UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
NOVI SAD

Marko Stupar

MODALNA LOGIKA I PRIMENA U ZAŠTITI INFORMACIONIH SISTEMA

- master rad -

Mentor: dr Silvia Ghilezan

Novi Sad, 2016.

Uvod

Modalna logika je vrsta formalne logike koja je razvijena 1960-ih godina. Ona proširuje iskaznu i predikatsku logiku sa modalitetima - rečima koje kvalifikuju iskaz. Postoji više vrsta modalne logike. Postoji epistemološka ili doksastička logika koje posmatraju znanje i verovanje; deontička logika posmatra moral; temporalna logika koja posmatra vremenski faktor. Međutim, najzastupljenija je logika koja se bavi mogućnostima i nužnostima. Ona se još naziva i alethička logika, prema grčkoj reči *'alethia'* što znači istina. Većina ljudi kada govori o modalnoj logici ima upravo ovu logika na umu zato što je toliko dominantna u svetu modalnih logika. U ovom radu ćemo se upravo bavit ovom logikom, dok ćemo se u samoj primeni modalne logike baviti i drugim vrstama modalne logike.

Ono što je bitno da se naglasi u uvodu jeste da se u master radu radi o hilbertovskoj formulaciji. Hilbertovsku formulaciju (Hilbertov sistem) karakteriše veliki broj aksiomskih shema i mali broj pravila izvoĐenja. Postoji više varijanti formalnih teorija koje opisuju iskaznu logiku i definisane su u Hilbertovom stilu, ali najčešće proučavani Hilbertovi sistemi imaju samo jedno pravilo izvoĐenja za iskaznu logiku - modus ponens; ili dva za predikatsku logiku - modus ponens i pravilo generalizacije. Uz ova pravila ide i nekoliko beskonačnih aksiomskih shema. Kasnije u radu ćemo videti da su Hilbertovi sistemi za modalnu logiku prošireni sa još dva pravila izvoĐenja a to su pravilo nužnosti i pravilo uniformne substitucije. TakoĐe, teoreme iz iskazne logike nećemo dokazivati već ćemo predpostaviti da su poznate jer ovaj rad se nastavlja na iskaznu logiku.

Da bi dali jedan kompletan prikaz modalne logike bitno je da počnemo od istorije modalne logike i načina na koji se ona razvijala. Zbog toga se u prvom poglavlju bavimo istorijom modalne logike i govorićemo o tri perioda kroz koja je modalna logika prošla u svom razvijanju.

U drugom poglavlju predstavljena je sintaksa modalne logike kao i pojam i semantiku mogućih svetova. Da bi razumeli modalnu logiku moramo razumeti koncept mogućih svetova koji na odličan način objašnjava modalnu logiku.

U trećem poglavlju dajemo detaljan prikaz osnovnih sistema modalne logike i govoriomo o njihovim sličnostima, razlikama kao i o teoremama koje važe u tim sistemima. TakoĐe tu možemo pronaći i dokaze navedenih teorema.

U četvrtom poglavlju je dat prikaz semantike sistema koji su predstavljeni u tećem poglavlju. Videćemo u kakvom su odnosu ti sistemi i šta ih čini jedinstvenima.

Takođe, tu ćemo videti jedan neformalan i jedan formalan pristup semantici sistema o kojima govorimo.

U poslednjem poglavlju date su neke primene modalne logike u zaštiti informacionih sistema. Ovo pitanje je veoma interesantno i aktuelno danas zbog brojnih zloupotreba i prevara koje se dešavaju više nego ikad i zbog toga je veoma važno unapređivati bezbednosne sisteme koje koristimo.

***

Izuzetnu zahvalnost dugujem svojoj mentorki, prof. dr Silviji Ghilezan, na ukazanom poverenju, pruženom znanju, požrtvovanosti, velikom strpljenju i pomoći, kao i na korisnim sugestijama i primedbama bez kojih ne bih uspeo da završim ovaj master rad.

Posebnu zahvalnost dugujem i svojoj porodici, supruzi i prijateljima koji su mi bili podrška tokom čitavih studija.

Novi Sad, septembar 2016. godina

Marko Stupar

Sadržaj

Glava 1

Istorija i razvoj modalne logike

U ovom poglavlju ćemo dati kratak pregled istorije modalne logike kao i način na koji se ona razvijala. Istorijiski podaci, kao i slike su preuzeti iz [15], [17] i [18]. Takođe ćemo govoriti o ljudima koji su najviše uticali i doprineli razvoju modalne logike. Istoriju modalne logike možemo podeliti u tri bitna perioda, a to su:

Rani period

Sintaksni period (od 1918. do 1959.)

Klasičan period (od 1959. do 1972.)

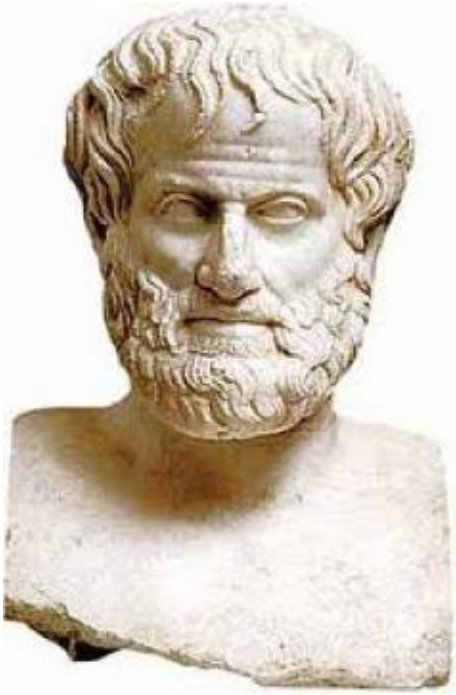
1.1 Rani period

Modalna logika se pojavljuje još kod antičkih Grka. Ona počinje sa Aristotelovom analizom izjava koje sadrže reči "nužno" i " moguće". Aristotel (384. pne.-322. pne.) je pisao i razvio argument o modalnoj silogistici u svojoj knjizi "Analytica Priora". Takođe, postoje neki odlomci u njegovim delima, poput argumenta "pomorske bitke" u knjizi "De Interpretatione" koje sada vidimo kao pokušaj spajanja modalne logike sa potencijalnošću i vremenom.

Aristotel je koristio bitku kod Salamine da pokaže ovaj argument. Argument može da se sumira na sledeći način: predpostavimo da sutra neće doći do pomorkse bitke. Pošto je svaki tačan iskaz o onome što će se desiti u budućnosti tačan i u prošlosti, onda je ovaj iskaz bio tačan i juče i pre nedelju dana i pre godinu dana. Dakle, sve ranije istine su sada i nužne istine. Zato je sada ova izjava nužna istina u prošlosti i sve do prvobitne izjave:"Pomorske bitke neće biti", da se bitka neće desiti, i zato je izjava da će pomorkse bitke desiti nužno netačna. Stoga, nije moguće da će se bitka voditi. U principu, ako nešto neće biti slučaj, nije moguće da to bude slučaj. Citat iz njegove knjige kaže:"Čovek može da predvidi događaj 10 000 godina unapred. Drugi može da predvidi suprotno. Ono što je bilo tačno predviđeno u prošlosti će se ispuniti u punini vremena".

Aristotel je rešio ovaj problem tvrdeći da dvovalentnost pravi izuzetak u ovom problemu. U ovom konkretnom slučaju, ono što je nemoguće je da obe alternative mogu biti moguće u isto vreme: ili će biti bitka, ili neće. Danas, one nisu ni istinitne ni lažne; ali ako je jedna istinita, onda druga postaje lažna. Moramo da sačekamo da se događaj desi (ili ne desi) kako bi utvrdili koje je tačan a koji ne.

Dakle, Aristotel je uveo pojam nepredviđene situacije. Ovaj pojam očuvava logiku dok u isto vreme ostavlja prostor za neodlučnost u realnosti. Nije nužno da li će biti ili neće biti bitke nego je nužna dihotomija. Aristotel dodaje:"Pomorska bitka ili mora da se desi sutra, ili se neće desiti, ali nije nužno da treba da se desi i nije nužno da ne treba da se desi. Nužno je da ili treba ili ne treba da se desi".



Slika 1: Aristotel

Diodor Kron (Diodorus Cronus) iz Megarske škole filozofije se takođe bavio ovim problemom. Za njega je buduća bitka na moru ili nemoguća ili nužna. On je smatrao da Aristotelov pojam nepredvidive situacije predstavlja samo naše neznanje.

Najraniji formalni sistem temporalne modalne logike je razvio persijski matematičar Avicena (980-1037). On je razvio teoremu "vremenskog modala". On je proučavao odnos između vremena i njegove implikacije. Njegov sistem je kasnije razvio Najm al Din al Kazvini al Katibi (Najm al-Din al-QazwinÄ« al-Katibi) i on je postao dominantan sistem islamske logike. Avicenina logika je takođe uticala na

nekoliko ranih evropskih logičara poput Vilijama od Okhama (William of Ockham), Alberta Magnusa (Albertus Magnus) i Džon Dans Skotusa (John Duns Scotus) koji su obrazložili na modalan način iskaze o suštini i slučajnosti.

Gotfrid Vilhelm Frajher (baron) fon Lajbnic (Gottfried Wilhelm Leibniz) (1646-1716) uvodi termin "mogući svetovi". On je tvrdio da su mogući svetovi sačinjeni od pojedinaca koji mogu da postoje zajedno. Takođe je tvrdio da svi mogući svetovi postoje u Božjem umu i da ovaj u kome živimo je najsavršeniji. Lajbnic uvodi dve vrste nužnosti: univerzalna nužnost i pojedinačna nužnost. Univerzalna nužnost se tiče univerzalnih istina, dok se pojedinačna nužnost odnosi na nešto nužno što nije trebalo da se desi (slučajno).

Slika 2: Gotfrid Vilhelm Frajher fon Lajbnic

1.2 Sintaksni period

Aristotel je razlikovao nužno, moguće, nemoguće, stvarno, sholastici su razlikovali realni i iskazni modalitet, prema čemu su formirali principe modaliteta, ali je tek Klarens Irving Luis (C. I. Lewis) (1883-1964) postavio prvi sistem modalne logike. K.I. Luis se smatra osnivačem moderne modalne logike. Njegove teze sa Harvarda i različiti naučni članci objedinjeni su 1932. godine u knjizi koja se zove "Logika simbola". U njoj je predstavio 5 sistema modalne logike (S1, S2, S3, S4 i S5).

Ovaj period takođe karakteriše paradoks materijalne implikacije. Ovaj paradoks predstavlja grupu formula koje su tačne u klasičnoj logici ali su intuitivno problematične. To je zbog načina na koji tumačimo implikaciju. U prirodnom jeziku

implikaciju tumačimo kao logičnu posledicu, međutim njena formalna interpretacija u klasičnoj logici je drugačija. Luis je 1912. godine definisao strogu implikaciju na sledeći način:"nužno je da iz p sledi q" ili matematički zapisano $_{def}\Box(p \Rightarrow q)$.On je želeo da eliminiše sve teoreme koje su tačne za materijalnu implikaciju ali nisu za strogu implikaciju.

Slika 2: Klarens Irving Luis

Pomenućemo još četiri naučnika čiji su radovi obeležili ovaj period a to su Rudolf Karnap (Rudolf Carnap) (1891-1970), Artur Prior (Arthur Prior) (1914-1969), Bjarni Džonson (Bjarni Jonsson) rođen 1920. godine i Alfred Tarski (1901 -1983).

Rudolf Karnap je razvio svoju ideju o opisu stanja. Ovaj model se tada koristio kao formalna semantika za sistem S5. Model je sličan Lajbnicovom modelu mogućih svetova i prethodnik je Kripkeove semantike mogućih svetova. Artur Prior je veliki doprinos dao postavljanjem osnova i radom na vremenskoj logici (Tense Logics).

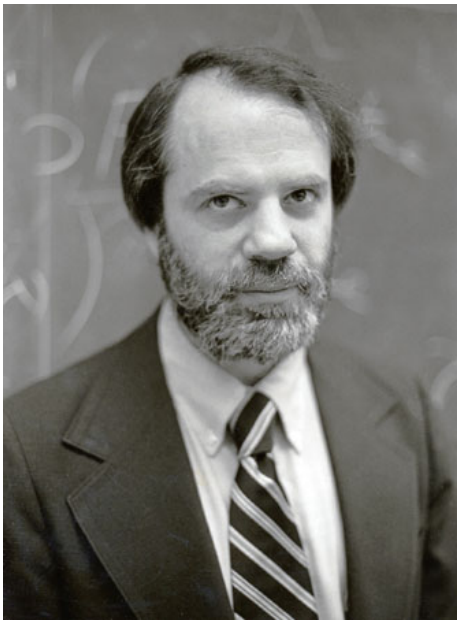
1.3 Klasičan period

Najuticajniji naučnik ovog perioda u svetu modalne logike je bio Saul Kripke. On je kao devetnaestogodišnji student Harvard Univerziteta predstavio novu semantiku

modalne logike, koja se sada po njemu naziva "Kripkeova semantika". Često je nazivana i semantika mogućih svetova. Ovo otkriće je bio proboj u teoriji neklasičnih logika, jer modalna teorija ovakve logike gotovo da nije postojala u to vreme. On je uveo i pojam relacije dostupnosti o čemu ćemo govoriti više kasnije. Iako su i drugi naučnici razmišljali o ovome, niko to nije tako dobro formalizovao poput Kripkea.

Džon Lemon (John Lemmon) (1930-1966) i Dejna Skot (Dana Scott), rođen 1932. godine su pioniri modernog pristupa sematici modalne logike. Njihova zajednička kniga "Uvod u modalnu logiku" izadata je 1977. godine, 11 godina nakon smrti Lemona.

U ovom kratkom razdoblju od 50 godina između Luisa i Kripkea, modalna logika je doživela svoj procvat u filozofskom ali i u matematičkom smislu.



Slika 4: Saul Kripke

Glava 2

Osnovni pojmovi modalne logike

U ovom poglavlju ćemo definisati osnovne pojmove modalne logike i pokazati u kakvoj su oni relaciji. Definisaćemo nužnost, nemogućnost, kontigentnost i mogućnost kao i podrazumevanje. Takođe ćemo uvesti i oznake sa kojim ih obeležavamo. Predstavićemo i koncept mogućih svetova. Literatura koja je korišćena je [2], [7] i [14].

2.1 Sintaksa modalne logike

Između tačnih iskaza možemo razlikovati one koji mogu da se dese da su istiniti i oni koji su uvek istiniti (ili koji ne mogu da su pogrešni). Slično, među netačnim iskazima možemo razlikovati one koji se dese da su netačni i oni koji su uvek netačni (koji ne mogu da budu istiniti). Iskaz koji je uvek tačan nazivamo *nužni iskaz* ; one koji su uvek netačni nazivamo *nemogući iskazi*; a oni koji nisu ni nužni ni nemogući nazivamo *kontigentni* iskazi. Neki kontigentni iskazi će biti tačni, a drugi neće. Ako iskaz nije nemoguć onda za njega kažemo da je *moguć* iskaz. Mogući iskazi uključuju sve iskaze osim onih koji su nemogući.

Ova četiri pojma, nužnost, nemogućnost, kontigentnost i mogućnost čine modalne pojmove. Modalni veznici $\Box$ i $\Diamond$ označavaju "nužno je da" i "moguće je da", respektivno. Ovo su unarni modalni veznici. Oni su povezani jedan sa drugim; čak možemo da objasnimo bilo koja tri pojma pomoću četvrtog. Posebno je važna sledeća veza između nužnosti i mogućnosti: ako kažemo da je iskaz p nužan iskaz, ekvivalentno je tome da kažemo da nije moguće da je p netačno; i ako kažemo da je p moguće tačan, ekvivalentno je tome da kažemo da nije nužno tačno da je p netačno. Ovo možemo zapisati i na ovaj način:

$$\Box p \Leftrightarrow \neg\Diamond\neg p$$

$$\Diamond p \Leftrightarrow \neg\Box\neg p$$

Formule u modalnoj logici se formiraju na isti način kao i formule u iskaznoj logici samo što još dodajemo gore 2 navedena pravila. Iskaz $\Box p$, čitamo "nužno je da p", je

tačan ako je p nužno, odnosno netačan ako p nije nužno. Međutim, samo na osnovu istinitosti iskaza p ne možemo da utvrdimo da li je $\Box p$ tačno ili ne. Isto važi i za $\Diamond p$; čitamo "moguće je da p". Formula $\Diamond p$ će biti tačna kada je p moguće a netačno kada p nije moguće. Takođe istinitost iskaza $\Diamond p$ ne zavisi od toga da li je iskaz p tačan ili ne. Uvodimo još jedan modalni pojam, a to je "podrazumevanje". Ako kažemo da se iz iskaza p podrazumeva iskaz q, to jednostavno znači da je q logička posledica iskaza p. Ovaj pojam ćemo obeležavati sa $\prec$.

Primer 2.1.0.1 *Moguće je da će padati kiša danas ako i samo ako nije nužno da neće padati kiša; i nužno je da će danas padati kiša ako i samo ako nije moguće da neće padati kiša danas.*

2.2 Mogući svetovi

Primer 2.2.0.1 *U našem svetu, svetu u kojem živimo, nacistička Nemačka je izgubila Drugi svetski rat. Ali naravno, stvari su mogle biti drugačije. Ono što radimo jeste da zamišljamo druge mogućnosti. U ovom svetu su Nemci izgubili rat ali u nekom mogućem svetu bi oni pobedili. Dakle, za svaki način na koje su stvari mogle biti drugačije postoji mogući svet. Isto možemo da uradimo i za nužnost. Kada tvrdimo da je 1+1=2 to mora biti tačno u svakom mogućem svetu.*

Kada kažemo "moguće da p" ili $\Diamond p$, to možemo da interpretiramo sa: "U nekom mogućem svetu, p je slučaj.". Analogno, kada tvrdimo da je $\Box p$ slučaj, znači da je p slučaj u svakom mogućem svetu.

2.3 Semantika mogućih svetova

Način na koji koristimo moguće svetove je pomoću modela. Svaki model se sastoji od tri elementa $< W, R, v >$. W predstavlja skup mogućih svetova $W \in (w_0, w_1, w_2, ...)$, v je funkcija dodele koja dodeljuje istinitostne vrednosti iskazima. U iskaznoj logici ona dodeljuje vrednosti iskazima dok u modalnoj logici, ona dodeljuje istinitosne vrednosti iskazu u svakom mogućem svetu. O ovome ćemo govoriti više u četvrtom poglavlju.

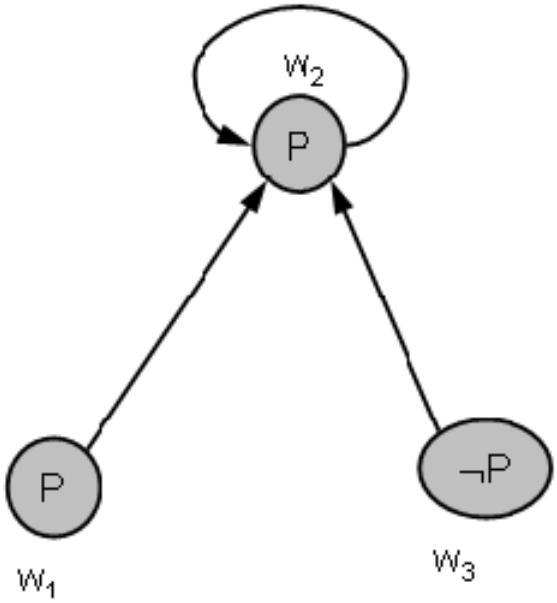
Primer 2.3.0.1 *Neka je w_0 svet u kojem živimo i neka sa p obeležavamo iskaz: "Svinje imaju krila". Tada dobijamo $v_{w0}(p) = 0$ što znači da je vrednost iskaza p u svetu w_0 netačna. Međutim ako izaberemo neki svet w_1 gde svinje imaju krila tada važi $v_{w1}(p) = 1$*

Binarna relacija između mogućih svetova u W označavamo sa R i naziva se relacija dostupnosti. Relaciju dostupnosti između svetova w_o i w_1 zapisuje se na sledeći način: w_oRw_1 i čitamo:"w_1 je dostupno iz w_0".

Definicija 2.3.0.1 *$v_{w1}(\Box p) = 1$ akko za svako w_i takav da w_1Rw_i , $v_{wi}(p) = 1$*

Definicija 2.3.0.2 *$v_{w1}(\Diamond p) = 1$ akko postoji w_i takav da w_1Rw_i , $v_{wi}(p) = 1$*

Pokazaćemo ovo na jednom primeru.



Slika 5: Primer mogućih svetova

Primer 2.3.0.2 *Na slici 5 vidimo da se skup mogućih svetova W sastoji od tri moguća sveta $W = \{w_1, w_2, w_3\}$. Odnos dostupnosti je na slici prikazan strelicama. Vidimo da je w_1Rw_2, w_2Rw_2 i w_3Rw_2. Takođe vidimo da $v_{w1}(p) = v_{w2}(p) = 1$ i $v_{w3}(p) = 0$. Sada pogledajmo neke primere u datom jeziku modalne logike:* $\Diamond p$ $v_{w1}(\Diamond p) = 1$ $v_{w2}(\Diamond p) = 1$ $v_{w3}(\Diamond p) = 1$ $\Box p$ $v_{w1}(\Box p) = 1$ $v_{w2}(\Box p) = 1$ $v_{w3}(\Box p) = 1$ $\Diamond\Box p$ $v_{w1}(\Diamond\Box p) = 1$ $v_{w2}(\Diamond\Box p) = 1$ $v_{w3}(\Diamond\Box p) = 1$ $\Box p \Rightarrow p$ $v_{w1}(\Box p \Rightarrow p) = 1$ $v_{w2}(\Box p \Rightarrow p) = 1$ $v_{w3}(\Box p \Rightarrow p) = 0$

Vidimo da je $v_{w1}(\Diamond p) = 1$ *zbog toga što postoji barem jedan svet koji svet* $w1$ *vidi gde je* $v(p) = 1$ *a to je svet* w_2*. Pošto je svet* w_2 *ujedno i jedini svet koji svet* w_1 *vidi dobijamo da je* $v_{w1}(\Box p) = 1$*. Pošto je* $v_{w2}(\Box p) = 1$ *dobijamo i da je* $v_{w1}(\Diamond\Box p) = 1$ *zato što postoji svet koji svet* w_1 *vidi gde je* $\Box p = 1$*, a to je upravo svet* w_2*. Na kraju lako zakljucujemo da je* $v_{w1}(\Box p \Rightarrow p) = 1$ *zato što je* $v_{w1}(\Box p) = 1$ *i* $v_{w1}(p) = 1$ *Na isti način pokazujemo i za svetove* w_2 *i* w_3*.*

Glava 3

Sistemi modalne logike

U ovom poglavlju ćemo posmatrati uslove koje svaki modalni sistem treba da ispuni. Takođe ćemo govoriti o T sistemu kao osnovnom sistemu, a zatim i o sistemima S4 i S5. Koritićemo osnovnu literaturu [5], [8] i [10].

3.1 Uslovi koje svaki sistem treba da ispunjava

Postoje određeni uslovi koje svaki sistem treba da ispunjava da bismo mogli uopšte da ga nazovemo modalnim sistemom. Ove uslove treba formula da ispunjava da bi bila valjana. Ali ze neke formule valjanost će biti neodređena. Uslovi su sledeći:

1. Već smo pomenuli vezu između "nužnosti" i "mogućnosti".

$$\Diamond P \Leftrightarrow \neg\Box\neg P$$

$$\Box P \Leftrightarrow \neg\Diamond\neg P$$

Sistemi za koje važe ove ekvivalencije ne moraju da imaju primitivne $\Box$ i $\Diamond$. Dovoljno je da $\Box$ primitivan i pomoću njega možemo definisati $\Diamond$.

Definicija 3.1.0.1 $\Diamond P \Leftrightarrow_{Df} \neg\Box\neg P$

ili da $\Diamond$ bude primitivan i pomoću njega da definišemo $\Box$.

Definicija 3.1.0.2 $\Box P \Leftrightarrow_{Df} \neg\Diamond\neg P$

Sistem koji definiše $\Diamond$ pomoću $\Box$ nazivamo *sistem baziran na* $\Box$, dok sistem gde $\Box$ definišemo preko $\Diamond$ nazivamo *sistem baziran na* $\Diamond$.

2. Takođe smo naveli da simbol $\prec$ interpretiramo sa "podrazumeva se". Postoje različita mišljenja na koji način ovo tačno da interpretiramo, ali jedna stvar oko koje se svi slažu jeste da kada god p podrazumeva q nemoguće je da p bude tačno bez q. Ovo nas dovodi do sledeće definicije:

Definicija 3.1.0.3 $(p \prec q) \Rightarrow \neg\Diamond(p \wedge \neg q)$.

Ono oko čega se vodi polemika jeste da li obrnuto tvrđenje takođe važi, tj. da li bi za sve slučajeve kada je nemoguće za p da bude tačno bez toga da je q tačno, trebalo da tvrdimo da p podrazumeva q. Ovo sigurno važi za jednostavnije modalne logike. Dakle, p podrazumeva q ako i samo ako je nemoguće za p da bude tačno ako q nije tačno. Onda važi sledeća definicija:

Definicija 3.1.0.4 $(p \prec q) \Leftrightarrow \neg\Diamond(p \wedge \neg q)$.

Zbog ove ekvivalencije nećemo $\prec$ posmatrati kao primitivnu relaciju nego možemo definisati $(p \prec q)$ kao $\neg\Diamond(p \wedge \neg q)$. Druga ekvivalentna definicija za $(p \prec q)$ bi bila $\Box(p \Rightarrow q)$ zato što se $\Diamond(p \wedge \neg q)$ lako transformiše u $\Box(p \Rightarrow q)$ koristeći pravilo $\Diamond p \Leftrightarrow \neg\Box\neg p$ i standardne ekvivalencije iskazne logike. Kada se $\prec$ definiše na ovaj način onda ga nazivamo strogom implikacijom. Kada dva iskaza strogo impoliciraju jedan drugome onda kažemo da su oni strogo ekvivalentni. Za ovo koristimo znak $=$ i definišemo ga sa :

Definicija 3.1.0.5 $(p = q) =_{Df} ((p \prec q) \wedge (q \prec p))$

Takođe možemo i da ga definišemo sa:

Definicija 3.1.0.6 $(p = q) =_{Df} \Box(p \Leftrightarrow q)$

3. Modalni operatori nisu u funkciji istinitosti. Ovo znači da $\Box$p ne sme da bude ekvivalentan istinosnoj vrednosti p. Isto važi i za $\Diamond$. Postoje samo četiri posebne istinitostne funkcije: jedna je negacija p, druga p, treća istinitosna funkcija koja je tautologija i četvrta je istinitosna funkcija koja je uvek netačna bez obzira koju vrednost p uzima (kontradikcija). Stoga zahtevamo da sledeće formule nisu valjane:

$$\Box p \Leftrightarrow \neg p$$

$$\Box p \Leftrightarrow p$$

$$\Box p \Leftrightarrow (p \vee \neg p)$$

$$\Box p \Leftrightarrow (p \wedge \neg p)$$

4. Iako $\Box p \Leftrightarrow p$ nije valjana, jasno je da njena implikacija $\Box p \Rightarrow p$ jeste (šta god da je nužno tačno je i samo tačno). Ovu formulu često nazivaju *aksiom nužnosti*. Analogni princip je: šta god da je tačno je moguće. Ovo izražavamo pomoću formule $p \Rightarrow \Diamond p$ i nazivamo *aksiom mogućnosti* koja je takođe valjana. Formule $\Box p \Rightarrow p$ i $p \Rightarrow \Diamond p$ lako se mogu izraziti jedna pomoću druge.

5. Poslednji princip je da šta god da logički sledi iz nečega što je nužno tačno je i samo nužno tačno. Ako predpostavimo da ovo ne važi, tj. tvrdimo da sled nemogućih iskaza proizilazi iz nužnog iskaza onda takođe tvrdimo da iz validnog sleda iskaza možemo da imamo netačan zaključak. Dakle, treba da zahtevamo da kada god da je p nužno i p strogo implicira q , q je takođe nužno. Ovo možemo zapisati na ovaj način:

$$(\Box p \wedge (p \prec q)) \Rightarrow \Box q$$

ili

$$\Box(p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$$

Primer 3.1.0.1 *Sada ćemo dati jedan primer formule koja je ostala neodređena ovim uslovom. To je formula:*

$$\Box p \Rightarrow \Box\Box p$$

Ova formula znači da ako je bilo koji dati iskaz nužno tačan onda iskaz koji je nužno tačan je sam po sebi nužno tačan. Jednostavnije rečeno, šta god da je nužno je i nužno nužno. U ovo je veoma teško biti siguran samo na osnovu intuicije. Sistem T koji ćemo posmatrati ne zadovoljava ovaj uslov.

Kada je neka formula teorema datog sistema, rećicemo da ona *pripada* ili *je sadržana* u datom sistemu. Ako je svaka teorema sistema A ujedno i teorema sistema B, ali sistem B sadrži još neke teoreme rećicemo da je A *slabiji* tj. da je B *jači* sistem. Ako svaka teorema sistema A je ujedno i teorema sistema B (bez obzira da li sistem B sadrži jos neke teoreme) kažemo da sistem B *sadrži* sistem A.

3.2 T sistem

Najslabiji sistem koji zadovoljava uslove koje smo naveli je T sistem. Sistem T je prvi predstavio Robert Fejs (Robert Feys) 1937. godine. Baza T sistema je sledeća:

Primitivni simboli (alfabet)

- ***p,q,r,...* - iskazne promenljive**
- **$\neg, \Box$ - unarni veznici**
- **$\vee$ - binarni veznik**
- ***(,)* - zagrade**

Pravila formiranja formula

- **Promenljiva koja je sama je dobro zasnovana formula**
- **Ako je p dobro zasnovana formula, onda je i $\neg p$ i $\Box p$ je dobro zasnovana formula**
- **Ako su p i q dobro zasnovane formule onda je i $(p \vee q)$ dobro zasnovana formula**

Dobro zasnovane formule ćemo obeležavati sa $\alpha, \beta, ...$ Osnovne definicije za $\wedge, \Rightarrow, \Leftrightarrow$ su iste kao i u iskaznoj logici, ali imamo i 3 dodatne definicije:

Definicija 3.2.0.1 $\Diamond\alpha =_{Df} \neg\Box\neg\alpha$

Definicija 3.2.0.2 $(\alpha \prec \beta) =_{Df} \Box(\alpha \Rightarrow \beta)$

Definicija 3.2.0.3 $(\alpha = \beta) =_{Df} ((\alpha \prec \beta) \wedge (\beta \prec \alpha))$

Jasno je da je svaka dobro zasnovana formula iskazne logike takođe i dobro zasnovana formula T sistema.

Aksiome
Prve četiri aksiome uzimamo iz iskazne logike i dodajemo još dve:

- **A1** $(p \vee q) \Rightarrow p$
- **A2** $q \Rightarrow (p \vee q)$
- **A3** $(p \vee q) \Rightarrow (q \vee p)$
- **A4** $(q \Rightarrow r) \Rightarrow ((p \vee q) \Rightarrow (p \vee r))$
- **A5** $\Box p \Rightarrow p$ **(aksioma nužnosti)**
- **A6** $\Box(p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$

Pravila transformacije
Postoje 3 pravila transformacije koje koristimo:

- **Pravilo uniformne supstitucije - Rezultat zamene bilo koje iskazne promenljive u dobro zasnovanoj formuli sa dobro zasnovanom formulom je takođe dobro zasnovana formula**

- **Pravilo Modus Ponens - Ako α i $\alpha \Rightarrow \beta$, onda β**

$$\frac{\alpha, \alpha \Rightarrow \beta}{\beta}$$

- **Pravilo nužnosti - Ako α onda $\Box\alpha$**

$$\frac{\alpha}{\Box\alpha}$$

3.2.1 Teoreme u T sistemu

Kod dokazivanja teorema u T sistemu veliku pomoć nam daje još jedno izvedeno pravilo transformacije. Predpostavimo da je $(\alpha \Rightarrow \beta)$ teorema. Tada prema pravilu nužnosti dobijamo i da je $\Box(\alpha \Rightarrow \beta)$ teorema. Primenom A6 aksiome dobijamo $\Box(\alpha \Rightarrow \beta) \Rightarrow (\Box\alpha \Rightarrow \Box\beta)$. Na kraju primenom Modus Ponens pravila dobijamo i da je $(\Box\alpha \Rightarrow \Box\beta)$ teorema. Ovo zapisujemo na sledeći način:

$$\frac{\alpha \Rightarrow \beta}{\Box\alpha \Rightarrow \Box\beta} \qquad (1)$$

Teorema 3.2.1.1 $p \Rightarrow \Diamond p$

Dokaz: Prema A5 važi sledeće:

$$\Diamond\neg p \Rightarrow \neg p.$$

Kada negiramo obe strane implikacije dobijamo:

$$\neg\neg p \Rightarrow \neg\Box\neg p.$$

Znamo da važi

$$p \Rightarrow \neg\neg p.$$

Pošto je po definiciji

$$\Diamond p = \neg\Box\neg p$$

dobijamo i da važi

$$p \Rightarrow \Diamond p$$

što je i trebalo dokazati.

Teorema 3.2.1.2 $(p = q) \Rightarrow (\Box p \Leftrightarrow \Box q)$

Dokaz: Primenom A6 i definicije o podrazumevanju dobijamo sledeću implikaciju:

$$(p \prec q) \Rightarrow (\Box p \Rightarrow \Box q).$$

Kada zamenimo p i q dobijamo sledeću implikaciju:

$$(q \prec p) \Rightarrow (\Box q \Rightarrow \Box p).$$

Iz iskazne logike znamo da važi sledeća implikacija:

$$(p \Rightarrow q) \Rightarrow ((r \Rightarrow s) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge s))).$$

Iz ovih implikacija sledi sledeća implikacija:

$$((p \prec q) \wedge (q \prec p)) \Rightarrow ((\Box p \Rightarrow \Box q) \wedge (\Box q \Rightarrow \Box p)).$$

Iz definicije o jednakosti i ekvivalencije dobijamo

$$(p = q) \Rightarrow (\Box p \Leftrightarrow \Box q)$$

ˇˇsto je i trebalo dokazati.

Teorema 3.2.1.3 $\Box(p \wedge q) \Leftrightarrow (\Box p \wedge \Box q)$

Dokaz: Primenom (1) znamo da važi

$$\Box(p \wedge q) \Rightarrow \Box p.$$

Takođe važi i

$$\Box(p \wedge q) \Rightarrow \Box q.$$

Odavde sledi da

$$\Box(p \wedge q) \Rightarrow (\Box p \wedge \Box q).$$

Ponovnom primenom (1) dobijamo

$$\Box p \Rightarrow \Box(q \Rightarrow (p \wedge q))$$

a primenom A6

$$\Box(q \Rightarrow (p \wedge q)) \Rightarrow (\Box q \Rightarrow \Box(p \wedge q)).$$

Odavde sledi

$$\Box p \Rightarrow (\Box q \Rightarrow \Box(p \wedge q)).$$

Ovo implicira da

$$(\Box p \wedge \Box q) \Rightarrow \Box(p \wedge q).$$

Sada vidimo da

$$(\Box p \wedge \Box q) \Leftrightarrow \Box(p \wedge q)$$

čime je naša teorema dokazana.

Teorema 3.2.1.4 $\Box(p \Leftrightarrow q) \Leftrightarrow (p = q)$

Dokaz: Koristeći prethodnu teoremu umesto p stavljamo $p \Rightarrow q$ i umesto q stavljamo $q \Rightarrow p$. Dobijamo sledeću ekvivalenciju

$$\Box((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (\Box(p \Rightarrow q) \wedge \Box(q \Rightarrow p)).$$

Primenom definicija o nužnosti, ekvivalenciji i jednakosti dobijamo

$$\Box(p \Leftrightarrow q) \Leftrightarrow (p = q)$$

što je i trebalo da pokažemo.

Sada ćemo da uvedemo i drugu izvedenu transformaciju. Ona glasi ovako:

$$\frac{\alpha \Leftrightarrow \beta}{\Box\alpha \Leftrightarrow \Box\beta} \qquad (2)$$

Izvođenje: Primenom transformacije nužnosti iz $\alpha \Leftrightarrow \beta$ dobijamo $\Box(\alpha \Leftrightarrow \beta)$. Primenom teoreme 3.2.1.2 dobijamo $(\alpha = \beta)$ a primenom teoreme 3.2.1.4 dobijamo $(\Box\alpha \Leftrightarrow \Box\beta)$

Teorema 3.2.1.5 $\Box p \Leftrightarrow \neg\Diamond\neg p$

Dokaz: Znamo da važi

$$p \Leftrightarrow \neg\neg p.$$

Kada zamenimo p sa $\Box p$ dobijamo

$$\Box p \Leftrightarrow \neg\neg\Box p.$$

Zatim vidimo da važi

$$\Box p \Leftrightarrow \neg\neg\Box\neg\neg p.$$

Primenom definicije mogućnosti dobijamo

$$\Box p \Leftrightarrow \neg\Diamond\neg p$$

što je i trebalo da dokažemo. Iz ove teoreme se lako pokazuju i sledeće ekvivalencije:

$$\Box\neg p \Leftrightarrow \neg\Diamond p$$

$$\neg\Box p \Leftrightarrow \Diamond\neg p$$

Teorema 3.2.1.5 nam dozvoljava da $\Box$ zamenimo sa $\neg\Diamond\neg$ i obrnuto. Još jedna

primena teoreme 3.2.1.5 je za dobijanje sledeće ekvivalencije:

$$\Box\Box p \Leftrightarrow \neg\Diamond\Diamond\neg p$$

Ovu ekvivalenciju izvodimo tako što primenom teoreme 3.2.1.5 dobijamo

$$\Box\Box p \Leftrightarrow \neg\Diamond\neg\Box p.$$

Sada primenom ekvivalencije

$$\neg\Box p \Leftrightarrow \Diamond\neg p$$

dobijamo upravo

$$\Box\Box p \Leftrightarrow \neg\Diamond\Diamond\neg p.$$

Na sličan način možemo da dokažemo i sledeće ekvivalencije:

$$\Box\Box\neg p \Leftrightarrow \neg\Diamond\Diamond p$$

$$\Diamond\Diamond\neg p \Leftrightarrow \neg\Box\Box p$$

$$\Box\Diamond\neg p \Leftrightarrow \neg\Diamond\Box p$$

$$\Diamond\Box\neg p \Leftrightarrow \neg\Box\Diamond p$$

Iz ovih ekvivalencija sledi sledeće pravilo: bilo koji niz modala $\Box$ i $\Diamond$, $\Box$ može da bude zamenjeno sa $\Diamond$ i $\Diamond$ sa $\Box$ ukoliko se negacija doda ili izbriše odmah ispred i odmah iza niza. Ovo nazivamo pravilom "$\Box - \Diamond$" razmene.

Teorema 3.2.1.6 $\neg\Diamond(p \vee q) \Leftrightarrow (\neg\Diamond p \wedge \neg\Diamond q)$

Dokaz: Iz teoreme 3.2.1.5 sledi sledeća ekvivalencija:

$$\Box(\neg p \wedge \neg q) \Leftrightarrow (\Box\neg p \wedge \Box\neg q)$$

Iz pravila "$\Box - \Diamond$" razmene dobijamo

$$\neg\Diamond\neg(\neg p \wedge \neg q) \Leftrightarrow (\neg\Diamond p \wedge \neg\Diamond q)$$

Primenom De Morganovog zakona dobijamo:

$$\neg\Diamond(p \vee q) \Leftrightarrow (\neg\Diamond p \wedge \neg\Diamond q)$$

što smo i trebali dokazati. Ova teorema pokazuje da ako je nemoguće da važi p ili q, da su onda i p i q nemogući, i obrnuto.

Teorema 3.2.1.7 $\Diamond(p \vee q) \Leftrightarrow (\Diamond p \wedge \Diamond q)$

Dokaz: Znamo da važi

$$(\neg p \Leftrightarrow q) \Rightarrow (p \Leftrightarrow \neg q).$$

Primenom teoreme 3.2.1.6 na ovu implikaciju dobijamo

$$\Diamond(p \vee q) \Leftrightarrow \neg(\neg\Diamond p \wedge \neg\Diamond q).$$

Kada primenimo De Morganov zakon na prethodnu ekvivalenciju dobijamo

$$\Diamond(p \vee q) \Leftrightarrow (\Diamond p \wedge \Diamond q)$$

što smo i trebali dokazati.

Teorema 3.2.1.8 $(p \prec q) \Rightarrow (\Diamond p \Rightarrow \Diamond q)$

Dokaz: Kada primenimo A6 i umesto p i q stavimo $\neg p$ i $\neg q$ respektivno dobijamo

$$\Box(\neg q \Rightarrow \neg p) \Rightarrow (\Box\neg q \Rightarrow \Box\neg p).$$

Primenom transpozicije na ovu implikaciju dobijamo

$$\Box(p \Rightarrow q) \Rightarrow (\neg\Box\neg p \Rightarrow \Box\neg q).$$

Kada primenimo definiciju podrazumevanja i definiciju mogućnosti dobijamo

$$(p \prec q) \Rightarrow (\Diamond p \Rightarrow \Diamond q)$$

što smo i trebali dokazati.

Teorema 3.2.1.9 $(\Box p \vee \Box q) \Rightarrow \Box(p \vee q)$

Dokaz: Znamo da važi

$$p \Rightarrow (p \vee q).$$

Kada na ovu implikaciju primenimo (1) dobijamo

$$\Box p \Rightarrow \Box(p \vee q).$$

Takođe znamo iz A2 da važi

$$q \Rightarrow (p \vee q).$$

Primenjujemo (1) i na ovu implikaciju i dobijamo

$$\Box q \Rightarrow \Box(p \vee q).$$

Iz iskazne logike znamo da važi

$$(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow r)).$$

Odavde dobijamo da važi i

$$(\Box p \vee \Box q) \Rightarrow \Box(p \vee q)$$

što je i trebalo dokazati.

Teorema 3.2.1.10 $\Diamond(p \wedge q) \Rightarrow (\Diamond p \wedge \Diamond q)$

Dokaz: Zamenom p i q za $\neg p$ i $\neg q$, respektivno, u teoremu 3.2.1.9 dobijamo

$$(\Box\neg p \vee \Box\neg q) \Rightarrow \Box(\neg p \vee \neg q).$$

Kada na ovu implikaciju primenimo transpoziciju dobijamo

$$\neg\Box(\neg p \vee \neg q) \Rightarrow \neg(\Box\neg p \vee \Box\neg q).$$

Na ovu implikaciju sada primenjujemo "$\Box - \Diamond$" zamenu i dobijamo

$$\Diamond\neg(\neg p \wedge q) \Rightarrow (\Diamond p \wedge \Diamond q).$$

Na kraju primenom de Morganovog zakona dolazimo do implikacije koju smo i trebali dokazati

$$\Diamond(p \wedge q) \Rightarrow (\Diamond p \wedge \Diamond q).$$

Primetimo da su teoreme 3.2.1.9 u 3.2.1.10 implikacije a ne ekvivalencije. Obrnuti smer ovih implikacija nisu teoreme i lako je pokazati da ne važe.

Ponekad formula koja sadrži "$\Rightarrow$" je teorema, međutim kada se "$\Rightarrow$" zameni sa "$\prec$" formula prestaje da bude teorema. Naravno, ovo nikada ne može da bude slučaj kada se "$\Rightarrow$" pojavljuje kao glavni operator. Tada obe formule ili jesu ili nisu teoreme. Sada ćemo da navedemo 2 primera gde je prva formula teorema a druga nije.

Primer 3.2.1.1

$$(p \Rightarrow q) \vee (q \Rightarrow p)$$

$$(p \prec q) \vee (q \prec p)$$

Primer 3.2.1.2

$$(p \wedge q) \Rightarrow (p \Rightarrow q)$$

$$(p \wedge q) \Rightarrow (p \prec q)$$

Takođe, nekad imamo ekvivalenciju koja je teorema, ali kada se "$\Rightarrow$" zameni sa "$\prec$" rezultujuća formula je samo implikacija.

Primer 3.2.1.3

$$((p \Rightarrow r) \vee (q \Rightarrow r)) \Leftrightarrow ((p \wedge q) \Rightarrow r)$$

$$((p \prec r) \vee (q \prec r)) \Leftrightarrow ((p \wedge q) \prec r)$$

Prva formula je teorema a druga nije.

Teorema 3.2.1.11 $(\neg p \prec p) \Leftrightarrow \Box p$

Dokaz: Koristimo sledeću ekvivalenciju:

$$(\neg p \Rightarrow p) \Leftrightarrow p.$$

Primenom (2) dobijamo

$$\Box(\neg p \Rightarrow p) \Leftrightarrow \Box p.$$

Na kraju primenjujemo definiciju 3.1.0.4 dobijamo upravo ono što je trebalo da dokažemo

$$(\neg p \prec p) \Leftrightarrow \Box p.$$

Teorema 3.2.1.12 $(p \prec \neg p) \Leftrightarrow \Box \neg p$

Dokaz: Dokaz je sličan dokazu teoreme 3.2.1.11

Teorema 3.2.1.13 $((q \prec p) \wedge (\neg q \prec p)) \Leftrightarrow \Box p$

Dokaz: Znamo da važi :

$$((q \Rightarrow p) \wedge (\neg q \Rightarrow p)) \Leftrightarrow p$$

Primenom (2) dobijamo sledeću ekvivalenciju:

$$\Box((q \Rightarrow p) \wedge (\neg q \Rightarrow p)) \Leftrightarrow \Box p$$

Primenom teoreme 3.2.1.3 dobijamo

$$(\Box(q \Rightarrow p) \wedge \Box(\neg q \Rightarrow p)) \Leftrightarrow \Box p).$$

Na kraju primenom definicije3.1.0.4 dobijamo

$$((q \prec p) \wedge (\neg q \prec p)) \Leftrightarrow \Box p$$

što je i trebalo dokazati.

Teorema 3.2.1.14 $((p \prec q) \wedge (p \prec \neg q)) \Leftrightarrow \Box \neg p$

Dokaz: Koristimo isti dokaz kao u teoremi 3.2.13 samo što umesto ekvivalencije

$$((q \Rightarrow p) \wedge (\neg q \Rightarrow p)) \Leftrightarrow p$$

koristimo ekvivalencije

$$((p \Rightarrow q) \wedge (p \Rightarrow \neg q)) \Leftrightarrow \neg p$$

Teorema 3.2.1.15 $\Box p \Rightarrow (q \prec p)$

Dokaz: Koristimo implikaciju

$$p \Rightarrow (q \Rightarrow p).$$

Primenom (1) dobijamo

$$\Box p \Rightarrow (q \prec p).$$

Kada primenimo definiciju 3.1.0.4 dobijamo

$$\Box p \Rightarrow (q \prec p)$$

što je i trebalo dokazati.

Teorema 3.2.1.16 $\Box \neg p \Rightarrow (p \prec q)$

Dokaz: Koristimo isti dokaz kao u teoremi 3.2.1.15 samo što koristimo

$$(\neg p \Rightarrow (p \Rightarrow q))$$

umesto

$$p \Rightarrow (q \Rightarrow p).$$

Teorema 3.2.1.17 $\Box p \Rightarrow (\Diamond q \Rightarrow \Diamond(p \wedge q))$

Dokaz: Koristimo sledeću implikaciju:

$$p \Rightarrow (q \Rightarrow (p \wedge q)).$$

Primenom (1) dobijamo

$$\Box p \Rightarrow \Box(q \Rightarrow (p \wedge q)).$$

Primenom teoreme 3.2.1.8 i definicije 3.1.0.4 dobijamo

$$\Box(q \Rightarrow (p \wedge q)) \Rightarrow (\Diamond q \Rightarrow \Diamond(p \wedge q)).$$

Vidimo da važi i implikacija koju je i trebalo da dokažemo

$$\Box p \Rightarrow (\Diamond q \Rightarrow \Diamond(p \wedge q)).$$

3.3 Sistemi S4 i S5

Sistem T zadovoljava sve uslove koje smo naveli u prethodnom poglavlju ali je ujedno i najslabiji sistem koji ih ispunjava. Sve teoreme koje on sadrži nisu problematične dok su neke od ostalih teorema koje se pominju u drugim sistemaima kontraverzne.

Jedna takva teorema je i $\Box p \Rightarrow \Box\Box p$ koju smo naveli u primeru 3.1.0.1. Formula poput ove je teško inuitivno shvatiti a razlog za to su sekvence modalnih operatora (modaliteta) koje se pojavljuju jedan do drugog. U formuli $\Box p \Rightarrow \Box\Box p$ sekvenca koja se pojavljuje je $\Box\Box$. Ovakve sekvence nazivamo *iterirarni modaliteti* (iterated modalities). Nisu sve formule koje imaju itarirarne modalitete problematične. Primer za to je formula $\Box\Box p \Rightarrow \Box p$ koja je samo verzija aksiome A5 ($\Box p \Rightarrow p$). Ako bi neformalno predstavili problem $\Box p \Rightarrow \Box\Box p$ on bi glasio: da li je nužno, obavezno nužno? Drugačije rečeno, kada je p nužno tačno, da li je činjenica da je p nužno tačno uvek i samo nužno tačno? Ovo je sporno pitanje jer ne znamo pod kojim uslovima je iskaz obavezno nužan. Ali ono što možemo da kažemo jeste da je ovo tvrđenje verodostojno. Ali ne moramo da rešimo ovaj problem ovde. Činjenica da postoji veliki broj ljudi koji tvrde da je $\Box p \Rightarrow \Box\Box p$ tačna formula je bila motivacija da se napravi sistem koji je jači od T sistema. U takvom sistemu je ova formula teorema.

Već smo rekli da je $\Box\Box p \Rightarrow \Box p$ formula koja je samo verzija aksiome A5 ($\Box p \Rightarrow p$) i teorema u T sistemu. Dakle, naš novi sistem bi imao za aksiomu sledeću ekvivalenciju:

$$\Box p \Leftrightarrow \Box\Box p.$$

Ova ekvivalencija nam dozvoljava da uvek zamenimo sekvencu modaliteta sa kraćom sekvencom i nazivamo je *pravilo redukcije* svakog sistema gde je ona aksioma.

Sada ćemo navesti 4 najvažnije ekvivalencije koje mogu koristiti kao redukciona pravila:

$$1.\Diamond p \Leftrightarrow \Box\Diamond p$$

$$2.\Box p \Leftrightarrow \Diamond\Box p$$

$$3.\Diamond p \Leftrightarrow \Diamond\Diamond p$$

$$4.\Box p \Leftrightarrow \Box\Box p.$$

Nijedna od ovih ekvivalencija nije teorema u T sistemu i to je jedna od bitnijih osobina T sistema: ne poseduje redukciono pravilo. Ako bismo želeli da proširimo T sistem sa ovim ekvivalencijama ne bismo morali da ih uvodimo kao nove aksiome iz 3 razloga:

1. Kao što smo vec rekli $\Box\Box p \Rightarrow \Box p$ je teorema u T sistemu i supstituciom u A5 ili teoremi 3.2.1.1 dobijamo $\Box\Diamond p \Rightarrow \Diamond p$, $\Box p \Rightarrow \Diamond\Box p$ i $\Diamond p \Rightarrow \Diamond\Diamond p$. Tako da je jedan pravac svake implikacije već u T sistemu i bilo bi suvišno da dodajemo ove implikacije:

$$\Diamond p \Rightarrow \Box\Diamond p$$

$$\Diamond\Box p \Rightarrow \Box p$$

$$\Diamond\Diamond p \Rightarrow \Diamond p$$

$$\Box p \Rightarrow \Box\Box p$$

2. Iz $\Box p \Rightarrow \Box\Box p$ možemo da izvedemo $\Diamond\Diamond p \Rightarrow \Diamond p$; a iz $\Diamond p \Rightarrow \Box\Diamond p$ možemo da izvedemo $\Diamond\Box p \Rightarrow \Box p$ i obrnuto. Ova izvođenja ćemo pokazati u sledećem poglavlju. Tako da bi bilo suvišno da stavljamo 2 aksiome.

3. $\Box p \Rightarrow \Box\Box p$ se izvodi iz $\Diamond p \Rightarrow \Box\Diamond p$ što ćemo takođe pokazati u sledećem poglavlju. Vidimo da možemo sva četiri redukciona zakona da izvedemo ako jednostavno dodamo $\Diamond p \Rightarrow \Box\Diamond p$ sistemu T. Takođe dodavanjem $\Box p \Rightarrow \Box\Box p$ sistemu T možemo da dobijemo treće i četvrto redukciono pravilo.

Sve ovo nam sugeriše da možemo da napravimo dva aksiomatska sistema koja su oba jača od T sistema, a jedan jači od drugog. Prvi od njih je ***sistem S4*** koji se dobija tako što se na sistem T dodaje aksioma $\Box p \Rightarrow \Box\Box p$, drugi je ***sistem S5*** koji se dobija tako što se na sistem T dodaje aksiomu $\Diamond p \Rightarrow \Box\Diamond p$.

3.3.1 Teoreme u S4 sistemu

Kao što smo rekli, osnova ovog sistema je T sistem plus sledeća aksioma:

- **A7** $\Box p \Rightarrow \Box\Box p$

Sada ćemo dati sedam teorema koje važe u **S4** sistemu, ali ne važe u T sistemu.

Teorema 3.3.1.1 $\Diamond\Diamond p \Rightarrow \Diamond p$

Dokaz: Ako u A7 zamenimo p sa $\neg p$ dobijamo sledeće:

$$\Box\neg p \Rightarrow \Box\Box\neg p.$$

Iz pravila '$\Diamond - \Box'$ razmene dobijamo:

$$\neg\Diamond p \Rightarrow \neg\Diamond\Diamond p.$$

Kada negiramo ovu impikaciju dobijamo upravo ono što je trebalo da pokažemo

$$\Diamond\Diamond p \Rightarrow \Diamond p.$$

Teorema 3.3.1.2 $\Box p \Leftrightarrow \Box\Box p$

Dokaz: Kada u A5 umesto p ubacimo $\Box p$ dobijamo:

$$\Box\Box p \Rightarrow \Box p.$$

Primenom A7 i definicije ekvivalencije na ovu implikaciju upravo dobijamo

$$\Box p \Leftrightarrow \Box\Box p$$

što je i trebalo dokazati.

Teorema 3.3.1.3 $\Diamond p \leftrightarrow \Diamond\Diamond p$

Dokaz: Koristimo sličan dokaza kao u teoremi 3.2.1.1 (samo što umesto p stavljamo $\Diamond p$) i teoremi 3.2.2.1.

Teorema 3.3.1.4 $\Box\Diamond p \Rightarrow \Box\Diamond\Box\Diamond p$

Dokaz: Koristimo teoremu 3.2.1.1. samo što umesto p stavljamo $\Box\Diamond p$ i dobijamo:

$$\Box\Diamond p \Rightarrow \Diamond\Box\Diamond p.$$

Primenom (1) na ovu implikaciju dobijamo:

$$\Box\Box\Diamond p \Rightarrow \Box\Diamond\Box\Diamond p.$$

Koristimo teoremu 3.3.1.2 i dobijamo

$$\Box\Diamond p \Rightarrow \Box\Diamond\Box\Diamond p$$

što je i trebalo da pokažemo.

Teorema 3.3.1.5 $\Box\Diamond p \Leftrightarrow \Box\Diamond\Box\Diamond p$

Dokaz: Kada na teoremu 3.3.1.4 primenimo (1) dobijamo:

$$\Box\Diamond\Box\Diamond p \Rightarrow \Box\Diamond p.$$

Na ovu implikaciju primenjujemo teoremu 3.3.1.5 i definiciju ekvivalencije i dobijamo

$$\Box\Diamond p \Leftrightarrow \Box\Diamond\Box\Diamond p$$

što je i trebalo dokažati.

Teorema 3.3.1.6 $\Diamond\Box p \Leftrightarrow \Diamond\Box\Diamond\Box p$

Dokaz: U prethodnu teoremu umesto p stavljamo $\neg p$ i dobijamo:

$$\Box\Diamond\neg p \Leftrightarrow \Box\Diamond\Box\Diamond\neg p.$$

Primenom pravila '$\Diamond - \Box'$ na ovu implikaciju dobijamo:

$$\neg\Diamond\Box p \Leftrightarrow \neg\Diamond\Box\Diamond\Box p.$$

Iz iskazne logike znamo da važi:

$$(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q).$$

Na kraju kada ovu tautologiju primenimo na prethodne implikacije dobijamo

$$\Diamond\Box p \Leftrightarrow \Diamond\Box\Diamond\Box p$$

što sje i trebalo dokažati.

3.3.2 Modaliteti u S4 sistemu

Modalitet definišemo kao povezan niz od nula ili više modalnih operatora ($\neg, \Box, \Diamond$). Ako nemamo niti jedan operator pišemo "-".

Primer 3.3.2.1 *Neki od primera modaliteta su:*$-, \neg, \Box, \Diamond\neg, \Box\Box, \neg\Diamond\Box\neg\Diamond$.

Jasno je da u svakm sistemu u kojem važi "$\Box - \Diamond$" zamena, svaki modalitet može da se predstavi ili bez negacije, ili maksimalno sa jednom negacijom koja je na početku niza. Modalitet koji je predstavljen u ovoj formi nazivamo *standardna forma*, i od sada ćemo predpostavljati da su svi modaliteti dati u standardnoj formi.

Kažemo da su dva modaliteta, A i B, jednaka u datom sistemu ako i samo ako je rezultat menjanja A sa B (ili B sa A) u bilo kojoj formuli je jednako u tom sistemu sa originalnom formulom. U suprotnom kažemo da su modaliteti različiti. Ako su A i B jednaki u datom sistemu, i A sadrži manje modalnih operatora od B, onda kažemo da B možemo da svedemo na A u tom sistemu. Jasno je da formule koje smo nazivali redukciona pravila pokazuju svodljivost nekih modaliteta u sistemu gde su one teoreme.

Sada možemo da dokažemo važnu stvar u vezi sistema S4:

Teorema 3.3.2.1 *Svaki modalitet je jednak barem nekom od sledećih modaliteta ili njihovim negacijama:*

1.$-$

2.$\Box$

3.$\Diamond$

4.$\Box\Diamond$

5.$\Diamond\Box$

6.$\Box\Diamond\Box$

7.$\Diamond\Box\Diamond$.

Dokaz: Očigledno 2 i 3 su jedini modaliteti koji sadrže jedan element. Iz teoreme 3.3.1.2 i 3.3.1.3 sledi da možemo da zamenimo $\Box\Box$ sa $\Box$ i $\Diamond\Diamond$ sa $\Diamond$, tako da ako dodamo modalni operator formuli 2 i 3, ili ćemo dobiti modalitet jednak prvobitnom ili formule 4 i 5, koje su jedini nesvodljivi dvočlani modaliteti. Na isti način ako dodamo modalne operatore formulama 4 i 5, jedine nesvodive tročlane operatore koje možemo da dobijemo su 6 i 7. Ako na ove tročlane modalitete dodamo modalni operator dobijamo isti modalitet kao pre ili formule 4 i 5 pomoću teorema 3.3.1.6 i 3.3.1.7.

Isto možemo da uradimo i sa negacijom tako da smo pokazali da postoji najviše 14 različitih modaliteta u S4 sistemu.

Ako ove modalitete dodamo na dobro zasnovanu formulu α, rezultat je takođe dobro zasnovana formula. Implikacije koje važe između ovih sedam dobro zasnovanih formula je prikazan u sledećem dijagramu:

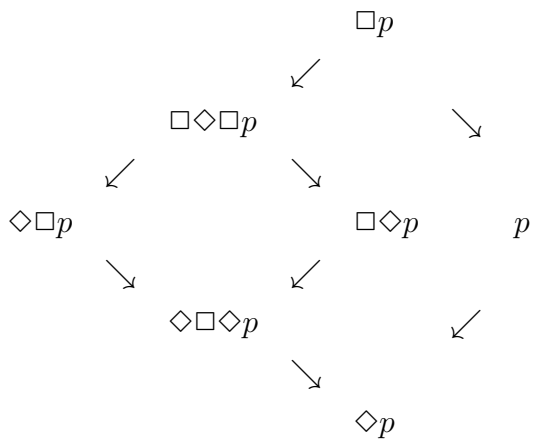


Tabela 3.1: Dijagram implikacija u S4

Takođe daćemo i analogni dijagram za negativne slučajeve u tabeli 3.2. Vidimo da se taj dijagram dobija tako što se negiraju sve formule i promeni smer implikacija.

Pošto T sistem nema redukciona pravila situacija je veoma drugačija. Bez obzira koliko modalnih operatora modalnost sadrži, uvek možemo da napravimo dužu modalnost koja neće biti jednaka prethodnoj. Dakle T sistem sadrži beskonačan broj različitih modalnosti.

3.3.3 Teoreme u S5 sistemu

Osnova S5 sistema je T sistem plus sledeća aksioma:

- **A8** $\Diamond p \Rightarrow \Box\Diamond p$

Prve tri teoreme sistema S5 se dokazuju na isti način kao teoreme 3.3.1.1, 3.3.1.2 i 3.3.1.3, ali umesto A7 aksiome koristimo aksiomu A8.

Teorema 3.3.3.1 $\Diamond\Box p \Rightarrow p$

Teorema 3.3.3.2 $\Diamond p \Leftrightarrow \Box\Diamond p$

Teorema 3.3.3.3 $\Box p \Leftrightarrow \Diamond\Box p$

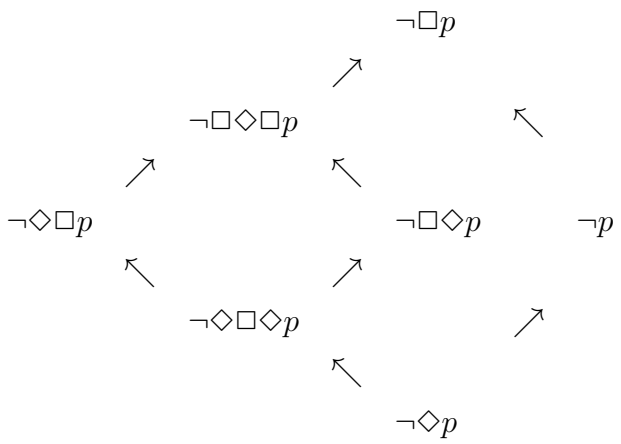


Tabela 3.2: Dijagram negacija formula u S4

$\Box p \Rightarrow \Box\Box p$, karakteristična aksioma sistema S4, nije aksioma sistem S5. Međutim, sada ćemo dokazati da je ona teorema sistema S5.

Teorema 3.3.3.4 $\Box p \Rightarrow \Box\Box p$

Dokaz: Koristimo teoremu 3.2.1.1 samo što umesto p stavljamo $\Box p$. Tada dobijamo:

$$\Box p \Rightarrow \Diamond\Box p.$$

Pomoću teoreme 3.3.3.2 dobijamo:

$$\Box p \Rightarrow \Box\Diamond\Box p.$$

Primenom teoreme 3.3.3.3 dobijamo:

$$\Box p \Rightarrow \Box\Box p$$

što je i trebalo dokazati.

Dakle ovom teoremom smo pokazali da se A7 sadrži u sistemu S5. Pošto je ovim sistemim T sistem zajedički, a A7 se sadrži u sistemu S5, ovo je dokaz da sistem S5 sadrži sistem S4. Sada ćemo navesti i dokazati pet teorema o redukciji koje koristimo u sistemu S5.

Teorema 3.3.3.5 $\Box(p \vee q) \Rightarrow (\Box p \vee \Diamond q)$

Dokaz: Počinjemo sa A6 aksiomom samo što umesto p i q pišemo $\neg q$ i $\neg p$ respektivno. Dobijamo sledeću implikaciju:

$$\Box(\neg q \Rightarrow p) \Rightarrow (\Box\neg q \Rightarrow \Box p).$$

Iz ove implikacije kada primenimo definiciju implikacije dobijamo:

$$\Box(q \vee p) \Rightarrow (\neg\Box\neg q \vee \Box p).$$

Kada na ovu implikaciju primenimo pravili "$\Box - \Diamond$" zamene dobijamo:

$$\Box(p \vee q) \Rightarrow (\Box p \vee \Diamond q)$$

što je i trebalo pokazati.

Teorema 3.3.3.6 $\Box(p \vee \Box q) \Leftrightarrow (\Box p \vee \Box q)$

Dokaz: Iz prethodne teoreme zamenom q sa $\Box q$ i primenom drugog redukcionog pravila dobijamo:

$$\Box(p \vee \Box q) \Rightarrow (\Box p \vee \Box q).$$

Iz teoreme 3.2.1.9 kada q zamenimo sa $\Box q$ dobijamo:

$$(\Box p \vee \Box\Box q) \Rightarrow (\Box p \vee \Box q).$$

Kada četvrto redukciono pravilo primenimo na prethodnu implikaciju dobijamo:

$$(\Box p \vee \Box q) \Rightarrow \Box(p \vee \Box q).$$

Iz prve i treće implikacije u ovom dokazu, primenom definicije o ekvivalenciji dobijamo:

$$\Box(p \vee \Box q) \Leftrightarrow (\Box p \vee \Box q)$$

što je i trebalo pokazati.

Teorema 3.3.3.7 $\Box(p \vee \Diamond q) \Leftrightarrow (\Box p \vee \Diamond q)$

Dokaz: Koristimo prethodnu teoremu samo što umesto q stavljamo $\Diamond q$ i dobijamo:

$$\Box(p \vee \Box\Diamond q) \Leftrightarrow (\Box p \vee \Box\Diamond q).$$

Kada na ovu ekvivalenciju primenimo prvo redukciono pravilo dobijamo:

$$\Box(p \vee \Diamond q) \Leftrightarrow (\Box p \vee \Diamond q)$$

što je i tebalo pokazati.

Teorema 3.3.3.8 $\Diamond(p \wedge \Diamond q) \Leftrightarrow (\Diamond p \wedge \Diamond q)$

Dokaz: Iz teoreme 3.3.3.6 kada zamenimo p i q sa i $\neg q$, resprektivno, dobijamo:

$$\Box(\neg p \vee \Box\neg q) \Leftrightarrow (\Box\neg p \vee \Box q).$$

Kada na ovu ekvivalenciju primenimo tautologiju iz iskazne logike

$$(p \Leftrightarrow q) \Leftrightarrow (\neg \Leftrightarrow \neg q)$$

dobijamo:

$$\neg\Box(\neg p \vee \Box\neg q) \Leftrightarrow \neg(\Box\neg p \vee \neg q).$$

Primenom "$\Box - \Diamond$" pravila dobijamo:

$$\Diamond\neg(\neg p \vee \neg\Diamond q) \Leftrightarrow \neg(\neg\Diamond p \vee \neg\Diamond q).$$

Kada na ovu implikaciju primenimo definiciju o konjukciji dobijamo:

$$\Diamond(p \wedge \Diamond q) \Leftrightarrow (\Diamond p \wedge \Diamond q)$$

što je i trebalo pokazati.

Teorema 3.3.3.9 $\Diamond(p \vee \Box q) \Leftrightarrow (\Diamond p \vee \Box q)$

Dokaz: Kada u prethodnu teoremu uvrstimo $\Box q$ umesto q dobijamo:

$$\Diamond(p \vee \Diamond\Box q) \Leftrightarrow (\Diamond p \vee \Diamond\Box q).$$

Primenom (2) na prethodnu ekvivalenciju dobijamo:

$$\Diamond(p \vee \Box q) \Leftrightarrow (\Diamond p \vee \Box q)$$

što je i trebalo dokazati.

3.3.4 Modaliteti u S5 sistemu

Pokazali smo da se sva četiri redukciona pravila nalaze u sistemu S5.

$$1.\Diamond p \Leftrightarrow \Box\Diamond p$$

$$2.\Box p \Leftrightarrow \Diamond\Box p$$

$$3.\Diamond p \Leftrightarrow \Diamond\Diamond p$$

$$4.\Box p \Leftrightarrow \Box\Box p$$

Ova pravila možemo sumirati na sledeći način: u svakom paru susednih unarnih modalnih operatora možemo da izbrišemo prvi. Pošto ovaj proces možemo ponoviti beskonačno puta možemo reći da u svakoj sekvenci modalnih operatora možemo da izbrižemo sve osim poslednjeg. Direktna posledica ovoga je da sistem S5 sadrži 6 različitih modaliteta a to su:

$$-, \Box, \Diamond$$

i njihove negacije.

Glava 4

Semantika sistema T, S4 i S5

U poglavlju 2 smo govorili o semantici mogućih svetova. Relaciju dostupnosti smo označili slovom R i definisali je kao binarnu relaciju između svetova. U ovom delu ćemo razmatrati njene osobine u sistemima koje smo proučavali. Najpre ćemo ovo pokazati kroz primer igre za svaki sistem a zatim dati i formalnu definiciju za taj sistem. Koristićemo osnovnu literaturu [8], [12] i [16]

4.1 Semantika T sistema

Kako bi bolje razumeli semantiku T sistema počećemo sa primerom jedne igre koja oslikava strukturu i semantiku T sistema.

Primer 4.1.0.1 *Potrebni elementi igre su igrači i moderator. Broj igrača nije uslovljen. Svaki igrač ima papirić sa napisanim slovom na njemu. Nije nam bitno na koji način igracč i sede. Možemo da ih postavimo na taj način da ni jedan igrač ne vidi drugog igrača, da neki igrači vide druge igrače ili da svi igrači vide sve igrače. Takođe vidljivost ne mora da bude međusobna. Ako igrač A vidi igrača B, igrač B ne mora da vidi igrača A. Zatim moderator proziva dobro zasnovane formule na koje se igrači odazivaju tako što ili dižu ili ne dižu ruku. Ali svaka prozivka mora biti dobro pripremljena tako što pre prozivanja formule moramo da prozovemo sve komponente te formule, počevši sa slovima (promenljivama). Zatim dajemo instrukcije igračima: 1. Ako moderator kaže slovo i to slovo se nalazi na tvom papiru podigni ruku 2. Ako moderator prozove formulu $\neg\alpha$ podigni ruku ako je nisi podigao kada je α prozvana 3. Ako moderator prozove $(\alpha \vee \beta)$, podigni svoju ruku ako si je podigao za α ili β (Preko negacije i disjunkcije možemo da definišemo i konjukciju, implikaciju i ekvi-*

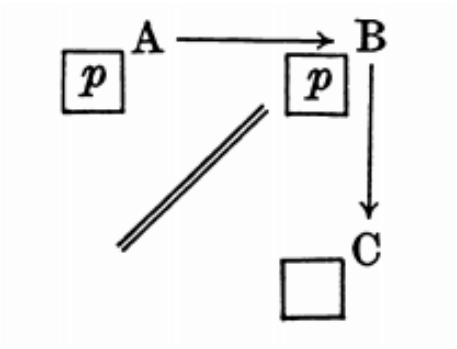
valenciju) 4. Ako moderator prozove $\Box\alpha$ podigni ruku ako je svaki igrač koga vidiš podigao ruku kada je α bilo prozvano 5. Ako moderator prozove $\Diamond\alpha$ podigni ruku ako je barem jedan igrač koga vidiš podigao ruku kada je α bilo prozvano

Primetimo da za prva 3 pravila igrač mora da pamti kada je dizao ruku dok za druga dva pravila mora da pamti i kada su ostali igrači dizali ruku. Ako na određenu prozivku svi igrači dignu ruku tu prozivku nazivamo *uspešnom*. Jasno je da neka prozivka može u jednom T sistemu biti uspešna, a ne mora u drugom. Međutim postoje određene prozivke koje bi bile uspešne u svim T sistemima, bez obzira na broj igrača i raspoeda sedenja. Takve prozivke nazivamo T uspešna.

Definicija 4.1.0.1 *Formula je valjana u T sistemu ako je prozivka T uspešna.*

Primer 4.1.0.2 *$\Box p \Rightarrow p$ je primer jedne ovakve formule. Posmatraćemo igrača A. Prema rasporedu, moderator mora prvo da prozove slovo p. Ako se p nalazi na papiriću igrača A on će podići ruku. Prema trećem pravilu podićice je i za $\neg\Box p \vee p$. Ako p nije na papiru, neće podići ruku za p i neće ni za $\Box p$. U tom slučaju prema pravilu dva, mora da je digne za $\neg\Box p$ i zbog toga i za $\neg\Box p \vee p$. Tako da će A da digne ruku za formulu $\neg\Box p \vee p$ bez obzira na to da li mu je p na papiru ili nije. Isto važi i za druge igrače.*

Primer 4.1.0.3 *Razmotrićemo sada primer $\Box p \Rightarrow \Box\Box p$. U nekim T sistemina ovo bi bila uspešna prozivka ali u nekim drugim ne bi. Sada ćemo pokazati jedan u kojem ne bi. Postoje tri igrača, A, B i C. Igrači A i B na svom papiru imaju p ali igrač C nema. A vidi B, B vidi C, ali A ne vidi C (ostali detalji nisu bitni). Na slici je ovo prikazano (slika 6). Strelica prikazuje ko koga vidi, a dupla linija je pregrada koja blokira pogled. Ovako bi se igra odvijala: Prva prozivka: p- Igrači A i B dižu ruke, C ne diže. Druga prozivka: $\Box p$- A diže ruku (jer su svi igrači koje vidi digli ruku na p, a vidi samo B), dok B i C ne dižu ruku. Treća prozivka: $\Box\Box p$- Niko ne diže ruku(Ni A ne diže ruku jer B, koga jedino vidi, nije digo ruku za $\Box p$). Četvrta prozivka: $\Box p \Rightarrow \Box\Box p$- B i C dižu ruke, ali A ne diže(zato što je digao ruku na $\Box p$ ali nije na $\Box\Box p$). Dakle vidimo da $\Box p \Rightarrow \Box\Box p$ nije T uspešan jer postoji barem jedan igrač u jednoj T postavci koji nije podigao ruku. Znači da ovo nije T valjana formula.*



Slika 6: Primer 4.1.0.3

Sada možemo da damo i formalnu definiciju valjanosti T sistema. Grupe igrača predstavljaju skup W koji sadrži sve moguće svetove $(w_1, w_2, w_3, ...)$. Vidimo da relacija dostupnosti ima sledeće osobine:

- Binarna je (zahteva dva terma)
- U svakom T sistemu definisana je nad svetovima (za svaki par svetova, w_1 i w_2, definisano je da ili w_1 vidi w_2, ili ga ne vidi).
- Relacija je refleksivna (svaki svet, bez izuzetka, vidi samog sebe $w_i R w_i$). Dakle u pitanju je binarna, refleksivna relacija nad skupom W.

Teorema 4.1.0.1 *T model je uređena trojka (W, R, V), gde je W skup svih mogućih svetova, R je binarna, refleksivna relacija definisana nad W, i V je funkcija koja dodeljuje vrednost i zadovoljava sledeće uslove:*

- *1. Za svaku promenljivu p_j, i za svaki w_i koji pripada skupu W, važi $v_{w_i}(p_j) = 1$ ili $v_{w_i}(p_j) = 0$*
- *2. Za svaku dobro zasnovanu formulu α i za svaki $w_i \in W$, $V_{w_i}(\neg\alpha) = 1$ ako $v_{w_i}(\alpha) = 0$; suprotno $v_{w_i}(\neg\alpha) = 0$*
- *3. Za svake dve dobro zasnovane formule, α i β, i za svaki $w_i \in W$, $v_{w_i}(\alpha \vee \beta) = 1$ ako $v_{w_i}(\alpha) = 1$ ili $v_{w_i}(\beta) = 1$. Suprotno $v_{w_i}(\alpha \vee \beta) = 0$*
- *4. Za svaku dobro zasnovanu formulu α i za svaki $w_i \in W$, $v_{w_i}(\Box\alpha) = 1$ ako za svaki $w_j \in W$ takav da $w_i R w_j$ $v_{w_j}(\alpha) = 1$; suprotno $v_{w_i}(\Box\alpha) = 0$*

4.2 Semantika S4 sistema

Igra koju smo naveli u primeru 4.1.0.1 može da se primeni na sistem S4 samo što ne možemo da zadamo proizvoljni red sedenja igrača. Igrači moraju da poštuju pravilo da ukoliko igrač A vidi igrača B, i igrač B vidi igrača C, onda i igrač A mora da vidi igrača C. Primetimo da svaki raspored sedenja koji ima manje od tri igrača automatski ispunjava ovaj uslov. Svaki raspored koji ispunjava ovaj uslov stoga nazivamo S4 raspored. Takođe svaki S4 raspored je ujedno i T raspored. Svaka prozivka koja bi bila uspešna u S4 rasporedu je S4 prozivka. Jasno je i da je i svaka prozivka koja je uspešna u T sistemu ujedno uspešna i u S4 sistemu. Međutim prozivka koja je uspešna u svakom S4 sistemu, ne mora da bude uspešna u svakom T sistemu i stoga nije T uspešna.

Primećujemo da raspored sedenja koji je dat u primeru 4.1.0.1 i tom primeru nije raspored sedenja u S4 sistemu. Tako da ovaj raspored ne možemo da koristimo u S4 sistemu i lako možemo da pokažemo da je formula $\Box p \Rightarrow \Box\Box p$ validna u S4 sistemu.

Primer 4.2.0.1 *Daćemo sada primer jedne formule koja ne važi u S4 sistemu. U pitanju je formula $\Diamond p \Rightarrow \Box\Diamond p$. Veoma jednostavan raspored sedenja igrača će to pokazati. Neka su u igru uključena samo 2 igrača A i B. Igrač A vidi igrača B, ali igrač B ne vidi igrača A. Na papiriću igrača A je napisano p, dok na papiriću igrača B ne piše p. Kada moderator prozove p, igrač A podiže ruku dok igrač B ne podiže ruku. Kada moderator prozove $\Diamond p$ igrač A opet podiže ruku dok je ruka igrača B opet spuštena. Kada moderator prozove $\Box\Diamond p$, igrač A ne diže ruku jer je ruka igrača B bila spuštena u prethodnoj prozivci. Dakle kada moderator prozove $\Diamond p \Rightarrow \Box\Diamond p$ igrač A neće podići ruku i stoga ova formula nije S4 validna.*

Primećujemo da je jedina razlika između T sistema i S4 sistema to što je relacija dostupnosti R takođe i tranzitivna. U S4 sistem R zadovoljava sledeće osobine:

- Binarna je (zahteva dva terma)
- U svakom S4 sistemu definisana je nad svetovima (za svaki par svetova, w_1 i w_2, definisano je da ili w_1 vidi w_2, ili ga ne vidi).
- Relacija je refleksivna i tranzitivna (za svaki x, y, z važi da ako xRy i yRz tada xRz). Dakle, u pitanju je binarna, refleksivna i tranzitivna relacija nad skupom W.

Definicija 4.2.0.1 *S4 model je uređena trojka (W, R, V) gde su W i V definisane kao u modelu T i R je refleksivna i tranzitivna relacija nad skupom W.*

Teorema 4.2.0.1 *Dobro zasnovana formula α je validna u S4 sistemu akko za svaki S4 model (W, R, V) i za svaki $w_i \in W, v_{w_i}(\alpha) = 1$.*

4.3 Semantika S5 sistema

Igra iz primera 4.1.0.1 se može primeniti i na sistem S5 samo što moramo da uvedemo dodatni uslov. U S5 rasporedu sedenja ako jedan igač vidi drugoga, i taj drugi igrač mora da vidi prvoga. Jasno je da je svaki S5 raspored takođe i S4 raspore a samim tim i T raspored, ali neki S4 rasporedi nisu S5 rasporedi. Prozivka koja je uspešna u svakom S5 sistemu nazivamo S5 uspešna prozivka.

Definicija 4.3.0.1 *Formula je S5 valjana ako je dobijamo S5 uspešnom prozivkom.*

Formula koju smo posmatrali u primeru 4.1.0.1 nije S4 uspešna ali jeste S5 uspešna. Sada ćemo dati primer jedne formule koja nije S5 uspešna.

Primer 4.3.0.1 *U pitanju je formula $p \Rightarrow \Box p$. Neka su data dva igrača A i B. Pošto je u pitanju S5 raspored jasno je da igrač A vidi igrača B i igrač B vidi igrača A. Na papiru igrača A je slovo p a na papiru igrača B nije. Tada će A dići ruku za p ali neće za $\Box p$ pa samim tim neće ni za $p \Rightarrow \Box p$.*

Primećujemo da je relacija R u S5 sistemu i simetrična. Dakle relacija R u S5 sistemu ima sledeće osobine:

- Binarna je (zahteva dva terma)
- U svakom S5 sistemu definisana je nad svetovima (za svaki par svetova, w_1 i w_2, definisano je da ili w_1 vidi w_2, ili ga ne vidi).
- Relacija je refleksivna, tranzitivna i simetrična (za svaki x, y važi da ako xRy sledi yRx). Dakle u pitanju je binarna, refleksivna, tranzitivna i simetrična relacija nad skupom W.

Definicija 4.3.0.2 *S5 model je uređena trojka (W, R, V) gde su W i V definisane kao u modelu T i R je refleksivna, tranzitivna i simetrična relacija nad skupom W.*

Teorema 4.3.0.1 *Dobro zasnovana formula α je validna u S5 sistemu akko za svaki S5 model (W, R, V) i za svaki $w_i \in W, v_{w_i}(\alpha) = 1$*

Glava 5

Primena modalne logike

U ovom poglavlju ćemo govoriti o primeni modalne logike. Najočiglednija primena koju modalna logika ima jeste da proširuje iskaznu logiku. Modalna logika pomoću modaliteta daje logičarima priliku da vide uticaj mogućnosti, verovanja, znanja i sigurnosti na iskaze. Dodavanjem samo jednog simbola smo uspeli da dobijemo da se iskazna logika ponaša onako kako smo želeli da se logički sistem ponaša.

Takođe, modalna logika nužnosti i mogućnosti je samo uvodni korak u svet modalnih logika. Ova logika ima široku primenu u podvrstama modalnih logika koje smo naveli na početku poput epistemološke, deontičke, doksastičke, temporalne modalne logike i drugih. Pogotovo veliku primenu ima Kripkeova semantika sa kojom smo formalizovali semantiku modalnih sistema nužnosti i mogućnosti u formalizaciji ostalih modalnih logika.

Modalna logika ima značajnu primenu u kreiranju bezbednosnih sistema i time ćemo se baviti u nastavku ovog rada. Literatura koja je korišćena je [3], [4], [6], [9], [11] i [13].

5.1 Primena modalne logike u zaštiti informacionih sistema

Krajem 20. i početkom 21. veka videli smo brz napredak u oblasti telekomunikacija, razvijanja hardvera i softvera, kao i u enkripciji podataka. Pošto je kompjuterska oprema postala manja, brža i jeftinija elektronska obrada podataka je postala deo svakog posla i gotovo svakog domaćinstva. Kompjuteri su ubrzo postali umreženi pomoću interneta. Brz rast i široka rasprostranjenost upotreba elektronske obrade podataka i elektronskog poslovanja koje se sprovodi putem interneta, stvorilo je veliku priliku za zloupotrebu sistema. Zloupotreba može biti u vidu novčanih prevara ili korišćenja informacija u terorističke svrhe. Ovo je podstaklo potrebu za boljim metodama zaštite računara i informacija koje oni čuvaju, obrađuju i prenose. Bezbednost

informacija je postala najvažnija stvar u mnogim informacionim sistemima.

Modalna logika se sve više koristi radi formiranja modalnog okvira koji bi služio kao bezbednosni sistem. Ovaj okvir nam pomaže u određivanju pravila poverljivosti, višeslojne bezbednosne politike kao i da iskažemo različite vrste bezbednosnih ograničenja. Ovaj modalni okvir će koristiti kombinaciju epistemološke, doksastičke i deontičke modalne logike pa pošto nismo spominjali ove logike do sada, napravićemo kratko predstavljanje osnovnih osobina ovih logika.

5.1.1 Epistemološka, doksastii deontička modalna logika

Epistemološka modalna logika je vrsta modalne logike koja se bavi znanjem, a doksastička se bavi verovanjem. Epistemologija je nauka koja se bavi znanjem tj. kako znamo stvari koje znamo, i upravo iz ove reči dolazi i pojam epistemološke logike.

Sintaktički, jezik iskazne epistemološke modalne logike dobijamo tako što proširujemo jezik iskazne modalne logike sa unarnim epistomološkim operatorom K_c tako da K_cA čitamo sa "osoba c zna A". Slično važi i za verovanje, B_cA čitamo sa "osoba c veruje A".

Semantičko tumačenje epistemološkog i doksastičkog operatera možemo predstaviti pomoću semantike mogućih svetova:

K_cA: u svim mogućim svetovima kompatibilnim sa onim što osoba c zna, važi A
B_cA: u svim mogućim svetovima kompatibilnim sa onim što osoba c veruje, važi A.

Skup svetova dostupnih osobi (agentu) zavisi od informacija koje ta osoba poseduje u određenom trenutku. Ovde opet koristimo relaciju dostupnosti R. Ako se osoba c nalazi u svetu w_1, informacije iz sveta w_2 su joj dostupne ako je svet w_2 dostupan iz sveta w_1 tj. w_1Rw_2. Ako je iskaz A tačan u svim svetovima koje su dostupni osobi c tada kažemo da osoba c zna A.

Semantika mogućih svetova iskaznu epistomološku logiku sa jednom osobom c se sastoji od okvira $\mathscr{F}$ koji čini uređeni par $< W, R_c >$ gde je W neprazan skup svih mogućih svetova, a R_c je binarna relacija dostupnosti, relevantna osobi c, nad skupom W. Model $\mathscr{M}$ se sastoji od okvira i funkcije označavanja ϕ koja dodeljuje skup svetova atomičkim formulama. Formula K_cA je tačna u svetu w_1 ako važi sledeće:

$$\mathscr{M}, w_1 \models K_cA \Leftrightarrow (\forall w_i \in W)(w_1Rw_i)\mathscr{M}, w_i \models A.$$

Slična semantika može da se formira i za operator verovanja. Pošto verovanje nije nužno tačno nego moguće ili verovatno da je tačno, moramo semantiku da prilagodimo ovome.

Primer 5.1.1.1 *Osoba zna (veruje u) neku tvrdnju ako je u svim svetovima koji su kompatibilni sa znanjem (verovanjem) te osobe ta tvrdnja tačna.*

Sa druge strane, deontička modalna logika se bavi obavezom i dozvolom. Ona je veoma povezana sa logikom nužnosti i mogućnosti. Deontička logika iskaz "obavezno je da A" obeležava sa OA a iskaz "dozvoljeno je da A" sa PA (prema engleskim rečima "obligatory" i "permitted").

5.1.2 Problemi bezbednosnog sistema

Sada ćemo primeniti epistemološku i deontičku logiku kako bi napravili okvir koji bismo koristili kao bezbednosni sistem u bazama podataka. Da bi ovaj sistem funkcionisao najpre sortiramo informacije iz baze podataka u nivoe u zavisnosti koliko su one poverljive, a zatim dodeljujemo korisnicima sistema nivoe u zavisnosti kojim podacima smeju da pristupe. Pravilo koje koristimo za ovu raspodelu je sledeće: *Korisnik može da pristupi određenom podatku samo ako je njegov nivo dostupnosti veći ili jednak nivou klasifikacije tog podatka.*

Da bi smo napravili dobar modalni okvir koji bi mogao da se primeni za bezbednost informacija unutar baze podataka, potrebno je da problem poverljivosti razložimo na dva problema: 1. Treba da kontrolišemo tok informacija u bazi podataka. Ako je ovaj problem rešen sigurni smo da će korisnik dobiti informaciju iz baze podataka samo ako ima dozvolu da je dobije.2. Da kontolišemo izvedene informacije (informacije koje potiču od nekih drugih). Ako ovaj problem rešimo sigurni smo da korisnik neće moći da zaključi informaciju koju ne bi trebalo da zna iz informacije koju može da zna.

Mi smo uglavnom zainteresoivani za ovaj drugi problem koji možemo da nazovemo i problemom zaključivanja. Rešiti ovaj problem nije ni malo jednostvano zbog velikog toka informacija unutar baze podataka. Daćemo sada jedan primer da pokažemo ovo:

Primer 5.1.2.1 *Predpostavimo da se informacije o nekom vojnom avionu nalaze u bazi podataka. Ove informacije su predstavljene u vidu atomičkih formula: a="avion je opremljen kamerama", b="avion je opremljen raketama" i c="misija aviona je da izvede vazdušne napade na datu metu". Tada informaciju $a \vee b$ koja govori o mogućnostima aviona dodeljujemo nivo 1, iskazima a i $\neg a$ koji govore o opremi aviona dodeljujemo nivo 2. Iskazu $b \Rightarrow c$ koji govori o misiji aviona takođe dodoljujemo nivo 2. Konačno iskazu c koja govori o konkretnim detaljima misije dodeljujemo najviši nivo 3. Dakle, nivoi su sledeći: nivo $1 = a \vee b$, nivo $2 = a, \neg a, b \Rightarrow c$ i nivo $3 = c$. U ovom primeru vidimo da klasifikacija nije završena pošto recimo iskazu b nije dodeljen nivo. Posledica je ta da ako neki korisnik zatraži od baze podataka*

informaciju b nije jasno da li baza podataka treba da mu da tu informaciju ili ne. Takođe vidimo da ovaj sistem nije dosledan. Korisnik koji može da pristupi informacijama iz drugog nivoa može da zna informaciju $a \vee b$ i $\neg a$ što mu dozvoljava da sazna i informaciju b. Takođe, pošto može da zna informaciju $b \Rightarrow c$, može i da zna i c informaciju a njoj ne bi smeo da pristupi.

Većina poteškoća sa razumevanjem bezbednosnih sistema dolaze upravo odavde. Da je sistem nekompletan, tj da nema odgovore na neke tražene informacije i da je skup informacija kome je dodeljen bezbednosni nivo nedosledan. Da bi prevazišli ovaj problem moramo da koristimo okvir modalne logike.

5.1.3 Okvir modalne logike za rešenje problema

Predpostavimo da se sadržaj baze podataka sastoji od skupa doslednih rečenica jezika $\mathscr{L}$ iskazne logike. Ne pretpostavljamo da su rečenice tačne u tom svetu, što znači da je baza podataka sačinjena od skupa verovanja. Da bi analizirali probleme poverljivosti koji mogu da se pojave kada pristupamo bazi podataka, prvo moramo da prikažemo kako korisnik komunicira sa bazom podataka. Zbog ovoga ćemo za svakog korisnika baze podataka n definisati modalitet KB_np, gde je p iskaz iz $\mathscr{L}$, i koji se čita:"korisnik n zna da baza podataka veruje p".

U modelu $\mathscr{M}$, modalitet KB_ip je tumačen relacijom dodeljivanja R_i, koja je definisana nad WxW. Dakle semantika za KB_np glasi ovako:

$$\mathscr{M}, w_1 \models KB_np \Leftrightarrow (\forall w_i \in W)(w_1R_nw_i)\mathscr{M}, w_i \models p.$$

Radi lakšeg zapisa, skup $w_i : w_1R_nw_i$ ćemo pisati $R_n(w_1)$. Skup svetova gde je p tačno možemo da obeležimo sa $|p|$. Sada prethodnu ekvivalenciju možemo zapisati ovako:

$$\mathscr{M}, w_1 \models KB_np \Leftrightarrow R_n(w_1) \subseteq |p|.$$

Modalitet KB_np ispunjava dve aksiome epistemološke logike a to su aksiome K i D:

- **K:** $KB_n(p \Rightarrow q) \Rightarrow (KB_np \Rightarrow KB_nq)$
- **D:** $KB_np \Rightarrow \neg KB_n\neg p$.

Aksiomu K interpretiramo na sledeći način:"Ako osoba n zna da baza podataka veruje $p \Rightarrow q$ onda osoba n zna da baza podataka veruje p što implicira da osoba n zna da baza podataka veruje q". Aksiomu D interpretiramo na sledeći način:"Ako osoba n zna da baza podataka veruje p onda osoba n ne zna da sistem veruje ne p".

Primećujemo da modalni operator KB_np predstavlja kombinaciju epistomološke i doksastičke modalne logike. Pomoću epistemološke logike predstavljamo znanje koje poseduje korisnik baze podataka, a pomoću doksastičke šta baza podataka veruje.

5.1.4 Dozvola i zabrana da znamo

Baze podataka koje nas zanimaju su one koje imaju neke osetljive informacije, poput onih u primeru 5.1.2.1. U tom kontekstu neki korisnici nemaju prava da pristupe svim informacijama iz baze podataka. Čemu će korisnik smeti da pristupi, a čemu neće to određujemo pomoću pravila poverljivosti. Pravilo poverljivosti zasnivamo na konceptu uloge. Svaki korisnik može da igra drugu ulogu u zavisnosti od toga šta on sme, a šta ne sme da zna. Zbog ovoga ćemo za svaku ulogu r definisati dva modaliteta PKB_rp i FKB_rp. Slova P i F obeležavaju reči "dozvoljeno" i "zabranjeno" (prema engleskim rečima "permitted" i "forbidden"). Formula PKB_rp (resp. FKB_rp) se čita :"Svakoj osobi koja ima ulogu r je dozvoljeno (resp. zabranjeno) da zna da baza podataka veruje p".

U modelu $\mathscr{M}$ modalitet PKB_rp imamo dve relacije dostupnosti koje su definisane nad WxW. Jedna relacija dostupnosti je D_r koja je deontička relacija dostupnosti koja karakteriše skup idealnih mentalnih stanja osobe (u našoj situaciji korisnika baze podataka) nr koja igra ulogu r. Relacija R_{nr} je doksastička relacija koja karakteriše skup verovanja koja osoba nr poseduje. Semantika modalnog operatore PKB_rp je definisana na sledeći način:

Definicija 5.1.4.1

$$\mathscr{M}, w_1 \models PKB_rp \Leftrightarrow (\exists w_i)(w_1 D_r w_i \wedge (\forall w_k)(w_i R_{nr} w_k \Rightarrow \mathscr{M}, w_k \models p)$$

ili ekvivalentno:

$$\mathscr{M}, w_1 \models PKB_rp \Leftrightarrow (\exists w_i)(w_1 D_r w_i \wedge R_{nr}(w_i) \subseteq |p|).$$

Kao i obično, zabranu definišemo kao negaciju dozvole zato važi:

Definicija 5.1.4.2 $FKB_rp \Leftrightarrow \neg PKB_rp$

Primetimo da možemo da definišemo i funkciju F_r za svaku ulogu r. Ona svakom svetu w u modelu $\mathscr{M}$ dodeljuje skup skupova svetova gde svaki skup svetova predstavlja moguće mentalno stanje korisnika xr. Formalno funkciju F_r zapisujemao na sledeći način:

$$F_r : W \to 2^{2^W}$$

i pomoću nje možemo da uvedemo još jednu definiciju modaliteta PKB_rp:

Definicija 5.1.4.3

$$\mathscr{M}, w_1 \models PKB_rp \Leftrightarrow (\exists X)(X \in F_r(w_1) \wedge X \subseteq |p|).$$

Iz ove semantike možemo videti da modaliteti PKB_rp i FKB_rp imaju sledeće osobine:

- Osobina 1: $(\models p \Rightarrow q) \Rightarrow (\models PKB_r p \Rightarrow PKB_r q)$
- Osobina 2: $(\models p \Rightarrow q) \Rightarrow (\models FKB_r p \Rightarrow FKB_r q)$
- Osobina 3: $\not\models PKB_r p \wedge PKB_r q \Rightarrow PKB_r(p \wedge q)$
- Osobina 4: $\not\models FKB_r(p \wedge q) \Rightarrow (FKB_r p \vee FKB_r q)$

Osobine 1 i 2 pokazuju da skup rečenica koje agent koji igra ulogu r sme da zna je proširen njihovim logičkim posledicama, dok je skup rečenica koje agent ne sme da zna je takođe proširen logičkim posledicama tih rečenica.

Treća osobina nam pokazuje da može da se desi da izvedemo p iz dozvoljenog mentalnog stanja u kom se nalazi agent xr, i da q možemo da izvedemo iz dozvoljenog mentalnog stanja u kom se nalazi agent xr, ali ne postoji dozvoljeno mentalno stanje agenta xr iz kog možemo da izvedemo $p \wedge q$. Četvrta osobina je suprotnost trećoj osobini. Ona nam govori da je moguće da je agentu koji igra ulogu r zabranjeno da zna $p \wedge q$, dok mu nije zabranjeno da zna p i nije mu zabranjeno da zna q.

5.1.5 Sigurnosni sistem više nivoa

Sigurnosni sistem više nivoa dodeljujuje klasifikacioni nivo rečenicama koje predstavljaju informacije u bazi podataka i dozvoljeni nivo korisnicima baze podataka. Klasifikacioni nivoi za informacije i dozvoljeni nivoi za korisnike su uzeti iz skupa sigurnosnih nivoa.

Primer 5.1.5.1 *Na primer, za sigurnosne nivoe možemo da koristimo strogo poverljivo (SP), tajno (T), poverljivo (P) i javno (J). U ovom slučaju redosled poverljivosti informacija je sledeći:*

$$J < P < T < SP.$$

Kako bismo formalno predstavili ovo, moramo da uvedemo funkciju koja dodeljuje klasifikacioni nivo rečenicama. Najpre definišemo za svaki bezbednosni nivo 1, modalitet [1], i formulu tipa $[1]p$ čitamo sa:"Formula p je svrstana u nivo 1".

Primer 5.1.5.2 *Rečenicu [T]Plata(Petrović, 60 000RSD) nam govori da je klasifikacioni nivo rečenice "Petrovićeva plata je 60 000RSD" tajna.*

Rečenica može biti klasifikovana iako se ne nalazi u bazi podataka. Ovako možemo da stavimo da je tajna iznos Petrovićeve plate iako je u bazi podataka kao poverljiva informacija stavljen tačan iznos plate. Radi lakše formalizacije, umesto korišćenja modaliteta $[1]p$ koristićemo modaliteta $[\leq 1]$. Formula koja ima formu $[\leq 1](p_1, ..., p_n)$ se čita:"$(p_1, ..., p_n)$ je skup svih formula koje su klasifikovane nivoom jednakim ili manjim od 1". Uvodimo funkcija C_1, za koju važi: $C_1 : W \to 2^{2^W}$. U svetu w, ako je data formula p svrstana u nivo koji je manji ili jednak nivou 1, tada $|p|$ pripada $C_1(w)$. Semantiku $[\leq 1]$ definišemo na sledeći način:

Definicija 5.1.5.1

$$\mathscr{M}, w \models [\leq 1](p_1, ..., p_n) \Leftrightarrow C_1(w) = \{|p_1|, ..., |p_n|\}$$

Pomoću ove semantike sada možemo i da objasnimo kako dozvola i zabrana funkcionišu u bezbednosnim sistemima sa više nivoa. Ono što moramo da uradimo jeste da za nivo 1 definišemo modalitet $PKB_1^e p$ ($FKB_1^e p$) koji čitamo:"Agentu kome je dodeljen nivo 1, dozvoljeno (zabranjeno) je da zna da baza podataka veruje p". Isto radimo za svaki nivo koji koristimo.

5.1.6 Ograničenja sigurnosnog sistema

Potrebno je da uvedemo određena ograničenja kako bi naš sigurnosni sistem što bolje funkcionisao. Prvo, predstavljamo bezbednosno ograničenje koje će garantovati poverljivost i doslednost. Ovo ograničenje se primenjuje na sledećem slučaju: u datom svetu w, ne postoji rečenica p i sigurnosni nivo 1, tako da je korisniku kome je dodeljen nivo 1 u isto vreme dozvoljeno i zabranjeno da zna p. Ovo možemo zapisati i na ovaj način:

$$\mathscr{M}, w \models \neg(PKB_1^e p \wedge FKB_1^e p).$$

Takođe zahtevamo da je sigurnosni sistem više nivoa kompletan. Kompletnost u svetu w znači da za svaku rečenicu p, svaki sigurnosni nivo 1 i za svakog korisnika kojem je dodeljen nivo 1, važi da mu je ili dozvoljeno ili zabranjeno da zna p. Ovo formalno predstavljamo na sledeći način:

$$\mathscr{M}, w \models PKB_1^e p \vee FKB_1^e p.$$

Još jedno bezbednosno ograničenje koje važi je da ako u svetu w, ako korisnik i koji igra ulogu r zna da baza podataka veruje rečenicu p, onda je dozvoljeno da svi korisnici koji igraju ulogu r znaju da baza podataka veruje p. Ovo zapisujemo na sledeći način:

$$\mathscr{M}, w \models KB_i p \Rightarrow PKB_r p.$$

Poslednje ograničenje se odnosi na situaciju kada korisnik i kome je odobren nivo 1, dobija neku informaciju p iz baze podataka. Ovo je moguće ukoliko infomacija p nije zabranjena korisniku i. Zbog toga važi:

$$KB_i p \Rightarrow PKB_1^i p.$$

Ovo ograničenje nam kaže da je osobi dozvoljeno da pristupi određenoj informaciji iz baze podataka, ako mu ta informacija ne omogućava da iz nje izvuče neku drugu poverljivu informaciju.

Predstavili smo bezbednosni sistem koji se može koristiti u netrivijalnim informacionim sistemima.Takođe smo videli da sigurnosna ograničenja zahtevaju detaljnu analizu i formalizovali smo ta ograničenja.

Glava 6

Zaključak

6.1 Rezime rada

Svrha pisanja ovog rada je bila da prikaže najbitnije pojmove za razumevanje modalne logike i da predstavi njenu veoma konkretnu primenu u zaštiti informacionih sistema. U radu smo najviše govorili o aletičkoj logici, kao osnovi za razumevanje drugih vrsta modalne logike.

Primentili smo da su sistemi o kojima smo govorili T, S4 i S5 povezani tj. da se S5 sistem sadrži S4 i T sistem i da S4 sistem sadrži T sistem. Ovo se izrazilo i na relaciju dostupnosti i na njene osobine u datim sistemima. U sistemu T ona je refleksivna, u sistem S4 je relfeksivna i tranzitivna, dok je u sistemu S5 refleksivna, tranzitivna i simetrična. Ovo praktično znači da u S5 sistemu svaki mogući svet mora da vidi svaki drugi mogući svet.

Takođe, videli smo veliku sličnost u semantici sistema u aletičkoj logici, sa sistemima u epistemološkoj logici. Glavna aksioma sistema S4 u aletičkoj logici je $\Box A \Rightarrow \Box\Box A$ dok se je glavna aksioma sistema S4 u epistemološkoj logici $K_c A \Rightarrow K_c K_c A$. Bitna razlika međutim jeste da se u aletičkoj i deontičkoj logici relacija dostupnosti odnosi na ceo mogući svet, dok se u epistemološkoj i doksastičkoj logici relacija dostupnosti odnosi na agenta (osobu) unutar mogućeg sveta.

6.2 Pravci daljih istraživanja

Mnogi smatraju da je matematička logika najbitnija grana logike zbog njene široke primene u računarstvu i informacionim sistemima. Takođe, modalna logika je veoma mlada grana matematičke logike i zbog toga su mogućnosti za dalja istraživanja zaista velike.

Što se tiče daljeg istraživanja zaštite informacionih sistema ona mogu ići u više pravaca. Jedan od mogućih pravaca je da definišemo efikasnu strategiju za racionalizaciju u ovoj logici kako bismo mogli da dizajniramo realnu implikaciju. Ovo

će možda zahtevati da ograničimo jezik baze pdoataka. Takođe, u radu smo podrazumevali da stepen poverljivosti podataka, kao i dodeljivanje nivoa kom korisnik može da pristupi određuju korisnici koji ubacuju podatke u bazu. Međutim šta ako korinik koji to određuje nema kompletne informacije i ne može lako da utvrdi da li treba da dâ dozbvolu za pristup podacima ili ne treba. Istraživanje nas dalje vodi u pravcu razvijanja semantiku za formalni jezik koji bi ovo mogao da radi umesto korisnika.

Literatura

[1] Aćimović, M. *Filozofija mišljenja*, Futura publikacije, Novi Sad, 2007.

[2] Chellas, B.F. *Modal Logic: An Introduction,* Cambridge University Press, 1988.

[3] Cuppens., F.Demolombe, R. *A Modal Logical Framework for Security Policies,* Foundations of Intelligent Systems, Volume 1325 of the series Lecture Notes in Computer Science pp 579-589, Toulouse 1997.

[4] Denning, D. *Cryptography and Data Security,* Addison-Wesley, 1982.

[5] Došen, K. *Osnovna logika,* Matematički institut SANU, Beograd 2008.

[6] Došen, K. *Sequent-Systems for Modal Logic, The Journal of Symbolic Logic 50*, Cambridge University Press, Association for Symbolic Logic, Cambridge 1985.

[7] Fitting, M. *First-Order Logic and Automated Theorem Proving* Springer, New York 1996.

[8] Hughes, G., Cresswell, M. *An Introduction To Modal Logic*, Methuen and CO LTD, London, 1968.

[9] Huth, M., Ryan, M. *Logic in Computer Science: Modelling and Reasoning about Systems*, Cambridge University Press, Cambridge, 2000.

[10] Janičic, P. *Matematiǩa logika u računarstvu,* Matematički fakultet,četvtro izdanje, Beograd 2008.

[11] Paulson, L.C. *Logic and Proof:Computer Science Tripos Part IB,* University of Cambridge , Computer Laboratory , Cambridge, 2012.

[12] Popkorn, S. *First Steps in Modal Logic,* Cambridge University Press, Cambridge 1995.

[13] Sutherland, D. *A Model of Information* In Proceedings of the 9th National Computer Security Conference, 1986.

[14] Van Dalen, D. *Logic and Structure,* Springer, Heidelberg 1994.

[15] Vuković, M. *Matematička logika 1*, četvrto izdanje, Prirodno-matematički fakultet, Zagreb, 2007.

[16] *mally.stanford.edu*

[17] *www.iep.utm.edu.*

[18] *www.plato.stanford.edu*

Biografija

Marko Stupar je rođen u Subotici 24.06.1988. godine. Ubrzo nakon rođenja se sa porodicom preselio u Novi Sad gde je završio osnovnu i srednju školu. U junu 2007. godine upisuje Prirodno-matematički fakultet na Univerzitetu u Novom Sadu, Departman za matematiku i informatiku, studijski program Finansijska matematika. 2013. godine je diplomirao i ubrzo zatim upisuje Fakultet tehničkih nauka u Novom Sadu. U međuveremenu je proveo godinu dana u Norveškoj gde je studirao međukulturnu komunikaciju. U avgustu 2014. godine se oženio Matejom što smatra najvećim uspehom u životu.