mathbf{n} \neq \mathbf{p} \\ m \cdot n = p &\Rightarrow \mathbf{m} \cdot \mathbf{n} = \mathbf{p} \\ m \cdot n \neq= p &\Rightarrow \mathbf{m} \cdot \mathbf{n} \neq \mathbf{p} \end{aligned}$$

gdje je $\mathbf{x} < \mathbf{y}$ formula $\exists \mathbf{z}\,(\mathbf{x} + \mathbf{z} = \mathbf{y}) \wedge \mathbf{x} \neq \mathbf{y}$.

Neka je $\mathcal{M}$ model od P^{II}. Kako je $\mathcal{M}$ model od Ind, svaki element domene $|\mathcal{M}| = M$ je denotacija barem jednog numerala $\mathbf{m}$, štoviše točno jednog numerala jer je $\mathcal{M}$ model aritmetike prvog reda Q pa vrijedi $m \neq n \Rightarrow \mathbf{m} \neq \mathbf{n}$. Definirajmo funkciju j sa skupa M u skup prirodnih brojeva tako da funkcija j elementu domene ($\mathbf{m}$) pridružuje broj čija je on denotacija (m). Iz navedenih svojstava slijedi da je j izomorfizam $\mathcal{M}$ i standardne interpretacije aritmetike Q.
Obratno, lako se pokazuje da je P^{II} istinito u standardnoj interpretaciji; skup prirodnih brojeva $\mathbb{N}$ model je aritmetike prvog reda Q. Preostaje ispitati istinitost aksioma Ind koji za prirodne brojeve predstavlja princip matematičke indukcije: ako proizvoljan podskup skupa prirodnih brojeva sadrži 0 i ako vrijedi da je za svaki njegov element i sljedbenik tog elementa u skupu, tada on sadrži brojeve 0, 1, 2,... pa je svaki prirodan broj u tom podskupu, odnosno $\mathbb{N}$ je model od Ind.
Pokažimo sada kategoričnost formalizacije aritmetike, odnosno da je $\mathbb{N}$ izomorfan sa svakim modelom $\mathcal{M}$ od P^{II}. Neka je $|\mathcal{M}| = M$ domena, a e, s, p i t redom denotacije od 0, $'$, $+$ i $\cdot$. Kako su aksiomi aritmetike i aksiom indukcije istiniti u $\mathcal{M}$, za svaki a i b iz M i svaki podskup A od M vrijedi:

1. $s(a) = s(b) \;\Rightarrow\; a = b$
2. $e \neq s(a)$
3. $p(a, e) = a$
4. $p(a, s(b)) = s(p(a, b))$
5. $t(a, e) = e$
6. $t(a, s(b)) = p(t(a, b), a)$
7. $(\; e \epsilon A \;\wedge\; \forall c \epsilon M(c \epsilon A \rightarrow s(c) \epsilon A)) \;\Rightarrow\; A = M$

Neka je h funkcija definirana s: $\quad h(0) = e \qquad h(n') = s(h(n))$
Tada je h izomorfizam struktura N i $\mathcal{M}$, odnosno h je bijekcija, i vrijede svojstva $h(m + n) = p(h(m) + h(n))$ i $h(m \cdot n) = t(h(m), h(n))$.

Dokaz injektivnosti: pretpostavimo da h nije injekcija, neka je tada m najmanji prirodni broj takav da postoji $n > m$, $h(m) = h(k)$.
Kako je $n > m$, $n = j'$ za neki j, pa je $h(n) = h(j') = s(h(j))$.
Ako je $m = 0$ tada je $h(m) = h(0) = e$, no prema (2) je $e \neq s(h(j))$.
Dakle $m \neq 0$, tj. $m = i'$ za neki i.
Iz $m < n$, odnosno $i' < j'$ slijedi $i < j$, a kako je m najmanji takav element vrijedi $h(i) \neq h(j)$, te zatim $s(h(i)) \neq s(h(j))$.
Stoga je $h(m) = h(i') = s(h(i)) \neq s(h(j)) = h(j') = h(n)$. Kontradikcija.

Dokaz surjektivnosti: Element e je u rangu $Image(h)$, a ako je $c \,\epsilon\, Image(h)$, tj. $c = h(n)$ za neki n, onda je $h(n') = s(h(n)) = s(c)$, tj. i $s(c) \epsilon Image(h)$.
Iz (7) slijedi $Image(h) = M$.

Svojstva homomorfizma dokazat ćemo indukcijom po n.
Dokaz jednakosti $h(m + n) = p(h(m) + h(n))$:
za $h(m + 0) = h(m)$ prema (3) i (1) vrijedi
$h(m) = p(h(m), e) = p(h(m), h(0))$.
Dalje je $h(m + n') = h((m + n)') = s(h(m + n))$
pretpostavkom indukcije jednako $s(p(h(m) + h(n)')$.
Prema (4) je $p(h(m), s(h(n))) = p(h(m), h(n'))$.

Dokaz jednakosti $h(m \cdot n) = t(h(m), h(n))$:
Kako je $h(m \cdot 0) = h(0) = e$ iz (5) dobijemo $e = t(h(m), e) = t(h(m), h(0))$.
Prema upravo dokazanoj jednakosti je:
$h(m \cdot n') = h(m \cdot n + n) = p(h(m \cdot n), h(m))$
što je prema pretpostavci indukcije jednako $p(t(h(m), h(n)), h(m))$
a prema (6) $t(h(m), s(h(n))) = t(h(m), h(n'))$. $\square$

3.3 Metateoremi

Teorem 1. *Löwenheim-Skolem teoremi (na dolje i na gore) ne vrijede za logiku drugog reda.*

Dokaz. $Inf \wedge \neg Enum$ i $Inf \wedge Enum$ su rečenice logike drugog reda koje imaju beskonačne modele, a nemaju konačnih modela.
Formula $Inf \wedge \neg Enum$ ima samo neprebrojive modele pa predstavlja kontraprimjer za Löwenheim-Skolem teorem na dolje.
Formula $Inf \wedge Enum$ ima samo prebrojive modele pa stoga ne vrijedi Löwenheim-Skolem teorem na gore. □

U logici prvog reda, kao neposredna posljedica Löwenheim-Skolem teorema na dolje i gore, vrijedi i tvrdnja da, ako skup rečenica logike prvog reda ima beskonačan model, onda on ima neizomorfne beskonačne modele.
Ni ovaj korolar ne vrijedi u logici drugog reda što pokazuje primjer aritmetike koja je kategorički karakterizirana formulom P^{II}.

Teorem 2. *Teorem kompaktnosti ne vrijedi za logiku drugog reda.*

Dokaz. Jeziku aritmetike drugog reda dodajmo konstantu c, te promotrimo skup

$$\Gamma = \{P^{II}, c \neq \mathbf{0}, c \neq \mathbf{1}, c \neq \mathbf{2}, ...\}$$

Svaki njegov konačan podskup Γ_0 ima model koji se dobije proširenjem standardne interpretacije tako da konstanti c pridružimo broj veći od svih onih čiji numerali dolaze u Γ_0. Međutim, kako je u svakom modelu od P^{II} svaki element domene denotacija nekog numerala, Γ nema model. □

Teorem 3. *Gödelov teorem potpunosti ne vrijedi za logiku drugog reda: skup valjanih formula logike drugog reda nije rekurzivano prebrojiv (niti aritmetički).*

Ova se tvrdnja često iskazuje ovako: *logika drugog reda nije potpuna, preciznije niti jedna korektna formalizacija logike drugog reda nije potpuna.*

Dokaz. Formula A, logike prvog reda u jeziku aritmetike, istinita je ako i samo ako je istinita u svim interpretacijama koje su izomorfne standardnoj interpretaciji. Prema prethodnom primjeru ona je istinita ako i samo ako je istinita u svim modelima P^{II}, ili ekvivalentno ako i samo ako je $P^{II} \rightarrow A$ valjano. Funkcija koja formuli prvog reda A pridružuje formulu drugog reda

$P^{II} \to A$ očito je rekurzivna. Stoga, kad bi skup valjanih formula drugog reda bio rekurzivano prebrojiv, tada bi skup istinitih formula jezika aritmetike također bio rekurzivno prebrojiv. Međutim, prema Gödelovom teoremu o nepotpunosti on nije aritmetički pa tim više niti rekurzivano prebrojiv. □

4 Dedukcije

4.1 Sustav dedukcije za logiku prvog reda

Sustav dedukcije za logiku prvog reda (bez jednakosti) zadan je shemama aksioma i pravilima izvođenja. Aksiom je svaka formula dobivena supstitucijom formula za simbole označene grčkim slovima u shemama aksioma.

Sheme aksioma:

$\Phi \to (\Psi \to \Phi)$
$(\Phi \to (\Psi \to \lambda)) \to ((\Phi \to \Psi) \to (\Phi \to \lambda))$
$(\neg\Phi \to \neg\Psi) \to (\Psi \to \Phi)$
$\forall x\, \Phi(x) \to \Phi(t)$

Neka je Γ skup formula i Φ formula.
Dedukcija od Φ *iz* Γ je konačan niz $\Phi_1 ... \Phi_n$ takav da je Φ_n formula Φ, a za svaki $i \leq n$, Φ_i je aksiom ili formula iz skupa Γ, ili pak Φ_i slijedi iz prethodnih formula u nizu jednim od sljedećih pravila izvođenja:

modus ponens : iz Φ i $\Phi \to \Psi$ zaključi Ψ
generalizacija : iz $\Phi \to \Psi(x)$ zaključi $\Phi \to \forall x \Psi(x)$

uz uvjet da x nije slobodan u Φ ili nekoj formuli iz Γ.

Nazovimo ovaj sustav D1.
Ako postoji dedukcija od Φ iz Γ u sustavu D1 pišemo $\Gamma \vdash_{D1} \Phi$.

Pravila i aksiomi koji se odnose na ostale logičke veznike izvedivi su u D1. Možemo ih stoga smatrati pokratama za pripadne formulacije u sustavu D1.

Ograničenje koje dolazi uz generalizaciju uvijek se poštuje. To osigurava konvenzija o varijablama.

Za sustav D1 vrijedi teorem dedukcije:

Ako $\Gamma \cup \Phi \vdash_{D1} \Psi$ onda $\Gamma \vdash_{D1} \Phi \to \Psi$.

Nadalje, sustav D1 korektan je i potpun.

Potpunost, međutim, ne vrijedi za deduktivni sustav logike drugog reda uz standardnu semantiku.

4.2 Sustav dedukcije za logiku drugog reda

Uvodimo jedno od mogućih proširenja sustava D1 na formule logike drugog reda. Taj ćemo sustav nazvati D2.
Sustav D1 prirodno proširujemo aksiomima i pravilima vezanim uz relacijske i funkcijske varijable kako bi mogli graditi dedukcije za formule drugog reda.

Konvencija o varijablama osigurava da su sve slobodne varijable različite od svih vezanih varijabli, pa uz nove sheme i aksiome nećemo navoditi uobičajena ograničenja na varijable.

Shemama aksioma sustava D1 dodajemo sljedeće sheme:

$\forall X^n\, \Phi(X^n) \to \Phi(T)$ gdje je T n-mjesna relacijska varijabla ili n-mjesni relacijski simbol.

$\forall f^n\, \Phi(f^n) \to \Phi(p)$ gdje je p n-mjesna funkcijska varijabla ili n-mjesni funkcijski simbol.

Pravilima izvođenja sustava D1 dodajemo sljedeća pravila:

(generalizacija za relacije)

Iz $\Phi \to \Psi(X)$ zaključi $\Phi \to \forall X \Psi(X)$

(generalizacija za funkcije)

Iz $\Phi \to \Psi(f)$ zaključi $\Phi \to \forall f \Psi(f)$

Nadalje, dodajemo:

(shema aksioma komprehenzije)

$\exists X^n\, \forall \langle x \rangle_n (X^n \langle x \rangle_n \leftrightarrow \Phi \langle x \rangle_n)$

(aksiom izbora)

$\forall X^{n+1}\, (\forall \langle x \rangle_n\, \exists y\, X^{n+1} \langle x \rangle_n y \to \exists f^n\, \forall \langle x \rangle_n\, X^{n+1} \langle x \rangle_n f \langle x \rangle_n)$

Shema aksioma komprehenzije kaže da svaka formula logike višeg reda određuje relaciju. Točnije, za svaku formulu postoji relacija s istom ekstenzijom.
Sa $\langle x \rangle_n$ označen je niz varijabli $x_1, ..., x_n$.
Antecedenta unutar aksioma izbora izražava da za svaki niz varijabli $\langle x \rangle_n$ postoji barem jedna varijabla y takva da niz varijabli $\langle x \rangle_n y$ zadovoljava X^{n+1}. Pripadna konzekventa izražava egzistenciju funkcije koja izabire jedan takav y za svaki niz $\langle x \rangle_n$. Dakle, za svaku relaciju postoji adekvatna funkcija izbora.

Ukoliko se aksiom izbora želi izbaciti iz deduktivnog sustava, zamjenjuje se slabijim principom:

(princip komprehenzije za funkcije)

$\forall X^{n+1}\,(\forall\langle x\rangle_n\,\exists y!\,X^{n+1}\langle x\rangle_n y \to \exists f^n\,\forall\langle x\rangle_n\,X^{n+1}\langle x\rangle_n f\langle x\rangle_n)$

Slično shemi aksioma komprehenzije, princip komprehenzije za funkcije naglašava mogućnost da se funkcijske varijable eliminiraju zamjenom s relacijskim varijablama. Preciznije, izražava tvrdnju da je svaka $(n+1)$-mjesna funkcijska relacija graf n-mjesne funkcije.

Teorem 4. *Neka je* Γ *skup formula i* Φ *formula logike drugog reda. Ako je formula* Φ *izvodljiva u sustavu D2, tada je formula* Φ *logička posljedica od* Γ*, odnosno vrijedi: ako* $\Gamma \vdash_{D2} \Phi$ *onda* $\Gamma \models \Phi$*.*

Dokaz. Potrebno je pokazati da su aksiomi sustava D2 valjane formule, te provjeriti svako pravilo izvođenja. Zbog korektnosti sustava D1, dokaz svodimo samo na aksiome i pravila kojima smo proširili sustav.

Dokaz valjanosti aksioma $\forall X^n\,\Phi(X^n) \to \Phi(T)$:

Aksiom ima formu kondicionala pa pretpostavimo da je formula $\forall X^n\,\Phi(X^n)$ istinita. Tada je ona istinita za svaku valuaciju od X pa je i formula $\Phi(T)$ istinita.

Analogno dokazujemo valjanost aksioma $\forall f^n\,\Phi(f^n) \to \Phi(p)$.

Dokaz preostalih dvaju aksioma formalne logike koristi iste te principe na meta-nivou. Kod sheme aksioma komprehenzije to je meta-princip da svaka formula određuje relaciju s istom ekstenzijom, a kod aksioma izbora princip izbora u meta-teoriji.

Dokaz korektnosti pravila izvođenja provodimo indukcijom po duljini dokaza. Baza indukcije je dokaz duljine 1, dakle sama formula Φ. Prema definiciji dedukcije ona je aksiom ili formula iz skupa Γ. Upravo smo pokazali da su aksiomi valjane formule, a trivijalno vrijedi da je formula logička posljedica skupa formula kojeg je i sama element.

Promatramo sada zadnje pravilo primjenjeno u dedukciji. Ako je to pravilo "Iz $\Theta \to \Psi(f)$ zaključi $\Theta \to \forall f\Psi(f)$" tada je Φ formula $\Theta \to \forall f\Psi(f)$, te prethodno imamo dedukciju $\Gamma \vdash_{D2} \Theta \to \Psi(f)$. Kako je taj dokaz duljine manje za 1, prema pretpostavci indukcije vrijedi $\Gamma \models \Theta \to \Psi(f)$. Za svaku interpretaciju u kojoj je skup formula Γ istinit i formula Θ istinita vrijedi da je i formula $\Psi(X)$ istinita. Budući da to ne ovisi o valuaciji, tada je i formula $\forall X\,\Psi(X)$ istinita, odnosno $\Gamma \models \Theta \to \forall X\,\Psi(f)$.

Analogno zaključujemo za drugo pravilo izvoda jer iz istinitosti od $\Psi(f)$ slijedi istinitost formule $\forall f\,\Psi(f)$. □

Definicija 18. *Za deduktivni sustav kažemo da je* efektivan *ako su skup dobro formiranih formula i skup dedukcija rekurzivni.*

Ako je sustav efektivan, tada je skup formula izvodljivih iz konačno mnogo pretpostavki rekurzivano prebrojiv.

Propozicija 4. *Neka je* D *proizvoljan efektivan deduktivni sustav korektan za aritmetiku drugog reda. Tada* D *nije slabo potpun: postoji valjana formula jezika aritmetike drugog reda koja nije dokaziva u sustavu* D*.*

Dokaz. Neka je $T = \{\Phi \mid \Phi$ je formula bez relacijskih i funkcijskih varijabli takva da vrijedi $\vdash_D P^{II} \to \Phi\}$. Formule skupa T su prvog reda.
Kako je sustav D efektivan skup T je rekurzivno prebrojiv.
Zbog korektnosti sustava D svaka formula skupa T je istinita za prirodne brojeve. Prema Gödelovom teoremu nepotpunosti skup valjanih formula prvog reda jezika aritmetike nije rekurzivno prebrojiv. Stoga postoji valjana formula prvog reda jezika aritmetike Φ koja nije element skupa T. To znači da formula $P^{II} \to \Phi$ nije dokaziva u sustavu D.
S druge strane $P^{II} \to \Phi$ je valjana formula, pa sustav D nije potpun. □

Korolar 1. *Sustav* D2 *nije potpun.*

5 Henkinova semantika logike drugog reda

Osnovna razlika između standardne i Henkinove sematike logike drugog reda je u tome što u danom modelu relacijske i funkcijske varijable poprimaju vrijednosti iz unaprijed zadanog skupa relacija, odnosno funkcija na domeni. To nisu nužno skup svih relacija niti skup svih funkcija.

Neka je S neprazan skup nelogičkih simbola jezika logike drugog reda.

Definicija 19. Henkinova S-struktura *je uređena četvorka* $\mathcal{M}^H = (M, D, F, i)$ *nepraznog skupa* M *kojeg nazivamo domena, nepraznog skupa* D *relacija na* M*, nepraznog skupa funkcija* F *na* M *i preslikavanja* i *definiranog na skupu nelogičkih simbola koje ima ista svojstva kao i kod standardnog modela:*

- *svakom konstantskom simbolu* c_k *iz* S *pridružuje se neki element* $i(c_k)$ *iz* M *(također u oznaci* $\boldsymbol{c}_k^{\mathcal{M}^H}$*) ;*
- *svakom funkcijskom simbolu* $\mathsf{f}_k^{n_k}$ *iz* S *pridružuje se* m_k*-mjesna funkcija* $i(\mathsf{f}_k^{n_k}) : M^{m_k} \to M$ *(također u oznaci* $\boldsymbol{f}_k^{\mathcal{M}^H}$*) ;*
- *svakom relacijskom simbolu* $\mathsf{R}_k^{n_k}$ *iz* S *pridružuje se* n_k*-mjesna relacija* $i(\mathsf{R}_k^{n_k})$ *na* M *(također u oznaci* $\boldsymbol{R}_k^{\mathcal{M}^H}$*) ;*
- *logičkoj konstnti* $\top$ *pridružuje se* 1 *(istina), a* $\bot$ 0 *(laž).*

Označimo sa $D(n)$ *podskup skupa* D *koji sadrži sve* n*-arne relacije , a sa* $F(n)$ *podskup skupa* F *koji sadrži sve funkcije sa skupa* M^n *u skup* M*. Za svaki* n *su skupovi* $D(n)$ *i* $F(n)$ *neprazni.*

Definicija 20. $\mathcal{M}^H = (M, D, F, i)$ *je* Henkinova struktura za formulu A *ako je funkcija* i *definirana za svaki nelogički simbol koji nastupa u formulu* A*.* $\mathcal{M}^H$ *je* Henkinova stuktura za skup formula Γ *ako je* $\mathcal{M}^H$ *Henkinova struktura za svaku formulu iz* Γ*.*

Definicija 21. *Za danu Henkinovu* S*-strukturu* $\mathcal{M}^H = (M, D, F, i)$ valuacija v *je funkcija koja:*

- *svakoj individualnoj varijabli* x *pridružuje element domene* $v(x)$ *;*
- *svakoj funkcijskoj varijabli* f^m *pridružuje funkciju* $v(f) : M^m \to M$ *iz skupa* $F(m)$ *;*

- *svakoj relacijskoj varijabli R^n pridružuje n-mjesnu relaciju na M $v(R^n)$ iz skupa $D(n)$.*

Ostale definicije (denotacija, interpretacija, ispunjivost, valjanost itd.) u osnovi su jednake standardnim definicijama; razlikuju se samo na relacijskim i funkcijskim varijablama. Kod standardne valuacije relacijske i funkcijske varijable prolaze kroz *sve* relacije i funkcije na domeni, a kod Henkinove interpretacije valuacije relacijskih varijabli poprimaju *samo* vijednosti iz skupa D, a valuacije funkcijskih varijabli poprimaju *samo* vijednosti iz skupa F.

Definicija 22. Henkinova S-interpretacija I *je uređeni par Henkinove S-strukture $\mathcal{M}^H = (M, D, F, i)$ i valuacije v na $\mathcal{M}^H$.*

Definicija 23. *U Henkinovoj interpretaciji $I = (\mathcal{M}^H, v)$* denotacija *je proširenje valuacije v sa skupa varijabli na skup svih terama:*

$$d(x) = v(x) \quad d(f) = v(f) \quad d(R) = v(R)$$

$$d(c) = i(c) = \boldsymbol{c}^{\mathcal{M}^{\mathcal{H}}}$$

$$d(\mathsf{f}(\overrightarrow{t})) = i(\mathsf{f})(d(\overrightarrow{t})) = \boldsymbol{f}^{\mathcal{M}^{\mathcal{H}}}(d(\overrightarrow{t}))$$

$$d(f(\overrightarrow{t})) = d(f)(d(\overrightarrow{t}))$$

Definicija 24. *Neka je $I = (\mathcal{M}^H, v)$ Henkinova S-interpretacija gdje je $\mathcal{M}^H = (M, D, F, i)$ i v valuacija na $\mathcal{M}^H$ te neka je F formula izgrađena od simbola iz S.* Istinitost formule F u interpretaciji I (*u oznaci: $I(F) = 1$, $\mathcal{M}^H \models_v F$ ili $\mathcal{M}^H, v \models F$) definiramo induktivno po složenosti formule F:*

- *ako je F atomarna formula oblika $\mathsf{R}(t_1, ..., t_n)$ gdje je R relacijski simbol, tada $\mathcal{M}^H, v \models F$ ako i samo ako $(v(t_1), ..., v(t_n)) \in i(R) = \boldsymbol{R}^{\mathcal{M}^H}$;*
- *ako je F atomarna formula oblika $R(t_1, ..., t_n)$ gdje je R relacijska varijabla, tada $\mathcal{M}^H, v \models F$ ako i samo ako $(v(t_1), ..., v(t_n)) \in v(R)$;*
- *ako je F logička konstanta, tada $\mathcal{M}^H, v \models \top$, a nije $\mathcal{M}^H, v \models \bot$;*
- *ako je F formula oblika $\neg G$, tada $\mathcal{M}^H, v \models F$ ako i samo ako nije $\mathcal{M}^H, v \models G$;*

- *ako je F formula oblika $A \wedge B$, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako* $\mathcal{M}^H, v \models A$ *i* $\mathcal{M}^H, v \models B$ *;*

- *ako je F formula oblika $A \vee B$, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako* $\mathcal{M}^H, v \models A$ *ili* $\mathcal{M}^H, v \models B$ *;*

- *ako je F formula oblika $A \rightarrow B$, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako nije* $\mathcal{M}^H, v \models A$ *ili je* $\mathcal{M}^H, v \models B$ *;*

- *ako je F formula oblika $A \leftrightarrow B$, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako je* $\mathcal{M}^H, v \models A$ *onda i samo onda kad* $\mathcal{M}^H, v \models B$ *;*

- *ako je F formula oblika $\forall w\, G$, gdje je w individualna varijabla x, funkcijska varijabla f, odnosno relacijska varijabla R, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako* $\mathcal{M}^H, v_w \models G$ *za svaku valuaciju v_w koja se podudara s valuacijom v na svim varijablama osim možda na varijabli w ;*

- *ako je F formula oblika $\exists w\, G$ gdje je w individualna varijabla x, funkcijska varijabla f, odnosno relacijska varijabla R, tada* $\mathcal{M}^H, v \models F$ *ako i samo ako* $\mathcal{M}^H, v_w \models G$ *za neku valuaciju v_w koja se podudara s valuacijom v na svim varijablama osim možda na varijabli w.*

Definicija 25. *Formula F logike drugog reda je* Henkin-ispunjiva *ako postoji Henkinova interpretacija I u kojoj je formula F istinita. Tada za interpretaciju I kažemo da je* Henkinov model *od F.*
Skup formula Γ je Henkin-ispunjiv ako je svaka formula iz skupa Γ Henkin-ispunjiva. Henkinova interpretacija I je Henkinov model skupa formula Γ ako je Henkinov model svake formule iz skupa Γ.

Definicija 26. *Formula F logike drugog reda F je* Henkin-valjana *ako je istinita u svakoj Henkinovoj interpretaciji.*

Definicija 27. *Formula logike drugog reda F_1* Henkin-implicira *formulu logike drugog reda F_2 ako je za svaku Henkinovu interpretaciju I u kojoj je formula F_1 istinita i formula F_2 istinita.*
Skup formula logike drugog reda Γ Henkin-implicira formulu logike drugog reda F ako je svaki Henkinov model od Γ ujedno i Henkinov model formule F.

Jasno je da je standardna semantika ekvivalentna Henkinovoj semantici u kojoj su skupovi D i F takvi da je za svaki n skup $D(n) = P(M^n)$ skup svih n-arnih relacija na domeni M, a $F(n) = (M^n \to M)$ skup svih funkcija sa skupa M^n u skup M.
Takvi Henkinovi modeli nazivaju se *potpuni modeli.*
Spomenuta ekvivalencija semantika formulirana je sljedećim teoremom.

Teorem 5. *Neka je $\mathcal{M}$ standardni model, a $\mathcal{M}_P^H$ odgovarajući potpun Henkinov model. Tada za svaku valuaciju v i svaku formulu F vrijedi:*

$$\mathcal{M}, v \models F \quad \textit{ako i samo ako} \quad \mathcal{M}_P^H, v \models F.$$

Korolar 2. *Ako je formula F Henkin-valjana, tada je F valjana u standardnoj semantici.*
Ako je formula F Henkin-logička posljedica skupa formula Γ, tada je F logička posljedica skupa formula Γ.
Ako je formula F ispunjiva u standardnoj semantici, tada je F Henkin-ispunjiva.

Obrat ne vrijedi. Za logiku drugog reda uz Henkinov semantiku vrijedi teorem potpunosti. Iz potpunosti se pokazuje da vrijedi i teorem kompaktnosti, kao i Skolem-Löwenheim teoremi.

5.1 Metateoremi uz Henkinovu semantiku

Uočimo najprije odnos Henkinove semantike i deduktivnog sustava $D2$.

Propozicija 5. *Deduktivni sustav D2 nije korektan za Henkinovu semantiku.*

Dokaz. Jednostavno se pokazuje da svaki Henkinov model zadovoljava aksiome i pravila izvođenja sustava D1. Međutim neki Henkinovi modeli ne zadovoljavaju shemu aksioma komprehenzije, dok neki od njih ne zadovoljavaju aksiom izbora.
Promotrimo npr. strukturu $\mathcal{M}^H = (M, D, F, i)$ za koju je domena M skup koji sadrži barem dva različita elementa $a \neq b$; skup relacija $D(2)$ jednočlan skup koji se sastoji od relacije $\{\langle x, a\rangle \,|\, x \,\epsilon\, M\}$; a skup funkcija $F(1)$ također jednočlan skup čiji je element funkcija identiteta na domeni.

Model $\mathcal{M}$ ne zadovoljava sljedeću instancu sheme aksioma komprenhenzije koja izražava egzistenciju prazne binarne relacije: $\exists X \forall x \forall y (Xxy \leftrightarrow x \neq x)$. $\mathcal{M}$ nema takvu relaciju, pa ne zadovoljava shemu aksioma komprehenzije. Može se dodatno pokazati da ovaj model ne zadovoljava niti aksiom izbora.

Dakle, shema aksioma komprehenzije i aksiom izbora nisu teoremi logike drugog reda uz Henkinovu semantiku. Stoga, sustav $D2$ čiji su to aksiomi nije korektan za tu logiku. □

Daljnja razmatranja provodimo na Henkinovim modelima za koje je sustav D2 korektan, tzv. vjernim modelima.

Definicija 28. *Henkinov je model vjeran sustavu D2, ili kraće* vjeran*, ako zadovoljava aksiom izbora i svaku instancu sheme komprehenzije.*

U sljedećoj lemi koristimo pojam konzistentnog skupa formula drugog reda. Definicija je u osnovi jednaka onoj za logiku prvog reda. Konzistentnost je vezana za sustav izvođenja, u ovom slučaju to je sustav D2.

Definicija 29. *Skup formula logike drugog reda S je* konzistentan *ako ne postoji formula logike drugog reda takva da vrijedi $S \vdash_{D2} \Phi$ i $S \vdash_{D2} \neg\Phi$. Inače kažemo da je skup S* inkonzistentan.
Konzistentan skup formula logike drugog reda S je maksimalno konzistentan *ako za svaku formulu logike drugog reda Φ vrijedi da je ili $\Phi \in S$ ili $\neg\Phi \in S$.*

Lema 1. (Lindenbaum lema)
Svaki konzistentan skup formula logike drugog reda ima maksimalno konzistentan nadskup.

Dokaz. Neka je S konzistentan skup i neka je $\Phi_1, \Phi_2, ...$ enumeracija formula logike drugog reda. Definiramo niz skupova formula logike drugog reda na sljedeći način: $S_1 = S$; ako je $S_n \vdash_{D2} \neg\Phi_n$ tada $S_{n+1} = S_n$; inače $S_{n+1} = S_n \cup \{\Phi_n\}$. Dakle, formulu Φ_n dodajemo u skup S_n ako on time ostaje konzistentan. Neka je S' unija skupova S_n. Dobiveni skup S' je nadskup od S. Budući da je on konzistentno proširenje skupa S, a kako su Φ_n sve formule logike drugog reda, skup S' je maksimalno konzistentan. □

Teorem 6. (potpunost)
Neka je Γ *skup formula, a* Φ *formula logike drugog reda. Tada za svaki vjeran Henkinov model* $\mathcal{M}$ *skupa formula* Γ *vrijedi:*

ako $\mathcal{M} \models \Phi$ *onda* $\Gamma \vdash_{D2} \Phi$.

Skica dokaza.
Teorem dokazujemo iz pomoćne tvrdnje:
Ako je skup Γ *konzistentan, tada je on ispunjiv u vjernom Henkinovom modelu.*

Pokažimo najprije da iz ove tvrdnje slijedi tvrdnja teorema.
Pretpostavimo da je za svaki vjeran Henkinov model $\mathcal{M}$ skupa formula Γ $\mathcal{M} \models \Phi$ i da $\Gamma \nvdash_{D2} \Phi$. Očito nije $\Phi \in \Gamma$.
Općenito se pokazuje da je skup konzistentan ako i samo ako iz njega nije izvediva bar jedna formula. Kako iz skupa Γ nije izvediva formula Φ on je konzistentan. Tada je i skup $\Gamma' = \Gamma \cup \{\neg\Phi\}$ konzistentan. Prema pomoćnoj tvrdnji postoji vjeran Henkin-model $\mathcal{M}'$ za Γ' pa je $\mathcal{M}' \models \neg\Phi$. Kontradikcija. Dakle, $\Gamma \vdash_{D2} \Phi$.

Bez gubitka općenitosti se u dokazu pomoćne tvrdnje možemo ograničiti na zatvorene formule. Neka je Γ konzistentan skup rečenica.
Proširimo jezik logike drugog reda sljedećim nelogičkim simbolima:

$c_0, c_1, ...$ prebrojivo mnogo konstantskih simbola,
$\mathsf{C}_0^n, \mathsf{C}_1^n, ...$ prebrojivo mnogo n-mjesnih relacijskih simbola za svaki n,
$\mathsf{g}_0^n, \mathsf{g}_1^n, ...$ prebrojivo mnogo n-arnih funkcijskih simbola za svaki n.

Neka je $\Psi_1, \Psi_2, ...$ enumeracija formula proširenog jezika u kojima je jedina slobodna varijabla individualna varijabla x; $\lambda_1, \lambda_2, ...$ enumeracija formula proširenog jezika u kojima je jedina slobodna varijabla neka od relacijskih varijabli $X^1, X^2, ...$; a $\Phi_1, \Phi_2, ...$ enumeracija formula proširenog jezika u kojima je jedina slobodna varijabla neka od funkcijskih varijabli $f^1, f^2, ...$.
Definiramo niz skupova rečenica proširenog jezika na sljedeći način:

$$T_0 = \Gamma$$
$$T_{m+1} = T_m \cup \{\ \exists x \Psi_m(x) \to \Psi_m(c_i), \quad \exists X^n \lambda_m(X^n) \to \lambda_m(\mathsf{C}_j^n),$$
$$\exists f^p\, \Phi_m(f^p) \to \Phi_m(\mathsf{g}_k^p)\ \}$$

gdje je c_i prvi konstantski simbol gornjeg niza koji se ne pojavljuje u formulama Ψ_m, λ_m, Φ_m i niti u jednoj formuli skupa T_m; n je mjesnost slobodne relacijske varijable u formuli λ_m, a C_j^n prvi relacijski simbol u gornjem nizu koji se ne pojavljuje u formulama Ψ_m, λ_m, Φ_m i niti u jednoj formuli skupa

T_m; p je mjesnost slobodne funkcijske varijable u formuli Φ_m, a g_k^p prvi funkcijski simbol u gornjem nizu koji se ne pojavljuje u formulama Ψ_m, λ_m, Φ_m i niti u jednoj formuli skupa T_m.
Neka je T unija skupova T_m. Skup T je konzistentan. Prema Lindenbaum lemi postoji maksimalno konzistentan nadskup $T' \supseteq T$. Posebno je $T' \supseteq \Gamma$.

Konstruiramo Henkinov model $\mathcal{M} = (M, D, F, i)$ skupa Γ na sljedeći način: domena M je skup novih konstantskih simbola $c_0, c_1, ...$; za svaki n skup $D(n)$ je skup relacija $S(\mathsf{C}_0^n), S(\mathsf{C}_1^n), ...$ gdje je $S(\mathsf{C}_j^n) = \{u \,\epsilon\, M^n | \mathsf{C}_j^n(u) \,\epsilon\, T'\}$; za svaki n skup $F(n)$ je skup funkcija $T(\mathsf{g}_0^n), T(\mathsf{g}_1^n), ...$ gdje je funkcija $T(\mathsf{g}_j^n) : M^n \to M$ takva da je $T(\mathsf{g}_j^n)\langle c\rangle_n$ prvi c_k u nizu za kojeg je $\mathsf{g}_j^n\langle c\rangle_n = c_k$ u T'.
Interpretacijska funkcija i je pridruživanje definirano kako slijedi. Svaki od konstantskih simbola c_i pridružen je sam sebi. Konstantskom simbolu c pridružen je prvi u nizu c_i za koji je rečenica $c = c_i$ u T'. Relacijskom simbolu R^n pridružena je relacija $\{\, \langle c\rangle_n \mid \mathsf{R}^n\langle c\rangle_n \,\epsilon\, T'\}$. Funkcijskom simbolu f^n pridružena je funkcija koja n-torki $\langle c\rangle_n$ pridružuje prvi c_j u nizu takav da je rečenica $\mathsf{f}^n\langle c\rangle_n = c_j$ u skupu T'. Posebno je relaciji C_j^n pridružena relacija $S(\mathsf{C}_j^n)$, a funkciji g_j^n funkcija $T(\mathsf{g}_j^n)$.
Vidljivo je da su u modelu $\mathcal{M}$ sve konstante, relacije i funkcije interpretirane kao u T'. Nadalje se pokazuje da je $\mathcal{M}$ vjeran.

Indukcijom po složenosti rečenice Φ pokazuje se da za svaku rečenicu proširenog jezika vrijedi $\mathcal{M} \models \Phi$ ako i samo ako $\Phi \,\epsilon\, T'$.
Slijedi da je $\mathcal{M}$ model skupa T', a time i model polaznog skupa Γ. □

Teorem 7. (kompaktnost)
Neka je Γ *skup formula logike drugog reda. Ako svaki konačni podskup od* Γ *ima vjeran Henkinov model, tada i skup* Γ *ima vjeran Henkinov model.*

Dokaz. Pretpostavimo da skup Γ nema vjeran Henkinov model. Prema teoremu potpunosti Γ nije konzistentan. Vrijedi $\Gamma \vdash_{D2} (\Phi \wedge \neg\Phi)$. Budući da su dedukcije konačne, postoji konačan podskup $\Gamma' \subseteq \Gamma$ takav da vrijedi $\Gamma' \vdash_{D2} (\Phi \wedge \neg\Phi)$. Prema korektnosti sustava D2 za vjerne modele, skup Γ' nema vjeran Henkinov model. Kontradikcija. □

Pokazuje se da, osim teorema potpunosti i kompaktnosti, vrijede i varijante Löwenheim-Skolemovih teorema. U tom je smislu, uz Henkinovu semantiku, logika drugog reda poput logike prvog reda. Možemo reći da niti jedna teorija s beskonačnim Henkinovim modelima nije Henkin-kategorična. Jezik logike drugog reda uz Henkinovu semantiku nije pogodan za karakterizaciju beskonačnih struktura do na izomorfizam.

6 Logika višeg reda

U standardnoj semantici jezik logike drugog reda ima istu klasu modela kao i jezik logike prvog reda. To su strukture $\mathcal{M} = (M, i)$. Denotacijska funkcija za terme drugog reda je proširenje denotacije prvog reda.

Ekspresivnost logike prvog reda znatno se proširuje prelaskom na logiku drugog reda. Logike viših redova, međutim, ne povećavaju znatno izražajnost jezika. Uz standardnu semantiku logike trećeg i višeg reda mogu se, u određenom smislu, svesti na logiku drugog reda, također sa standardnom semantikom.
Predikatske relacije između svojstava i objekata odgovaraju relaciji pripadnosti između skupova i elemenata: Px je analogon za $x \,\epsilon\, C$. Relacija pripadnosti iz teorije skupova može se uspješno izraziti jezikom drugog reda. Predikatska relacija višeg reda tretira se kao nelogička i pridružuje joj se aksiomatizacija u jeziku drugog reda.

Prisjetimo se da jezik drugog reda $L2K$ sadrži varijable i kvantifikatore po relacijama i funkcijama. Radi jednostavnosti, u jeziku n-tog reda LnK dozvolit ćemo samo monadske relacijske (predikatske) varijable i kvantifikatore. Tako su dopuštene varijable koje su predikati na predikatima, ali nisu dopuštene varijable koje su m-mjesne relacije predikata za $m > 1$, kao ni funkcijske varijable.

Ovim ograničenjem na predikatske varijable ne gubi se na općenitosti. Tako je konstrukciju uređenog para iz teorije skupova moguće simulirati jezikom n-tog reda s monadskim relacijama za dovoljno veliki n. Npr. binarna relacijska varijabla drugog reda simulira se predikatskom varijablom četvrtog reda. Funkcije i općenito m-mjesne relacije također se mogu predstaviti.

Ograničenje na predikate uvodi se radi jednostavnosti. S druge strane pri tom nailazimo na nedostatak što jezici n-tog reda nisu direktna proširenja jezika drugog reda koji sadrži funkcijske varijable i sve relacije. Stoga bi bilo zgodno u jezicima višeg reda dozvoliti funkcijske i relacijske varijable drugog reda.

Uvodimo osnove jezika n-tog reda LnK i njegove semantike za $n > 2$. Krećemo od jezika prvog reda s jednakošću $L1K =$.

Za svaki prirodan broj i, takav da je $2 \leq i \leq n$, uvodimo skup svježih varijabli i-tog reda P_i, Q_i,... i kvantifikatore. Indeksi označavaju red varijable, a mogu se izostaviti ukoliko je red jasan iz konteksta. Varijable prvog reda označavamo malim slovima.

Dodajemo sljedeća pravila za formiranje formula:

- ako je P varijabla m-tog reda i Q varijabla $(m+1)$-reda, tada je QP formula;
- ako je Φ formula i X varijabla m-tog reda, tada je i $\forall X\Phi$ formula.

Npr. X_6Y_5, $\forall X_6\exists Y_5(X_6Y_5)$ su formule.

Semantika se proširuje u standardnom smislu.
Ako je $\mathcal{M} = (M, i)$ model jezika LnK, varijable drugog reda poprimaju vrijednosti iz partitivnog skupa domene $\mathcal{P}(M)$, varijable trećeg reda poprimaju vrijednosti iz partitivnog skupa partitivnog skupa domene $\mathcal{P}(\mathcal{P}(M))$ itd.

6.1 Redukcija na logiku drugog reda

Prelazimo na redukciju na logiku drugog reda.

Neka su $\mathsf{T}_1, \mathsf{T}_2, ...$ skupovi nelogičkih predikatskih simbola, a PR nelogički binarni relacijski simbol, te pretpostavimo da se niti jedan od njih ne pojavljuje u skupu K nelogičkih simbola jezika LnK.
Neka je $K' = K \cup \{\mathsf{PR}, \mathsf{T}_1, \mathsf{T}_2, ...\}$.

Ideja je da varijable m-tog reda poprimaju vrijednosti iz skupa T_m, tako da $\mathsf{T}_m(x)$ izražava činjenicu da x odgovara nekom objektu reda m. Formula $\mathsf{PR}(t, u)$ izražava činjenicu da t predstavlja svojstvo objekta predstavljenog sa u (u smislu predikatske relacije).

Slijedi preslikavanje formula jezika LnK u odgovarajuće formule jezika $L1K' =$, te u pripadne formule jezika $L2K'$.

Najprije fiksiramo binarnu funkciju *preformuliranja* formula jezika LnK u odgovarajuće formule jezika $L1K$.
Svakoj varijabli X, odnosno x, jezika LnK pridružuje se varijabla jezika $L1K$ X', odnosno x'. Varijable X' i x' su varijable prvog reda.
Ovo se preslikavanje proširuje na sve terme jezika LnK na uobičajen način :

- ako je t konstanta, tada je t' jednako t ;
- ako je t term $ft_1, ..., t_m$, tada je t' jednako $ft'_1, ..., t'_m$.

Zatim se svakoj formuli Φ jezika LnK pridružuje formula Φ' jezika $L1K' =$ na sljedeći način:

- ako je R m-mjesni relacijski simbol, $(\mathsf{Rt}_1, ..., t_m)'$ je jednako $\mathsf{Rt}'_1, ..., t'_m$;
- ako je T varijabla m-tog reda i Y varijabla $(m+1)$-tog reda, tada je $(YT)'$ jednako $\mathsf{PR}(Y', T')$;
- $(\neg\Phi)'$ je jednako $\neg(\Phi')$;
- $(\Phi \to \Phi)'$ je jednako $(\Phi)' \to (\Psi)'$;
- ako je X varijabla m-tog reda, tada je $(\forall X\Phi)'$ jednako $\forall X'(\mathsf{T}_m(X') \to (\Phi'))$.

Sada treba izraziti predikatsku relaciju pomoću relacije PR, interpretirajući PR kao relaciju pripadnosti skupu. Potrebno je postići da vrijedi sljedeće:

(i) ekstenzija od T_{m+1} je izomorfna partitivnom skupu ekstenzije od T_m, za svaki $m < n$;
(ii) T_1 nije prazan;
(iii) svi T_i skupa iscrpljuju domenu.

To se može postići za konačne skupove nelogičkih simbola.
Ako je skup K^- konačan podskup od K, neka je $STAN(K^-, n)$ konjunkcija sljedećih rečenica jezika $L2K$':

(1) $\mathsf{T}_1(c)$ za svaki konstantski simbol c iz K^- ;

(2) $\forall x_1...\forall x_m((\mathsf{T}_1(x_1) \wedge ... \wedge \mathsf{T}_1(x_m)) \to \mathsf{T}_1(\mathsf{f}x_1...x_m))$
za svaki m-mjesni funkcijski simbol f iz K^- ;

(3) $\forall x_1...\forall x_m(\mathsf{R}x_1...x_m \to (\mathsf{T}_1(x_1) \wedge ... \wedge \mathsf{T}_1(x_m)))$
za svaki m-mjesni relacijski simbol R iz K^- ;

(4) $\exists x\mathsf{T}_1(x)$;

(5) $\forall x(\mathsf{T}_1(x_1) \vee ... \vee \mathsf{T}_1(x_n))$;

(6) $\forall x\forall y((\mathsf{PR}(y, x) \wedge \mathsf{T}_{m+1}(y)) \to \mathsf{T}_m(x))$ za svaki m, $1 \leq m \leq n$;

(7) $\forall y\forall z((\neg\mathsf{T}_1(y) \wedge \neg\mathsf{T}_1(z) \wedge \forall x(\mathsf{PR}(y, x) \leftrightarrow \mathsf{PR}(z, x))) \to y = z)$;

(8) $\forall X\exists y\,(\mathsf{T}_{m+1}(y) \wedge \forall x(\mathsf{PR}(y, x) \leftrightarrow (Xx \wedge \mathsf{T}_m(x))))$ za svaki m, $1 \leq m \leq n$.

Formula (1) izriče tvrdnju da su sve konstante iz K^- u ekstenziji od T_1, čiji su elementi pridruženi varijablama prvog reda jezika LnK. Formula (2) izriče tvrdnju da su funkcijski simboli zatvoreni u odnosu na ekstenziju od T_1. Formula (3) izriče tvrdnju da relacijski simboli poprimaju vrijednosti iz ekstenzije od T_1. Formulom (4) izriče se da ekstenzija od T_1 nije prazna, a formulom (5) da ekstenzije svih simbola T_i iscrpljuju domenu. Formula (6) izriče da ako je y predikat na x, onda je red od y za jedan veći od reda od x. Formula (7) je ekstenzionalnost relacije PR. Sve su formule (1)-(7) formule prvog reda. Jedina formula drugog reda je (8), koja ima jednu univerzalnu kvantifikaciju po varijabli drugog reda, a njezin je doseg čitava formula. Ona predstavlja neku vrstu principa komprehenzije i izriče da za svaki skup X postoji y $(m+1)$-tog reda takav da je y predikat na točno onim x-evima koji su u skupu X.

Za svaku rečenicu Φ iz LnK, označimo sa Φ^+ formulu $STAN(K^-, n) \rightarrow \Phi'$, gdje se skup K^- sastoji od elemenata skupa K koji nastupaju u Φ.
Formula Φ^+ je drugog reda.

Ovime je dana redukcija jezika višeg reda LnK na jezik drugog reda $L2K'$.

Neka je $\mathcal{P}$ operator partitivnog skupa: $\mathcal{P}^0(a) = a$ i $\mathcal{P}^{m+1}(a) = \mathcal{P}(\mathcal{P}^m(a))$ za svaki m.

Lema 2. *Neka je $\mathcal{M} = (M, i)$ struktura u jeziku LnK.*
Tada postoji struktura $\mathcal{M}^+ = (M^+, i^+)$ u jeziku $L2K'$ takva da vrijedi:
$\mathcal{M} \models STAN(K^-, n)$ *za svaki konačan* $K^- \subseteq K$ *i*
$\mathcal{M} \models \Phi$ *ako i samo ako* $\mathcal{M}^+ \models \Phi^+$ *za svaku rečenicu* Φ *jezika LnK.*

Dokaz. Neka je domena $M^+ = M \cup \mathcal{P}(M) \cup ... \cup \mathcal{P}^{n-1}(M)$.
Interpretacija na M^+ se nasljeđuje:
$i^+(c) = i(c)$ za svaki konstantski simbol c ;
$i^+(\mathsf{R}) = i(\mathsf{R})$ za svaki relacijski simbol R ;
$i^+(\mathsf{f}) = i(\mathsf{f})$ za svaki funkcijski simbol f .
Za one x koji nisu u domeni M je $i^+(\mathsf{f})(x) = x$.
Na novim relacijskim simbolima T_i i PR interpretacija je definirana sa:
$i^+(\mathsf{T}_m) = \mathcal{P}^{m-1}(M)$ za svaki m, $1 \leq m \leq n$;
$i^+(\mathsf{PR}) = \{(x, y) \mid$ postoji m, $1 < m < n$, takav da je $y \,\epsilon\, \mathcal{P}^m(M)$ *i* $x \,\epsilon\, y\}$.
Dakle, relacija PR interpretirana je na M^+ kao relacija pripadnosti skupu.
Lako se pokazuje da vrijedi $\mathcal{M}^+ \models STAN(K^-, n)$ i da vrijedi
$\mathcal{M} \models \Phi$ ako i samo ako $\mathcal{M}^+ \models \Phi'$ ako i samo ako $\mathcal{M}^+ \models \Phi^+$. $\square$

Lema 3. *Neka je* $\mathcal{M} = (M, i)$ *struktura u jeziku* $L2K'$ *takva da za svaki konačan* $K^- \subseteq K$ *vrijedi* $M \models STAN(K^-, n)$.
Tada postoji struktura $\mathcal{M}' = (M', i')$ *u jeziku* LnK *takva da za svaku rečenicu* Φ *jezika* LnK *vrijedi:*

$\mathcal{M}' \models \Phi$ *ako i samo ako* $\mathcal{M} \models \Phi'$ *ako i samo ako* $\mathcal{M} \models \Phi^+$.

Dokaz. Neka je M' ekstenzija relacije T_1 u M, tj. $M' = i(T_1)$, te neka je i' restrikcija od i tako da je M' podmodel od M.
Lako se pokazuje da vrijedi: $\mathcal{M}' \models \Phi$ ako i samo ako $\mathcal{M} \models \Phi'$ ako i samo ako $\mathcal{M} \models \Phi^+$. □

Ove dvije leme imaju za posljedicu sljedeći teorem koji predstavlja bazu redukcije logike višeg reda na logiku drugog reda.

Teorem 8. *Za svaku rečenicu* Φ *n-tog reda jezika* LnK *postoji rečenica* Φ^+ *drugog reda jezika* $L2K'$ *takva da vrijedi:*

ako je Φ *ispunjiva, onda je i* Φ^+ *ispunjiva ;*

Φ *je valjana u jeziku* LnK *ako i samo ako je* Φ^+ *valjana u jeziku* $L2K'$.

Nelogički simboli korišteni za definiciju formule Φ^+ mogu se eliminirati. Formula jezika višeg reda reducira se na taj način na formulu drugog reda s istim skupom nelogičkih simbola.

Teorem 9. *Za svaku rečenicu* Φ *n-tog reda jezika* LnK *postoji rečenica* Φ^{++} *drugog reda jezika* $L2K$ *takva da vrijedi:*

ako je Φ *ispunjiva, onda je i* Φ^{++} *ispunjiva ;*

Φ *je valjana ako i samo ako je* Φ^{++} *valjana.*

Dokaz. Svaki nastup simbola T_i u formuli Φ^+ zamijeni se s monadskom relacijskom varijablom Y_i koja se ne pojavljuje u Φ', a svaki nastup simbola PR binarnom relacijskom varijablom P^2 koja se ne pojavljuje u Φ'.
Označimo dobivenu formulu sa Φ^{++}.
To je formula jezika $L2K$ u kojoj su varijable $Y_1, ..., Y_n$ i P^2 slobodne.
Formula Φ^{++} je valjana ako i samo ako je $\forall P^2 \forall Y_1 ... \forall Y_n(\Phi^{++})$ valjana formula jezika $L2K$. □

Dio II
Isabelle

Robin Milner, potaknut Scottovom "Logikom izračunljivih funkcija" (1969), izgradio je *Edinburgh LCF*, sustav za provjeru dokaza (proof checker) koji je bio programabilan. Meta-jezik Edinburgh LCF-a, ML (Meta Language), ne predstavlja samo nizove naredbi. ML daje generalnu reprezentaciju logike. Termi i formule su izračunljivi podaci. Takvi su također i teoremi. Svako pravilo izvođenja je funkcija sa teorema na teoreme. Teorem se može izgraditi jedino primjenom pravila na postojeće teoreme.
Iako je dokazivanje unaprijed fundamentalno, obično se u dokazivanju preferira krenuti od cilja unatrag. Svako pravilo izvođenja preslikava premise u konkluziju. Inverz tog preslikavanja, kojeg zovemo *taktika*, cilj preslikava u podciljeve. Taktika uz to daje i validaciju, funkciju s teorema na teorem. Kada je dokaz unatrag završen, validacijska funkcija izvrši dokaz unaprijed i daje traženi teorem. *Taktikali* (tacticals) operiraju taktikama, predstavljajući kontrolne strukture kao što su sekvencijalno izvođenje ili ponovna aplikacija taktike.
Korektnost je osigurana ML-ovom sigurnom provjerom tipova: teoremi se konstruiraju samo pomoću pravila izvođenja. Slučajevi kada se pravilo ili taktika krivo koriste se signalizira. Ipak, taktika može biti nevaljana: obećava više no što može dati. Ukoliko je njena validacija kriva, konačni dokaz unaprijed ne daje očekivani teorem.
LCF okolina raste s upotrebom, pravila se komponiraju kao funkcije, taktike se kombiniraju pomoću taktikala.

Do 1986. godine tehnike Edinburgh LCF-a proširile su se na nekoliko sustava. ML je postao zaseban jezik. Isabelle je dostigla upotrebljivu formu. Ona se razvila kao pokušaj da se u LCF-stilu dozvoli dokazivanje u različitim logikama. U Isabelle-86 pravilo je predstavljeno Hornovom klauzulom. Dokazi se grade kombinacijom pravila. Pošto su dokazivanje unaprijed i unatrag samo stilovi u konstukciji dokaza, nema razlike između pravila izvođenja i taktike. Svako stanje u dokazu unatrag je izvedeno pravilo:

$$\frac{\text{podcilj ... podcilj}}{\text{cilj}}$$

Pravila izvođenja kod Isabelle su aksiomi u meta-logici kojima se izražava da premise impliciraju konkluziju. Isabelle-ine taktike i taktikali mogli su se koristiti kao kod LCF-a, iako su bili bazirani na drugim principima.

Početni su problemi bili oko implementacije. Kvantifikatori su tražili sintaksu s tipiziranim λ-računom, dok je kombiniranje pravila zahtjevalo unifikaciju. Zajedno, zahtjevali su unifikaciju višeg reda. L.C.Paulson eksperimentirao je s raznim načinima nametanja ograničenja na varijable pri kvantifikaciji. Konačno, Isabelle-86 podržavala je mnoge logike: Martin-Löf-ovu teoriju tipova, intuicionistički i klasičan sekventni račun, Zermelo-Fraenkel-ovu teoriju skupova. Bila je implementirana u standardnom ML-u. Bazirala se na naivnom računu s pravilima. Mnoga su pitanja ostala otvorena, kao npr. treba li sljedeća pravila smatrati različitim:

$$\frac{A \quad B}{C} \qquad \frac{B \quad A}{C} \qquad \frac{A \quad B \quad A}{C}$$

Danas je meta-logika Isabelle dio logike višeg reda. Implikacija izražava logičku posljedičnost, univerzalni kvantifikator izražava shematska pravila izvođenja i sheme aksioma, ekvivalencija izražava definicije. Isabelle konstruira dokaze dedukcijama u meta-logici. Njezin tretman dokazivanja unatrag ima znatne prednosti u odnosu na LCF. Stanje dokaza kod Isabelle je formalizirano meta-teoremom; nema validacija. Osigurava se da su podciljevi dostatni da bi se postigao konačni cilj.

Matematika zahtjeva živi jezik. Definicije proširuju sintaksu, teoremi proširuju primitivne modele zaključivanja. Tako se npr. u Zermelo-Fraenkel-ovoj teoriji skupova kartezijev produkt definira pomoću partitivnog skupa, unije, sparivanja i aksioma projekcija. "Očita" svojstva kao npr.

$$\frac{a \in A \quad b \in B}{\langle a, b \rangle \in A \times B}$$

imaju naporne dokaze. Matematičar će, nakon što dokaže svojstvo, koristiti kartezijev produkt s ovim svojstvom kao novim pravilom zaključivanja. Isabelle je pokušaj da se slijedi taj stil.

7 Meta-logika $\mathcal{M}$

Isabelle je interaktivni dokazivatelj teorema (theorem prover) koji podržava razne logike. Svaka se tzv. objektna logika formalizira pomoću Isabelle-ine meta-logike. Novi tipovi i konstante izražavaju sintaksu objektne logike, a novi aksiomi objektna pravila izvođenja.
Meta-logiku (logical framework = logičko okružje) čine formule (propositions) koje predstavljaju pravila. Dokazi se grade kombinacijom pravila.

Isabelle-ina meta-logika je logika višeg reda (simple type theory - prosta teorija tipova), a bazira se na tipiziranom λ računu. Isabelle podržava inferenciju tipova u ML stilu uz unifikaciju. Unifikacija višeg reda (Huet, [22]) koristi α, β i η-konverzije i može vratiti višestruko ili čak beskonačno mnogo rezultata. Iako je općenito ovaj problem neodlučiv, procedura unifikacije dobro funkcionira u Isabelle.

Ono zbog čega je prosta teorija tipova (Church, [21]) logika višeg reda je to što je dozvoljena neograničena kvantifikacija po propozicijama svakog reda. Logika prvog reda dozvoljava kvantifikaciju po individualnim varijablama; logika drugog reda dozvoljava kvantifikaciju po svojstvima individualnih varijabli; logika trećeg reda dozvoljava kvantifikaciju po svojstvima svojstava individulanih varijabli; itd. Logika višeg reda (reda ω) dozvoljava sve te kvantifikacije.
Church je, pomoću tipiziranog λ-računa, precizno formulirao sintaksu proste teorije tipova, uključujući kvanitfikatore. Njegova je tehnika danas standardna kod generičkih dokazivatelja teorema.

Prirodno je zapitati se može li meta-logika formalizirati samu sebe. Zapravo, objektna verzija logike višeg reda mnogo je šira od meta-logike jer izražava razne vrste matematika. Meta-logika treba samo izraziti druge formalne sustave.

7.1 λ-račun

λ-račun je teorija koja funkcije promatra kao pravila računanja, a ne kao grafove, odnosno relacije. Time je naglašen računalni aspekt funkcije.
Uobičajeno je uz funkcije promatrati izraze oblika $f(x) = x + 1$. Međutim, kako zapisati što je sama funkcija f ? U λ-računu f je funkcija $\lambda x.x + 1$.
Funkcija je pravilo kojim od argumenta dolazimo do vrijednosti, a to je pravilo kodirano u samoj definiciji funkcije.

Tipizirani λ-račun ima osnovne tipove i funkcijske tipove: ako su A i B tipovi, onda je $A \to B$ tip. Svakom je termu pridružen tip, u oznaci: $term : tip$.
Termi λ-računa su riječi definirane sljedećom induktivnom definicijom:

- konstante $a, b, ..$ su termi λ-računa za svaki tip A
- varijable $x, y, ..$ su termi λ-računa za svaki tip A
- ako je $x : A$ varijabla, a $b : B$ term, tada je $\lambda x.b$ term tipa $A \to B$
- ako su $a : A \to B$ i $b : A$ termi, tada je (ab) term tipa B.

Termi se, dakle, izgrađuju funkcijskom apstrakcijom $\lambda x.b$ i aplikacijom (ab).
Funkcijska apstrakcija $\lambda x.b$ veže varijablu x.

Uobičajeno je koristiti sljedeće pokrate. Aplikacija asocira s lijeva, tako da uzastopnu aplikaciju $(...(ab_1)...b_m)$ kraće pišemo $ab_1, ..., b_m$.
Uzastopnu apstrakciju $\lambda x_1(\lambda x_2(...(\lambda x_n.t)...))$ kraće pišemo $\lambda x_1 x_2 ... x_n.t$
Vanjske zagrade se ne pišu.

Od velike je koristi prihvatiti *konvenciju o varijablama*. Ona osigurava da su u svakom nastupu, u svakom kontekstu slobodne varijable različite od svih vezanih varijabli.

Među termima se definira relacija ekvivalencije pravilima λ-*konverzije*. Tako se izjednačuju termi koji su jednaki u smislu funkcijskog procesa. Ta pravila možemo promatrati kao pravila za računanje terama.

Pravila λ-konverzije

$$a \equiv a \qquad \frac{a \equiv b}{b \equiv a} \qquad \frac{a \equiv b \quad b \equiv c}{a \equiv c}$$

$$\frac{f \equiv g \quad a \equiv b}{fa \equiv gb} \qquad \text{kompatibilnost}$$

$$\lambda x.a \equiv \lambda y.a[y/x] \qquad \alpha\text{-konverzija } *$$

$$(\lambda x.a)(b) \equiv a[b/x] \qquad \beta\text{-konverzija}$$

$$\frac{a \equiv b}{\lambda x.a \equiv \lambda x.b} \qquad \eta\text{-konverzija}$$

$$\frac{fx \equiv gx}{f \equiv g} \qquad \text{ekstenzionalnost } **$$

Prva tri pravila su refleksivnost, simetričnost i tranzitivnost.
Kompatibilnost izražava činjenicu da su termi izgrađeni od ekvivalentnih komponenti ekvivalenti.
α-konverzija je preimenovanje vezane varijable uz ograničenje * da y nije slobodna u a, što je jasno po konvenciji o varijablama.
Uz ekstenzionalnost dolazi ograničenje ** da x nije slobodna u f i g. Konvencija o varijablama osigurava ispunjenje tog uvjeta.
Ekstenzionalnost je ekvivalentna η-konverziji: $\lambda x.fx \equiv f$ gdje x nije slobodna u f. U pravilima smo koristili supstituciju. Ona se definira induktivno:

- $x[b/x] \equiv b$
- $y[b/x] \equiv y \quad$ za $y \neq x$
- $(\lambda y.a)[b/x] \equiv \lambda y.a[b/x]$
- $cd[b/x] \equiv c[b/x]d[b/x]$

Ako je b term, $x_1, ..., x_k$ različite varijable, a $a_1, ..., a_k$ termi redom istog tipa kao varijable $x_1, ..., x_k$, tada je $b[a_1/x_1, ..., a_k/x_k]$ term koji dobijemo istovremenom supstitucijom svakog slobodnog nastupa varijable x_i termom a_i u b za $i = 1, ..., k$.
Ponekad ćemo koristiti i notaciju bs gdje je s supstitucija $[a_1/x_1, ..., a_k/x_k]$. Iz konteksta će biti jasno radi li se o supstituciji ili o funkcijskoj aplikaciji. Štoviše, supstitucija iz objektne logike se na meta nivou izražava upravo aplikacijom fa preko β-redukcije $(\lambda x.b)(a) \equiv b[a/x]$.

Konačno, navodimo rezultate na koje ćemo se kasnije pozivati.
Tipizirani λ-račun zadovoljava jaku normalizaciju i Church-Rosserovo svojstvo. Svaki se term može na određen način, izračunati "do kraja", do normalne forme, određene do na α-konverziju. Vrijedi jaki teorem normalizacije: *Svaki term ima normalnu formu, jedinstvenu do na α-konverziju.* [7]

7.2 Sintaksa meta-logike $\mathcal{M}$

Tipovi (arities) meta-logike se sastoje od osnovnih tipova σ i funkcijskih tipova oblika $\sigma \to \tau$. Tipove označavamo grčkim slovima σ, τ, υ.
Termi meta-logike su termi λ-računa; konstante, varijable, apstrakcije i aplikacije (kombinacije).
Činjenicu da je term a tipa σ označavamo s $a : \sigma$.

Osnovni tipovi i konstante ovise o logici koja se želi reprezentirati, a uvijek sadrže tip propozicija *prop* i logičke konstante. Formula je term tipa *prop*.
Konstantski simboli sadrže za svaki tip σ:

$$\Rightarrow : prop \to (prop \to prop)$$
$$\bigwedge_{\sigma} : (\sigma \to prop) \to prop$$
$$\equiv_{\sigma} : \sigma \to (\sigma \to prop)$$

Simboli implikacije $\Rightarrow$, ekvivalencije $\equiv$ i univerzalni kvantifikator $\bigwedge$ u meta-logici, radi preglednosti, različiti su od odgovarajućih simbola iz objektnog jezika.

Implikacija $\Rightarrow$ asocira s desna. Ako je Φ niz formula $\Phi_1, ..., \Phi_m$ implikaciju $\Phi_1 \Rightarrow (... \Rightarrow (\Phi_m \Rightarrow \Psi)...)$ kraće pišemo na jedan od sljedećih načina:

$$\Phi_1 \Rightarrow ... \Rightarrow \Phi_m \Rightarrow \Psi \qquad [\Phi_1, ..., \Phi_m] \Rightarrow \Psi \qquad \Phi \Rightarrow \Psi.$$

7.3 Semantika meta-logike $\mathcal{M}$

Logika višeg reda jezik je u kojem se piše formalna matematika. Moguće ju je opravdati intuitivno, ili pak pokazati konzistentnost konstrukcijom standardnog modela u teoriji skupova. Tipovi predstavljaju skupove, apstrakcije funkcije na skupovima, a tipiziranje pripadnost skupu.

Svaki tip predstavlja neprazan skup. Ako su dani skupovi za svaki osnovni tip, tada je interpretacija tipa $\sigma \to \tau$ skup funkcija sa skupa σ u skup τ.

Zatvoren term (term bez slobodnih varijabli) tipa σ predstavlja vrijednost iz odgovarajućeg skupa. Uz dane vrijednosti za konstante, λ-apstrakcije predstavljaju funkcije.

Tip *prop* predstavlja skup istinosnih vrijednosti. Klasična logika koristi $\{\top, \bot\}$.
Logičke konstante $\Rightarrow$, $\bigwedge_\sigma$ i $\equiv_\sigma$ predstavljaju odgovarajuće istinosne funkcije.
Implikacija $\Phi \Rightarrow \Psi$ znači "formula Φ implicira formulu Ψ".
Univerzalno kvantificirana formula $\bigwedge_\sigma x.\Phi$ znači "za svaki x iz skupa predstavljenog tipom σ, formula Φ je istinita".
Ekvivalencija $a \equiv b$ znači "a jednako b".

Kvantifikacija koristi λ-apstakciju. Za svaki tip σ imamo logičku konstantu $\bigwedge_\sigma$ tipa $(\sigma \to prop) \to prop$. Formula $\bigwedge_\sigma x.\Phi$ kraći je zapis od $\bigwedge_\sigma(\lambda x.\Phi)$. Pomoću λ-konverzija svaka se kvantifikacija može svesti na oblik $\bigwedge_\sigma(f)$, gdje je f term tipa $\sigma \to prop$. Preglednije je umjesto $\bigwedge_\sigma(f)$ koristiti zapis $\bigwedge x.f(x)$.

Istinitost na nivou objektne logike (tip $form$) razlikuje se od istinitosti na nivou meta-logike (tip *prop*). Međutim, one su povezane. Na meta-nivou potrebno je samo znati da li je dana vrijednost iz $form$ istinita. Može se uvesti konstanta $\top$ kako bi se izrazilo "P je istinito" pomoću $P \equiv \top$, no općenitije je uvesti meta-predikat koji iskazuje sve istinitosti:

$$true : form \to prop$$

Tada "P je istinito" iskazujemo s $true(P)$, ili kraće $[\![P]\!]$. Dakle, formula objektne logike A unutar zagrada $[\![\ \ ]\!]$ predstavlja meta-formulu $[\![A]\!]$ koja je pokrata za $true(A)$ što znači da je A istinito. Ovim razdvajanjem istinosnih vrijednosti objektne i meta-logike, postiže se preglednost i izbjegava miješanje dviju logika, isto kao i kod upotrebe različitih simbola za implikaciju, ekvivalenciju i kvantifikaciju.

Napomena: Zahtjev da svaki tip predstavlja neprazan skup dozvoljava sljedeći jednostavan sustav zaključivanja u kojem je $(\bigwedge x.\bigwedge \theta.\theta) \Rightarrow (\bigwedge \theta.\theta)$ teorem. Ovdje je θ vezana varijabla tip *prop*.
Kada bi dozvolili da je tip od x prazan, tada bi $\bigwedge \theta.\theta$ bilo istinito. Svaka bi formula bila istinita, pa bi logika bila inkonzistentna.

Lambek i Scott [20] prezentirali su sustav zaključivanja za logiku višeg reda u kojem su dozvoljeni prazni tipovi.

7.4 Pravila izvođenja

Meta-dokazivanje provodi se sljedećim pravilima izvođenja.

$$\frac{\begin{array}{c}[\Phi]\\ \Psi\end{array}}{\Phi \Rightarrow \Psi} \qquad \frac{\Phi \Rightarrow \Psi \quad \Phi}{\Psi}$$

$$\frac{\Phi}{\bigwedge x.\Phi}\ * \qquad \frac{\bigwedge x.\Phi}{\Phi[b/x]}$$

$$a \equiv a \qquad \frac{a \equiv b}{b \equiv a} \qquad \frac{a \equiv b \quad b \equiv c}{a \equiv c}$$

$$(\lambda x.a) \equiv (\lambda y.a[y/x]) \qquad ((\lambda x.a)(b)) \equiv (a[b/x]) \qquad \frac{fx \equiv gx}{f \equiv g}\ **$$

$$\frac{a \equiv b}{(\lambda x.a) \equiv (\lambda x.b)} \qquad \frac{f \equiv g \quad a \equiv b}{fa \equiv gb}$$

Pravila izvođenja vezana za $\Rightarrow$ i $\bigwedge$ su pravila prirodne dedukcije.
Kod $\Rightarrow$-introdukcije otpušta se pretpostavka. Pravilo $\bigwedge$-introdukcije (generalizacija) ima za uvjet * da varijabla x ne nastupa slobodna u pretpostavkama. Uz ekvivalenciju vezana su pravila refleksivnosti, simetričnosti i tranzitivnosti.
Preostala pravila su pravila λ-računa: α-konverzija, β-konverzija, ekstenzionalnost uz uvjet ** da x nije slobodna pretpostavkama niti u f i g, apstrakcija i aplikacija.
α-konverziju smo mogli i ispustiti kao pravilo izvođenja budući da se podrazumijeva prema konvenciji o varijablama.
Logička ekvivalencija znači ekvivalenciju istinosnih vrijednosti:

$$\frac{\begin{array}{cc}[\Phi] & [\Psi]\\ \Psi & \Phi\end{array}}{\Phi \equiv \Psi} \qquad \frac{\Phi \equiv \Psi \quad \Phi}{\Psi}$$

8 Formalizacija logike prvog reda

Reprezentacija klasične logike prvog reda metalogikom Isabelle je vjerna, odnosno korektna je i potpuna. Korektnost znači da se svakom meta-dokazu može prodružiti pripadajući dokaz u objektnoj logici, dok potpunost za svaki dokaz u objektnoj logici zahtjeva adekvatan dokaz u meta-logici.

Sljedeći deduktivni sustav za logiku prvog reda ekvivalentan je sustavu D1. To je standardni sustav prirodne dedukcije (Prawitz, [4]) gdje je $\bot$ laž, a $\neg P$ je pokrata za $P \to \bot$.

$$\frac{P \quad Q}{P \wedge Q} \qquad \frac{P \wedge Q}{P} \quad \frac{P \wedge Q}{Q}$$

$$\frac{P}{P \vee Q} \quad \frac{Q}{P \vee Q} \qquad \frac{P \vee Q \quad \begin{matrix}[P] \\ R\end{matrix} \quad \begin{matrix}[Q] \\ R\end{matrix}}{R}$$

$$\frac{\begin{matrix}[P] \\ Q\end{matrix}}{P \to Q} \qquad \frac{P \to Q \quad P}{Q}$$

$$\frac{\begin{matrix}[P \to \bot] \\ \bot\end{matrix}}{P}$$

$$\frac{P(x)}{\forall x P(x)} \qquad \frac{\forall x P(x)}{P(t)}$$

$$\frac{P(t)}{\exists x P(x)} \qquad \frac{\exists x P(x) \quad \begin{matrix}[P(x)] \\ Q\end{matrix}}{Q}$$

U logici prvog reda služimo se termima i formulama. Kako bismo ih predstavili u tipiziranom λ-računu, uvodimo tipove $term$ i $form$, te konstantske simbole za logičke veznike i kvantifikatore:

$$\begin{aligned} \bot &: form \\ \wedge, \vee, \rightarrow &: form \rightarrow (form \rightarrow form) \\ \forall, \exists &: (term \rightarrow form) \rightarrow form \end{aligned}$$

Za veznike $\wedge, \vee, \rightarrow$ koristit ćemo infiksnu notaciju.

Sa sintaktičkog gledišta, svaki meta-logički term tipa *term* reprezentira neki term logike prvog reda, a svaki meta-logički term tipa $form$ reprezenitra neku formulu.
Logičkim simbolima gradimo formule; ako P i Q reprezentiraju formule, tada i $P \wedge Q$ reprezentira formulu. Upotreba kvantifikatora reprezentira se λ-apstrakcijom: formula $\forall x P(x)$ reprezentira se sa $\forall(\lambda x.P(x))$.

Semantički pogled potreban je kako bi razumjeli reprezentaciju pravila. Tip $form$ ima za denotaciju skup istinosnih vrijednosti $\{\top, \bot\}$. Denotacija veznika $\wedge, \vee, \rightarrow$ definirana je tablicama istine. Tip *term* ima za denotaciju neprazan skup individua.

Kvanitfikatori $\forall$ i $\exists$ beskonačne su verzije veznika $\wedge$ i $\vee$. Neka je $P(x)$ tipa $form$, gdje je x tipa *term*. Ako je $P(x)$ istinito, tj. jednako $\top$ za svaki x, tada je $\lambda x.P(x)$ funkcija definirana na individuama koja je konstantno jednaka $\top$, odnosno $\lambda x.P(x)$ je jednako $\top$. Općenito, $\forall(F)$ je jednako $\top$ ako i samo ako je $F(x)$ jednako $\top$ za svaki x.
Egzistencijalni kvantifikator može se slično interpretirati beskonačnom tablicom istine koja definira $\exists(F)$: $\exists(F)$ je jednako $\bot$ ako i samo ako je $F(x)$ jednako $\bot$ za svaki x.

8.1 Formalizacija pravila dedukcije

Za svako pravilo na nivou objektne logike uvodimo meta-aksiom.

$$\bigwedge PQ.[\![P]\!] \Rightarrow ([\![Q]\!] \Rightarrow [\![P \wedge Q]\!])$$

$$\bigwedge PQ.[\![P \wedge Q]\!] \Rightarrow [\![P]\!] \qquad \bigwedge PQ.[\![P \wedge Q]\!] \Rightarrow [\![Q]\!]$$

$$\bigwedge PQ.[\![P]\!] \Rightarrow [\![P \vee Q]\!] \qquad \bigwedge PQ.[\![Q]\!] \Rightarrow [\![P \vee Q]\!]$$

$$\bigwedge PQR.[\![P \vee Q]\!] \Rightarrow ([\![P]\!] \Rightarrow [\![R]\!]) \Rightarrow ([\![Q]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]$$

$$\bigwedge PQ.([\![P]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![P \rightarrow Q]\!]$$
$$\bigwedge PQ.[\![P \rightarrow Q]\!] \Rightarrow ([\![P]\!] \Rightarrow [\![Q]\!])$$

$$\bigwedge P.([\![P \rightarrow \bot]\!] \Rightarrow [\![\bot]\!]) \Rightarrow [\![P]\!]$$

$$\bigwedge F.(\bigwedge x.[\![F(x)]\!]) \Rightarrow [\![\forall x F(x)]\!]$$
$$\bigwedge Fy.[\![\forall x F(x)]\!] \Rightarrow [\![F(y)]\!]$$

$$\bigwedge Fy.[\![F(y)]\!] \Rightarrow [\![\exists x F(x)]\!]$$
$$\bigwedge FQ.[\![\exists x F(x)]\!] \Rightarrow (\bigwedge x.[\![F(x)]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![Q]\!]$$

Sintaktički, i aplikacija pravila i otpuštanje pretpostavki reprezentirani su pomoću $\Rightarrow$. Treba primjetiti da $\Rightarrow$ asocira s desna.

Semantički, aksiomi se jasno iščitavaju, npr. "ako je $P \wedge Q$ istinito, onda je P istinito". Kod otpuštanja pretpostavki, npr. kod introdukcije kondicionala čitali bismo "ako iz pretpostavke P slijedi Q, tada $P \rightarrow Q$ mora biti istinito". Ovo uobičajeno zaključivanje formalizirano je tim meta-aksiomom. Aksiomi introdukcije i eliminacije kondicionala zajedno daju ekvivalenciju $[\![P \rightarrow Q]\!]$ i $[\![P]\!] \Rightarrow [\![Q]\!]$, pa su na taj način i $\Rightarrow$ i $\rightarrow$ meta-implikacije.

Kod reprezentacije kvantifikacijskih pravila u Isabelle, doseg kvantifikatora je funkcijska varijabla F. Sintaktički, ako je F $\lambda x.P(x)$, tada je funkcijska aplikacija $F(t)$ jednaka $(\lambda x.P(x))(t)$, što je po β-konverziji $P(t)$. Semantički, F je funkcija sa skupa individua u skup istinosnih vrijednosti.
Pravilo uvođenja univerzalnog kvantifikatora izražava da je $\forall$ beskonačna konjunkcija, kao što smo već spomenuli: $\forall x F(x)$ će biti istinito ako vrijedi premisa da je $F(x)$ istinito za svaki x. Aksiomi introdukcije i eliminacije univerzalnog kvantifikatora zajedno daju ekvivalenciju $[\![\forall x F(x)]\!]$ i $\bigwedge x.[\![F(x)]\!]$.
Pravilo eliminacije egzistencijalnog kvantifikatora semantički izražava: ako je $\exists x F(x)$ istinito, tada je F(x) istinito za neki x, a pošto iz $F(x)$ slijedi Q za svaki x, tada je zaista Q istinito.

8.2 Potpunost i korektnost reprezentacije logike prvog reda

Svaki je meta-aksiom korektan u odnosu na semantičke tablice logičkih konstanti. Vrijedi i jača tvrdnja: meta-dokazi i objektni dokazi mogu se sintaktički, pravilo-po-pravilo prevoditi:

$$\begin{array}{c} [\![P_1]\!] \ldots [\![P_m]\!] \\ \bigtriangledown \\ [\![Q]\!] \end{array} \quad \rightleftharpoons \quad \begin{array}{c} P_1 \ldots P_m \\ \bigtriangledown \\ Q \end{array}$$

Teorem 10. *Reprezentacija klasične logike prvog reda u Isabelle je potpuna.*

Dokaz. Treba pokazati da za svaki dokaz u objektnoj logici postoji odgovarajući meta-dokaz.
Bez gubitka općenitosti možemo pretpostaviti da u formuli objektne logike nastupaju samo logički veznici $\vee, \rightarrow$ i kvantifikator $\forall$.
Dokaz provodimo indukcijom po veličini objektnog dokaza.
Promatramo zadnje primjenjeno pravilo prirodne dedukcije u dokazu.

Kod $\vee$ introdukcije pripadne meta-aksiome instanciramo za formule p i q ($\bigwedge$-eliminacija), a prema pretpostavci indukcije postoji meta-dokaz za $[\![p]\!]$, te je traženi meta-dokaz:

$$\dfrac{\dfrac{\dfrac{\bigwedge PQ.[\![P]\!] \Rightarrow [\![P \vee Q]\!]}{\bigwedge Q.[\![p]\!] \Rightarrow [\![p \vee Q]\!]} \quad \bigtriangledown}{[\![p]\!] \Rightarrow [\![p \vee q]\!]} \quad [\![p]\!]}{[\![p \vee q]\!]}$$

Kod $\rightarrow$ introdukcije pripadne meta-aksiome instanciramo za formule p i q, a prema pretpostavci indukcije postoji dokaz za $[\![q]\!]$ iz pretpostavke $[\![p]\!]$. Otpuštanje ove pretpostavke na meta-nivou dokazuje $[\![p]\!] \Rightarrow [\![q]\!]$. Traženi meta-dokaz je:

$$\dfrac{\dfrac{\dfrac{\bigwedge PQ.([\![P]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![P \rightarrow Q]\!]}{\bigwedge Q.([\![p]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![p \rightarrow Q]\!]} \quad \begin{array}{c}[[\![p]\!]] \\ \bigtriangledown \\ [\![q]\!]\end{array}}{([\![p]\!] \Rightarrow [\![q]\!]) \Rightarrow [\![p \rightarrow q]\!]} \quad \dfrac{}{[\![p]\!] \Rightarrow [\![q]\!]}}{[\![p \rightarrow q]\!]}$$

Kod $\vee$ eliminacije pripadne meta-aksiome instanciramo za formule p, q i r. Prema pretpostavci indukcije postoji dokaz za $[\![p \vee q]\!]$, te dokazi za $[\![r]\!]$ iz

pretpostavke $[\![p]\!]$ i za $[\![r]\!]$ iz pretpostavke $[\![q]\!]$. Tu se na meta-nivou otpuštaju pretpostavke pravilima $\Rightarrow$-introdukcije. Dobili smo meta-dokaz:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge PQR.[\![P \vee Q]\!] \Rightarrow ([\![P]\!] \Rightarrow [\![R]\!]) \Rightarrow ([\![Q]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]}{\bigwedge QR.[\![p \vee Q]\!] \Rightarrow ([\![p]\!] \Rightarrow [\![R]\!]) \Rightarrow ([\![Q]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]}}{\bigwedge R.[\![p \vee q]\!] \Rightarrow ([\![p]\!] \Rightarrow [\![R]\!]) \Rightarrow ([\![q]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]} \quad \nabla \; [\![p \vee q]\!]}{[\![p \vee q]\!] \Rightarrow ([\![p]\!] \Rightarrow [\![r]\!]) \Rightarrow ([\![q]\!] \Rightarrow [\![r]\!]) \Rightarrow [\![r]\!]} \quad \dfrac{[[\![p]\!]] \quad \nabla \; [\![r]\!]}{[\![p]\!] \Rightarrow [\![r]\!]}}{([\![p]\!] \Rightarrow [\![r]\!]) \Rightarrow ([\![q]\!] \Rightarrow [\![r]\!]) \Rightarrow [\![r]\!]} \quad \dfrac{[[\![q]\!]] \quad \nabla \; [\![r]\!]}{[\![q]\!] \Rightarrow [\![r]\!]}}{([\![q]\!] \Rightarrow [\![r]\!]) \Rightarrow [\![r]\!]}}{[\![r]\!]}$$

Kod $\rightarrow$ eliminacije pripadne meta-aksiome instanciramo za formule p i q, a prema pretpostavci indukcije postoji dokaz za $[\![p \rightarrow q]\!]$ i dokaz za $[\![p]\!]$, pa imamo meta-dokaz:

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge PQ.[\![P \rightarrow Q]\!] \Rightarrow ([\![P]\!] \Rightarrow [\![Q]\!])}{\bigwedge Q.[\![p \rightarrow Q]\!] \Rightarrow ([\![p]\!] \Rightarrow [\![Q]\!])} \quad \nabla \; [\![p \rightarrow q]\!]}{[\![p \rightarrow q]\!] \Rightarrow ([\![p]\!] \Rightarrow [\![q]\!])} \quad \nabla \; [\![p]\!]}{[\![p]\!] \Rightarrow [\![q]\!]}}{[\![q]\!]}$$

Kod introdukcije univerzalnog kvantifikatora u odgovarajućem meta-aksiomu doseg kvantifikatora (F) instanciran je na λ-apstrakciju $\lambda x.p(x)$. Prema pretpostavci indukcije postoji dokaz za $[\![p(x)]\!]$. Stoga meta-pravilo $\bigwedge$-introdukcije dokazuje $\bigwedge x.[\![p(x)]\!]$:

$$\dfrac{\dfrac{\bigwedge F.(\bigwedge x.[\![F(x)]\!]) \Rightarrow [\![\forall x F(x)]\!]}{(\bigwedge x.[\![p(x)]\!]) \Rightarrow [\![\forall x p(x)]\!]} \quad \dfrac{\nabla \; [\![p(x)]\!]}{\bigwedge x.[\![p(x)]\!]}}{[\![\forall x p(x)]\!]}$$

Kod eliminacije univerzalnog kvantifikatora u odgovarajućem meta-aksiomu doseg kvantifikatora (F) instanciran je na λ-apstrakciju $\lambda x.p(x)$, a zatim y instanciran za proizvoljnu varijablu t. Prema pretpostavci indukcije postoji dokaz za $[\![\forall x p(x)]\!]$, pa je traženi meta-dokaz:

$$\dfrac{\dfrac{\dfrac{\bigwedge Fy.[\![\forall x F(x)]\!] \Rightarrow [\![F(y)]\!]}{\bigwedge y.[\![\forall x p(x)]\!] \Rightarrow [\![p(y)]\!]} \quad \nabla \; [\![\forall x p(x)]\!]}{[\![\forall x p(x)]\!] \Rightarrow [\![p(t)]\!]} \quad [\![\forall x p(x)]\!]}{[\![p(t)]\!]}$$

□

Teorem 11. *Reprezentacija klasične logike prvog reda u Isabelle je korektna.*

Dokaz. Treba pokazati da za svaki meta-dokaz od $[\![B]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$ postoji odgovarajući dokaz u objektnoj logici. Prema teoriji dokaza (Prawitz, [5]) svaki meta-dokaz može se zapisati u normalnoj formi, koja se sastoji od grana koje se dižu na lijevo i završavaju s aksiomom ili pretpostavkom. Osim toga, na svakoj grani, gledano odogzo prema dolje, nakon aksioma ili pretpostavke slijedi niz pravila eliminacije, a zatim niz pravila introdukcije. Pravilima eliminacije formula se svede na minimum, a introdukcijama opet naraste. Nadalje, svaka se normalna forma dokaza može prevesti u tzv. razvijenu normalnu formu u kojoj je svaka minimalna formula atomarna. Poddokazi imaju isti oblik. Stoga se rekurzivno može prevoditi meta-dokaze u odgovarajuće dokaze u objektnoj logici. Valja primijetiti da je na meta-nivou $[\![B]\!]$ atomarna.
Dokaz indukcijom po veličini razvijenog normalnog meta-dokaza od $[\![B]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$ konstruira objektni dokaz od B iz $A_1, ..., A_m$. Kako je $[\![B]\!]$ atomarna formula, tada zbog normalne forme meta-dokaza u dokazu nema introdukcijskih pravila, pa nema ni otpuštanja pretpostavki pošto je jedino hipotetičko pravilo $\Rightarrow$-introdukcija. U meta-dokazu imamo samo eliminacijska pravila. U slučaju da je dokaz samo $[\![B]\!]$, tada je B pretpostavka, jedna od $A_1, ..., A_m$. Inače, meta-dokaz ima eliminacijska pravila pa prva meta-formula u dokazu nije atomarna. Ona je neki aksiom na koji se primjenjuje eliminacijsko pravilo.
Promotrimo slučajeve prema akisomima.

Za aksiom $\wedge$-introdukcije, B je formula oblika $C \wedge D$. Meta-dokaz ima dvije $\bigwedge$-eliminacije i dvije $\Rightarrow$-eliminacije u kojima nastupaju meta-dokazi od $[\![C]\!]$ i $[\![D]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge AB.[\![A]\!] \Rightarrow ([\![B]\!] \Rightarrow [\![A \wedge B]\!])}{\bigwedge B.[\![C]\!] \Rightarrow ([\![B]\!] \Rightarrow [\![C \wedge B]\!])} \quad \vdots}{[\![C]\!] \Rightarrow ([\![D]\!] \Rightarrow [\![C \wedge D]\!])} \quad [\![C]\!]}{[\![D]\!] \Rightarrow [\![C \wedge D]\!]} \quad \vdots}{[\![C \wedge D]\!]} \quad [\![D]\!]$$

Prema pretpostavci indukcije postoje objektni dokazi za C, odnosno D iz $A_1, ..., A_m$. Primjenimo li na njih objektno pravilo $\wedge$-introdukcije dobivamo objektni dokaz za $C \wedge D$, tj. B iz $A_1, ..., A_m$.
Za aksiom $\rightarrow$-introdukcije, B je formula oblika $C \rightarrow D$. Meta-dokaz ima dvije $\bigwedge$-eliminacije, $\Rightarrow$-eliminaciju i sadrži meta-dokaz od $[\![C]\!] \Rightarrow [\![D]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!], [\![C]\!]$. Prema normalnoj formi, ovaj se dokaz sastoji od dokaza

$[\![D]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!], [\![C]\!]$ i pravila $\Rightarrow$-introdukcije kojim se otpušta pretpostavka $[\![C]\!]$.

$$\dfrac{\dfrac{\dfrac{\bigwedge AB.([\![A]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![A \to B]\!]}{\bigwedge B.([\![C]\!] \Rightarrow [\![B]\!]) \Rightarrow [\![C \to B]\!]}}{([\![C]\!] \Rightarrow [\![D]\!]) \Rightarrow [\![C \to D]\!]} \quad \dfrac{\begin{array}{c}[[\![C]\!]] \\ \vdots \\ [\![D]\!]\end{array}}{[\![C]\!] \Rightarrow [\![D]\!]}}{[\![C \to D]\!]}$$

Prema pretpostavci indukcije, za meta-dokaz od $[\![D]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!], [\![C]\!]$ postoji objektni dokaz od D iz $A_1, ..., A_m, C$. Objektnim pravilom $\to$ -introdukcije otpušta se pretpostavka C pa se dobije objektni dokaz od $C \to D$ iz $A_1, ..., A_m$.

Za aksiom $\forall$-introdukcije, B je formula oblika $\forall x G(x)$. Meta-dokaz ima $\bigwedge$-eliminaciju, $\Rightarrow$-eliminaciju i sadrži meta-dokaz od $\bigwedge x.[\![G(x)]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$ u kojem je zadnje primjenjeno pravilo $\bigwedge$-introdukcija na dokaz od $[\![G(x)]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$.

$$\dfrac{\dfrac{\dfrac{\bigwedge F.(\bigwedge x.[\![F(x)]\!]) \Rightarrow [\![\forall x F(x)]\!]}{(\bigwedge x.[\![G(x)]\!]) \Rightarrow [\![\forall x G(x)]\!]} \quad \dfrac{\begin{array}{c}\vdots \\ [\![G(x)]\!]\end{array}}{\bigwedge x.[\![G(x)]\!]}}{[\![\forall x G(x)]\!]}$$

Prema pretpostavci indukcije, za meta-dokaz od $[\![G(x)]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!]$ postoji objektni dokaz od $G(x)$ iz $A_1, ..., A_m$, gdje varijabla x nije slobodna u pretpostavkama. Objektnim pravilom $\forall$-introdukcije dobije se dokaz od $\forall x G(x)$ iz $A_1, ..., A_m$.

Slično dobijemo objektne dokaze za preostale aksiome.

Za aksiome $\wedge$-eliminacije, pretpostavku indukcije primjenimo na poddokaz od $[\![C \wedge D]\!]$, a dobivenom objektnom dokazu dodamo odgovarajuće pravilo $\wedge$-eliminacije, ovisno o tome radi li se o lijevom ili desnom konjunktu, npr:

$$\dfrac{\dfrac{\dfrac{\bigwedge AB.[\![A \wedge B]\!] \Rightarrow [\![A]\!]}{\bigwedge B.[\![C \wedge B]\!] \Rightarrow [\![C]\!]}}{[\![C \wedge D]\!] \Rightarrow [\![C]\!]} \quad \dfrac{\begin{array}{c}\vdots \\ [\![C \wedge D]\!]\end{array}}{}}{[\![C]\!]}$$

Za aksiom $\to$-eliminacije, pretpostavku indukcije primjenimo na poddokaze od $[\![C \to D]\!]$ i $[\![C]\!]$, a na dobivene objektne dokaze primjenimo pravilo $\to$-eliminacije:

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge AB.[\![A \to B]\!] \Rightarrow [\![A]\!] \Rightarrow [\![B]\!]}{\bigwedge B.[\![C \to B]\!] \Rightarrow [\![C]\!] \Rightarrow [\![B]\!]} \quad \vdots}{[\![C \to D]\!] \Rightarrow [\![C]\!] \Rightarrow [\![D]\!]} \quad [\![C \to D]\!]}{[\![C]\!] \Rightarrow [\![D]\!]} \quad \vdots}{[\![D]\!]} \quad [\![C]\!]$$

Za aksiom $\forall$-eliminacije, pretpostavku indukcije primjenimo na poddokaz od $[\![\forall x G(x)]\!]$, a dobivenom objektnom dokazu dodamo pravilo $\forall$-eliminacije:

$$\dfrac{\dfrac{\dfrac{\bigwedge Fy.[\![\forall x F(x)]\!] \Rightarrow [\![F(y)]\!]}{\bigwedge y.[\![\forall x G(x)]\!] \Rightarrow [\![G(y)]\!]} \quad \vdots}{[\![\forall x G(x)]\!] \Rightarrow [\![G(z)]\!]} \quad [\![\forall x G(x)]\!]}{[\![G(z)]\!]}$$

Za $\bot$-aksiom pretpostavku indukcije primjenimo na poddokaz od $[\![\bot]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!], [\![B \to \bot]\!]$ te na dobiveni objektni dokaz dodamo $\bot$-pravilo. Ovdje meta-logika i objektna logika imaju iste sisteme otpuštanja pretpostavke $[\![B \to \bot]\!]$, odnosno $B \to \bot$.

$$\dfrac{\dfrac{\bigwedge A.([\![A \to \bot]\!] \Rightarrow [\![\bot]\!]) \Rightarrow [\![A]\!]}{([\![B \to \bot]\!] \Rightarrow [\![\bot]\!]) \Rightarrow [\![B]\!]} \quad \dfrac{\dfrac{[[\![B \to \bot]\!]]}{\vdots}}{[\![\bot]\!]}}{[\![B]\!]} \quad [\![B \to \bot]\!] \Rightarrow [\![\bot]\!]$$

Za aksiome $\vee$-introdukcije, pretpostavku indukcije primjenimo na poddokaz od $[\![C]\!]$, a dobivenom objektnom dokazu dodamo pravilo $\vee$-introdukcije za lijevi, odnosno desni alternat, npr:

$$\dfrac{\dfrac{\dfrac{\bigwedge AB.[\![A]\!] \Rightarrow [\![A \vee B]\!]}{\bigwedge B.[\![C]\!] \Rightarrow [\![C \vee B]\!]} \quad \vdots}{[\![C]\!] \Rightarrow [\![C \vee D]\!]} \quad [\![C]\!]}{[\![C \vee D]\!]}$$

Za aksiom $\vee$-eliminacije, pretpostavku indukcije primjenimo na poddokaz od $[\![D \vee E]\!]$, te na poddokaz od $[\![F]\!]$ u kojem se otpušta pretpostavka $[\![D]\!]$ i poddokaz od $[\![F]\!]$ u kojem se otpušta pretpostavka $[\![E]\!]$. Objektni dokazi otpuštaju pretpostavke D, odnosno E. Dobivene objektne dokaze spojimo

pravilom $\vee$-eliminacije.

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge ABC.[\![A \vee B]\!] \Rightarrow ([\![A]\!] \Rightarrow [\![C]\!]) \Rightarrow ([\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]}{\bigwedge BC.[\![D \vee B]\!] \Rightarrow ([\![D]\!] \Rightarrow [\![C]\!]) \Rightarrow ([\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]} \quad \begin{matrix}[[\![D]\!]] \\ \vdots \\ [\![F]\!]\end{matrix}}{\bigwedge C.[\![D \vee E]\!] \Rightarrow ([\![D]\!] \Rightarrow [\![C]\!]) \Rightarrow ([\![E]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]} \quad \begin{matrix}\vdots \\ [\![D]\!] \Rightarrow [\![F]\!]\end{matrix} \quad \begin{matrix}[[\![E]\!]] \\ \vdots \\ [\![F]\!]\end{matrix}}{[\![D \vee E]\!] \Rightarrow ([\![D]\!] \Rightarrow [\![F]\!]) \Rightarrow ([\![E]\!] \Rightarrow [\![F]\!]) \Rightarrow [\![F]\!]} \quad [\![D \vee E]\!] \qquad [\![E]\!] \Rightarrow [\![F]\!]}{([\![D]\!] \Rightarrow [\![F]\!]) \Rightarrow ([\![E]\!] \Rightarrow [\![F]\!]) \Rightarrow [\![F]\!]}}{([\![E]\!] \Rightarrow [\![F]\!]) \Rightarrow [\![F]\!]}}{[\![F]\!]}$$

Za aksiom $\exists$-introdukcije, pretpostavku indukcije primjenimo na poddokaz od $[\![G(z)]\!]$, a dobivenom objektnom dokazu dodamo pravilo $\exists$-introdukcije:

$$\dfrac{\dfrac{\dfrac{\bigwedge Fy.[\![F(y)]\!] \Rightarrow [\![\exists x F(x)]\!]}{\bigwedge y.[\![G(y)]\!] \Rightarrow [\![\exists x G(x)]\!]} \quad \vdots}{[\![G(z)]\!] \Rightarrow [\![\exists x G(x)]\!]} \quad [\![G(z)]\!]}{[\![\exists x G(x)]\!]}$$

Za aksiom $\exists$-eliminacije, prema normalnoj formi, imamo poddokaz od $\bigwedge x.[\![G(x)]\!] \Rightarrow [\![R]\!]$, koji se sastoji od dokaza $[\![R]\!]$ iz $[\![A_1]\!], ..., [\![A_m]\!], [\![G(x)]\!]$ nakon kojeg slijedi $\Rightarrow$-introdukcija kojom se otpušta pretpostavka $[\![G(x)]\!]$, a zatim $\bigwedge$-introdukcija. Pretpostavku indukcije primjenimo na poddokaz $[\![R]\!]$ i poddokaz od $[\![\exists x G(x)]\!]$. Objektno pravilo $\exists$-eliminacije daje traženi dokaz. Meta i objektni dokazi otpuštaju pretpostavku $[\![G(x)]\!]$, odnosno $G(x)$:

$$\dfrac{\dfrac{\dfrac{\bigwedge FQ.[\![\exists x F(x)]\!] \Rightarrow (\bigwedge x.[\![F(x)]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![Q]\!]}{\bigwedge Q.[\![\exists x G(x)]\!] \Rightarrow (\bigwedge x.[\![G(x)]\!] \Rightarrow [\![Q]\!]) \Rightarrow [\![Q]\!]} \quad \vdots}{[\![\exists x G(x)]\!] \Rightarrow (\bigwedge x.[\![G(x)]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]} \quad [\![\exists x G(x)]\!] \qquad \dfrac{\begin{matrix}[[\![G(x)]\!]] \\ \vdots \\ [\![R]\!]\end{matrix}}{[\![G(x)]\!] \Rightarrow [\![R]\!]}}{(\bigwedge x.[\![G(x)]\!] \Rightarrow [\![R]\!]) \Rightarrow [\![R]\!]} \qquad \bigwedge x.[\![G(x)]\!] \Rightarrow [\![R]\!]}{[\![R]\!]}$$

$\square$

9 Formalizacija dokaza "unatrag"

Za svaki logički simbol postoje dvije vrste pravila, pravilo introdukcije i pravilo eliminacije. Introdukcijskim pravilima omogućuje se uvođenje simbola u konkluziju. Eliminacijskim pravilima izvodimo posljedice iz simbola.
Svaki se korak u dokazivanju prirodnom dedukcijom svodi na uočavanje logičkog simbola koji u formuli zadnji djeluje i primjene odgovarajućeg pravila. Tako se prema pravilu kreiraju novi podciljevi, sastavljeni od potformula.

Dokazivati unaprijed znači izvoditi nove činjenice iz već poznatih. Posebno se to aplicira pri zaključivanju od općenitog prema specifičnom. Zamjena vrijednosti za varijable (instanciranje) također je dokazivanje prema naprijed.

U Isabelle većinom dokazujemo unatrag. Kod dokazivanja unatrag introdukcijskim pravilom za neki simbol, konkluzija je formula koja sadrži taj simbol. Primjenom pravila taj se simbol gubi. Kod eliminacijskih pravila potrebno je obrnuto; dokaz formule svesti na dokaz nove formule koja sadrži dotični simbol.
Dokazivanje konstrukcijom dokaza "unatrag" kreće od korijena stabla, formule koju treba dokazati, i raste prema gore.
Da bi dokazali cilj Φ, tako da dokaz svedemo na dokaze podciljeva $\Phi_1, ..., \Phi_m$, moramo izvesti pravilo:

$$\frac{\Phi_1, ..., \Phi_m}{\Phi} \quad .$$

U meta-logici to se objektno pravilo reprezenitira implikacijom:

$$[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!] \ .$$

Osim pravila izvođenja ovakve meta-formule mogu predstavljati i stanja u dokazu. Stanje dokaza može se tako predstaviti izvedenim pravilom čija je konkluzija glavni cilj, a premise trenutni podciljevi. Inicijalno stanje dokaza predstavlja se trivijalnim pravilom čija su premisa i konkluzija jednake. Stanje dokaza koje nema podciljeva je meta-teorem. To je završno stanje. Jednako je samom cilju, formuli koja je dokazana.

9.1 Rezolucija

Meta-formule koje predstavljaju stanja dokaza i pravila izvođenja kombiniraju se izvedenim meta-pravilom: rezolucijom. Većina metoda u Isabelle koristi rezoluciju.

Rezolucija ima dvije premise. Prva je pravilo izvođenja, druga stanje dokaza, a konkluzija novo stanje dokaza:

$$\frac{\text{pravilo izvođenja} \qquad \text{stanje dokaza}}{\text{novo stanje dokaza}}$$

Rezolucija instancira slobodne varijable iz pravila izvođenja unifikacijom s podciljem iz stanja dokaza. Slobodne varijable iz pravila izvođenja moraju se razlikovati od slobodnih varijabli stanja dokaza. Varijable se preimenuju indeksiranjem.

Pravilo rezolucije:

Ako supstitucija s za neki i daje $\Phi s \equiv \Psi_i$, tada rezolucija u novom stanju dokaza zamijeni podcilj Ψ_i sa $\Phi_1 s, ..., \Phi_m s$:

$$\frac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!] \qquad [\![\Psi_1, ..., \Psi_i, ..., \Psi_n]\!] \Rightarrow [\![\Theta]\!]}{[\![\Psi_1, ..., \Phi_1 s, ..., \Phi_m s, ..., \Psi_n]\!] \Rightarrow [\![\Theta]\!]}$$

Propozicija 6. *Pravilo rezolucije korektno je meta-pravilo.*

Dokaz. Pravilo rezolucije izvodljivo je meta-pravilima za ekvivalenciju, pravilima $\Rightarrow$-eliminacije i $\Rightarrow$-introdukcije:

$$\dfrac{\dfrac{[\![\Psi_1, ..., \Psi_i, ..., \Psi_n]\!] \Rightarrow [\![\Theta]\!] \qquad \dfrac{[\![\Phi s]\!] \equiv [\![\Psi_i]\!] \qquad \dfrac{\dfrac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!]}{[\![\Phi_1 s, ..., \Phi_m s]\!] \Rightarrow [\![\Phi s]\!]} \quad [[\![\Psi_1, ..., \Phi_1 s, ..., \Phi_m s, ..., \Psi_n]\!]]}{[\![\Psi_1, ..., \Phi s, ..., \Psi_n]\!]}}{[\![\Psi_1, ..., \Psi_i, ..., \Psi_n]\!]}}{[\![\Theta]\!]}}{[\![\Psi_1, ..., \Phi_1 s, ..., \Phi_m s, ..., \Psi_n]\!] \Rightarrow [\![\Theta]\!]}$$

Supstitucija je,zapravo, instanciranje varijabli pravilom za kvanitfikator:

$$\frac{[\![\Phi]\!]}{[\![\Phi[a_1/x_1, ..., a_k/x_k]]\!]}$$

Varijable $x_1, ..., x_k$ su varijable koje nisu slobodne u pretpostavkama. Pravilom $\Rightarrow$-introdukcije otpušta se pretpostavka $[\![\Psi_1, ..., \Phi_1 s, ..., \Phi_m s, ..., \Psi_n]\!]$. Preostale pretpostavke u dokazu su premise pravila rezolucije te ekvivalencija koju zadovoljava supstitucija s. Stoga je pravilo rezolucije korektno. □

9.2 Novo pravilo ∧-eliminacije

Pravila ∧-eliminacije su pravila koja jasno djeluju u dokazima unaprijed, npr. iz $A \wedge B$ zaključujemo A. U dokazivanju unatrag teško ih je koristiti. Ako imamo A, teško je odrediti povoljnu konjunkciju iz koje smo zaključili A. Ova nova verzija pravila ∧-eliminacije pogodnija je za dokazivanje unatrag, a podsjeća na pravilo ∨-eliminacije. Ona koristi pomoćnu tvrdnju C i otpušta pretpostavke A i B u drugoj premisi:

$$\frac{A \wedge B \qquad \begin{array}{c}[A, B]\\ \vdots \\ C\end{array}}{C}$$

Formalizacija meta-teoremom glasi:

$$\bigwedge ABC.[\![A \wedge B]\!] \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]$$

Propozicija 7. $\bigwedge ABC.[\![A \wedge B]\!] \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]$ *je meta-teorem.*

Dokaz. Dokažimo najprije $[\![C]\!]$ iz pretpostavki $[\![A \wedge B]\!]$ i $[\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]$. Rezolucija s drugom pretpostavkom daje:

$$\frac{[\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!] \qquad [\![C]\!] \Rightarrow [\![C]\!]}{[\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]}$$

Potrebna instanca aksioma ∧-eliminacije rezolucijom daje:

$$\frac{[\![A \wedge B]\!] \Rightarrow [\![A]\!] \qquad [\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]}{[\![A \wedge B]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]}$$

Rezolucija s prvom pretpostavkom daje:

$$\frac{[\![A \wedge B]\!] \qquad [\![A \wedge B]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]}{[\![B]\!] \Rightarrow [\![C]\!]}$$

Sada nam je potrebna instanca drugog aksioma ∧-eliminacije za rezoluciju:

$$\frac{[\![A \wedge B]\!] \Rightarrow [\![B]\!] \qquad [\![B]\!] \Rightarrow [\![C]\!]}{[\![A \wedge B]\!] \Rightarrow [\![C]\!]}$$

Konačno, rezolucija s prvom pretpostavkom daje:

$$\frac{[\![A \wedge B]\!] \qquad [\![A \wedge B]\!] \Rightarrow [\![C]\!]}{[\![C]\!]}$$

Konstruirali smo dokaz od $[\![C]\!]$ iz pretpostavki $[\![A \wedge B]\!]$ i $[\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]$. Sada pravilom $\Rightarrow$-introdukcije otpustimo ove pretpostavke te generalizacija daje traženi meta-teorem. □

9.3 $\Rightarrow$ - podizanje

Još jedno korisno izvedeno meta-pravilo je $\Rightarrow$-podizanje (lifting) pravilo ili podizanje pravila $[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!]$ preko niza pretpostavki Θ.
Tim se pravilom formalizira postavljanje pretpostavki na meta-nivou.

$\Rightarrow$-podizanje:

$$\frac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!]}{[\![\Theta \Rightarrow \Phi_1, ..., \Theta \Rightarrow \Phi_m]\!] \Rightarrow (\Theta \Rightarrow \Phi)}$$

Propozicija 8. *$\Rightarrow$-podizanje pravilo korektno je meta-pravilo.*

Dokaz. $\Rightarrow$-podizanje je izvedivo meta-pravilima $\Rightarrow$-eliminacije i $\Rightarrow$-introdukcije:

$$\dfrac{\dfrac{\dfrac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!] \qquad \dfrac{[[\![\Theta \Rightarrow \Phi_1, ..., \Theta \Rightarrow \Phi_m]\!]] \quad [[\![\Theta]\!]]}{[\![\Phi_1, ..., \Phi_m]\!]}}{[\![\Phi]\!]}}{[\![\Theta]\!] \Rightarrow [\![\Phi]\!]}}{[\![\Theta \Rightarrow \Phi_1, ..., \Theta \Rightarrow \Phi_m]\!] \Rightarrow ([\![\Theta]\!] \Rightarrow [\![\Phi]\!])}$$

Najgornje desno pravilo je ustvari kraći zapis više $\Rightarrow$-eliminacija s istom premisom Θ. Pravilima $\Rightarrow$-introdukcije otpuštaju se pretpostavke
$[\![\Theta \Rightarrow \Phi_1, ..., \Theta \Rightarrow \Phi_m]\!]$ i $[\![\Theta]\!]$. □

Primjer 1. *Dokaz teorema: $A \wedge B \rightarrow (C \rightarrow A \wedge C)$*

U sustavu prirodne dedukcije dokaz izgleda ovako:

$$\dfrac{\dfrac{\dfrac{\dfrac{[A \wedge B]}{A} \quad [C]}{A \wedge C}}{C \to A \wedge C}}{A \wedge B \to (C \to A \wedge C)}$$

Meta-dokaz unatrag kreće od početnog stanja u kojem su premisa i konkluzija jednaki zadanoj formuli. Za prvu rezoluciju potreban je aksiom $\to$-introdukcije, točnije njegova instanca koju dobijemo dvjema $\bigwedge$-eliminacijama.

$$\dfrac{(\llbracket A_1 \rrbracket \Rightarrow \llbracket B_1 \rrbracket) \Rightarrow \llbracket A_1 \to B_1 \rrbracket \qquad \llbracket A \wedge B \to (C \to A \wedge C) \rrbracket \Rightarrow \llbracket A \wedge B \to (C \to A \wedge C) \rrbracket}{(\llbracket A \wedge B \rrbracket \Rightarrow \llbracket C \to A \wedge C \rrbracket) \Rightarrow \llbracket A \wedge B \to (C \to A \wedge C) \rrbracket}$$

Rezolucija instancira A_1 u $A \wedge B$, a B_1 u $C \to A \wedge C$.
Radi kraćeg zapisa, označimo $\llbracket A \wedge B \to (C \to A \wedge C) \rrbracket$ s Ψ.
Sada treba dokazati $\llbracket C \to A \wedge C \rrbracket$ iz $\llbracket A \wedge B \rrbracket$.
Podizanje aksioma $\to$ - introdukcije preko pretpostavke $\llbracket A \wedge B \rrbracket$:

$$\dfrac{(\llbracket A_2 \rrbracket \Rightarrow \llbracket B_2 \rrbracket) \Rightarrow \llbracket A_2 \to B_2 \rrbracket}{(\llbracket A \wedge B \rrbracket \Rightarrow (\llbracket A_2 \rrbracket \Rightarrow \llbracket B_2 \rrbracket)) \Rightarrow (\llbracket A \wedge B \rrbracket \Rightarrow \llbracket A_2 \to B_2 \rrbracket)}$$

daje meta-teorem $(\llbracket A \wedge B \rrbracket \Rightarrow (\llbracket A_2 \rrbracket \Rightarrow \llbracket B_2 \rrbracket)) \Rightarrow (\llbracket A \wedge B \rrbracket \Rightarrow \llbracket A_2 \to B_2 \rrbracket)$ potreban za sljedeću rezoluciju.

$$\dfrac{(\llbracket A \wedge B \rrbracket \Rightarrow (\llbracket A_2 \rrbracket \Rightarrow \llbracket B_2 \rrbracket)) \Rightarrow (\llbracket A \wedge B \rrbracket \Rightarrow \llbracket A_2 \to B_2 \rrbracket) \quad (\llbracket A \wedge B \rrbracket \Rightarrow \llbracket C \to A \wedge C \rrbracket) \Rightarrow \Psi}{(\llbracket A \wedge B \rrbracket \Rightarrow (\llbracket C \rrbracket \Rightarrow \llbracket A \wedge C \rrbracket)) \Rightarrow \Psi}$$

Rezolucija instancira A_2 u C, a B_2 u $A \wedge C$. Za sljedeću rezoluciju ponovno je prethodno potrebano izvesti $\Rightarrow$ - podizanje, i to instance aksioma $\wedge$ - introdukcije preko pretpostavki $\Phi = [\llbracket A \wedge B \rrbracket, \llbracket C \rrbracket]$:

$$\dfrac{\llbracket A_3 \rrbracket \Rightarrow \llbracket B_3 \rrbracket \Rightarrow \llbracket A_3 \wedge B_3 \rrbracket}{(\Phi \Rightarrow \llbracket A_3 \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket B_3 \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket A_3 \wedge B_3 \rrbracket)}$$

Rezolucija instancira A_3 u A, a B_3 u C:

$$\dfrac{(\Phi \Rightarrow \llbracket A_3 \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket B_3 \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket A_3 \wedge B_3 \rrbracket) \qquad (\Phi \Rightarrow \llbracket A \wedge C \rrbracket) \Rightarrow \Psi}{((\Phi \Rightarrow \llbracket A \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket C \rrbracket)) \Rightarrow \Psi}$$

Sada se dokaz zapravo sveo na dva poddokaza, dokaz $\Phi \Rightarrow \llbracket A \rrbracket$ i dokaz $\Phi \Rightarrow \llbracket C \rrbracket$. Drugi od njih dokazuje se metodom "by assumption" (vidi 10.2), što se formalno izvodi rezolucijom s meta-tautologijom $\Phi \Rightarrow \llbracket C \rrbracket$, bez podizanja:

$$\dfrac{\Phi \Rightarrow \llbracket C \rrbracket \qquad ((\Phi \Rightarrow \llbracket A \rrbracket) \Rightarrow (\Phi \Rightarrow \llbracket C \rrbracket)) \Rightarrow \Psi}{(\Phi \Rightarrow \llbracket A \rrbracket) \Rightarrow \Psi}$$

Sljedeći je korak rezolucija s aksiomom $\wedge$-eliminacije kojom dokaz od $[\![A]\!]$ svodimo na dokaz od $[\![A \wedge B]\!]$. Ponovo je potrebno najprije izvesti podizanje:

$$\frac{[\![A_4 \wedge B_4]\!] \Rightarrow [\![A_4]\!]}{(\Phi \Rightarrow [\![A_4 \wedge B_4]\!]) \Rightarrow (\Phi \Rightarrow [\![A_4]\!])}$$

pa rezolucija instancira A_4 u A:

$$\frac{(\Phi \Rightarrow [\![A_4 \wedge B_4]\!]) \Rightarrow (\Phi \Rightarrow [\![A_4]\!]) \quad (\Phi \Rightarrow [\![A]\!]) \Rightarrow \Psi}{(\Phi \Rightarrow [\![A \wedge B_4]\!]) \Rightarrow \Psi}$$

Kako se unatrag ne može instancirati varijabla B_4 u varijablu B, potrebno je uzeti tu instancu aksioma $\wedge$-eliminacije za rezoluciju:

$$\frac{(\Phi \Rightarrow [\![A \wedge B]\!]) \Rightarrow (\Phi \Rightarrow [\![A]\!]) \qquad (\Phi \Rightarrow [\![A]\!]) \Rightarrow \Psi}{(\Phi \Rightarrow [\![A \wedge B]\!]) \Rightarrow \Psi}$$

Završimo dokaz "by assumption", odnosno rezolucijom s meta-tautologijom:

$$\frac{\Phi \Rightarrow [\![A \wedge B]\!] \qquad (\Phi \Rightarrow [\![A \wedge B]\!]) \Rightarrow \Psi}{\Psi}$$

Ova formalizacija objektnog dokaza valjana je za proizvoljne objektne formule A, B i C. To se može izraziti generalizacijom od Ψ po slobodnim varijablama, što daje konačni meta-teorem:

$$\bigwedge ABC.[\![A \wedge B \to (C \to A \wedge C)]\!]$$

Rezolucija s unifikacijom može instancirati varijable u dokazima. Međutim, ovdje je zgodno koristiti i izvedeno pravilo $\wedge$-eliminacije koje bolje prati intuiciju dokazivanja unatrag. Na problem s instanciranjem varijable B_4 naišli smo za stanje dokaza $(\Phi \Rightarrow [\![A]\!]) \Rightarrow \Psi$. Izvedeni aksiom $\wedge$-eliminacije $\bigwedge ABC.[\![A \wedge B]\!] \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![C]\!]) \Rightarrow [\![C]\!]$ instanciramo te nakon podizanja preko pretpostavki Φ primjenimo rezoluciju:

$$\frac{(\Phi \Rightarrow [\![A_5 \wedge B_5]\!]) \Rightarrow (\Phi \Rightarrow ([\![A_5]\!] \Rightarrow [\![B_5]\!] \Rightarrow [\![C_5]\!])) \Rightarrow (\Phi \Rightarrow [\![C_5]\!]) \quad (\Phi \Rightarrow [\![A]\!]) \Rightarrow \Psi}{(\Phi \Rightarrow [\![A_5 \wedge B_5]\!]) \Rightarrow (\Phi \Rightarrow ([\![A_5]\!] \Rightarrow [\![B_5]\!] \Rightarrow [\![A]\!])) \Rightarrow \Psi}$$

Ova rezolucija instancira samo C_5 u A. Sljedeća rezolucija s meta-tautologijom instancira A_5 u A i B_5 u B:

$$\frac{\Phi \Rightarrow [\![A \wedge B]\!] \quad (\Phi \Rightarrow [\![A_5 \wedge B_5]\!]) \Rightarrow (\Phi \Rightarrow ([\![A_5]\!] \Rightarrow [\![B_5]\!] \Rightarrow [\![A]\!])) \Rightarrow \Psi}{(\Phi \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![A]\!])) \Rightarrow \Psi}$$

Kako je $[\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![A]\!]$ meta-tautologija, i $\Phi \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![A]\!])$ je meta-tautologija pa rezolucija dokazuje Ψ:

$$\frac{\Phi \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![A]\!]) \qquad (\Phi \Rightarrow ([\![A]\!] \Rightarrow [\![B]\!] \Rightarrow [\![A]\!])) \Rightarrow \Psi}{\Psi}$$

9.4 $\bigwedge$ - podizanje

Rezolucija s ciljevima u kojima se javlja kvantifikacija zahtjeva novo pravilo, dizanje pravila izvođenja preko kvantificirane varijable.
To se pravilo naziva $\bigwedge$-podizanje.
$\bigwedge$-podizanje za dano pravilo izvođenja varijable vezane vanjskim kvantifikatorima zamjenuje novim varijablama funkcijskog tipa.

$\bigwedge$-podizanje

$$\frac{\bigwedge y.\Psi}{\bigwedge z.\Psi[f(z)/y]}$$

Kvantificirana varijabla y tipa τ zamijenjena je varijablom f funkcijskog tipa $\sigma \to \tau$, gdje je σ tip varijable z.

Propozicija 9. *Pravilo $\bigwedge$-podizanje korektno je meta-pravilo.*

Dokaz. Očito je ovo pravilo izvođenja korektno, što pokazuje sljedeći kratki izvod u kojem se primjenjuje $\bigwedge$-eliminacija i $\bigwedge$-introdukcija.

$$\frac{\dfrac{\bigwedge y.\Psi}{\Psi[f(z)/y]}}{\bigwedge z.\Psi[f(z)/y]}$$

□

Ovo se pravilo izvođenja, primjenom uzastopnih $\bigwedge$-eliminacija i $\bigwedge$-introdukcija, može poopćiti na slučaj s k kvantificiranih varijabli:

$$\frac{\bigwedge y_1 ... y_k.\Psi}{\bigwedge z.\Psi[f_1(z)/y_1, ..., f_k(z)/y_k]}$$

Tipično, Ψ je implikacija $\Phi \Rightarrow \Psi'$ pa pravilo $\bigwedge$-podizanje poprima oblik:

$$\frac{\bigwedge y.\Phi \Rightarrow \Psi'}{\bigwedge z.\Phi \Rightarrow \bigwedge z.\Psi'}$$

Propozicija 10. *Pravilo $\bigwedge$-podizanje za implikaciju $\Phi \Rightarrow \Psi'$:*

$$\frac{\bigwedge y.\Phi \Rightarrow \Psi'}{\bigwedge z.\Phi[f(z)/y] \Rightarrow \bigwedge z.\Psi'[f(z)/y]}$$

korektno je meta-pravilo.

Dokaz. U dokazu koristit ćemo još jedno izvedeno pravilo čiju ćemo korektnost najprije pokazati, a to je pravilo:

$$\frac{\bigwedge z.\Phi \Rightarrow \Psi' \quad \bigwedge z.\Phi}{\bigwedge z.\Psi'}$$

Izvod koristi $\bigwedge$-eliminaciju, $\Rightarrow$-eliminaciju, te $\bigwedge$-introdukciju:

$$\dfrac{\dfrac{\bigwedge z.\Phi \Rightarrow \Psi' \qquad \dfrac{\bigwedge z.\Phi}{\Phi(w/z)}}{\Phi(w/z) \Rightarrow \Psi'(w/z)} \qquad}{\dfrac{\Psi'(w/z)}{\bigwedge z.\Psi'}}$$

Za izvod pravila $\bigwedge$-podizanja za implikaciju $\Phi \Rightarrow \Psi'$, pretpostavimo $\bigwedge z.\Phi$. Koristeći pretpostavku $\bigwedge z.\Phi \Rightarrow \Psi'$ i upravo dokazano pravilo možemo zaključiti $\bigwedge z.\Psi'$. Pravilom $\Rightarrow$-introdukcije otpustimo pretpostavku $\bigwedge z.\Phi$, pa imamo traženi dokaz:

$$\dfrac{\dfrac{\bigwedge z.\Phi \Rightarrow \Psi' \quad [\bigwedge z.\Phi]}{\bigwedge z.\Psi'}}{\bigwedge z.\Phi \Rightarrow \bigwedge z.\Psi'}$$

□

Uzastopno $\bigwedge$-podizanje preko varijabli $z_n, .., z_1$ omogućuje rezoluciju s ciljem oblika $\bigwedge z_n, .., z_1.\Theta$.

Primjer 2. *Izvod* $\forall z.G(z) \vee H(z)$ *iz* $\forall z.G(z)$

Izvod u sustavu prirodne dedukcije je:

$$\dfrac{\dfrac{\dfrac{\forall z.G(z)}{G(z)}}{G(z) \vee H(z)}}{\forall z.G(z) \vee H(z)}$$

Formalizirajmo ovaj izvod, odnosno dokažimo:

$$[\![\forall z.G(z)]\!] \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]$$

Dokaz unatrag kreće od početnog stanja, rezolucijom s aksiomom $\forall$-introducije:

$$\frac{(\bigwedge z.[\![F_1(z)]\!]) \Rightarrow [\![\forall z.F_1(z)]\!] \qquad [\![\forall z.G(z) \vee H(z)]\!] \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]}{(\bigwedge z.[\![G(z) \vee H(z)]\!]) \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]}$$

Rezolucija funkcijsku varijablu F_1 instancira u funkciju $\lambda z.G(z) \vee H(z)$. U sljedećem koraku koristimo metateorem dobiven $\bigwedge$-podizanjem. Istanca $[\![G(y)]\!] \Rightarrow [\![G(y) \vee H(y)]\!]$ aksioma $\vee$-introdukcije $\bigwedge AB.[\![A]\!] \Rightarrow [\![A \vee B]\!]$ vrijedi za sve y, G, H pa vrijedi $\bigwedge y.[\![G(y)]\!] \Rightarrow [\![G(y) \vee H(y)]\!]$.
$\bigwedge$-podizanje nad tim pravilom daje $\bigwedge z.[\![G(z)]\!] \Rightarrow \bigwedge z.[\![G(z) \vee H(z)]\!]$, a generalizacija potreban metateorem $\bigwedge GH.(\bigwedge z.[\![G(z)]\!]) \Rightarrow (\bigwedge z.[\![G(z) \vee H(z)]\!])$.
Rezolucija instancira G_2 u G, a H_2 u H, a novi podcilj postaje $\bigwedge z.[\![G(z)]\!]$:

$$\frac{\bigwedge z.[\![G_2(z)]\!] \Rightarrow \bigwedge z.[\![G_2(z) \vee H_2(z)]\!] \qquad (\bigwedge z.[\![G(z) \vee H(z)]\!]) \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]}{(\bigwedge z.[\![G(z)]\!]) \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]}$$

Sljedeći je korak $\forall$-eliminacija, no nju nije moguće jednostavno koristiti unatrag. Konkluzija je oblika $A[t/x]$, pa je unifikacija višeg reda s termom $F(y)$, gdje su F i y varijable, moguća na više načina.
Stoga, zaključivanje provodimo unaprijed.
Pretpostavimo $[\![\forall z.G(z)]\!]$. Rezolucija s aksiomom $\forall$-eliminacije daje $\bigwedge y.[\![G(y)]\!]$ (varijabla F instancirana je u G), a $\bigwedge$-podizanje po z $\bigwedge f. \bigwedge z.[\![G(f(z))]\!]$:

$$\frac{\dfrac{\bigwedge Fy.[\![\forall x F(x)]\!] \Rightarrow [\![F(y)]\!] \qquad [\![\forall z.G(z)]\!]}{\bigwedge y.[\![G(y)]\!]}}{\bigwedge f. \bigwedge z.[\![G(f(z))]\!]}$$

Konačno, rezolucija instacira f_3 u $\lambda z.z$, pa imamo:

$$\frac{\bigwedge z.[\![G(f_3(z))]\!] \qquad (\bigwedge z.[\![G(z)]\!]) \Rightarrow [\![\forall z.G(z) \vee H(z)]\!]}{[\![\forall z.G(z) \vee H(z)]\!]}$$

9.5 Unifikacija

Unifikacija je proces izjednačavanja dvaju terama. Unificirati dva izraza t i u znači riješiti jednadžbu $t = u$ instanciranjem njihovih varijabli. Algoritam unifikacije daje najopćenitiji unifikator dvaju izraza, ako on postoji, ili pak izvještava da unifikator ne postoji.

Isabelle koristi unifikaciju višeg reda. Svodi se na rješavanje jednadžbi u tipiziranom λ-računu λ-konverzijom.
Unifikacija višeg reda je rekurzivno prebrojiva: ako je izraze nemoguće unificirati, postupak traženja unifikatora može divergirati.

Unifikacija je od velike pomoći kod rezoniranja o kvantifikaciji. Njome se instanciraju nepoznanice u ciljevima.

Želimo li npr. dokazati $\forall x.P(x) \vee Q(x)$, možemo promatrati po slučajevima vrijedi li $P(a) \vee Q(a)$, gdje a ostaje nespecificirano. Svi ti slučajevi sadrže nepoznanice: terme koje treba specificirati kako bi završili dokaz.

Kao što smo već vidjeli na prethodnim primjerima instancijacija varijabli jednostavno se provodi rezolucijom. Pravilo rezolucije može se proširiti tako da instancira obje premise, i pravilo izvođenja i stanje u dokazu. Primjenjuje se kad supstitucija s unificira Φ i Ψ.
Rezolucija unifikacijom može djelovati na varijable bilo gdje u stanju dokaza: Ψ postaje Ψs, a Θ postaje Θs.

Propozicija 11. *Rezolucija unifikacijom:*

$$\frac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!] \qquad [\![\Psi_1, ..., \Psi_n]\!] \Rightarrow [\![\Psi]\!] \Rightarrow [\![\Theta]\!]}{[\![\Psi_1 s, ..., \Psi_n s]\!] \Rightarrow [\![\Phi_1 s, ..., \Phi_m]\!] \Rightarrow [\![\Theta s]\!]}$$

gdje supstitucija s zadovoljava $\Phi s \equiv \Psi s$, korektno je meta-pravilo.

Dokaz. Pravilo rezolucije unifikacijom izvedivo je meta-pravilima za ekvivalenciju, supstitucijom, te pravilima $\Rightarrow$-eliminacije i $\Rightarrow$-introdukcije. Stablo izvoda je:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\![\Phi_1, ..., \Phi_m]\!] \Rightarrow [\![\Phi]\!]}{[\![\Phi_1 s, ..., \Phi_m s]\!] \Rightarrow [\![\Phi s]\!]} \quad [[\![\Phi_1 s, ..., \Phi_m s]\!]]}{[\![\Phi s]\!]} \quad [\![\Phi \equiv \Psi s]\!]}{[\![\Psi s]\!]} \qquad [\![\Psi_1, ..., \Psi_n]\!] \Rightarrow [\![\Psi]\!] \Rightarrow [\![\Theta]\!]}{[\![\Psi_1 s, ..., \Psi_n s]\!] \Rightarrow [\![\Psi s]\!]} \quad [\![\Psi_1 s, ..., \Psi_n s]\!] \Rightarrow [\![\Psi s]\!] \Rightarrow [\![\Theta s]\!]}{[\![\Theta s]\!]}}{[\![\Phi_1 s, ..., \Phi_m]\!] \Rightarrow [\![\Theta s]\!]}}{[\![\Psi_1 s, ..., \Psi_n s]\!] \Rightarrow [\![\Phi_1 s, ..., \Phi_m]\!] \Rightarrow [\![\Theta s]\!]}$$

□

Kako unifikacija određuje instance varijabli, promotrit ćemo na primjeru uspješnog i neuspješnog dokaza.

Primjer 3. *Dokaz teorema* $\forall x \exists y.x \equiv y$

U sustavu prirodne dedukcije dokaz izgleda ovako:

$$\dfrac{\dfrac{x \equiv x}{\exists y.x \equiv y}}{\forall x \exists y.x \equiv y}$$

Meta-dokaz unatrag u prvoj rezoluciji koristi aksiom $\forall$-introdukcije, a F_1 instancira se u $\lambda x.\exists y.x \equiv y$:

$$\frac{(\bigwedge x.[\![F_1(x)]\!]) \Rightarrow [\![\forall x.F_1(x)]\!] \qquad [\![\forall x \exists y.x \equiv y]\!] \Rightarrow [\![\forall x \exists y.x \equiv y]\!]}{(\bigwedge x.[\![\exists y.x \equiv y]\!]) \Rightarrow [\![\forall x \exists y.x \equiv y]\!]}$$

Aksiom $\exists$-introdukcije ima kvantificirane dvije varijable, F i y_1. $\bigwedge$-podizanje po x nad tim aksiomom daje nove funkcijske varijable G i f:

$$\frac{\bigwedge F y_1.[\![F(y_1)]\!] \Rightarrow [\![\exists y.F(y)]\!]}{\bigwedge G f.(\bigwedge x.[\![G(x, f(x))]\!]) \Rightarrow (\bigwedge x.[\![\exists y.G(x, y)]\!])}$$

Dobiveni meta-teorem rezolucijom instancira G_2 u $\lambda x y.x \equiv y$:

$$\frac{(\bigwedge x.[\![G_2(x, f_2(x))]\!]) \Rightarrow (\bigwedge x.[\![\exists y.G_2(x, y)]\!]) \qquad (\bigwedge x.[\![\exists y.x \equiv y]\!]) \Rightarrow [\![\forall x \exists y.x \equiv y]\!]}{(\bigwedge x.[\![x \equiv f_2(x)]\!]) \Rightarrow [\![\forall x \exists y.x \equiv y]\!]}$$

Primjenimo li $\bigwedge$-podizanje po x na aksiom refleksivnosti za relaciju ekvivalencije $\bigwedge y.y \equiv y$, dobijemo metateorem $\bigwedge x.[\![g_3(x) \equiv g_3(x)]\!]$, pa je rezolucijom:

$$\frac{\bigwedge x.[\![g_3(x) \equiv g_3(x)]\!] \qquad (\bigwedge x.[\![x \equiv f_2(x)]\!]) \Rightarrow [\![\forall x \exists y.x \equiv y]\!]}{[\![\forall x \exists y.x \equiv y]\!]}$$

Za unifikaciju u ovom je slučaju polazni par koji treba unificirati:

$$\langle \bigwedge x.[\![g_3(x) \equiv g_3(x)]\!], \bigwedge x.[\![x \equiv f_2(x)]\!] \rangle$$

Izjednačujući terme s lijeve i desne strane ekvivalencije on se svodi na parove

$$\langle \lambda x.g_3(x), \lambda x.x \rangle \qquad \text{i} \qquad \langle \lambda x.g_3(x), \lambda x.f_2(x) \rangle$$

Prvi par nužno zahtjeva da g_3 bude funkcija $\lambda x.x$, a drugi par da f_2 bude funkcija $\lambda x.x$. To je unifikator. Zajednička instanca je $\bigwedge x.[\![x \equiv x]\!]$.

Primjer 4. *Neuspjeli dokaz* $\quad \exists y \forall x.x \equiv y$

Pokušaj dokaza u sustavu prirodne dedukcije izgleda ovako:

$$\frac{\dfrac{x \equiv t}{\forall x.x \equiv t}}{\exists y \forall x.x \equiv y}$$

gdje je t proizvoljan term koji ne sadrži x slobodan. Niti jedan takav term ne zadovoljava $x \equiv t$, pa je najgornja formula lažna.

Pokušaj formalizacije dokaza započinje rezolucijom s instancom aksioma $\exists$-introdukcije:

$$\frac{[\![F_1(y_1)]\!] \Rightarrow [\![\exists x.F_1(x)]\!] \qquad [\![\exists y \forall x.x \equiv y]\!] \Rightarrow [\![\exists y \forall x.x \equiv y]\!]}{[\![\forall x.x \equiv y_1]\!] \Rightarrow [\![\exists y \forall x.x \equiv y]\!]}$$

kojom je funkcijska varijabla F_1 instancirana u funkciju $\lambda y.\forall x.x \equiv y$. Novo stanje dokaza sadrži novu varijablu y_1. Rezolucija s aksiomom $\forall$-introdukcije daje:

$$\frac{(\bigwedge x.[\![F_2(x)]\!]) \Rightarrow [\![\forall x.F_2(x)]\!] \qquad [\![\forall x.x \equiv y_1]\!] \Rightarrow [\![\exists y \forall x.x \equiv y]\!]}{(\bigwedge x.[\![x \equiv y_1]\!]) \Rightarrow [\![\exists y \forall x.x \equiv y]\!]}$$

Ovdje je dokaz zaglavio. Niti jedna fiksirana varijabla y_1 ne može biti ekvivalentna svakom x. Podcilj $\bigwedge x.[\![x \equiv y_1]\!]$ nije valjan.
Rezolucija s aksiomom refleksivnosti relacije ekvivalencije ne uspijeva.
Polazni par za unifikaciju:

$$\langle \bigwedge x.[\![g_3(x) \equiv g_3(x)]\!], \bigwedge x.[\![x \equiv y_1]\!] \rangle$$

svodi se na parove $\langle \lambda x.g_3(x), \lambda x.x \rangle$ i $\langle \lambda x.g_3(x), \lambda x.y_1 \rangle$.
Zbog prvog para g_3 mora biti $\lambda x.x$ pa se drugi par svodi na $\langle \lambda x.x, \lambda x.y_1 \rangle$.
Ovaj par nema unifikator. Dokaz nije uspio.

10 Interakcija s Isabelle

Isabelle je sistem za specifikaciju i verifikaciju. To je generički sistem za implementaciju raznih logičkih formalizama.
Isabelle/HOL je specijalizacija Isabelle za logiku višeg reda, HOL (Higer Order Logic).
Interakcija s Isabelle može se provoditi na bazičnom, shell nivou ili putem naprednijih sučelja kao što je npr. *Proof General*, sučelje koje se preporuča za *Isabelle/Isar*, proširenje Isabelle kod kojeg je jezik implementacije gotovo potpuno skriven.
(Puno ime sistema je ustvari Isabelle/Isar/HOL).

10.1 Isabelle/HOL

HOL je tipizirana logika. Među osnovnim su tipovima *bool*, tip istinosnih vrijednosti, te *nat*, tip prirodnih brojeva. Funkcijski tipovi označavaju se s $\Rightarrow$ i reprezentiraju *totalne* funkcije. Od konstruktora tipova, istaknimo *set*, tip skupova, *list*, tip listi. Konstruktori se pišu postfiksno. Npr. $(nat)set$, ili kraće $nat\,set$ je tip skupova čiji su elementi prirodni brojevi. Tip varijabli označava se $'a$, $'b$ itd.
Tipovi su iznimno važni jer se njima sprečava pisanje besmislenih izraza. Isabelle zahtjeva da su svi termi i formule dobro tipizirani. Inače, vraća grešku. Greške u tipiziranju Isabelle detektira tokom dokazivanja. Dokazi uključuju eksplicitnu provjeru tipova.
Kako bi se smanjila količina eksplicitnog tipiziranja od strane korisnika, Isabelle tipizira sve varijable automatski (*type inference*). Ponekad je ipak potrebno eksplicitno definirati tip kako bi se izbjegle nejasnoće.
Termi se formiraju aplikacijom funkcija na argumente, kao kod funkcijskog programiranja. Termi mogu sadržavati λ-apstrakcije.
Formule su termi tipa *bool*. Osnovne su konstante $True$ i $False$. Logički veznici su uobičajeni: $\neg, \wedge, \vee$ i $\rightarrow$, dok se ekvivalencija izražava infiksno funkcijom $= : 'a \Rightarrow 'a \Rightarrow bool$ za terme istog tipa. Kvantifikatori su $\forall$, $\exists$, $\exists!$.

Isabelle razlikuje slobodne i vezane varijable. Vezane varijable Isabelle automatski preimenuje kako bi se izbjegli konflikti sa slobodnim varijablama.
Dodatno, Isabelle ima i treću vrstu varijabli, tzv. logičke varijable ili nepoznanice (*schematic variable/unknown*). Njihov je prvi znak u imenu ?.

Logički, nepoznanice su slobodne varijable, no tokom dokaza može ih se instancirati drugim termima.
Npr. matematički teorem $x = x$ u Isabelle se reprezentira sa $?x = ?x$, što znači da Isabelle može proizvoljno instancirati tu nepoznanicu. To nije slučaj s običnim varijablama, koje ostaju fiksirane.

10.2 Funkcijsko programiranje u HOL

Raditi s Isabelle znači kreirati teorije (*theory*). Teorija je imenovan skup tipova, funkcija i teorema. U nju su ugrađeni termi, tipovi i formule logike HOL.
Osnovni format teorije T je:

theory T = $B_1 + ... + B_n$:
deklaracije, *definicije*, *dokazi*
end

$B_1, ..., B_n$ su imena već postojećih teorija na kojima se bazira teorija T, tzv. roditeljske teorije (*parent theories*) od T. Sve što je definirano u roditeljskim teorijama, te rekurzivno i njima roditeljskim teorijama, nasljeđuje se.
Svaka teorija T sprema se u datoteku T.thy .
HOL ima već predefinirane mnoge teorije. Teorija *Main* sadrži osnovne teorije kao što su aritmetika, liste, skupovi itd.

Konkretna formalizacija samih teorija i interakcije s Isabelle/HOL nije predmet ovog rada. Cilj je pokazati osnovnu intuiciju dokazivanja pomoću Isabelle. U tu svrhu spomenut ćemo neke osnovne naredbe i metode dokazivanju.

10.2.1 Osnovne naredbe

Standardni postupak u dokazivanju započinje postavljanjem cilja, nekog teorema ili leme. Postupak dokazivanja nastavljamo sve dok nam ne zatreba dodatna lema. Dokažemo je, te se vratimo polaznom cilju. Nastavljamo postupak.

Cilj koji želimo dokazati postavljamo naredbama theorem ili lemma.
Naredba ***theorem*** deklarira novi teorem koji treba dokazati, npr.
theorem *ime-teorema* [simp]: "*izraz1 = izraz2*"

Uz to, imenuje teorem - *ime-teorema* za kasniju upotrebu. Dodatno, pomoću atributa [*simp*] daje se Isabelle taj teorem kao pravilo za simplifikaciju. Kasniji dokazi koji budu koristili simplifikaciju mogu zamijeniti *izraz*1 s *izraz*2. Analogna je upotreba naredbe ***lemma***. Sami određujemo važnost koju pridodajemo nekoj propoziciji, smatramo li je teoremom ili lemom.

Činjenicu da je dokaz završio potrebno je potrvditi naredbom ***done***. Kao rezultat izvršavanja ove naredbe, Isabelle upravo dokazanoj lemi ili teoremu pridružuje njeno ime.

Jednostavne naredbe u dokazivanju oblika su ***apply*** (method). One kažu Isabelle da primjeni strategiju dokazivanja koja je navedena (method). Npr. metoda *induct_tac* vezana je uz indukciju.
U pravilu, metoda pokušava riješiti prvi podcilj. Iznimka je npr. metoda *auto* koja djeluje na sve podciljeve. Tom metodom Isabelle pokušava riješiti sve trenutne podciljeve automatski, u osnovi simplifikacijom.

Simplifikacija je jedna od osnova u dokazivanju (sam alat zove se *simplifier*). Osnova simplifikacije je uzastopna aplikacija jednadžbi s lijeva na desno. Taj je postupak poznat i kao tzv. *term rewriting*. Koje jednadžbe - teoremi se koriste za simplifikaciju deklarira se atributom [simp]. Osim toga, neke definicije implicitno deklariraju pravila simplifikacije, npr. definicija primitivnom rekurzijom *primrec*.
Potencijalno, svaki teorem može biti simplifikacijsko pravilo, međutim samo ona pravila koja doista pojednostavljuju trebala bi se deklarirati kao simplifikacijska. Zakon distributivnosti npr, može dovesti do eksponencijalnog rasta terama, a ne do simplifikacije. Simplifikacija može dovesti i do beskonačnih petlji (ako su npr. $f(x) = g(x)$ i $g(x) = f(x)$ istovremeno deklarirana simplifikacijska pravila).
Atribut simplifikacije za teoreme može se isključiti ili uključiti.

Metoda *assumption* dokazuje podcilj, odnosno konkluziju ako se ona nalazi među pretpostavkama.

Naredba ***by*** (method) koristi se u dokazima s puno ponavljanja metode assumption. Njome se izvrši naredba apply (method), a zatim se svi podciljevi pokušaju riješiti metodom assumption. Ako se pritom riješe svi podciljevi i time završi cijeli dokaz, naredba by zamjenjuje i naredbu done. Često se, stoga, by koristi u dokazu umjesto posljednjeg apply i done.

Metoda *blast* provodi automatsko zaključivanje unaprijed i unatrag koristeći sve leme koje su na raspolaganju. Vrlo je brza.

10.3 Deduktivne metode

Općenito, pravilo prirodne dedukcije ima oblik $\frac{A_1 \quad ... \quad A_n}{B}$, u notaciji Isabelle $[\![A_1 \quad ... \quad A_n]\!] \Rightarrow B$.
Premisa A_1 naziva se glavna premisa. Nazovimo ovo pravilo R pravilo.

Napomenimo da semantičke zagrade iz meta-logike $[\![\quad]\!]$ ovdje koristimo za grupiranje pretpostavki.

Osnovne metode koje se primjenjuju uz pravila prirodne dedukcije su *rule*, *erule*, *drule* i $frule$.
Odabir metode je na korisniku. Uglavnom ovisi o tipu pravila. Neke su metode tako pogodnije za eliminacijska pravila.
Metoda određuje kako će se pravilo protumačiti.
Mnoga pravila mogu se koristiti na više načina.

U svakom koraku dokaza podciljevi nasljeđuju postojeće pretpostavke, s tim što se ponekad neke od njih brišu ili se pak neke nove dodaju. Npr. pravilo $disjE$ dodaje pretpostavke, dok se primjenom metode *erule* ili *drule* pretopostavka briše.

10.3.1 Metoda *rule*

Metoda ***rule*** R unificira B s trenutnim podciljem te ga zamjenjuje sa n novih podciljeva: A_1,...,A_n.
Ona utjelovljuje intuiciju dokazivanja "unatrag": ako imamo pravilo R tada je, da bi dokazali B, dovoljno dokazati A_1,...,A_n.

Koristi se uz pravila introdukcije.
Neka takva pravila su:

$$\begin{aligned} [\![?P; ?Q]\!] \Rightarrow ?P \wedge ?Q \qquad & (conjI) \\ ?P \Rightarrow ?P \vee ?Q \qquad & (disjI1) \\ ?Q \Rightarrow ?P \vee ?Q \qquad & (disjI2) \\ ?P\ ?x \Rightarrow \exists x.\ ?Px \qquad & (exI) \end{aligned}$$

Uočimo da u pravilima nastupaju nepoznanice, označene znakom ?. One se mogu zamijeniti proizvoljnim formulama.

Koristimo li npr. pravilo *conjI* u dokazivanju unatrag metodom *rule*, Isabelle će pokušati unificirati trenutni podcilj s konkluzijom pravila, koje je u ovom slučaju $?P \wedge ?Q$. Ako u tome uspije, postavlja nove podciljeve određene formulama $?P$ i $?Q$.

Primjer 5. lemma conj-rule*:* "$[\![P; Q]\!] \Rightarrow P \wedge (Q \wedge P)$"

Pokazat ćemo na primjeru kako to pravilo djeluje uz metodu *rule*. Želimo dokazati danu lemu.

Naredbom lemma conj-rule: "$[\![P; Q]\!] \Rightarrow P \wedge (Q \wedge P)$" Isabelle postavlja pretpostavke P i Q te cilj $P \wedge (Q \wedge P)$.
Dokazujemo unatrag. Naredba apply (rule conjI) pronalazi simbol $\wedge$ koji zadnji djeluje u cilju, a za nove podciljeve postavlja konjunkte:

1. $[\![P; Q]\!] \Rightarrow P$
2. $[\![P; Q]\!] \Rightarrow Q \wedge P$

Dokazati prvi podcilj je trivijalno, konkluzija je među pretpostavkama. Naredba apply assumption dokazuje prvi podcilj te nam ostaje dokazati:

1. $[\![P; Q]\!] \Rightarrow Q \wedge P$

Ponovno primjenimo naredbu apply (rule conjI):

1. $[\![P; Q]\!] \Rightarrow Q$
2. $[\![P; Q]\!] \Rightarrow P$

Oba podcilja dokazujemo metodom assumption pa je potpun dokaz lemme:

lemma conj-rule: "$[\![P; Q]\!] \Rightarrow P \wedge (Q \wedge P)$"
apply (rule conjI)
apply assumption
apply (rule conjI)
apply assumption
apply assumption
done

10.3.2 Metoda *erule*

Metoda ***erule*** R unificira B s trenutnim podciljem i istovremeno unificira A_1 s nekom pretpostavkom. Podcilj se zamjenjuje s $n-1$ novih podciljeva: A_2,...,A_n, s tim da se pretpostavka koja je unificirana briše.

Koristi se uz pravila eliminacije.
Najčešće je *erule* najbolji način za upotrebu eliminacijskih pravila. Na taj se način pretpostavka briše i zamjenjuje njenim potformulama.

Primjer pravila eliminacije su npr. eliminacijska pravila za $\vee$ i $\exists$:

$$[\![?P \vee ?Q; ?P \Rightarrow ?R; ?Q \Rightarrow ?R]\!] \Rightarrow ?R \qquad (disjE)$$

$$[\![\exists x.\, ?P\, x\, ; \bigwedge x.\, ?P\, x \Rightarrow ?Q]\!] \Rightarrow ?Q \qquad (exE)$$

Promotrimo kako djeluje metoda erule na primjeru pravila disjE.

Metoda *erule* $disjE$ unificira podcilj s $?R$ te pokušava unificirati neku od pretpostavki s prvom premisom pravila, premisom $?P \vee ?Q$. Ako uspije pronaći takvu pretpostavku, tada ju briše, smatrajući je dokazanom. Novi podciljevi su preostale premise: $?P \Rightarrow ?R$ i $?Q \Rightarrow ?R$.
Dokaz od $?R$ iz $?P \vee ?Q$, sveli smo na dokaze od $?R$ iz $?P$ i $?R$ iz $?Q$.

Primjer 6. lemma disj-swap*:* "$P \vee Q \Rightarrow Q \vee P$"

Naredbom apply(erule disjE) cilj $Q \vee P$ unificira se s $?R$. Pretpostavka $P \vee Q$ se unificira, zatim briše, a novi su podciljevi:

1. $P \Rightarrow Q \vee P$
2. $Q \Rightarrow Q \vee P$

Introdukcijsko pravilo za drugi konjunkt $disjI2$ pojednostavljuje prvi podcilj:

1. $P \Rightarrow P$
2. $Q \Rightarrow Q \vee P$

Prvi podcilj završavamo s assumption pa ostaje:

1. $Q \Rightarrow Q \vee P$

čiji je dokaz analogan koristeći ovaj put pravilo $disjI1$.

Potpun dokaz je:

lemma disj-swap: "$P \vee Q \Rightarrow Q \vee P$"
apply (erule disjE)
apply (rule disjI2)
apply assumption
apply (rule disjI1)
apply assumption
done

Primjer 7. lemma *:* "$\exists x.\, P \wedge Q(x) \Rightarrow P \wedge (\exists x. Q(x))$"

Naredbom apply (rule conjI) dobijemo dva podcilja, konjunkte polaznog cilja koje treba dokazati iz polaznog skupa pretpostavki:

1. $\exists x.\, P \wedge Q(x) \Rightarrow P$
2. $\exists x.\, P \wedge Q(x) \Rightarrow \exists x. Q(x)$

Konkluzija prvog podcilja je konjunkt u premisi, no kako je premisa formula oblika $\exists x. F(x)$, najprije se treba osloboditi kvantifikacije u premisi. To činimo naredbom apply (erule exE):

1. $\bigwedge x.\, P \wedge Q(x) \Rightarrow P$
2. $\exists x.\, P \wedge Q(x) \Rightarrow \exists x. Q(x)$

Egistencijalni kvantifikator objektne logike uzamijenjen je kvantifikatorom $\bigwedge$ meta-logike. Varijabla x je vezana.
Sada možemo dokazati prvi podcilj naredbom apply (erule conjunct1), budući da je konkluzija prvi konjunkt premise.
Time je prvi podcilj dokazan i preostaje nam dokazati drugi podcilj.

1. $\exists x.\, P \wedge Q(x) \Rightarrow \exists x. Q(x)$

Naredbom apply (erule exE) eliminiramo kvantifikaciju u premisi:

1. $\bigwedge x.\, P \wedge Q(x) \Rightarrow \exists x. Q(x)$

Zatim eliminiramo kvantifikaciju u konkluziji naredbom apply (rule exI):

1. $\bigwedge x.\, P \wedge Q(x) \Rightarrow Q(?x4\, x)$

Logička varijabla $?x4$ može se zamijeniti bilo kojim termom kojeg je moguće izgraditi iz x. Formalno, nepoznanica $?x4$ je funkcijskog tipa i aplicira se na argument x.
Konačno, naredba apply (erule conjunct2) završava dokaz.

Potpun dokaz je:

lemma "$\exists x.\, P \wedge Q(x) \Rightarrow P \wedge (\exists x.Q(x))$"
apply (rule conjI)
apply (erule exE)
apply (erule conjunct1)
apply (erule exE)
apply (rule exI)
apply (erule conjunct2)
done

10.3.3 Metode *drule* i *frule*

Metoda ***drule*** R unificira A_1 s nekom pretpostavkom, te se ta pretpostavka briše. Podcilj se zamjenjuje s $n-1$ podciljeva A_2,...,A_n i n-tim podciljem koji je jednak originalnom, no ima dodatnu pretpostavku, B.

Koristi se uz pravila destrukcije. To su pravila kod kojih je konkluzija potformula premise. Ona "unište" premisu i uzmu samo neki njezin dio. Ostatak premise se gubi.
Takva su npr. eliminacijska pravila za konjunkciju:

$$?P \wedge ?Q \Rightarrow ?P \qquad (conjunct1)$$

$$?P \wedge ?Q \Rightarrow ?Q \qquad (conjunct2)$$

Primjer 8. lemma conj-swap*:* "$P \wedge Q \Rightarrow Q \wedge P$"

Dokaz ove leme je :

lemma conj-swap: "$P \wedge Q \Rightarrow Q \wedge P$"
apply(rule conjI)
apply(drule conjunct2)
apply assumption
apply(drule conjunct1)
apply assumption
done

Prva naredba polazni cilj svodi na dva podcillja:

1. $P \wedge Q \Rightarrow Q$
2. $P \wedge Q \Rightarrow P$

Metodom *drule* pretpostavka $P \wedge Q$ se unificira i zatim briše. Novi podcilj ima originalnu konkluziju te dodatnu pretpostavku, konkluziju pravila $conjunct2, \ \ Q$:

1. $Q \Rightarrow Q$
2. $P \wedge Q \Rightarrow P$

Prvi podcilj dokazujemo s assumption, a dokaz drugog podcilja je analogan.

Destrukcijska su pravila jednostavnije forme od indirektnih pravila kao što je $disjE$, no mogu biti nezgodna. Svakom se primjenom gubi dio formule. Kako bi dokaz završio, ponekad je potrebno uzeti oba djela polazne formule za nove pretpostavke.

Ovaj se problem može riješiti upotrebom metode $frule$ ili preformuliranjem destrukcijskih pravila. Takvo je rješenje npr. alternativno pravilo za eliminaciju konjunkcije kojim se čuvaju oba konjunkta:

$$[\![?P \wedge ?Q; [\![?P; ?Q]\!] \Rightarrow ?R]\!] \Rightarrow ?R \qquad (conjE)$$

Primjer 9. Drugačiji dokaz leme: lemma disj-swap*:* "$P \vee Q \Rightarrow Q \vee P$"

Upotrebom pravila $conjE$ skratili smo gornji dokaz leme:

lemma conj-swap: "$P \wedge Q \Rightarrow Q \wedge P$"
apply(erule conjE)
apply(rule conjI)
by assumption

Metoda ***frule*** R je slična metodi *drule* R, s tim da se pretpostavka koja je unificirana ne briše. Time se omogućava ponovna upotreba te pretpostavke.

Sažetak

Ovaj je rad podijeljen u dva dijela. Prvi od njih odnosi se na logiku drugog reda. Uvode se sintaksa i standardna semantika kako bi pokazali gubitak najvećih rezultata koji vrijede za logiku prvog reda. Uvodi se i nestandardna semantika logike drugog reda u kojoj spomenuti rezultati vrijede. Deduktivnim sustavima upoznajemo se s dokazivanjem. Pokazuje se redukcija logike višeg reda na logiku drugog reda.

Drugi dio odnosi se na Isabelle, generički dokazivatelj teorema koji implementira logiku višeg reda. Njenom sintaksom i semantikom formaliziraju se razne objektne logike. Pokazuje se korektnost i potpunost reprezentacije logike prvog reda. Zatim se prelazi na dokazivanje pomoću Isabelle. Prezentiraju se neki koraci u dokazivanju te deduktivne metode.

Higher-order logic and system Isabelle

Summary

This work is divided in two parts. The first is concerned with second-order logic. We introduce its syntax and standard semantics in order to demonstrate failure of the major results established for the first-order logic. We also introduce the alternative semantics which holds on those results. Deduction systems are presented to get acquainted with proofs. A reduction of higher-order logic to second-order logic is presented.

The second part concerns Isabelle, a generic theorem prover implementing higher-order logic. It's syntax and semantics are introduced to formalize various object logics. We show that Isabelle's representation of first order-logic is sound and complete. Then we get into constructing proofs with Isabelle. We present some of its proof steps and deductive methods in proofs.

Životopis

Rođena sam 18. ožujka 1972. godine u Rijeci, gdje sam završila osnovnu i srednju školu. Studij matematike i informatike upisala sam 1991. godine na Pedagoškom fakultetu u Rijeci gdje sam diplomirala 1996. godine. Diplomski rad pod naslovom *Koherencijski prostori i Gödelov sistem T* izradila sam pod vodstvom prof.dr.sc. Deana Rosenzweiga. Poslijediplomski studij upisala sam iste godine na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.

Od 1999. godine zaposlena sam kao mlađi asistent na Filozofskom fakultetu u Rijeci. Član sam Seminara za matematičku logiku i Seminara za teorijsko računarstvo.

Literatura

[1] S.Shapiro, *Foundations without Foundationalism, A Case for Second-order Logic*, Clarendon Press, Oxford, 2000.

[2] G.Boolos, R.Jefferey, *Computability and Logic*, Cambridge University Press, 1989.

[3] D.Leivant, *Higher Order Logic*, Handbook of Logic, Artificial Intelligence and Logic Programming, D. M. Gabbay, C. J. Hogger, and J. A. Robinson, editors, Volume 2, p. 229-321., Clarendon Press, Oxford 1994.

[4] D.Prawitz, *Natural Deduction, A Proof-Theoretical Study*, Almqvist and Winskel, 1965.

[5] D.Prawitz, *Ideas and Results in Proof Theory*, In: J.E.Fenstad, editor, Proceedings of the Second Scandinavian Logic Symposium (North-Holland, 1971), 235-308

[6] D.van Dalen, *Logic and Structure*, Springer Verlag, Berlin 1980.

[7] H.P.Barendregt, *The Lambda Calculus, Its Syntax and Semantics*, North-Holland Publishing Company, Amsterdam, 1981.

[8] M.Vuković, *Matematička Logika 1*, PMF MO, Zagreb 1999.

[9] L.C.Paulson, *The Foundations of a Generic Theorem Prover*, J. Automated Reasoning 5 (1989), 363397.

[10] L.C.Paulson, *Isabelle: The Next 700 Theorem Provers*, In: P. Odifreddi (editor), Logic and Computer Science (Academic Press, 1990), 361386.

[11] L.C.Paulson, *Natural Deduction as Higher-Order Resolution*, Journal of Logic Programmig 3 (1985), 237-258.

[12] L.C.Paulson, *A Formulation of the Simple Theory of Types, (for Isabelle)*, In: P. Martin-Lf and G. Mints (editors), COLOG-88: International Conf. in Computer Logic.Tallinn, Estonia (1988). Published as Springer LNCS 417, 1990), 246-274.

[13] L.C.Paulson, *Tool support for Logic of Programms*, In: M. Broy (editor), Mathematical Methods in Program Development (Summer School Marktoberdorf 1996), Springer-Verlag, 461498. Also Report 406, Computer Lab (1996).

[14] L.C.Paulson, *Generic Automatic Proof Tools*, In: Robert Veroff (editor), Automated Reasoning and its Applications: Essays in Honor of Larry Wos (MIT Press, 1997), 2347.

[15] T.Nipkov, *Structured Proofs in Isar/HOL*, In: Types for Proofs and Programs (TYPES 2002), LNCS 2646, 259-278, 2003.

[16] T.Nipkov, L.C.Paulson, M.Wenzel, *Isabelle/HOL, A Proof Assistant for Higher-Order Logic*, Springer Verlag, 2002.

[17] L.C.Paulson, T.Nipkov, M.Wenzel, *The Isabelle Reference Manual*, Computer Laboratory, University of Cambridge, Cambridge, 2002.

[18] M.Wenzel, *The Isabelle/Isar Reference Manual*, TU München, 2002.

[19] T.Nipkov, L.C.Paulson, M.Wenzel, *Isabelle's Logics: HOL*, Computer Laboratory, University of Cambridge, Cambridge, 2002.

[20] J.Lambek, P.J.Scott, *Introduction to Higher Order Categorical Logic*, Cambridge University Press, 1986.

[21] A.Church, *A Formulatioon of the simple theory of types*, Journal of Symbolic Logic, 5:56-68, 1940.

[22] G.P.Huet, *A unification algorithm for typed λ-calculus*, Theoretical Computer Science, 1:27-57, 1975.