SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Filip Skrinjar

ALGORITMI ZA STANDARDNU TRANSLACIJU MODALNIH FORMULA

Diplomski rad

Voditelj rada:
Prof.dr.sc. Mladen Vuković

Zagreb, Prosinac, 2019

Ovaj diplomski rad obranjen je dana ____________________ pred ispitnim povjerenstvom u sastavu:

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom _______________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Ovaj rad posvećujem svojoj obitelji. Svatko od njih imao je veliku ulogu u mom školovanju i odrastanju.

Sadržaj

Uvod

U ovom radu promatramo Szalasov algoritam koji za danu modalnu formulu pronalazi njenog korespondenta prvog reda. Szalasov algoritam se može primijeniti u sustavima za automatsko dokazivanje teorema modalne logike. U prvom poglavlju definiramo osnovni modalni jezik te Kripkeovu semantiku za modalnu logiku. Zatim iznosimo potrebne definicije i rezultate logike prvog reda te ukratko iznosimo potrebne pojmove logike drugog reda. U drugom poglavlju rada bavimo se temom korespondencije formula osnovnog modalnog jezika i formula logike prvog i drugog reda. Promatramo funkciju standardne translacije te definiramo jednu istaknutu klasu modalnih formula zvanu Sahlqvistove formule. U trećem poglavlju detaljno promatramo Szalasov algoritam. Teorijski ga analiziramo i opisujemo po koracima, potom iznosimo pseudokod algoritma kao i neke primjere rada.

Poglavlje 1

Modalna logika i logika prvog reda

U prvom dijelu rada definiramo sintaksu i semantiku modalne logike a potom iznosimo najbitnije definicije logike prvog reda. Pojmovi i rezultati izneseni u ovom poglavlju nužni su za razmatranje algoritama automatske korespondencije modalne logike i logike prvog reda. Na kraju poglavlja ukratko iznosimo i neke pojmove logike drugog reda, za koju ćemo vidjeti da je također nužna za daljnja razmatranja.

1.1 Osnovni modalni jezik

Modalna logika je u svojoj osnovi nastala kao nadogradnja na logiku sudova. Jedna od glavnih mana klasične logike sudova je definicija interpretacije logičkog veznika kondicionala. Semantička interpretacija kondicionala razlikuje se od govorne intuicije. Tako je rečenica ”*Ako sam visok pet metara onda dobro igram šah*” istinita u klasičnoj logici sudova dok govorno nema nekog smisla.

Uz to željelo se proširiti ekspresivne moći logike sudova da bi se matematički mogle opisati rečenice kao ”*Ako je oblačno tada je moguće da će padati kiša.*” ili ”*Ako je UV-index 8 i sunčam se 5 sati tada ću nužno dobiti opekotine.*”

Želja za takvim proširenjima dovodi do promatranja operatora na sudovima koji su dobili naziv **modalni operatori**, pa se iz tog razloga i pripadne logike nazivaju **modalne logike**. U prethodnim primjerima koristili smo dva operatora: ”nužno” i ”moguće”, koje redom označavamo sa $\Box$ i $\Diamond$.

Ne postoji jedna modalna logika, pa tako ne postoji niti jedinstveni modalni jezik. Postoje razne modalne logike čiji modalni jezici mogu imati i više operatora na sudovima ili u kojima modalni operatori mogu djelovati na više sudova. Mi ćemo se fokusirati na osnovni modalni jezik gdje se jeziku klasične logike sudova dodaje samo jedan unarni operator $\Diamond$. Definirajmo sintaksu osnovnog modalnog jezika.

Definicija 1.1.1. *Abecedu* ***osnovnog modalnog jezika*** *čini prebrojiv skup propozicionalnih varijabli Φ čije elemente označavamo sa $P_0, P_1, P_2, \ldots$, zatim bulovski veznici negacije $\neg$, konjunkcije $\wedge$, disjunkcije $\vee$, kondicionala $\rightarrow$ i bikondicionala $\leftrightarrow$, logička konstanta za laž $\perp$, te unarni modalni operator $\Diamond$.*
Formula *osnovnog modalnog jezika definira se rekurzivno:*

1. *Svaka propozicionalna varijabla je formula i $\perp$ je formula.*

2. *Ako su A i B formule, onda su riječi $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ i $(\Diamond A)$ također formule.*

Za operator $\Diamond$ definiramo njemu dualni operator $\Box$ sa $\Box A := \neg\Diamond\neg A$. Formulu $\Diamond A$ čitamo "*Moguće je A.*", a formulu $\Box A$ čitamo kao dual "*Nije moguće da nije A.*" odnosno "*Nužno je A.*". Iz tog razloga operatore $\Diamond$ i $\Box$ redom zovemo **operator mogućnosti** i **operator nužnosti**. Neki primjeri formula osnovnog modalnog jezika su: $\Diamond P_0 \rightarrow \Box P_{14}$, $\Diamond\Box\Diamond P_7 \rightarrow P_5$, $P_0 \vee \neg P_4, \ldots$, dok su primjeri riječi koje nisu formule osnovnog modalnog jezika: $\forall x\, \Box P(x)$, $\triangle(P_0, P_{14}) \rightarrow P_7$, $R(\Diamond P_1, P_2) \rightarrow P(\Box P_6), \ldots$

Prirodno pitanje koje se dalje nameće jest kako definirati semantiku, odnosno značenje prethodno definirane sintakse. Kako je osnovni modalni jezik proširenje jezika logike sudova s jednim operatorom, tada je razumno probati proširiti definiciju interpretacije kao istinitosnu funkciju koja bi sada dodatno djelovala i na operator $\Diamond$. Tada imamo sljedeće mogućnosti: možemo dodefinirati interpretaciju I tako da $I(\Diamond A) := 1$ ili $I(\Diamond A) := 0$, za svaku formulu A. No takvo dodefiniranje nam nije od neke koristi jer njime dobivamo konstante koje već postoje u jeziku. Dalje nam ostaju još dvije mogućnosti: $I(\Diamond A) := I(A)$ ili $I(\Diamond A) := 1 - I(A)$, za svaku formulu A. No u takvom dodefiniranju uvedeni operator $\Diamond$ je ili identiteta ili negacija što nam opet nije od koristi. Dakle interpretaciju modalnih operatora ne možemo jednostavno zadati pomoću neke istinitosne funkcije. Semantika modalne logike koju ćemo mi koristiti u ovome radu zove se **Kripkeova semantika**.

1.2 Kripkeova semantika

Kripkeovu semantiku razvio je Saul Kripke šezdesetih godina prošlog stoljeća. U Kripkeovoj semantici ključnu ulogu imaju pojmovi okvira i modela, stoga prije daljnjeg razmatranja prvo dajemo njihovu definiciju.

Definicija 1.2.1. ***Kripkeov okvir*** *(skraćeno* ***okvir****) je uređeni par (W, R) gdje je W neki neprazan skup kojeg nazivamo* ***domena*** *i čije elemente zovemo* ***svjetovi****, a $R \subseteq W \times W$*

binarna relacija koju zovemo ***relacija dostiživosti****. Ako za x i y iz W vrijedi da je uređeni par (x, y) u relaciji R, tada to označavamo sa xRy i kažemo da je svijet y* ***R-dostiživ*** *iz svijeta x.*
Kripkeov model *$\mathfrak{M}$ je uređena trojka $(W, R, \Vdash)$, gdje je (W, R) okvir, a $\Vdash$ je binarna relacija između svjetova i formula koja ima sljedeća svojstva:*

1. $w \nVdash \perp$
2. $w \Vdash \neg A$ *ako i samo ako* $w \nVdash A$
3. $w \Vdash A \wedge B$ *ako i samo ako* $w \Vdash A$ *i* $w \Vdash B$
4. $w \Vdash A \vee B$ *ako i samo ako* $w \Vdash A$ *ili* $w \Vdash B$
5. $w \Vdash A \rightarrow B$ *ako i samo ako* $w \nVdash A$ *ili* $w \Vdash B$
6. $w \Vdash A \leftrightarrow B$ *ako i samo ako* $w \Vdash A$ *je ekvivalentno sa* $w \Vdash B$
7. $w \Vdash \Diamond A$ *ako i samo ako* $\exists v\ (wRv \text{ i } v \Vdash A)$

Relaciju $\Vdash$ zovemo ***relacija forsiranja****.*

Napomena 1.2.2. *Iz definicije modalnog operatora nužnosti direktno slijedi $w \Vdash \Box A$ ako i samo ako za svaki svijet v takav da wRv vrijedi $v \Vdash A$.*

Primijetimo da se u definiciji forsiranja formula oblika $\Diamond A$, pa onda i u forsirsiranju formula oblika $\Box A$, redom javlja egzistencijalna i univerzalna kvantifikacija prvog reda po elementima domene. Definicija istinitosti formule direktno se veže na pojmove Kripkeovog modela i Kripkeovog okvira te razlikujemo značenje istinitosti formule na modelu i na okviru.

Definicija 1.2.3. *Neka je $\mathfrak{M} = (W, R, \Vdash)$ Kripkeov model. Kažemo da je neka formula F* ***istinita na modelu*** *$\mathfrak{M}$ ako za svaki svijet $w \in W$ vrijedi $\mathfrak{M}, w \Vdash F$. To kratko označavamo sa $\mathfrak{M} \models F$.*
Kažemo da je formula F ***valjana*** *ako za svaki Kripkeov model $\mathfrak{M}$ vrijedi $\mathfrak{M} \models F$.*
Neka je $\mathcal{F} = (W, R)$ neki Kripkeov okvir, te F neka formula. Kažemo da je formula F ***istinita na okviru*** *$\mathcal{F}$ ako za svaku relaciju forsiranja $\Vdash$ na okviru $\mathcal{F}$ vrijedi da za model $\mathfrak{M} = (W, R, \Vdash)$ vrijedi $\mathfrak{M} \models F$. To označavamo sa $\mathcal{F} \models F$.*

Primijetimo da u definiciji valjanosti formule imamo univerzalnu kvantifikaciju po modelima, što je kvantifikacija drugog reda.

U današnje vrijeme modalna logika se koristi kao sredstvo za opis relacijskih struktura. Za neki okvir $\mathcal{F} = (W, R)$ kažemo da je tranzitivan (refleksivan; simetričan) ako je relacija R tranzitivna (refleksivna; simetrična). Sljedeća propozicija služi kao motivacija za razmatranje modalne logike kao sredstvo opisa relacijskih struktura.

Propozicija 1.2.4. *Neka je $\mathcal{F} = (W, R)$ proizvoljan okvir. Tada vrijede slijedeće tvrdnje:*

1. $\mathcal{F} \Vdash \Diamond\Diamond P \to \Diamond P$ *ako i samo ako* $\mathcal{F}$ *je tranzitivan okvir*
2. $\mathcal{F} \Vdash P \to \Diamond P$ *ako i samo ako* $\mathcal{F}$ *je refleksivan okvir*
3. $\mathcal{F} \Vdash P \to \Box\Diamond P$ *ako i samo ako* $\mathcal{F}$ *je simetričan okvir*

Dokaz. Dokažimo prvu tvrdnju. Neka je $\mathcal{F}$ tranzitivan okvir, $\Vdash$ proizvoljna relacija forsiranja i $w \in W$ proizvoljan svijet. Označimo sa $\mathfrak{M} = (W, R, \Vdash)$ model nad okvirom $\mathcal{F}$. Ako $\mathfrak{M}, w \nVdash \Diamond\Diamond P$ tada iz definicije relacije forsiranja (1.2.1) slijedi $\mathfrak{M}, w \Vdash \Diamond\Diamond P \to \Diamond P$. Ako $\mathfrak{M}, w \Vdash \Diamond\Diamond P$ tada pokažimo da $\mathfrak{M}, w \Vdash \Diamond P$. Dakle, trebamo pokazati da postoji svijet v koji je R-dostiživ iz w i da vrijedi $\mathfrak{M}, v \Vdash P$. Kako po pretpostavci $\mathfrak{M}, w \Vdash \Diamond\Diamond P$, tada iz definicije (1.2.1) slijedi da postoji svijet $v \in W$ takav da vrijedi wRv i $\mathfrak{M}, v \Vdash \Diamond P$. Kako $\mathfrak{M}, v \Vdash \Diamond P$, tada ponovno iz definicije (1.2.1) slijedi da postoji svijet $u \in W$ takav da vrijedi vRu i $\mathfrak{M}, u \Vdash P$. Budući da nam je osnovna pretpostavka da je $\mathcal{F}$ tranzitivan okvir, tada po svojstvu tranzitivnosti iz wRv i vRu slijedi wRu. Dakle postoji svijet u koji je R-dostiživ iz w i $\mathfrak{M}, u \Vdash P$ pa tada iz definicije (1.2.1) slijedi $\mathfrak{M}, w \Vdash \Diamond P$. Time, imamo da za svaki svijet $w \in W$ vrijedi $\mathfrak{M}, w \Vdash \Diamond\Diamond P \to \Diamond P$. Iz definicije sada slijedi $\mathfrak{M} \models \Diamond\Diamond P \to \Diamond P$. No iz proizvoljnosti relacije forsiranja slijedi da je formula $\Diamond\Diamond P \to \Diamond P$ istinita na okviru $\mathcal{F}$, što dokazuje prvi smjer.

Dokažimo obrat. Neka je $\mathcal{F}$ okvir takav da $\mathcal{F} \Vdash \Diamond\Diamond P \to \Diamond P$. Tada iz definicije (1.2.1) slijedi da za svaku relaciju forsiranja $\Vdash$ i za svaki svijet $w \in W$ vrijedi $\mathfrak{M}, w \Vdash \Diamond\Diamond P \to \Diamond P$, gdje je $\mathfrak{M} = (W, R, \Vdash)$. Tada vrijedi:

$$\mathfrak{M}, w \nVdash \Diamond\Diamond P \quad \textit{ili} \quad \mathfrak{M}, w \Vdash \Diamond P \tag{1.1}$$

Ako pretpostavimo da $\mathcal{F}$ nije tranzitivan, tada postoje svjetovi $w, v, u \in W$ takvi da wRv i vRu, te da u nije R-dostiživ iz w. No tada za relaciju forsiranja $\Vdash'$ za koju vrijedi:

1. $\mathfrak{M}, w \nVdash' P$
2. $\mathfrak{M}, u \Vdash' P$
3. $\mathfrak{M}, t \nVdash' P$, za svaki svijet t koji je R-dostiživ iz w

imamo $\mathfrak{M}, w \Vdash' \Diamond\Diamond P$ i $\mathfrak{M}, w \nVdash' \Diamond P$, što nam daje kontradikciju sa (1.1). Dakle $\mathcal{F}$ je tranzitivan okvir.

Dokažimo sada drugu tvrdnju. Neka je $\mathcal{F}$ refleksivan okvir, $\Vdash$ proizvoljna relacija forsiranja i $w \in W$ proizvoljan svijet. Označimo sa $\mathfrak{M} = (W, R, \Vdash)$ model nad okvirom $\mathcal{F}$. Ako $\mathfrak{M}, w \nVdash P$ tada iz definicije relacije forsiranja (1.2.1) slijedi $\mathfrak{M}, w \Vdash P \to \Diamond P$. Pretpostavimo $\mathfrak{M}, w \Vdash P$, te pokažimo da vrijedi $\mathfrak{M}, w \Vdash \Diamond P$. Dakle, pokažimo da postoji $v \in W$ koji je R-dostiživ iz w i za koji vrijedi $\mathfrak{M}, v \Vdash P$. Kako je po pretpostavci $\mathcal{F} = (W, R)$ refleksivan okvir, tada je svaki svijet $w \in W$ R-dostiživ iz samoga sebe. Sada iz pretpostavke $\mathfrak{M}, w \Vdash P$ te iz definicije (1.2.1) direktno slijedi $\mathfrak{M}, w \Vdash \Diamond P$.

Dokažimo obrat. Neka je $\mathcal{F}$ okvir takav da $\mathcal{F} \Vdash P \to \Diamond P$. Tada iz definicije (1.2.1) slijedi da za svaku relaciju forsiranja $\Vdash$ i za svaki svijet $w \in W$, $\mathfrak{M}, w \Vdash P \to \Diamond P$, gdje je $\mathfrak{M} = (W, R, \Vdash)$. Tada imamo:

$$\mathfrak{M}, w \nVdash P \qquad \textit{ili} \qquad \mathfrak{M}, w \Vdash \Diamond P \tag{1.2}$$

Ako pretpostavimo da $\mathcal{F}$ nije refleksivan okvir, tada postoji svijet $w \in W$ koji nije R-dostiživ iz samoga sebe. Tada za relaciju forsiranja $\Vdash'$ za koju vrijedi:

1. $\mathfrak{M}, w \Vdash' P$ i
2. $\mathfrak{M}, v \nVdash' P$, za svaki svijet v koji je R-dostiživ iz w

imamo $\mathfrak{M}, w \Vdash' P$ i $\mathfrak{M}, w \nVdash' \Diamond P$ jer za niti jedan svijet v koji je R-dostiživ iz w ne vrijedi $\mathfrak{M}, v \Vdash' P$. To nam daje kontradikciju sa (1.2). Dakle, $\mathcal{F}$ je refleksivan okvir.

Dokažimo sada i posljednju tvrdnju propozicije. Neka je $\mathcal{F}$ simetričan okvir, $\Vdash$ proizvoljna relacija forsiranja i $w \in W$ proizvoljan svijet. Označimo sa $\mathfrak{M} = (W, R, \Vdash)$ model nad okvirom $\mathcal{F}$. Ako $\mathfrak{M}, w \nVdash P$ tada iz definicije relacije forsiranja (1.2.1) slijedi $\mathfrak{M}, w \Vdash P \to \Box\Diamond P$. Ako $\mathfrak{M}, w \Vdash P$ tada pokažimo da $\mathfrak{M}, w \Vdash \Box\Diamond P$. Dakle, trebamo pokazati da za svaki svijet v koji je R-dostiživ iz w, postoji svijet u koji je R-dostiživ iz v takav da $\mathfrak{M}, u \Vdash P$.

Kako je po pretpostavci $\mathcal{F} = (W, R)$ simetričan okvir, tada

$$(\forall v \in W)\ \Big(\text{ako } wRv \text{ tada } vRw\Big) \tag{1.3}$$

Dalje, kako $\mathfrak{M}, w \Vdash P$ tada

$$(\forall v \in W)\ \Big(\text{ako } vRw \text{ onda } \mathfrak{M}, v \Vdash \Diamond P\Big) \tag{1.4}$$

Iz (1.3) i (1.4) slijedi da za svaki svijet $v \in W$, ako wRv onda $\mathfrak{M}, v \Vdash \Diamond P$. Što je, po napomeni (1.2.2) upravo $\mathfrak{M}, w \Vdash \Box\Diamond P$.

Dokažimo obrat. Neka je $\mathcal{F}$ okvir takav da $\mathcal{F} \Vdash P \to \Box\Diamond P$. Tada iz definicije (1.2.1) slijedi da za svaku relaciju forsiranja $\Vdash$ i za svaki svijet $w \in W$, $\mathfrak{M}, w \Vdash P \to \Box\Diamond P$, gdje je $\mathfrak{M} = (W, R, \Vdash)$. Tada imamo:

$$\mathfrak{M}, w \nVdash P \qquad ili \qquad \mathfrak{M}, w \Vdash \Box\Diamond P \tag{1.5}$$

Ako pretpostavimo da $\mathcal{F}$ nije simetričan okvir tada postoje svijetovi $w, v \in W$ takvi da vrijedi wRv i da w nije R-dostiživ iz v. Tada za relaciju forsiranja $\Vdash'$ za koju vrijedi:

1. $\mathfrak{M}, w \Vdash' P$,
2. $\mathfrak{M}, v \nVdash' P$ i
3. $\mathfrak{M}, t \nVdash' P$, za svaki svijet t koji je R-dostiživ iz v

imamo $\mathfrak{M}, w \Vdash' P$ i $\mathfrak{M}, w \nVdash' \Box\Diamond P$ jer postoji svijet v koji je R-dostiživ iz w i za koji $\mathfrak{M}, v \nVdash' \Diamond P$ pošto niti jedan svijet R-dostiživ iz v ne forsira P. To nam daje kontradikciju sa (1.5). Dakle, $\mathcal{F}$ je simetričan okvir. $\Box$

Ovi rezultati motiviraju istraživanje modalne logike kao sredstvo za opis relacijskih struktura jer izuzetno jednostavnim izrazima, kao što je npr. $\Diamond\Diamond P \to \Diamond P$, možemo opisati svojstva relacija kao što je tranzitivnost. Ako zanemarimo interpretaciju, sintaktički zapis svojstva tranzitivnosti u modalnom jeziku nema kvantifikatora. Ima dva pojavljivanja iste propozicionalne varijable, tri pojavljivanja istog operatora i jedan logički veznik.

1.3 Sistem K

Iako aksiomatski sistemi modalnih logika nisu glavna tema ovoga rada, oni će nam biti korisni u kasnijim razmatranjima. Prve formalizacije modalne logike bile su aksiomatske. Pojam nužnosti i mogućnosti je u nekim situacijama nejasan u intuitivnom smislu. Tako se na primjer postavlja pitanje hoćemo li uzeti formulu $\Box A \to \Box\Box A$ kao aksiom u modalnim sistemima ili ne? Ovisno o prihvaćanju ili ne prihvaćanju pojedinih formula kao aksioma u aksiomatskom sistemu dolazimo do različitih aksiomatskih sistema modalne logike. Jedan od najjednostavnijih modalnih sistema obično se označava sa **K** (u čast S. Kripkeu).

Alfabet sistema **K** je osnovni modalni jezik a aksiomi sistema **K** su sve tautologije i aksiom distribucije: $\Box(A \to B) \to (\Box A \to \Box B)$. Napomenimo da se pod tautologije smatraju tautologije u osnovnom modalnom jeziku, što znači da se uz valjane formule klasične logike sudova tu ubrajaju i modalne formule nastale uniformnom supstitucijom propozicionalnih varijabli u tautologijama proizvoljnim formulama. Tako su $\Box A \vee \neg\Box A$, $\bot \to \Diamond A$ i $\Diamond A \to \Diamond A$ neki primjeri tautologija u sistemu **K**. Pravila izvoda sistema **K** su klasični modus ponens i pravilo nužnosti: iz A slijedi $\Box A$. Sasvim analogno kao za sistem **RS** definiraju se pojmovi dokaza, izvoda i teorema.

Spomenimo ukratko još neke aksiomatske sisteme. Sistem **T** dobiva se dodavanjem sistemu **K** aksiom refleksivnosti: $\Box A \to A$. Lako je vidjeti da je formula $\Box A \to A$ ekvivalentna formuli $A \to \Diamond A$ koja po prethodnoj propoziciji određuje refleksivnost relacije dostiživosti. Sistem **S4** dobiva se dodavanjem sistemu **T** aksiom $\Box A \to \Box\Box A$. Lako je vidjeti da je formula $\Box A \to \Box\Box A$ ekvivalentna formuli $\Diamond\Diamond A \to \Diamond A$ koja po prethodnoj propoziciji određuje tranzitivnost relacije dostiživosti. Sistem **S5** koji je od izrazite važnosti dobiva se dodavanjem sistemu **T** aksiom $\Diamond A \to \Box\Diamond A$.

1.4 Logika prvog reda

Za razumijevanje algoritama koji će se javljati u ovom radu, uz modalnu logiku nužno je i poznavanje logike prvog reda. Sada ćemo ukratko, u svrhu ponavljanja, iznijeti najbitnije definicije logike prvog reda koje će nam biti bitne u daljnjim razmatranjima. Dodatno razjašnjenje svih navedenih definicija i rezultata može se pronaći u knjizi [8]. Počinjemo s definicijom alfabeta proizvoljne teorije prvog reda.

Definicija 1.4.1. ***Alfabet*** *neke teorije prvog reda je unija prebrojivog skupa individualnih varijabli* $\{x_0, x_1, \ldots\}$*, skupa logičkih simbola* $\{\neg, \wedge, \vee, \to, \leftrightarrow, \forall, \exists\}$*, skupa relacijskih simbola* $\{R_k^{n_k} : k \in I\}$ *, skupa funkcijskih simbola* $\{f_k^{m_k} : k \in J\}$ *, skupa konstantskih simbola* $\{c_k : k \in K\}$ *, te skupa pomoćnih simbola* { ( ) , }*. Skupovi indeksa* I, J *i* K *su neki podskupovi skupa* $\mathbb{N}$ *a prirodne brojeve* n_k *i* m_k *nazivamo mjesnosti. Dodatno pretpostavljamo da skup relacijskih simbola sadrži barem jedan dvomjesni relacijski simbol kojeg ćemo označavati sa* $=$*.*
Uniju skupova relacijskih, funkcijskih i konstantskih simbola zovemo ***skup nelogičkih simbola*** *ili* ***signatura****, te je označavamo sa* σ*.*

Primijetimo da su za različite teorije prvog reda signature upravo ono po čemu se razlikuju pripadni alfabeti. Sada ćemo definirati alfabet jedne istaknute teorije prvog reda: logike prvog reda.

Definicija 1.4.2. *Signatura logike prvog reda je unija prebrojivo mnogo relacijskih simbola, prebrojivo mnogo funkcijskih simbola i prebrojivo mnogo konstantskih simbola. Što-*

više, smatramo da za svaki $k \in \mathbb{N}$ postoji prebrojivo mnogo relacijskih i funkcijskih simbola mjesnosti k.

U nastavku ove točke sa σ označavamo proizvoljan, ali fiksiran, skup nelogičkih simbola. Nastavljamo s definicijom terma i formule.

Definicija 1.4.3. ***Term*** *je riječ definirana sljedećom rekurzivnom definicijom:*

1. *svaka individualna varijabla i svaki konstantski simbol koji pripada σ su termi*
2. *ako je f neki n-mjesni funkcijski simbol iz σ i $t_1, \ldots, t_n$ σ-termi, tada je riječ $f(t_1, \ldots, t_n)$ term*
3. *riječ je σ-term ako i samo ako je nastala pomoću konačno mnogo primjena pravila 1. i 2.*

Definicija 1.4.4. *Ako je R neki n-mjesni relacijski simbol iz σ, te su $t_1, \ldots, t_n$ termi, tada riječ $R(t_1, \ldots, t_n)$ nazivamo* ***atomarna formula****.*
Formula *je riječ definirana sljedećom rekurzivnom definicijom:*

1. *svaka atomarna formula je formula*
2. *ako su A i B formule tada su riječi $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ i $(A \leftrightarrow B)$ također formule*
3. *ako je A formula, a x varijabla, tada su riječi $(\forall x\, A)$ i $(\exists x\, A)$ također formule*
4. *rječ je formula ako i samo ako je nastala pomoću konačno mnogo primjena pravila 1. , 2. i 3.*

Dakle, iz definicija slijedi da su $\forall x \forall y\ R(x, y)$ i $\forall x \forall y \exists z\ f(x, y) = z$ formule logike prvog reda dok $\triangle x \to P$ i $\forall x\ f(\Diamond x)$ nisu formule logike prvog reda. Dalje iznosimo još tri defincije vezane za sintaksu logike prvog reda koje su nam također važne u daljnjim razmatranjima.

Definicija 1.4.5. *Atomarnu formulu i njezinu negaciju nazivamo* ***literal****.Neka su $A_1, \ldots, A_n$ proizvoljne formule prvog reda. Tada formulu oblika $A_1 \wedge \cdots \wedge A_n$ nazivamo* ***konjunkcija*** *a formulu oblika $A_1 \vee \cdots \vee A_n$ nazivamo* ***disjunkcija****.* ***Elementarna konjunkcija*** *je konjunkcija literala a* ***elementarna disjunkcija*** *je disjunkcija literala.* ***Konjunktivna normalna forma*** *je konjunkcija elementarnih disjunkcija.*

Dakle $f(x_1) = x_2 \vee \neg R(x_1, x_2)$ je jedan primjer formule logike prvog reda koja je elementarna disjunkcija, dok je $((R(f(x_1)) \vee \neg P(f(x_2))) \wedge (\neg R(x_1) \vee \neg P(x_2)))$ formula logike prvog reda koja je u konjunktivnoj normalnoj formi.

Definicija 1.4.6. *Za formulu $Q_1x_1 \dots Q_mx_m\ A$ kažemo da je u **preneksnoj normalnoj formi** ako je A otvorena formula (ne sadrži kvantifikatore), a $Q_i \in \{\forall, \exists\}$, za $i = 1, \dots, m$. Po definiciji smatramo da je svaka otvorena formula u preneksnoj normalnoj formi.*

Kasnije, u razmatranju Szalasovog algoritma, od bitnog značaja biti će nam upravo formule koje su u konjunktivnoj normalnoj formi i u preneksnoj normalnoj formi.

Definicija 1.4.7. *U svakoj atomarnoj formuli svaki nastup varijable je **slobodan**. U formulama oblika $\forall x\ A$ i $\exists x\ A$ svaki nastup varijable x je **vezan**. Ako varijabla x ima slobodan (vezan) nastup u formuli A tada je taj nastup varijable x slobodan (vezan) i u formulama $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$, $(\forall y\ A)$ i $(\exists y\ A)$, gdje je B proizvoljna formula i y varijabla različita od x.*

Sada kada smo definirali sintaksu jezika logike prvog reda, idemo definirati semantiku. Vidjet ćemo kako će pojam istinitosti formule ponovno biti složeniji nego kod logike sudova.

Definicija 1.4.8. *σ**-struktura**, odnosno kratko **struktura**, je uređeni par $\mathfrak{M} = (M, \varphi)$, gdje je M neprazni skup koji nazivamo **nosač**, a φ je preslikavanje sa skupa nelogičkih simbola σ koje ima sljedeća svojstva:*

1. *svakom relacijskom simbolu $R_k^{n_k}$ iz σ pridružuje se n_k-mjesna relacija $\varphi(R_k^{n_k})$ na M*
2. *svakom funkcijskom simbolu $f_k^{m_k}$ iz σ pridružuje se n_k-mjesna funkcija $\varphi(f_k^{m_k})$ sa M^{m_k} u M*
3. *svakom konstantskom simbolu c_k iz σ pridružuje se neki element $\varphi(c_k)$ iz M.*

*Za danu strukturu $\mathfrak{M}$, svaku funkciju sa skupa individualnih varijabli u nosač strukture nazivamo **valuacija.***

Lagano se dokazuje da se na danoj strukturi $\mathfrak{M}$ svaka valuacija v može jedinstveno proširiti tako da je proširenje definirano na skupu svih terma koje određuje dani skup nelogičkih simbola σ.

Definicija 1.4.9. *Svaki uređeni par neke σ-strukture $\mathfrak{M}$ i proizvoljne valuacije v na M nazivamo σ**-interpretacija**, ili kratko **interpretacija**.*

Primijetimo da je zadavanjem interpretacije određena "vrijednost" svakog simbola u proizvoljnoj formuli. Zadavanjem strukture $\mathfrak{M}$ po definificiji (1.4.8) slijedi da smo za svaki relacijski, funkcijski i konstantski simbol zadali redom relaciju, funkciju i konstantu u M. Zadavanjem valuacije, zadali smo svakoj individualnoj varijabli "vrijednost" iz nosača.

U nastavku ćemo umjesto $\varphi(R), \varphi(f)$ i $\varphi(c)$ redom koristiti oznake $R^{\mathfrak{M}}, f^{\mathfrak{M}}$ i $c^{\mathfrak{M}}$. Dalje, ako je $\mathfrak{M}$ struktura, v valuacija na $\mathfrak{M}$ i t term, tada ćemo umjesto $v(t)$ pisati $t^{\mathfrak{M}}[v]$.

Za danu valuaciju v i varijablu x sa v_x označavamo svaku valuaciju koja se podudara sa v na svim varijablama osim možda na varijabli x. Sada možemo definirati istinitost formule u odnosu na interpretaciju.

Definicija 1.4.10. *Neka je $(\mathfrak{M}, v)$ neka σ-interpretacija.* ***Istinitost σ-formule*** *F za danu interpretaciju, u oznaci $\mathfrak{M} \models_v F$, definiramo rekurzivno po složenosti formule F ovako:*

1. *ako je F atomarna formula, tj. F je oblika $R(t_1, \ldots, t_n)$, tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako $(t_1^{\mathfrak{M}}[v], \ldots, t_n^{\mathfrak{M}}[v]) \in R^{\mathfrak{M}}$

2. *ako je F formula oblika $\neg G$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako ne vrijedi $\mathfrak{M} \models_v G$

3. *ako je F formula oblika $A \wedge B$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_v A$ i $\mathfrak{M} \models_v B$

4. *ako je F formula oblika $A \vee B$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_v A$ ili $\mathfrak{M} \models_v B$

5. *ako je F formula oblika $A \rightarrow B$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako ne vrijedi $\mathfrak{M} \models_v A$ ili vrijedi $\mathfrak{M} \models_v B$

6. *ako je F formula oblika $A \leftrightarrow B$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako vrijedi da je $\mathfrak{M} \models_v A$ ekvivalentno sa $\mathfrak{M} \models_v B$

7. *ako je F formula oblika $\forall x\, G$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_{v_x} G$ za sve valuacije v_x

8. *ako je F formula oblika $\exists x\, G$ tada definiramo :*
   $\mathfrak{M} \models_v F$ ako i samo ako $\mathfrak{M} \models_{v_x} G$ za neku valuaciju v_x

Sada kada imamo definiranu istinitost formule, možemo definirati ispunjivost i oborivost formule.

Definicija 1.4.11. *Kažemo da je formula F* ***ispunjiva*** *(****oboriva****) ako postoji interpretacija $(\mathfrak{M}, v)$ tako da vrijedi $\mathfrak{M} \models_v F$ ($\mathfrak{M} \not\models_v F$).*
Kažemo da je struktura $\mathfrak{M}$ ***model*** *za formulu F ako je $\mathfrak{M}$ struktura za F i ako vrijedi $\mathfrak{M} \models_v F$ za sve valuacije v. Tu činjenicu označavamo sa $\mathfrak{M} \models F$.*
Kažemo da je formula ***valjana*** *ako je istinita za svaku interpretaciju.*

Neka je Γ skup formula, te $\mathfrak{M}$ struktura za Γ. Sa $\mathfrak{M} \models \Gamma$ kratko označavamo da za sve $F \in \Gamma$ vrijedi $\mathfrak{M} \models F$. Sada možemo definirati relaciju logičke poslijedice za logiku prvog reda.

Definicija 1.4.12. *Neka je F neka σ-formula i Γ skup σ-formula. Kažemo da formula F **logički slijedi** iz skupa formula Γ ako za svaku σ-strukturu $\mathfrak{M}$ vrijedi: $\mathfrak{M} \models \Gamma$ povlači $\mathfrak{M} \models F$. To kratko označavamo sa $\Gamma \models F$. Relaciju $\models$ nazivamo **relacija logičke poslijedice**. Ako je skup Γ jednočlan, tj. $\Gamma = \{A\}$, tada umjesto $\{A\} \models B$ pišemo $A \Rightarrow B$.*
*Kažemo da su σ-formule F i G **logički ekvivalentne** ako vrijedi $F \Rightarrow G$ i $G \Rightarrow F$. Tu činjenicu označavamo sa $F \Leftrightarrow G$.*

U daljnjim razmatranjima, uz logiku prvog reda, biti će nam bitna i logika drugog reda. Dok su u logici prvog reda sve varijable individualne, u logici drugog reda za svaki prirodni broj n postoje varijable koje mogu poprimiti vrijednosti proizvoljne n-mjesne relacije i postoje varijable koje mogu poprimiti vrijednosti proizvoljne n-mjesne funkcije. Formula logike drugog reda definira se analogno kao i formula logike prvog reda uz dodatnu mogućnost kvantifikacije po relacijskim i funkcijskim varijablama. Važno je primijetiti da nema razlike u alfabetu logike prvog i drugog reda. Tako formula $P(x) \to R(y) \vee R(f(y))$ može biti formula logike prvog ali i drugog reda, dok je $\forall P \exists R, f \forall x \exists y\ (P(x) \to R(y) \vee R(f(y)))$ formula logike drugog reda jer su P i R relacijske varijable a f funkcijska varijabla po kojima se kvantificira. Struktura se u logici drugog reda definira analogno kao i u logici prvog reda, dok se definicija valuacije u logici drugog reda proširuje tako da je domena valuacije unija individualnih, relacijskih i funkcijskih varijabli, te valuacija dodjeljuje individualnim varijablama vrijednosti iz nosača, relacijskim varijablama dodjeljuje relacije nad nosačem a funkcijskim varijablama dodjeljuje funkcije s nosača u nosač. Interpretacija se u logici drugog reda definira analogno kao uređeni par strukture i valuacije, te su definicije istinitosti i ispunjivosti formule te logičke ekvivalencije formula također analogne definicijama za logiku prvog reda uz poštivanje proširenja definicije valuacije. Vidimo da je logika drugog reda proširenje logike prvog reda što joj daje izuzetnu ekspresivnost no istovremeno oduzima neka dobra svojstva. Prije kraja ovog poglavlja uvodimo još jedan pojam koji će nam kasnije biti od važnosti.

Definicija 1.4.13. *Neka je F formula logike prvog reda koja ne sadrži kvantifikatore. Za prirodni broj $n \geq 0$ formulu $\exists x_1, \dots \exists x_n \forall y_1, \dots \forall y_n F$ nazivamo **Skolemova normalna forma**.*

Nije teško dokazati da za svaku formulu logike prvog reda F postoji Skolemova normalna forma F' tako da vrijedi: F je ispunjiva ako i samo ako je F' ispunjiva. Tada kažemo da je F' Skolemova normalna forma za formulu F. Dalje, neka je F formula logike prvog reda. Proces nalaženja Skolemove normalne forme za formulu F nazivamo **skolemizacija**.

Skolemizaciju formule logike prvog reda F provodimo tako da prvo pronađemo preneksnu normalnu formu za formulu F a zatim zamijenimo svaku egzistencijalno kvantificiranu individualnu varijablu y termom $f(x_1, \ldots, x_n)$ gdje su $x_1, \ldots, x_n$ univerzalno kvantificirane individualne varijable koje su u preneksnoj normalnoj formi kvantificirane prije individualne varijable y, a f je novi funkcijski simbol koji se ne javlja u polaznoj formuli. Funkcijski simbol f uveden Skolemizacijom nazivamo **Skolemova funkcija**. Ukoliko je Skolemova funkcija mjesnosti 0 tada je nazivamo **Skolemova konstanta** te je sukladno tome obično označavamo sa c.

Primjer 1.4.14. *Skolemova normalna forma za formulu logike prvog reda* $\forall x \exists y \forall z\, P(x, y, z)$ *je formula* $\forall x \forall z\, P(x, f(x), z)$. *Također, Skolemova normalna forma za formulu* $\forall z \exists u \forall x \exists y$ $(Q(z, u) \to Q(x, y))$ *je formula* $\forall z \forall x (Q(z, f(z)) \to Q(x, g(z, x)))$.

Pokažimo ispravnost skolemizacije na primjeru formule:
$F \equiv \forall x_1, \ldots \forall x_n \exists y\, R(x_1, \ldots, x_n, y)$, gdje je R neki $n + 1$-mjesni relacijski simbol. Po definiciji ispunjivosti formule logike prvog reda, prethodna formula je ispunjiva ako postoji interpretacija $(\mathfrak{M}, v)$ za koju je formula F istinita. Odnosno ako za svaku moguću vrijednost iz nosača pridruženu varijablama $x_1, \ldots, x_n$ postoji vrijednost iz nosača pridružena varijabli y tako da $({x_1}^{\mathfrak{M}}, \ldots {x_n}^{\mathfrak{M}}, y^{\mathfrak{M}}) \in R^{\mathfrak{M}}$. Tada postoji funkcija f takva da $y^{\mathfrak{M}} = f({x_1}^{\mathfrak{M}}, \ldots {x_n}^{\mathfrak{M}})$. Stoga je formula $F' \equiv \forall x_1, \ldots \forall x_n\, R(x_1, \ldots, x_n, f(x_1, \ldots, x_n))$ ispunjiva u strukturi $\mathfrak{M}'$ koja je dobivena kao proširenje strukture $\mathfrak{M}$ tako da smo interpretirali funkcijski simbol f prethodno opisanom funkcijom. Time smo pokazali da ukoliko je F ispunjiva u strukturi $\mathfrak{M}$, tada je F' ispunjiva u proširenju strukture $\mathfrak{M}'$. Obratno, ako je F' ispunjiva tada postoji interpretacija $(\mathfrak{M}', v)$ za koju je formula F' istinita. Tada postoji funkcija $f^{\mathfrak{M}'}$ takva da za svaku vrijednost individualnih varijabli $x_1, \ldots, x_n$ vrijedi $({x_1}^{\mathfrak{M}'}, \ldots, {x_n}^{\mathfrak{M}'}, f^{\mathfrak{M}'}({x_1}^{\mathfrak{M}'}, \ldots, {x_n}^{\mathfrak{M}'})) \in R^{\mathfrak{M}'}$. Tada je formula F ispunjiva za istu interpretaciju kako je $y^{\mathfrak{M}'} = f^{\mathfrak{M}'}({x_1}^{\mathfrak{M}'}, \ldots {x_n}^{\mathfrak{M}'})$. U logici drugog reda opisanu tvrdnju možemo iskazati slijedećom formulom:

$$\forall x_1, \ldots \forall x_n \exists y R(x_1, \ldots, x_n, y) \leftrightarrow \exists f \forall x_1, \ldots \forall x_n R(x_1, \ldots, x_n, f(x_1, \ldots, x_n)).$$

Dakle, na nivou logike drugog reda, formule F i Skolemova normalna forma za F su logički ekvivalentne.

Poglavlje 2

Korespondencija

2.1 Standardna translacija

Sada se počinjemo baviti temom korespondencije. Ključno pitanje koje nam je od interesa je možemo li na neki način "preslikati" formule osnovnog modalnog jezika u jezik neke teorije prvog reda? Jedan od razloga zašto nam je tako nešto od interesa je taj što je modalna logika ekspresivnija od logike prvog reda, no u logici prvog reda postoje jako optimizirani i efikasni algoritmi za provjeru je li dana formula ispunjiva (vidi [2]). Kada bi imali efikasan algoritam koji bi za danu formulu osnovnog modalnog jezika odredio formulu neke teorije prvog reda i to tako da su pritom sačuvana neka određena svojstva ulazne formule, kao primjerice ispunjivost ili valjanost, tada bi mogli iskorištavati prednosti obje logike.

Prije nego krenemo dalje, moramo prvo vidjeti u koji jezik teorije prvog reda moramo preslikavati formule osnovnog modalnog jezika. Očito je glavno pitanje kako "tumačiti" modalni operator $\Diamond$ i propozicionalne varijable.

Definicija 2.1.1. *Za osnovni modalni jezik s prebrojivim skupom propozicionalnih varijabli $\Phi = \{P_0, P_1, P_2, \dots\}$ definiramo* ***jezik korespondencije (na modelima) prvog reda*** *(s jednakošću) $\mathcal{L}^1(\Phi)$ s jednim binarnim relacijskim simbolom R pridruženim modalnom operatoru $\Diamond$ i unarnim relacijskim simbolima $P_0, P_1, P_2, \dots$ pridruženim istoimenim propozicionalnim varijablama.*

Dakle $R(x, y) \land P_0(y)$, $P_1(x) \land P_2(x) \lor R(x, y)$ i $\forall x \forall y\ (P_0(x) \to P_1(y) \lor R(x, y))$ su primjeri formula jezika korespondencije prvog reda. Model osnovnog modalnog jezika $\mathfrak{M} = (W, R, \Vdash)$ sada na prirodan način možemo promatrati i kao strukturu jezika korespondencije prvog reda. Naime, W možemo gledati i kao nosač, a R isto tako kao relaciju pridruženu istoimenom relacijskom simbolu. Što se tiče relacije forsiranja $\Vdash$, za svaku propozicionalnu varijablu P osnovnog modalnog jezika gledamo skup svjetova u kojima se forsira P kao unarnu relaciju pridruženu odgovarajućem unarnom relacijskom simbolu P jezika korespondencije prvog reda.

Sada kada smo definirali jezik korespondencije možemo se pozabaviti pitanjem kako preslikati formule osnovnog modalnog jezika u jezik korespondencije prvog reda.

Definicija 2.1.2. *Neka je x varijabla u jeziku $\mathcal{L}^1(\Phi)$, te neka su A i B formule osnovnog modalnog jezika. Rekurzivno definiramo* ***standardnu translaciju*** *ST_x kao preslikavanje koje formule osnovnog modalnog jezika preslikava u formule jezika korespondencije prvog reda:*

1. $ST_x(P) := P(x)$
2. $ST_x(\bot) := x \neq x$
3. $ST_x(\neg A) := \neg ST_x(A)$
4. $ST_x(A \wedge B) := ST_x(A) \wedge ST_x(B)$
5. $ST_x(A \vee B) := ST_x(A) \vee ST_x(B)$
6. $ST_x(A \rightarrow B) := ST_x(A) \rightarrow ST_x(B)$
7. $ST_x(A \leftrightarrow B) := ST_x(A) \leftrightarrow ST_x(B)$
8. $ST_x(\Diamond A) := \exists y\ (R(x,y) \wedge ST_y(A))$*, gdje je y nova varijabla, tj. različita od svih koje smo u prijevodu formule koristili prije primjene (8).*

U definiciji standardne translacije ne definira se njezino djelovanje na formule oblika $\Box A$, no iz dualnosti modalnih operatora nužnosti i mogućnosti, lako možemo dobiti to djelovanje:

$$ST_x(\Box A) = ST_x(\neg\Diamond\neg A) = \neg ST_x(\Diamond\neg A) =^{(8)} \neg\exists y\ (R(x,y) \wedge ST_y(\neg A)) =$$
$$= \neg\exists y\ (R(x,y) \wedge \neg ST_y(A)) = \forall y\ (\neg R(x,y) \vee ST_y(A)) = \forall y\ (R(x,y) \rightarrow ST_y(A)).$$

Dakle, za propozicionalnu varijablu P osnovnog modalnog jezika standardna translacija od $\Box P$ je: $ST_x(\Box P) = \forall y\ (R(x,y) \rightarrow P(y))$. Standardna translacija svake modalne formule sadrži točno jednu slobodnu varijablu, i to x.

Idemo sada promotriti semantiku standardne translacije. Neka je A formula osnovnog modalnog jezika. Zanima nas u kakvom su odnosu istinitosti formula A i formula jezika korespondencije prvog reda $ST_x(A)$. Sjetimo se kako smo istinitost formule osnovnog modalnog jezika u svijetu w definirali preko relacije forsiranja (1.2.1). Dakle, istinitost modalne formule u svijetu w ovisi direktno o tome je li dana formula forsirana na svijetu

w. Ako model osnovnog modalnog jezika tumačimo kao strukturu jezika korespondencije prvog reda, tada vidimo da će slobodna varijabla koja se nalazi u standardnoj translaciji upravo reprezentirati svijet u kojem promatramo istinitost, odnosno forsiranje, modalnih formula.

Neka je sada $\mathfrak{M}$ model za osnovni modalni jezik, te neka je w svijet iz tog modela, a A formula osnovnog modalnog jezika. Izraz $\mathfrak{M} \models ST_x(A)[w]$ sada nam označava da je formula prvog reda $ST_x(A)$ istinita u modelu $\mathfrak{M}$, kojeg sada promatramo kao strukturu jezika korespondencije, uz valuaciju koja slobodnoj varijabli x pridružuje w. Iz prethodnog razmatranja sada prirodno slijedi slijedeće propozicija.

Propozicija 2.1.3. *Neka je A formula osnovnog modalnog jezika. Tada vrijedi:*

1. *za svaki model $\mathfrak{M}$ i svijet w vrijedi: $\mathfrak{M}, w \Vdash A$ ako i samo ako $\mathfrak{M} \models ST_x(A)[w]$*

2. *za svaki model $\mathfrak{M}$ vrijedi: $\mathfrak{M} \models A$ ako i samo ako $\mathfrak{M} \models \forall x ST_x(A)$*

Dokaz. Dokažimo prvu tvrdnju indukcijom po složenosti formule osnovnog modalnog jezika. Složenost formule osnovnog modalnog jezika A definiramo kao ukupan broj pojavljivanja znakova $\neg$, $\vee$ i $\Diamond$ i označavamo s $k(A)$. Iako smo u definiciji (1.1.1) osnovnog modalnog jezika rekli da se abeceda sastoji i od bulovskih veznika $\wedge$, $\rightarrow$ i $\leftrightarrow$, radi sažetijeg dokaza, pretpostavljamo da su ti veznici samo pokrate. Naime, postoji više ekvivalentnih definicija sintakse osnovnog modalnog jezika, te uvođenje veznika $\wedge$, $\rightarrow$ i $\leftrightarrow$ u definiciju nije nužno jer se oni mogu zapisati samo korištenjem veznika $\neg$ i $\vee$. Tako na primjer formulu $A \wedge B$ možemo zapisati kao ekvivalentnu formulu $\neg(\neg A \vee \neg B)$.

Baza: neka je $k(A) = 0$. Tada je A neka propozicionalna varijabla P ili logička konstanta $\perp$. U prvom slučaju, iz $\mathfrak{M}, w \Vdash P$ slijedi da je w element skupa $\{v \in W \mid \mathfrak{M}, v \Vdash P\}$. Kako je $ST_x(P) = P(x)$, što je u kontekstu jezika $\mathcal{L}^1(\Phi)$ upravo prethodno iskazani skup, tada je formula $ST_x(P)$ istinita za sve valuacije koje pridružuju slobodnoj varijabli x vrijednost w iz nosača, tj. slijedi $\mathfrak{M} \models ST_x(A)[w]$. U drugom smjeru, iz $\mathfrak{M} \models ST_x(P)[w]$ slijedi da je w element $\{v \in W \mid \mathfrak{M}, v \Vdash P\}$, tada posebno vrijedi $\mathfrak{M}, w \Vdash P$.

U drugom slučaju, $\perp$ nije nikad istina u modalnoj logici, a njen prijevod $x \neq x$ isto tako nikad nije istinit u logici prvog reda, pa tvrdnja slijedi trivijalno.

Pretpostavka: neka tvrdnja vrijedi za sve formule osnovnog modalnog jezika složenosti manje ili jednake n.

Korak: neka je $k(A) = n + 1$. Tada je A jednaka $(\neg B)$, $(B \vee C)$ ili $(\Diamond B)$, pri čemu su formule B i C složenosti manje ili jednake od n. Pogledajmo prvo slučaj $A = \Diamond B$. Iz definicije (1.2.1) slijedi $\mathfrak{M}, w \Vdash \Diamond B$ ako i samo ako postoji svijet v iz domene W takav da je wRv i $\mathfrak{M}, v \Vdash B$. S druge strane iz definicije (2.1.2) $\mathfrak{M} \models ST_x(\Diamond B)[w]$ ako i samo ako postoji svijet v iz domene W takav da je wRv i $\mathfrak{M} \models ST_x(B)[v]$. Kako je formula B složenosti manje ili jednake od n tada po pretpostavci indukcije slijedi $\mathfrak{M}, v \Vdash B$ ako i samo ako $\mathfrak{M} \models ST_x(B)[v]$, čime je prvi slučaj dokazan.

Pogledajmo sada slučaj $A = B \vee C$. Ponovno iz definicije (1.2.1) slijedi $\mathfrak{M}, w \Vdash B \vee C$ ako i samo ako $\mathfrak{M}, w \Vdash B$ ili $\mathfrak{M}, w \Vdash C$. Kako su i B i C formule osnovnog modalnog jezika složenosti manje ili jednake od n, tada po pretpostavci indukcije slijedi:

$$\mathfrak{M}, w \Vdash B \text{ ako i samo ako } \mathfrak{M} \models ST_x(B)[w] \text{ i}$$

$$\mathfrak{M}, w \Vdash C \text{ ako i samo ako } \mathfrak{M} \models ST_x(C)[w].$$

Dakle, $\mathfrak{M}, w \Vdash B$ ili $\mathfrak{M}, w \Vdash C$ ako i samo ako $\mathfrak{M} \models ST_x(B)[w]$ ili $\mathfrak{M} \models ST_x(C)[w]$, što je ekvivalentno sa $\mathfrak{M} \models ST_x(B)[w] \vee ST_x(C)[w]$, što je po definiciji (2.1.2) upravo $\mathfrak{M} \models ST_x(B \vee C)[w]$.

Pogledajmo još zadnji slučaj kada imamo $A = \neg B$. Iz definicije (1.2.1) slijedi $\mathfrak{M}, w \Vdash \neg B$ ako i samo ako $\mathfrak{M}, w \nVdash B$. Kako je složenost formule B manja ili jednaka od n tada iz pretpostavke indukcije slijedi $\mathfrak{M}, w \nVdash B$ ako i samo ako $\mathfrak{M} \not\models ST_x(B)[w]$. S druge strane, iz definicije (2.1.2) slijedi $\mathfrak{M} \models ST_x(\neg B)[w]$ ako i samo ako $\mathfrak{M} \models \neg ST_x(B)[w]$. Kako formula prvog reda $ST_x(B)[w]$ nema slobodnih varijabli osim varijable x kojoj valuacija pridružuje vrijednost w, tada $\mathfrak{M} \models \neg ST_x(B)[w]$ ako i samo ako $\mathfrak{M} \not\models ST_x(B)[w]$, čime je zadnji slučaj, a time i prva tvrdnja, dokazana.

Dokažimo sada drugu tvrdnju. Po definiciji (1.2.3), $\mathfrak{M} \models A$ ako i samo ako $\mathfrak{M}, w \Vdash A$ za svaki svijet w iz domene W. Po upravo dokazanoj prvoj tvrdnji propozicije imamo: $\mathfrak{M}, w \Vdash A$ ako i samo ako $\mathfrak{M} \models ST_x(A)[w]$ za svaki w iz W, što u logici prvog reda vrijedi ako i samo ako $\mathfrak{M} \models \forall x\, ST_x(A)$. □

Primijetimo da u iskazu prethodne propozicije nismo označavali za koju valuaciju je formula prvog reda $ST_x(A)[w]$ istinita. Razlog tome je, kao što smo prethodno komentirali, da standardna translacija modalne formule ima samo jednu slobodnu varijablu. Stoga, gornja tvrdnja vrijedi za svaku valuaciju koja slobodnoj varijabli u standardnoj translaciji pridružuje vrijednost w iz nosača.

No ako se želimo udaljiti od konkretnog svijeta prilikom utvrđivanja istinitosti, tada moramo promatrati korespondenciju na okvirima. Kako je formula osnovnog modalnog jezika istinita na okviru $\mathcal{F}$ ako je istinita na svakom modelu tog okvira, tada istinitost formule na okviru ne ovisi o relaciji forsiranja. Tada, iz istog razloga, u translaciji prvog reda formule koja je istinita na okviru ne želimo imati unarne relacijske simbole koji odgovaraju skupovima svjetova u kojima se istoimena propozicionalna varijabla forsira, kao što smo htjeli kod korespondencije na modelima. Prisustvo unarnih relacija u jeziku korespondencije na okvirima značilo bi da istinitost translatirane formule ovisi o tome u kojim svjetovima se forsira koja propozicionalna varijabla, što dovodi do ovisnosti između istinitosti formule i relacije forsiranja.

Definicija 2.1.4. *Za osnovni modalni jezik definiramo* ***jezik korespondencije (na okvirima) prvog reda*** *(s jednakošću)* $\mathcal{L}^1$ *kao jezik prvog reda s dvočlanim skupom binarnih relacijskih simbola* $\{R, =\}$ *te praznim skupovima funkcijskih simbola i konstantskih simbola.*

Okvir $\mathcal{F} = (W, R)$ osnovnog modalnog jezika sada možemo promatrati kao strukturu jezika $\mathcal{L}^1$, no radi izbjegavanja zabune, također ćemo govoriti da je $\mathcal{F}$ okvir za $\mathcal{L}^1$. Neka je P zadana propozicionalna varijabla osnovnog modalnog jezika. Iz definicije (1.2.3) slijedi da je formula P istinita na okviru $\mathcal{F} = (W, R)$ ako i samo ako je istinita za svaku relaciju forsiranja. Relacija forsiranja pridružuje formule svjetovima, ali isto tako njeno djelovanje možemo gledati na način da svakoj formuli pridružuje skup svjetova (podskup domene W) u kojima je ta formula istinita. Tada se istinitost za svaku relaciju forsiranja prirodno prikazuje kao kvantifikacija drugog reda.

Dok logika prvog reda dopušta kvantifikaciju samo po individualnim ili objektnim varijablama, logika drugog reda kvantificira i po relacijskim i funkcijskim simbolima. To čini logiku drugog reda izuzetno izražajnom ali ona istovremeno gubi neka dobra svojstva. Tako ako želimo iskazati princip bivalencije u terminima logike prvog reda, moramo se koristiti shemom $\forall x(x \in P \vee x \notin P)$. Ono što time želimo iskazati jest da za svaki skup P vrijedi da za svaki x, ili je x u P ili x nije u P. No primijetimo da nam je za taj iskaz potrebno onoliko formula logike prvog reda koliko je i skupova. S druge strane, dovoljna nam je jedna jedina rečenica logike drugog reda da u potpunosti iskažemo princip bivalencije: $\forall P \forall x(x \in P \vee x \notin P)$.

Ovdje je izraz $\forall P$ kvantifikator drugog reda, a P varijabla kojoj se u interpretaciji pridružuju skupovi. Kvantifikator drugog reda uvijek ćemo koristiti samo nad unarnim relacijama. Takve se formule drugog reda zovu **monadske formule**. Također, koristit ćemo samo univerzalni kvantifikator drugog reda i to uvijek samo na početku formule. Takve se formule zovu **univerzalne formule** drugog reda.

Iz prethodnog razmatranja vidimo da nam se u proučavanju jezika korespondencije prirodno nameću i jezici drugog reda. Iz svega navedenog dolazimo do slijedeće definicije.

Definicija 2.1.5. *Za osnovni modalni jezik s prebrojivim skupom propozicionalnih varijabli* $\Phi = \{P_0, P_1, P_2, \dots\}$ *definiramo* ***jezik korespondencije drugog reda*** $\mathcal{L}^2$ *kao monadski jezik drugog reda dobiven tako da jeziku* $\mathcal{L}^1$ *dodamo po jednu monadsku relacijsku varijablu za svaku propozicionalnu varijablu iz skupa* Φ*.*

Monadske varijable u jeziku $\mathcal{L}^2$ označavat ćemo isto kao i unarne relacijske simbole u jeziku $\mathcal{L}^1(\Phi)$, tj. s $P_0, P_1.P_2, \dots$ Dalje, okvir $\mathcal{F} = (W, R)$ osnovnog modalnog jezika sada možemo promatrati i kao strukturu jezika $\mathcal{L}^2$. Dakle, uz sve što može jezik $\mathcal{L}^1$, jezik $\mathcal{L}^2$ ima i mogućnost kvantifikacije po podskupovima okvira.

Definicija 2.1.6. *Neka je A formula osnovnog modalnog jezika i F klasa okvira. Kažemo da A* ***definira*** *F ako za svaki okvir* $\mathcal{F}$ *vrijedi da je* $\mathcal{F}$ *u F ako i samo ako vrijedi* $\mathcal{F} \Vdash A$*. Slično, za skup* Γ *formula osnovnog modalnog jezika kažemo da definira F ako za svaki okvir* $\mathcal{F}$ *iz F vrijedi da je* $\mathcal{F}$ *u F ako i samo ako je svaka formula iz* Γ *valjana na* $\mathcal{F}$*.*

Kažemo da je klasa okvira ***(modalno) definabilna*** *ako postoji skup formula koji je definira.*

Neka je α *formula jezika korespondencije prvog ili drugog reda (*$\mathcal{L}^1$ *ili* $\mathcal{L}^2$*). Kažemo da* α ***definira*** *klasu okvira F ako za sve okvire* $\mathcal{F}$ *vrijedi da je* $\mathcal{F}$ *iz F ako i samo ako je* α *valjana na* $\mathcal{F}$ *(istinita na* $\mathcal{F}$ *za svaku valuaciju). Analogna je definicija za skup formula jezika korespondencije prvog ili drugog reda.*

Kažemo da su formula A osnovnog modalnog jezika i formula α *jezika korespondencije (*$\mathcal{L}^1$ *ili* $\mathcal{L}^2$*) jedna drugoj* ***korespondenti*** *(na okvirima) ako definiraju istu klasu okvira.*

Neformalno kažemo da formula ili skup formula definira neko svojstvo ako definira klasu okvira s tim svojstvom. Tako ćemo za formulu prvog reda $\forall x\, R(x, x)$ reći da definira refleksivnost zato što ona definira klasu refleksivnih okvira. Kako smo u propoziciji (1.2.4) dokazali da modalna formula $P \to \Diamond P$ isto definira refleksivnost, tada direktno iz prethodne definicije slijedi da su te formule korespondenti na okvirima. Također, formula prvog reda $\forall x \forall y \forall z\, (R(x, y) \land R(y, z) \to R(x, z))$ definira tranzitivnost a formula prvog reda $\forall x \forall y\, (R(x, y) \to R(y, x))$ definira simetričnost, pa ponovno po propoziciji (1.2.4) slijedi da su korespondenti na okviru tih formula redom $\Diamond\Diamond P \to \Diamond P$ i $P \to \Box\Diamond P$.

Za proizvoljnu modalnu formulu A cilj nam je pronaći formulu jezika korespondencije (korespondenta) koja je valjana na istim okvirima kao i A. Kao što smo prethodno razmatrali, ako relaciju forsiranja promatramo kao relaciju koja svakoj formuli dodjeljuje podskup svjetova u kojima je ta formula istinita, tada kvantificiranje po relacijama forsiranja u definiciji valjanosti zapravo znači kvantificiranje po svim podskupovima okvira.

Tako izravno dolazimo do sljedeće propozicije, koja proizvoljnoj modalnoj formuli nalazi korespondenta u jeziku $\mathcal{L}^2$.

Propozicija 2.1.7. *Neka je A formula osnovnog modalnog jezika. Tada za svaki okvir $\mathcal{F}$ i svijet w iz $\mathcal{F}$ vrijedi:*

1. $\mathcal{F}, w \Vdash A$ *ako i samo ako* $\mathcal{F} \models \forall P_1 \dots \forall P_n \, ST_x(A)[w]$
2. $\mathcal{F} \Vdash A$ *ako i samo ako* $\mathcal{F} \models \forall P_1 \dots \forall P_n \forall x \, ST_x(A)$

gdje kvantifikatori drugog reda vežu monadske varijable drugog reda P_i pridružene istoimenim propozicionalnim varijablama koje se pojavljuju u A.

Formulu $\forall P_1 \dots \forall P_n \forall x \, ST_x(A)$ zovemo **prijevod** ili **translacija drugog reda** formule A. Dokaz prethodne propozicije može se naći u [6]. Napomenimo još da simboli $P_1, \dots, P_n$ u translaciji drugog reda označavaju monadske varijable, dok oni u translaciji prvog reda označavaju unarne relacijske simbole.

2.2 Sahlqvistov teorem

Sada kada imamo definirane translacije prvog i drugog reda, postavlja se pitanje koje formule osnovnog modalnog jezika imaju svog korespondenta prvog reda na okvirima. Iz propozicije (2.1.7) slijedi da svaka formula osnovnog modalnog jezika ima svog korespondenta drugog reda na okvirima, no općenito ne vrijedi da svaka formula osnovnog modalnog jezika ima korespondenta prvog reda na okvirima. Sahlqvistov teorem nam daje široku klasu formula osnovnog modalnog jezika koje imaju korespondenta prvog reda na okvirima. U ovom dijelu samo iskazujemo Sahlqvistov teorem jer nam on služi kao motivacija za proučavanje algoritama korespondencije u idućem poglavlju. Dodatni detalji vezani uz ovaj dio rada mogu se pronaći u [6]. Kako bi iskazali Sahlqvistov teorem prvo moramo definirati neke sintaktičke i semantičke pojmove.

Definicija 2.2.1. *Neka je φ formula osnovnog modalnog jezika i $\alpha(x)$ formula jezika korespondencije prvog ili drugog reda (x je jedina slobodna varijabla formule α). Kažemo da su φ i $\alpha(x)$ međusobno* ***lokalni korespondenti*** *ako za svaki okvir $\mathcal{F}$ i za svaki svijet w iz $\mathcal{F}$ vrijedi: $\mathcal{F}, w \Vdash \varphi$ ako i samo ako $\mathcal{F} \models \alpha[w]$.*

Nakon semantičkog pojma lokalnog korespondenta definiramo neke sintaktične pojmove. Iduću definiciju najlakše je formulirati ukoliko promatramo osnovni modalni jezik kao jezik koji sadrži samo veznike $\neg$, $\vee$ i $\Diamond$ kao što smo učinili u dokazu propozicije (2.1.3).

Definicija 2.2.2. *Kažemo da se propozicionalna varijabla P pojavljuje* ***pozitivno*** *u formuli osnovnog modalnog jezika A ako je u dosegu parnog broja negacija, a* ***negativno*** *ako je u dosegu neparnog broja negacija. Za modalnu formulu B kažemo da je* ***pozitivna u*** *P (****negativna u*** *P) ako se P u B pojavljuje samo pozitivno (negativno). Za formulu kažemo da je* ***pozitivna (negativna)*** *ako je pozitivna (negativna) u svakoj varijabli koja se u njoj pojavljuje.*
Dalje, kažemo da se P pojavljuje ***uniformno*** *u B ako se pojavljuje samo pozitivno ili samo negativno, odnosno ako je B pozitivna ili negativna u P. Za formulu kažemo da je* ***uniformna*** *ako se sve propozicionalne varijable koje sadrži pojavljuju uniformno.*

Napomena 2.2.3. *Svi navedeni pojmovi se potpuno analogno definiraju i za jezike korespondencije prvog i drugog reda, s tim da se umjesto o pojavljivanju propozicionalnih varijabli govori o pojavljivanju relacijskih simbola odnosno o pojavljivanju monadskih varijabli drugog reda.*

Dakle, u danoj formuli drugog reda $\forall P, Q, R\ \forall x\ (P(x) \wedge \neg Q(x)) \vee (R(x) \wedge \neg P(x))$ monadska varijabla R se javlja pozitivno, monadska varijabla Q se javlja negativno, dok za monadsku varijablu P kažemo da se ona ne javlja uniformno, odnosno da se javlja i pozitivno i negativno. No, u modalnoj formuli $\neg(P \to Q)$ se propozicionalna varijabla P javlja pozitivno dok se propozicionalna varijabla Q javlja negativno zato jer je prethodna formula ekvivalentna modalnoj formuli $\neg(\neg P \vee Q)$ pa je propozicionalna varijabla P u dosegu parnog broja negacija a propozicionalna varijabla Q je u dosegu neparnog broja negacija. Sada možemo definirati pojam Sahlqvistove formule a potom iskazujemo Sahlqvistov teorem.

Definicija 2.2.4. *Formulu osnovnog modalnog jezika zovemo* ***$\Box$-atom*** *ako je oblika $\Box \dots \Box P$, gdje je P propozicionalna varijabla.*

Sahlqvistova antecedenta *je formula osnovnog modalnog jezika izgrađena od logičkih konstanti, $\Box$-atoma i negativnih formula, uz upotrebu veznika konjunkcije $\wedge$, disjunkcije $\vee$ i modalnog operatora mogućnosti $\Diamond$.*

Sahlqvistova implikacija *je formula oblika $\varphi \to \psi$ takva da je φ Sahlqvistova antecedenta, a ψ pozitivna formula.*

Sahlqvistova formula *je formula sastavljena od Sahlqvistovih implikacija slobodnom primjenom operatora nužnosti $\Box$ i veznika konjunkcije $\wedge$, te primjenom disjunkcije samo među formulama koje nemaju zajedničkih propozicionalnih varijabli.*

Teorem 2.2.5. ***(Sahlqvist)*** *Neka je χ Sahlqvistova formula. Tada χ lokalno korespondira s formulom prvog reda $\alpha_\chi(x)$ koju je moguće efektivno odrediti.*

Dokaz Sahlqvistovog teorema možete vidjeti u [2] i [6]. Primijetimo da nam Sahlqvistov teorem ne daje formulu prvog reda koja korespondira sa χ već govori da takva formula postoji. Dalje, primijetimo da je pojam Sahlqvistove formule čisto sintaktični pojam, dakle ako imamo formulu osnovnog modalnog jezika koja je svojim oblikom Sahlqvistova, tada znamo da ta formula ima izračunljivog korespondenta prog reda. Napomenimo još da je klasa Sahlqvistovih formula jedna široka klasa te se poslije ovakvog rezultata prirodno nameće pitanje kako izračunati korespondenta prvog reda.

Poglavlje 3

Szalasov algoritam

U protekla četiri desetljeća puno pažnje je posvećeno automatskom dokazivanju teorema. Nakon Robinsonovog iznošenja metode rezolucije 1968 godine, veliki fokus u automatskom dokazivanju teorema bio je usmjeren na logiku prvog reda. To je rezultiralo velikim brojem implementacijsko-orijentiranih optimizacija metode rezolucije i otkrivanjem novih tehnika za automatsko dokazivanje. No kako smo vidjeli u uvodu rada, logika prvog reda ima svoje nedostatke te su modalne logike predložene kao alternativa. U pokušaju automatiziranja modalnog zaključivanja postoje dva moguća smjera: dizajniranje cijelog sustava od početka, što iziskuje puno truda i vremena, ili korištenje postojećih dokazivača teorema u logici prvog reda. Kako bi se mogli iskoristiti postojeći dokazivači teorema za logiku prvog reda, potrebno je interpretirati modalne formule kao formule prvog reda. Jedan od načina za to postići je translacijom formula.

No to je samo dio problema. Kada želimo imati automatsko dokazivanje teorema, tada moramo imati definiran aksiomatski sistem unutar kojega će se provoditi dokazivanje. To znači da moramo imati definirane aksiome i pravila izvođenja koja smijemo koristiti u dokazu. Svojstva modalnih operatora obično su zadana shemom aksioma. Tako, na primjer, ako kažemo da modalni operator $\Diamond$ zadovoljava $P \to \Diamond P$, ono što zapravo mislimo pod tim je da za svaku modalnu formulu P vrijedi da P povlači $\Diamond P$. Szalasov algoritam, koji ćemo proučavati u ovom poglavlju, za danu formulu osnovnog modalnog jezika vraća formulu jezika korespondencije prvog reda koja je korespondent na okvirima ulazne formule. Traženje korespondenta prvog reda za shemu aksioma je primjer kada tražimo korespondenta na okvirima. Dakle, Szalasov algoritam je prvotno razvijen u svrhu nalaženja korespondenta prvog reda za modalnu shemu aksioma, no kao što ćemo vidjeti, on je primijenjiv i za općenitiji problem nalaženja korespondenta prvog reda na okvirima za danu formulu osnovnog modalnog jezika.

Pojasnimo još malo "prenošenje" dokazivanja iz modalne logike u logiku prvog reda. Pretpostavimo da nam je dana formula osnovnog modalnog jezika A, te želimo dokazati A u modalnom sistemu u kojemu su aksiomi sve tautologije osnovnog modalnog jezika te $P \to \Diamond P$, $\Diamond\Diamond P \to \Diamond P$ i $P \to \Box\Diamond P$. U prethodnom poglavlju smo pokazali da su korespondenti prvog reda na okvirima prethodnih aksioma redom $\forall x\, R(x,x)$, $\forall x \forall y \forall z\, (R(x,y) \land R(y,z) \to R(x,z))$ i $\forall x \forall y\, (R(x,y) \to R(y,x))$. Tada, umjesto traženja dokaza u modalnom sistemu, možemo translatirati formulu osnovnog modalnog jezika A u formulu logike prvog reda A' te probati dokazati da A' slijedi iz korespondenata danih aksioma.

Sam algoritam koji ćemo promatrati je neovisan o odabiru funkcije translacije jer je ona jedan od ulaznih parametara algoritma. No ipak odabrana translacija mora zadovoljavati da je modalna formula valjana ako i samo ako je translatirana formula valjana. Iz propozicije (2.1.3) i definicija valjanosti modalne formule i formule logike prvog reda, slijedi da je jedan primjer takve translacije funkcija koja formulu A osnovnog modalnog jezika translatira u formulu logike prvog reda $\forall x\, ST_x(A)$.

Uočimo još jednu pojavu. Ako promatramo $\Box P$ kao aksiom zadan modalnom shemom tada, kao i prije, mislimo da za svaku modalnu formulu P vrijedi da je formula $\Box P$ valjana na svakom okviru. Po propoziciji (2.1.7) je tada formula drugog reda $\forall P \forall x\, ST_x(\Box P)$, što je ekvivalentno sa $\forall P \forall x \forall y (R(x,y) \to P(y))$, korespondent u $\mathcal{L}^2$ formule $\Box P$. Kako nam je krajnji cilj pronaći korespondenta u $\mathcal{L}^1$, tada moramo eliminirati monadsku varijablu P iz dobivene formule drugog reda, što je upravo glavni fokus Szalasovog algoritma.

Prije nego nastavimo sa daljnjim razmatranjima Szalasovog algoritma, prvo iznosimo tvrdnju koja nam daje jedno teorijsko ograničenje.

Teorem 3.0.1. ***(L. A. Chagrova)*** *Neodlučivo je ima li proizvoljna modalna formula osnovnog modalnog jezika korespondenta prvog reda na okvirima.*

Prethodni teorem može se pronaći u [2]. Teorem Chagrove nam govori da ne postoji algoritam koji će u konačno mnogo koraka za proizvoljnu formulu osnovnog modalnog jezika dati korespondentna na okvirima, ukoliko on postoji, odnosno javiti neuspjeh ukoliko korespondent ne postoji. Dakle sam problem kojeg Szalasov algoritam pokušava riješiti je neodlučiv, no kao što smo prethodno komentirali znamo da Sahlqvistove formule imaju korespondenta prvog reda. Idemo sada detaljnije razmotriti Szalasovo algoritam.

3.1 Uvod

Iskažimo jednu propoziciju i lemu koje će biti bitne u radu samog algoritma. Sa $A(\sigma := \delta)$ ćemo označavati formulu dobivenu iz formule A zamjenom svakog pojavljivanja izraza σ

sa izrazom δ.

Propozicija 3.1.1. *Neka je Q proizvoljni kvantifikator, te neka su A, B i C formule logike prvog reda takve da se u formuli C varijabla x ne pojavljuje kao slobodna varijabla. Tada vrijede sljedeće tvrdnje:*
(1) $\neg\neg A \Leftrightarrow A$
(2) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
(3) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
(4) $\neg\forall x\, A(x) \Leftrightarrow \exists x\, \neg A(x)$
(5) $\neg\exists x\, A(x) \Leftrightarrow \forall x\, \neg A(x)$
(6) $\exists x\, (A(x) \vee B(x)) \Leftrightarrow \exists x\, A(x) \vee \exists x\, B(x)$
(7) $\forall x\, (A(x) \wedge B(x)) \Leftrightarrow \forall x\, A(x) \wedge \forall x\, B(x)$
(8) $Qx\, (A(x)) \wedge C \Leftrightarrow Qx\, (A(x) \wedge C)$
(9) $C \wedge Qx\, (A(x)) \Leftrightarrow Qx\, (C \wedge A(x))$
(10) $Qx\, (A(x)) \vee C \Leftrightarrow Qx\, (A(x) \vee C)$
(11) $C \vee Qx\, (A(x)) \Leftrightarrow Qx\, (C \vee A(x))$
(12) $QxQy\, A \Leftrightarrow QyQx\, A$
(13) $\forall x\, (x \neq t \vee C(t := x)) \Leftrightarrow C(t)$ *(gdje je t term koji ne sadrži variajblu x)*
(14) $\exists x\, (x = t \wedge C(t := x) \Leftrightarrow C(t)$ *(gdje je t term koji ne sadrži variajblu x)*

Prethodna propozicija sumira dobro poznate tvrdnje matematičke logike čije dokaze možete pronaći u [8]. Prije iznošenja najavljene leme, prvo moramo definirati neke pojmove koji će nam biti bitni u daljnjim razmatranjima.

U uskoj vezi sa sintaktičkim pojmovima pozitivnosti i negativnosti propozicijske (ili monadske) varijable, koje smo definirali u prethodnom poglavlju, su semantički pojmovi monotonog rasta i pada.

Definicija 3.1.2. *Neka je P propozicionalna varijabla. Kažemo da je modalna formula A* ***monotono rastuća*** *u P ako za svaki model $\mathfrak{M} = (W, R, \Vdash)$, svaki svijet w i svaku relaciju forsiranja $\Vdash'$ takvu da je $\{w \in W \mid \mathfrak{M}, w \Vdash P\} \subseteq \{w \in W \mid \mathfrak{M}, w \Vdash' P\}$ i $\{w \in W \mid \mathfrak{M}, w \Vdash Q\} = \{w \in W \mid \mathfrak{M}, w \Vdash' Q\}$ za sve $Q \neq P$, vrijedi : ako $\mathfrak{M}, w \Vdash A$ onda $(W, R, \Vdash'), w \Vdash' A$.*
Analogno, kažemo da je modalna formula A ***monotono padajuća*** *u P ako za svaki model $\mathfrak{M} = (W, R, \Vdash)$, svaki svijet w i svaku relaciju forsiranja $\Vdash'$ takvu da je $\{w \in W \mid \mathfrak{M}, w \Vdash P\} \supseteq \{w \in W \mid \mathfrak{M}, w \Vdash' P\}$ i $\{w \in W \mid \mathfrak{M}, w \Vdash Q\} = \{w \in W \mid \mathfrak{M}, w \Vdash' Q\}$ za sve $Q \neq P$, vrijedi : ako $\mathfrak{M}, w \Vdash A$ onda $(W, R, \Vdash'), w \Vdash' A$.*

Napomena 3.1.3. *Slično se definira rastuća i padajuća monotonost formule logike prvog i drugog reda u relacijskom simbolu P.*

Primjer 3.1.4. *Pokažimo da je modalna formula $P \wedge Q$ monotono rastuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash P \wedge Q$. Tada po definiciji relacije forsiranja* *imamo $\mathfrak{M}, w \Vdash P$ i $\mathfrak{M}, w \Vdash Q$. Neka je sada $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz gornje definicije. Tada iz uvjeta $\{w \in W \mid \mathfrak{M}, w \Vdash P\} \subseteq \{w \in W \mid \mathfrak{M}, w \Vdash' P\}$ slijedi $\mathfrak{M}, w \Vdash' P$, a iz uvjeta $\{w \in W \mid \mathfrak{M}, w \Vdash Q\} = \{w \in W \mid \mathfrak{M}, w \Vdash' Q\}$ slijedi $\mathfrak{M}, w \Vdash' Q$, pa imamo $\mathfrak{M}, w \Vdash' P \wedge Q$. Sada po gornjoj definiciji slijedi da je modalna formula $P \wedge Q$ monotono rastuća u P.*

Sljedeća lema daje vezu sintaktičkih pojmova pozitivnosti i negativnosti sa semantičkim pojmovima monotonog rasta i pada.

Lema 3.1.5. *Neka je A formula osnovnog modalnog jezika ili formula logike prvog ili drugog reda. Tada vrijedi:*

1. *Ako je formula A pozitivna u P, onda je formula A monotono rastuća u P.*
2. *Ako je formula A negativna u P, onda je formula A monotono padajuća u P.*

Dokaz. Provest ćemo dokaz tvrdnje samo za formule osnovnog modalnog jezika jer se sličnom argumentacijom mogu dokazati tvrdnje za formule logike prvog i drugog reda. Obje tvrdnje dokazujemo simultano indukcijom po složenosti modalne formule A. Iz tog razloga, kao i u dokazu propozicije (2.1.3), smatramo da osnovni modalni jezik sadrži samo veznike $\neg$, $\vee$ i $\Diamond$. Bez smanjenja općenitosti možemo pretpostaviti da se propozicionalna varijabla P pojavljuje u formuli A (inače je formula A očito i pozitivna i negativna u propozicionalnoj varijabli P, a isto tako je očito i rastuća i padajuća u P, pa tvrdnje vrijede trivijalno).

Baza: neka je $k(A) = 0$. Tada je formula A neka propozicionalna varijabla P pa je po definiciji formula A pozitivna u P. Pokažimo da je formula A monotono rastuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash P$.Dalje, neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Tada iz uvjeta $\{w \in W \mid \mathfrak{M}, w \Vdash P\} \subseteq \{w \in W \mid \mathfrak{M}, w \Vdash' P\}$ slijedi $\mathfrak{M}, w \Vdash' P$. Time smo dokazali prvu tvrdnju za bazu indukcije dok druga tvrdnja slijedi trivijalno jer se u modalnoj formuli složenosti 0 propozicionalna varijabla P ne može pojaviti negativno.

Pretpostavka: neka obje tvrdnje vrijede za sve formule složenosti manje ili jednake n

Korak: neka je modalna formula A složenosti $n + 1$. Tada je formula A jednaka $(\neg B)$, $(B \vee C)$ ili $(\Diamond B)$, pri čemu su modalne formule B i C složenosti manje ili jednake n.

Pogledajmo prvo slučaj kada je modalna formula A jednaka $(\Diamond B)$. Neka je formula A pozitivna u propozicionalnoj varijabli P. Tada je i potformula B pozitivna u P pa je po pretpostavci indukcije monotono rastuća u P. Trebamo dokazati da je i formula A

monotono rastuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash (\Diamond B)$ tada po definiciji relacije forsiranja postoji svijet v takav da je $R(w, v)$ i $\mathfrak{M}, v \Vdash B$. Kako je formula B monotono rastuća u propozicionalnoj varijabli P, slijedi $\mathfrak{M}, v \Vdash' B$. Tada po definiciji relacije forsiranja vrijedi $\mathfrak{M}, w \Vdash' \Diamond B$ tj. $\mathfrak{M}, w \Vdash' A$. Pogledajmo sada slučaj kada je modalna formula A negativna u propozicionalnoj varijabli P. Tada je i potformula B negativna u P pa je po pretpostavci indukcije monotono padajuća u P. Trebamo dokazati da je i formula A monotono padajuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash (\Diamond B)$ tada po definiciji relacije forsiranja postoji svijet v takav da je $R(w, v)$ i $\mathfrak{M}, v \Vdash B$. Kako je formula B monotono padajuća u propozicionalnoj varijabli P, slijedi $\mathfrak{M}, v \Vdash' B$. Tada po definiciji relacije forsiranja vrijedi $\mathfrak{M}, w \Vdash' \Diamond B$ tj. $\mathfrak{M}, w \Vdash' A$.

Pogledajmo sada slučaj kada je formula A jednaka $(B \vee C)$. Neka je formula A pozitivna u propozicionalnoj varijabli P. Tada se propozicionalna varijabla P pojavljuje u formuli A samo pozitivno, pa se P pojavljuje samo pozitivno i u potformulama B i C. Dakle, formule B i C su po pretpostavci indukcije monotono rastuće u P. Trebamo dokazati da je i formula A monotono rastuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash (B \vee C)$ tada po definiciji relacije forsiranja $\mathfrak{M}, w \Vdash B$ ili $\mathfrak{M}, w \Vdash C$. Kako su formule B i C monotono rastuće u propozicionalnoj varijabli P, slijedi da je $\mathfrak{M}, w \Vdash' B$ ili $\mathfrak{M}, w \Vdash' C$. Dakle, $\mathfrak{M}, w \Vdash' B \vee C$ tj. $\mathfrak{M}, w \Vdash' A$. Pogledajmo sada slučaj kada je modalna formula A negativna u propozicionalnoj varijabli P. Tada se propozicionalna varijabla P pojavljuje u formuli A samo negativno, pa se P pojavljuje samo negativno i u potformulama B i C. Dakle, formule B i C su po pretpostavci indukcije monotono padajuće u P. Trebamo dokazati da je i formula A monotono padajuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash (B \vee C)$ tada po definiciji relacije forsiranja $\mathfrak{M}, w \Vdash B$ ili $\mathfrak{M}, w \Vdash C$. Kako su formule B i C monotono padajuće u propozicionalnoj varijabli P, slijedi da je $\mathfrak{M}, w \Vdash' B$ ili $\mathfrak{M}, w \Vdash' C$. Dakle, $\mathfrak{M}, w \Vdash' B \vee C$ tj. $\mathfrak{M}, w \Vdash' A$.

Neka je sada formula A jednaka $(\neg B)$. Neka je formula A pozitivna u propozicionalnoj varijabli P. Tada je očito modalna formula B negativna u P, pa je po pretpostavci indukcije formula B padajuća u P. Dokažimo da je formula A monotono rastuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash \neg B$ tada po definiciji relacije forsiranja ne vrijedi $\mathfrak{M}, w \Vdash B$. No, tada ne vrijedi ni $\mathfrak{M}, w \Vdash' B$ jer bi to bilo u kontradikciji s padajućom monotonošću od B. Sada odmah iz definicije relacije forsiranja slijedi $\mathfrak{M}, w \Vdash' \neg B$ tj. $\mathfrak{M}, w \Vdash' A$, što smo i trebali dokazati. Pogledajmo sada slučaj kada je formula A negativna u propozicionalnoj varijabli P. Tada je modalna formula B pozitivna u P, pa je po pretpostavci indukcije formula B monotono rastuća u propozicionalnoj varijabli P. Dokažimo da je formula A monotono padajuća u P. Neka je $\mathfrak{M}$ neki model i w neki svijet takav da $\mathfrak{M}, w \Vdash A$, te neka je $\Vdash'$ neka relacija forsiranja za koju vrijede uvjeti iz definicije (3.1.2). Kako vrijedi $\mathfrak{M}, w \Vdash A$ tj. $\mathfrak{M}, w \Vdash \neg B$ tada po definiciji relacije forsiranja ne vrijedi $\mathfrak{M}, w \Vdash B$. No, tada ne vrijedi ni $\mathfrak{M}, w \Vdash' B$ jer bi to bilo u kontradikciji s rastučom monotonošću od B u propozicionalnoj varijabli P. Sada odmah iz definicije relacije forsiranja slijedi $\mathfrak{M}, w \Vdash' \neg B$ tj. $\mathfrak{M}, w \Vdash' A$. Dakle formula A je monotono padajuća u propozicionalnoj varijabli P.

$\square$

Prethodna lema nam na osnovi sintaktičkog zapisa formule daje semantičko svojstvo koje ta formula zadovoljava. Monotoni rast, odnosno pad, formule je svojstvo koje za sobom povlači mnoga druga svojstva. Iskažimo jedno od njih koje ćemo kasnije koristiti.

Lema 3.1.6. *Neka je B formula logike prvog reda koja je monotono rastuća u relacijskom simbolu P, te neka su C i D neke formule logike prvog reda. Tada za svaku strukturu $\mathfrak{M}$ vrijedi: ako $\mathfrak{M} \models \forall x_1, \ldots, x_n(C(x_1, \ldots, x_n) \to D(x_1, \ldots, x_n))$ tada $\mathfrak{M} \models B(P := C(x_1, \ldots, x_n)) \to B(P := D(x_1, \ldots, x_n))$.*

Tvrdnju leme je lako dokazati indukcijom po složenosti formule B. Lemu (3.1.6) ćemo koristiti u dokazu iduće tvrdnje koja ima ključnu ulogu u Szalasovom algoritmu. Naime, iduća lema nam pruža mogućnost eliminacije varijabli drugog reda. No, prije samog iskaza dajemo primjer koji može poslužiti kao motivacija za najavljenu lemu.

Primjer 3.1.7. *Pokažimo kako za formulu logike drugog reda, koja ima odgovarajući oblik, možemo pronaći njoj ekvivalentnu formulu u kojoj nema pojavljivanja jednog unarnog relacijskog simbola. Označimo s R neki jednomjesni relacijski simbol. Zatim neka je formula prvog reda $B(x) \equiv \forall x R(x)$ i $A(x) \equiv Q(x)$ formula prvog reda, gdje je Q neki jednomjesni relacijski simbol. Nije teško pokazati da je formula $B(x)$ pozitivna u relacijskom simbolu R. Pogledajmo formulu drugog reda $\exists R(\ \forall x[R(x) \vee A(x)] \wedge B(R := \neg R)\ )$. Označimo sa F formulu dobivenu zamjenom potformula $A(x)$ i $B(x)$ u prethodnoj formuli sa formulama $Q(x)$ i $\forall x R(x)$. Sada imamo*

$$F \equiv \exists R(\ \forall x[R(x) \vee Q(x)] \wedge (\forall x \neg R(x))\ ).$$

Neka je $\mathfrak{M}$ struktrua drugog reda takva da $\mathfrak{M} \models F$. Iz $\mathfrak{M} \models F$ posebno slijedi $\mathfrak{M} \models \forall x(R(x) \vee Q(x))$. No, iz $\mathfrak{M} \models F$ imamo i $\mathfrak{M} \models \forall x \neg R(x)$. Sada $\mathfrak{M} \models \forall x(R(x) \vee Q(x))$ i $\mathfrak{M} \models \forall x \neg R(x)$ povlače $\mathfrak{M} \models \forall x Q(x)$. Obratno, Neka je $\mathfrak{M}$ neka struktura prvog reda. Dokažimo sada da $\mathfrak{M} \models \forall x Q(x)$ povlači $\mathfrak{M} \models F$. Iz $\mathfrak{M} \models \forall x Q(x)$ posebno slijedi $\mathfrak{M} \models \forall x(\bot \vee Q(x)) \wedge \top$. Promotrimo sada $\mathfrak{M}$ kao strukturu drugog reda u kojoj je unarna *relacijska varijabla R interpretirana praznim skupom. Tada očito vrijedi $\mathfrak{M} \models \forall x\, R(x) \leftrightarrow \bot$ i $\mathfrak{M} \models \forall x\, (\neg R(x)) \leftrightarrow \top$. Iz prethodnog očito slijedi $\mathfrak{M} \models F$.*

Lema 3.1.8. *Neka je P relacijski simbol te neka su $A(x_1, \dots, x_n)$ i $B(P)$ formule logike prvog reda. Neka je svako pojavljivanje od P u B pozitivno te neka se P ne pojavljuje u A. Tada vrijedi:*

1. *Formula drugog reda*

$$\exists P \left(\forall x_1, \dots, x_n \left[P(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\right] \wedge B(P := \neg P)\right) \tag{3.1}$$

   je logički ekvivalentna formuli

$$B(P := A(x_1, \dots, x_n)) \tag{3.2}$$

   gdje su varijable $x_1, \dots, x_n$ od A zamijenjene odgovarajućim termima od P, uz preimenovanje vezanih varijabli kada god je to potrebno.

2. *Formula drugog reda*

$$\exists P \left(\forall x_1, \dots, x_n \left[\neg P(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\right] \wedge B(P)\right) \tag{3.3}$$

   je logički ekvivalentna formuli

$$B(P := A(x_1, \dots, x_n)) \tag{3.4}$$

   gdje su varijable $x_1, \dots, x_n$ od A zamijenjene odgovarajućim termima od P, uz preimenovanje vezanih varijabli kada god je to potrebno.

Dokaz. Ako za neku formulu logike prvog ili drugog reda F postoji struktura $\mathfrak{M}$ takva da $\mathfrak{M} \models F$, tada ćemo u dokazu skraćeno pisati da formula F "vrijedi". Dokažimo sada prvu tvrdnju. Prvo pokažimo da (3.1) $\Rightarrow$ (3.2). Po pretpostavci, P se u B pojavljuje samo pozitivno pa iz leme (3.1.5) slijedi da je B monotono rastuća u P. Pretpostavimo da vrijedi (3.1). Označimo valuaciju relacijske varijable P s P'. Sada vrijedi

$$\forall x_1, \dots, x_n \Big[P'(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\Big] \wedge B(P := \neg P').$$

Standardnom reformulacijom logičkog veznika disjunkcije slijedi

$$\forall x_1, \dots, x_n \Big[\neg P'(x_1, \dots, x_n) \rightarrow A(x_1, \dots, x_n)\Big] \wedge B(P := \neg P').$$

Kako je B monotono rastuća u P, tada primjenom leme (3.1.6) slijedi

$$\Big[B(P := \neg P') \to B(P := A(x_1, \dots, x_n))\Big] \wedge B(P := \neg P').$$

Sada iz $B(P := \neg P')$ i $B(P := \neg P') \to B(P := A(x_1, \dots, x_n))$ slijedi $B(P := A(x_1, \dots, x_n))$ čime je dokazana prva implikacija.

Pokažimo sada da (3.2) $\Rightarrow$ (3.1). Neka je $P \equiv \neg A(x_1, \dots, x_n)$. Tada je formula (3.1) ekvivalentna formuli

$$\forall x_1, \dots, x_n\Big[\neg A(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\Big] \wedge B(P := \neg\neg A(x_1, \dots, x_n)).$$

Kako je konjunkt $\forall x_1, \dots, x_n\Big[\neg A(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\Big]$ ispunjiv za svaku strukturu, te pošto je zamijenjeni P bio izvan dosega kvantifikatora $\forall x_1, \dots, x_n$ i pošto su varijable $x_1, \dots, x_n$ u A zamijenjene termima od P, posljednja je formula ekvivalentna sa

$$B(P := A(x_1, \dots, x_n)).$$

Dokažimo sada drugu tvrdnju. Pokažimo prvo da (3.3) $\Rightarrow$ (3.4). Ponovno se po pretpostavci P u B pojavljuje samo pozitivno pa iz leme (3.1.5) slijedi da je B monotono rastuća u P. Pretpostavimo da vrijedi (3.3). Tada postoji valuacija relacijskog simbola P, koju ćemo označiti s P', za koju vrijedi

$$\forall x_1, \dots, x_n\Big[\neg P'(x_1, \dots, x_n) \vee A(x_1, \dots, x_n)\Big] \wedge B(P').$$

Standardnom reformulacijom logičkog veznika disjunkcije iz prethodne formule slijedi

$$\forall x_1, \dots, x_n\Big[\neg\neg P'(x_1, \dots, x_n) \to A(x_1, \dots, x_n)\Big] \wedge B(P').$$

Kako je B monotono rastuća u P, tada primjenom leme (3.1.6) na prethodnu formulu slijedi

$$\Big[B(P := \neg\neg P') \to B(P := A(x_1, \dots, x_n))\Big] \wedge B(P').$$

Formula $B(P := \neg\neg P')$ je logički ekvivalentna formuli $B(P := P')$ koja je opet logički ekvivalentna formuli $B(P')$. Sada iz $B(P')$ i $B(P') \to B(P := A(x_1, \dots, x_n))$ slijedi $B(P := A(x_1, \dots, x_n))$ čime je prva implikacija druge tvrdnje dokazana.
Pokažimo sada da (3.4) $\Rightarrow$ (3.3). Neka je $P \equiv A(x_1, \dots, x_n)$. Tada formula (3.3) poprima oblik

$$\forall x_1, \ldots, x_n \Big[\neg A(x_1, \ldots, x_n) \vee A(x_1, \ldots, x_n) \Big] \wedge B(P := A(x_1, \ldots, x_n)).$$

Kako je konjunkt $\forall x_1, \ldots, x_n \Big[\neg A(x_1, \ldots, x_n) \vee A(x_1, \ldots, x_n) \Big]$ ispunjiv za svaku strukturu, te pošto je zamijenjeni P bio izvan dosega kvantifikatora $\forall x_1, \ldots, x_n$ i pošto su varijable $x_1, \ldots, x_n$ u A zamijenjene termima od P, posljednja je formula ekvivalentna sa $B(P := A(x_1, \ldots, x_n))$ čime je i druga tvrdnja ove leme dokazana. □

Napomena 3.1.9. *Iako se u jeziku korespondencije drugog reda javljaju samo monadske varijable, prethodna lema je iskazana u općenitijem slučaju gdje mjesnost relacijske varijable može biti i veća od 1. Razlog tome je da se pokaže općenitost algoritma. Također, iako ćemo mi promatrati samo osnovni modalni jezik, Szalasov algoritam se može lagano proširiti tako da prihvaća i polimodalne logike, višemjesne modalne operatore,... Više detalja o potencijalnim proširenjima Szalasovog algoritma može se pronaći u [7].*

Prethodna lema nagovještava strategiju Szalasovog algoritma. Naime iz modalne formule primjenom propozicije (2.1.7) dolazimo do formule drugog reda koja je korespondent na okvirima modalne formule. Potom za dobivenu formulu drugog reda moramo pronaći njoj ekvivalentnu formulu drugog reda koja je u formi prikladnoj za primjenu prethodne leme. Zatim primjenom prethodne leme dolazimo do formule koja je ekvivalentna korespondentu drugog reda i u kojoj više nema pojavljivanja jedne monadske varijable. Time je i ta nova formula korespondent na okvirima polazne modalne formule. Primijetimo da ukoliko polazna modalna formula sadrži više od jedne propozicionalne varijable tada korespondent drugog reda dobiven primjenom propozicije (2.1.7) također sadrži više od jedne monadske varijable. Tada svakim ponavljanjem prethodnih koraka (svakim prolazom) dobivamo novog korespondenta na okvirima koji sadrži jednu monadsku varijablu manje nego prethodni korespondent dok konačno ne dobijemo korespondenta koji nema niti jedno pojavljivanje monadskih varijabli i time je taj korespondent ujedno i korespondent prvog reda na okvirima.

U radu algoritma pretpostavlja se postojanje sljedećih procedura:

1. CNF(A) ... procedura koja prima formulu prvog reda A te vraća formulu prvog reda koja je logički ekvivalentna sa A te koja je u konjunktivnoj normalnoj formi i u preneksnoj normalnoj formi (svi kvantifikatori se nalaze u prefiksu formule).

2. Skolemize(A) ... procedura koja prima formulu prvog reda A te za izlaz vraća formulu drugog reda koja je dobivena skolemizacijom formule A.

3. Unskolemize(A) ... procedura koja prima formulu drugog reda A te za izlaz vraća formulu prvog reda dobivenu eliminacijom Skolemovih funkcija iz formule A uvedenih procedurom Skolemize()

Za rad samog algoritma je bitno da procedura CNF() za izlaz vraća formulu koja je logički ekvivalentna formuli na ulazu, dok je za proceduru Skolemize() bitno da je izlazna formula ispunjiva na proširenjima struktura u kojima je ispunjiva ulazna formula. Procedura Unskolemize() mora vratiti formulu koja je logički ekvivalentna ulaznoj formuli. Za procedure Skolemize() i Unskolemize() to nije tipični zahtjev, no one to mogu zadovoljavati ako su na primjer bazirane na sljedećoj ekvivalenciji:

$$\forall x_1, \dots, x_n \, \exists y \, A(x_1, \dots, x_n, y, \dots) \Leftrightarrow \exists f \, \forall x_1, \dots, x_n \, A(x_1, \dots, x_n, y := f(x_1, \dots, x_n), \dots).$$

Tada bi procedura Skolemize() mogla koristiti prethodnu ekvivalenciju za uvođenje egzistencijalne kvantifikacije drugog reda umjesto egzistencijalne kvantifikacije prvog reda, a procedura Unskolomize() bi mogla koristiti prethodnu ekvivalenciju kako bi eliminirala kvantifikaciju drugog reda i zamijenila je kvantifikacijom prvog reda.

3.2 Opis rada algoritma

U ovoj točki proširujemo prethodni opis Szalasovog algoritma. Algoritam za ulaz prima formulu osnovnog modalnog jezika A te funkciju translacije T koja preslikava formule osnovnog modalnog jezika u formule jezika korespondencije prvog reda. Izlaz algoritma je formula koja je korespondent prvog reda na okvirima formule A. Szalasov algoritam ima 13 koraka. Sada ih redom navodimo:

Algoritam 3.2.1. ***(Szalasov algoritam)***

1. korak. Na početku rada algoritma odmah primijenjujemo propoziciju (2.1.7) na polaznu formulu A i time dobivamo formulu $\forall P_1, \dots, P_k \; T(A)$ koja je korespondent u $\mathcal{L}^2$ formule A gdje su $P_1, \dots, P_k$ monadske varijable koje odgovaraju istoimenim propozicionalnim varijablama iz A. Kao što smo već najavili, u ostatku algoritma pokušavamo redom "eliminirati" monadske varijable $P_1, \dots, P_k$.

2. korak. Označimo sa B formulu $\neg(\forall P_1, \dots, P_k \; T(A))$. Dok postoji barem jedna kvantificirana monadska varijabla $\{P_1, \dots, P_k\}$ ponavljamo slijedeće korake.

3. korak. Označimo s P neku kvantificiranu monadsku varijablu iz formule B.

4. korak. Primijenimo propoziciju (3.1.1.12) na B tako da monadska varijabla označena s P bude prva kvantificirana monadska varijabla. Sada je B u formi $\exists P \; B'$, gdje smo sa B' označili potformulu formule B. Sada iz proizvoljnosti modalne formule A slijedi da je oblik potformule B' također proizvoljan no znamo da za svaku formulu postoji njoj ekvivalentna formula koja je u konjunktivnoj normalnoj formi i u preneksnoj normalnoj formi.

5. korak. Koristimo proceduru CNF() s ulazom B' i izlaz označimo s C kako bi dobili formulu koja je logički ekvivalentna formuli B' i koja je u konjunktivnoj i preneksnoj normalnoj formi. Tada iz logičke ekvivalencije formula B' i C slijedi da je formula logike drugog reda B logički ekvivalentna formuli $\exists P\, C$.

6. korak. Ako C počinje s egzistencijalnim kvantifikatorom onda primjenom propozicije (3.1.1.12) pomičemo egzistencijalno kvantificiranje monadskih varijabli u C ispred egzistencijalne kvantifikacije monadske varijable označene s P. [1]

7. korak. Ako se u svim konjunktima formule C u kojima se javlja monadska varijabla označena s P ona javlja samo pozitivno ili samo negativno, onda označimo s F formulu dobivenu iz C brisanjem svih konjunkta koji sadrže monadsku varijablu označenu s P. Tada je formula $\exists P_{i_1}, \dots, P_{i_r}\, F$, gdje su $P_{i_1}, \dots, P_{i_r} \in \{P_1, \dots P_k\}$, logički ekvivalentna formuli B te formula F ne sadrži niti jedno pojavljivanje monadske varijable označene s P. [2] *Stoga možemo ukloniti $\exists P$ iz prethodne formule i označiti sa B formulu $\exists P_{j_1}, \dots, P_{j_r}\, F$, gdje su $P_{j_1}, \dots, P_{j_r} \in \{P_1, \dots P_k\} \setminus \{P\}$. Ukoliko u formuli B ima još kvantificiranih monadskih varijabli vratimo se na 3. korak.*[3]

8. korak. Ako postoji konjunkt u formuli C koji sadrži i pozitivno i negativno pojavljivanje monadske varijable označene s P onda javljamo da algoritam nije uspio i stajemo s izvršavanjem algoritma.

9. korak. Ako uvjeti 7. i 8. koraka nisu zadovoljeni tada se u nekim konjunktima formule C monadska varijabla označena s P javlja samo pozitivno, a u drugim konjunktima se javlja samo negativno. Tada transformiramo formulu C u ekvivalentnu formulu koja ima formu $\underline{C} \wedge \overline{C}$, gdje potformula označena s $\underline{C}$ sadrži samo pozitivna pojavljivanja monadske varijable označene s P a potformula označena s $\overline{C}$ sadrži samo negativna pojavljivanja monadske varijable označene s P.

10. korak.[4] *Ako proizvoljni konjunkt formule $\underline{C}$ sadrži najviše jedno pojavljivanje monadske varijable označene s P onda korištenjem algoritma (3.2.3) s ulazom $\underline{C}$ dobivamo*

[1] Sada kada imamo formulu C u konjunktivnoj i preneksnoj normalnoj formi, možemo početi iskorištavati njen oblik.

[2] Razlog zašto je prethodno definirana formula F logički ekvivalenta formuli C ilustrirat ćemo primjerom (3.2.2).

[3] Dakle ako se u svim konjunktima formule C u kojima se javlja varijabla označena s P ona javlja samo pozitivno ili samo negativno, onda možemo lagano eliminirati jednu monadsku varijablu.

[4] U ovom koraku algoritma koristiti ćemo pomoćni algoritam (3.2.3) kojeg ćemo iznjeti kasnije. Algoritam (3.2.3) smo izdvojili radi preglednosti.

ekvivalentnu formulu koja je u formi $\exists f_1 \dots f_l \; \forall z_1 \dots z_n \; (P(z_1 \dots z_n) \vee D_1) \wedge D_2$*, gdje su* f_i *Skolemove funkcije te* D_1 *i* D_2 *formule koje ne sadrže pojavljivanja monadske varijable označene s* P*. Ako proizvoljni konjunkt od* $\underline{C}$ *ne sadrži najviše jedno pojavljivanje monadske varijable označene s* P *onda provjeravamo ako proizvoljni konjunkt od* $\overline{C}$ *sadrži najviše jedno pojavljivanje monadske varijable označene s* P*. Ako sadrži onda korištenjem algoritma analognog algoritmu (3.2.3) s ulazom* $\overline{C}$ *dobivamo ekvivalentnu formulu koja je u formi* $\exists f_1 \dots f_l \; \forall z_1 \dots z_n \; (\neg P(z_1 \dots z_n) \vee D_1) \wedge D_2$*, gdje su* $f_1, \dots, f_l$ *te* D_1 *i* D_2 *kao prethodno. Ukoliko ni jedan ni drugi uvijet nisu zadovoljeni onda javljamo da algoritam nije uspio.*[5]

11. korak. Primijenimo lemu (3.1.8) na prethodnu formulu kako bi dobili formulu koja više nema pojavljivanja monadske varijable označene s P*. te označimo formulu koju smo dobili primjenom leme s* E*.*

12. korak. Ukoliko smo prilikom primjene algoritma (3.2.3) koristili skolemizaciju onda se još moramo riješiti funkcijskih varijabli uvedenih prilikom skolemizacije. To ćemo učiniti pozivom procedure Unskolemize() s ulazom E.

13. korak. Označimo formulu koju procedura Unskolemize() vratila kao izlaz s F. Ukoliko procedura Unskolemize(E*) nije uspjela onda se ne možemo riješiti uvedenih funkcijskih varijabli pa javljamo da algoritam nije uspio i stajemo s daljnjim izvršavanjem. No ukoliko je procedura Unskolemize(*E*) uspjela, tada označimo s B formulu* $\exists P_{i_1}, \dots, P_{i_r} \; F$*, gdje su* $P_{i_1}, \dots, P_{i_r} \in \{P_1, \dots P_k\}$*, te sada možemo obrisati u formuli B kvantificiranje monadske varijable označene s* P *te sve druge kvantifikatore drugog reda koji se ne javljaju u* F*. Time je jedan prolaz algoritma završen.*

Kao što smo prethodno rekli, svakim prolazom algoritma dobivamo formulu koja je logički ekvivalentna polaznoj formuli te koja sadrži jednu monadsku varijablu manje od prethodne formule. Algoritam uspješno staje kada formula označena s B više nema monadskih varijabli te kao izlaz algoritma vraćamo formulu $\neg B$.

Ilustrirajmo sada 7. korak Szalasovog algoritma primjerom. Dokaz ispravnosti 7. koraka može se pronaći u [7].

Primjer 3.2.2. *Pogledajmo formulu*

$$C \equiv \exists P \forall x, y \exists P_2 \; ((P(x) \vee P_2(x)) \wedge (P_2(y) \vee P_2(x)) \wedge (P(y) \vee P_2(y))). \tag{3.5}$$

[5] Primijetimo da ukoliko prethodni korak uspije tada je formula B ekvivalentna formuli oblika $\exists f_1 \dots f_l \; \exists P[\forall z_1 \dots z_n(P(z_1 \dots z_n) \vee D_1)] \wedge [D_2 \wedge \overline{C}]$ ili $\exists f_1 \dots f_l \; \exists P \; [\forall z_1 \dots z_n(\neg P(z_1 \dots z_n) \vee D_1)] \wedge [D_2 \wedge \underline{C}]$.

Tada za $P \equiv \top$ slijedi

$$\forall x, y \exists P_2 \left((\top \vee P_2(x)) \wedge (P_2(y) \vee P_2(x)) \wedge (\top \vee P_2(y))\right). \tag{3.6}$$

Formula (3.6) je logički ekvivalentna s $\forall x, y \exists P_2$ $(\top \wedge (P_2(y) \vee P_2(x)) \wedge \top)$ što je opet logički ekvivalentno s $\forall x, y \exists P_2$ $(P_2(y) \vee P_2(x))$. U drugom smjeru iz (3.6) trivijalno slijedi (3.5). Upravo provedeni dokaz logičke ekvivalencije formula bio je moguć zbog pozitivnog pojavljivanja varijable P. Također, ukoliko je svaki nastup varijable P negativan, tada možemo provesti isto zaključivanje samo koristeći $\neg P \equiv \top$.

Kako bi u potpunosti opisali Szalasov algoritam još nam preostaje opisati pomoćni algoritam kojeg koristimo u 10. koraku.

Algoritam 3.2.3. *Ulaz pomoćnog algoritma je formula logike prvog reda C koja je u konjunktivnoj normalnoj formi i koja sadrži samo pozitivna pojavljivanja relacijskog simbola P. Izlaz algoritma je formula logike drugog reda koja ima oblik $\exists f_1 \dots f_l \, \forall z_1 \dots z_n$ $(P(z_1, \dots, z_n) \vee D_1) \wedge D_2$, gdje su $f_1, \dots, f_l$ Skolemove funkcije a D_1 i D_2 formule koje ne sadrže pojavljivanje relacijskog simbola P.*

1. korak. Ako formula C sadrži egzistencijalne kvantifikatore onda pozivamo metodu Skolemize() sa ulazom C te izlaz metode označimo s E. Sada formula E ima oblik $\exists f_1 \dots f_l \forall x_1 \dots x_m (E_1 \wedge \dots \wedge E_k)$, gdje su $f_1, \dots, f_l$ Skolemove funkcije a $E_1, \dots, E_k$ elementarne disjunkcije.

2. korak. Označimo s D_2 formulu $\forall x_1 \dots x_m (E_{i_1} \wedge \dots \wedge E_{i_q})$ gdje su $E_{i_1}, \dots, E_{i_q}$ svi konjunkti formule E u kojima se ne javlja relacijski simbol P. Obrišimo konjunkte $E_{i_1}, \dots, E_{i_q}$ iz formule E.

3. korak. Pomaknimo sve univerzalne kvantifikatore u formuli E ispred svakog od preostalih konjunkta koristeći propoziciju (3.1.1.7). Sada formula E ima oblik $\exists f_1 \dots f_l$ $(\forall x_1 \dots x_m (E_{j_1}) \wedge \dots \wedge \forall x_1 \dots x_m (E_{j_q}))$, gdje su $E_{j_1}, \dots, E_{j_q}$ elementarne disjunkcije polazne formule od kojih svaka sadrži točno jedno pojavljivanje relacijskog simbola P.

4. korak. Korištenjem propozicije (3.1.1.13) zamijenimo svaki konjunkt formule E formulom $\forall x_1 \dots x_m \forall z_1 \dots z_n (P(z_1, \dots, z_n) \vee F)$, gdje su $z_1, \dots, z_n$ novo uvedene varijable.

5. korak. Koristeći propoziciju (3.1.1.11 i .12) i distributivnost disjunkcije prema konjunkciji, iz formule E dolazimo do ekvivalentne formule oblika

$$\exists f_1 \dots f_l \forall z_1 \dots z_n [P(z_1, \dots, z_n) \vee \forall x_1 \dots x_m (F_1 \wedge \dots \wedge F_r)].$$

6. korak. Kao rezultat algoritma vratimo formulu

$$\exists f_1 \dots f_l \forall z_1 \dots, z_n [P(z_1, \dots, z_n) \vee \forall x_1 \dots x_m (F_1 \wedge \dots \wedge F_r)] \wedge D_2.$$

Iz opisa Szalasovog algoritma vidimo da na kraju svakog prolaza algoritma formula označena s B sadrži jednu monadsku varijablu manje nego što je imala formula označena s B na početku prolaza algoritma. Kako modalna formula na ulazu algoritma ima konačano mnogo propozicionalnih varijabli tada algoritam može imati samo konačno prolaza. Nije teško vidjeti da svaki prolaz algoritma dolazi do kraja ili staje, a time i cijeli algoritam uvijek staje. Dalje, Szalasov algritam je ispravan u smislu da kada vrati formulu, ta formula jest korespondent prvog reda na okvirima ulazne formule. No, vidimo da postoje koraci algoritma (npr. 13. korak) u kojima algoritam staje i javlja da nije uspio pronaći korespondenta prvog reda na okvirima za ulaznu formulu, ali nije očito da li tada nužno korespondent prvog reda ne postoji. Odnosno nije očito je li Szalasov algoritam potpun. Iz teorema (3.0.1) slijedi da nije a dati ćemo i modalne formule koje imaju korespondenta prvog reda na okvirima a koje Szalasov algoritam ne uspije izračunati. Prvo iznosimo pseudokod Szalasovog algoritma a potom ćemo pokazati neke primjere rada.

---

ulaz : funkcija translacije T koja prevodi modalne formule u formule logike prvog reda i modalna formula A

izlaz: korespondent prvog reda na okvirima formule A ili odgovor da algoritam nije uspio

1 *neka su* $P_1, \ldots, P_k$ *sve propozicionalne varijable koje se javljaju u formuli* A;
2 $H \leftarrow \forall P_1, \ldots, P_k\, T(S)$;
3 $B \leftarrow \neg H$;
4 **dok** *postoji kvantificirani* P_i *u formuli B,* $P_i \in \{P_1, \ldots, P_k\}$ **ponavljaj:**
5 $\quad P \leftarrow P_i$;
6 $\quad B \leftarrow \exists P\, B'$; `// elemente` $\{P_1, \ldots, P_k\} \setminus P$ `tretiramo kao konstante`
7 $\quad C \leftarrow \mathrm{CNF}(B')$;
8 $\quad B \leftarrow \exists P\, C$;
9 $\quad$ **ako** *C počinje sa egzistencijalnim kvantifikatorom* **onda:**
10 $\qquad$ koristeći Propoziciju 3.1.1 (12) pomakni ih ispred $\exists P$
11 $\quad$ **ako** *se u svim konjunktima od C u kojima se javlja relacijski simbol P, on javlja samo pozitivno ili samo negativno* **onda:**
12 $\qquad F \leftarrow$ formula dobivena iz C brisanjem svih konjunkta koji sadrže P;
13 $\qquad$ odi na korak 31.
14 $\quad$ **ako** *postoji konjunkt u C koji sadrži i pozitivno i negativno pojavljivanje relacijskog simbola P* **onda:**
15 $\qquad$ javi da algoritam nije uspio i stani
16 $\quad$ **inače:**
17 $\qquad$ transformiraj C u ekvivalentnu formulu koja ima formu $\underline{C} \wedge \overline{C}$ gdje potformula $\underline{C}$ ne sadrži negativna pojavljivanja relacijskog simbola P a $\overline{C}$ ne sadrži pozitivna pojavljivanja relacijskog simbola P
18 $\quad$ **ako** *proizvoljni konjunkt od* $\underline{C}$ *sadrži najviše jedno pojavljivanje relacijskog simbola P* **onda:**
19 $\qquad$ koristeći algoritam (3.2.3) sa ulazom $\underline{C}$ dobivamo ekvivalentnu formulu koja je u formi $\exists f_1 \ldots f_l\, \forall z_1 \ldots z_n\, (P(z_1 \ldots z_n) \vee D_1) \wedge D_2$, gdje su f_i Skolemove funkcije te D_1, D_2 ne sadrže pojavljivanja od P;
20 $\qquad B \leftarrow \exists f_1 \ldots f_l \exists P([\forall z_1 \ldots z_n(P(z_1, \ldots, z_n) \vee D_1)] \wedge [D_2 \wedge \overline{C}])$;
21 $\quad$ **inače ako** *proizvoljni konjunkt od* $\overline{C}$ *sadrži najviše jedno pojavljivanje relacijskog simbola P* **onda:**
22 $\qquad$ koristeći algoritam analogan algoritmu (3.2.3) sa ulazom $\overline{C}$ dobivamo ekvivalentnu formulu koja je u formi $\exists f_1 \ldots f_l\, \forall z_1 \ldots z_n$ $(\neg P(z_1 \ldots z_n) \vee D_1) \wedge D_2$, gdje su $f_1, \ldots, f_l$ te D_1 i D_2 kao i prije;
23 $\qquad B \leftarrow \exists f_1 \ldots f_l \exists P([\forall z_1 \ldots z_n(\neg P(z_1, \ldots, z_n) \vee D_1)] \wedge [D_2 \wedge \underline{C}])$;

---

inače:
  javi da algoritam nije uspio i stani
$E \leftarrow$ formula koja je dobivena primjenom Leme 3.1.8 na B;
ako *je skololemizacija bila potrebna za izvršavanje linija 19 ili 22* **onda:**
  $F \leftarrow$ Unskolemize(E);
  ako *procedura Unskolemize() nije uspjela* **onda:**
    javi da algoritam nije uspio i stani
$B \leftarrow \exists P_{i_1}, \ldots, P_{i_r}\ F$, gdje su $P_{i_1}, \ldots, P_{i_r} \in \{P_1, \ldots, P_k\} \setminus P$;
obriši u B kvantifikator $\exists P$ (odnosno $\exists P_i$) te sve druge kvantifikatore drugog reda koji se ne javljaju u F;
vrati $\neg B$;   `// ¬B je korespondent prvog reda na okvirima`

Sada ćemo prikazati rad algoritma kroz nekoliko primjera. Napomenimo da ćemo u sljedećim primjerima koristiti neke dodatne optimizacije kao npr. kada pozitivna i negativna pojavljivanja relacijskog simbola P budu razdvojena, nećemo transformirati cijelu formulu u konjunktivnu normalnu formu već samo jedan dio formule. Dalje, kao što smo prethodno naveli, za funkciju translacije T koristiti ćemo funkciju definiranu sa $T(A) := \forall x ST_x(A)$, gdje je A neka modalna formula. Također, za ulaz algoritma ćemo zapisati sve modalne formule koristeći samo logičke simbole $\vee$ i $\neg$.

Primjer 3.2.4. *Pogledajmo prvo modalnu formulu $\Box P \to P$ za koju smo pokazali da definira svojstvo refleksivnosti. Formula koju dajemo algoritmu na ulazu je tada $\neg\Box P \vee P$.*

- *translatirana formula:* $\forall P \forall x \neg(\forall y(\neg R(x,y) \vee P(y))) \vee P(x)$.
- *negirana formula:* $\exists x \exists P(\forall y(\neg R(x,y) \vee P(y))) \wedge \neg P(x)$. *— primijetimo da je formula već u rastavljenom obliku te da možemo primijeniti lemu (3.1.8).*
- *P eliminaran:* $\exists x \neg R(x,x)$.
- *negirana formula:* $\forall x R(x,x)$.

Dakle algoritam kao rezultat daje korespondenta prvog reda na okvirima kojega smo prethodno i teorijski pronašli.

Primjer 3.2.5. *Pogledajmo sada rad algoritma za modalnu formulu $\Box P \to \Box\Box P$. Formula koju dajemo algoritmu na ulazu je tada $\neg\Box P \vee \Box\Box P$.*

- *translatirana formula:* $\forall P \forall x \neg(\forall y(\neg R(x,y) \vee P(y))) \vee \forall y(\neg R(x,y) \vee \forall z(\neg R(y,z) \vee P(z)))$.

- *negirana formula:* $\exists P \exists x (\forall y (\neg R(x,y) \vee P(y))) \wedge \exists y (R(x,y) \wedge \exists z (R(y,z) \wedge \neg P(z)))$ — *primijetimo da je formula već u rastavljenom obliku.*

- *transformirana formula:* $\exists P \exists x \forall y [P(y) \vee \neg R(x,y)] \wedge [\exists y (R(x,y) \wedge \exists z (R(y,z) \wedge \neg P(z)))]$ — *sada možemo primijeniti lemu (3.1.8).*

- *P eliminiran:* $\exists x \exists y (R(x,y) \wedge \exists z (R(y,z) \wedge \neg R(x,z)))$.

- *negirana formula:* $\forall x \forall y (\neg R(x,y) \vee \forall z (\neg R(y,z) \vee R(x,z)))$ — *Szalasov algoritam ovdje staje no vraćena formula se može još pojednostaviti.*

- *pojednostavljena formula:* $\forall x \forall y \forall z\ (R(x,y) \to (R(y,z) \to R(x,z))))$ — *što je formula prvog reda koja definira tranzitivnost.*

Primjer 3.2.6. *Pogledajmo sada rad algoritma na primjeru modalne formule koja ima dvije propozicionalne varijable. Formula koju dajemo algoritmu na ulazu je* $\neg \Box (P \vee Q) \vee (\Box P \vee \Box Q)$.

- *translatirana formula:* $\forall P \forall Q \forall x \neg (\forall y (\neg R(x,y) \vee (P(y) \vee Q(y))) \vee (\forall z (\neg R(x,z) \vee P(z)) \vee \forall v (\neg R(x,v) \vee Q(v))))$.

- *negirana formula:* $\exists P \exists Q \exists x (\forall y (\neg R(x,y) \vee P(y) \vee Q(y)) \wedge (\exists z (R(x,z) \wedge \neg P(z)) \wedge \exists v\ (R(x,v) \wedge \neg Q(v))))$.

- *rastavljena formula s obzirom na Q:* $\exists x \exists z \exists v\ \exists P \exists Q \forall y [Q(y) \vee (\neg R(x,y) \vee P(y)))] \wedge [R(x,z) \wedge \neg P(z) \wedge R(x,v) \wedge \neg Q(v)]$.

- *Q eliminiran:* $\exists x \exists z \exists v\ \exists P (R(x,z) \wedge \neg P(z) \wedge R(x,v) \wedge (\neg R(x,v) \vee P(v)))$.

- *rastavljena formula s obzirom na P:* $\exists x \exists z \exists v\ \exists P [P(v) \vee \neg R(x,v)] \wedge R(x,z) \wedge \neg P(z) \wedge R(x,v) \wedge \neg P(v)$ — *sada koristimo propoziciju (3.1.1.13).*

- *transformirana formula:* $\exists x \exists z \exists v\ \exists P \forall u [P(u) \vee (u \neq v \vee \neg R(x,u))] \wedge [R(x,z) \wedge \neg P(z) \wedge R(x,v)]$ — *sada možemo primijeniti lemu (3.1.8).*

- *P eliminitran:* $\exists x \exists z \exists v\ [R(x,z) \wedge (z \neq v \vee \neg R(x,z)) \wedge R(x,v)]$.

- *negirana formula:* $\forall x \forall z \forall v\ [\neg R(x,z) \vee (z = v \wedge R(x,z)) \vee \neg R(x,v)]$ — *Szalasov algoritam ovdje staje no vraćena formula se može još pojednostaviti.*

- *pojednostavljena formula:* $\forall x \forall z \forall v\ ((R(x,z) \wedge R(x,v)) \to (z = v \wedge R(x,z))$ *odnosno* $\forall x \forall z \forall v\ ((R(x,z) \wedge R(x,v)) \to z = v$.

Kao što smo rekli Szalasov algoritam nije potpun. Primjer formule za koji Szalasov algoritam ne uspije pronaći korespondenta prvog reda na okvirima je $(\Box P \rightarrow \Box\Box P) \wedge (\Box\Diamond P \rightarrow \Diamond\Box P)$. Modalna formula $\Box\Diamond P \rightarrow \Diamond\Box P$ poznata je pod imenom McKinseyev aksiom te je za nju dokazano da općenito nema korespondenta prvog reda na okvirima, no dokazano je da ima korespondenta prvog reda na tranzitivnim okvirima što se može pronaći u [1].

Poglavlje 4

Zaključak

Problem pronalaženja korespondenta prvog reda na okvirima modalne formule je i dalje predmet intezivnog istraživanja. Značaj Szalasovog algoritma leži u činjenici da je on drugi objavljeni algoritam za prolaženje korespondenta. Prvi objavljeni algoritam na tu temu bio je SCAN algoritam. Veliki nedostatak tog algoritma bilo je to što SCAN algoritam ne staje uvijek. Nakon Szalasovog algoritma objavljen je DLS algoritam za nalaženje korespondenta prvog reda na okvirima. No DLS algoritam ima slične nedostatke kao i Szalasov. Najveći nedostatak Szalasovog i DLS algoritma je korištenje skolemizacije. Prilikom korištenja skolemizacije u algoritmu uvode se nove kvantifikacije drugog reda koje se potom moraju eliminirati primjenom procedure Unskolemize(). Općenito je problem odskolemizacije[1] neodlučiv te se pokazalo da je upravo taj korak najkritičniji i glavni razlog kada algoritam ne uspije pronaći korespondenta prvog reda. Godine 2006. W. Conradie, V. Goranko i D. Vakarelov izdaju svoj prvi članak [3] iz serije od četiri članka o novom algoritmu SQEMA. Algoritam SQEMA nadilazi prethodne algoritme time što izbjegava korištenje skolemizacije a time i potrebu za odskolemiziranjem. Naime, SQEMA algoritam radi transformacije direktno nad modalnim formulama umjesto nad translatiranim formulama. Po teoremu (3.0.1) znamo da ne može postojati algoritam koji je potpun na klasi svih formula osnovnog modalnog jezika. No, znamo da postoje podklase formula (kao npr. Sahlqvistova) za koju je moguće imati potpun algoritam. U idućim člancima [4] i [5], W. Conradie, V. Goranko i D. Vakarelov proširuju SQEMA algoritam tako da on bude potpun na klasi složenih induktivnih formula, što je puno šira klasa i od složenih Sahlqvistovih formula.

[1] Odskolemizacija je proces eliminacije Skolemovih funkcija uvedenih skolemizacijom.

Bibliografija

[1] Benthem, J.Van: *Correspondence theory*. Handbook of Philosophical Logic, 2:167–247, 1984.

[2] Blackburn, P., M. de Rijke i Y. Venema: *Modal Logic*. Cambridge University Press, 2002.

[3] Conradie, W., V. Goranko i D. Vakarelov: *Algorithmic correspondence and completenees in modal logic. I. The core algorithm SQEMA*. Logical Methods in Computer Science, 2:1–26, 2006.

[4] Conradie, W., V. Goranko i D. Vakarelov: *Algorithmic correspondence and completenees in modal logic. II. Polyadic and Hybrid Extensions of the Algorithm SQEMA*. Journal of Logic and Computation, 16:579–612, 2006.

[5] Conradie, W., V. Goranko i D. Vakarelov: *Algorithmic correspondence and completenees in modal logic. III. Extensions of the algorithm SQEMA with substitutions*. Journal Fundamenta Informaticae, 92:307–343, 2009.

[6] Perkov, T.: *Sahlqvistove formule*. diplomski rad, PMF-MO, Zagreb, 2006.

[7] Szalas, A.: *On the Correspondence Between Modal and Classical Logic: an Automated Approach*. Journal of Logic and Computation, 3(6):605–620, 1993.

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

Sažetak

Glavna tema ovog rada je Szalasov algoritma koji za danu modalnu formulu pronalazi njenog korespondenta prvog reda na okvirima. U prvom poglavlju rada promatramo osnovni modalni jezik, Kripkeovu semantiku te iznosimo potrebne definicije i pojmove logike prvog i drugog reda. Potom se bavimo temom korespondencije formula osnovnog modalnog jezika i formula logike prvog i drugog reda. Uz to promatramo i funkciju standardne translacije za formule osnovnog modalnog jezika. U trećem poglavlju detaljno promatramo Szalasov algoritam. Teorijski ga analiziramo, opisujemo po koracima, iznosimo pseudokod algoritma kao i neke primjere rada.

Summary

The main topic of this Master thesis is Szalas' algorithm which for a given modal formula, finds its first-order correspondent. In the first chapter of the thesis, we look at the basic modal language, Kripke semantics, and present the necessary definitions and concepts of first and second-order logic. We then address the topic of correspondence between basic modal formulas and first or second-order formulas. We also look at the standard translation function for basic modal formulas. In the third section, we look at the Szalas' algorithm in detail. We analyze it theoretically, describe it step by step, present the pseudocode of the algorithm and present some examples.

Životopis

Rođen sam 28. kolovoza 1995. godine u Rijeci. Pohađao sam osnovnu školu Dr. Andrija Mohorovičić u Matuljima. Nakon osnovne škole upisujem gimnaziju Andrije Mohorovičića u Rijeci te nastavljam školovanje na preddiplomskom studiju Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Godine 2017. po završetku preddiplomskog studija upisujem diplomski studij Računarstvo i matematika također na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Od svibnja 2018. godine do kolovoza 2019. godine radio sam na studentskoj poziciji softverskog inžinjera u AVL-AST. Od kolovoza 2019. godine radim kao inžinjer robotike na koordinaciji flota u Gideon Brothers d.o.o.