math.e

Hrvatski matematički elektronički časopis

Topološka semantika logika dokazivosti

logika dokazivosti

Sažetak

Modalna logika obuhvaća široku familiju formalnih jezika i sistema s brojnim primjenama u računarstvu, lingvistici, filozofiji, teoriji informacija itd. Modalna logika ima iznenađujuće jednostavnu sintaksu i relacijsku semantiku koja se gotovo bez modifikacija uklapa u prividno vrlo različite primjene. U ovom članku[1] fokusiramo se na primjenu modalne logike koja je od možda najvećeg interesa za matematičare: formalizaciju Gödelovog[2] predikata dokazivosti, ključnog pojma Gödelovih teorema nepotpunosti. Uobičajenim matematičkim postupkom apstrakcije, ključna svojstava predikata dokazivosti proglašena su aksiomima i polazeći od njih izgrađen je logički sistem. Uz standardnu relacijsku semantiku, topološka semantika također se pokazuje pogodnom, pa i nužnom za jedno proširenje logike dokazivosti koje razmatramo na kraju članka.

1 Modalna logika

1.1 Sintaksa i intendirana interpretacija

Modalna logika motivirana je potrebom da se formalizira nužnost i mogućnost, znanje i vjerovanje, dokazivost i mnoga druga svojstva koja se mogu smatrati operatorima na logičkim sudovima.[3] Stroga izgradnja logičkog sustava, pa tako i modalne logike, podrazumijeva definiranje sintakse (jezik, izvod, dokaz, teorem) i semantike (model, istinitost, valjanost), te dokazivanje teorema adekvatnosti i potpunosti kao veze sintakse i semantike. U nastavku pretpostavljamo da su ovi pojmovi poznati iz logike sudova i logike prvog reda. Detalji se po potrebi mogu pronaći u svakom početnom udžbeniku matematičke logike, npr. [12].

U ovom članku razmatramo samo propozicionalne modalne logike. Najprije ćemo definirati alfabet osnovne modalne logike.

Alfabet osnovne modalne logike je proširenje alfabeta logike sudova simbolom $\Box$, tj. skup simbola koji sadrži:

- prebrojivo mnogo *propozicionalnih varijabli*, koje označavamo p, q i sl.
- *logičke veznike* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- *logičke konstante* $\top, \bot$
- $\Box$, koji zovemo *modalni operator*.

Formule modalne logike definiraju se rekurzivno:

- propozicionalne varijable i logičke konstante su formule
- ako su A i B formule, onda su $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$, $\Box A$ također formule.

Definiramo dualni modalni operator $\Diamond A$ kao pokratu za $\neg\Box\neg A$.

Napomena 1. *Formulu oblika $\Box A$ čitamo "nužno je A", "agent[4] zna A", "dokazivo je A" i slično, ovisno o interpretaciji. Postavlja se pitanje za koje formule očekujemo da uvijek vrijede. Npr. ako formulu $\Box A \rightarrow A$ čitamo kao "ako agent zna A, onda vrijedi A", složit ćemo se da je to u skladu sa značenjem glagola "znati" u prirodnom jeziku. No, to nije slučaj ako $\Box$ interpretiramo kao vjerovanje. Čitatelj može razmisliti i o sljedećim primjerima:*

- $\Box A \rightarrow \Box\Box A$
- $\Diamond A \rightarrow \Box\Diamond A$
- $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$

Formulu oblika $\Diamond A$ često čitamo kao " moguće je A" (" nije nužno $\neg A$").

Napomena 2. *Očigledni pravci generalizacije modalne logike su jezici s više modalnih operatora (npr. za modeliranje sistema s više agenata; još jedan primjer je u posljednjoj točki ovog članka), kao i višemjesni modalni operatori (npr. za modeliranje algoritamskih koncepata kao što je relacija "until": formulu oblika $U(A, B)$, gdje je U dvomjesni modalni operator, čitamo kao "vrijedit će A sve do trenutka u kojem će početi vrijediti B"). Također, mogu se promatrati i modalne logike s kvantifikatorima, no u ovom članku razmatramo samo propozicionalne modalne sisteme.*

Formula oblika $\Box(A \to B) \to (\Box A \to \Box B)$, posljednja navedena u napomeni 1, u skladu je s gotovo svim interpretacijama operatora $\Box$ koje se pojavljuju u primjenama, te se stoga uzima kao aksiom osnovnog modalnog sistema, kojeg zovemo *sistem* **K** (oznaka je u čast Kripkea[5]).

Definicija 3. *Aksiomi sistema **K** su sve tautologije logike sudova, ali u proširenom jeziku (npr. $\Box A \vee \neg\Box A$ je tautologija u modalnom jeziku), te svaka formula oblika*

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

*Pravila izvoda su modus ponens $\dfrac{A \quad A \to B}{B}$ i generalizacija $\dfrac{A}{\Box A}$. Kažemo da je formula A teorem sistema **K** (oznaka: $\vdash A$) ako je A element najmanjeg skupa formula koji sadrži sve aksiome i zatvoren je na pravila izvoda.*

Ovisno o intendiranoj interpretaciji, različiti modalni sistemi dobivaju se dodavanjem jednog ili više drugih aksioma, npr. formula $\Box A \to A$ iz napomene 1. je jedan od aksioma *epistemičke logike* (u kojoj je $\Box$ interpretiran kao operator znanja).

1.2 Relacijska semantika

Za modalnu logiku postoji više vrsta semantike (relacijska, topološka, okolinska, algebarska, ...). U ovom dijelu članka razmatramo relacijsku semantiku, koja se često naziva i Kripkeova semantika ili semantika mogućih svjetova. Kasnije ćemo upoznati i topološku semantiku.

Definicija 4. *Kripkeov okvir (ili samo okvir) je uređeni par (W, R), gdje je $W \neq \emptyset$ skup koji zovemo nosač, a R binarna relacija na W koju zovemo relacija dostiživosti. Elemente nosača zovemo svjetovi ili točke.*

(Kripkeov) model je uređena trojka (W, R, V), gdje je (W, R) okvir, a V valuacija, funkcija koja svakoj propozicionalnoj varijabli p pridružuje podskup nosača $V(p) \subseteq W$.

Pritom kažemo da je formula p istinita u svijetu $w \in W$ i pišemo $w \Vdash p$ ako je $w \in V(p)$. Definicija istinitosti rekurzivno se proširuje na sve formule:

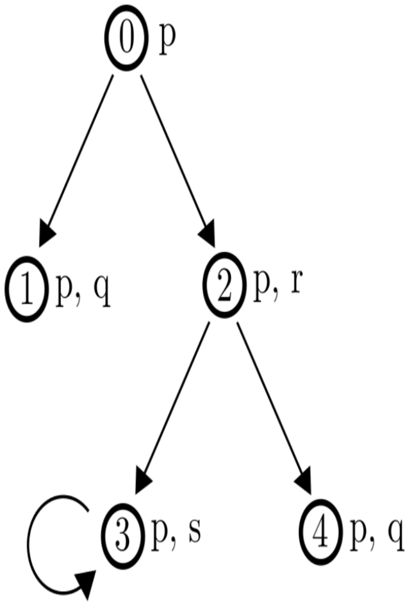
- *za svaki svijet w vrijedi $w \Vdash \top$ i $w \nVdash \bot$*
- *$w \Vdash \neg A$ ako ne vrijedi $w \Vdash A$*
- *$w \Vdash A \wedge B$ ako $w \Vdash A$ i $w \Vdash B$*
- *$w \Vdash \Box A$ ako za svaki $v \in W$ takav da je wRv vrijedi $v \Vdash A$.*

Kažemo da je formula valjana na okviru (W, R) ako je istinita u svakom svijetu za svaku valuaciju na tom okviru. Pišemo $\Vdash A$ ako je formula A valjana na svakom okviru.

Uočimo da iz definicije slijedi da je $w \Vdash \Diamond A$ ako i samo ako postoji $v \in W$ takav da je wRv i $v \Vdash A$.

Kripkeove modele možemo zamišljati kao jednostavne usmjerene grafove ako svakoj točki grafa (svijetu modela) x pridružimo neki skup propozicionalnih varijabli p za koje vrijedi $x \in V(p)$.

Primjer 5. *Na slici je jedan Kripkeov model. Skup svjetova W je skup $\{0,1,2,3,4\}$. Vrijedi xRy ako i samo postoji strelica iz svijeta x u svijet y. Za svijet $x \in W$ i propozicionalnu varijablu ℓ vrijedi $x \in V(\ell)$ ako i samo ako je ℓ napisan pokraj x.*



Pogledajmo nekoliko primjera istinitih i neistinitih formula u svijetu 0. Vrijedi li $0 \Vdash \Box p$? Da, jer su iz svijeta 0 dostižni samo svjetovi 1 i 2, te u oba vrijedi p. U svijetu 1 nije istinito r, a u svijetu 2 nije istinito q. Stoga ne vrijedi $0 \Vdash \Box r$ niti $0 \Vdash \Box q$. No, primijetimo da vrijedi $0 \Vdash \Diamond q$ te $0 \Vdash \Diamond r$.

Ne vrijedi $0 \Vdash \Diamond s$ (postoji put, ali ne postoji strelica, iz 0 u 3). Ali, vrijedi $0 \Vdash \Diamond\Diamond s$. Zatim, iako ne vrijedi $0 \Vdash \Box q$, vrijedi $0 \Vdash \Box(q \vee \Diamond q)$.

Još neki primjeri formula koje su istinite u 0 su $\Box(r \to \Diamond\Diamond\Box s)$, $\Diamond\Diamond\Diamond\Diamond s$ i $\Box(\Diamond q \to \Diamond s)$. Primijetite petlju na slici. Ona je bitna za istinitost prvih dviju navedenih formula.

Neke formule koje nisu istinite u svijetu 0 su primjerice sljedeće: $\Box(\Box q \to q) \to \Box q$, $\neg q \to \Box\Diamond\neg q$ i $\Diamond\Diamond s \to \Diamond s$.

Na internetu postoje stranice na kojima je moguće konstruirati primjere Kripkeovih modela i ispitivati istinitost formula. Jedna takva stranica je na adresi http://rkirsling.github.io/modallogic/.

Sada smo modalnim formulama dali matematičko značenje, pa možemo o ranije spomenutim primjerima formula razmišljati na precizniji način.

Primjer 6. *Svaka formula oblika $\Box A \to A$ je valjana na okviru (W, R) ako i samo ako je R refleksivna relacija.*

Zaista, neka je R refleksivna i $w \in W$ takav da je $w \Vdash \Box A$. To znači $v \Vdash A$ za sve v takve da je wRv. No zbog refleksivnosti relacije R vrijedi wRw, pa je posebno $w \Vdash A$. Iz $w \Vdash \Box A$ zaključili smo $w \Vdash A$, što po semantici logičkog veznika $\to$ povlači $w \Vdash \Box A \to A$

Obratno, neka je svaka formula oblika $\Box A \to A$ valjana na okviru (W, R). Pretpostavimo da R nije refleksivna, tj. postoji $w \in W$ takav da ne vrijedi wRw. Neka je V valuacija takva da je $V(p) = W \setminus \{w\}$. Lako se vidi da tada vrijedi $w \Vdash \Box p$, ali ne $w \Vdash p$, dakle u w nije istinita $\Box p \to p$, što je u kontradikciji s pretpostavkom.

Iz prethodnog primjera slijedi da okviri za epistemičku logiku, u kojoj su formule oblika $\Box A \to A$ aksiomi, nužno imaju refleksivnu relaciju dostiživosti.

Zadatak 7. *Neka je (W, R) okvir. Slično kao u prethodnom primjeru, dokažite:*

- $\Box A \to \Box\Box A$ *je valjana na (W, R) ako i samo ako je R tranzitivna*
- $\Diamond A \to \Box\Diamond A$ *je valjana na (W, R) ako i samo ako R ima sljedeće svojstvo: za sve $w, v, u \in W$, ako je wRv i wRu, onda je vRu*
- $\Box(A \to B) \to (\Box A \to \Box B)$*je valjana na svakom okviru.*

Općenito, nužni i dovoljni uvjeti da se neko svojstvo relacije može definirati modalnom formulom dani su poznatim Goldblatt–Thomasonovim teoremom (detalji se mogu vidjeti npr. u knjizi [2]).

Za sistem **K** vrijedi teorem adekvatnosti i potpunosti u odnosu na relacijsku semantiku, tj. za svaku formulu A vrijedi: $\vdash A$ ako i samo ako $\Vdash A$. Adekvatnost slijedi iz prethodnog zadatka, dok dokaz potpunosti nadilazi okvire ovog članka. Spomenimo, također bez dokaza, da za modalni sistem dobiven dodavanjem aksioma $\Box A \to A$ sistemu **K** vrijedi adekvatnost i potpunost u odnosu na klasu svih okvira čija je relacija dostižnosti refleksivna. Analogni rezultati vrijede i za ostale spomenute formule, ali i mnoge druge (v. npr. [6]).

2 Logika dokazivosti – sistem GL

2.1 Sintaksa i aritmetička interpretacija

Sistem **GL** (Gödel, Löb[6]) proširenje je osnovnog modalnog sistema **K** svim formulama oblika $\Box(\Box A \to A) \to \Box A$ kao aksiomima. Shema formula $\Box(\Box A \to A) \to \Box A$ naziva se Löbovim aksiomom i označava s L. Uvodimo oznaku $\vdash GLA$ za modalnu formulu A koja je teorem sistema **GL**.

Sada ćemo reći nešto o tome što predstavljaju teoremi sistema **GL**. Radi se o određenoj vezi s Peanovom aritmetikom i drugim formalnim teorijama aritmetike. Peanova aritmetika je jedna teorija prvog reda (v. [12]).

Pišemo $\vdash PAA$ ako je A teorem Peanove aritmetike. Predikat dokazivosti Peanove aritmetike je formula $Pr(n)$ čije je neformalno značenje "broj n je kod nekog teorema Peanove aritmetike".

Prostor nam ne dopušta da pobliže obrazložimo postupak kodiranja koji omogućuje da se dokazivost formula Peanove aritmetike izrazi u samoj Peanovoj aritmetici. Detalji ove konstrukcije mogu se vidjeti u knjizi [9], ili u sažetoj skripti te knjige namijenjenoj studentima[7].

Jednom kad smo konstruirali predikat dokazivosti ili se već nekako uvjerili da on postoji, prirodno je pitati se koja su njegova svojstva. Ako je A neka formula Peanove aritmetike, s $\ulcorner A \urcorner$ ćemo označavati njezin kod.

Podsjetimo da je *rečenica* bilo koja zatvorena formula prvog reda, tj. formula čije su sve varijable u dosegu kvantifikatora. Jedno prirodno pitanje koje bi nas moglo zanimati jest je li formula $Pr(\ulcorner A \urcorner) \to A$ ("ako je A dokaziva, onda vrijedi A") teorem aritmetike za svaku rečenicu A. Poznati Löbov teorem za Peanovu aritmetiku kaže da je za danu rečenicu A, formula $Pr(\ulcorner A \urcorner) \to A$ dokaziva jedino ako je već i sama formula A dokaziva. Uočimo da to zapravo govori o slabosti Peanove aritmetike. Löbov teorem je tvrdnja koja govori *o* Peanovoj aritmetici. No, dokaz tvrdnje tog teorema moguće je provesti i unutar same Peanove aritmetike. Pritom je tvrdnja Löbovog teorema formalizirana sljedećom formulom:

$$Pr(\ulcorner Pr(\ulcorner A \urcorner) \to A \urcorner) \to Pr(\ulcorner A \urcorner).$$

Primijetimo da je ova formula sintaktički nalik shemi aksioma L sistema **GL**.

Sada ćemo precizirati vezu logike dokazivosti i aritmetike.

Definicija 8. *Aritmetička interpretacija sistema **GL** je svaka funkcija $*$ sa skupa svih modalnih formula u skup rečenica Peanove aritmetike sa sljedećim svojstvima:*

- *svakoj propozicionalnoj varijabli p pridružena je proizvoljna rečenica p^*;*
- *funkcija * komutira s logičkim veznicima (npr. $(A \wedge B)^* = A^* \wedge B^*$);*
- *za svaku modalnu formulu A vrijedi $(\Box A)^* = Pr(\ulcorner A^* \urcorner)$.*

Solovayev[8] prvi teorem govori o aritmetičkoj potpunosti sistema **GL**.

Teorem 9. *[Solovay, 1976] Neka je A proizvoljna modalna formula. Tada vrijedi $\vdash GLA$ ako i samo ako je $\vdash PAA^*$ za sve aritmetičke interpretacije *.*

Solovayev teorem nam govori da je, u određenom smislu, sve što Peanova aritmetika može reći o predikatu dokazivosti sadržano u teoriji GL . Vidimo da je njezin aksiom L upravo formalizacija Löbovog teorema. Izrečena veza je vrijedan rezultat jer Peanova aritmetika ima svojstvo neodlučivosti. Neodlučivost teorije je svojstvo da ne postoji algoritam koji će za danu formulu u konačno mnogo koraka ispravno reći je li ona teorem. S druge strane, GL je odlučiva teorija. U idućem ćemo poglavlju napomenuti kako bi izgledao algoritam koji određuje je li dana formula teorem sistema GL . Dakle, kroz sistem GL možemo na jednostavan način, štoviše potpuno mehanički, odgovoriti na preostala pitanja poput ranijeg (negativno odgovorenog) "je li $Pr(\ulcorner A \urcorner) \rightarrow A$ teorem aritmetike za svaku rečenicu A?"

2.2 Relacijska semantika

Ranije smo spomenuli da za sistem **K** proširen novom shemom aksioma $\Box A \rightarrow A$ vrijede teoremi adekvatnosti i potpunosti u odnosu na klasu svih okvira kod kojih je relacija dostiživosti refleksivna. Sličan rezultat vrijedi za sistem **GL**.

Zadatak 10. *Neka je (W, R) okvir. Kažemo da je relacija R inverzno dobro fundirana ako ne postoji niz svjetova $(w_i)_{i \in \mathbb{N}}$ takav da vrijedi $w_0 R w_1 R w_2 \ldots$*

Dokažite: ako je R tranzitivna i inverzno dobro fundirana, onda je Löbov aksiom valjan na (W, R).

Napominjemo da vrijedi i obrat, koji je nešto teže dokazati, no zainteresiraniji čitatelj može pokušati. No, već i lakši smjer dovoljan je za ključni dio dokaza teorema adekvatnosti za sistem **GL**, tj. da za svaki formulu A

vrijedi: ako je $\vdash GLA$, onda je A valjana na svakom tranzitivnom i inverzno dobro fundiranom okviru. Vrijedi i obrat, tj. teorem potpunosti, čiji dokaz je, kao što je to i obično slučaj u logici, bitno složeniji. Može se pronaći npr. u knjigama [3] i [10].

Primijetimo da su konačna (tranzitivna) stabla poseban slučaj tranzitivnih inverzno dobro fundiranih relacijskih struktura. Stoga je klasa konačnih tranzitivnih stabala adekvatna za **GL**. No, vrijedi i potpunost.

Teorem 11. *Neka je A proizvoljna modalna formula koja nije teorem sistema **GL**. Tada postoji konačno stablo (W, R), valuacija V i svijet $w \in W$ tako da vrijedi $w \nVdash A$.*

Ovo je vrlo značajan teorem. Prvo, on se na esencijalan način koristi u Solovayevu teoremu aritmetičke potpunosti. Drugo, on nam daje algoritam provjere je li neka formula A teorem sistema **GL**. Naprosto simultano prolazimo svim dokazima teorema sustava **GL** (npr. leksikografski od kraćih ka duljima), i svim konačnim stablima i njihovim valuacijama. Prije ili kasnije će se dogoditi nešto od sljedećeg:

- pronaći ćemo dokaz formule A;
- pronaći ćemo model u čijem je nekom svijetu istinita formula A.

2.3 Topološka semantika

Sada želimo izgraditi još jednu semantiku za sistem **GL**. Ovoga puta kao temeljnu strukturu ne želimo koristiti okvire već topološke prostore. Naime, u posljednjem dijelu članka promatrat ćemo sistem u kojem nije moguće (na zadovoljavajuć način) definirati relacijsku semantiku, pa moramo posegnuti za topološkom. No, prije toga će nam sistem **GL** poslužiti kao jednostavniji primjer na kojem ćemo upoznati taj tip semantike. U nastavku pretpostavljamo poznavanje osnovnih pojmova topologije, kao što su topološki prostor, baza, uređajna topologija, gomilište, diskretna topologija i sl. Ako je čitatelju potreban podsjetnik, sve potrebne definicije mogu se pronaći npr. u [11].

Neka je $(X, \mathcal{T})$ topološki prostor. Na njemu možemo definirati model na posve analogan način kao i na okviru. Ono što trebamo promijeniti je definicija istinitosti za formule oblika $\Box A$. Naime, u topološkom prostoru više nemamo relaciju dostižnosti.

Definicija 12. *Topološki model je uređena trojka $(X, \mathcal{T}, V)$, gdje je $(X, \mathcal{T})$ topološki prostor, a V valuacija, funkcija koja svakoj propozicionalnoj varijabli p pridružuje $V(p) \subseteq X$.*

Istinitost modalnih formula u točki $x \in X$ definira se rekurzivno, pri čemu su slučajevi propozicionalnih varijabli, logičkih konstanti i formula dobivenih primjenom logičkih veznika isti kao kod relacijske semantike, te se definira $x \Vdash \Box A$ ako postoji $U \in \mathcal{T}$ takav da je $x \in U$ i za sve $y \in U$ takve da je $y \neq x$ vrijedi $y \Vdash A$.

Kažemo da je formula valjana na topološkom prostoru $(X, \mathcal{T})$ ako je istinita u svakoj točki svakog topološkog modela $(X, \mathcal{T}, V)$.

Uočimo da je $x \Vdash \Diamond A$ ako i samo ako za svaki $U \in \mathcal{T}$ takav da je $x \in U$ postoji $y \in U$ takav da je $y \neq x$ i $y \Vdash A$. Drugim riječima, $x \Vdash \Diamond A$ ekvivalentno je s činjenicom da je x gomilište skupa $\{y \in X : y \Vdash A\}$.

Kažemo da je topološki prostor $(X, \mathcal{T})$ *raspršen* ako svaki neprazan podskup $S \subseteq X$ ima izoliranu točku, tj. postoji točka $s \in S$ i neka njena okolina $O \in \mathcal{T}$ tako da vrijedi $S \cap O = \{s\}$.

Primjer 13. *Trivijalni primjer raspršenog prostora je diskretni topološki prostor. Netrivijalni primjer je $(\alpha, \mathcal{T})$, gdje je α ordinal, a $\mathcal{T}$ uređajna topologija. Naime, svaki $S \subseteq \alpha$ je dobro uređen, pa ima najmanji element $\min S$. On je izolirana točka, jer $[0, \min S + 1\rangle \in \mathcal{T}$ siječe S samo u $\min S$.*

Propozicija 14. *Formula $\Box(\Box A \to A) \to \Box A$ je valjana na topološkom prostoru $(X, \mathcal{T})$ ako i samo ako je on raspršen.*

Propozicija se dokazuje raspisivanjem definicija, na sličan način kao 6.

Adekvatnost i potpunost sistema **GL** u odnosu na klasu svih raspršenih topoloških prostora dokazao je Esakia[9] 1981. Iako je sam teorem dobro poznat, njegov dokaz je, koliko nam je poznato, objavljen samo u publikaciji [4] i nije nam dostupan. Međutim, za pretpostaviti je da je Esakijin dokaz sličan ovdje navedenom.

Uvedimo jednu oznaku. Neka je dan okvir (X, R). Za točku $x \in X$ označimo s $R[x]$ skup $\{y \in X \mid xRy\}$.

Propozicija 15. *Neka je R tranzitivna i inverzno dobro fundirana relacija na skupu X. Označimo $B = \{R[x] \cup \{x\} \mid x \in X\}$. Tada je familija B baza za neku topologiju $\mathcal{T}$. Štoviše, $(X, \mathcal{T})$ je raspršen prostor.*

Prethodna propozicija ima jednostavan dokaz (v. [8]).

U dokazu idućeg teorema ćemo s $\Vdash_R$ označavati istinitost u Kripkeovom modelu, a s $\Vdash_T$ istinitost u topološkom modelu.

Teorem 16. *[topološka potpunost] Neka je F formula koja je valjana na svim raspršenim topološkim prostorima. Tada vrijedi $\vdash GLF$.*

Dokaz. Neka vrijedi $\nvdash GLF$. Tada (zbog potpunosti u odnosu na relacijsku semantiku – vidjeti teorem 11) postoji model (W, R, V) takav da je R tranzitivna i inverzno dobro fundirana, te točka $w \in W$ takva da vrijedi $w \nVdash_R F$.

Neka je topologija $\mathcal{T}$ generirana familijom B sljedećeg oblika:

$$B = \{\{x\} \cup R[x] \mid x \in W\}.$$

Tada iz prethodne propozicije proizlazi da je prostor $(W, \mathcal{T})$ raspršen, a familija B čini bazu za $\mathcal{T}$.

Promotrimo topološki model $(W, \mathcal{T}, V)$ s istim nosačem i valuacijom kao (W, R, V). Dokažimo da za sve formule G i točke $x \in W$ vrijedi:

$$x \Vdash_R G \text{ ako i samo ako } x \Vdash_T G.$$

Tvrdnju dokazujemo indukcijom po složenosti formule G. Jasno je da tvrdnja vrijedi za bazu, te korak indukcije za slučaj logičkih veznika. Promotrimo korak indukcije za slučaj $G = \Box H$. Neka je $x \in W$ proizvoljna točka.

Neka vrijedi $x \Vdash_R G$. Dakle, za sve točke $y \in R[x]$ vrijedi $y \Vdash_R H$. Kako je H manje složenosti od G, po pretpostavci indukcije za sve točke $y \in R[x]$ vrijedi $y \Vdash_T H$. Kratko pišemo $R[x] \Vdash_T H$. No iz definicije baze B slijedi da je $\{x\} \cup R[x]$ okolina točke x, pa po definiciji istinitosti u točki topološkog modela slijedi $x \Vdash_T G$. Slično se dokazuje i obrat.

Sada iz ranije dokazane činjenice $w \nVdash_R F$ i upravo dokazane tvrdnje slijedi $w \nVdash_T F$. ■

Teoremi adekvatnosti i potpunosti za **GL** u odnosu na topološku semantiku ponekad se formuliraju tako da se kaže da je "**GL** logika raspršenih prostora". Semantike modalnih logika nam olakšavaju analizu njihovih svojstava. Primjerice, puno je lakše semantički argumentirati da neka formula nije teorem dane modalne logike. No veza je dvosmjerna. Primjerice, dobro je poznato da su formule oblika $\Diamond\Diamond A \to \Diamond A$ teoremi sustava **GL**. No iz činjenice da je "**GL** logika raspršenih prostora" odmah slijedi da je za svaki raspršen prostor $(X, \mathcal{T})$ i njegov podskup $S \subseteq X$, skup gomilišta skupa gomilišta od S podskup skupa gomilišta od S.

3 Polimodalna logika dokazivosti – GLP

Vidjeli smo vezu između **GL** i raspršenih prostora. No, vidjeli smo i da za **GL** imamo jednostavnu relacijsku semantiku. Važnost se topološkog pristupa vidi tek u proširenjima sistema **GL**.

3.1 Uvod

Sistem **GLP** uveo je Japaridze[10] 1986. Radi se o proširenju sistema **GL** s prebrojivo mnogo modalnih operatora $[n]$ indeksiranih prirodnim brojevima.[11] Formule sistema **GLP** se definiraju rekurzivno, slično kao formule sistema **GL**. Naglasimo samo dio definicije koji se odnosi na nove modalne operatore: ako je A formula, onda je i $[n]A$ formula (za sve prirodne brojeve n). Slično kao ranije, koristimo pokratu $\langle n\rangle A$ za $\neg[n]\neg A$.

Aksiomi su sve tautologije (u novom jeziku!), te sheme aksioma:

- $(K_n)[n](A \to B) \to ([n]A \to [n]B)$
- $(L_n)[n]([n]A \to A) \to [n]A$
- $(P_n^m)[n]A \to [m]A$, ako je $n < m$
- $(Q_n^m)\langle n\rangle A \to [m]\langle n\rangle A$, ako je $n < m$

Uočimo da prve dvije sheme aksioma sugeriraju da se radi o nizu operatora dokazivosti, dok druge dvije određuju odnos među njima. Pravila izvoda su modus ponens i $\dfrac{A}{[n]A}$, $n \in \mathbb{N}$.

Aritmetička interpretacija sistema **GLP** je svaka funkcija $*$ sa skupa svih formula sistema **GLP** u skup rečenica Peanove aritmetike sa svojstvima analognim aritmetičkoj interpretaciji sistema **GL**, pri čemu je $[0]$ interpretiran kao $\Box$, tj. $([0]A)^* = Pr(\ulcorner A^* \urcorner)$, te je $([n]A)^*$ definirana tako da, neformalno govoreći, ima značenje "A^* je dokaziva u teoriji proširenoj svim istinitim Π_n rečenicama", gdje su Π_n rečenice one koje sadrže kvantifikatore samo na početku formule i imaju n alternacija kvantifikatora od kojih je prvi $\forall$. Potrebno je dokazati da je ovako definirani niz predikata dokazivosti moguće formalizirati koristeći kodiranje, no ovdje nećemo ulaziti u detalje.

Aritmetičku adekvatnost i potpunost dokazao je Japaridze u radu [5].

3.2 Relacijska semantika?

Okvir za polimodalnu logiku je relacijska struktura s nosačem $W \neq \emptyset$ i indeksiranom familijom relacija dostižnosti pridruženih modalnim operatorima. Istinitost formula definira se za svaki modalni operator analogno kao za $\Box$ u slučaju osnovnog modalnog jezika. Dakle, u slučaju sistema **GLP** okvir bi bio $(W, (R_n)_{n\in\mathbb{N}})$, $R_n \subseteq W \times W$, $n \in \mathbb{N}$, a iz definicije istinitosti istaknimo samo da se definira $w \Vdash [n]A$ ako za sve u takve da je wR_nu vrijedi $u \Vdash A$.

Analogno sistemu **GL**, $[n]([n]A \to A) \to [n]A$ je valjana ako i samo ako je R_n tranzitivna i inverzno dobro fundirana.

Zadatak 17. *Dokažite da vrijedi:*

- $[n]A \to [n+1]A$ *je valjana na okviru* $(W, (R_n)_{n\in\mathbb{N}})$ *ako i samo ako* $R_{n+1} \subseteq R_n$
- $\langle n\rangle A \to [n+1]\langle n\rangle A$ *je valjana na okviru* $(W, (R_n)_{n\in\mathbb{N}})$ *ako i samo ako* wR_nv *i* $wR_{n+1}u$ *povlači* uR_nv*.*

Korolar 18. *Ako su na okviru* $(W, (R_n)_{n\in\mathbb{N}})$ *valjani svi aksiomi sistema **GLP**, onda je* $R_n = \emptyset$ *za svaki* $n > 0$*.*

Dokaz. Pretpostavimo $R_1 \neq \emptyset$, tj. postoje w, u tako da je wR_1u. No, tada iz prve tvrdnje prethodnog zadatka slijedi wR_0u, a onda iz druge tvrdnje uR_0u, dakle imamo beskonačan niz $uR_0uR_0u\ldots$, što je nemoguće jer je R_0 inverzno dobro fundirana. Dakle, $R_1 = \emptyset$, pa iz prve tvrdnje zadatka slijedi tvrdnja. ■

Dakle, postoji samo trivijalna relacijska semantika za **GLP**. Stoga koristimo topološku semantiku.

3.3 Topološka semantika

Neka je $X \neq \emptyset$ i $(X, \mathcal{T}_n)$ topološki prostor, za svaki $n \in \mathbb{N}$. Uređeni par $(X, (\mathcal{T}_n)_{n\in\mathbb{N}})$ zvat ćemo *politopološki prostor*. Za $S \subseteq X$, s dS standardno se označava skup gomilišta skupa S. U politopološkom prostoru ćemo s d_nS označavati skup gomilišta skupa S s obzirom na topologiju $\mathcal{T}_n$.

Definicija 19. *Politopološki model je uređena trojka $(X, (\mathcal{T}_n)_{n\in\mathbb{N}}, V)$, gdje je $(X, (\mathcal{T}_n)_{n\in\mathbb{N}})$ politopološki prostor i V valuacija. Istinitost formula definirana je analogno topološkoj semantici sistema **GL**. Istaknimo samo da se definira $x \Vdash [n]A$ ako postoji $U \in \mathcal{T}_n$ takav da je $x \in U$ i za sve $y \in U$ takve da je $y \neq x$ vrijedi $y \Vdash A$.*

Kažemo da je formula valjana na politopološkom prostoru $(X, (\mathcal{T}_n)_{n\in\mathbb{N}})$ ako je istinita u svakoj točki svakog politopološkog modela $(X, (\mathcal{T}_n)_{n\in\mathbb{N}}, V)$.

Uočimo da vrijedi $x \Vdash \langle n\rangle A$ ako i samo ako je $x \in d_n\{y \in X : y \Vdash A\}$

Istaknimo teorem adekvatnosti topološke semantike za **GLP**.

Teorem 20. *Neka je $(X, (\mathcal{T}_n)_{n\in\mathbb{N}})$ politopološki prostor takav da za svaki $n \in \mathbb{N}$ vrijedi:*

(1) $(X, \mathcal{T}_n)$ je raspršen topološki prostor
(2) $\mathcal{T}_n \subseteq \mathcal{T}_{n+1}$ (tj. $\mathcal{T}_{n+1}$ je finija topologija od $\mathcal{T}_n$)
(3) za svaki $S \subseteq X$ vrijedi $d_n S \in \mathcal{T}_{n+1}$

*Tada je svaki teorem sistema **GLP** valjan na $(X, (\mathcal{T}_n)_{n\in\mathbb{N}})$.*

Dokaz ovog teorema prepuštamo čitatelju (detalji se mogu pronaći i u radu [8]).

Politopološke prostore za koje vrijede pretpostavke prethodnog teorema zovemo **GLP**-*prostori*. Potpunost sistema **GLP** u odnosu na **GLP**-prostore dokazana je u članku [1]. Detaljnije o dokazu potpunosti govori se i u [8].{00}

Bibliografija

[1] L. Beklemishev, D. Gabelaia: Topological completeness of provability logic GLP, *Annals of Pure and Applied Logic* 164 (2013) 1201–1223.

[2] P. Blackburn, M. de Rijke, Y. Venema: *Modal Logic*, Cambridge University Press, 2001.

[3] G. Boolos: *The Logic of Provability*, Cambridge University Press, 1995.

[4] L. Esakia: Dijagonalne konstrukcije, Löbova formula i Cantorovi raspršeni prostori, u: *Istraživanja u logici i semantici*, str. 128-–143, Metsniereba, Tbilisi 1981. (na ruskom jeziku)

[5] G. Japaridze: Polimodalna logika dokazivosti, u: Intenzionalne logike i logička sturktura teorija, str. 16–48, Metsniereba, Tbilisi 1988. (na ruskom jeziku)

[6] J. Garson: Modal logic, u: E. N. Zalta (ur.) *The Stanford Encyclopedia of Philosophy*, Stanford University, 2016. (pristupljeno 16. 2. 2017. na https://plato.stanford.edu/entries/logic-modal/)

[7] I. Gavran, M. Vuković: Logička analiza hibridnih sustava, *Poučak* 58 (2014) 4–16.

[8] L. Mikec: *Topološka potpunost logika dokazivosti* (diplomski rad), Prirodoslovno-matematički fakultet – Matematički odsjek, 2016. (pristupljeno 16. 2. 2017. na https://www.math.pmf.unizg.hr/sites/default /files/pictures/mikec-toplosk...)

[9] P. Smith: *An Introduction to G"odel's Theorems*, Cambridge University Press, 2007.

[10] C. Smorynski: *Self–Reference and Modal Logic*, Springer, 1985.

[11] Š. Ungar: *Opća topologija* (materijali za kolegij), Zagreb 2012. (pristupljeno 16. 2. 2017. na https://web.math.pmf.unizg.hr/ ungar/NASTAVA/OT/)

[12] M. Vuković: *Matematička logika*, Element, Zagreb 2009.

---

[1] Ovaj pregledni članak je nastao na osnovi diplomskog rada [8].
[2] Kurt Gödel (1906–1978), austrijski matematičar.
[3] Još jedna motivacija je potreba da se razriješe poteškoće oko materijalne implikacije, o čemu se nešto detalja može pronaći u udžbeniku [12].
[4] Ovo je standardna terminologija u teorijskom računarstvu. Agent može biti osoba, ali i robot i sl.
[5] Saul Kripke (r. 1940), američki filozof i logičar.
[6] Martin Löb (1921–2006), njemački matematičar.
[7] Na adresi http://www.logicmatters.net/igt/godel-without-tears .
[8] Robert M. Solovay (r. 1938), američki matematičar.
[9] Leo Esakia (1934–2010), gruzijski matematičar.
[10] Giorgi Japaridze (r. 1961), gruzijski logičar.
[11] Polimodalni sistemi razmatraju se i u članku [7].

ISSN 1334-6083