Uvod u matematičku logiku

Milenko Mosurović

Univerzitet Crne Gore

studijska godina 2020/21.

Uvodne napomene o predmetu

- Fond časova 2+1.
- Kolokvijum XI nedenje nastave nosi 60 bodova (popravni XIII nedelje).
- Završni ispit nosi 40 bodova.
- Prelazna ocjena se dobija za 50 ili više bodova. Tačnije: 0-49 ocjena F, 50-59 ocjena E, 60-69 ocjena D, 70-79 ocjena C, 80-89 ocjena B i 90-100 ocjena A.
- Literatura: Knjiga u elektronskom obliku može se naći na sajtu www.ucg.ac.me od autora S. Vujoševića i Ž. Kovijanić.

Napomena o jezicima

- Neka je Σ neprazan skup koji nazivamo azbukom, a njegove elemente slovima azbuke.
- **Def.** Skup svih riječi nad azbukom Σ, u oznaci Σ', je minimalni skup koji zadovoljava sledeća svojstva: 1) prazna riječ λ pripada Σ' (tj. $\lambda \in \Sigma'$), 2) Ako je $\omega \in \Sigma'$ i $a \in \Sigma$ onda je i $\omega a \in \Sigma'$ (tj. nadovezivanjem/konkatenacijom slova a na već postojeću riječ ω dobijamo novu riječ ωa).
- Primjer. Ako je $\Sigma = \{x, y\}$ onda je $\Sigma' = \{\lambda, x, y, xx, xy, yx, yy, xxx, xxy, ...\}$.
- **Def.** Neka je Σ' skup svih riječi nad azbukom Σ. Za skup L kažemo da je jezik nad azbukom Σ ako je $L \subset \Sigma'$.
- Drugim riječima ako od skupa svih riječi izdvojimo neke koje su važeće onda nam te riječi čine jezik. Npr. KOŹE, KIŚELO, MLIJEKO jesu riječi crnogorskog jezika a ZZRVFT nije riječ crnogorskog jezika i ako je to riječ nad crnogorskom azbukom.

Uvod o logikama

- Logika se tradicionalno shvata kao nauka o pravilima korektnog zaključivanja. U zaključivanju sa jednog skupa rečenica prelazimo na novu rečenicu. Rečenice od kojih polazimo su *pretpostavke*, a rezultat je *zaključak*.
- Zaključivanje je logički ispravno ako "čuva istine" (SALVA VERITATE).
- Dedukcija je zaključivanje u kome koristimo samo pravila koja čuvaju istine.
- Induktivno zaključivanje (na osnovu nekoliko primjera zaključimo opšte svojstvo) ne čuva istine.
- Napomena: Matematička indukcija je dedukcija tj. čuva istine.

- Bitna su zaključivanja u kojima se javljaju veznici (iskazni: *i, ili, ako, nije*; predikatski: *za svako, postoji,...*). Jer se korektnost zaključivanja bazira na smislu veznika.
- Obično pri zaključivanju prelazimo sa jednog skupa formi na novu formu pa se otuda koristi i termin formalni pristup (formalna logika)
- Primjer. Ako pretpostavimo A *i* B, možemo zaključiti B *i* A.
- Kurs obuhvata dva dijela: Iskazna logika i Predikatska logika prvog reda (kraće Predikatska logika)
- Biće spomenute i intuicionistička logika, modalne logike, deskriptivne logike,...

Uvod- šta proučavamo

I kod iskazne i kod predikatske logike proučavamo 4 cjeline

1. Sintaksa (tj. koje simbole koristimo to nazivamo jezikom, koji su važeći nizovi simbola i to nazivamo formulama)
2. Semantika (tj. kako interpretiramo formule odnosno određujemo njihovo značenje tj. istinitosnu vrijednost).
3. Formalni pristup (na osnovu aksioma i pravila izvođenja dolazimo do istina). Napomena: u udžbeniku se ovo naziva sintaksa - sintaksni pristup.
4. Odnos 2 i 3 (da li nam semantički pristup i formalni pristup daju iste istine - Teorema korektnosti i Teorema potpunosti).

ISKAZNA LOGIKA

Iskazna logika-uvod

- Rečenica je iskaz ako možemo sa smislom postaviti pitanje njene istinitosti.
- Ako takva rečenica može biti samo istinita ili neistinita, govorimo o dvovalentnoj logici. Ako istinitosnih vrijednosti ima više od dvije, logika je viševalentna.
- Primjeri. $3|15$, $3|17$, $\exists x(x^2+1=0)$, Uvod u logiku, ...
- Elementarne iskaze možemo zamijeniti slovima npr. A, B, s_0, s_5 a složene dobijamo ako koristimo iskazne veznike: $\wedge$ - konjunkcija čita se "*i*", $\vee$ - disjunkcija čita se "*ili*", $\to$ - implikacija čita se "*onda*" i $\neg$ - negacija čita se "*nije*".
- Primjeri. $(A \vee B)$, $(s_0 \wedge \neg s_5)$

Sintaksa iskazne logike

- **Def.** *Jezik iskazne logike* je skup $\mathcal{L} = P \cup \{\wedge, \vee, \rightarrow, \neg\} \cup \{(,)\}$, gdje je $P = \{s_0, s_1, s_2, ...\}$ prebrojiv skup iskaznih simbola.
- Simbole skupa P nazivamo i iskaznim slovima i to su nelogički simboli jer se mogu mijenjati a ostali simboli su logički simboli.
- **Def.** *Iskazne formule* definišemo induktivno na sledeći način:
  1. Iskazna slova su iskazne formule - nazivamo ih još i elementarne (atomarne) fromule;
  2. Ako su A i B iskazne formule, onda su $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ i $\neg A$ iskazne formule;
  3. Iskazne formule se mogu dobiti isključivo konačnom primijenom prethodne dvije stavke.
- Skup svih iskaznih formula označavamo sa F.

- Da li su sledeće rečenice iskazne formule: s_3, $s_5 s_1 \neg$, $s_7 \vee s_3$, $(p \wedge q)$, $(s_0 \vee s_1 \vee s_2)$, $((\neg s_3 \to \neg s_2) \to (s_2 \to s_3))$?
- Dogovor. Spoljne zagrade možemi izostaviti. Koristićemo i slpva p, q, r, p_1,... kao zamijenu za neko od slova $s_i \in P$.
- Drugačija definicija: $P \subset F$;
  $A, B \in F \quad \Rightarrow \quad (A \wedge B), (A \vee B), (A \to B), \neg A \in F$.
- $F = \cup_{n=0}^{\infty} F_n$, gdje je $F_0 = P$,
  $F_{n+1} = \{(A \wedge B), (A \vee B), (A \to B), \neg A \ : \ A, B \in \cup_{k=0}^{n} F_k\}$
- Skup podformula formule A u oznaci $sub(A)$ možemo definisati induktivno sa: $sub(s_i) = \{s_i\}$; $sub(\neg A) = sub(A) \cup \{\neg A\}$; $sub(A * B) = sub(A) \cup sub(B) \cup \{A * B\}$, gdje je $* \in \{\wedge, \vee, \to\}$. IF $B \in sub(A)$ je podformula od A – javlja se bar jednom u A.

Zbog induktivne definicije formule mnogi dokazi se izvode *indukcijom po složenosti formule*. To sada ilustrujemo.

Lema. Svaka formula ima jednak broj lijevih i desnih zagrada. **Dokaz.** Neka je $A \in F$ proizvoljna formula. Sa l_A i d_A označavamo redom broj lijevih i broj desnih zagrada u formuli A.

- Ako je A elementarna formula ti. $A = s_i \in P$ onda je $l_A = d_A = 0$ pa tvrđenje važi.
- Neka je A složena formula i neka tvrđenje važi za sve formule manje složenosti od formule A. Tada A ima jedan od oblika $(B \wedge C), (B \vee C), (B \rightarrow C), \neg B$. Razmotrimo slučaj $A = (B \wedge C)$. Tada je $l_A = 1 + l_B + l_C$ i $d_A = d_B + d_C + 1$. Kako je po indukcijskoj pretpostavci (kraće ind.p.p) $l_B = d_B$ i $l_C = d_C$ (jer B i C imaju manju složenost od A) to je $l_A = d_A$. Što je trebalo dokazati. Preostala tri slučaja uradite sami.

Semantika iskazne logike

- Kako tumačiti (istinitosnu vrijednost) iskazne formule?
- s_0 =Uvod, s_1=logiku i $\vee$ =u pa je $s_0 \vee s_1$ = Uvod u logiku.
- Da bi utvrdili istinitost IF (IF -skraćeica od iskazna formula) uvodimo pojam valuacije (ocjene) IF. Koristimo oznaku $\overline{2}$ za skup $\{0, 1\}$.
- **Def.** Preslikavanje $v \; : \; P \to \overline{2}$ je *valuacija iskaznih slova (elementarnih formula)* jezika $\mathcal{L}$.
- Skup svih valuacija označavamo sa 2^P. Ako je $v(p) = 1$ onda je iskaz p istinit (tačan) u suprotnom je neistinit (netačan).
- Primjer. $v(s_0) = 0$, $v(s_1) = 1$, $v(s_2) = 1$, $v(s_3) = 1$, $v(s_4) = 0$, $v(s_5) = 1$, ... ili
$$v \; : \; \begin{pmatrix} s_0 & s_1 & s_2 & s_3 & s_4 & s_5 & \dots \\ 0 & 1 & 1 & 1 & 0 & 1 & \dots \end{pmatrix}$$

- **Def.** Preslikavanje $\overline{v} \ : \ F \to \overline{2}$ je proširenje valuacije $v \in 2^P$ ako zadovoljava sledeća (semantička) pravila:
  1. $\overline{v}(p) = v(p)$ za svako $p \in P$,
  2. $\overline{v}(A \wedge B) = 1$ akko $\overline{v}(A) = 1$ i $\overline{v}(B) = 1$,
  3. $\overline{v}(A \vee B) = 1$ akko $\overline{v}(A) = 1$ ili $\overline{v}(B) = 1$,
  4. $\overline{v}(A \to B) = 0$ akko $\overline{v}(A) = 1$ i $\overline{v}(B) = 0$,
  5. $\overline{v}(\neg A) = 1$ akko $\overline{v}(A) = 0$
- **Teorema.** (o j.p.v.) Svaka valuacija elementarnih formula ima jedinstveno proširenje na sve IF.
- **Dokaz.** Neka su v_1 i v_2 dva proširenja valuacije $v \in 2^P$. Dokažimo da je za svaku formulu $A \in F$ $v_1(A) = v_2(A)$ tj. $v_1 = v_2$. Ako je $A = s_i \in P$ onda je $v_1(A) = v_2(A) = v(A)$. Neka je A složena formula i neka tvrđenje važi za sve formule manje složenosti od formule A. Tada A ima jedan od oblika $(B \wedge C), (B \vee C), (B \to C), \neg B$.

Razmotrimo slučaj $A = (B \vee C)$. Po ind. p.p $v_1(B) = v_2(B)$ i $v_1(C) = v_2(C)$ pa je $v_1(A) = 1$ akko $v_1(B) = 1$ ili $v_1(C) = 1$ akko $v_2(B) = 1$ ili $v_2(C) = 1$ akko $v_2(A) = 1$. Dakle, $v_1(A) = v_2(A)$.
Preostala tri slučaja uradite sami.
Kako je $v_1 = v_2$ tj. sva proširenja se poklapaju što znači da je proširenje jedinstveno.

- Zbog jedinstvenosti proširenja valuacije v obično i $\overline{v}$ označavamo sa v i govorimo o valuaciji IF.
- Primjer. Neka je $A = ((s_0 \to s_3) \to ((s_0 \vee s_3) \to s_0))$. Odrediti $v(A)$, ako je v ranije navedena valuacija.
- $v(s_0) = 0$ i $v(s_3) = 1$ pa je $v(s_0 \to s_3) = 1$ i $v(s_0 \vee s_3) = 1$. Dalje je $v((s_0 \vee s_3) \to s_0) = 0$ i konačno $v(A) = 0$.

- Istinitosna vrijednost formule A iz prethodnog primjera zavisi samo od istinitnosne vrijednosti iskaznih slova s_0 i s_3. Da bi to istakli možemo zapisati $A(s_0, s_3)$.
- Ako je A IF, sa $A(p_1, \ldots, p_n)$ označavamo da su sva iskazna slova koja se javljaju u formuli A neka od $p_1, \ldots, p_n$, ali ne obavezno sva. Tako za prethodni primjer možemo pisati i $A(s_0, s_1, s_2, s_3)$ dok ne možemo pisati $A(s_0)$.
- Neka je $A(p_1, \ldots, p_n)$ IF i $v, w \in 2^P$. Ako je $v(p_i) = w(p_i), i = 1, \ldots, n$ onda je i $v(A) = w(A)$.
- Neka su $A(p_1, \ldots, p_n), A_1, \ldots, A_n$ IF. Tada formulu $A(A_1, \ldots, A_n)$ koja se iz formule A dobija zamenom svih javljanja promenljivih $p_1, \ldots, p_n$ redom formulama $A_1, \ldots, A_n$ nazivamo supstituciona instanca formule A.

Tablica iskazne formule

Imajući u vidu semantiku složenih IF možemo napraviti tablicu:

$v(A)$	$v(B)$	$v(A \wedge B)$	$v(A \vee B)$	$v(A \rightarrow B)$	$v(\neg A)$
0	0	0	0	1	1
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	1	1	0

Primjer. Neka je $A(s_0, s_3) = ((s_0 \rightarrow s_3) \rightarrow ((s_0 \vee s_3) \rightarrow s_0))$. Odrediti valuaciju v za koju je $v(A) = 1$.
Rj. Istinitosna vrijednost IF A zavisi samo od istinitosnih vrjednosti slova s_0 i s_3. Postoje 4 moguće kombinacije za istinitosne vrijednosti ova dva slova. Zato pravimo tablicu.

$v(s_0)$	$v(s_3)$	$v(s_0 \to s_3)$	$v(s_0 \vee s_3)$	$v((s_0 \vee s_3) \to s_0)$	$v(A)$
0	0	1	0	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	1	1	1	1	1

Iz tabele vidimo da npr. za valuaciju $v \in 2^P$ za koju je za svako $i \in N_0$ $v(s_i) = 0$ važi $v(A) = 1$. Naravno takvih valuacija ima beskonačno mnogo. Naime samo za valuacije kod kojih je $v(s_0) = 0$ i $v(s_3) = 1$ važi $v(A) = 0$ a za sve ostale važi $v(A) = 1$.

Napomena. Kad pravimo tablicu obično radi kraćeg zapisa, u zaglavlju tablice, umjesto $v(A)$ pišemo samo A.

Logički zakoni

- **Def.** Kažemo da valuacija $v \in 2^P$ zadovoljava IF A (ili A važi za v) i označavamo sa $v \models A$ ako je $v(A) = 1$.
  Kažemo da je IF A zadovoljiva ako postoji valuacija $v \in 2^P$ tako da je $v \models A$ (tj. $v(A) = 1$).
- **Def.** Za IF A kažemo da je logički zakon ili tautologija i označavamo sa $\models A$ ako za svaku valuaciju $v \in 2^P$ važi $v(A) = 1$.
- Formula $A \to A$ koja je logički zakon prvobitno se nazivala tautologija (ista riječ) a onda se po njoj u iskaznoj logici za svaki logički zakon kaže da je tautologija.
- Logički zakoni su uvjek istiniti (ili prosto rečeno istine). Kako su u logici od posebnog značaja istine onda će nas interesovati da "otkrijemo" one formule koje su logički zakoni tj. tautologije.

Supstitucija ekvivalentnih formula

- **Def.** IF A i B su logički ekvivalentne ako je $v(A) = v(B)$ za svaku valuaciju $v \in 2^P$.
- Zadatak. Dokazati da su IF $(p \wedge q) \wedge r$ i $p \wedge (q \wedge r)$ logički ekvivalentne. Upustvo. Napraviti tablicu i uočiti da im se istinitosne vrijednosti poklapaju.
- Zadatak. Dokazati da su IF A i B logički ekvivalentne akko IF $(A \to B) \wedge (B \to A)$ tautologija.
  Rj. $(\Rightarrow)$. Neka su IF A i B logički ekvivalentne. Treba dokazati da je IF $(A \to B) \wedge (B \to A)$ tautologija.
  Neka je $v \in 2^P$ proizvoljna valuacija tada je $v(A) = v(B)$ (jer su po pretpostavci A i B logički ekvivalentne) pa je $v(A \to B) = 1$ i $v(B \to A) = 1$ (po svojstvu 4 proširenja valuacije) pa je $v((A \to B) \wedge (B \to A)) = 1$ (po svojstvu 2 proširenja valuacije).

Dakle, za proizvoljnu (tj. svaku) valuaciju $v \in 2^P$ važi $v((A \rightarrow B) \wedge (B \rightarrow A)) = 1$ pa je IF $(A \rightarrow B) \wedge (B \rightarrow A)$ tautologija.
($\Leftarrow$) Neka je IF $(A \rightarrow B) \wedge (B \rightarrow A)$ tautologija. Treba dokazati da su IF A i B logički ekvivalentne.
Neka je $v \in 2^P$ proizvoljna valuacija tada je $v((A \rightarrow B) \wedge (B \rightarrow A)) = 1$ po svojstvu 2 proširenja valuacije važi $v(A \rightarrow B) = 1$ i $v(B \rightarrow A) = 1$.
Ako je $v(A) = 1$ onda je (zbog $v(A \rightarrow B) = 1$) $v(B) = 1$; ako je $v(B) = 1$ onda je (zbog $v(B \rightarrow A) = 1$) $v(A) = 1$.
Dakle, za proizvoljnu valuaciju $v \in 2^P$ važi $v(A) = 1$ akko $v(B) = 1$ tj. $v(A) = v(B)$ pa su IF A i B logički ekvivalentne.

- Dogovor. Koristimo $(A \leftrightarrow B)$ kao skraćenicu za IF $((A \rightarrow B) \wedge (B \rightarrow A))$.

- Formula B se javlja u formuli A ako je $B \in sub(A)$ (tj. ako je B podformula od A). Međutim, formula B se može javljati u formuli A i više puta.
- Primjer. IF B sa javlja dva puta u IF $(B \to C) \to B$.
- Napomena. Intuitivno je jasno kako da odredimo broj javljanja formule B u formuli A. Međutim, uvjek je bolje da to precizno matematički definišemo i onda će nam u dokazima biti lakše da koristimo taj pojam.
- **Def.** Broj javljanja IF B u IF A u oznaci $brj(B, A)$ definišemo induktivno na sledeći način: 1) Ako $B \notin sub(A)$ onda je $brj(B, A) = 0$; 2) Ako je $A = B$ onda je $brj(B, A) = 1$; 3) Ako je $A \neq B$ i $A = (C * D)$, gdje je $* \in \{\wedge, \vee, \to\}$, onda je $brj(B, A) = brj(B, C) + brj(B, D)$; 4) Ako je $A \neq B$ i $A = \neg C$ onda je $brj(B, A) = brj(B, C)$.

- Ako su A, B i C IF onda sa $A(B/C)$ označavamo IF koja se dobija kada se u formuli A neka javljanja formule B zamijene formulom C. Primetimo da formula $A(B/C)$ nije jednoznačna i da oznaka $A(B/C)$ podrazumeva i mogućnost da nijedno javljanje formule B u formuli A nismo zamenili sa C.
- Primjer. Neka je $A = (B \to D) \to B$ tada sa $A(B/C)$ označavamo jednu od formula $(B \to D) \to B$, $(C \to D) \to B$, $(B \to D) \to C$ i $(C \to D) \to C$.
- I oznaka $A(B/C)$ može biti precizno definisana (induktivno). Uradite to sami. Upustvo. Npr. ako je $A = B$ onda je $A(B/C) = B$ ili $A(B/C) = C$; ako je $A = (A_1 \vee A_2)$ onda je $A(B/C) = (A_1(B/C) \vee A_2(B/C))$.

- **Lema**(o zamjeni ekvivalentnih formula). Neka su A, B i C IF. Tada,

$$\models (B \leftrightarrow C) \rightarrow (A \leftrightarrow A(B/C)).$$

- Dokaz. Sami indukcijom po složenosti formule A.

Zadaci

Pomoću tablice provjeriti da li su sledeće IF tautologije.

- $p \to (q \to p)$;
- $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$;
- $((p \wedge q) \to r) \leftrightarrow (p \to (q \to r))$;
- $(p \wedge q) \to p)$;
- $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$;
- $(r \to p) \to ((r \to q) \to (r \to (p \wedge q)))$;
- $(p \to r) \to ((q \to r) \to ((p \vee q) \to r))$;
- $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$.

Uraditi isti zadatak samo umjesto iskaznih slova p, q, r stavite redom IF A, B, C. Šta uočavaš?

Logička svojstva implikacije

- U (matematičkim) zaključivanjima obično se koristi implikacija. Otuda je inplikacija ključni logički veznik.
- Zadatak. Neka su A , B i C IF. Dokazati da važi
  - $\models A \to (B \to A)$
  - $\models (A \to (B \to C)) \to ((A \to B) \to (A \to C))$.
- Rj. Neka je $v \in 2^P$ proizvoljna valuacija. Dokažimo da je $v(A \to (B \to A)) = 1$. Ako pretpostavimo da je $v(A \to (B \to A)) = 0$ onda je $v(A) = 1$ i $v(B \to A) = 0$. Sada iz $v(B \to A) = 0$ zaključujemo da je $v(B) = 1$ i $v(A) = 0$ a to nije moguće, jer smo već ustanovili da mora biti $v(A) = 1$. Ovo znači da ne može važiti $v(A \to (B \to A)) = 0$. Dakle, za svaku valuaciju $v \in 2^P$ važi $v(A \to (B \to A)) = 1$ pa je $\models A \to (B \to A)$.
  Za drugu formulu dokaz izvedite sami.

Drugi način-uputstvo. Postoje 4 kombinacije istinitosnih vrjednosti za IF A i B. Napravimo tabelu i vidimo da za svaku kombinaciju važi $v(A \to (B \to A)) = 1$.

$v(A)$	$v(B)$	$v(B \to A)$	$v(A \to (B \to A))$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

- Prethodne dvije tautologije su vrlo važna svojstva implikacije i treba da ih znate napamet. Da bi ih lakše pamtili treba da znamo šta one izrašavaju.
- Za prvu formulu, tj. $A \to (B \to A)$, kažemo da istina slijedi iz bilo šta. Riječima prepričana formula može da glasi: ako je A istina onda iz bilo koje formule B dobijamo tu intinu A.

- Za drugu formulu kažemo da predstavlja distirbutivnost implikacije u odnosu na samu sebe (tj. implikaciju). Naime zakon distributivnosti npr. množena u odnosu na sabiranje glasi:[1]

$$(A \cdot (B + C)) = ((A \cdot B) + (A \cdot C)).$$

  Ako u prethodnoj jednakosti umjeto $+$ i $\cdot$ stavimo $\to$ (tj. implikaciju) dobili bi u nekom smislu zakon distributivnosti implikacije u odnosu na implikaciju. Međutim, kako u iskaznoj logici nemamo simbol jednakosti (tj. $=$) onda i njega zamjenjujemo sa $\to$. Tako dobijamo formulu:

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

- Zadatak. Napisati tautologiju tranzitivnosti implikacije.

[1] Znak $=$ jasno razdaja lijevu i desnu strnu a dogovoreno je da množenje ima prioritet u odnosu na sabiranje pa se zagrade na desnoj strani mogu izostaviti kao i spoljnje zagrade na lijevoj strani.

Logička svojstva konjunkcije i disjunkcije

- U svojstvima niže A, B i C su IF.
- Da bi lakše pamtili formule koje slijede (a ponekad i da bi "brzo" ocjenili istinitosnu vrijednost formule) možemo zamišljati da su A, B i C prirodni brojevi da je $A \wedge B = \min\{A, B\}$, $A \vee B = \max\{A, B\}$ i $A \to B$ označava $A \leq B$.
- Za miniimum važi: *i*) $\min\{A, B\} \leq A$, *ii*) $\min\{A, B\} \leq B$ i *iii*) ako je $C \leq A$ i $C \leq B$ onda je $C \leq \min\{A, B\}$. Otuda imamo.
- Svojstva konjunkcije:

$$\models (A \wedge B) \to A, \tag{1}$$

$$\models (A \wedge B) \to B, \tag{2}$$

$$\models ((C \to A) \wedge (C \to B)) \to (C \to (A \wedge B)). \tag{3}$$

- Imajući u vidu tautologiju $((p \wedge q) \rightarrow r) \leftrightarrow (p \rightarrow (q \rightarrow r))$ svojstvo (3) konjunkcije češće zapisujemo

$$\models (C \rightarrow A) \rightarrow ((C \rightarrow B) \rightarrow (C \rightarrow (A \wedge B))$$

i nazivamo tautologijom infimuma.[2]

- Za maksimum važi: *i*) $A \leq \max\{A, B\}$, *ii*) $B \leq \max\{A, B\}$ i *iii*) ako je $A \leq C$ i $B \leq C$ onda je $\max\{A, B\} \leq C$.
- Svojstva disjunkcije:

$$\models A \rightarrow (A \vee B), \tag{4}$$

$$\models B \rightarrow (A \vee B), \tag{5}$$

$$\models (A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C)). \tag{6}$$

- Svojstvo (6) disjunkcije se naziva tautologija supremuma.[3]

[2] Infimum je uopštenje minimuma. Učićete iz analize.

[3] Supremuma je uopštenje maksimuma.

Prethodno navedena svojstva za konjunkciju i disjunkciju treba da znate napamet ali pored njih važe (treba znati) i sledeća svojstva.

- Zakoni apsorpcije:
  $\models (A \wedge (A \vee B)) \leftrightarrow A$,
  $\models (A \vee (A \wedge B)) \leftrightarrow A$.
- Zakoni komutativnosti:
  $\models (A \wedge B) \leftrightarrow (B \wedge A)$,
  $\models (A \vee B) \leftrightarrow (B \vee A)$.
- Zakoni asocijativnosti:
  $\models (A \wedge (B \wedge C)) \leftrightarrow ((A \wedge B) \wedge C)$,
  $\models (A \vee (B \vee C)) \leftrightarrow ((A \vee B) \vee C)$.
- Zakoni distributivnosti:
  $\models (A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$,
  $\models (A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$.

- Po definiciji $(A \wedge B \wedge C)$ nije IF. Ali kako važi zakon asocijativnosti to formule $(A \wedge (B \wedge C))$ i $((A \wedge B) \wedge C)$ imaju istu istinitosnu vrijednost. Drugim riječima sa stanovišta istinitosnih vrijednosti nije bitno gdje stavljamo zagrade.
- Otuda pišemo $(A \wedge B \wedge C)$ i kažemo da je to IF imajući u vidu da je to jedna od dvije ekvivalentne IF $(A \wedge (B \wedge C))$ ili $((A \wedge B) \wedge C)$.
- Uvodimo i oznaku $\bigwedge_{i=1}^{n} A_i$ i definišemo induktivno na sledeći način: $\bigwedge_{i=1}^{1} A_i = A_1$ i $\bigwedge_{i=1}^{n+1} A_i = (\bigwedge_{i=1}^{n} A_i) \wedge A_{n+1}$.
- Slično prethodnom uvodimo i oznaku $\bigvee_{i=1}^{n} A_i$ i definišemo induktivno na sledeći način: $\bigvee_{i=1}^{1} A_i = A_1$ i $\bigvee_{i=1}^{n+1} A_i = (\bigvee_{i=1}^{n} A_i) \vee A_{n+1}$.

Logička svojstva negacije

- $\models \neg A \to (A \to B)$
  Riječima prepričana formula može da glasi: ako je A laž (nije istina) onda iz te laži možemo da zaključimo bilo koju formulu B tj. bilo šta. Dakle, iz lažne pretpostavke slijedi sve.
- Svođenje na apsurd: $\models (A \to B) \to ((A \to \neg B) \to \neg A)$
  Ako iz A možemo zaključiti i B i $\neg B$ onda A nije istina.
- De Morganovi zakoni:
  $\models \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$,
  $\models \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$.
- Zakon kontrapozicije: $\models (A \to B) \leftrightarrow (\neg B \to \neg A)$.
- Zakon dvojne negacije: $\models A \leftrightarrow \neg\neg A$.
- Zakon isključenja trećeg: $\models A \vee \neg A$.

Normalne forme

- Normalna forma IF A je njoj ekvivalentna formula A' sa negacijam ispred iskaznih slova i veznicima $\wedge$ i $\vee$.
- Neka je $p \in P$ iskazno slovo i $\delta \in \{0, 1\}$. Uvedimo oznaku $p^\delta = \begin{cases} p & , \quad \delta = 1 \\ \neg p & , \quad \delta = 0 \end{cases}$, koju nazivamo literalom.
- Za $v \in 2^P$ i $p \in P$ pisaćemo p^v umjeto $p^{v(p)}$. Očito $p^v = p$ ako je $v(p) = 1$ a $p^v = \neg p$ ako je $v(p) = 0$. Pa je $v(p^v) = 1$.
- Oznaka $A^v = A^{v(A)}$ se može uopštiti za proizvoljnu IF A i $v \in 2^P$. Naime, uzimamo $A^v = A$ ako je $v(A) = 1$ i $A^v = \neg A$ ako je $v(A) = 0$.
- Formule oblika $\bigwedge\limits_{i \leq n} p_i^{\delta_i}$ i $\bigvee\limits_{i \leq n} p_i^{\delta_i}$, gdje je $p_i \in P$ a $\delta_i \in \{0, 1\}$ nazivamo redom elementarna konjunkcija i elementarna disjunkcija.

- Kažemo da je formula zapisana u disjunktivnoj normalnoj formi (DNF) ako ima oblik $\bigvee\limits_{j\leq k} K_j$, gdje je K_j elementarna konjunkcija.
- Kažemo da je formula zapisana u konjunktivnoj normalnoj formi (KNF) ako ima oblik $\bigwedge\limits_{j\leq k} D_j$, gdje je D_j elementarna disjunkcija.
- **Teorema.** Svaka IF $A(p_1, \ldots, p_n)$ ekvivalentna je IF A' koja je (zapisana) u DNF (KNF).
- Dokaz za DNF. Ako je za svaku valuaciju $v \in 2^P$ $v(A) = 0$ onda za A' možemo uzeti $A' = p_1 \wedge \neg p_1$ koja je ekvivalentna formuli A.

U suprotnom neka je $A' = \bigvee\limits_{v:v(A)=1} \left(\bigwedge\limits_{i=1}^{n} p_i^v \right)$. Ovakav oblik formule nazivamo savršena DNF ili skraćeno SDNF.
Treba dokazati da je IF A' ekvivalentna IF A.
Neka $w \in 2^P$ proizvoljna valuacija. Ako je $w(A) = 1$ onda zbog $w(p^w) = 1$ imamo $w(\bigwedge_{i=1}^{n} p_i^w) = 1$ pa je i $w(A') = 1$. Ako je $w(A) = 0$ posmatrajmo valuaciju $v \in 2^P$ za koju je $v(A) = 1$. Kako je $w(A) \neq v(A)$ postoji p_i tako da je $v(p_i) \neq w(p_i)$ pa je $w(p_i^v) = 0$ (jer je $v(p_i^v) = 1$). Zbog toga je $w(\bigwedge_{i=1}^{n} p_i^v) = 0$ pa je i $w(A') = 0$. Dakle, $w(A) = w(A')$ pa su formule A i A' ekvivalentne.

- Dokaz za KNF. Dokaz je sličan prethodnom samo za A' treba uzeti savrženu KNF (SKNF) tj. $A' = \bigwedge\limits_{v:v(A)=0} \left(\bigvee\limits_{i=1}^{n} p_i^{v(\neg p_i)} \right)$.
- Napomena. Formula A' se naziva SDNF jer sve njene elementarne konjunkcije sadrže svih n iskaznih slova.

Zadatak. Naći SDNF za formulu $A(p,q,r) = (p \to r) \to \neg q$
Rj. Pravimo tablicu i gledamo one vrste gdje je $v(A) = 1$[4]

p	q	r	$p \to r$	$\neg q$	A	
0	0	0	1	1	1	$\leftarrow$
0	0	1	1	1	1	$\leftarrow$
0	1	0	1	0	0	
0	1	1	1	0	0	
1	0	0	0	1	1	$\leftarrow$
1	**0**	**1**	1	1	1	$\leftarrow$
1	1	0	0	0	1	$\leftarrow$
1	1	1	1	0	0	

Te vrste su označene strelicom. Za svaku takvu vrstu pravimo odgovarajuču elementarnu konjunkciju $p^v \wedge q^v \wedge r^v$.

[4] U tabeli pišemo samo formule tj. izostavljamo v

Npr. za vrstu označenu crvenom strelicom imamo da je $v(p) = 1$, $v(q) = 0$ i $v(r) = 1$ pa dobijamo $p^v \wedge q^v \wedge r^v = p^1 \wedge q^0 \wedge r^1 = p \wedge \neg q \wedge r$. Slično radimo za preostale 4 vrste.
Tako za A' dobijamo formulu:

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r).$$

- **Teorema.**(interpolacije) Neka IF A nije kontradikcija a IF B nije tautologija. Ako je $\models A \to B$ onda postoji formula C koja samo sadrži iskazne promenljive koje su zajedničke za formule A i B takva da $\models A \to C$ i $\models C \to B$.
- Dokaz. Uradite sami.

Komentar

- U računarstvu su važne Bulove funkcije tj. funkcije $f : \{0,1\}^n \to \{0,1\}$. One se mogu zadati tablicom (sa 2^n nizova nula i jedinica dužine n, tj. tačaka, i vrijednostima funkcije u tim nizovima) a mogu se zadati formulama.
- Prethodna teorema nam u stvari kaže da se svaka Bulova funkcija može zadati pomoću formule (koja je u DNF ili KNF).
- Ako funkciju zapišemo formulom onda je možemo realizovati hardverski koristeći "I","ILI" i "NE" kola (sekvencijalno kolo). Otuda je u računarstvu bitna minimizacija formula tj. traženje ekvivalentne formule sa minimalnim brojem veznika.
- Fve funkcije možemo zapisati koristeći npr. veznike $\wedge, \neg$. Interesantno je da ih možemo zapisati koristeći samo veznik $\uparrow$ (Šeferov veznik-operacija) ili veznik $\downarrow$ (Lukašijevičeva operacija). Važi $p \uparrow q = \neg(p \wedge q)$ a $p \downarrow q = \neg(p \vee q)$.

Logičke posljedice

- Kažemo da valuacija v zadovoljava skup IF Σ, u oznaci $v(\Sigma) = 1$, ako za svaku formulu $A \in \Sigma$ važi $v(A) = 1$ (tj. ako su za valuaciju v istinite sve formule skupa Σ).
- Za skup IF Σ kažemo da je zadovoljiv ako postoji valuacija v takva da je $v(\Sigma) = 1$.
- **Def.** Za formulu A kažemo da je logička posljedica skupa pretpostavki (formula) Σ, i označavamo sa $\Sigma \models A$, ako za svaku valuaciju $v \in 2^P$ za koju je $v(\Sigma) = 1$ važi $v(A) = 1$.
  (Drugim riječima sve valuacije koje zadovoljavaju Σ zadovoljavaju i A).
- Uočimo da ako je $\Sigma = \emptyset$ onda umjesto zapisa $\emptyset \models A$ možemo pisati $\models A$ tj. logička posljedica praznog skupa je tautologija.

- **Def.** Za skup IF Σ kažemo da je logički neprotivrečan (ili logički konzistentan) ako ne postoji IF A za koju je $\Sigma \models A$ i $\Sigma \models \neg A$.
- Napomena. Umjesto $\Sigma \cup \{A\} \models B$ koristi se oznaka $\Sigma, A \models B$ analogno tome umjesto $\{A_1, \dots, A_n\} \models B$ koristi se oznaka $A_1, \dots, A_n \models B$.

Zadatak. Dokazati sledeća tvrđenja.

a) Skup formula Σ je logički konzistentan akko Σ je zadovoljiv.

b) Skup formula je logički nekonzistentan akko svaka IF je njegova logička posljedica.

c) (Teorema dedukcije) Ako su A i B formule i Σ skup formula iskazne logike, onda $\Sigma, A \models B \Rightarrow \Sigma \models A \to B$.

Formalni pristup (Formalni sistemi)

- Napomena. U udžbeniku se Formalni pristup naziva sintaksa.
- Komentar. Algoritam, Odlučivost (rješivost), Algoritam za provjeru da li je IF A tautologija, Algoritam za provjeru da li je IF A zadovoljiva...
- Formalizacija podrazumjeva zadavanje dva skupa i to:
  1. skupa logičkih zakona tj. aksioma i
  2. skupa pravila izvođenja (zaključivanja).
- Postoje razne formalizacije (tj. izbori skupova 1 i 2). Gencenovi sistemi imaju mali broj aksioma a veći broj pravila izvođenja dok Hilbertovski sistemi imaju malo pravila izvođenja a veći broj aksioma.

- Označimo sa $I = \{A \in F \ : \models A\}$ skup logičkih zakona i neka je $T \subset I$ skup aksioma. Sa $Con(T)$ ($Con(T) \subset F$) označavamo skup zaključaka (konkluzija) koje dobijamo polazeći od aksioma T uz pomoć pravila izvođenja.
- Interesuje nas odnos skupova I i $Con(T)$.
  - Ako je $Con(T) \subset I$ formalizacija je korektna.
  - Ako je $I \subset Con(T)$ formalizacija je potpuna.
- Komentar. Odnos I i $Con(T)$ je odnos semantike i formalnog pristupa i to će mo proučavati kasnije.
  Korektna formalizacija podrazumjeva da svi zaključci koje dobijamo su istiniti (tj. logički zakoni).
  Potpuna formalizacija podrazumjeva da zaključke koje dobijamo sadrže sve istinie (tj. logičke zakone).

Aksiome iskaznog računa

- Opredjelili smo se za Hilbertovski sistem.
- Aksiome su date shemom tj. oblikom IF tako da su u svim aksiomama niže A, B i C proizvoljne IF; drugi pristup je da koristimo supstituciju.
- Skup navedenih aksioma nije minimalan i nije nezavisan.
- Navodimo 11 shema (skupova) aksioma podjeljenih u 5 grupa (po jedna grupa za svaki od 4 veznika i zakon isključenja trećeg).
- Pisaćemo npr. $T_1 : A \to (B \to A)$ a to nam preciznije zapisano znači da je $T_1 = \{A \to (B \to A) \ : \ A, B \in F\}$. Slično za ostale sheme aksioma T_i.
- Skup svih aksioma označavamo sa T, $T = \bigcup_{i=1}^{11} T_i$, gdje su T_i:

- Aksiome implikacije:

$$T_1 : A \to (B \to A)$$
$$T_2 : (A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

- Aksiome konjunkcije:

$$T_3 : (A \wedge B) \to A$$
$$T_4 : (A \wedge B) \to B$$
$$T_5 : A \to (B \to (A \wedge B))$$

- Aksiome disjunkcije:

$$T_6 : A \to (A \vee B)$$
$$T_7 : B \to (A \vee B)$$
$$T_8 : (A \to C) \to ((B \to C) \to ((A \vee B) \to C))$$

- Aksiome negacije:

$$T_9 : \neg A \to (A \to B)$$
$$T_{10} : (A \to B) \to ((A \to \neg B) \to \neg A)$$

- Aksiome zakona isključenja trećeg:

$$T_{11} : A \vee \neg A$$

Pravilo izvođenja

- U formalizaciji za koju smo se opredjelili jedino pravilo izvođenja (tj. zaključivanja) je modus ponendo ponens (način tvrdeći tvrdim) ili kratko modus ponens.
- MODUS PONENS. Za proizvoljne iskazne formule A i B iz formula A i $A \to B$ zaključujemo B.
- Za modus ponens koristićemo skraćenicu MP i prikazujemo sa:

$$\frac{A,\ A \to B}{B}$$

- MP čuva istine, jer ako su pretpostavke A i $A \to B$ istinite onda je i zaključak B istinit.
- Obično se pretpostavka A naziva malom a pretpostavka $A \to B$ velikom premisom.

Dokaz u iskaznom računu

- **Def.** Dokaz IF A u iskaznom računu je konačan niz iskaznih formula $(A_1, \ldots, A_n)$, $n \geq 1$, takav da je $A = A_n$ i za svako $i \leq n$ za iskaznu formulu A_i važi jedan od uslova:
  1. $A_i \in T$ tj. A_i je aksioma ili
  2. postoje $k, j < i$ takvi da je $A_j = A_k \to A_i$ tj. A_i se po MP dobija iz njoj prethodnih članova niza.
- **Def.** Ako postoji dokaz IF A onda za formulu A kažemo da je dokaziva ili teorema (iskaznog računa) i označavamo sa $\vdash A$.
- **Def.** Dokaz IF A iz skupa IF (pretpostavki) Σ je konačan niz IF $(A_1, \ldots, A_n)$, $n \geq 1$, takav da je $A = A_n$ i za svako $i \leq n$ za iskaznu formulu A_i važi jedan od uslova:
  1. $A_i \in \Sigma$ tj. A_i je pretpostavka ili
  2. $A_i \in T$ tj. A_i je aksioma ili
  3. postoje $k, j < i$ takvi da je $A_j = A_k \to A_i$ tj. A_i se po MP dobija iz njoj prethodnih članova niza.

- **Def.** Kažemo da je IF A posljedica skupa pretpostavki Σ, u oznaci $\Sigma \vdash A$, ako postoji dokaz formule A iz skupa IF Σ.
- Uočimo da ako ja A posljedica praznog skupa onda je ona teorema tj. $\emptyset \vdash A \ \Rightarrow \vdash A$.
- Teoreme iskaznog računa mi smatramo istinama. Skup svih teorema označavamo sa $\mathcal{T} = Con(T) = \{A \in F \ : \vdash A\}$.
- Skup svih posljedica skupa Σ označavamo sa $Con(\Sigma) = \{A \in F \ : \ \Sigma \vdash A\}$. Preciznija oznaka bi bila $Con(T \cup \Sigma)$.
- Broj formula u dokazu nazivamo dužinom dokaza tj. dužina dokaza $(A_1, \ldots, A_n)$ je n.
- **Def.** Za skup IF Σ kažemo da je neprotivrečan (ili konzistentan) ako ne postoji IF A za koju je $\Sigma \vdash A$ i $\Sigma \vdash \neg A$.

- Napomena. Dokaz ćemo zapisivati sa $A_1, \ldots, A_n$ umjesto $(A_1, \ldots, A_n)$ tj. izostavljamo zagrade.
  Umjesto $\Sigma \cup \{A\} \vdash B$ koristi se oznaka $\Sigma, A \vdash B$ analogno tome umjesto $\{A_1, \ldots, A_n\} \vdash B$ koristi se oznaka $A_1, \ldots, A_n \vdash B$.
  Koristimo i oznaku $\Sigma, \Gamma \vdash A$ umjesto $\Sigma \cup \Gamma \vdash A$ i sl.
- Uporedna tabela nekih oznaka i pojmova uvedenih u semantičkom i formalnom pristupu

sem.p.	$\models A$	tautologija	log. posljedica	log. konzistentan
form.p.	$\vdash A$	teorema	posljedica	konzistentan

Izvedena pravila zaključivanja

- Ako iz pretpostavki P zaključujemo Z (tj. $P \Rightarrow Z$) onda to pravilo zapisujemo sa $\dfrac{P}{Z}$. A sa $\dfrac{P}{\overline{\overline{Z}}}$ ako važi i obrnuto (tj. $P \Leftrightarrow Z$) i ovakvo pravilo nazivamo dvojnim pravilom.
- Neka su Σ, Σ_1, Σ_2 skupovi IF i A, B, C proizvoljne IF. Tada važe sledeća pravila:

  a) Uopštenje MP $\quad \dfrac{\Sigma_1 \vdash A, \Sigma_2 \vdash A \to B}{\Sigma_1, \Sigma_2 \vdash B}$.

  b) Pravilo slabljenja $\quad \dfrac{\Sigma \vdash A}{\Sigma, B \vdash A}$.

  c) Pravilo permutacije pretpostavki $\quad \begin{array}{c} \Sigma, B, C \vdash A \\ \hline\hline \Sigma, C, B \vdash A \end{array}$.

Dokaz.

a) Drugačije zapisano pravilo glasi

$$\left(\Sigma_1 \vdash A \text{ i } \Sigma_2 \vdash A \to B\right) \;\Rightarrow\; \Sigma_1, \Sigma_2 \vdash B.$$

Pretpostavimo da važi $\Sigma_1 \vdash A$ i $\Sigma_2 \vdash A \to B$ (tj. je A posljedic od Σ_1 i $A \to B$ je posljedic od Σ_2). Ovo po definiciji (posljedice) znači da postoji dokaz $A_1, \dots, A_n$ za formulu $A = A_n$ iz Σ_1 ($A_i \in T \cup \Sigma_1$ ili $\exists p, q < i\ A_q = A_p \to A_i$) i postoji dokaz $B_1, \dots, B_k$ za formulu $B_k = A \to B$ iz Σ_2 ($B_i \in T \cup \Sigma_2$ ili $\exists p, q < i\ B_q = B_p \to B_i$). Treba da dokažemo $\Sigma_1, \Sigma_2 \vdash B$ (tj. B posljedica od $\Sigma_1 \cup \Sigma_2$). Za to nam je potrebno da nađemo dokaz za B iz $\Sigma_1 \cup \Sigma_2$. Posmatrajmo niz formula $C_1, \dots, C_n, C_{n+1}, \dots, C_{n+k}, C_{n+k+1}$ gdje je $C_i = A_i$ za $i \leq n$, $C_i = B_{i-n}$ za $n < i \leq n + k$ i $C_{n+k+1} = B$ (to je u stvari niz $A_1, \dots, A_n, B_1, \dots, B_k, B$).

Za ovaj niz važi:

- ako je $i \leq n$ tj. $C_i = A_i$ onda je $C_i \in T \cup \Sigma_1 \subset T \cup \Sigma_1 \cup \Sigma_2$ ili $\exists p, q < i \ A_q = A_p \to A_i$ tj. $C_q = C_p \to C_i$;
- ako je $n < i \leq n + k$ tj. $C_i = B_{i-n}$ onda je $C_i \in T \cup \Sigma_2 \subset T \cup \Sigma_1 \cup \Sigma_2$ ili $\exists p, q < i - n \ B_q = B_p \to B_{i-n}$ tj. $C_{q+n} = C_{p+n} \to C_i$;
- ako je $i = n + k + 1$ tj. $C_i = B$ onda zbog $C_n = A_n = A$ i $C_{n+k} = B_k = A \to B$ postoje $p = n < i$ i $q = n + k < i$ takvi da je $C_q = C_p \to C_i$.

Pa je ovaj niz dokaz za formulu $C_{n+k+1} = B$ iz skupa $\Sigma_1 \cup \Sigma_2$. Dakle, $\Sigma_1, \Sigma_2 \vdash B$ što je i trebalo dokazati.

Komentar. Pošto je ovo prvi dokaz ove vrste ispisan je detaljnije. Takođ tekst plavom bojom možemo izostaviti, ali je on ovde naveden da bi studenti znali šta u nastavku dokaza radimo.

Kraći dokaz (kako to u buduće radimo) bi zamjenio dio teksta počev od redova obojenih plavom bojom sa rečenicom koja slijedi.
Tada je niz formula $A_1, \ldots, A_n, B_1, \ldots, B_k, B$ dokaz za formulu B iz skupa Σ_1, Σ_2.

b) Ako je $A_1, \ldots, A_n$ dokaz za $A_n = A$ iz Σ onda je to i dokaza za A iz Σ, B (samo B ne koristimo).

c) Dokaz je sličan prethodnom. Naime $A_i \in \Sigma, B, C \;\Leftrightarrow\; A_i \in \Sigma, C, B$.

- Osnovna ideja u gore navedenom dokazu je nadovezivanje postojećih nizova formula (koji predstavljaju dokaze) i eventualno njihovo dopunjavanje novim formulama.
- Da bi skratili dokaz iskazne formule pored MP možemo koristiti i izvedena pravila.

Posljedice aksioma implikacije

- **Teorema** (tautologije). Neka je A IF. Tada $\vdash A \to A$.
- **Dokaz**. Niz formula
  $A_1 = A \to (A \to A) \in T_1$, $\lceil$ uzeto $B = A$ $\rfloor$
  $A_2 = A \to ((A \to A) \to A) \in T_1$, $\lceil$ uzeto $B = (A \to A)$ $\rfloor$
  $A_3 = (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) \in T_2$, $\lceil$ uzeto $B = (A \to A)$ i $C = A$ $\rfloor$
  $A_4 = (A \to (A \to A)) \to (A \to A)$ (MP 2,3),
  $A_5 = A \to A$ (MP 1,4)
  je dokaz za formulu $A_5 = A \to A$.

- **Teorema** (dedukcije). Neka su A, B IF i Σ skup IF. Tada

$$\Sigma, A \vdash B \quad \Rightarrow \quad \Sigma \vdash A \to B.$$

Dokaz. Neka je $\Sigma, A \vdash B$. Znači da postoji niz formula $A_1, \ldots, A_n$ koji je dokaz za formulu $A_n = B$ iz Σ, A (tj. $A_i \in T, \Sigma, A$ ili se dobija po MP q, p za $q, p < i$). Uočimo da iz prethodnog slijedi $\Sigma, A \vdash A_i$ za svako $i \leq n$ (naime $A_1, \ldots, A_i$ je dokaz za A_i). Dokažimo $\Sigma \vdash A \to B$ indukcijom po dužini dokaza za B.

Za $n = 1$ imamo dokaz $A_1 = B$, gdje je $A_1 \in T, \Sigma, A$.

- Ako je $B \in T, \Sigma$ onda je niz formula $B_1 = B \in T, \Sigma$, $B_2 = B \to (A \to B) \in T_1$, $B_3 = A \to B$ (MP 1,2) dokaz za $A \to B$ iz Σ tj. $\Sigma \vdash A \to B$
- Ako je $B = A$ onda $\vdash A \to A$ po teoremi tautologije, a na osnovu pravila slabljenja dobijamo i $\Sigma \vdash A \to A$.

Neka je $n > 1$ i neka tvrđenje važi za sve formule koje imaju dokaz iz Σ, A dužine manje od n. Dokažimo da tvrđenje važi i za formulu B čiji je dokaz $A_1, \ldots, A_n$ dužine n.

Za formulu $A_n = B$ važi $B \in T, \Sigma, A$ ili se B dobija po MP tj. postoje $i, j < n$ tako da je $A_j = A_i \to B$.

- Za $B \in T, \Sigma, A$ onda B ima i dokaz dužine jedan pa se svodi na slučaj $n = 1$.
- Ako postoje $i, j < n$ tako da je $A_j = A_i \to B$ onda po ind.p.p. važi $\Sigma \vdash A \to A_i$ i $\Sigma \vdash A \to A_j$ tj. $\Sigma \vdash A \to (A_i \to B)$.
  Otuda postoji $C_1, \ldots, C_k$ dokaz za $C_k = A \to (A_i \to B)$ iz Σ i postoji $C_{k+1}, \ldots, C_m$ dokaz za $C_m = A \to A_i$ iz Σ.
  Onda je niz formula $C_1, \ldots, C_k, C_{k+1}, \ldots, C_m$,
  $C_{m+1} = (A \to (A_i \to B)) \to ((A \to A_i) \to (A \to B)) \in T_2$,
  $C_{m+2} = (A \to A_i) \to (A \to B)$ (MP $k, m+1$), $C_{m+3} = A \to B$ (MP $m, m+2$) dokaz za $C_{m+3} = A \to B$ iz Σ.
  Pa $\Sigma \vdash A \to B$.

Na osnovu principa matematičke indukcije tvrđenje važi za svaku formulu B koja ima dokaz. Što je i trebalo dokazati.

- Teorema dedukcije važi i u drugom smjeru. Naime ako je $A_1, \dots, A_n$ dokaza za $A_n = A \to B$ iz Σ onda je $A_1, \dots, A_n$, $A_{n+1} = A \in \Sigma, A$, $A_{n+2} = B$ (MP $n+1$, n) dokaz za $A_{n+2} = B$ iz Σ, A.
- Dakle važi dvostrano pravilo dedukcije

$$\frac{\Sigma, A \vdash B}{\overline{\Sigma \vdash A \to B}}.$$

- **Teorema** (tranzitivnosti). Neka su A, B i C IF. Tada

$$\vdash (A \to B) \to ((B \to C) \to (A \to C)).$$

- Komentar. Relacija $\leq$ je tranzitivna u $\mathbb{R}$:
$(a \leq b)$ i $(b \leq c) \Rightarrow (a \leq c)$.

Dokaz(teoreme tranzitivnosti). Primijenjujemo teoremu dedukcije. Pripremni korak. Treba da vidimo od kog skupa formula polazimo i koju formulu dokazujemo. Zato koristimo teoremu dedukcije u suprotnom smjeru. Primijenjujemo je dok god je to moguće. Polazimo od $\vdash (A \to B) \to ((B \to C) \to (A \to C))$ iz čega zaključimo da treba da važi $A \to B \vdash ((B \to C) \to (A \to C))$. Opet primjenom teoreme dedukcije (2 puta) zaključujemo da je $A \to B, B \to C \vdash A \to C$ i konačno $A \to B, B \to C, A \vdash C$. Sad smo spremni da krenemo sa dokazom.
Neka je $\Sigma = \{A \to B, B \to C, A\}$ tada $\Sigma \vdash C$ a dokaz za to je niz formula $A_1 = A \in \Sigma$, $A_2 = A \to B \in \Sigma$, $A_3 = B$ (MP 1,2), $A_4 = B \to C \in \Sigma$, $A_5 = C$ (MP 3,4). Sada primjenom 3 puta teoreme dedukcije na $A \to B, B \to C, A \vdash C$ dobijamo redom $A \to B, B \to C \vdash A \to C$ pa $A \to B \vdash ((B \to C) \to (A \to C))$ i
$\vdash (A \to B) \to ((B \to C) \to (A \to C))$.

Posljedice aksioma konjunkcije

- **Teorema** (pravilo konjunkcije). Neka su A, B IF i Σ skup IF. Tada

$$P\wedge : \frac{\Sigma \vdash A \quad \Sigma \vdash B}{\Sigma \vdash A \wedge B}. \quad \lceil A, B \text{ dokazivi } \Leftrightarrow A \wedge B \text{ dokazivo} \rfloor$$

- **Dokaz**(uputstvo) ($\downarrow$:) $A_1, \ldots, A_n = A$, $B_1, \ldots, B_k = B$, $C_1 = A \to (B \to (A \wedge B)) \in T_5$, $C_2 = B \to (A \wedge B)$ (MP A_n, C_1), $C_3 = A \wedge B$ (MP B_k, C_2).
  ($\uparrow$:) $C_1, \ldots, C_n = A \wedge B$, $C_{n+1} = (A \wedge B) \to A \in T_3$, $C_{n+2} = A$ (MP $n, n+1$). Slično za B koristimo aksiomu T_4.
- **Teorema** (infimuma). Neka su A, B i C IF. Tada

$$\vdash (C \to A) \to ((C \to B) \to (C \to (A \wedge B)).$$

- **Dokaz**(uputstvo) Primijeniti 3 puta teoremu dedukcije na $C \to A, C \to B, C \vdash A \wedge B$. Dokaz za poslednje je C, $C \to A$, A, $C \to B$, B, $A \to (B \to (A \wedge B))$, $B \to (A \wedge B)$, $A \wedge B$.

- Zadatak. Dokazati (teorema i pravilo o konjunkciji pretpostavki):
$$a)\ \vdash ((A \to (B \to C)) \leftrightarrow ((A \wedge B) \to C), \quad b)\ \dfrac{\Sigma, A, B \vdash C}{\Sigma, A \wedge B \vdash C}.$$
- Rj.(uputstvo) a) Primjeniti teoremu dedukcije i aksiome za $\wedge$.
b) ($\downarrow$:) Dokazu $A_3, \ldots, A_n = C$, dodamo $A_0 = (A \wedge B) \in \Sigma'$, $A_1 = (A \wedge B) \to A \in T_3$, $A_2 = (A \wedge B) \to B \in T_4$ pa A i B dobijamo po MP. ($\uparrow$:) Dokazu $A_4, \ldots, A_n = C$, dodamo $A_0 = A \in \Sigma''$, $A_1 = B \in \Sigma''$, $A_2 = A \to (B \to (A \wedge B)) \in T_5$, $A_3 = B \to (A \wedge B)$ (MP 1,2), pa $A \wedge B$ dobijamo po MP.
- Zadatak. $\vdash A \leftrightarrow (A \wedge A)$ tj. $\vdash (A \to (A \wedge A)) \wedge ((A \wedge A) \to A)$.
- Rj. $A_1 = (A \wedge A) \to A \in T_3$ je dokaz za $\vdash (A \wedge A) \to A$. Dok je $A_1 = A$, $A_2 = A \to (A \to (A \wedge A)) \in T_5$, $A_3 = A \to (A \wedge A)$, $A_4 = A \wedge A$ dokaz za $A \vdash A \wedge A$ tj. $\vdash A \to (A \wedge A)$. Ostaje da primijenimo $P\wedge$ (p. konjunk.).

Posljedice aksioma disjunkcije

- **Teorema** (pravilo disjunkcije). Neka su A, B, C IF i Σ skup IF. Tada

$$P\vee : \ \frac{\Sigma, A \vdash C \ \ \Sigma, B \vdash C}{\Sigma, A \vee B \vdash C}. \qquad \lceil \text{dokazivanje po slučajevima} \rfloor$$

- **Dokaz**(uputstvo) ($\downarrow$:) Po teoremi dedukcije $\Sigma \vdash A \to C$ i $\Sigma \vdash B \to C$. Ako nadovežemo dokaze za prethodne IF sa $(A \to C) \to ((B \to C) \to ((A \vee B) \to C)) \in T_8$ i primjenimo MP dobijamo dokaz za $(A \vee B) \to C$ tj. $\Sigma \vdash (A \vee B) \to C$.
  ($\uparrow$:) Dokazu $A_3, \ldots, A_n = C$, dodamo $A_1 = A \in \Sigma, A$, $A_2 = A \to (A \vee B) \in T_6$, pa $A_i = A \vee B$ (MP 1,2).
- Zadatak. Dokazati zakone distributivnosti za $\wedge$ i $\vee$.
  (a) $\vdash (A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$,
  (b) $\vdash ((A \wedge B) \vee (A \wedge C)) \leftrightarrow (A \wedge (B \vee C))$.

- Zadatak. Dokazati
  - (a) Zakone idempotencije ($a^2 = a$):
    $\vdash (A \vee A) \leftrightarrow A, \quad \vdash (A \wedge A) \leftrightarrow A.$
  - (b) Zakone apsorpcije:
    $\vdash (A \wedge (A \vee B)) \leftrightarrow A, \quad \vdash (A \vee (A \wedge B)) \leftrightarrow A.$
  - (c) Zakone komutativnosti:
    $\vdash (A \wedge B) \leftrightarrow (B \wedge A), \quad \vdash (A \vee B) \leftrightarrow (B \vee A).$
  - (d) Zakone asocijativnosti:
    $\vdash (A \wedge (B \wedge C)) \leftrightarrow ((A \wedge B) \wedge C), \quad \vdash (A \vee (B \vee C)) \leftrightarrow ((A \vee B) \vee C).$
- Rj. (b) $\vdash (A \wedge (A \vee B)) \to A$ po aksiomi T_3. Dokažimo i $\vdash A \to (A \wedge (A \vee B))$. Iz $A \vdash A$ (teor. taut.) i $A \vdash A \vee B$ (po T_6) primjenom $(P\wedge)$ dobijamo $A \vdash A \wedge (A \vee B)$.
  (c) Iz $A \wedge B \vdash B$ (po T_4) i $A \wedge B \vdash A$ (po T_3) slijedi $A \wedge B \vdash B \wedge A$ $(P\wedge)$ tj. $\vdash (A \wedge B) \to (B \wedge A)$.
  (d) Iz $A \wedge (B \wedge C) \vdash A$, $A \wedge (B \wedge C) \vdash (B \wedge C)$ po $(P\wedge \uparrow)$ dobijamo $A \wedge (B \wedge C) \vdash A$, $A \wedge (B \wedge C) \vdash B$ i $A \wedge (B \wedge C) \vdash C$. Ostaje da dva puta primjenimo $(P\wedge \downarrow)$.

Posljedice aksioma negacije

- **Teorema** (pravilo za dokazivanje negacije). Neka su A, B i Σ skup IF. Tada
$$P\neg : \quad \frac{\Sigma, A \vdash B \quad \Sigma, A \vdash \neg B}{\Sigma \vdash \neg A}.$$
- **Dokaz**(uputstvo) ($\downarrow$:) Po teoremi dedukcije $\Sigma \vdash A \to B$ i $\Sigma \vdash A \to \neg B$. Ako nadovežemo dokaze za prethodne IF sa $(A \to B) \to ((A \to \neg B) \to \neg A) \in T_{10}$ i primjenimo MP dobijamo dokaz za $\neg A$ tj. $\Sigma \vdash \neg A$.
($\uparrow$:) $\Sigma \vdash \neg A \;\Rightarrow\; \Sigma, A \vdash \neg A$. Pa zbog $\Sigma, A \vdash A$ i $\vdash \neg A \to (A \to C)$ dobijamo $\Sigma, A \vdash C$. Ostaje da prvo stavimo $C = B$ a drugi put $C = \neg B$.

- **Teorema** (slabe kontrapozicije). Neka su A i B IF. Tada $\vdash (A \to B) \to (\neg B \to \neg A)$.
- **Dokaz**(uputstvo) Uzmimo $\Sigma = \{A \to B, \neg B\}$. Uočimo da je $\Sigma, A \vdash B$ i $\Sigma, A \vdash \neg B$, pa po pravilu za dokazivanje negacije dobijamo $\Sigma \vdash \neg A$.
- Zadatak. Dokazati teoremu slabe dvojne negacije tj. $\vdash A \to \neg\neg A$.
- Zadatak. Dokazati modus (tolendo) tolens tj. $\dfrac{\neg B, A \to B}{\neg A}$.

Zakon isključena trećeg

- Zakon isključena trećeg je izazvao najviše polemike. Njegova primjena je npr. ako dokažemo da nije A onda tvrdimo da je A (i ako nemamo konstrukciju A tj. nemamo direktni dokaz za A). Pa je pitanje da li možemo tvrditi da nešta postoji bez negove eksplicitne konstrukcije?
- **Teorema** (o jakoj dvojnoj negaciji). Neka je A IF. Tada $\vdash \neg\neg A \to A$.
- **Dokaz**(uputstvo) $A \vee \neg A, \neg\neg A \vdash A$, dokazujemo po slučajevima: (1^o) $A, \neg\neg A \vdash A$ očigledno, (2^o) $\neg A, \neg\neg A \vdash A$ iz $\neg(\neg A) \to (\neg A \to A) \in T_9$.
- **Teorema** (o jakoj kontrapoziciji). Neka su A i B IF. Tada $\vdash (\neg B \to \neg A) \to (A \to B)$.
- **Dokaz**(uputstvo) Za $\Sigma = \{\neg B \to \neg A, A\}$ dobijamo $\Sigma, \neg B \vdash A$ i $\Sigma, \neg B \vdash \neg A$ pa po pravilu za dokazivanje negacije $\Sigma \vdash \neg\neg B$ tj. $\Sigma \vdash B$ (po prethodno navedenom pravilu).

Zadatak.

a) Ako aksiomu T_{11} zamjenimo sa $\neg\neg A \to A$ onda je $\vdash A \vee \neg A$. Dokazati.

b) Dokazati da aksima T_{10} slijedi iz ostalih aksioma.

c) Koristeći zakon isključenja trećeg (z.i.3) dokazati $\vdash ((A \vee B) \to A) \vee (A \vee B) \to B))$.

d) Neka je $T_0 = \{(\neg A \to \neg B) \to (B \to A) \; : \; A, B \in F\}$ i $T' = T_1 \cup T_2 \cup T_0$. Ako je T' skup aksioma a modus ponens (MP) pravilo izvođenja dokazati da je $T_i \subset Con(T')$ za $i = 3, 4, ..., 11$ tj. svaka instanca aksioma T_i je dokaziva. Veznici $\wedge$ i $\vee$ se uvode kao skraćenice preko veznika $\neg$ i $\to$.

e) Dokazati De Morganove zakone.

Svojstva ekvivalencije -sintaksna (formalna)

- **Def.** Za IF A i B kažemo da su (sintaksno) ekvivalentne ako $\vdash A \leftrightarrow B$.
- Zadatak. Dokazati: a) $\vdash (A \leftrightarrow B) \leftrightarrow (\neg A \leftrightarrow \neg B)$.
  b) $\vdash (A \leftrightarrow B) \leftrightarrow ((A \wedge B) \vee (\neg A \wedge \neg B))$.
- **Teorema** (o zamjeni ekvivalentnih formula). Neka su A, B i C proizvoljne IF. Tada $\vdash (B \leftrightarrow C) \rightarrow (A \leftrightarrow A(B/C))$.
- **Dokaz**. Sami.
- Zadatak. Dokazati pravilo zamjene ekvivalentnih pretpostavki

$$\frac{\Gamma, A \vdash C \quad \Sigma \vdash A \leftrightarrow B}{\Gamma, \Sigma, B \vdash C}.$$

Teorema korektnosti iskaznog računa

- Označimo sa $I = \{A \in F \ : \models A\}$ skup tautologija a sa $\mathcal{T} = \{A \in F \ : \vdash A\}$ skup teorema.
  - Ako je $\mathcal{T} \subset I$ formalizacija je korektna.
  - Ako je $I \subset \mathcal{T}$ formalizacija je potpuna.
- **Teorema**.(korektnosti) Svaka teorema iskaznog računa je tautologija tj. $\mathcal{T} \subset I$ (odnosno $\vdash A \ \Rightarrow \models A$).
- **Teorema**.(opšta teorema korektnosti) Neka je A IF i Σ skup IF. Tada, ako je $\Sigma \vdash A$ onda je $\Sigma \models A$.
  $\lceil$ Tj. svaka posljedica od Σ je logička posljedica od Σ. $\rfloor$
- Teorema korektnosti slijedi iz opšte teoreme korektnosti kada uzmemo $\Sigma = \emptyset$.
- Zato dokazujemo samo opštu teoremu korektnosti jer su dokazi slični.

- **Dokaz**. (opšte teoreme korektnosti)

  Neka je $\Sigma \vdash A$. To (po definiciji) znači da postoji niz formula $A_1, \ldots, A_n$ koji je dokaz za IF A iz Σ. Dokažimo da je tada $\Sigma \models A$. Dokaz izvodimo indukcijom po dužini dokaza za IF.

  Baza indukcije: $n = 1$.
  Imamo da je niz A_1 dokaz za IF A_1 iz Σ pa je $A_1 \in T \cup \Sigma$.

  - Ako je $A_1 \in T$ onda je (po izboru skupa aksioma) $\models A_1$ pa je i $\Sigma \models A_1$.
  - Ako je $A_1 \in \Sigma$ onda je $\Sigma \models A_1$ (jer ako je $v(\Sigma) = 1$ onda je i $v(A_1) = 1$).

  Indukcijski korak.
  Pretpostavimo da tvrđenje važi za svaku formulu koja ima dokaz dužine k, $k < n$, dokažimo da tada tvrđenje važi i za formulu koja ima dokaz dužine n.

Neka je $A_1, \ldots, A_n$ dokaz za IF A_n iz Σ. Tada je $A_n \in T \cup \Sigma$ ili postoje $i, j < n$ takvi da je $A_j = A_i \to A_n$.

- Ako je $A_n \in T \cup \Sigma$ onda A_n ima dokaz dužine 1 pa se dokaz svodi na bazu indukcije.
- Ako postoje $i, j < n$ takvi da je $A_j = A_i \to A_n$ (tj. A_n se dobija po MP iz A_i i A_j) onda po ind. p.p. $\Sigma \vdash A_i \Rightarrow \Sigma \models A_i$ i $\Sigma \vdash A_j \Rightarrow \Sigma \models A_j$. Odnosno imamo $\Sigma \models A_i$ i $\Sigma \models A_i \to A_n$. Pa ako je $v \in 2^P$ proizvoljna valuacija takva da je $v(\Sigma) = 1$ onda je $v(A_i) = 1$ i $v(A_i \to A_n) = 1$ pa je i $v(A_n) = 1$. Što upravo znači da je $\Sigma \models A_n$.

Na osnovu principa matematičke indukcije zaključujemo da važi $\Sigma \models A$ (jer IF A ima dokaz određene dužine). Što je i trebalo dokazati.

- Komentar. Direktni dokaz za teoremu korektnosti možemo dobiti tako što prepišemo prethodni samo izostavljamo savko pojavljivanje Σ i tekst direktno vezan za Σ.

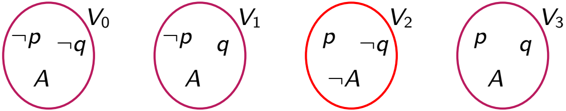
Teorema potpunosti isklaznog računa

- Postoji više načina da se dokaže teorema potpunosti iskaznog računa. Navodimo jedan od tih dokaza čija se ideja koristi za dokaz teoreme potpunosti i kod drugih logika.
- Da bi mogli da sprovedemo takav dokaz izvršićemo određene pripreme.

Primjer. Neka je $A = p \to q$ i $\overline{Sub}(A) = \{p, q, A, \neg p, \neg q, \neg A\}$. Svakoj od 4 moguće valuacije (promenljivih p i q)

$$v_0 : \begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix} \quad v_1 : \begin{pmatrix} p & q \\ 0 & 1 \end{pmatrix} \quad v_2 : \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix} \quad v_3 : \begin{pmatrix} p & q \\ 1 & 1 \end{pmatrix}$$

možemo pridružiti (logički) konzistentan skup
$V_i = \{B \in \overline{Sub}(A) : v_i(B) = 1\}$, $i = 0, 1, 2, 3$.



Uočimo sledeće.

- Ako skupu V_i dodamo formulu $B \in \overline{Sub}(A) \setminus V_i$ dobijamo (logički) nekonzistentan skup.
- Skupovi npr. $\{p, q, \neg A\}$ i $\{p, \neg q, A\}$ su (logički) nekonzistentni, dok skup $\hat{V} = \{\neg p, A\}$ je (logički) konzistentan i možemo ga "proširiti" sa konzistentnim skupom V_0 ili V_1.
- Svaki od skupova V_i jednoznačno određuje valuaciju v_i koja ga zadovaoljava. Takvu valuaciju možemo definisati sa: $v_i(s) = \begin{cases} 0 & , \quad \neg s \in V_i \\ 1 & , \quad s \in V_i \end{cases}$ ili sa $v_i(s) = \begin{cases} 0 & , \quad s \notin V_i \\ 1 & , \quad s \in V_i \end{cases}$ gdje je $s \in \{p, q\}$.
- Skup $\hat{V}$ ne određuje jedinstveno valuaciju, jer ga zadovaljavaju v_0 i v_1. Razlog je što ga možemo "proširiti".

Pripreme

- **Def.** Za skup IF Σ kažemo da je kompletan ako je Σ konzistentan i za svaku IF A važi $\Sigma \vdash A$ ili $\Sigma \vdash \neg A$.
- **Def.** Za skup IF Σ kažemo da ima kompletno proširenje ako postoji kompletan skup $\overline{\Sigma}$ takav da je $\Sigma \subset \overline{\Sigma}$.
- **Lema**. Svaki konzistentan skup IF ima kompletno proširenje.
- **Dokaz**. Neka je Σ konzistentan skup. Poređajmo sve IF u niz $A_1, A_2, \ldots$ tj. $F = \cup\{A_i\}$. Induktivno formirajmo niz konzistentnih skupova formula (Σ_i) sa: $\Sigma_0 = \Sigma$, ako smo formirali konzistentan skup Σ_{k-1} onda za Σ_k uzimamo jedan od skupova Σ_{k-1}, A_k ili $\Sigma_{k-1}, \neg A_k$ koji je konzistentan.
  ⌈ Bar jedan od navedena dva skupa je konzistentan, jer bi u suprotnom (po $\neg P$) $\Sigma_{k-1} \vdash \neg A_k$ i $\Sigma_{k-1} \vdash \neg(\neg A_k)$. ⌋
  Neka je $\overline{\Sigma} = \cup_{k=0}^{\infty} \Sigma_k$. Očito, $\Sigma \subset \overline{\Sigma}$ i $\Sigma_{k-1} \subset \Sigma_k$.

Skup $\overline{\Sigma}$ je konzistentan. Zaista, u suprotnom postoji formula B takva da je $\overline{\Sigma} \vdash B$ i $\overline{\Sigma} \vdash \neg B$. Odnosno postoji niz formula $C_1, \ldots, C_p$ dokaz za $C_p = B$ iz $\overline{\Sigma}$ i niz $D_1, \ldots, D_q$ dokaz za $D_q = \neg B$ iz $\overline{\Sigma}$. Skup $C_i, D_j \in \overline{\Sigma}$ je konačan pa postoji m tako da Σ_m sadrži te formule. Otude $\Sigma_m \vdash B$ i $\Sigma_m \vdash \neg B$ što je u suprotnosti sa činjenicom da je Σ_m konzistenta.

Za proizvoljnju formulu $E = A_r$ važi $E \in \Sigma_r \subset \overline{\Sigma}$ ili $\neg E \in \Sigma_r \subset \overline{\Sigma}$ pa je $\overline{\Sigma} \vdash E$ ili $\overline{\Sigma} \vdash \neg E$ tj. $\overline{\Sigma}$ je kompletan.

Dakle, $\overline{\Sigma}$ je kompletan i $\Sigma \subset \overline{\Sigma}$ pa je skup $\overline{\Sigma}$ kompletno proširenje od Σ.

- **Lema**. Svaki kompletan skup iskaznih formula je zadovoljiv. (tj. Σ kompletan $\quad \Rightarrow \quad (\exists v \in 2^P) v(\Sigma) = 1$.)
- **Dokaz**. Neka je $v \in 2^P$ valuacija definisana sa: za $p \in P$

$$v(p) = \begin{cases} 1 & , \quad \Sigma \vdash p \\ 0 & , \quad \text{inače} \end{cases}$$

Dokažimo da tada za svaku IF A važi:

$$v(A) = 1 \quad \text{akko} \quad \Sigma \vdash A.$$

Dokaz možemo izvesti indukcijom po složenosti formule A.

1. $A = p \in P$: $v(p) = 1 \Leftrightarrow \Sigma \vdash p$ po definiciji v.
2. $A = \neg B$: $v(A) = 1 \overset{semantika}{\Longleftrightarrow} v(B) = 0 \overset{ind.p.p.}{\Longleftrightarrow} \Sigma \nvdash B \overset{\star\star\star}{\Longleftrightarrow}$ $\Sigma \vdash \neg B \Leftrightarrow \Sigma \vdash A$, ($\overset{\star\star\star}{\Longrightarrow}$ zbog Σ kompletan; $\overset{\star\star\star}{\Longleftarrow}$ zbog Σ konzistentan).
3. $A = B \wedge C$: $v(A) = 1 \overset{semantika}{\Longleftrightarrow} v(B) = 1$ i $v(C) = 1 \overset{ind.p.p.}{\Longleftrightarrow} \Sigma \vdash B$ i $\Sigma \vdash C \overset{P\wedge}{\Longleftrightarrow} \Sigma \vdash B \wedge C \Leftrightarrow \Sigma \vdash A$.

Dakle, ako je $A \in \Sigma$ onda $\Sigma \vdash A$ pa $v(A) = 1$ tj. $v(\Sigma) = 1$.

- **Teorema**. (opšta teorema potpunosti) Skup iskaznih formula je zadovoljiv akko je konzistentan.
- Tj. Σ zadovoljiv akko Σ konzistentan.

- **Dokaz**. $(\Rightarrow)$: Neka je skup IF Σ zadovoljiv. Tada postoji $v \in 2^P$ tako da je $v(\Sigma) = 1$, odnosno za svako $A \in \Sigma$ je $v(A) = 1$. Za proizvoljnu IF C tvrdimo da važi:

  $$\text{ako je } \Sigma \vdash C \text{ onda je } v(C) = 1. \qquad (\star)$$

  Tvrđenje $(\star)$ dokazujemo indukcijom po dužini dokaza za C. Ako je C_1 dokaz (dužine $n = 1$) za $C = C_1$ iz Σ onda je $C_1 \in T, \Sigma$ pa je $v(C_1) = 1$ tj. $v(C) = 1$.
  Neka je $C_1, \ldots, C_n$ dokaz za $C = C_n$ iz Σ. Pretpostavimo da tvrđenje važi za sve IF koji imaju dokaz dužine manje od n. C_n se dobija po MP iz njoj prethodnih formula C_k i $C_j = C_k \to C_n$, $k, j < n$. Pa po ind.p.p. $\Sigma \vdash C_k \Rightarrow v(C_k) = 1$ i $\Sigma \vdash C_j \Rightarrow v(C_j) = 1$
  tj. $v(C_k \to C_n) = 1$. Pa po semantičkim pravilima iz $v(C_k) = 1$ i $v(C_k \to C_n) = 1$ dobijamo $v(C_n) = 1$ tj. $v(C) = 1$.

  Ako Σ nije konzistentan onda bi postojala IF B takva da je $\Sigma \vdash B$ i $\Sigma \vdash \neg B$ tj. $v(B) = 1$ i $v(\neg B) = 1$, što je nemoguće. Dakle, Σ je konzistentan.

$(\Leftarrow)$: Neka je skup IF Σ konzistentan i neka je (po Lemi) $\overline{\Sigma}$ njegovo kompletno proširenje. Postoji (po drugoj Lemi) valuacija $v \in 2^P$ takva da je $v(\overline{\Sigma}) = 1$ pa je i $v(\Sigma) = 1$ (jer je $\Sigma \subset \overline{\Sigma}$). Dakle, skup IF Σ je zadovoljiv.

- **Teorema**. (potpunosti) Svaka tautologija je teorema iskaznog računa. $\lceil$ Tj. $I \subset \mathcal{T}$; odnosno $\models A \Rightarrow \vdash A$. $\rfloor$
- **Dokaz**. Neka je IF A tautologija (tj. $\models A$). Tada skup $\Sigma = \{\neg A\}$ nije zadovoljiv pa po opštoj teoremi potpunosti on nije konzistentan. Znači da postoji IF B takva da je $\neg A \vdash B$ i $\neg A \vdash \neg B$. Sada po $P\neg$ (tj. pravilu za dokazivanje negacije) dobijamo $\emptyset \vdash \neg(\neg A)$. Odnosno $\vdash A$, tj. A je teorema.
- Iz teoreme korektnosti i teoreme potpunosti dobijamo da važi:
- **Teorema**. Iskazna formula je teorema akko je tautologija.

  $\lceil$ Tj. $\mathcal{T} = I$; odnosno $\vdash A \Leftrightarrow \models A$. $\rfloor$

- Znači i u semantičkom i u formalnom pristupo dolazimo do istog skupa istina.
- **Teorema**. (kompaktnosti) Ako je svaki konačni podskup skupa iskaznih formula Σ zadovoljiv onda je i Σ zadovoljiv.
- **Dokaz**. Pretpostavimo suprotno tj. Σ nije zadovoljiv. Po opštoj teoremi potpunosti onda Σ nije konzistentan. Poslednje znači da postoji IF B takva da $\Sigma \vdash B$ i $\Sigma \vdash \neg B$.

  Neka je niz IF $C_1, \ldots, C_k$ dokaz za IF $B = C_k$ iz Σ a niz $C_{k+1}, \ldots, C_n$ dokaz za IF $\neg B = C_n$ iz Σ. Formirajmo konačan skup $\Sigma_1 = \{C_j \ : \ 1 \leq j \leq n \text{ i } C_j \in \Sigma\}$. Navedeni dokazi iz Σ su ujedno i dokazi iz Σ_1 tj. važi $\Sigma_1 \vdash B$ i $\Sigma_1 \vdash \neg B$. Što znači da Σ_1 nije konzistentan pa samim tim (po opštoj teoremi potpunosti) nije zadovoljiv.

  Dakle, našli smo konačan skup Σ_1 koji je podskup od Σ i koji nije zadovoljiv. Ovo je u suprotnosti sa pretpostavkom teoreme. Znači Σ je zadovoljiv.

Intuicionistička logika

- Stinaksa intuicionističke logike je ista kao sintaksa iskazne logike, koju smo proučili. Pa se zato naziva **intuicionistička iskazna logika**. A onda se logika koju smo prethodno proučavali naziva **klasična iskazna logika** stim što se cesto izostavlja atribut klasična.
- Intuicionistička od klasične iskazne logike se razlikuje po skupu "istina". Tako se mora razlikovati po semantici (koja je trovalentna) kao i u formalizaciji (izostavlja se zakon isključenja trećeg).
- Intuicionistička (matematička) rasuđivanja se razlikuju od klasičnih što ne prihvataju postojanje (matematičkih) objekata bez njihove eksplicitne (direktne) konstrukcije.
- Klasični matematičari ponekad tvrde (dokažu) da nešta postoji a da ne mogu pokazati primjer toga tj. ne znaju šta je to.

- Zadatak. Pokazati da postoje iracionalni brojevi α i β takvi da je broj α^β racionalan.
- Rj. Ako je broj $\gamma = \sqrt{2}^{\sqrt{2}}$ racionalan onda treba uzeti $\alpha = \sqrt{2}$ i $\beta = \sqrt{2}$. Ako je γ iracionalan broj onda treba uzeti $\alpha = \gamma$ i $\beta = \sqrt{2}$.
- Klasični matematematičar prihvata prethodni dokaz a intuicionista to ne prihvata jer se ne zna da li je $\alpha = \sqrt{2}$ ili $\alpha = \sqrt{2}^{\sqrt{2}}$.
  Napomena. Danas zna da je $\sqrt{2}^{\sqrt{2}}$ iracionalan broj.

- Da bi izbjegli da zakon isključenja trečeg bude tautologija neophodno je da u semantici dopustimo i treću vrijednost. To onda povlači da i veznike drugačije tumačimo (tj. veznici imaju drugu semantiku).

Semantika

Preslikavanje $v : P \to \{0, \frac{1}{2}, 1\}$ je valuacija iskaznih slova intuicionističke logike a (semantička) pravila njenog proširenja (na skup svih formula) su data tablicom.

$v(A)$	$v(B)$	$v(\neg A)$	$v(A \wedge B)$	$v(A \vee B)$	$v(A \to B)$
0	0	1	0	0	1
0	$\frac{1}{2}$	1	0	$\frac{1}{2}$	1
0	1	1	0	1	1
$\frac{1}{2}$	0	0	0	$\frac{1}{2}$	0
$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	1
$\frac{1}{2}$	1	0	$\frac{1}{2}$	1	1
1	0	0	0	1	0
1	$\frac{1}{2}$	0	$\frac{1}{2}$	1	$\frac{1}{2}$
1	1	0	1	1	1

- Uočimo da je $v(p \wedge q) = \min\{v(p), v(q)\}$; $v(p \vee q) = \max\{v(p), v(q)\}$; $v(p \to q) = 1$ za $v(p) \leq v(q)$, $v(p \to q) = \frac{1}{2}$ za $v(p) = 1$ i $v(q) = \frac{1}{2}$ i $v(p \to q) = 0$ u ostalim slučajevima.
- Formula A je 3-tautologija ako za svaku valuaciju v važi $v(A) = 1$.
- **Teorema**. Formula $p \vee \neg p$ nije 3-tautologija.
- **Dokaz**. Za $p = \frac{1}{2}$ dobijamo $v(p \vee \neg p) = \frac{1}{2}$.
- Dakle u ovakoj semantici ne važi zakon isključenja trećeg.
- Zadatak. Dokazati da su svaka od aksioma T_1 do T_{10} 3-tautologije.
- **Teorema**. Svaka 3-tautologija je tautologija klasične logike.

Formalizacija

- Za aksiome se uzimaju formule iz skupova T_1 do T_{10}.
- Pravilo izvođenja je MP.
- Definicije dokaza, teoreme, posljedice su iste klasičnoj logici.

- **Teorema**. Formula $p \vee \neg p$ nije dokaziva u intuicionističkoj logici.

- Zadatak. Dokazati da formula $\neg\neg p \to p$ nije dokaziva u intuicionističkoj logici a formula $\neg\neg(\neg p) \to (\neg p)$ jeste dokaziva u intuicionističkoj logici. Provjeri da li su navedene formule 3-tautologije. $\lceil$ Uočiti: $v(\neg p) \in \{0, 1\}$. $\rfloor$
- Prethodni zadatak nam ukazuje da dokazivost formula zadatih shemom $\neg\neg A \to A$ zavisi od strukture formule A.

KRAJ!

slajdova sa iskaznom logikom

SLIJEDI:

Predikatska logika prvoga reda