Teorija dokaza: Što i zašto?

Edi Pavlović

Sveučilište u Rijeci,
26. srpnja 2021.

Prije nego počnemo...

Pretpostavke: ne pretpostavlja nikakvo predznanje logike. Ali, vjerovatno će biti prebrzo za one bez predznanja. Izlaganje se (nadamo se) snima.

Dva skoka u kompleksnosti tokom predavanja.

Pitanja tokom izlaganja za one koji bi htjeli znati više.

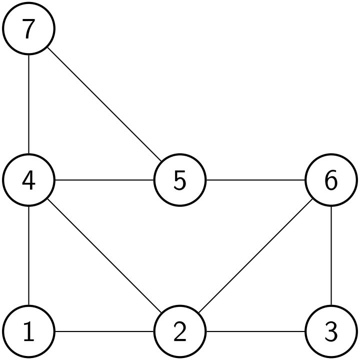
+ snimke dužeg izlaganja na sličnu temu (na engleskom).

Terminologija nije potpuno standardna.

Logika (shvaćena vrlo široko)

Primjer „logičkog“ zadatka:

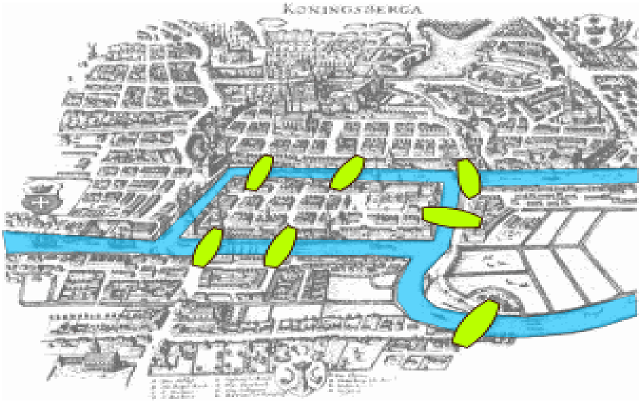
1. Nacrtajte ovu sliku bez da podignete olovku ili prijeđete istom linijom dvaput:



2. Možete li naći različita rješenja?

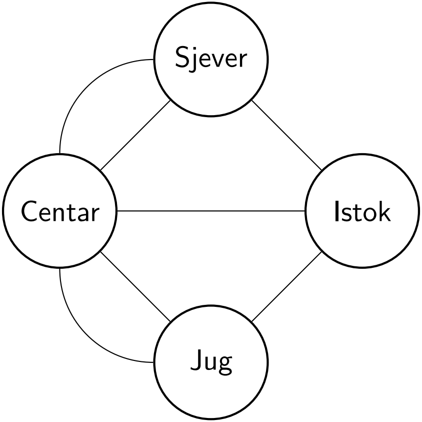
Formalni pristup

3. Sedam mostova Königsberga (1736): nađite put preko svih mostova bez da i jedan prijeđete dvaput:



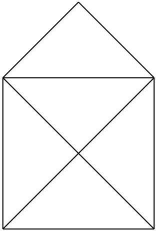
Formalni pristup

Možemo upotrijebiti istu metodu kao i u prethodnom zadatku:



Formalni pristup

4. Nacrtajte ovaj lik bez da podignete olovku ili prijeđete istom linijom dvaput:



5. Možete li naći različita rješenja?

Formalni pristup

Formalizam je *apstrakcija* - opis situacije lišen većine detalja.

Budući da je opis manji, izvlačenje informacija o situaciji je lakše.

Ovo nam omogućava da izvučemo

1. istu količinu informacija u kraćem vremenu (Königsberg), ili
2. više informacija (kućica).

Formalizam *primjenjujemo* tako da ga dopunimo detaljima pojedinačne situacije - informacije koje izvučemo će sada također biti primjenjene.

Korisnost primjene formalizma usko se oslanja na činjenicu da raspolažemo samo ograničenim resursima, bilo pažnje, vremena, sjećanja i sl. u slučaju mozga ili memorije, procesorske snage, propusnosti itd. u slučaju računala.

Malo terminologije

Izvlačenje informacija nazivamo **zaključivanjem**.

Deduktivno zaključivanje: sigurnost zaključaka barem je jednaka sigurnosti početnih informacija.

Kombinaciju početnih informacija i zaključka nazivamo *argumentom*.

Argument je *valjan* ukoliko **uvijek** čuva sigurnost. Kod valjanog argumenta kažemo da zaključak („konkluzija“) slijedi iz/je posljedica početnih informacija („premisa“).

Logiku možemo shvatiti kao kolekciju valjanih argumenata (u nekom formalizmu).

Različiti formalizmi i različiti kriteriji sigurnosti daju različite logike.

Propozicijska logika

Započnimo sa (naj?)jednostavnijim formalizmom.

Simboli	**Namjeravana primjena**	**Naziv**
$p, q, r, \ldots$	jednostavne činjenice	propozicionalne varijable
$\wedge$	sastavni veznici 'i','no','ali'...	konjunkcija
$\vee$	rastavni veznici 'ili', 'bilo'...	disjunkcija
$\rightarrow$	pogodbena konstrukcija 'ako... onda'	implikacija
$\neg$	negativna konstrukcija 'nije...'	negacija
(,)		zagrade

Rečenice stvaramo jedino prema sljedećim pravilima

1. Propozicionalne varijable su rečenice,
2. $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ je rečenica jedino kad su A i B obje rečenice,
3. $\neg A$ je rečenica jedino kad je A rečenica.

Zadnja primjena pravila određuje *glavni veznik* rečenice, a ukupni broj upotrijebljenih pravila njenu *kompleksnost*.

Propozicijska logika

Kriterij sigurnosti: **istinitost** - od dva moguća svojstva, istinitosti i neistinitosti, prvo je poželjno.

Propozicionalne varijable su istinite (I) ili neistinite (N) neovisno o bilo kojoj drugoj rečenici.

Ostale rečenice slijede pravila za stvaranje:

- $A \wedge B$ je I jedino kad su A i B obje I.
- $A \vee B$ je N jedino kad su A i B obje N.
- $A \rightarrow B$ je N jedino kad je A I, a B N.
- $\neg A$ je I jedino kad je A N.

Definicija valjanosti sada postaje:

ako su sve početne informacije („premise“) I, onda je zaključak („konkluzija“) I.

Propozicijska logika

Primjetimo dva intuitivna svojstva:

Slabljenje opisa: Ako je rečenica posljedica općenitog opisa situacije, onda je posljedica svake pojedinačne situacije na koju se taj opis primjenjuje.

Neovisnost od opisa: Ako je rečenica posljedica opisa situacije, onda je posljedica svakog drugog opisa iste situacije.

Sve što trebamo?

1. Popis posljedica opisa situacije duži je od samog opisa.
   $\Rightarrow$ Bolji je pristup pitanje-odgovor, kada provjeravamo je li pojedinačna tvrdnja posljedica opisa situacije.
2. Sama je logika *puno* duža od opisa situacije.
   $\Rightarrow$ Problem kompaktnog opisa logike.
   $\Rightarrow$ Problem učinkovitog pretraživanja logike.

6.* Kako znamo da su duži?

Opis logike

Prvo, možemo smanjiti formalizam (zbog neovisnosti od opisa):
$A \wedge B \equiv \neg(A \to \neg B)$
$A \vee B \equiv \neg A \to B$
Dovoljno je opisati logiku koja sadrži samo prop. varijable, $\to$, i $\neg$.

Najučestalija metoda opisa - aksiomatski sustavi.

Sve primjene sljedećih rečenica („aksioma"):

1. $A \to (B \to A)$,
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
3. $(A \to B) \to (\neg B \to \neg A)$,
4. $\neg\neg A \to A$,
5. $A \to \neg\neg A$,

te načelo („pravilo"):

ako imamo A i $A \to B$, možemo dobiti i B (modus ponens, MP).

Dokazivanje aksiomima

Dokazivanje: proces odlučivanja da li je konkluzija B posljedica premisa $A_1, A_2, ..., A_n$.

Ukoliko od bilo kojih primjena aksioma, koristeći načelo MP, dobijemo $A_1 \to (A_2 \to (\ldots \to (A_n \to B)))$, onda je B posljedica premisa $A_1, A_2, ..., A_n$ (pišemo kao $A_1, A_2, ..., A_n \vdash B$).

7.* Provjerite da li $A \vdash A$.

$$\dfrac{\dfrac{A\to(B\to A)}{A\to(A\to A)} \qquad \dfrac{\dfrac{A\to(B\to A)}{A\to((A\to A)\to A)} \qquad \dfrac{(A\to(B\to C))\to((A\to B)\to(A\to C))}{(A\to((A\to A)\to A))\to((A\to(A\to A))\to(A\to A))}}{(A\to(A\to A))\to(A\to A)}}{A\to A}$$

Aksiomatski sustavi su izrazito nepraktična metoda dokazivanja:

1. Rastu nepredvidivo (i proždiru resurse),
2. Zahtjevaju inventivnost (što u praksi najćešće znači pokušaje i pogreške).

Dokazivanje prirodnom dedukcijom

Da bi se izbjegle manjkavosti aksioma, u 1930ima su neovisno Gerhard Gentzen i Stanisław Jaśkowski predložili sustave *prirodne dedukcije*, koji sadrže samo pravila, ne i aksiome.

Ukoliko pretpostavimo premise, moramo dobiti i konkluziju, primjenom pravila i na osnovi tih premisa.

Pretpostavka, PI: Možemo pretpostaviti bilo koju rečenicu:

$$\mathrm{A}^i \qquad\qquad \text{i} \quad (i) \quad A \quad \mathrm{PI}$$

8. Provjerite da li $A \vdash A$.

Da li ovo pravilo čuva sigurnost (t.j. istinitost)?

Sva ostala pravila dijele se na pravila uvođenja (**I**, introdukcija), i iskorištavanja (E, eliminacija).

Prirodna dedukcija

Implikacija:

$$\dfrac{\begin{matrix}[A^i] \\ \vdots \\ B\end{matrix}}{A \to B} \to \mathrm{I},\ \mathrm{i} \qquad\qquad \dfrac{A \to B \qquad A}{B} \to \mathrm{E}$$

i	(i)	A	PI	Γ_1	(i)	$A \to B$	
Γ	(j)	B		Γ_2	(j)	A	
Γ'	(k)	$A \to B$	$\to$ I, i,j	Γ_1, Γ_2	(k)	B	$\to$ E, i, j

Da li ova pravila čuvaju istinitost?

Ako su sve rečenice u Γ' istinite, onda je $A \to B$ istinita?
$\Rightarrow$ Pretpostavimo da je do ove točke istinitost očuvana. Dakle, ako su sve rečenice u Γ istinite, onda je istina i B. Γ je upravo Γ' i (možda) A. Stoga, ako su sve rečenice u Γ' istinite, onda (i) ako je A istina, istina je i B, pa i $A \to B$, a (ii) ako A nije istina onda je $A \to B$ opet istina ($A \to B$ je neistina samo kada je A istina a B neistina).

Prirodna dedukcija

Negacija:

$$\dfrac{\begin{matrix}[A]^i & & [A]^i \\ \vdots & & \vdots \\ B & & \neg B\end{matrix}}{\neg A}\ \neg\text{I,i} \qquad\qquad \dfrac{\neg\neg A}{A}\ \neg\text{E}$$

i	(i)	A	PI
Γ	(j)	B	
Γ	(k)	$\neg B$	
Γ'	(l)	$\neg A$	$\neg$I, i, j, k

Γ	(i)	$\neg\neg A$	
Γ	(j)	A	$\neg$E, i

Ako su sve rečenice u Γ' istinite, onda je $\neg A$ istina?
$\Rightarrow$ Pretpostavimo opet da je do ove točke istinitost očuvana. Onda, ako su sve rečenice u Γ' istinite, onda ako je A istina, istina su i B i $\neg B$. Ali to nije moguće. Dakle, A nije istina, pa je $\neg A$ istina.

Prirodna dedukcija

9. Provjerite za pravila eliminacije.

Vidjeli smo da niti jedno pravilo ne može prvo uzrokovati gubitak očuvanja istinitosti.

Dakle, ako možemo dokazati konkluziju iz premisa, onda, ako su premise istinite, istinita je i konkluzija, te je argument stoga valjan.

Ovo svojstvo prirodne dedukcije naziva se *pouzdanost*.

Primjetite da smo stekli informaciju (zaključili nešto) o samom sustavu dokazivanja, što je područje interesa *teorije dokaza*.

Teorija dokaza proučava svojstva (sustava) dokaza.

Teorija dokaza

Iako sami pojedinačni dokazi izgledaju značajno drugačije ovisno o metodi koju usvojimo, naš dokaz izgleda potpuno jednako u oba slučaja.

Teorija dokaza je *apstrakcija*.

Trebamo naći odgovarajući formalizam, koji će nam omogućiti da izvučemo najveći broj traženih informacija o dokazima u najkraćem mogućem vremenu.

Teorija dokaza

Primjer traženja dokaza:

$A \to B \vdash \neg B \to \neg A$

1	(1)	$A \to B$	PI
2	(2)	$\neg B$	PI
3	(3)	A	PI
1,3	(4)	B	$\to$E, 1,3
	( )		
	( )		
1,2	(5)	$\neg A$	$\neg$ I, 3,2,4
1	(6)	$\neg B \to \neg A$	$\to$I, 2,5

Primjetite da smo se mogli zaustaviti na bilo kojem redu i imali bi *neki* dokaz (ne nužno traženi). Pravila možemo promatrati kao metode pretvaranja dokaza u (duže) dokaze.

Teorija dokaza

Potraga za dokazom u prirodnoj dedukciji događa se istovremeno u dva smjera:

Premise $\Downarrow$

Eliminacija $\Downarrow$

Atomi

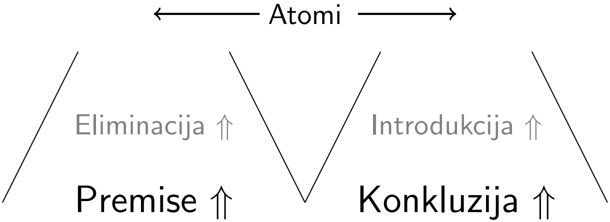
Introdukcija $\Uparrow$

Konkluzija $\Uparrow$

Posljedično, ponekad se dva smjera neće savršeno spojiti. Također, moramo biti oprezni sa uvođenjem novih pretpostavki.

Teorija dokaza

Da bi riješili prvi problem, ovu sliku možemo promijeniti na slijedeći način (o drugom kasnije):



Upravo ovo radimo kada prijeđemo na **račun sekvenata**.

Račun sekvenata

Apstrakcija od pojedinačnih sustava prirodne dedukcije.

Osnovna jedinica – sekvent: $\Gamma \Rightarrow \Delta$

Shvaćen kao: Ako je sve na lijevoj strani (Γ) istinito, onda je *nešto* na desnoj strani (Δ) istinito $\longrightarrow$ generalizacija valjanog argumenta/ uspješnog dokaza.

Γ i Δ su konačni popisi formula (možda prazni) u kojima poredak nije bitan, a elementi se mogu ponavljati.

Pravila

Inicijalni sekvent:

$\Gamma, p \Rightarrow \Delta, p$, gdje je p propozicionalna varijabla, odgovara najjednostavnijem slučaju pravila PI.

Ostala pravila podijeljena su na desna (R, „right") koja odgovaraju pravilima uvođenja – kako dobiti simbol? i lijeva (L) koja odgovaraju pravilima iskorištavanja – kako ih upotrijebiti?

$$\frac{\Gamma \Rightarrow \Delta, A \qquad B, \Gamma \Rightarrow \Delta}{A \to B, \Gamma \Rightarrow \Delta}\,\mathrm{L}{\to} \qquad\qquad \frac{A, \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \to B}\,\mathrm{R}{\to}$$

$$\frac{\Gamma \Rightarrow \Delta, A}{\neg A, \Gamma \Rightarrow \Delta}\,\mathrm{L}\neg \qquad\qquad \frac{A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg A}\,\mathrm{R}\neg$$

Slažemo ih u *stablo* čiji su vrhovi inicijalni sekventi, a baza jedan *završni* sekvent. Kažemo da je stablo *izvođenje* toga sekventa.

Pravila

R$\rightarrow$ je lakše razumjeti ako je Δ prazan:

$$\frac{A, \Gamma \Rightarrow \; B}{\Gamma \Rightarrow \; A \rightarrow B} \, R\rightarrow$$

Ovakvo smo zaključivanje već vidjeli kada smo dokazivali očuvanje istine za $\rightarrow$I: ako su A i Γ svi istiniti, onda je istina i B. Dakle, ako je sve u Γ istina, istina je i $A \rightarrow B$.

No, ovdje je to iskazano konciznije. Slučaj negacije je sličan.
10.* Provjerite.

Sada imamo formalizaciju meta-teorije prirodne dedukcije. Ona nam i dalje omogućava izvlačenje informacija o prirodnoj dedukciji, budući da:

$$\Gamma \vdash A \rightarrow \Gamma \Rightarrow A, \text{ i}$$

$$\Gamma \Rightarrow \Delta \rightarrow \Gamma \vdash \bigvee \Delta.$$

Svojstva računa sekvenata G3cp

G3cp ima nekoliko svojstava koja zajedno jamče da će stabla biti izrazito predvidiva, do te mjere da ćemo njihov oblik, veličinu i sadržaj moći predvidjeti samo promatranjem završnog sekventa.

Ovo se svojstvo stabala naziva **analitičnost**.

Svojstva računa sekvenata G3cp

Generalizacija inicijalnih sekvenata: za bilo koji A možemo izvesti $A, \Gamma \Rightarrow \Delta, A$.

Provjeravamo (po redu) za svaku kompleksnost A.

Ako je A propozicionalna varijabla p (kompleksnost 0), onda je ovo samo inicijalni sekvent.

Inače provjeravamo za svaki glavni veznik. Ako je to implikacija $B \to C$, onda

$$\dfrac{\dfrac{\dfrac{\text{prema pretpostavci}}{B, \Gamma \Rightarrow \Delta, C, B} \qquad \dfrac{\text{prema pretpostavci}}{C, B, \Gamma \Rightarrow \Delta, C}}{B, B \to C, \Gamma \Rightarrow \Delta, C}\,\mathrm{L}{\to}}{B \to C, \Gamma \Rightarrow \Delta, B \to C}\,\mathrm{R}{\to}$$

Slično za negaciju.

11. Provjerite.

Svojstva računa sekvenata G3cp

Slabljenje (weakening): ako možemo izvesti sekvent $\Gamma \Rightarrow \Delta$, onda možemo izvesti sekvent $C, \Gamma \Rightarrow \Delta$, iste visine stabla.

Jednostavno dopišemo C na svaki sekvent u stablu. Npr.

$$\dfrac{\dfrac{\dfrac{A \Rightarrow A, B}{\Rightarrow A, A \to B}\,\mathrm{R}\!\to \qquad A \Rightarrow A}{(A \to B) \to A \Rightarrow A}\,\mathrm{L}\!\to}{\Rightarrow ((A \to B) \to A) \to A}\,\mathrm{R}\!\to$$

$$\downarrow$$

$$\dfrac{\dfrac{\dfrac{C, A \Rightarrow A, B}{C \Rightarrow A, A \to B}\,\mathrm{R}\!\to \qquad C, A \Rightarrow A}{C, (A \to B) \to A \Rightarrow A}\,\mathrm{L}\!\to}{C \Rightarrow ((A \to B) \to A) \to A}\,\mathrm{R}\!\to$$

Isto tako možemo izvesti i $\Gamma \Rightarrow \Delta, C$.

Svojstva računa sekvenata G3cp

Ostala svojstva predstavljamo bez demonstracije jer je previše duga i kompleksna.

Invertibilnost (invertibility): neka $\vdash_n \Gamma \Rightarrow \Delta$ znači da je $\Gamma \Rightarrow \Delta$ izvodiv sa visinom n. Onda:

1. Ako $\vdash_n A \to B, \Gamma \Rightarrow \Delta$ onda $\vdash_n \Gamma \Rightarrow \Delta, A$ i $\vdash_n B, \Gamma \Rightarrow \Delta$.
2. Ako $\vdash_n \neg A, \Gamma \Rightarrow \Delta$ onda $\vdash_n \Gamma \Rightarrow \Delta, A$.
3. Ako $\vdash_n \Gamma \Rightarrow \Delta, A \to B$ onda $\vdash_n A, \Gamma \Rightarrow \Delta, B$.
4. Ako $\vdash_n \Gamma \Rightarrow \Delta, \neg A$ onda $A, \vdash_n \Gamma \Rightarrow \Delta$.

Svojstva računa sekvenata G3cp

Sužavanje (contraction):

1. Ako $\vdash_n D, D, \Gamma \Rightarrow \Delta$ onda $\vdash_n D, \Gamma \Rightarrow \Delta$.
2. Ako $\vdash_n \Gamma \Rightarrow \Delta, D, D$ onda $\vdash_n \Gamma \Rightarrow \Delta, D$.

Ovo je svojstvo povezano sa neovisnošću od opisa – npr. D, D, Γ opisuje istu situaciju kao i D, Γ.

Svojstva računa sekvenata G3cp

Uklanjanje Reza (Cut elimination): neka je neki sekvent izvodiv uz upotrebu pravila Reza (Cut):

$$\frac{\Gamma_1 \Rightarrow \Delta_1, A \qquad A, \Gamma_2 \Rightarrow \Delta_2}{\Gamma_1, \Gamma_2 \Rightarrow \Delta_1, \Delta_2}\ \mathrm{Cut}$$

onda je taj sekvent izvodiv i bez ovoga pravila.

Rez

Zašto trebamo Rez?

Sažetost:
G. Boolos, 1984: „Don't eliminate cut" (Ne uklanjajte Rez) – predstavlja izvođnje koje, uz upotrebu Reza, sadrži 3175 simbola. Bez reza, dug je preko (nekoliko kvinitilijuna više ili manje) 10^{38} simbola.

Radi usporedbe, od Velikog je praska prošlo 4,3x10^{26} nanosekundi.

Zašto bi ga se onda rješavali?

Svojstvo podformule: svaka rečenica koja se pojavljuje u izvođenju sekventa $\Gamma \Rightarrow \Delta$, ukoliko ovo ne sadrži Rez, je podformula (t.j. korak u stvaranju rečenice) neke rečenice u završnom sekventu.

$\Rightarrow$ ključan element analitičnosti.

Rez

Primjer:

$$\dfrac{\dfrac{P \Rightarrow P, Q}{P \Rightarrow P \vee Q}\,\mathrm{R}\vee \qquad \dfrac{\dfrac{\dfrac{P, Q, P \Rightarrow Q}{Q, P \Rightarrow P \to Q}\,\mathrm{R}\!\to}{P \Rightarrow Q \to (P \to Q)}\,\mathrm{R}\!\to \qquad \dfrac{\dfrac{P, Q, Q \Rightarrow Q}{Q, Q \Rightarrow P \to Q}\,\mathrm{R}\!\to}{Q \Rightarrow Q \to (P \to Q)}\,\mathrm{R}\!\to}{P \vee Q \Rightarrow Q \to (P \to Q)}\,\mathrm{L}\vee}{P \Rightarrow Q \to (P \to Q)}\,\mathit{Cut}$$

$$\downarrow$$

$$\dfrac{\dfrac{P, Q, P \Rightarrow Q}{P, Q \Rightarrow P \to Q}\,\mathrm{R}\!\to}{P \Rightarrow Q \to (P \to Q)}\,\mathrm{R}\!\to$$

Konzistentnost

Svojstvo podformule lako vodi do konzistentnosti:

Račun sekvenata je **konzistentan** ukoliko prazni sekvent,

$$„ \Rightarrow “$$

nije izvediv.

Korolar (Konzistentnost)

G3cp je konzistentan.

Ako je prazni sekvent izvediv, onda je izvediv bez Reza. Dakle, prema svojstvu podformule, svaki sekvent u stablu može biti samo prazan. No, nijedan inicijalni sekvent nije prazan. Dakle, to stablo nema inicijalnih sekvenata, te stoga ne postoji.

Odlučivost

G3cp im jednostavan postupak potrage za izvodima.

Aktivni sekvent: sekvent $\Gamma \Rightarrow \Delta$ je aktivan ako ne postoji propozicionalna varijabla p koja je i u Γ i u Δ.

Potraga za izvodima: počevši od završnog sekventa $\Gamma \Rightarrow \Delta$, gradimo stablo (prema gore) primjenjivanjem pravila na aktivne sekvente u ciklusu:

L$\neg$; R$\neg$; L$\rightarrow$; R$\rightarrow$

Ako ne možemo primjeniti ni jedno pravilo na aktivni sekvent zaustavimo potragu. Tada je potraga *neuspjela*. Ako naprotiv više nema aktivnih sekvenata potraga je *uspjela*.

Odlučivost

Kompleksnost sekventa, k: zbroj kompleksnosti svih rečenica u njemu.

Lako je vidjeti da

Lema (Odlučivost)

Potraga za izvodom završava u konačnom broju koraka.

Za svako pravilo P:

$$\frac{\Gamma' \Rightarrow \Delta' \qquad [\Gamma'' \Rightarrow \Delta'']}{\Gamma \Rightarrow \Delta} \text{P}$$

vrijedi da $k(\Gamma \Rightarrow \Delta) > k(\Gamma' \Rightarrow \Delta')$ i $k(\Gamma \Rightarrow \Delta) > k(\Gamma'' \Rightarrow \Delta'')$. Pošto opada, kompleksnost će s vremenom biti 0 (samo propozicionalne varijable). Tada imamo ili inicijalni sekvent ili je potraga neuspjela.

Primjetite da ovo ne bi vrijedilo kada bi Rez bilo jedno od pravila.

Na kraju...

Račun sekvenata nudi sažet opis logike.

Istovremeno, izvodi u računu sekvenata rastu predvidivo i ne zahtjevaju inventivnost.

Stoga su koristan alat za zaključivanje sa ograničenim resursima. Nadalje, njihova predvidivost omogućava mnoštvo primjena u filozofiji, informatici, matematici i lingvistici.

Hvala na pažnji!

Daljnje čitanje

Uvod u teoriju dokaza:

Negri, S. & von Plato, J. (2001) *Structural Proof Theory*, Cambridge University Press.

Prirodna dedukcija i njen odnos sa računom sekvenata:

von Plato, J. (2013) *Elements of Logical Reasoning*, Cambridge University Press.

Kratki kurs „Introduction to Proof Theory“, CEU Beč, 19. veljače 2021:

Prvi dio

Drugi dio