Složenost modalnih logika

Marciuš, Helena

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Helena Marciuš

SLOŽENOST MODALNIH LOGIKA

Diplomski rad

Voditelj rada:
prof. dr. sc. Mladen Vuković

Zagreb, rujan, 2022.

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. _____

Obitelji, Aleksu i ekipi s veslanja.

Veliko hvala mentoru prof. dr. sc. Mladenu Vukoviću na strpljenju i pomoći u pisanju ovog rada.

Sadržaj

Uvod

Problem SAT, odnosno problem ispunjivosti formula logike sudova, jedan je od najpoznatijih problema teorije složenosti. Cook i Levin 1970-ih godina dokazuju da je problem SAT jedan NP–potpun problem. Time problem SAT postaje prvi poznati NP–potpun problem. Kažemo još da je logika sudova odlučiva i NP–potpuna. A. Church je 1930-ih dokazao je da je problem ispunjivosti logike prvog reda neodlučiv problem - ne postoji algoritam koji bi za proizvoljnu formulu logike prvog reda odlučio je li ispunjiva. Prirodno je pitati se što je s drugim logikama - jesu li odlučive te, ako jesu, koja je njihova složenost.

Modalna logika nastala je kao proširenje logike sudova. Potreba za proširenjem javila se radi definicije interpretacije kondicionala (tzv. paradoks materijalne implikacije). Gledajući interpretaciju kondicionala neformalno možemo reći da u klasičnoj logici sudova "iz laži slijedi sve". Druga motivacija za uvođenje modalnih logika je povećanje ekspresivnosti jezika. Naime, u logici sudova možemo izreći rečenicu "Danas ne idem školu", ali ne možemo izreći "Moguće danas ne idem u školu." Stoga je jezik logike sudova proširen modalnim operatorima $\Diamond$ i $\Box$ koje redom nazivamo operatorima mogućnosti i nužnosti. Danas se modalna logika ne smatra samo sredstvom za izražavanje nužnosti i mogućnosti, već se koristi kao sredstvo za opis relacijskih struktura te se primijenjuje u računarstvu, umjetnoj inteligenciji, filozofiji, lingvistici itd.

Cilj ovog diplomskog rada je dokazati nekoliko rezultata o složenosti modalnih logika. Prve rezultate o složenosti modalnih logika iznio je Ladner u [2] dokazavši NP–potpunost logike **S5** te PSPACE–potpunost logika **K**, **T** i **S4**. Dvije godine nakon toga dokazana je EXPTIME–potpunost za logiku PDL. Najviše rezultata o složenosti modalnih logika nastalo je 1980-ih kada je, između ostaloga, dokazana PSPACE–potpunost linearne temporalne logike te EXPTIME–potpunost modalnog μ-računa. U ovome se radu prvenstveno bavimo logikama osnovnog modalnog jezika čije su složenosti dokazali Ladner u [2] te Hemaspaandra u [7].

Ovaj diplomki rad podijeljen je u dva poglavlja. U prvom se poglavlju bavimo sintaksom i semantikom osnovnog modalnog jezika. Prvo definiramo najmanju normalnu modalnu logiku **K** te neka njezina proširenja - logike **K4**, **T**, **S4**, **S5** te **S4.3**. Navodimo i

osnovne pojmove i rezultate teorije modela modalne logike. Na kraju poglavlja opisujemo karakteristične klase okvira raznih modalnih logika.

U drugom poglavlju bavimo se složenošću normalnih modalnih logika koje smo definirali u prvom poglavlju. Prvo definiramo polinomno svojstvo konačnih modela te pojam definabilnosti klase okvira u logici prvog reda. Ovi su pojmovi ključni za dokaz NP–potpunost logike **S5** te za dokaz Hemaspaandrinog teorema o NP–potpunosti modalnih logika koje proširuju **S4.3**.

Drugi dio drugog poglavlja posvećen je PSPACE–potpunim modalnim logikama. Prvo dokazujemo da logika **K** nema polinomno svojstvo konačnih modela (iz tog rezultata možemo naslutiti da logika **K** nije NP–potpuna modalna logika). Zatim definiramo pojam Hintikkinog skupa i pojam skupa svjedoka. Nakon toga dokazujemo tvrdnje koje nam daju sintaktički kriterij za provjeru ispunjivosti formule. Navodimo algoritam *Svjedok* te opisujemo rad Turingovog stroja koji provjerava **K**–ispunjivost koristeći taj algoritam, ali tako da pritom koristi samo polinomno mnogo registara. Time i dokazujemo da je logika **K** jedna PSPACE–složena modalna logika. Zatim definiramo problem TQBF koji je PSPACE–potpun. Svođenjem problema TQBF na problem ispunjivosti proizvoljne normalne modalne logike Λ takve da je $\mathbf{K} \subseteq \Lambda \subseteq \mathbf{S4}$ dokazujemo Ladnerov teorem koji govori da je svaka logika između **K** i **S4** nužno PSPACE–teška.

Poglavlje 1

Osnovne definicije i činjenice

Rad započinjemo definiranjem osnovnih pojmova modalne logike. Najprije definiramo pojmove alfabeta i formule modalne logike. Zatim definiramo ispunjive i valjane modalne formule. Nakon toga definiramo sisteme modalne logike čije probleme ispunjivosti ćemo promatrati u sljedećem poglavlju. U nastavku navodimo osnovne pojmove teorije modela modalne logike. Na kraju poglavlja dokazujemo nekoliko tvrdnji o vezi valjanosti modalne formule na okvirima i svojstava relacija dostiživosti na okvirima.

1.1 Sintaksa modalne logike

Definirajmo prvo osnovni modalni jezik. Prvo definiramo alfabet, odnosno skup simbola od kojih se sastoji jezik. Taj skup sadrži alfabet logike sudova i simbol $\Diamond$. Nakon toga, definiramo na koji se način grade specifični nizovi simbola koje zovemo formule.

Definicija 1.1.1. ***Alfabet osnovnog modalnog jezika*** *je unija sljedećih skupova:*

- *skup prebrojivo mnogo propozicionalnih varijabli* $\{p_0, p_1, p_2, \dots\}$
- *skup logičkih veznika, modalnih operatora i logičkih konstanti* $\{\neg, \vee, \Diamond, \bot\}$
- *skup pomoćnih simbola* $\{(,)\}$ *(zagrade)*

Koristimo i logičke veznike $\wedge$, $\rightarrow$ i $\leftrightarrow$ kao uobičajane pokrate te unarni modalni operator $\Box$ kao pokratu za $\neg\Diamond\neg$. Skup propozicionalnih varijabli označavamo s $Prop$, a propozicionalne varijable sa p, q, r itd.
Operatore $\Diamond$ i $\Box$ čitamo redom ”diamond” i ”box”. Nazivamo ih i operator mogućnosti i operator nužnosti.

U nastavku definiramo pojam formule osnovnog modalnog jezika. Definicija je analogna definiciji formule logike sudova uz dodatak operatora $\Diamond$.

Definicija 1.1.2. ***Atomarna formula osnovnog modalnog jezika*** *je svaka propozicionalna varijabla ili logička konstanta* $\bot$.

Pojam ***formule*** *osnovnog modalnog jezika definiramo rekurzivno na sljedeći način:*

a) svaka atomarna formula je formula

b) ako su φ *i* ψ *formule, tada su i izrazi* $\neg\varphi$, $\varphi \vee \psi$ *i* $\Diamond\varphi$ *također formule.*

Skup svih formula osnovne modalne logike označavamo s $Form$, a formule obično označavamo simbolima φ, ϕ, ψ itd. Formule oblika $\Diamond\varphi$ gdje je φ proizvoljna formula nazivamo $\Diamond$–formule.

Primjer 1.1.3. *Riječi* $\Diamond p \vee (\Diamond\bot \vee \neg q)$ *i* $\neg\Diamond p \vee \Diamond\neg q$ *su primjeri modalnih formula. Riječi* $\neg \vee \Diamond p$ *i* $\vee pq\Diamond r$ *nisu formule.*

Osim složenosti modalne formule koja se, analogno logici sudova, definira kao broj veznika i modalnih operatora u formuli, definiramo i stupanj modalne formule. Intuitivno, stupanj formule je broj ugniježđenih modalnih operatora.

Definicija 1.1.4. ***Stupanj*** *modalne formule* φ*, u oznaci* $deg(\varphi)$*, definiramo rekurzivno ovako:*

$$\begin{aligned} deg(\bot) &= 0 \\ deg(p) &= 0 \\ deg(\neg\varphi) &= deg(\varphi) \\ deg(\varphi \vee \psi) &= max\{deg(\varphi), deg(\psi)\} \\ deg(\Diamond\varphi) &= 1 + deg(\varphi) \end{aligned}$$

Stupanj konačnog skupa formula Σ *definiramo kao maksimalni stupanj svih formula iz* Σ*, to jest* $deg(\Sigma) = max\{deg(\varphi), \varphi \in \Sigma\}$.

Primjer 1.1.5. *a) Stupanj formule* $\neg(\Diamond\Diamond p \vee \bot) \vee \Diamond(q \vee \Diamond\neg\Diamond p)$ *je 3.*

b) Neka je $\Sigma = \{\Diamond p, p \vee \neg q, \Diamond\bot, \Diamond(p \vee \Diamond q)\}$. *Stupanj skupa* Σ *je 2.*

U ovom radu bavimo se samo osnovnim modalnim jezikom čiji alfabet sadrži samo jedan unarni modalni operator. Međutim, postoji puno modalnih logika i svaka ima svoj alfabet. Tako primjerice alfabet logike interpretabilnosti sadrži dva modalna operatora, unarni operator $\Diamond$ te binarni operator $\triangleright$, dok alfabet sustava **GLP** ima prebrojivo mnogo unarnih modalnih operatora.

1.2 Semantika modalne logike

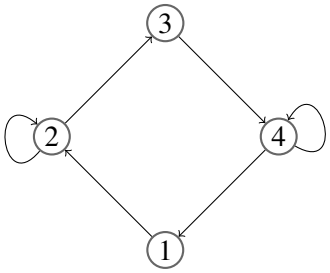
Semantiku modalne logike razvio je Saul Kripke sredinom 20. stoljeća te ju nazivamo i Kripkeova semantika. Iako je sintaksa modalne logike slična sintaksi logici sudova, semantika modalne logike je nešto složenija od semantike logike sudova. U logici sudova istinitost formule ovisila je samo o interpretaciji. U modalnoj logici, istinitost formule promatramo lokalno, unutar relacijske strukture zvane Kripkeov okvir.

Definicija 1.2.1. ***Kripkeov okvir*** *za osnovni modalni jezik je uređeni par* $\mathfrak{F} = (W, R)$ *gdje je* W *neprazni skup kojeg nazivamo* ***nosač*** *(domena), a* R *binarna relacija na* W *koju nazivamo* ***relacija dostižívosti****. Elemente nosača* W *nazivamo* ***svjetovi****. Za svjetove* $w, v \in W$ *kažemo da je svijet* v ***dostižív*** *iz svijeta* w *ako je* $(w, v) \in R$*.*

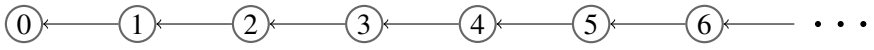
Umjesto $(w, v) \in R$ pisat ćemo wRv. Reći ćemo da je v sljedbenik od w.

Primjer 1.2.2. *Navodimo primjere nekih okvira te ih ilustriramo.*

a) Neka je $\mathfrak{F} = (W, R)$ *gdje je* $W = \{1, 2, 3, 4\}$ *i* $R = \{(1, 2), (2, 3), (3, 4), (4, 1), (2, 2), (4, 4)\}$



b) Neka je $\mathfrak{F} = (W, R)$ *gdje je* $W = \mathbb{N}$*, a relacije* R *definirana je ovako:* xRy *ako i samo ako* $x = y + 1$*.*



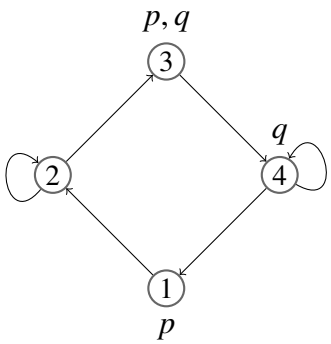
Kako bismo definirali istinitost formule prvo dodajemo svakom Kripkeovom okviru preslikavanje iz skupa propozicionalnih varijabli u neki podskup nosača. Time dobivamo strukturu zvanu Kripkeov model.

Definicija 1.2.3. ***Kripkeov model*** *za osnovni modalni jezik je uređeni par* $\mathfrak{M} = (\mathfrak{F}, V)$ *gdje je* $\mathfrak{F} = (W, R)$ *okvir za osnovni modalni jezik, a* $V\colon Prop \to \mathcal{P}(W)$ *funkcija koju nazivamo* ***valuacija****. Kažemo da je model* $\mathfrak{M}$ *baziran na okviru* $\mathfrak{F}$*.*

U nastavku umjesto Kripkeov okvir i Kripkeov model pišemo samo kratko okvir, odnosno model.

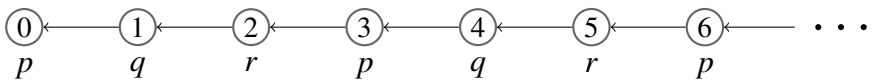
Primjer 1.2.4. *Navodimo primjere nekih modela te ih ilustriramo.*

a) Neka je $\mathfrak{M} = (W, R, V)$ *gdje je* $W = \{1, 2, 3, 4\}$ *i* $R = \{(1,2), (2,3), (3,4), (4,1), (2,2), (4,4)\}$, *a valuacija* V *definirana je sa* $V(p) = \{1, 3\}$, $V(q) = \{3, 4\}$ *i* $V(r) = \emptyset$ *za preostale* $r \in Prop$.



b) Neka je $\mathfrak{M} = (W, R, V)$ *gdje je* $W = \mathbb{N}$, *relacija* R *definirana je s* $xRy \overset{def}{\Longleftrightarrow} x = y + 1$, *a valuacija* V *definirana je sa*

- $V(p) = \{n \in \mathbb{N} \mid n \equiv 0 \ (mod\ 3)\}$
- $V(q) = \{n \in \mathbb{N} \mid n \equiv 1 \ (mod\ 3)\}$
- $V(r) = \{n \in \mathbb{N} \mid n \equiv 2 \ (mod\ 3)\}$
- $V(s) = \emptyset$, *za preostale* $s \in Prop$



Skup $V(p)$ zapravo nam govori na kojim je svjetovima propozicionalna varijabla p istinita. Iz toga se na očekivan način definicija istinitosti na svijetu proširuje na proizvoljne formule. Sada ćemo pojam istinitosti formule na svijetu i formalno definirati.

Definicija 1.2.5. *Neka je* $\mathfrak{M} = (W, R, V)$ *model i neka je* $w \in W$ *svijet.* ***Istinitost formule*** φ ***na svijetu*** w ***iz modela*** $\mathfrak{M}$, *u oznaci* $\mathfrak{M}, w \Vdash \varphi$, *definiramo rekurzivno na sljedeći način:*

- $\mathfrak{M}, w \Vdash p$ *ako i samo ako* $w \in V(p)$, *za svaki* $p \in Prop$

- $\mathfrak{M}, w \nVdash \bot$
- $\mathfrak{M}, w \Vdash \neg\varphi$ *ako i samo ako nije* $\mathfrak{M}, w \Vdash \varphi$
- $\mathfrak{M}, w \Vdash \varphi \vee \psi$ *ako i samo ako* $\mathfrak{M}, w \Vdash \varphi$ *ili* $\mathfrak{M}, w \Vdash \psi$
- $\mathfrak{M}, w \Vdash \Diamond\varphi$ *ako i samo ako postoji* $v \in W$ *takav da vrijedi* wRv *i* $\mathfrak{M}, v \Vdash \varphi$

Kažemo da je formula φ ***globalno istinita na modelu*** $\mathfrak{M}$ *ako je istinita na svakom svijetu modela* $\mathfrak{M}$*. To označavamo sa* $\mathfrak{M} \Vdash \varphi$*.*
Kažemo da je formula φ ***ispunjiva na modelu*** $\mathfrak{M}$ *ako je istinita na nekom svijetu modela* $\mathfrak{M}$*.*
Kažemo da je formula φ ***oboriva na modelu*** $\mathfrak{M}$ *ako je njena negacija* $\neg\varphi$ *ispunjiva na modelu* $\mathfrak{M}$*.*

Napomena 1.2.6. *Ako vrijedi* $\mathfrak{M}, w \Vdash p$ *za neku* $p \in Prop$*, kažemo i da svijet w forsira propozicionalnu varijablu p.*

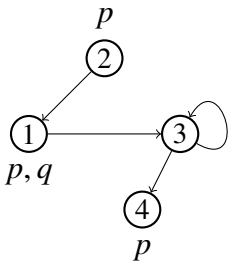
Napomena 1.2.7. *Iz definicije modalnog operatora* $\Box$ *lako se vidi da vrijedi sljedeća tvrdnja:*

$$\mathfrak{M}, w \Vdash \Box\varphi \text{ ako i samo ako za svaki svijet } v \in W \text{ takav da } wRv \text{ vrijedi } \mathfrak{M}, v \Vdash \varphi.$$

Primjer 1.2.8. *Neka je* $\mathfrak{M} = (W, R, V)$ *model gdje je* $W = \{1, 2, 3, 4\}$*, relacija dostižívosti je* $R = \{(1,3), (2,1), (3,3), (3,4)\}$*, a valuacija V zadana je sa* $V(p) = \{1, 2\}$*,* $V(q) = \{1, 4\}$ *i* $V(r) = \emptyset$ *za preostale propozicionalne varijable* $r \in Prop$*. Tada vrijedi:*

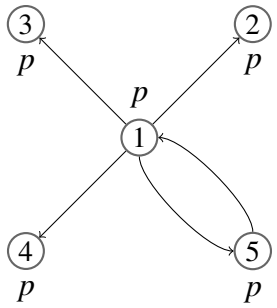
- $\mathfrak{M}, 1 \Vdash \neg\Diamond p \vee \Diamond\neg q$
- $\mathfrak{M}, 2 \nVdash \neg\Diamond p \vee \Diamond\neg q$
- $\mathfrak{M}, 3 \Vdash \neg\Diamond p \wedge \Diamond\neg q$

Na sljedećoj slici ilustriran je model $\mathfrak{M}$*.*

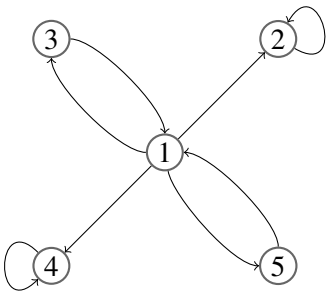


Definicija 1.2.9. *Kažemo da je formula φ **valjana na svijetu** w **u okviru** $\mathfrak{F}$ ako za svaku valuaciju V vrijedi $(\mathfrak{F}, V), w \Vdash \varphi$.*
*Kažemo da je formula φ **valjana na okviru** $\mathfrak{F}$ ako je valjana na svakom svijetu okvira $\mathfrak{F}$.*
*Kažemo da je formula φ **valjana** ako je valjana na svakom okviru.*
*Kažemo da je formula φ **valjana na klasi okvira** F ako je valjana na svakom okviru iz F.*

Primjer 1.2.10. *Neka je $\mathfrak{F} = (W, R)$, gdje je $W = (1, 2, 3, 4, 5)$ i relacija dostiživosti je zadana sa $R = \{(1,2),(1,3),(1,4),(1,5),(5,1)\}$. Tada, primjerice, formula $\varphi \equiv \Box p \to \Diamond p$ nije valjana na okviru $\mathfrak{F}$. Kako bismo to pokazali, promotrimo valuaciju V koja je zadana sa $V(p) = \{1,2,3,4,5\}$. Označimo model $(\mathfrak{F}, V)$ sa $\mathfrak{M}$. Tada za svijet 2 vrijedi $\mathfrak{M}, 2 \Vdash \Box p$ i $\mathfrak{M}, 2 \nVdash \Diamond p$, odnosno $\mathfrak{M}, 2 \nVdash \Box p \to \Diamond p$. Na sljedećoj slici ilustriran je model $\mathfrak{M}$.*



Međutim, ista formula φ valjana je na okviru $\mathfrak{F}' = (W', R')$ gdje je $W' = \{1,2,3,4,5\}$ i relacija dostiživosti je zadana sa $R' = \{(1,2),(1,3),(1,4),(1,5),(2,2),(3,1),(4,4),(5,1)\}$. Na sljedećoj slici ilustriran je okvir $\mathfrak{F}'$.



Štoviše, formula φ valjana je na svakom okviru $\mathfrak{F} = (W, R)$ čija relacija dostiživosti R je neograničena s desna, odnosno za svaki svijet $w \in W$ postoji svijet $v \in W$ takav da je wRv.

Napomena 1.2.11. *Definicije ispunjivosti i valjanosti možemo proširiti i na skupove formula.*
Skup formula Σ istinit je na nekom svijetu w modela $\mathfrak{M}$ ako je svaka formula iz Σ istinita

na w. To označavamo sa $\mathfrak{M}, w \Vdash \Sigma$.
Skup formula Σ *ispunjiv je na modelu* $\mathfrak{M}$ *ako je istinit na nekom svijetu modela* $\mathfrak{M}$.
Skup formula Σ *valjan je na nekom okviru* $\mathfrak{F}$ *ako je svaka formula iz* Σ *valjana na* $\mathfrak{F}$. *To označavamo sa* $\mathfrak{F} \Vdash \Sigma$.
Skup formula Σ *valjan je na klasi okvira* F *ako je svaka formula iz* Σ *valjana na* F. *To označavamo sa* $F \Vdash \Sigma$.

1.3 Normalne modalne logike

Promotrimo sada neke sisteme modalne logike. Prvo definiramo normalnu modalnu logiku te sistem **K** nazvanom po Saulu Kripkeu. Nakon toga, dodavanjem aksioma definiramo nove sisteme. Na kraju točke definiramo pojam konzistentne formule u odnosu na neku logiku Λ.

Definicija 1.3.1. ***Normalna modalna logika*** Λ *je skup formula koji sadrži sve tautologije, sve formule oblika* $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$ *i* $\Diamond\varphi \leftrightarrow \neg\Box\neg\varphi$ *te je zatvoren na pravila izvoda modus ponens, uniformnu supstituciju i generalizaciju.*
Najmanju normalnu modalnu logiku označavamo sa **K**.

U sljedećoj definiciji uvodimo neka proširenja sistema **K** koja ćemo kasnije koristiti.

Definicija 1.3.2. *Redom uvodimo oznake za modalne formule:*

(4) $\equiv \Diamond\Diamond p \to \Diamond p$

(T) $\equiv p \to \Diamond p$

(B) $\equiv p \to \Box\Diamond p$

(.3) $\equiv \Diamond p \wedge \Diamond q \to \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(q \wedge \Diamond p)$

Sa **T** *označavamo proširenje logike* K *aksiomom* (T).

Sa **KB** *označavamo proširenje logike* K *aksiomom* (B).

Sa **K4** *označavamo proširenje logike* K *aksiomom* (4).

Sa **S4** *označavamo proširenje logike* K *aksiomima* (T) *i* (4).

Sa **S4.3** *označavamo proširenje logike* K *aksiomima* (T), (4) *i* (.3).

Sa **S5** *označavamo proširenje logike* K *aksiomima* (T), (4) *i* (B).

Kasnije ćemo pokazati da formule navedene u definiciji 1.3.2 zapravo opisuju relaciju dostiživosti okvira na kojima su valjane.

Definicija 1.3.3. *Neka je* Λ *normalna modalna logika i* $\mathfrak{F} = (W, R)$ *proizvoljan okvir. Okvir* $\mathfrak{F}$ *nazivamo* Λ***–okvir*** *ako vrijedi* $\mathfrak{F} \Vdash \Lambda$*. Model baziran na* Λ*–okviru nazivamo* Λ*–model. Ako je formula* φ *ispunjiva na nekom* Λ*–modelu, kažemo da je* φ Λ*–ispunjiva.*

Neka je Λ normalna modalna logika. Pojam Λ-dokaza i Λ-dokazivosti formule definira se standardno kao i u logici sudova. Pišemo $\vdash_\Lambda \varphi$ ako je formula φ Λ-dokaziva.

Definicija 1.3.4. *Neka je* Γ *skup formula, a* φ *proizvoljna formula. Neka je* Λ *normalna modalna logika. Kažemo da je formula* φ ***izvodiva iz skupa*** Γ ***u logici*** Λ *ili* Λ***-izvediva iz skupa*** Γ *ako vrijedi jedno od sljedećeg:*

a) $\vdash_\Lambda \varphi$

b) postoje formule $\psi_1, \ldots, \psi_n \in \Gamma$ *takve da vrijedi* $\vdash_\Lambda (\psi_1 \wedge \cdots \wedge \psi_n) \to \varphi$

U tom slučaju pišemo $\Gamma \vdash_\Lambda \varphi$*. U suprotnom pišemo* $\Gamma \nvdash_\Lambda \varphi$*.*
Za skup formula Γ *kažemo da je* Λ***-konzistentan*** *ako vrijedi* $\Gamma \nvdash_\Lambda \bot$*. Inače kažemo da je* Λ*–nekonzistentan.*
Formula φ *je* Λ*-konzistentna ako ja skup* $\{\varphi\}$ Λ*-konzistentan.*

1.4 Osnove teorije modela modalne logike

U točki 1.2 definirali smo okvire i modele te istinitost na modelima i valjanost na okvirima. Možemo se pitati kada će to svojstvo biti očuvano. Primjerice, ako je formula φ valjana na okviru $\mathfrak{F} = (W, R)$, hoće li φ biti valjana i na okviru $\mathfrak{F}' = (W', R')$ gdje je $W' \subseteq W$, a relacija dostiživosti R' je restrikcija od R na W'.

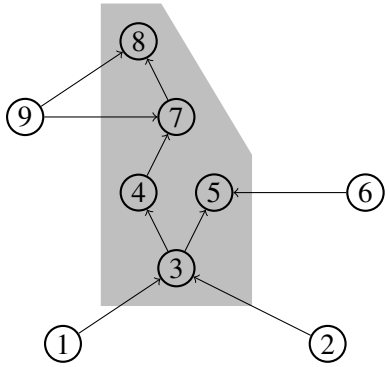
U ovoj točki definiramo generirane podmodele, odnosno okvire i ograničene morfizme te dokazujemo da čuvaju istinitost i valjanost. Također definiramo i jake homomorfizme i izomorfizme. Na kraju točke definiramo svojstvo konačnih okvira i svojstvo konačnih modela. Najprije definiramo generirane podmodele.

Definicija 1.4.1. *Neka su* $\mathfrak{M} = (W, R, V)$ *i* $\mathfrak{M}' = (W', R', V')$ *modeli. Kažemo da je* $\mathfrak{M}'$ ***podmodel*** *od* $\mathfrak{M}$ *ako je* $W' \subseteq W$*,* R' *je restrikcija od* R *na* W' *te za svaki* $p \in Prop$ *vrijedi* $V'(p) = V(p) \cap W'$*.*
Kažemo da je $\mathfrak{M}'$ ***generirani podmodel*** *modela* $\mathfrak{M}$ *ako je* $\mathfrak{M}'$ *podmodel od* $\mathfrak{M}$ *i za svaki* $w \in W'$ *i svaki* $v \in W$ *vrijedi da* wRv *povlači* $v \in W'$*.*
Ako je $X \subseteq W$ *definiramo* ***podmodel generiran s*** X *kao najmanji podmodel od* $\mathfrak{M}$ *čija domena sadrži* X*.*

Kažemo da je $\mathfrak{M}$ ***model s korijenom*** *ako je generiran jednočlanim skupom čiji element zovemo* ***korijen modela****.*

Na analogan se način definira pojam podokvira i generiranih podokvira.

Primjer 1.4.2. *Neka je* $\mathfrak{M} = (W, R, V)$ *gdje je* $W = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$*, relacija dostižívosti zadana je sa* $R = \{(1, 3), (2, 3), (3, 4), (3, 5), (6, 5), (4, 7), (7, 8), (9, 7), (9, 8)\}$ *te je* $V(p) = \emptyset$ *za svaku propozicionalnu varijablu* p*.*
Tada je $\mathfrak{M}' = (W', R', V')$ *gdje je* $W' = \{3, 4, 5, 7, 8\}$ *i* $R = \{(3, 4), (3, 5), (4, 7), (7, 8)\}$ *jedan generirani podmodel modela* $\mathfrak{M}$ *s korijenom* 3*. Na sljedećoj slici ilustriran je model* $\mathfrak{M}$ *te je sivom bojom označen model* $\mathfrak{M}'$*.*



Primijetimo da za svaki svijet w generiranog podmodela s korijenom w_0 vrijedi w_0Rw ili postoje svjetovi $w_1, \ldots, w_k$ takvi da vrijedi $w_0Rw_1R \ldots Rw_kRw$.

Definicija 1.4.3. *Neka je* $\mathfrak{M} = (W, R, V)$ *Kripkeov model i* S *proizvoljan neprazan podskup od* W*. Sa* $\mathfrak{M} \restriction S$ *označavamo podmodel od* $\mathfrak{M}$ *čiji je nosač skup* S*, pripadna relacija dostižívosti je restrikcija relacije* R *na skup* S*, a pripadna valuacija je restrikcija valuacije* V *na skup* S*.*

Neka je $\mathfrak{M} = (W, R, V)$ gdje je $W = \{1, 2\}$, relacija dostižívosti je $R = \{(1, 1), (1, 2)\}$ te je valuacija V zadana s $V(p) = \{2\}$. Lako se vidi da vrijedi $\mathfrak{M}, 1 \Vdash \Diamond p$. Neka je $\mathfrak{M}' = \mathfrak{M} \restriction \{1\}$. Očito vrijedi $\mathfrak{M}', 1 \nVdash \Diamond p$. Dakle, proizvoljni podmodeli ne čuvaju istinitost. Međutim, generirani podmodeli čuvaju istinitost što dokazujemo sljedećom propozicijom.

Propozicija 1.4.4. *Neka je* $\mathfrak{M} = (W, R, V)$ *model i* $\mathfrak{M}' = (W', R', V')$ *generirani podmodel od* $\mathfrak{M}$*. Tada za svaku formulu* φ *i svaki svijet* $w \in W'$ *vrijedi sljedeća ekvivalencija:*

$$\mathfrak{M}, w \Vdash \varphi \text{ ako i samo ako } \mathfrak{M}', w \Vdash \varphi$$

Dokaz. Tvrdnju dokazujemo indukcijom po složenosti formule φ.

Pretpostavimo prvo da je formula φ složenosti 0. Tada je $\varphi \equiv \bot$ ili $\varphi \equiv p$, gdje je $p \in Prop$. Ako je $\varphi \equiv \bot$, tada vrijedi $\mathfrak{M}, w \nVdash \bot$ i $\mathfrak{M}', w \nVdash \bot$. Ako je $\varphi \equiv p$, tada vrijedi $\mathfrak{M}, w \Vdash \varphi$ ako i samo ako $\mathfrak{M}', w \Vdash \varphi$ jer je $w \in W'$ i $V'(p)$ je restrikcija od $V(p)$ na W'.

Pretpostavimo da je $n \in \mathbb{N}$ takav da za sva formule složenosti strogo manje od n vrijedi tvrdnja. Neka je φ neka formula složenosti n.

Promatramo slučajeve obzirom na oblik formule φ . Promotrimo prvo slučaj kada imamo $\varphi \equiv \phi \vee \psi$. Očito su formule ϕ i ψ složenosti strogo manje od n pa za njih vrijedi pretpostavka indukcije. Vrijede sljedeće ekvivalencije:

$$\begin{array}{lll} \mathfrak{M}, w \Vdash \phi \vee \psi & \text{ako i samo ako} & \mathfrak{M}, w \Vdash \phi \text{ ili } \mathfrak{M}, w \Vdash \psi \\ & \text{ako i samo ako} & \mathfrak{M}', w \Vdash \phi \text{ ili } \mathfrak{M}', w \Vdash \psi \\ & \text{ako i samo ako} & \mathfrak{M}', w \Vdash \phi \vee \psi \end{array}$$

Na sličan se način dokaže slučaj kada imamo $\varphi \equiv \neg\phi$.

Promotrimo sada slučaj kada imamo $\varphi \equiv \Diamond\phi$. Pretpostavimo prvo da vrijedi $\mathfrak{M}, w \Vdash \varphi$. Tada postoji svijet v takav da je wRv i $\mathfrak{M}, v \Vdash \phi$. Formula ϕ je složenosti $n-1$ pa po pretpostavci indukcije vrijedi $\mathfrak{M}, w \Vdash \phi$. Budući da je $w \in W'$ i wRv, po definiciji generiranog podmodela vrijedi $v \in W'$. Po definiciji generiranog podmodela je R' restrikcija od R na W' pa vrijedi $wR'v$. Time imamo $\mathfrak{M}', w \Vdash \Diamond\phi$.

Dokažimo sada obratnu implikaciju. Pretpostavimo da vrijedi $\mathfrak{M}', w \Vdash \varphi$. Tada postoji svijet $v \in W'$ takav da je $wR'v$ i $\mathfrak{M}', v \Vdash \phi$. Formula ϕ je složenosti $n-1$ pa po pretpostavci indukcije vrijedi $\mathfrak{M}, v \Vdash \phi$. Iz definicije generiranog podmodela znamo da vrijedi $W' \subseteq W$ i $R' \subseteq R$. Iz toga slijedi da imamo $v \in W$ i wRv, a onda i $\mathfrak{M}, w \Vdash \Diamond\phi$. □

Napomena 1.4.5. *Iz propozicije 1.4.4 slijedi da generirani podmodeli čuvaju istinitost na modelima, odnosno vrijedi sljedeća ekvivalencija: $\mathfrak{M} \Vdash \varphi$ ako i samo ako $\mathfrak{M}' \Vdash \varphi$. Iz toga lako slijedi da generirani podokviri čuvaju valjanost na okvirima.*

Definicija 1.4.6. *Neka su $\mathfrak{M} = (W, R)$ i $\mathfrak{M}' = (W', R')$ dva modela. Funkcija $f\colon W \to W'$ je* **jaki homomorfizam** *između modela ako vrijedi:*

(i) svi svjetovi w i $f(w)$ forsiraju iste propozicionalne varijable

(ii) vrijedi wRv ako i samo ako vrijedi $f(w)R'f(v)$

Za jaki homomorfizam $f\colon W \to W'$ kažemo da je ***izomorfizam*** *ako je f bijekcija.*

Definicija 1.4.7. *Neka su $\mathfrak{M} = (W, R)$ i $\mathfrak{M}' = (W', R')$ dva modela. Funkcija $f\colon W \to W'$ je* **ograničeni morfizam** *između modela ako vrijedi:*

(at) svi svjetovi w i $f(w)$ forsiraju iste propozicionalne varijable

(forth) ako wRv tada vrijedi i $f(w)R'f(v)$

(back) ako $f(w)R'v'$ *tada postoji* $v \in W$ *takav da vrijedi* wRv *i* $f(v) = v'$

Ako je f *surjekcija, tada model* $\mathfrak{M}'$ *zovemo* ***homomorfnom ograničenom slikom*** *modela* $\mathfrak{M}$ *i to označavamo sa* $\mathfrak{M} \twoheadrightarrow \mathfrak{M}'$.

Sljedeća propozicija dokazuje se na sasvim analogan način kao propozicija 1.4.4, a govori da ograničeni morfizmi čuvaju istinitost.

Propozicija 1.4.8. *Neka su* $\mathfrak{M} = (W, R)$ *i* $\mathfrak{M}' = (W', R')$ *modeli te neka je funkcija* $f\colon W \to W'$ *ograničeni morfizam. Tada za svaku formulu* φ *i svaki svijet* $w \in W$ *vrijedi sljedeća ekvivalencija:*

$$\mathfrak{M}, w \Vdash \varphi \text{ ako i samo ako } \mathfrak{M}', f(w) \Vdash \varphi$$

Jaki homomorfizam između dva okvira $\mathfrak{F} = (W, R)$ i $\mathfrak{F}' = (W', R')$ definiramo na način da u definiciji 1.4.6 ispustimo uvjet (i).

Ograničeni morfizam između dva okvira $\mathfrak{F} = (W, R)$ i $\mathfrak{F}' = (W', R')$ definiramo na način da u definiciji 1.4.7 ispustimo uvjet (at). Ako je funkcija $f\colon W \to W'$ ograničeni morfizam okvira i surjekcija, tada kažemo da je okvir $\mathfrak{F}'$ **homomorfna ograničena slika** okvira $\mathfrak{F}$ i to označavamo sa $\mathfrak{F} \twoheadrightarrow \mathfrak{F}'$.

Napomena 1.4.9. *Iz propozicije 1.4.8 slijedi da ograničeni morfizmi čuvaju istinitost na modelima, odnosno vrijedi sljedeća ekvivalencija:* $\mathfrak{M} \Vdash \varphi$ *ako i samo ako* $\mathfrak{M}' \Vdash \varphi$. *Lako je vidjeti da iz toga onda slijedi da ograničeni morfizmi čuvaju valjanost na okvirima.*

Lako je smisliti primjer formule logike prvog reda koja je istinita samo na beskonačnim strukturama. Postavlja se pitanje postoje li takve formule i u modalnoj logici. Može se pokazati da je odgovor negativan, odnosno da je svaka ispunjiva formula ispunjiva na konačnom modelu. Štoviše, može se pokazati da je svaka ispunjiva formula φ ispunjiva na modelu veličine $2^{|\varphi|}$. Iz tog razloga kažemo da osnovni modalni jezik ima svojstvo konačnih modela. Svojstvo konačnih modela možemo definirati i za normalne modalne logike.

Definicija 1.4.10. *Neka je* Λ *normalna modalna logika, a* M *proizvoljna klasa konačnih modela. Kažemo da* Λ *ima svojstvo konačnih modela u odnosu na klasu modela* M *ako vrijedi* $M \Vdash \Lambda$ *i svaka formula* $\varphi \notin \Lambda$ *je oboriva na nekom modelu iz klase* M.

Kažemo da Λ *ima* ***svojstvo konačnih modela*** *ako ima svojstvo konačnih modela u odnosu na neku klasu konačnih modela.*

Slično se definira i svojstvo konačnih okvira.

Definicija 1.4.11. *Neka je* Λ *normalna modalna logika, a* F *proizvoljna klasa konačnih okvira. Kažemo da logika* Λ *ima svojstvo konačnih okvira u odnosu na klasu okvira* F *ako vrijedi* $F \Vdash \Lambda$ *i svaka formula* $\varphi \notin \Lambda$ *je oboriva na nekom okviru iz klase* F.

Kažemo da logika Λ ima ***svojstvo konačnih okvira*** *ako ima svojstvo konačnih okvira u odnosu na neku klasu konačnih okvira.*

Propozicija 1.4.12. *Neka je Λ proizvoljna normalna modalna logika. Ako Λ ima svojstvo konačnih okvira, tada ima i svojstvo konačnih modela.*

Dokaz. Neka je Λ proizvoljna normalna logika koja ima svojstvo konačnih okvira. Tada postoji klasa konačnih okvira F takva da $F \Vdash \Lambda$ i svaka formula $\varphi \notin \Lambda$ je oboriva na nekom okviru $\mathfrak{F}$ iz klase F. Označimo sa M klasu modela $\{(\mathfrak{F}, V) \mid \mathfrak{F} \in F,\ V \text{ je proizvoljna valuacija}\}$. Očito je M klasa konačnih modela i vrijedi $M \Vdash \Lambda$. Neka je $\varphi \notin \Lambda$. Tada postoji okvir $\mathfrak{F} \in F$ takav da $\mathfrak{F} \nVdash \varphi$. Tada postoji svijet w i valuacija V takvi da $(\mathfrak{F}, V), w \nVdash \varphi$. Sada je $(\mathfrak{F}, V)$ model iz klase M na kojem je formula φ oboriva. Dakle, Λ ima svojstvo konačnih modela. □

Napomena 1.4.13. *Zapravo vrijedi i obrat propozicije 1.4.12: ako Λ ima svojstvo konačnih modela, tada ima i svojstvo konačnih okvira. Međutim, ta nam tvrdnja neće trebati u radu pa ju ni ne dokazujemo. Dokaz se može pronaći u [1].*

1.5 Karakteristične klase okvira

U definiciji 1.3.2, sistemu **K** dodavali smo određene formule te smo tako dobili nove sisteme modalne logike. Sada ćemo pokazati da svaka formula iz navedene definicije opisuje neko svojstvo relacije dostiživosti te da je valjana samo na okvirima čija relacija dostiživosti ima to svojstvo. Primjerice, pokazat ćemo da formula $p \to \Diamond p$ opisuje refleksivnost relacije dostiživosti te je valjana samo na okvirima čija relacija dostiživosti je refleksivna.

Propozicija 1.5.1. *Za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash p \to \Diamond p \ \text{ ako i samo ako relacija } \ R \ \text{ je refleksivna.}$$

Dokaz. Pretpostavimo prvo da relacija R nije refleksivna. Tada postoji svijet $w \in W$ takav da ne vrijedi wRw. Definiramo valuaciju V na okviru $\mathfrak{F}$ sa $V(p) = \{w\}$, gdje je p proizvoljna propozicionalna varijabla. Očito vrijedi $w \Vdash p$ te je lako vidjeti da imamo $w \nVdash \Diamond p$. Time imamo $\mathfrak{F} \nVdash p \to \Diamond p$.

Pretpostavimo sada da je R refleksivna relacija. Neka je V proizvoljna valuacija na okviru $\mathfrak{F}$ i neka je $w \in W$ proizvoljan svijet. Ako vrijedi $w \nVdash p$ tada očito vrijedi $w \Vdash p \to \Diamond p$. Promotrimo sada slučaj kada vrijedi $w \Vdash p$. Iz refleksivnosti relacije R slijedi $w \Vdash \Diamond p$. Time smo pokazali da vrijedi $w \Vdash p \to \Diamond p$. Kako je svijet w bio proizvoljan, zaključujemo da vrijedi $\mathfrak{F} \Vdash p \to \Diamond p$. □

Kripkeov okvir čija je relacija dostiživosti refleksivna nazivamo **T**–okvir.

Propozicija 1.5.2. *Za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash p \to \Box\Diamond p \text{ ako i samo ako relacija } R \text{ je simetrična.}$$

Dokaz. Pretpostavimo prvo da R nije simetrična relacija. Tada postoje svjetovi $w, v \in W$ takvi da vrijedi wRv i ne vrijedi vRw. Definiramo valuaciju V na okviru $\mathfrak{F}$ sa $V(p) = \{w' \in W \mid \text{ne vrijedi } vRw'\}$. Budući da ne vrijedi vRw tada imamo $w \Vdash p$. Za svaki svijet v' takav da vRv' imamo $v' \nVdash p$. Dakle, vrijedi $v \nVdash \Diamond p$. Kako imamo wRv tada vrijedi $w \nVdash \Box\Diamond p$. Time smo dokazali $w \nVdash p \to \Box\Diamond p$.

Pretpostavimo sada da je R simetrična relacija. Neka je V proizvoljna valuacija na okviru $\mathfrak{F}$ i neka je $w \in W$ proizvoljan svijet. Ako vrijedi $w \nVdash p$ tada očito vrijedi $w \Vdash p \to \Box\Diamond p$. Promotrimo slučaj kada vrijedi $w \Vdash p$. Zbog simetričnosti relacije imamo da za svaki svijet v takav da je wRv također vrijedi i vRw. Budući da $w \Vdash p$, tada vrijedi i $v \Vdash \Diamond p$. Dakle, vrijedi $w \Vdash \Box\Diamond p$, odnosno $w \Vdash p \to \Box\Diamond p$. Kako je svijet w bio proizvoljan, zaključujemo da vrijedi $\mathfrak{F} \Vdash p \to \Box\Diamond p$. □

Kripkeov okvir čija je relacija dostiživosti simetrična nazivamo **KB**–okvir.
Dokaz sljedeće propozicije je sasvim analogna dokazima prethodne dvije propozicije pa ga ispuštamo.

Propozicija 1.5.3. *Za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash \Diamond\Diamond p \to \Diamond p \text{ ako i samo ako relacija } R \text{ je tranzitivna.}$$

Kripkeov okvir čija je relacija dostiživosti tranzitivna nazivamo **K4**–okvir.

Propozicija 1.5.4. *Za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash (T) \wedge (B) \wedge (4) \text{ ako i samo ako relacija } R \text{ je relacija ekvivalencije.}$$

Dokaz. Pretpostavimo da vrijedi $\mathfrak{F} \Vdash (T) \wedge (B) \wedge (4)$. Tada iz propozicija 1.5.1, 1.5.2 i 1.5.3 slijedi redom da je relacija R refleksivna, simetrična i tranzitivna, odnosno da je R relacija ekvivalencije.
Pretpostavimo da je R relacija ekvivalencije. Tada je R refleksivna pa iz propozicije 1.5.1 slijeda $\mathfrak{F} \Vdash (T)$. Relacija R je također i simetrična pa iz propozicije 1.5.2 slijedi $\mathfrak{F} \Vdash (B)$. Relacija R je i tranzitivna pa iz propozicije 1.5.3 slijedi $\mathfrak{F} \Vdash (4)$. Dakle, vrijedi $\mathfrak{F} \Vdash (T) \wedge (B) \wedge (4)$ □

Kripkeov okvir čija relacija dostiživosti je relacija ekvivalencije nazivamo **S5**–okvir.

Za binarnu relaciju R kažemo da je **bez grananja** ako vrijedi $\forall x \forall y \forall z (xRy \wedge xRz \to (yRz \vee y = z \vee zRy))$.

Za relaciju R kažemo da je **povezana** ako vrijedi $\forall x \forall y(xRy \vee yRx)$.

U nastavku definiramo **S4.3**–okvire. Za neki okvir $\mathfrak{F}$ kažemo da je **S4.3**–okvir ako je to okvir s korijenom generiran iz okvira čija relacija dostiživosti je tranzitivna, refleksivna te bez grananja. Primijetimo još da će relacija dostiživosti proizvoljnog **S4.3**–okvira biti i povezana.

Propozicija 1.5.5. *Za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash (T) \wedge (4) \wedge (.3) \quad \textit{ako i samo ako} \quad \textit{relacija } R \textit{ je refleksivna i tranzitivna te je bez grananja.}$$

Dokaz. Dokažimo prvo da vrijedi sljedeća tvrdnja

$$\mathfrak{F} \Vdash (.3) \text{ ako i samo ako relacija } R \text{ je bez grananja} \tag{1.1}$$

Pretpostavimo da R nije ograničena s desna. Tada postoje svjetovi $w_1, w_2, w_3 \in W$, $w_2 \neq w_3$, takvi da vrijedi w_1Rw_2 i w_1Rw_3 i ne vrijedi w_2Rw_3, a ni w_3Rw_2.

Definiramo valuaciju V sa $V(p) = \{w_2\}$ i $V(q) = \{w_3\}$. Lako se pokaže da vrijedi $w_1 \Vdash \Diamond p \wedge \Diamond q$.
Pretpostavimo sada da vrijedi $w_1 \Vdash \Diamond(p \wedge \Diamond q)$. Tada postoji svijet $w \in W$ takav da je w_1Rw i $w \Vdash p \wedge \Diamond q$. Mora vrijediti $w \Vdash p$ pa iz definicije valuacije V zaključujemo da je $w = w_2$. No iz pretpostavke da relacija R nije ograničena s desna slijedi da ne vrijedi w_2Rw_3, odnosno $w_2 \nVdash \Diamond q$. Dakle, vrijedi $w_1 \nVdash \Diamond(p \wedge \Diamond q)$. Na sličan se način pokaže da vrijedi $w_1 \nVdash \Diamond(p \wedge q)$ i $w_1 \nVdash \Diamond(q \wedge \Diamond p)$. Time imamo $\mathfrak{F} \nVdash \Diamond p \wedge \Diamond q \to \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(q \wedge \Diamond p)$.

Pretpostavimo sada da je relacije R ograničena s desna. Neka je V proizvoljna valuacija na okviru $\mathfrak{F}$ i neka je $w \in W$ proizvoljan svijet. Ako vrijedi $w \nVdash \Diamond p \wedge \Diamond q$, tada očito vrijedi $w \Vdash \Diamond p \wedge \Diamond q \to \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(q \wedge \Diamond p)$. Pretpostavimo da vrijedi $w \Vdash \Diamond p \wedge \Diamond q$. Tada postoje w_1 i w_2 takvi da je wRw_1 i wRw_2 te vrijedi $w_1 \Vdash p$ i $w_2 \Vdash q$. Iz pretpostavke da je relacije R ograničena slijedi da vrijedi barem jedna od sljedećih mogućnosti: w_1Rw_2, $w_1 = w_2$ i w_1Rw_2. Pretpostavimo da vrijedi w_1Rw_2. Tada vrijedi $w_1 \Vdash \Diamond q$, odnosno $w_1 \Vdash p \wedge \Diamond q$. Dakle, vrijedi $w \Vdash \Diamond(p \wedge \Diamond q)$. Time smo pokazali da vrijedi $w \Vdash \Diamond p \wedge \Diamond q \to \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(q \wedge \Diamond p)$. Na sličan se način dokazuju slučajevi $w_1 = w_2$ i w_2Rw_1. Kako je svijet w bio proizvoljan, zaključujemo da vrijedi $\mathfrak{F} \Vdash \Diamond p \wedge \Diamond q \to \Diamond(p \wedge \Diamond q) \vee \Diamond(p \wedge q) \vee \Diamond(q \wedge \Diamond p)$.

Iz propozicije 1.5.1 znamo da vrijedi $\mathfrak{F} \Vdash (T)$ ako i samo ako je R refleksivna. Nadalje, iz propozicije 1.5.3 znamo da vrijedi $\mathfrak{F} \Vdash (4)$ ako i samo ako je R tranzitivna. Sada tvrdnja propozicije slijedi iz navedenih propozicija i tvrdnje 1.1. □

Propozicija 1.5.6. *Neka je $\mathfrak{F} = (W, R)$ okvir s korijenom takav da vrijedi $\mathfrak{F} \Vdash (T) \wedge (4) \wedge (.3)$. Tada je relacija R povezana.*

Dokaz. Neka je w_0 korijen okvira $\mathfrak{F}$. Neka su $w, v \in W$ proizvoljni svjetovi. Tada postoje svjetovi $w_1, \ldots, w_k$ takvi da vrijedi $w_0 R w_1 R \ldots R w_k R w$. Iz tranzitivnosti relacije R slijedi da vrijedi $w_0 R w$. Analogno, vrijedi $w_0 R v$. Kako je R bez grananja, slijedi da vrijedi wRv, $w = v$ ili vRw. Ako vrijedi $w = v$, tada iz refleksivnosti relacije R slijedi wRw. Dakle, relacija R je povezana. □

Napomena 1.5.7. *Neka je $\mathfrak{M} = (W, R, V)$ konačan **S4.3**-model s korijenom w_1. Neka je $\mathfrak{M}' = \mathfrak{M} \restriction W'$, gdje je $W' \subseteq W$ te $w_1 \in W'$. Tada je i $\mathfrak{M}'$ također **S4.3**-model s korijenom w_1. Naime, ako je okvir (W, R) generiran svijetom w_1 iz okvira (W_1, R_1) čija relacija dostižívosti je tranzitivna, refleksivna te bez grananja, tada je okvir modela $\mathfrak{M}'$ generiran svijetom w_1 iz okvira čiji je nosač $W_1 \setminus W''$ gdje je $W'' = W \setminus W'$. Pripadna relacija dostižívosti je tranzitivna, refleksivna te bez grananja kao podrelacija relacije R_1.*

Poglavlje 2

Složenost modalnih logika

Znamo da problem ispunjivosti logike prvog reda nije odlučiv. S druge strane, problem ispunjivosti logike sudova jest odlučiv te je NP–potpun. Zato kažemo da je logika sudova NP–potpuna. Za normalnu modalnu logiku Λ, problem ispunjivosti definiramo kao određivanje je li proizvoljna modalna formula φ Λ–ispunjiva, odnosno postoji li Λ-model na kojem je φ ispunjiva.

U ovom poglavlju dokazujemo nekoliko rezultata o složenosti normalnih modalnih logika. Dokaz odlučivosti logika čiju složenost dokazujemo može se naći u [1]. Prvo promatramo NP–potpune modalne logike. Definiramo polinomno svojstvo konačnih modela te definabilnost klase okvira u logici prvog reda. Koristeći ova dva pojma dokazujemo NP–potpunost logike **S5** te Hemaspaandrin teorem o NP–potpunosti modalnih logika koje proširuju logiku **S4.3**. Zatim promatramo PSPACE–potpune modalne logike. Dokazujemo da logika **K** nema polinomno svojstvo konačnih modela te dokazujemo da problem ispunjivosti logike **K** pripada klasi PSPACE. Nakon toga dokazujemo Ladnerov teorem koji govori da je svaka normalna modalna logika koja je između **K** i **S4** nužno PSPACE–teška. Na kraju poglavlja spominjemo još nekoliko logika i ukratko opisujemo njihovu složenost.

2.1 NP-potpune modalne logike

Iz definicije NP–potpunog problema znamo da je svaki NP–potpun problem NP–težak problem i da pripada klasi NP. NP–teške probleme možemo shvatiti kao probleme koji su teški barem onoliko koliko su teški problemi iz klase NP. Iz Cook–Levinovog teorema znamo da je problem ispunjivosti logike sudova, odnosno problem SAT, jedan NP–potpun problem. Dakle, NP–teški problemi su teški barem onoliko koliko i problem SAT. U ovoj točki bavimo se normalnim modalnim logikama čiji je problem ispunjivosti također NP–potpun problem.

Normalne modalne logike možemo gledati kao proširenje logike sudova. Stoga je problem ispunjivosti svake normalne modalne logike težak barem koliko i problem SAT. Odnosno, problem ispunjivosti svake normalne modalne logike je NP–težak. Dakle, ako želimo odrediti za koje normalne modalne logike je problem ispunjivosti NP–potpun, tada je dovoljno utvrditi koje normalne modalne logike imaju problem ispunjivosti koji pripada klasi NP.

Probleme iz klase NP možemo opisati na sljedeći način: ako postoji rješenje problema, možemo ga pronaći nedeterminističkim polinomnim algoritmom, a točnost rješenja možemo provjeriti determinističkim polinomnim algoritmom. Upravo navedenu činjenicu koristimo u dokazu NP–potpunosti problema ispunjivosti normalne modalne logike **S5** i normalnih modalnih logika koje proširuju **S4.3**.

Prvo dokazujemo jednu tehničku lemu o složenosti algoritma za provjeru ispunjivosti formula normalne modalne logike φ na modelu $\mathfrak{M}$.

Lema 2.1.1. *Neka je $\mathfrak{M} = (W, R, V)$ konačan model i φ proizvoljna formula. Ispunjivost formule φ na modelu $\mathfrak{M}$ može se provjeriti u vremenu $O(|\varphi| \cdot ||\mathfrak{M}||)$ gdje je $||\mathfrak{M}||$ zbroj broja svjetova u nosaču W i broja parova u relaciji R.*

Dokaz. Neka su $\psi_1, \psi_2, \ldots, \psi_m$ potformule od φ poredane rastući po duljini. Sada je $\psi_m \equiv \varphi$ i za svaki i, j, ako je ψ_i potformula od ψ_j, tada je $i < j$. Primijetimo da je $m \leq |\varphi|$.

Indukcijom po m dokazujemo da se u vremenu $O(m \cdot ||\mathfrak{M}||)$ svaki svijet $w \in W$ može označiti sa ψ_j ako je ψ_j istinita na w, odnosno sa $\neg\psi_j$ ako ψ_j nije istinita na w. Zapravo dokazujemo da se u vremenu $O(m \cdot ||\mathfrak{M}||)$ može provjeriti jesu li potformule $\psi_1, \ldots, \psi_m$ od φ ispunjive na modelu $\mathfrak{M}$. Specijalno se tada i ispunjivost od ψ_m može provjeriti u vremenu $O(m \cdot ||\mathfrak{M}||)$, a onda i ispunjivost od formule φ budući da je $\varphi \equiv \psi_m$.

Za $m = 1$ imamo da je $\varphi \equiv \bot$ ili je $\varphi \equiv p$, za neku propozicionalnu varijablu $p \in Prop$. Ako je $\varphi \equiv \bot$ tada svaki svijet modela $\mathfrak{M}$ označimo sa $\neg\varphi$. Ako je $\varphi \equiv p$, svijet w označimo sa φ ako je $w \in V(p)$, odnosno sa $\neg\varphi$ ako je $w \notin V(p)$. U oba nam je slučaja potrebno $O(||\mathfrak{M}||)$ vremena.

Pretpostavimo da tvrdnja vrijedi za neki $m \geq 1$ i neka su $\psi_1, \ldots, \psi_{m+1}$ potformule neke formule φ. Promotrimo slučajeve obzirom na formulu ψ_{m+1}.

Pretpostavimo prvo da je $\psi_{m+1} \equiv \psi_i \vee \psi_j$, gdje je $i, j < m + 1$. Iz pretpostavke indukcije slijedi da je za označavanje modela $\mathfrak{M}$ formulom ψ_i, odnosno formulom ψ_j, potrebno najviše $O(m \cdot ||\mathfrak{M}||)$ vremena. Označavanje modela $\mathfrak{M}$ formulom ψ_{m+1} možemo provesti tako da neki svijet $w \in W$ označimo sa ψ_{m+1} ako je taj svijet w već označen s nekom od dvije formule ψ_i i ψ_j. Za to označavanje modela $\mathfrak{M}$ formulom ψ_{m+1} treba $O(||\mathfrak{M}||)$ vremena. Dakle, sveukupno je potrebno za označavanje $O(m \cdot ||\mathfrak{M}||) + O(||\mathfrak{M}||)$ vremena, tj. $O((m + 1) \cdot ||\mathfrak{M}||)$ vremena.

Na sličan se način dokazuje slučaj $\psi_{m+1} \equiv \neg\psi_i,\ i < m+1$.

Pretpostavimo sada da je $\psi_{m+1} \equiv \Diamond\psi_i$, gdje je $i < m+1$. Iz pretpostavke indukcije slijedi da model $\mathfrak{M}$ možemo označiti formulom ψ_i u najviše $O(m \cdot \|\mathfrak{M}\|)$ vremena. Tada označavanje modela formulom $\Diamond\psi_i$ možemo provesti tako da neki svijet $w \in W$ označimo sa ψ_{m+1} ako postoji svijet $v \in W$ koji je označen formulom ψ_i i vrijedi wRv. Za to označavanje modela formulom ψ_{m+1} potrebno je najviše $O(\|\mathfrak{M}\|)$ vremena. Dakle, ukupno je potrebno $O((m+1) \cdot \|\mathfrak{M}\|)$ vremena.

Budući da je $m \leq |\varphi|$ tada se ispunjivost formule φ na modelu $\mathfrak{M}$ može provjeriti u vremenu $O(|\varphi| \cdot \|\mathfrak{M}\|)$. □

U prvom poglavlju definirali smo pojam svojstva konačnih modela. Ovo svojstvo, uz još neke pretpostavke, dovoljno je da se pokaže odlučivost nekih normalnih modalnih logika ([1]). Međutim, konačan model, čija egzistencija slijedi iz svojstva konačnih modela, može biti proizvoljno velik. Ako veličina modela ovisi eksponencijalno o duljini formule, iz leme 2.1.1 slijedi da je tada algoritam za provjeru ispunjivosti proizvoljne formule na zadanom modelu eksponencijalne složenosti. No, nama je potreban algoritam polinomne vremenske složenosti. Iz tog razloga razmatrat ćemo nešto jače svojstvo koje se naziva polinomno svojstvo konačnih modela. To svojstvo navodimo u sljedećoj definiciji. No, prije uvodimo dvije oznake.

Ako je M neka klasa Kripkeovih modela, tada sa Λ_M označavamo skup svih modalnih formula koje su istinite na svakom modelu iz klase M.

Ako je F neka klasa Kripkeovih okvira, tada a Λ_F označavamo skup svih modalnih formula koje su valjane na svakom okviru iz klase F.

Definicija 2.1.2. *Neka je Λ normalna modalna logika i M skup konačnih modela tako da vrijedi $\Lambda = \Lambda_M$, a $f : \mathbb{N} \to \mathbb{N}$ neka funkcija.*

Kažemo da logika Λ ima ***svojstvo konačnih modela reda f(n)*** *u odnosu na skup modela M ako je svaka Λ–konzistentna formula φ ispunjiva na nekom modelu iz skupa modela M koji sadrži najviše $f(|\varphi|)$ svjetova.*

Kažemo da logika Λ ima ***polinomno svojstvo konačnih modela*** *u odnosu na skup modela M ako postoji polinom p takav da Λ ima svojstvo konačnih modela reda $p(n)$ u odnosu na skup modela M.*

Kažemo da logika Λ ima ***polinomno svojstvo konačnih modela*** *ako postoji skup M konačnih modela tako da je $\Lambda = \Lambda_M$ i logika Λ ima polinomno svojstvo konačnih modela u odnosu na skup modela M.*

U definiciji 1.4.11 definirali smo svojstvo konačnih okvira. Sada ga definiramo na jednostavniji način.

Lema 2.1.3. *Neka je Λ normalna modalna logika, a F klasa konačnih okvira. Tada Λ ima svojstvo konačnih okvira ako i samo ako je $\Lambda = \Lambda_F$.*

Dokaz. Ako Λ ima svojstvo konačnih okvira u odnosu na F, tada vrijedi $F \Vdash \Lambda$ te za svaku formulu $\varphi \notin \Lambda$ postoji okvir $\mathfrak{F} \in F$ takav da $\mathfrak{F} \nVdash \varphi$. Iz $F \Vdash \Lambda$ slijedi $\Lambda \subseteq \Lambda_F$. Kada bi vrijedilo $\Lambda \subset \Lambda_F$, tada bi postojala formula ψ takva da je $\psi \in \Lambda_F$ i $\psi \notin \Lambda$. Odnosno, vrijedilo bi $\psi \notin \Lambda$ i za svaki okvir $\mathfrak{F} \in F$ vrijedilo bi $\mathfrak{F} \Vdash \psi$ što je kontradikcija s definicijom svojstva konačnih okvira.
Obratno, ako je $\Lambda = \Lambda_F$, tada vrijedi $F \Vdash \Lambda$. Kada bi postojala formula φ takvda da $\varphi \notin \Lambda$ i $F \Vdash \varphi$, tada bi vrijedilo $\Lambda \subset \Lambda_F$ što je kontradikcija. □

Sada možemo dokazati lemu koja nam govori koja svojstva trebaju zadovoljavati normalne modalne logike čiji problem ispunjivosti je NP–potpun.

Lema 2.1.4. *Neka je Λ konzistentna normalna modalna logika koja ima polinomno svojstvo konačnih modela u odnosu na neku klasu modela* M*. Ako je problem odlučivanja je li $\mathfrak{M} \in$ M odlučiv u polinomnom vremenu u odnosu na $|\mathfrak{M}|$, tada je problem ispunjivosti logike Λ NP–potpun.*

Dokaz. Kao što je prije već bilo spomenuto, znamo da je problem ispunjivosti svake normalne modalne logike, a onda i logike Λ, jedan NP–težak problem. Preostalo je dokazati da problem ispunjivosti za logiku Λ pripada klasi NP.

Za zadanu formulu φ prvo nedeterministički konstruiramo model $\mathfrak{M} = (W, R, V)$ čija je veličina polinomna u odnosu na $|\varphi|$. Kako je $\mathfrak{M}$ konačan model, tada iz leme 2.1.1 slijedi da se ispunjivost formule φ na $\mathfrak{M}$ može provjeriti u vremenu $O(|\varphi| \cdot \|\mathfrak{M}\|)$ gdje je $\|\mathfrak{M}\|$ zbroj broja svjetova u W i broja parova u R.

Kako je po pretpostavci leme veličina modela $\mathfrak{M}$ polinomna u odnosu na $|\varphi|$, također je i veličina $\|\mathfrak{M}\|$ polinomna u odnosu na $|\varphi|$. Stoga se ispunjivost formule φ na modelu $\mathfrak{M}$ može provjeriti u polinomnom vremenu u odnosu na $|\varphi|$.

Primijetimo da je moguće u polinomnom vremenu u odnosu na $|\varphi|$ provjeriti je li $\mathfrak{M} \in$ M. To slijedi iz činjenice da je veličina $|\mathfrak{M}|$ polinomna u odnosu na $|\varphi|$ te iz pretpostavke leme koja kaže da u polinomnom vremenu u odnosu na $|\mathfrak{M}|$ možemo provjeriti je li $\mathfrak{M} \in$ M. □

Napomena 2.1.5. *Zašto u prethodnoj lemi nije dovoljno da Λ ima polinomno svojstvo konačnih modela nego nam treba i pretpostavka da se u polinomnom vremenu može odrediti je li $\mathfrak{M} \in M$? Razlog tome je što postoji neprebrojivo mnogo normalnih modalnih logika koje imaju polinomno svojstvo konačnih modela, a odlučivih normalnih modalnih logika je prebrojivo mnogo. Stoga polinomno svojstvo konačnih modela ne osigurava ni odlučivost, a onda ne može osigurati ni pripadnost klasi NP.*

Pokazat ćemo za koje je normalne modalne logike problem odlučivanja je li $\mathfrak{M} \in M$ odlučiv u polinomnom vremenu. No prije toga moramo još razmotriti vezu Kripkeovih okvira i σ-struktura logike prvog reda.

Svaki okvir $\mathfrak{F} = (W, R)$ možemo promatrati kao σ-strukturu logike prvog reda. Signatura σ sadrži točno dva binarna relacijska simbola: simbol = i simbol Q koji se interpretira relacijom dostiživosti R. Želimo još naglasiti da svaki okvir promatramo kao normalni model, odnosno σ-strukturu u kojoj se simbol = interpretira relacijom jednakosti.

Ako je $\mathfrak{F}$ okvir i A neka σ-formula, tada sa $\mathfrak{F} \models A$ označavamo istinitost formule A na strukturi $\mathfrak{F}$.

Definicija 2.1.6. *Kažemo da je klasa okvira* F ***definabilna u logici prvog*** *reda ako postoji σ–rečenica A logike prvog reda tako da za svaki okvir $\mathfrak{F} = (W, R)$ vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \in \mathrm{F} \text{ ako i samo ako } \mathfrak{F} \models A$$

Primjer 2.1.7. *Promotrimo neke klase okvira koje su definabilne u logici prvog reda:*

a) *Klasa svih refleksivnih okvira definabilna je rečenicom $\forall x\, xRx$.*

b) *Klasa svih simetričnih okvira definabilna je rečenicom $\forall x \forall y(xRy \to yRx)$.*

c) *Klasa svih tranzitivnih okvira definabilna je rečenicom $\forall x \forall y \forall z(xRy \wedge yRz \to xRz)$.*

d) *Klasa svih okvira bez grananja definabilna je rečenicom $\forall x \forall y \forall z(xRy \wedge xRz \to (yRz \vee y = z \vee zRy))$.*

e) *Klasa svih **S5** okvira definabilna je rečenicom nastalom konjunkcijom rečenica iz* a), b) *i* c).

f) *Klasa svih **S4.3** okvira definabilna je rečenicom nastalom konjunkcijom rečenica iz ie* a), c) *i* d).

Lema 2.1.8. *Neka je* F *klasa konačnih okvira koja je definabilana u logici prvog reda. Problem odlučivanja vrijedi li $\mathfrak{F} \in$ F odlučiv je u polinomnom vremenu u odnosu na veličinu okvira $\mathfrak{F}$.*

Dokaz. Neka je A formula logike prvog reda koja definira klasu okvira F.

Iz definicije definabilnosti klase okvira u logici prvog reda slijedi da je dovoljno dokazati da postoji polinomni vremenski algoritam (u odnosu na veličinu okvira) koji za zadani konačni okvir $\mathfrak{F}$ provjerava vrijedi li $\mathfrak{F} \models A$.

Indukcijom po složenosti formule A dokazujemo da se istinitost formule A logike prvog reda na nekoj σ–strukturi $\mathfrak{F}$ može provjeriti u vremenu $O(|A| \cdot |\mathfrak{F}|^{m+l+2})$ gdje je m broj individualnih varijabli u A, a l broj egzistencijalnih kvntifikatora u A.

Pretpostavimo da je formula A složenosti 0. Tada je A atomarna formula, odnosno $A \equiv xQy$. Dakle, broj individualnih varijabli je jednak 2, a broj kvantifikatora je jednak

0. Neka je v proizvoljna valuacija. Vrijedi $\mathfrak{F} \models A$ ako je $(v(x), v(y)) \in R$, što možemo provjeriti u $O(|\mathfrak{F}|^2)$ vremena. Kako imamo $|\mathfrak{F}|^2$ parcijalnih valuacija čija je domena $\{x, y\}$, tada vrijedi tražena tvrdnja.

Neka je $n \in \mathbb{N}$ takav da tvrdnja vrijedi za sve formule složenosti strogo manje od n. Neka je A formula složenosti n u kojoj je m individualnih varijabli i l egzistencijalnih kvantifikatora. Promatramo tri slučaja obzirom na strukturu od A.

Pretpostavimo prvo da imamo $A \equiv \neg B$. Tada imamo $\mathfrak{F} \models A$ ako $\mathfrak{F} \not\models B$. Primijetimo da u formuli B ima m individualnih varijabli i l egzistencijalnih kvantifikatora. Formula B je složenosti $n-1$ pa po pretpostavci indukcije možemo u vremenu $O(|B| \cdot |\mathfrak{F}|^{m+l+2})$ provjeriti vrijedi li $\mathfrak{F} \not\models B$. Kako je $|A| = |B| + 1$, možemo provjeriti vrijedi li $\mathfrak{F} \models A$ u najviše $O(|A| \cdot |\mathfrak{F}|^{m+l+2})$ vremena.

Neka sada vrijedi $A \equiv B_1 \vee B_2$. Pretpostavimo da se u formuli B_1 nalazi m_1 individualnih varijbali i l_1 egzistencijalnih kvantifikatora, a u formuli B_2 ima m_2 individualnih varijabli i l_2 egzistencijalnih kvantifikatora. Vrijedi $\mathfrak{F} \models B_1 \vee B_2$ ako je $\mathfrak{F} \models B_1$ ili $\mathfrak{F} \models B_2$. Formule B_1 i B_2 su složenosti strogo manje od n pa je po pretpostavci indukcije potrebno $O(|B_1| \cdot |\mathfrak{F}|^{m_1+l_1+2})$ koraka da bismo provjerili vrijedi li $\mathfrak{F} \models B_1$ te $O(|B_2| \cdot |\mathfrak{F}|^{m_2+l_2+2})$ koraka da bismo provjerili vrijedi li $\mathfrak{F} \models B_2$. Kako vrijedi $|A| = |B_1| + |B_2| + 1$, $m = m_1 + m_2$ i $l = l_1 + l_2$, istinitost formule A na $\mathfrak{F}$ možemo provjeriti u najviše $O(|A| \cdot |\mathfrak{F}|^{m+l+2})$ koraka.

Promotrimo na kraju slučaj kada imamo $A \equiv \exists x B$. Po definiciji vrijedi $\mathfrak{F} \models A$ ako za svaku valuaciju v postoji valuacija v_x takva da vrijedi $\mathfrak{F} \models_{v_x} B$. Primijetimo da je broj individualnih varijabli u B jednak m, a broj egzistencijalnih kvantifikatora jednak je $l - 1$. Formula B je složenosti strogo manje od n pa je po pretpostavci indukcije potrebno $O(|B| \cdot |\mathfrak{F}|^{m+l-1+2})$ vremena da provjerimo vrijedi li $\mathfrak{F} \models_{v_x} B$. Kako ima $|\mathfrak{F}|$ različitih valuacija v_x i vrijedi $|A| = |B| + 2$, potrebno je najviše $O(|A| \cdot |\mathfrak{F}|^{m+l+2})$ vremena da bismo provjerili vrijedi li $\mathfrak{F} \models A$.

□

Napomena 2.1.9. *Neka je M klasa konačnih modela baziranih na okvirima iz neke zadane klase F konačnih okvira. Iz leme 2.1.8 slijedi da je problem odlučivanja vrijedi li $\mathfrak{M} \in M$ odlučiv u polinomnom vremenu u odnosu na veličinu modela $\mathfrak{M}$.*

Primjenom leme 2.1.4 i leme 2.1.8 možemo dokazati da su mnoge normalne modalne logike NP–potpune. Glavna ideja dokaza je konstrukcija konačnog modela za zadanu formulu φ čija je veličina polinomna u odnosu na $|\varphi|$. Model konstruiramo odabirom polinomno mnogo točaka u odnosu na $|\varphi|$ iz modela na kojem je φ ispunjiva. U sljedećem teoremu prvo razmatramo logiku **S5**.

Teorem 2.1.10. *Problem ispunjivosti normalne modalne logike* **S5** *je NP-potpun.*

Dokaz. Neka je φ proizvoljna formula i neka je $\mathfrak{M} = (W, R, V)$ **S5**–model u kojem je formula φ ispunjiva. Pokazat ćemo da postoji **S5**–model s najviše $m + 1$ svjetova, gdje je m broj modalnih operatora u formuli φ, u kojem je formula φ ispunjiva.

Prvo definiramo funkciju $\mathbf{s}\colon Form \times W \to \mathcal{P}(W)$ na sljedeći način:

$$\mathbf{s}(\bot, w) = \{w\}$$
$$\mathbf{s}(p, w) = \{w\}$$
$$\mathbf{s}(\neg\phi, w) = \mathbf{s}(\phi, w)$$
$$\mathbf{s}(\phi \vee \psi, w) = \mathbf{s}(\phi, w) \cup \mathbf{s}(\psi, w)$$
$$\mathbf{s}(\Diamond\phi, w) = \begin{cases} \{w\} \cup \mathbf{s}(\phi, w') \text{ za neki } w' \text{ takav da } \mathfrak{M}, w' \Vdash \phi \text{ i } wRw', & \text{ako } \mathfrak{M}, w \Vdash \Diamond\phi \\ \{w\}, & \text{ako } \mathfrak{M}, w \nVdash \Diamond\phi \end{cases}$$

Primijetimo da u definiciji skupa $\mathbf{s}(\Diamond\phi, w)$ izbor svijeta w' nije jedinstven budući da može postojati više svjetova koji zadovoljavaju navedeni uvjet. Samim time, ni skup $\mathbf{s}(\Diamond\phi, w)$ nije jedinstven. Međutim, iz daljnjeg će se dokaza vidjeti da nam nije potreban jedinstveni svijet w'. Pokazat će se da je dovoljno da skup $\mathbf{s}(\Diamond\phi, w)$ sadrži neki takav svijet. Lako se vidi da vrijedi sljedeće:

$$\mathbf{s}(\Box\phi, w) = \begin{cases} \{w\}, & \text{ako } \mathfrak{M}, w \Vdash \Box\phi \\ \{w\} \cup \mathbf{s}(\phi, w') \text{ za neki } w' \text{ takav da } \mathfrak{M}, w' \nVdash \phi \text{ i } wRw', & \text{ako } \mathfrak{M}, w \nVdash \Box\phi \end{cases}$$

Funkciju $\mathbf{s}$ nazivamo funkcija selekcije. Intuitivno promatrano, možemo reći da se u skupu $\mathbf{s}(\phi, w)$ nalaze svi svjetovi koji su potrebni da se ispita istinitost formule ϕ na svijetu w. Prvo ćemo dokazati dvije pomoćne tvrdnje.

Prva pomoćna tvrdnja. Vrijedi sljedeća ekvivalencija:

$$\mathfrak{M}, w \Vdash \phi \text{ ako i samo ako } \mathfrak{M} \restriction \mathbf{s}(\phi, w), w \Vdash \phi$$

Tvrdnju dokazujemo indukcijom po složenosti formule ϕ. Pretpostavimo prvo da je ϕ formula složenosti 0. Ako je $\phi \equiv \bot$ tada po definiciji relacije forsiranja vrijedi $\mathfrak{M}, w \nVdash \bot$ i $\mathfrak{M} \restriction \mathbf{s}(\bot, w), w \nVdash \bot$. Promotrimo sada slučaj kada imamo $\phi \equiv p$ gdje je $p \in Prop$. Ako $\mathfrak{M}, w \Vdash p$ tada $w \in V(p)$. Po definiciji je $\mathbf{s}(p, w) = \{w\}$ pa imamo $w \in V(p) \cap \mathbf{s}(p, w)$, odnosno $\mathfrak{M} \restriction \mathbf{s}(p, w), w \Vdash p$. Ako $\mathfrak{M} \restriction \mathbf{s}(p, w), w \Vdash p$ tada vrijedi $w \in V(p) \cap \mathbf{s}(p, w)$, odnosno $\mathfrak{M}, w \Vdash p$.

Pretpostavimo sada da tvrdnja vrijedi za svaku modalnu formulu složenosti strogo manje od n. Neka je ϕ formula složenosti n. Razmatramo slučajeve obzirom na oblik formule ϕ.

Promotrimo prvo slučaj kada imamo $\phi \equiv \neg\psi$. Pretpostavimo da vrijedi $\mathfrak{M}, w \Vdash \phi$. Tada vrijedi $\mathfrak{M}, w \nVdash \psi$. Formula ψ je složenosti $n-1$ pa po pretpostavci indukcije vrijedi $\mathfrak{M} \restriction \mathbf{s}(\psi, w), w \nVdash \psi$, odnosno $\mathfrak{M} \restriction \mathbf{s}(\psi, w), w \Vdash \neg\psi$. Po definiciji je $\mathbf{s}(\psi, w) = \mathbf{s}(\neg\psi, w)$, odnosno vrijedi $\mathfrak{M} \restriction \mathbf{s}(\neg\psi, w), w \Vdash \neg\psi$. Drugi smjer dokazuje se analogno.

Promotrimo sada slučaj kada je $\phi \equiv \psi_1 \vee \psi_2$. Pretpostavimo prvo da vrijedi $\mathfrak{M}, w \Vdash \phi$. Tada vrijedi $\mathfrak{M}, w \Vdash \psi_1$ ili $\mathfrak{M}, w \Vdash \psi_2$. Formule ψ_1 i ψ_2 su složenosti strogo manje od n pa po pretpostavci indukcije vrijedi $\mathfrak{M} \restriction \mathbf{s}(\psi_1, w), w \Vdash \psi_1$ ili $\mathfrak{M} \restriction \mathbf{s}(\psi_2, w), w \Vdash \psi_2$. Tada vrijedi $\mathfrak{M} \restriction \mathbf{s}(\psi_1, w) \cup \mathbf{s}(\psi_2, w), w \Vdash \psi_1$ ili $\mathfrak{M} \restriction \mathbf{s}(\psi_1, w) \cup \mathbf{s}(\psi_2, w), w \Vdash \psi_2$, a onda i $\mathfrak{M} \restriction \mathbf{s}(\psi_1, w) \cup \mathbf{s}(\psi_2, w), w \Vdash \psi_1 \vee \psi_2$.
Po definiciji funkcije $\mathbf{s}$ imamo $\mathbf{s}(\psi_1 \vee \psi_2, w) = \mathbf{s}(\psi_1, w) \cup \mathbf{s}(\psi_2, w)$ iz čega slijedi $\mathfrak{M} \restriction \mathbf{s}(\psi_1 \vee \psi_2, w) \Vdash \psi_1 \vee \psi_2$. Analogno se dokazuje drugi smjer.

Promotrimo još na kraju slučaj kada vrijedi $\phi \equiv \Diamond\psi$. Tu imamo sljedeća dva podslučaja:

- $\mathfrak{M}, w \Vdash \phi$.
  Tada postoji svijet w' takav da wRw' i $\mathfrak{M}, w' \Vdash \psi$. Formula ψ je složenosti $n-1$ pa po pretpostavci indukcije vrijedi $\mathfrak{M} \restriction \mathbf{s}(\psi, w'), w' \Vdash \psi$. Tada vrijedi $\mathfrak{M} \restriction \{w\} \cup \mathbf{s}(\psi, w'), w' \Vdash \psi$. Po definiciji funkcije $\mathbf{s}$ imamo $\mathbf{s}(\Diamond\psi, w) = \{w\} \cup \mathbf{s}(\psi, w')$, odnosno vrijedi $\mathfrak{M} \restriction \mathbf{s}(\Diamond\psi, w), w' \Vdash \psi$. Budući da vrijedi wRw' tada slijedi $\mathfrak{M} \restriction \mathbf{s}(\Diamond\psi, w), w \Vdash \Diamond\psi$.

- $\mathfrak{M}, w \nVdash \phi$.
  Tada za svaki svijet $w' \in W$ takav da je wRw' vrijedi $\mathfrak{M}, w' \nVdash \psi$. Po pretpostavci je $\mathfrak{M}$ jedan **S5**–model. Iz propozicije 1.5.1 tada posebno slijedi da je relacija R refleksivna. Zbog refleksivnosti relacije R specijalno vrijedi $\mathfrak{M}, w \nVdash \psi$. Formula ψ je složenosti $n-1$ pa po pretpostavci indukcije vrijedi $\mathfrak{M} \restriction \mathbf{s}(\psi, w), w \nVdash \psi$, a tada vrijedi i $\mathfrak{M} \restriction \{w\}, w \nVdash \psi$. Po definiciji je $\mathbf{s}(\Diamond\psi, w) = \{w\}$ pa vrijedi $\mathfrak{M} \restriction \mathbf{s}(\Diamond\psi, w), w \nVdash \psi$. Kako je (w, w) jedini element relacije dostiživosti modela $\mathfrak{M} \restriction \mathbf{s}(\Diamond\psi, w)$, vrijedi $\mathfrak{M} \restriction \mathbf{s}(\Diamond\psi, w), w \nVdash \Diamond\psi$.

Time je prva pomoćna tvrdnja potpuno dokazana.

Budući da je model $\mathfrak{M}$ jedan **S5**–model, iz propozicije 1.5.4 slijedi da je relacija dostiživosti R relacija ekvivalencije. Relacija dostiživosti modela $\mathfrak{M} \restriction \mathbf{s}(\varphi, w)$ je restrikcija relacije R na skup $\mathbf{s}(\varphi, w) \subseteq W$. Restrikcija relacije ekvivalencije je ponovo relacija ekvivalencije pa zaključujemo da je $\mathfrak{M} \restriction \mathbf{s}(\varphi, w)$ također **S5**–model.

Druga pomoćna tvrdnja. Neka je m broj modalnih operatora koji se pojavljuju u formuli ϕ. Tada vrijedi:

$$|\mathbf{s}(\phi, w)| \leq m + 1.$$

Ovu tvrdnju također dokazujemo indukcijom po složenosti formule ϕ. Ako je formula ϕ složenosti 0 tada je $\phi \equiv p$ za neki $p \in Prop$ ili je $\phi \equiv \bot$. Vrijedi $|\mathbf{s}(p, w)| = |\{w\}| = 1$ i $|\mathbf{s}(\bot, w)| = |\{w\}| = 1$.

Neka je $n \in \mathbb{N}$ takav da tvrdnja vrijedi za svaku formulu složenosti strogo manje od n. Neka je ϕ neka formula složenosti n koja ima m modalnih operatora. Razmatramo slučajeve obzirom na oblik formule ϕ.

Pretpostavimo prvo da imamo $\phi \equiv \neg\psi$. Primijetimo da formule ϕ i ψ imaju jednak broj modalnih operatora. Po definiciji funkcije $\mathbf{s}$ je $\mathbf{s}(\neg\psi, w) = \mathbf{s}(\psi, w)$. Kako je složenost formule ψ jednaka $n-1$ tada iz pretpostavke indukcije slijedi $|\mathbf{s}(\neg\psi, w)| = |\mathbf{s}(\psi, w)| \leq m+1$.

Promotrimo sada slučaj kada imamo $\phi \equiv \psi_1 \vee \psi_2$. Ako je m_1 broj modalnih operatora u ψ_1, a m_2 broj modalnih operatora u ψ_2, tada je očito $m = m_1 + m_2$. Kako su ψ_1 i ψ_2 formule složenosti strogo manje od n, za njih vrijedi pretpostavka indukcije. Tada redom imamo:

$$|\mathbf{s}(\psi_1 \vee \psi_2, w)| = |\mathbf{s}(\psi_1, w) \cup \mathbf{s}(\psi_2, w)| < |\mathbf{s}(\psi_1, w)| + |\mathbf{s}(\psi_2, w)| \leq m_1 + 1 + m_2 + 1 = m + 2.$$

Dakle, dokazali smo da vrijedi $|\mathbf{s}(\psi_1 \vee \psi_2, w)| < m+2$ pa očito vrijedi $|\mathbf{s}(\psi_1 \vee \psi_2, w)| \leq m+1$.

Promotrimo na kraju slučaj kada je $\phi \equiv \Diamond\psi$. Budući da je po pretpostavci formula ϕ složenosti n i sadrži m modalnih operatora, tada je očito formula ψ složenosti $n-1$ i sadrži $m-1$ modalnih operatora. U svrhu dokaza pomatramo sljedeća dva slučaja:

- $\mathfrak{M}, w \Vdash \Diamond\psi$.
  Tada postoji svijet $w' \in W$ takav da imamo $\mathfrak{M}, w' \Vdash \psi$ i wRw'. No, tada imamo redom sljedeće:

  $$|\mathbf{s}(\Diamond\psi, w)| = |\{w\} \cup \mathbf{s}(\psi, w')| \leq 1 + |\mathbf{s}(\psi, w')| \leq 1 + m - 1 + 1 = m + 1$$

- $\mathfrak{M}, w \nVdash \Diamond\psi$.
  Tada imamo $|\mathbf{s}(\Diamond\psi, w)| = |\{w\}| = 1 \leq m + 1$.

Time je i druga pomoćna tvrdnja potpuno dokazana.

Prvom pomoćnom tvrdnjom dokazali smo da za svaku formulu φ, koja je ispunjiva na nekom **S5**–modelu $\mathfrak{M}$, možemo konstruirati podmodel od $\mathfrak{M}$ na kojem je φ također ispunjiva i koji je i sam jedan **S5**–model. Taj podmodel konstruirali smo pomoću funkcije selekcije $\mathbf{s}$. Drugom pomoćnom tvrdnjom dokazali smo da konstruirani **S5**–model ima najviše $m + 1$ svjetova gdje je m broj modalnih operatora u formuli φ. Broj modalnih operatora u φ je sigurno manji od $|\varphi|$ pa je veličina modela polinomna u odnosu na $|\varphi|$.

Dakle, za svaku ispunjivu formulu φ postoji konačan **S5**–model čija veličina je polinomna u odnosu na $|\varphi|$ i na kojem je φ ispunjiva. Ovime smo pokazali da normalna modalna logika **S5** ima polinomno svojstvo konačnih modela u odnosu na klasu konačnih **S5**–modela.

Iz primjera *e*) u 2.1.7 slijedi da je klasa svih **S5**–okvira definabilna u logici prvog reda. Tada je i klasa svih konačnih **S5**–okvira također definabilna u logici prvog reda. Sada iz leme 2.1.8 slijedi da je pripadnost proizvoljnog okvira $\mathfrak{F}$ klasi konačnih **S5**–okvira odlučiva u polinomnom vremenu u odnosu na $|\mathfrak{F}|$. Iz napomene 2.1.9 sada slijedi da je pripadnost proizvoljnog modela $\mathfrak{M}$ klasi konačnih **S5**–modela odlučiva u polinomnom vremenu u odnosu na $|\mathfrak{M}|$. Sada iz leme 2.1.4 slijedi da je problem ispunjivosti normalne modalne logike **S5** jedan NP–potpun problem. □

U nastavku promatramo normalne modalne logike koje proširuju logiku **S4.3** i dokazujemo Hemaspaandrin teorem koji kaže da je problem ispunjivosti svake normalne modalne logike koja proširuje logiku **S4.3** NP–potpun. Za razliku od dokaza NP–potpunosti logike **S5** gdje smo sve tvrdnje detaljno dokazali, u dokazu Hemaspaandrinog teorema koristit ćemo sljedeća dva rezultata koje nećemo dokazivati, a dokazi se mogu pronaći u [1].

Teorem 2.1.11 (Bullov teorem)**.** *Svaka normalna modalna logika koja proširuje logiku* **S4.3** *ima svojstvo konačnih okvira.*

Propozicija 2.1.12. *Za svaku normalnu modalnu logiku* Λ *koja proširuje logiku* **S4.3** *postoji konačan skup N konačnih* **S4.3***–okvira tako da za svaki konačan okvir* $\mathfrak{F}$ *vrijedi sljedeća ekvivalencija:*

$$\mathfrak{F} \Vdash \Lambda \quad \textit{ako i samo ako} \quad \begin{array}{l} \mathfrak{F} \textit{ je } \textbf{\textit{S4.3}}\textit{–okvir i ne postoji ograničeni morfizam} \\ \textit{iz } \mathfrak{F} \textit{ u neki okvir iz } N. \end{array}$$

U dokazu teorema 2.1.10 na jednostavan smo način mogli odrediti koje svjetove treba odabrati za novi model jer je podokvir proizvoljnog **S5**–okvira ponovo **S5**–okvir. Međutim, za normalnu modalnu logiku Λ koja proširuje **S4.3**, podokvir proizvoljnog Λ–okvira, ne mora biti Λ–okvir.

Iz teorema 2.1.11 znamo da svaka normalna modalna logika Λ koja proširuje logiku S4.3 ima svojstvo konačnih okvira. Iz propozicije 1.4.12 slijedi da Λ ima svojstvo konačnih modela. Sada, umjesto da svjetove za novi model polinomne veličine u odnosu na duljine zadane formule biramo iz proizvoljnog modela, možemo ih birati iz proizvoljnog konačnog modela. Važni će se pokazati maksimalni svjetovi te svjetovi maksimalni u odnosu na neku formulu. Upravo te pojmove navodimo u sljedećoj definiciji.

Definicija 2.1.13. *Neka je* $\mathfrak{M} = (W, R, V)$ *neki model. Kažemo da je neki svijet* $w \in W$ ***maksimalan*** *ako za svaki svijet* $v \in W$ *vrijedi* vRw.

Kažemo da je svijet $w \in W$ ***maksimalan u odnosu na formulu*** φ *ako vrijedi* $\mathfrak{M}, w \Vdash \varphi$ *te za svaki svijet* $v \in W \setminus \{w\}$ *takav da* $\mathfrak{M}, v \Vdash \varphi$ *vrijedi* vRw.

Dokažimo sada da u svakom **S4.3**-modelu postoji maksimalan svijet.

Lema 2.1.14. *U svakom **S4.3**–modelu $\mathfrak{M} = (W, R, V)$ postoji maksimalan svijet.*

Dokaz. Tvrdnju dokazujemo indukcijom po kardinalnosti nosača W.

Ako je $W = \{w\}$, tada iz refleksivnosti slijedi wRw pa je w maksimalan svijet.
Neka je $n \in \mathbb{N}$ takav da svaki **S4.3**-model čiji nosač sadrži n svjetova ima maksimalan svijet. Neka je $\mathfrak{M} = (W, R, V)$ jedan **S4.3**-model gdje je $W = \{w_1, \ldots, w_{n+1}\}$ te je svijet w_1 korijen modela. Iz napomene 1.5.7 slijedi da je tada i $\mathfrak{M} \restriction \{w_1, \ldots, w_n\}$ jedan **S4.3**-model s korijenom w_1.

Iz pretpostavke indukcije slijedi da i taj model ima maksimalan svijet w_{max}. Tada vrijedi $w_i R w_{max}$ za svaki $i \in \{1, \ldots, n\}$. Iz povezanosti relacije R slijedi da su moguća samo sljedeća dva slučaja:

- $w_{n+1} R w_{max}$
  Tada je w_{max} maksimalan svijet modela $\mathfrak{M}$.

- $w_{max} R w_{n+1}$
  Tada iz tranzitivnosti relacije R slijedi wRw_{n+1} za svaki $w \in \{w_1, \ldots, w_n\}$. Iz refleksivnosti relacije R slijedi $w_{n+1} R w_{n+1}$. Dakle, w_{n+1} je maksimalan svijet.

□

Na sličan se način dokazuje da za svaku formulu φ koja je ispunjiva na nekom **S4.3**-modelu postoji maksimalan svijet u odnosu na formulu φ.

Odabirom polinomno mnogo točaka (u odnosu na duljinu zadane formule) iz konačnog modela dokazat ćemo da normalne modalne logike koje proširuju logiku **S4.3** imaju polinomno svojstvo konačnih modela. Nakon toga ćemo pomoću propozicije 2.1.12 dokazati NP–potpunost problema ispunjivosti takvih logika. Trebat će nam i sljedeća lema.

Lema 2.1.15. *Neka su $\mathfrak{F} = (W, R)$ i $\mathfrak{G} = (W', R')$ konačni **S4.3**–okviri. Tada su sljedeće tvrdnje ekvivalentne:*

(i) Postoji surjektivni ogranični morfizam iz $\mathfrak{F}$ u $\mathfrak{G}$.

(ii) okvir $\mathfrak{G}$ je izomorfan nekom podokviru okvira $\mathfrak{F}$ koji sadrži neki maksimalni svijet okvira $\mathfrak{F}$.

Dokaz. Dokažimo prvo da tvrdnja (i) povlači tvrdnju (ii). Neka je $f\colon \mathfrak{F} \to \mathfrak{G}$ surjektivni ograničeni morfizam. Neka je w_{max} neki maksimalni svijet okvira $\mathfrak{F}$. Očito takav svijet postoji jer je po pretpostavci okvir $\mathfrak{F}$ konačan.

Označimo sa v svijet $f(w_{max})$, a preostale svjetove okvira $\mathfrak{G}$ označimo sa $v_1, \ldots, v_m$. Neka je za svaki $i \in \{1, \ldots, m\}$ sa v_i^{max} označen neki maksimalan svijet skupa $f^{-1}(\{v_i\})$.

Očito za sve $i, j \in \{1, \ldots, m\}$ takve da je $i \neq j$ vrijedi $v_i^{max} \neq v_j^{max}$. Definiramo skup $\widehat{W} \subseteq W$ ovako:

$$\widehat{W} = \{w_{max}\} \cup \{v_1^{max}, \ldots, v_m^{max}\}$$

Označimo sa $\widehat{\mathfrak{F}}$ okvir $\mathfrak{F} \restriction \widehat{W}$, a sa $\widehat{R}$ označimo relaciju dostiživosti okvira $\widehat{\mathfrak{F}}$. Primijetimo da okviri $\widehat{\mathfrak{F}}$ i $\mathfrak{G}$ imaju jednak broj svjetova.

Tvrdimo da je $f|_{\widehat{\mathfrak{F}}}\colon \widehat{\mathfrak{F}} \to \mathfrak{G}$ jedan izomorfizam između okvira $\widehat{\mathfrak{F}}$ i $\mathfrak{G}$. Primijetimo prvo da je $f|_{\widehat{\mathfrak{F}}}$ ograničeni morfizam okvira $\widehat{\mathfrak{F}}$ i $\mathfrak{G}$. Iz uvjeta (forth) iz definicije 1.4.7 tada slijedi da za sve svjetove $w, w' \in \widehat{W}$, za koje vrijedi $w\widehat{R}w'$, također vrijedi $f(w)R'f(w')$. Iz uvjeta (back) iste definicije slijedi da $f(w)R'f(w')$ povlači $w\widehat{R}w'$. Ovime smo dokazali uvjet (ii) iz definicije 1.4.6. Odnosno, dokazali smo da je $f|_{\widehat{\mathfrak{F}}}$ jaki homomorfizam.

Primijetimo sada da za svijet $v \in \mathfrak{G}$ imamo $v = f(w_{max})$ te za svaki $i \in \{1, \ldots, m\}$ vrijedi $v_i = f(v_i^{max})$. Dakle, funkcija $f|_{\widehat{\mathfrak{F}}}$ je surjekcija.

Za svaki $i \in \{1, \ldots, m\}$ imamo $v_i \neq w_{max}$. Sada vrijedi $f(w_{max}) = v \neq v_i = f(v_i^{max})$. Također, za svaki v_i^{max} i v_j^{max}, $i \neq j$ vrijedi $f(v_i^{max}) = v_i \neq v_j = f(v_j^{max})$. Time je dokazano da je $f|_{\widehat{\mathfrak{F}}}$ injekcija.

Ovime smo dokazali da je funkcija $f|_{\widehat{\mathfrak{F}}}$ izomorfizam okvira $\widehat{\mathfrak{F}}$ i $\mathfrak{G}$. Iz definicije skupa $\widehat{W}$ slijedi da okvir $\widehat{\mathfrak{F}}$ sadrži neki maksimalan svijet okvira $\mathfrak{F}$. Dakle, $\widehat{\mathfrak{F}}$ je traženi podokvir.

Dokažimo sada da tvrdnja (ii) povlači tvrdnju (i). Neka je w_{max} neki maksimalni svijet okvira $\mathfrak{F}$. Neka je zatim $\widehat{W}$ podskup od W takav da je podokvir $\mathfrak{F} \restriction \widehat{W}$ izomorfan okviru $\mathfrak{G}$ te sadrži svijet w_{max}. Definiramo funkciju $f\colon W \to \widehat{W}$ ovako:

$$f(w) = \begin{cases} w, \text{ ako } w \in \widehat{W}, \\ \hat{w}, \text{ ako } w \notin \widehat{W} \text{ i } \hat{w} \in \widehat{W} \text{ je minimalni svijet tako da vrijedi } wR\hat{w}. \end{cases}$$

U prethodnoj definiciji funkcije "minimalan svijet tako da vrijedi $wR\hat{w}$" nam znači da za svaki svijet $v \in W$ za koji imamo wRv vrijedi $\hat{w}Rv$.

Tvrdimo da je funkcija f ograničeni morfizam. Dokažimo prvo da vrijedi uvjet (forth) iz definicije 1.4.7. Neka su $w, w' \in W$ svjetovi takvi da je wRw'. Dokažimo da vrijedi $f(w)Rf(w')$. Prvo dokazujemo da vrijedi $wRf(w')$. U tu svrhu promatramo sljedeća dva slučaja:

- $w' \in \widehat{W}$.
  Tada je $f(w') = w'$ pa tvrdnja slijedi zbog pretpostavke da vrijedi wRw'.

- $w' \notin \widehat{W}$.
  Tada je po definiciji $f(w')$ minimalan svijet takav da je $w'Rf(w')$. Budući da je po pretpostavci $\mathfrak{F}$ jedan **S4.3**–okvir tada iz propozicije 1.5.5 posebno slijedi da je relacija R tranzitivna. Sada iz wRw' i $w'Rf(w')$ slijedi $wRf(w')$

Sada dokazujemo za svaki svijet $v \in W$ vrijedi da je $f(v)$ minimalni svijet sa svojstvom $vRf(v)$. U tu svrhu promatramo dva slučaja:

- $v \notin \widehat{W}$.
  U ovom slučaju tvrdnja slijedi iz definicije funkcije f.

- $v \in \widehat{W}$.
  Tada je $f(v) = v$ pa za svaki v' takav da je vRv' vrijedi $f(v)Rv'$

Budući da smo dokazali da vrijedi $wRf(w')$ te smo upravo dokazali da je $f(w)$ minimalni svijet za koji vrijedi $wRf(w)$, tada imamo $f(w)Rf(w')$, odnosno vrijedi uvjet (forth).

Dokažimo sada da vrijedi uvjet (back). U tu svrhu pretpostavimo da su $w, w' \in W$ svjetovi takvi da vrijedi $f(w)Rf(w')$. Trebamo dokazati da postoji svijet $v \in W$ takav da vrijedi wRv i $f(v) = f(w')$.

Tvrdimo da za svaki $v \in W$ vrijedi $f(f(v)) = f(v)$. U svrhu dokaza promatramo sljedeća dva slučaja:

- $v \in \widehat{W}$.
  Tada je $f(v) = v$ pa je $f(v) \in \widehat{W}$, a onda iz definicije funkcije f imamo $f(f(v)) = f(v)$.

- $v \notin \widehat{W}$.
  Tada je $f(v) = v'$, gdje je v' svijet takav da vrijedi vRv' i za svaki svijet v'' takav da je vRv'' vrijedi $v'Rv''$. Kako je $v' \in \widehat{W}$ tada iz definicije funkcije f vrijedi $f(v') = v'$. Time imamo: $f(f(v)) = f(v') = v' = f(v)$.

Budući da je po pretpostavci $\mathfrak{F}$ jedan **S4.3**–okvir tada iz propozicije 1.5.5 posebno slijedi da je relacija R refleksivna. Iz refleksivnosti relacije R i definicije funkcije f slijedi da imamo $wRf(w)$. Po pretpostavci je $f(w)Rf(w')$ pa iz tranzitivnosti relacije R slijedi $wRf(w')$. Kako smo dokazali da je $f(f(w')) = f(w')$, slijedi da je za traženi svijet v iz uvjeta (back) možemo uzeti svijet $f(w')$. Ovime smo dokazali da vrijedi uvjet (back). Dakle, f je ograničeni morfizam.

Tvrdimo još da je funkcija f surjekcija. Kako bismo to dokazali, uzmimo svijet $v \in \widehat{W}$ proizvoljan. Kako je $\widehat{W} \subseteq W$ tada vrijedi posebno $v \in W$ a onda i $v = f(v)$.

Dakle, f je surjektivni ograničeni morfizam. Budući da smo pretpostavili da vrijedi tvrdnja (ii) iz iskaza leme, tada postoji izomorfizam $f' \colon \widehat{W} \to W'$. Očito je tada funkcija $g \colon W \to W'$ koja je definirana sa $g = f' \circ f$ jedan traženi surjektivni ograničeni morfizam iz okvira $\mathfrak{F}$ u okvir $\mathfrak{G}$. □

Sada nam je cilj dokazati da je svaka ispunjiva formula φ normalne modalne logike koja proširuje logiku **S4.3** ispunjiva na okviru čija veličina linearno ovisi o broju modalnih

operatoru formule φ. Iz toga će lako slijediti da svaka normalna modalna logika koja proširuje **S4.3** ima polinomno svojstvo konačnih modela.

Lema 2.1.16. *Neka je Λ normalna modalna logika koja proširuje logiku* **S4.3**. *Svaka formula φ koja je ispunjiva na nekom Λ-okviru ispunjiva je i na Λ-okviru koji sadrži najviše $m + 2$ svijeta gdje je m broj modalnih operatora formule φ.*

Dokaz. Neka je formula φ ispunjiva na nekom Λ–modelu. Iz Bullovog teorema, to jest teorema 2.1.11, slijedi da logika Λ ima svojstvo konačnih okvira. Iz propozicije 1.4.12 sada slijedi da Λ ima svojstvo konačnih modela. Tada postoji konačan Λ–model $\mathfrak{N} = (W', R', V')$ i svijet $w_0 \in W'$ takvi da vrijedi $\mathfrak{N}, w_0 \Vdash \varphi$.
Neka je $\mathfrak{M} = (W, R, V)$ podmodel od $\mathfrak{N}$ generiran svijetom w_0. Iz propozicije 1.4.4 slijedi $\mathfrak{M}, w_0 \Vdash \varphi$. Zatim, iz napomene 1.4.5 znamo da generirani podmodeli čuvaju valjanost na okvirima. Dakle, okvir (W, R) je jedan Λ–okvir.
Odaberimo sada svjetove za traženi okvir koji treba sadržavati najviše $m + 2$ svijeta. Neka su $\Diamond\psi_1, \ldots, \Diamond\psi_k$ sve $\Diamond$-potformule formule φ koje su ispunjive na svijetu w_0. Za svaki prirodan broj i za koji vrijedi $1 \leq i \leq k$ odaberemo svijet w_i koji je maksimalan u odnosu na formulu ψ_i. Odnosno, odaberemo svijet w_i takav da vrijedi $\mathfrak{M}, w_i \Vdash \psi_i$ i za svaki svijet $w' \in W$ na kojem je formula ψ_i istinita vrijedi $w'Rw_i$. Svjetovi $w_1, \ldots, w_k$ su potrebni da bi osigurali da je φ istinita na svijetu w_0. No, ne možemo biti sigurni da smo konstruirali Λ–okvir.
Neka je w_{k+1} neki maksimalan svijet modela $\mathfrak{M}$. Označimo sa $\widehat{\mathfrak{M}}$ podmodel $\mathfrak{M} \restriction \{w_0, w_1, \ldots, w_k, w_{k+1}\}$. Očito model $\widehat{\mathfrak{M}}$ sadrži najviše $m + 2$ svijeta, gdje je m broj modalnih operatora u formuli φ. Dokažimo da je model $\widehat{\mathfrak{M}}$ baziran na jednom Λ–okviru.
Primijetimo da je pripadni okvir modela $\widehat{\mathfrak{M}}$ podokvir okvira (W, R) te sadrži neki maksimalan svijet okvira (W, R). Dakle, pripadni okvir modela $\widehat{\mathfrak{M}}$ zadovoljava uvjet (ii) iz leme 2.1.15 pa postoji surjektivni ograničeni morfizam iz modela $\mathfrak{M}$ u model $\widehat{\mathfrak{M}}$. Iz napomene 1.4.9 znamo da ograničeni morfizmi čuvaju valjanost na okvirima iz čega slijedi da je $\widehat{\mathfrak{M}}$ baziran na Λ–okviru.
Prestalo je dokazati da vrijedi $\widehat{\mathfrak{M}}, w_0 \Vdash \varphi$. U tu svrhu, indukcijom po složenosti formule dokazujemo da za svaku potformulu ψ od φ i za svaki i, $0 \leq i \leq k + 1$ vrijedi sljedeća ekvivalencija:

$$\mathfrak{M}, w_i \Vdash \psi \text{ ako i samo ako } \widehat{\mathfrak{M}}, w_i \Vdash \psi.$$

U slučaju da je ψ propozicionalna varijabla, tvrdnja slijedi iz definicije podmodela. U slučaju da je $\psi \equiv \bot$ vrijedi $\mathfrak{M}, w_i \nVdash \bot$ i $\widehat{\mathfrak{M}}, w_i \nVdash \bot$.

Neka je $n \in \mathbb{N}$ takav da tvrdnja vrijedi za svaku potformulu složenosti storog manje od n. Neka je ψ potformula od φ složenosti n. Promatramo slučajeve obzirom na oblik formule ψ.

Promotrimo prvo slučaj kada imamo $\psi \equiv \neg\phi$. Formula ϕ je složenosti $n-1$ pa za nju vrijedi pretpostavka indukcije. Redom imamo sljedeće ekvivalencije:

$$\begin{aligned}\mathfrak{M}, w_i \Vdash \neg\phi \text{ ako i samo ako } & \mathfrak{M}, w_i \nVdash \phi \\ \text{ako i samo ako } & \widehat{\mathfrak{M}}, w_i \nVdash \phi \\ \text{ako i samo ako } & \widehat{\mathfrak{M}}, w_i \Vdash \neg\phi\end{aligned}$$

Na sličan se način dokazuje i slučaj $\psi \equiv \phi_1 \vee \phi_2$.

Na kraju razmatramo slučaj kada imamo $\psi \equiv \Diamond\phi$. Pretpostavimo prvo da vrijedi $\mathfrak{M},\ w_i \Vdash \Diamond\phi$. Budući da je model $\mathfrak{M}$ generiran svijetom w_0 i tranzitivan je, tada mora vrijediti $w_0 R w_i$. Dakle, vrijedi $\mathfrak{M}, w_0 \Vdash \Diamond\Diamond\phi$.
Model $\mathfrak{M}$ je jedan Λ–model, a logika Λ proširuje logiku **S4.3**. Tada je model $\mathfrak{M}$ posebno i **S4.3**–model pa vrijedi $\mathfrak{M} \Vdash \Diamond\Diamond\phi \to \Diamond\phi$. Posebno, vrijedi i $\mathfrak{M}, w_0 \Vdash \Diamond\Diamond\phi \to \Diamond\phi$.
Sada iz $\mathfrak{M}, w_0 \Vdash \Diamond\Diamond\phi$ i $\mathfrak{M}, w_0 \Vdash \Diamond\Diamond\phi \to \Diamond\phi$ odmah slijedi $\mathfrak{M}, w_0 \Vdash \Diamond\phi$. Budući da po pretpostavci skup $\{\psi_1, \ldots, \psi_k\}$ sadrži sve $\Diamond$–potformule formule φ koje su ispunjive na svijetu w_0, tada postoji $j \in \{1, \ldots, k\}$ tako da vrijedi $\phi \equiv \psi_j$. Prilikom definicije modela $\widehat{\mathfrak{M}}$ odabrali smo uvijek maksimalni svijet w_j takav da vrijedi $\mathfrak{M}, w_j \Vdash \psi_j$. Iz toga slijedi da vrijedi $w_i R w_j$. Kako je formula ψ_j potformula formule φ složenosti $n-1$, iz pretpostavke indukcije slijedi da vrijedi $\widehat{\mathfrak{M}}, w_j \Vdash \psi_j$. Stoga vrijedi $\widehat{\mathfrak{M}}, w_i \Vdash \Diamond\psi_j$.

Dokažimo još obratnu implikaciju. U tu svrhu pretpostavimo da vrijedi $\widehat{\mathfrak{M}}, w_i \Vdash \Diamond\phi$. Tada postoji $j \leq k$ tako da imamo $\widehat{\mathfrak{M}}, w_j \Vdash \phi$ i $w_i R w_j$. Iz pretpostavke indukcije slijedi $\mathfrak{M}, w_j \Vdash \phi$, a onda i $\mathfrak{M}, w_i \Vdash \Diamond\phi$.

□

Korolar 2.1.17. *Svaka normalna modalna logika koja proširuje **S4.3** ima polinomno svojstvo konačnih modela.*

Dokaz. Neka je Λ normalna modalna logika koja proširuje **S4.3**. Iz Bullovog teorema, tj. teorema 2.1.11, znamo da logika Λ ima svojstvo konačnih okvira. Iz leme 2.1.3 slijedi da postoji klasa konačnih okvira F takva da je $\Lambda = \Lambda_F$. Označimo sa M sljedeći skup $\{\mathfrak{M} = (\mathfrak{F}, V) \mid \mathfrak{F} \in F\}$. Očito je svaki model iz skupa M konačan. Nadalje, za svaku formulu $\varphi \in \Lambda$ i svaki okvir $\mathfrak{F} \in F$ vrijedi $\mathfrak{F} \Vdash \varphi$. Tada za proizvoljnu valuaciju V vrijedi $(\mathfrak{F}, V) \Vdash \varphi$ iz čega slijedi $\Lambda \subseteq \Lambda_M$. Pretpostavimo da vrijedi $\Lambda \subset \Lambda_M$. Tada postoji formula $\varphi \in \Lambda$ i model $\mathfrak{M} \in M$, gdje je $\mathfrak{M} = (\mathfrak{F}, V)$ za neki $\mathfrak{F} \in F$, takav da $\mathfrak{M} \nVdash \varphi$. No tada vrijedi $\mathfrak{F} \nVdash \varphi$ što je kontradikcija s $\Lambda = \Lambda_F$. Slijedi da je $\Lambda = \Lambda_M$.

Neka je p polinom definiran sa $p(x) = x+2$. Iz leme 2.1.16 znamo da je svaka ispunjiva formula φ ispunjiva na Λ-okviru koji sadrži najviše $m+2$ svijeta gdje je m broj modalnih operatoru u formuli φ. Sada je $p(|\varphi|) = |\varphi| + 2$ što je sigurno veće od $m+2$. □

Sada možemo dokazati glavni rezultat ove točke.

Teorem 2.1.18 (Hemaspaandrin teorem)**.** *Problem ispunjivosti svake normalne modalne logike koja proširuje normalnu modalnu logiku* **S4.3** *je* NP*-potpun problem.*

Dokaz. Neka je Λ normalna modalna logika koja proširuje logiku **S4.3**. Iz korolara 2.1.17 slijedi da Λ ima polinomno svojstvo konačnih modela. Iz leme 2.1.4 slijedi da je za NP-potpunost logike Λ dovoljno dokazati da za proizvoljan model $\mathfrak{M}$ možemo u polinomnom vremenu u odnosu na $|\mathfrak{M}|$ provjeriti je li $\mathfrak{M}$ jedan Λ–model.

Neka je $\mathfrak{M} = (\mathfrak{F}, V)$ proizvoljan konačan model gdje je $\mathfrak{F} = (W, R)$. Iz napomene 2.1.9 znamo da je dovoljno provjeriti možemo li u polinomnom vremenu u odnosu na $|\mathfrak{F}|$ provjeriti je li $\mathfrak{F}$ jedan Λ–okvir, odnosno vrijedi li $\mathfrak{F} \Vdash \Lambda$.

Iz primjera *f*) u 2.1.7 slijedi da je klasa svih **S4.3**–okvira definabila u logici prvog reda. Sada iz leme 2.1.8 slijedi da se u polinomnom vremenu u odnosu na $|\mathfrak{F}|$ može provjeriti vrijedi li $\mathfrak{F} \Vdash$ **S4.3**.

Iz propozicije 2.1.12 slijedi da postoji konačan skup N konačnih **S4.3**–okvira takav da ako u polinomnom vremenu u odnosu na $|\mathfrak{F}|$ možemo provjeriti da ne postoji ograničeni morfizam iz okvira $\mathfrak{F}$ u neki okvir iz skupa N, tada slijedi da u polinomnom vremenu u odnosu na $|\mathfrak{F}|$ možemo provjeriti vrijedi li $\mathfrak{F} \Vdash \Lambda$. Da bismo dokazali da ne postoji ograničeni morfizam iz okvira $\mathfrak{F}$ u neki okvir iz skupa N koristimo lemu 2.1.15. Iz dokaza navedene leme slijedi da je dovoljno dokazati da ne postoji skup $\widehat{W} \subseteq W$ koji sadrži neki maksimalan svijet skupa W te je okvir $\mathfrak{F} \restriction \widehat{W}$ izomorfan nekom okviru iz N.

Označimo $n_0 = \max\{|\mathfrak{G}| \colon \mathfrak{G} \in N\}$. Postoji najviše $|N| \cdot |\mathfrak{F}|^{n_0}$ funkcija čija domena je nosač okvira $\mathfrak{F}$, a kodomena je nosač nekog okvira $\mathfrak{G} \in N$. Očito u polinomnom vremenu u odnosnu na $|\mathfrak{F}|$ možemo provjeriti je li neka od tih funkcija ograničeni morfizam.

Dakle, logika Λ ima polinomno svojstvo konačnih modela i za proizvoljan model $\mathfrak{M}$ možemo u polinomnom vremenu u odnosu na $\mathfrak{M}$ provjeriti je li $\mathfrak{M}$ jedan Λ–model. Sada iz leme 2.1.4 slijedi da je problem ispunjivosti logike Λ jedan NP–potpun problem. □

Kada znamo složenost problema ispunjivosti nekih normalnih modalnih logika, možemo reći nešto i o složenosti problema valjanosti. Formula φ valjana je ako i samo ako formula $\neg\varphi$ nije ispunjiva, odnosno problem valjanosti je komplement problema ispunjivosti. Komplementi problema koji pripadaju klasi NP čine klasu co-NP. Iako nije dokazano, smatra se da vrijedi NP $\neq$ co-NP.

U ovoj točki pokazali smo da klasi NP pripadaju problem ispunjivosti normalnih modalnih logika koje proširuju **S4.3** i problem ispunjivosti normalne modalna logike **S5**. Dakle, problemi valjanosti ovih logika pripadaju klasi co-NP. Štoviše, problem valjanosti ovih normalnih modalnih logika je co-NP težak iz čega slijedi da je co-NP potpun.

2.2 PSPACE-potpune modalne logike

U ovoj točki razmatramo modalne logike čiji problem ispunjivosti je PSPACE-potpun. Želimo istaknuti da se smatra da je klasa NP pravi podskup klase PSPACE. No, to još nitko nije uspio dokazati. Iz tog razloga problemi iz klase PSPACE smatraju se "težima" od onih iz klase NP. To pak povlači da logike koje sada razmatramo imaju teži problem ispunjivosti od logika koje smo promatrali u prethodnoj točki.

U ovoj točki prvo dokazujemo da logika **K** nema polinomno svojstvo konačnih modela. Zatim opisujemo prostorno polinoman nedeterministički Turingov stroj koji odlučuje je li proizvoljna modalna formula **K**-ispunjiva iz čega će kao posljedica Savitchevog teorema slijediti da problem ispunjivosti logike **K** pripada klasi PSPACE. Zatim dokazujemo Ladnerov teorem koji govori da je svaka normalna modalna logika između **K** i **S4** PSPACE-teška. Na kraju točke ukratko opisujemo složenost logika `LTL` i `PDL`. Također dajemo primjer neodlučive modalne logike `Tile`.

Kroz cijelu točku bit će nam važan pojam stabla koji sada definiramo.

Definicija 2.2.1. ***Stablo*** $\mathcal{T}$ *je uređeni par* (S, R) *gdje je* S *neprazan skup, a* R *binarna relacija na* S*, koja ima sljedeća svojstva:*

a) *postoji jedinstveni* $r \in S$ *takav da za svaki* $s \in S$*,* $s \neq r$ *postoji jedinstveni konačni niz* $s_1, \ldots, s_k \in S$ *takav da je* $s_k = s$ *i vrijedi* $rRs_1R \ldots Rs_{k-1}Rs_k$*. Element r nazivamo* ***korijen***

b) *za svaki* $s \in S$*,* $s \neq r$ *postoji jedinstveni* $s' \in S$ *takav da* $s'Rs$

c) R *je aciklička relacija*

Elemente stabla nazivamo ***čvorovi****.*
Visina čvora *s je duljina jedinstvenog puta od s do korijena. Smatramo da je* ***visina korijena jednaka nula****.* ***Visina stabla*** *je duljina najdužeg puta u stablu.*
Kažemo da je $\mathfrak{M} = (W, R, V)$ ***stablasti model*** *ako je pripadni okvir* (W, R) *stablo.*

Prvo pokazujemo da najmanja normalna modalna logika **K** nema polinomno svojstvo konačnih modela. To ćemo pokazati tako da definiramo formulu koja je ispunjiva na modelu čija veličina eksponencijalno ovisi o duljini formule.

Teorem 2.2.2. *Normalna modalna logika **K** nema polinomno svojstvo konačnih modela.*

Dokaz. Neka je $m \in \mathbb{N}$ proizvoljan. Definirat ćemo formulu $\varphi(m)$ koja ima sljedeća dva svojstva:

(i) duljina formule $\varphi(m)$ polinomno ovisi o m

(ii) veličina najmanjeg modela na kojem je $\varphi(m)$ ispunjiva eksponencijalno ovisi o $|\varphi(m)|$

Okvir najmanjeg modela na kojem je formula $\varphi(m)$ istinita zapravo će biti potpuno binarno stablo visine m. Takvo stablo ima $2^{m+1} - 1$ čvorova pa će i nosač modela imati toliko svjetova.

Formula $\varphi(m)$ sastojat će se od propozicionalnih varijabli $q_0, q_1, \ldots, q_m$ i $p_1, \ldots, p_m$. Varijable $q_0, \ldots, q_m$ služit će kao "oznake" razine stabla - varijabla q_i bit će istinita samo na svjetovima na i-toj razini stabla. Nadalje, svaki podskup skupa $\{p_1, \ldots, p_k\}$ bit će istinit na točno jednom svijetu na k-toj razini stabla. Kako takvih podskupova ima 2^k, na k-toj razini stabla bit će točno 2^k svjetova.

Prvo za svaki $i = 1, \ldots, m-1$ definiramo sljedeće pokrate za formule:

$$B_i \equiv q_i \to (\Diamond(q_{i+1} \wedge p_{i+1}) \wedge \Diamond(q_{i+1} \wedge \neg p_{i+1})) \tag{2.1}$$

$$S(p_i, \neg p_i) \equiv (p_i \to \Box p_i) \wedge (\neg p_i \to \Box \neg p_i) \tag{2.2}$$

Primijetimo da formula B_i opisuje grananje na svim svjetovim na i-toj razini. Naime, kako je varijabla q_i istinita na svakom svijetu w na i-toj razini, tada moraju postojati svjetovi v_1 i v_2 takvi da vrijedi wRv_1 i wRv_2 te je varijabla p_{i+1} istinita na svijetu v_1 i nije istinita na svijetu v_2.

Nadalje, formula $S(p_i, \neg p_i)$ "čuva" istinitost varijable p_i na "sljedećoj" razini - ako je varijabla p_i istinita na nekom svijetu w na nekoj k-toj razini, tada varijabla p_i mora biti istinita na svim svijetovima v na razini $k+1$ za koje vrijedi wRv. Obratno, ako varijabla p_i nije istinita na svijetu w na nekoj k-toj razini, tada varijabla p_i nije istinita ni na svjetovima v na razini $k+1$ za koje vrijedi wRv.

Dalje definiramo pomoćne formule:

$$\varphi_1(m) \equiv \bigwedge_{i=0}^{m} \Box^{(m)} \left(q_i \rightarrow \wedge_{j \neq i} \neg q_j \right)$$

$$\varphi_2(m) \equiv B_0 \wedge \Box B_1 \wedge \Box^2 B_2 \wedge \Box^3 B_3 \wedge \cdots \wedge \Box^{m-1} B_{m-1}$$

$$\begin{aligned} \varphi_3(m) \equiv \Box S(p_1, \neg p_1) \wedge \Box^2 S(p_1, \neg p_1) \wedge \Box^2 S(p_1, \neg p_1) \wedge \cdots \wedge \Box^{m-1} S(p_1, \neg p_1) \\ \wedge \Box^2 S(p_2, \neg p_2) \wedge \Box^3 S(p_2, \neg p_2) \wedge \cdots \wedge \Box^{m-1} S(p_2, \neg p_2) \\ \wedge \Box^3 S(p_3, \neg p_3) \wedge \cdots \wedge \Box^{m-1} S(p_3, \neg p_3) \\ \vdots \\ \wedge \Box^{m-1} S(p_{m-1}, \neg p_{m-1}) \end{aligned}$$

gdje je $\Box^{(m)}\phi = \phi \wedge \Box\phi \wedge \Box^2\phi \wedge \cdots \wedge \Box^m\phi$.

Konačno definiramo formulu traženu formulu $\varphi(m)$ ovako:

$$\varphi(m) \equiv q_0 \wedge \varphi_1(m) \wedge \varphi_2(m) \wedge \varphi_3(m)$$

Ako je $\varphi(m)$ ispunjiva tada iz istinitosti formule $\varphi_1(m)$ slijedi da su varijable q_i istinite samo na svjetovima na i-toj razini. Nadalje, formula $\varphi(m)$ istinita je na svijetu na razini 0, to jest na korijenu stabla. Istinitost formule $\varphi_2(m)$ ima za posljedicu grananje na svjetovima na svakoj razini stabla i svako takvo grananje garantira da će varijabla p_i na nekom svijetu na razini i biti istinita, a na nekom svijetu na razini i neće biti istinita. Formula $\varphi_3(m)$ čuva istinitost varijable p_i sve do razine m.

Dakle, okvir najmanjeg modela $\mathfrak{M} = (W, R, V)$ na kojem je $\varphi(m)$ istinita je potpuno binarno stablo visine m.

Valuaciju V definiramo na sljedeći način:

- $V(q_i) = \{w \in W \mid w \text{ se nalazi na } i\text{-toj razini stabla } (W, R)\}$, za svaki $i \in \{0, \ldots, m\}$
- Za svaki p_i, ako je w neki svijet na k-toj razini, gdje je $k < i$, tada $w \notin V(p_i)$
- Ako je w neki svijet na razini $i - 1$ te su v_1 i v_2 njegovi sljedbenici, tada je $v_1 \in V(p_i)$ i $v_2 \notin V(p_i)$
- Ako je w neki svijet na razini i te za neku propozicionalnu varijablu p_k vrijedi $w \in V(p_k)$, tada za svaki sljedbenik v od w vrijedi $v \in V(p_k)$

- Ako je w neki svijet na razini i te za neku propozicionalnu varijablu p_k vrijedi $w \notin V(p_k)$, tada za svaki sljedbenik v od w vrijedi $v \notin V(p_k)$

Lako je provjeriti da je $\varphi(m)$ istinita na korijenu stabla (W, R).

Promotrimo još duljinu formule $\varphi(m)$. Formula $\varphi_1(m)$ ima $O(m^3)$ veznika $\wedge$ te ta formula ima $O(m^3)$ nastupa operatora $\Box$. U svakoj potformuli oblika $q_i \to \wedge_{i \neq j} q_j$ imamo $m+1$ propozicionalnih varijabli. Iz svega toga slijedi $|\varphi_1(m)| \in O(m^3)$.
Formula $\varphi_2(m)$ građena je od $m-1$ konjunkcije i $O(m^2)$ operatora $\Box$, dok je veličina formula B_i konstantna. Dakle, imamo $|\varphi_2(m)| \in O(m^2)$.
Formula $\varphi_3(m)$ sadrži $O(m^2)$ nastupa veznika $\wedge$ te najviše $O(m^3)$ operatora $\Box$. Kako je veličina formula $S(p_i, \neg p_i)$ konstantna, sijedi da je $|\varphi_3(m)| \in O(m^3)$.
Konačno, $\varphi(m)$ je konjunkcija propozicionalne varijable q_0 te formula $\varphi_1(m)$, $\varphi_2(m)$ te $\varphi_3(m)$ pa slijedi da je $|\varphi(m)| \in O(m^3)$. Dakle, duljina formule $\varphi(m)$ polinomno ovisi o m. Kako veličina modela $\mathfrak{M}$ eksponencijalno ovisi o m, a $|\varphi(m)|$ polinomno ovisi o m, slijedi da veličina modela $\mathfrak{M}$ eksponencijalno ovisi o duljini formule $\varphi(m)$. $\Box$

Kako bismo objasnili formulu $\varphi(m)$ iz dokaza prethodnog teorema, u sljedećem primjeru promatramo tu formulu za jedan fiksirani broj m.

Primjer 2.2.3. *Promotrimo jedan konkretan primjer formule iz dokaza prethodnog teorema 2.2.2 i to za $m = 2$. Tada prvo redom imamo sljedeće formule:*

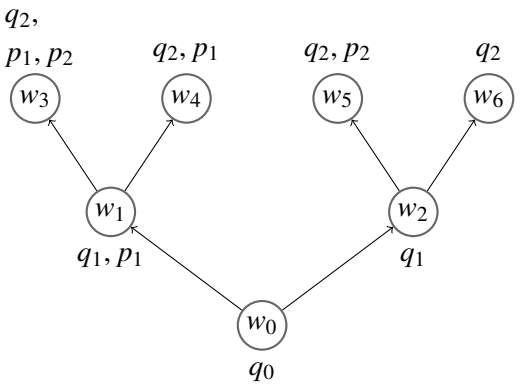
$$\begin{aligned}\varphi_1(2) \equiv\ & q_0 \to (\neg q_1 \wedge \neg q_2) \wedge \Box(q_0 \to (\neg q_1 \wedge \neg q_2)) \wedge \Box\Box(q_0 \to (\neg q_1 \wedge \neg q_2)) \wedge \\ & q_1 \to (\neg q_0 \wedge \neg q_2) \wedge \Box(q_1 \to (\neg q_0 \wedge \neg q_2)) \wedge \Box\Box(q_1 \to (\neg q_0 \wedge \neg q_2)) \wedge \\ & q_2 \to (\neg q_0 \wedge \neg q_1) \wedge \Box(q_2 \to (\neg q_0 \wedge \neg q_1)) \wedge \Box\Box(q_2 \to (\neg q_0 \wedge \neg q_1))\end{aligned}$$

$$\varphi_2(2) \equiv q_0 \to (\Diamond(q_1 \wedge p_1) \wedge \Diamond(q_1 \wedge \neg p_1)) \wedge \Box(q_1 \to (\Diamond(q_2 \wedge p_2) \wedge \Diamond(q_2 \wedge \neg p_2)))$$

$$\varphi_3(2) \equiv \Box((p_1 \to \Box p_1) \wedge (\neg p_1 \to \Box \neg p_1))$$

Kao i u dokazu prethodnog teorema imamo $\varphi(2) \equiv q_0 \wedge \varphi_1(2) \wedge \varphi_2(2) \wedge \varphi_3(2)$.

Na sljedećoj slici ilustriran je najmanji model na kojemu je $\varphi(2)$ istinita.



Dokazali smo da logika **K** nema polinomno svojstvo konačnih modela. To je svojstvo inače bilo ključno za dokaz NP-potpunosti neke logike. Iz toga naravno ne slijedi da logika **K** nije NP–potpuna. Složenost logike **K** ne možemo dokazati na isti način kao što smo dokazali složenost, primjerice logike **S5** u teoremu 2.1.10.

U nastavku pokazujemo da je problem ispunjivosti normalne modalne logike **K** jedan PSPACE problem. Prvo ćemo pokazati da je svaka ispunjiva formula φ istinita na modelu čiji okvir je stablo polinomne visine u odnosu na duljinu formule, tj. $|\varphi|$. Tada ćemo definirati algoritam, koji ćemo nazivati *Svjedok*, pomoću kojeg ćemo odlučivati je li proizvoljna formula φ **K**-ispunjiva te ćemo pokazati da se algoritam *Svjedok* može implementirati na deterministčkom Turingovom stroju koji koristi polinomno mnogo (u odnosu na $|\varphi|$) registara. Algoritam *Svjedok* radi s posebnim skupovima formula koji se nazivaju Hintikkini skupovi. Navedene skupove formula ćemo definirati u nastavku. Prvo definiramo pojam zatvorenja skupa formula.

Definicija 2.2.4. *Neka je Σ skup formula. Kažemo da je skup Σ **zatvoren na potformule** ako vrijedi sljedeće: ako je $\varphi \in \Sigma$ i ψ je neka potformula od φ, tada je i $\psi \in \Sigma$.*
*Kažemo da je skup formula Σ **zatvoren na jednostruke negacije** ako vrijedi sljedeće: ako je $\varphi \in \Sigma$ i $\varphi \not\equiv \neg\psi$ za neku formulu ψ, tada je $\neg\varphi \in \Sigma$.*
*Kažemo da je Σ **zatvoren** ako je zatvoren na potformule i jednostruke negacije.*

*Neka je Γ skup formula. **Zatvorenje** skupa Γ, u oznaci Cl(Γ), je najmanji zatvoreni skup formula koji sadrži Γ.*
Ako je $\Gamma = \{\varphi\}$, tada umjesto Cl($\{\varphi\}$) pišemo Cl(φ) i skup Cl(φ) nazivamo zatvorenje formule φ.

Definicija 2.2.5. *Neka je Σ skup formula zatvoren na potformule. **Hintikkin skup** H nad Σ je maksimalni podskup od Σ koji zadovoljava sljedeće uvjete:*

(H1) $\bot \notin H$

(H2) Ako je $\neg\varphi \in \Sigma$ *tada vrijedi:* $\neg\varphi \in H$ *ako i samo ako vrijedi* $\varphi \notin H$

(H3) Ako je $\varphi \vee \psi \in \Sigma$ *tada vrijedi:* $\varphi \vee \psi \in H$ *ako i samo ako vrijedi* $\varphi \in H$ *ili* $\psi \in H$

Ispunjivi Hintikkin skup nazivamo ***atom****.*

Algoritam *Svjedok* će kao ulaz primiti dva skupa H i Σ te će odlučiti je li H atom nad Σ. To radi tako da provjerava takozvane zahtjeve koje H kreira i rekurzivno provjerava jesu li ti zahtjevi ispunjeni. U sljedećoj definiciji navodimo pojam zahtjeva.

Definicija 2.2.6. *Neka je* H *Hintikkin skup nad skupom formula* Σ *i neka je* $\Diamond\varphi \in H$*.* ***Zahtjev*** *koji formula* $\Diamond\varphi$ *kreira u* H*, u oznaci* $Dem(H,\Diamond\varphi)$*, je skup formula*

$$\{\varphi\} \cup \{\sim\psi \mid \neg\Diamond\psi \in H\}$$

gdje je

$$\sim\psi \equiv \begin{cases} \phi, & \text{ako je } \psi \equiv \neg\phi \text{ za neku formulu } \phi \\ \neg\psi, & \text{inače} \end{cases}$$

Sa $H_{\Diamond\varphi}$ *označavamo skup svih Hintikkinih skupova nad skupom* $Cl(Dem(H,\Diamond\varphi))$ *koji sadrže skup* $Dem(H,\Diamond\varphi)$*.*

Lema 2.2.7. *Neka je* H *atom nad* Σ *i neka je* $\Diamond\varphi \in H$*. Tada postoji barem jedan atom* $A \in H_{\Diamond\varphi}$*.*

Dokaz. Dokažimo prvo da je skup formula $Dem(A,\Diamond\varphi)$ ispunjiv. Po pretpostavci je skup formula H ispunjiv. Tada postoji model $\mathfrak{M} = (W,R,V)$ i svijet $w \in W$ takav da za svaku $\psi \in H$ vrijedi $\mathfrak{M}, v \Vdash \psi$. Posebno, vrijedi i $\mathfrak{M}, w \Vdash \Diamond\varphi$. Tada postoji svijet $v \in W$ takav da wRv i $\mathfrak{M}, v \Vdash \varphi$. Neka je $\sim\psi \in Dem(H,\Diamond\varphi)$ proizvoljna formula. Tada je $\neg\Diamond\psi \in H$ i vrijedi $\mathfrak{M}, w \Vdash \neg\Diamond\psi$, odnosno $\mathfrak{M}, w \nVdash \Diamond\psi$. Tada za svaki svijet $v' \in W$ takav da je wRv' vrijedi $\mathfrak{M}, v' \nVdash \psi$. Posebno vrijedi $\mathfrak{M}, v \nVdash \psi$. Ako je $\psi \equiv \neg\phi$ za neku formulu ϕ, tada je $\sim\psi \equiv \phi$ pa vrijedi $\mathfrak{M}, v \Vdash \sim\psi$. U suprotnom je $\sim\psi \equiv \neg\psi$ pa opet vrijedi $\mathfrak{M}, v \Vdash \sim\psi$. Dakle, vrijedi $\mathfrak{M}, v \Vdash Dem(H,\Diamond\varphi)$.

Definiramo skup formula Ψ ovako: $\Psi = \{\psi \mid \mathfrak{M}, v \Vdash \psi\}$. Zatim, označimo sa A skup formula $Cl(Dem(H,\Diamond\varphi)) \cap \Psi$. Tada imamo $Dem(H,\Diamond\varphi) \subseteq A$, a zbog $A \subseteq \Psi$ vrijedi $\mathfrak{M}, v \Vdash A$.

Dokažimo još da je skup formula A jedan Hintikkin skup nad $Cl(Dem(H,\Diamond\varphi))$. Svojstvo (H1) očito vrijedi jer je skup formula A ispunjiv. U svrhu dokaza svojstva (H2) uzmimo proizvoljnu formulu $\neg\psi$ iz skupa $Cl(Dem(H,\Diamond\varphi))$. Pretpostavimo prvo da vrijedi $\neg\psi \in A$. Tada je posebno $\neg\psi \in \Psi$, to jest $\mathfrak{M}, v \Vdash \neg\psi$. Sada slijedi $\mathfrak{M}, v \nVdash \psi$, odnosno $\psi \notin \Psi$ pa je $\psi \notin A$. Pretpostavimo sada da je $\psi \notin A$. Kako je po pretpostavci $\neg\psi \in Cl(Dem(H,\Diamond\varphi))$, a skup $Cl(Dem(H,\Diamond\varphi))$ je zatvoren na potformule, vrijedi

$\psi \in Cl(Dem(H, \Diamond\varphi))$. Dakle, mora vrijediti $\psi \notin \Psi$. Tada $\mathfrak{M}, v \nVdash \psi$, odnosno $\mathfrak{M}, v \Vdash \neg\psi$ pa je $\neg\psi \in \Psi$. Sada slijedi $\neg\psi \in A$.
Preostalo je provjeriti da vrijedi i svojstvo (H3). U tu svrhu uzmimo proizvoljnu formulu oblika $\psi_1 \vee \psi_2 \in Cl(Dem(H, \Diamond\varphi))$. Kako je skup $Cl(Dem(H, \Diamond\varphi))$ zatvoren na potformule tada vrijedi $\psi_1 \in Cl(Dem(H, \Diamond\varphi))$ i $\psi_2 \in Cl(Dem(H, \Diamond\varphi))$. Pretpostavimo prvo da je $\psi_1 \vee \psi_2 \in A$. Iz $\psi_1 \vee \psi_2 \in \Psi$ slijedi $\psi_1 \in \Psi$ ili $\psi_2 \in \Psi$. Tada je $\psi_1 \in A$ ili $\psi_2 \in A$. Pretpostavimo sada da je $\psi_1 \in A$ Iz $\psi_1 \in \Psi$ slijedi $\mathfrak{M}, v \Vdash \psi_1$, a tada i $\mathfrak{M}, v \Vdash \psi_1 \vee \psi_2$. Sada slijedi $\psi_1 \vee \psi_2 \in \Psi$, odnosno $\psi_1 \vee \psi_2 \in A$. Analogno se dokazuje slučaj $\psi_2 \in A$.

Time smo dokazali da je skup formula A atom nad skupom $Cl(Dem(H, \Diamond\varphi))$ koji sadrži $Dem(H, \Diamond\varphi)$, to jest vrijedi $A \in H_{\Diamond\varphi}$. □

Lema 2.2.8. *Neka formula φ je ispunjiva ako i samo ako postoji atom H nad $Cl(\varphi)$ koji sadrži φ.*

Dokaz. Neka je H atom nad $Cl(\varphi)$ takav da vrijedi $\varphi \in H$. Po definiciji atoma imamo da je skup formula H ispunjiv pa je ispunjiva i svaka formula iz H. Tada je posebno i formula φ ispunjiva.

Dokažimo sada obrat. U tu svrhu pretpostavimo sada da je formula φ ispunjiva. Tada postoji model $\mathfrak{M} = (W, R, V)$ i svijet $w_0 \in W$ takav da $\mathfrak{M}, w_0 \Vdash \varphi$. Definiramo skup H ovako:

$$H = \{\psi \in Cl(\varphi) \mid \mathfrak{M}, w_0 \Vdash \psi\}$$

Dokažimo da je H Hintikkin skup nad $Cl(\varphi)$. Očito je $H \subseteq Cl(\varphi)$ i $\bot \notin H$, to jest vrijedi uvjet (H1).
Neka je $\neg\psi \in Cl(\varphi)$ proizvoljna formula. Tada vrijedi: $\neg\psi \in H$ ako i samo ako $\mathfrak{M}, w_0 \Vdash \neg\psi$, odnosno $\mathfrak{M}, w_0 \nVdash \psi$ što je ekvivalentno $\neg\psi \in H$. Slijedi da je ispunjen uvjet (H2).
Neka je $\psi_1 \vee \psi_2 \in Cl(\varphi)$. Tada je $\psi_1 \vee \psi_2 \in H$ ako i samo ako $\mathfrak{M}, w_0 \Vdash \psi_1 \vee \psi_2$, odnosno $\mathfrak{M}, w_0 \Vdash \psi_1$ ili $\mathfrak{M}, w_0 \Vdash \psi_2$. Vrijedi $\mathfrak{M}, w_0 \Vdash \psi_1$ ili $\mathfrak{M}, w_0 \Vdash \psi_2$ ako i samo ako $\psi_1 \in H$ ili $\psi_2 \in H$ pa je ispunjen uvjet (H3).

Time smo dokazali da je H Hintikkin skup nad $Cl(\varphi)$. Iz činjenice $\mathfrak{M}, w_0 \Vdash H$ slijedi da je H atom. Očito je $\varphi \in H$. □

Definicija 2.2.9. *Neka su H i Σ konačni skupovi formula takvi da je H Hintikkin skup nad Σ. Skup $\mathcal{H} \subseteq \mathcal{P}(\Sigma)$ nazivamo **skup svjedoka generiran Hintikkinim skupom** H **nad** Σ ako je $H \in \mathcal{H}$ i vrijedi sljedeće:*

(1) ako je $I \in \mathcal{H}$, tada za svaku formulu $\Diamond\varphi \in I$ postoji skup $J \in I_{\Diamond\varphi}$ takav da je $J \in \mathcal{H}$

(2) ako je $J \in \mathcal{H}$ i $J \neq H$ tada postoji $n > 0$ takav da postoje skupovi $I^0, \ldots, I^n \in \mathcal{H}$ takvi da je $H = I^0$, $J = I^n$ te za svaki i, $0 \leq i < n$, postoji formula $\Diamond\varphi \in I^i$ takva da je $I^{i+1} \in I^i_{\Diamond\varphi}$.

Napomena 2.2.10. *Kako su H i Σ konačni skupovi, tada je i skup svjedoka $\mathcal{H}$ generiran skupom H također konačan jer je $\mathcal{H} \subseteq \mathcal{P}(\Sigma)$. Nadalje, primijetimo da za svaki Hintikkin skup H nad Σ i svaku $\Diamond\varphi \in H$ vrijedi $Cl(Dem(H, \Diamond\varphi))$. Tada za sve skupove $I, J \in \mathcal{H}$ takve da $J \in I_{\Diamond\psi}$ za neku formulu $\Diamond\psi \in I$ vrijedi $deg(J) < deg(I)$.*

Lema 2.2.11. *Neka su H i Σ konačni skupovi formula takvi da je H Hintikkin skup nad Σ. Tada je H atom ako i samo ako postoji skup svjedoka koji je generiran Hintikkinim skupom H nad Σ.*

Dokaz. Indukcijom po stupnju skupa[1] Σ dokazujemo da za svaki atom H nad Σ postoji skup svjedoka generiran skupom H nad Σ.

Pretpostavimo da je stupanj skupa Σ jednak 0, odnosno Σ ne sadrži $\Diamond$-formule, te neka je H atom. Tada je skup $\mathcal{H} = \{H\}$ skup svjedoka koji je generiran Hintikkinim skupom H. Očito je $H \in \mathcal{H}$. Uvjet (1) iz definicije 2.2.9 ispunjen je jer u skupu H ne postoje $\Diamond$-formule, a uvjet (2) ispunjen je jer ne postoji $J \in \mathcal{H}$ takav da je $J \neq H$.

Neka je $n \in \mathbb{N}$ i pretpostavimo da tvrdnja vrijedi za sve parove skupova H' i Σ' gdje je H' atom nad Σ' i $deg(\Sigma') < n$. Neka je H atom nad Σ i $deg(\Sigma) = n$. Iz leme 2.2.7 slijedi da za svaku formulu $\Diamond\varphi \in H$ postoji barem jedan atom $I^\varphi \in H_{\Diamond\varphi}$. Kako iz napomene 2.2.10 slijedi da je stupanj skupa $Cl(Dem(H, \Diamond\varphi))$ manji od n i $I^\varphi \subseteq Cl(Dem(H, \Diamond\varphi))$, tada je i $deg(I^\varphi) < n$. Po pretpostavci indukcije tada slijedi da za svaku formulu $\Diamond\varphi \in H$ atom I^φ generira skup svjedoka $\mathcal{I}^\varphi$ nad $Cl(Dem(H, \Diamond\varphi))$. Definiramo skup

$$\mathcal{H} = \{H\} \cup \bigcup_{\Diamond\varphi \in H} \mathcal{I}^\varphi.$$

Dokažimo da je skup $\mathcal{H}$ skup svjedoka generiran skupom H nad Σ. Očito je $H \in \mathcal{H}$. Da bismo dokazali uvjet (1) iz definicije 2.2.9, neka je $I \in \mathcal{H}$ proizvoljan i $\Diamond\varphi \in I$. Promatramo dva slučaja:

- $I = H$
  Iz definicije skupa $\mathcal{H}$ znamo da je $\mathcal{I}^\varphi \subseteq \mathcal{H}$ gdje je $\mathcal{I}^\varphi$ skup svjedoka generiran skupom $I^\varphi \in H_{\Diamond\varphi}$. Kako je $I^\varphi \in \mathcal{I}^\varphi$, slijedi $I^\varphi \in \mathcal{H}$.

- $I \neq H$
  Tada je $I \in \mathcal{I}^\psi$ za neku formulu ψ takvu da je $\Diamond\psi \in H$. Kako je $\mathcal{I}^\psi$ skup svjedoka nad $Cl(Dem(H, \Diamond\varphi))$ slijedi da postoji skup $J \in I_{\Diamond\varphi}$ takav da je $J \in \mathcal{I}^\psi \subseteq \mathcal{H}$.

Kako bismo dokazali da vrijedi uvjet (2) iz definicije 2.2.9, uzmimo proizvoljan $J \in \mathcal{H}$ takav da $J \neq H$. Tada je $J \in \mathcal{I}^\varphi$ za neku formulu φ takva da $\Diamond\varphi \in H$ te je $\mathcal{I}^\varphi$ skup svjedoka generiran skupom $I^\varphi \in H_{\Diamond\varphi}$. Promatramo dva slučaja:

[1] Pojam stupnja skupa formula dan je u definiciji 1.1.4.

- $J = I^{\varphi}$
  Tada je traženi n jednak 1 jer je $\Diamond\varphi \in H = I^0$ i $I^1 = I^{\varphi} \in H_{\Diamond\varphi}$ pa vrijedi uvjet (2).

- $J \neq I^{\varphi}$
  Kako je $\mathcal{I}^{\varphi}$ skup svjedoka generiran skupom I^{φ}, postoji $m > 0$ i skupovi $J^0, \ldots, J^m$ takvi da je $J^0 = I^{\varphi}$ i $J^m = J$ te za svaki $0 \leq i < m$ postoji formula $\Diamond\psi \in J^i$ takva da $J^{i+1} \in J^i_{\Diamond\psi}$. Sada je $n = m + 1$, a traženi skupovi su $I^0 = H$, $I^i = J^{i-1}$ za $i = 1, \ldots, n$. Kako je $\Diamond\varphi \in H$ i $I^1 = I^{\varphi} \in H_{\Diamond\varphi}$, vrijedi uvjet (2).

Time je dokazano da je $\mathcal{H}$ generiran skupom H nad Σ.

Pretpostavimo sada da je $\mathcal{H}$ skup svjedoka nad Σ generiran skupom H. Pokazat ćemo da je skup H istinit na nekom modelu $\mathfrak{M} = (\mathfrak{F}, V)$ gdje je $\mathfrak{F}$ konačno stablo visine najviše $deg(H)$. Neka je $W = \{w_0, w_1, w_2, \ldots\}$ prebrojiv skup svjetova. Koristeći konačno mnogo svjetova iz W konstruirat ćemo stablasti model za H. Definiramo skupove

$$\begin{aligned} W_0 &= \{w_0\} \\ R_0 &= \emptyset \\ f_0(w_0) &= H. \end{aligned}$$

Pretpostavimo da su već definirani skupovi W_n, R_n i f_n. Ako za svaki svijet $w \in W_n$ i svaku formulu $\Diamond\varphi \in f_n(w)$ postoji svijet $w' \in W_n$ takav da je $\varphi \in f_n(w')$ i $f_n(w') \in f_n(w)_{\Diamond\varphi}$, tada stajemo s konstrukcijom. U suprotnom, neka je $w \in W_n$ takav da postoji $\Diamond\varphi \in f_n(w)$ i ne postoji $w' \in W_n$ takav da $\varphi \in f_n(w')$ i $f_n(w') \in f_n(w)_{\Diamond\varphi}$. Definiramo skupove W_{n+1}, R_{n+1} i f_{n+1} na sljedeći način:

$$\begin{aligned} W_{n+1} &= W_n \cup \{w_{n+1}\} \\ R_{n+1} &= R_n \cup \{(w, w_{n+1})\} \\ f_{n+1} &= f_n \cup \{(w_{n+1}, I)\} \end{aligned}$$

gdje je $I \in \mathcal{H}$ takav da je $I \in f_n(w)_{\Diamond\varphi}$. Primijetimo da takav skup I uvijek postoji jer je $\mathcal{H}$ skup svjedoka pa vrijedi uvjet (1) definicije 2.2.9.

Kako je Σ konačan skup te je $\mathcal{H} \subseteq \Sigma$, tada i svaki $I \in \mathcal{H}$ ima konačno mnogo formula oblika $\Diamond\varphi$ pa ovaj proces mora završiti nakon konačno mnogo koraka. Iz konačnosti skupova $I \in \mathcal{H}$ također slijedi da će stablo koje konstruiramo imati konačno mnogo grananja. Nadalje, iz napomene 2.2.10 slijedi da za svaki $w, w' \in W_n$ takve da wR_nw' vrijedi $deg(f_n(w')) < deg(f_n(w))$ pa će visina stabla biti najviše $deg(H)$.

Neka je m broj iteracija nakon kojih proces stane. Definiramo okvir $\mathfrak{F} = (W_m, R_m)$. Za valuaciju odaberemo bilo koju funkciju $V : \Sigma \to \mathcal{P}(W_m)$ za koju vrijedi da je $w \in V(p)$ ako i samo ako je $p \in f_m(w)$. Neka je model $\mathfrak{M} = (\mathfrak{F}, V)$. Preostalo je još dokazati da $\mathfrak{M}, w_0 \Vdash H$.

Indukcijom po složenosti formule φ dokazujemo da za svaki $w \in W_m$ vrijedi sljedeća ekvivalencija:

$$\mathfrak{M}, w \Vdash \varphi \text{ ako i samo ako } \varphi \in f_m(w).$$

Ako je $\varphi \equiv p$ za neku propozicionalnu varijablu p, tada tvrdnja slijedi iz definicije valuacije V. Ako je $\varphi \equiv \bot$, tvrdnja slijedi iz uvjeta (H1) u definiciji Hintikkinog skupa.
Neka je $n \in \mathbb{N} \setminus \{0\}$ i pretpostavimo da za sve formule složenosti strogo manje od n vrijedi tvrdnja. Slučaj $\varphi \equiv \neg\psi$ slijedi iz pretpostavke indukcije i uvjeta (H2). Slučaj $\varphi \equiv \psi_1 \vee \psi_2$ slijedi iz pretpostavke indukcije i uvjeta (H3).
Promotrimo još slučaj $\varphi \equiv \Diamond\psi$. Pretpostavimo da vrijedi $\mathfrak{M}, w \Vdash \Diamond\psi$. Tada postoji $w' \in W_m$ takav da wR_mw' i $\mathfrak{M}, w' \Vdash \psi$. Iz pretpostavke indukcije tada slijedi $\psi \in f_m(w')$.
Pretpostavimo sada da vrijedi $\Diamond\psi \in f_m(w)$. Iz konstrukcije modela slijedi da postoji $w' \in W_m$ takav da $\psi \in f_m(w')$ i $f_m(w') \in f_m(w)_{\Diamond\psi}$ te je wRw'. Kako je ψ složenosti strogo manje od n, iz pretpostavke indukcije slijedi $\mathfrak{M}, w' \Vdash \psi$ pa zbog wRw' imamo $\mathfrak{M}, w \Vdash \Diamond\psi$.

Kako je $H = f_m(w_0)$, tada za svaku formulu $\varphi \in H$ vrijedi $\mathfrak{M}, w_0 \Vdash \varphi$, odnosno vrijedi $\mathfrak{M}, w_0 \Vdash H$. □

Leme 2.2.8 i 2.2.11 daju nam strategiju za ispitivanje ispunjivosti proizvoljne modalne formule φ. Naime, iz leme 2.2.8 slijedi da je formula φ ispunjiva ako i samo ako postoji atom nad $Cl(\varphi)$ koji sadrži φ, a iz leme 2.2.11 slijedi da takav atom postoji ako i samo ako postoji Hintikkin skup nad $Cl(\varphi)$ koji generira skup svjedoka nad $Cl(\varphi)$.

Nadalje, iz leme 2.2.11 slijedi da je svaki atom H ispunjiv na stablastom modelu polinomne visine u odnosu na $deg(H)$.

Također, iz navedene leme dobili smo sintaktički kriterij za provjeru ispunjivosti formule φ - postojanje skupa svjedoka. Kako su skupovi svjedoka konačni skupovi, možemo osmisliti algoritam koji provjerava njihovo postojanje.

Sada navodimo pseudokod već spomenutog algoritma *Svjedok*. Taj algoritam kao ulaz prima dva konačna skupa H i Σ te vraća DA ako i samo ako je H Hintikkin skup i postoji skup svjedoka generiran skupom H nad Σ.

Algoritam *Svjedok*(H, Σ)
ako H je Hintikkin skup nad Σ **i** za svaku $\Diamond\psi \in H$ postoji skup formula $I \in H_{\Diamond\psi}$
takav da Svjedok$(I, Cl(Dem(H, \Diamond\psi))) =$ DA
tada vrati DA
inače vrati NE

Sada dokazujemo da je navedeni algoritam korektan. Indukcijom po stupnju skupa Σ lako se pokaže da algoritam *Svjedok* vraća DA ako je H Hintikkin skup nad Σ koji generira skup svjedoka. Dokaz da je H Hintikkin skup nad Σ koji generira skup svjedoka ako

algoritam *Svjedok* vraća DA analogan je dokazu tvrdnje da H generira skup svjedoka ako je H atom koju smo dokazali lemom 2.2.11.

Sada možemo dokazati da problem složenosti logike **K** pripada klasi PSPACE. U tu ćemo svrhu opisati implementaciju jednog algoritma koji odlučuje je li zadana formula φ ispunjiva na Turingovom stroju koji koristi $O(|\varphi|^k)$ registara za neki $k \in \mathbb{N}$. Glavna komponenta algoritma biti će upravo prethodno opisani algoritam *Svjedok* koji će provjeriti postoji li skup svjedoka generiran Hintikkinim skupom H nad $Cl(\varphi)$ takav da $\varphi \in H$, čime će ujedno provjeriti i ispunjivost formule φ. Algoritam ćemo implementirati na nedeterminističkom Turingovom stroju iz čega će slijediti da problem ispunjivosti logike **K** pripada klasi NPSPACE, no time ćemo ujedno dokazati i pripadnost klasi PSPACE jer znamo da iz Savitchevog teorema slijedi NPSPACE = PSPACE.

Teorem 2.2.12. *Problem ispunjivosti normalne modalne logike **K** pripada klasi PSPACE.*

Dokaz. Iz leme 2.2.8 slijedi da je formula φ ispunjiva ako i samo ako postoji atom H nad $Cl(\varphi)$ takav da je $\varphi \in H$. Zatim, iz leme 2.2.11 slijedi da takav atom H postoji ako i samo ako H generira skup svjedoka nad $Cl(\varphi)$. Kako je skup H Hintikkin skup nad $Cl(\varphi)$, H generira skup svjedoka ako i samo ako algoritam *Svjedok* vraća DA kada na ulazu ima skupove H i $Cl(\varphi)$. Primijetimo da je za dokaz teorema dovoljno dokazati da postoji Turingov stroj koji za proizvoljnu formulu φ pronalazi skup $H \subseteq Cl(\varphi)$ takav da $\varphi \in H$ i pomoću algoritma *Svjedok* odlučuje je li H Hintikkin skup nad $Cl(\varphi)$ koji generira skup svjedoka. Pri tome stroj smije koristiti najviše polinomno mnogo registara u odnosu na $|\varphi|$.

Opišimo sada rad nedeterminističkog Turingovog stroja T koji odlučuje ispunjivost proizvoljne formule. Na početku je na traci stroja zapisana formula φ. Taj početni zapis stroj nikada ne mijenja nego prepisuje formulu φ svaki put kada mu je potrebna. Stroj T nedeterministički odabere Hintikkin skup $H \subseteq Cl(\varphi)$ takav da $\varphi \in H$. Nakon toga stroj T pokrene algoritam *Svjedok* sa skupovima H i $Cl(\varphi)$ kao ulaznim podacima. Ako algoritam *Svjedok* vrati DA, stroj staje u stanju prihvaćanja. U suprotnom stane u stanju odbijanja. Preostalo je još opisati implementaciju algoritma *Svjedok*.

Primijetimo prvo da su ulazni podaci u svim pozivima algoritma *Svjedok* podskupovi od $Cl(\varphi)$. Proizvoljan skup $S \subseteq Cl(\varphi)$ možemo reprezentirati na Turingovom stroju koristeći zapis formule φ i posebne oznake koje ćemo zvati pokazivači. Pokazivač na propozicionalnu varijablu p u φ znači da p pripada skupu S. Pokazivač na veznik znači da potformula ψ od φ čiji je glavni veznik upravo označeni veznik znači da ψ pripada skupu S. Ako je pokazivač na modalnom operatoru, tada potformula od φ koja započinje tim operatorom pripada skupu S. Dakle, za reprezentaciju proizvoljnog podskupa od $Cl(\varphi)$ dovoljno nam je $O(|\varphi|)$ registara. Nadalje, algoritam *Svjedok* je rezukurzivni algoritam. Da bismo omogućili rekurzivne pozive, stroju T dodajemo stog. Prije svakog rekurzivnog

poziva na stog prepišemo reprezentaciju skupova koja se trenutno nalazi na traci te ju izbrišemo s trake, a na traku prepišemo formulu φ i pokazivačima odredimo skupove za novi poziv algoritma *Svjedok*. Kada taj poziv završi, na traku prepisujemo formule sa stoga te ih brišemo sa stoga. Na stogu koristimo i posebne znakove koje koristimo kao granice između formula.

Sada opisujemo rad stroja za prvi poziv algoritma *Svjedok* sa skupovima H i $Cl(\varphi)$ kao ulaznim podacima. Svi ostali pozivi algoritma rade analogno, samo s drugim ulaznim podacima. Stroj prvo provjerava je li H Hintikkin skup nad $Cl(\varphi)$ tako da prolazi kroz formulu φ i traži pokazivače, odnosno potformule od φ koje pripadaju skupu H. Istovremeno stroj provjerava vrijede li uvjeti iz definicije 2.2.5. Ako H nije Hintikkin skup, stroj prekida rad i odlazi u stanje odbijanja. U suprotnom, stroj ponovo prolazi po formuli φ i traži potformule oblika $\Diamond\psi$ koje su u skupu H. Za svaku potformulu $\Diamond\psi$ nedeterministički odabire skup $I \in H_{\Diamond\psi}$ za koji algoritam $Svjedok(I, Cl(Dem(H, \Diamond\psi)))$ vraća DA. Ako takav skup ne postoji, stroj odlazi u stanje odbijanja. U suprotnom, stroj traži sljedeću $\Diamond$-potformulu. Ako je za svaku formulu $\Diamond\psi \in H$ stroj T pronašao skup $I \in H_{\Diamond\psi}$ takav da algoritam $Svjedok(I, Cl(Dem(H, \Diamond\psi)))$ vraća DA, stroj odlazi u stanje prihvaćanja, odnosno zaključujemo da je formula φ ispunjiva.

Primijetimo da algoritam *Svjedok* ne može raditi beskonačno. Za svaki Hintikkin skup H nad $Cl(\varphi)$ takav da je $deg(\varphi) = n$ i proizvoljnu formulu $\Diamond\psi \in H$ očito vrijedi sljedeća nejednakost:

$$deg(Cl(Dem(H, \Diamond\psi))) < n$$

Kako je svaki skup $I \in H_{\Diamond\psi}$ podskup od $Cl(Dem(H, \Diamond\psi))$ tada je i $deg(I) < n$. Nakon najviše $deg(\varphi)$ rekurzivnih poziva algoritma *Svjedok* dolazimo do skupa stupnja 0 koji ne sadrži $\Diamond$-formule te više nema rekurzivnih poziva. Dakle, dubina rekurzije je najviše $deg(\varphi)$ pa stroj T sigurno staje u nekom završnom stanju nakon konačno mnogo koraka.

Preostalo nam je još analizirati prostornu složenost stroja T. Na traci stroja T u svakom je trenutku iskorišteno najviše $O(|\varphi|)$ registara jer na traci imamo:

- zapis formule φ,
- jedan zapis formule φ s pokazivačima koji reprezentira prvi ulazni podatak algoritma *Svjedok*,
- jedan zapis formule φ s pokazivačima koji reprezentira drugi ulazni podatak algoritma *Svjedok*.

Između svakog zapisa od formule φ koristimo kao i na stogu poseban znak kao graničnik. Na stog stroja zapisujemo dva zapisa formule φ s pokazivačima prije svakog rekurzivnog poziva. Kako je dubina rekurzije najviše $deg(\varphi)$ što je manje ili jednako od $|\varphi|$, u svakom

trenutku na stogu može biti iskorišteno najviše $O(|\varphi|^2)$ registara. Dakle, stroj T koristi najviše $O(|\varphi|^2)$ registara.

Ovime smo dokazali da problem ispunjivosti normalne modalne logike **K** pripada klasi NPSPACE. Sada iz PSPACE = NPSPACE slijedi da problem ispunjivosti modalne logike **K** pripada klasi PSPACE. □

Klasi PSPACE pripadaju i problem ispunjivosti modalnih logika **T**, **K4** i **S4** što se može dokazati na način sličan dokazu teorema 2.2.12 uz modifikaciju algoritma *Svjedok*.

U nastavku dokazujemo Ladnerov teorem koji kaže da je problem ispunjivosti svake normalne modalne logike Λ takve da $\mathbf{K} \subseteq \Lambda \subseteq \mathbf{S4}$ jedan PSPACE-težak problem. U dokazu koristimo problem određivanja istinitosti zatvorenih **QBF**-formula koji sada opisujemo.

Definicija 2.2.13. ***Skup kvantificiranih formula logike sudova*** *je najmanji skup X koji sadrži sve formule logike sudova takav da za svaku $F \in X$ i propozicionalnu varijablu p vrijedi $\forall pF \in X$ i $\exists pF \in X$.*

Kažemo da je kvantificirana formula logike sudova zatvorena ako je svaka propozicionalna varijabla p, koja nastupa u formuli, u dosegu nekog kvantifikatora $\forall$ ili $\exists$.

Kažemo da je kvantificirana formula logike sudova u preneksnoj formi ako je oblika $Q_1 p_1 \ldots Q_m p_m F(p_1, \ldots, p_m)$ gdje je F formula logike sudova, a $Q_i \in \{\forall, \exists\}$.

*Skup **QBF** definiramo kao skup svih kvantificiranih formula logike sudova u preneksnoj formi. Formule koje pripadaju skupu **QBF** nazivamo **QBF-formule**.*

Primijetimo da je formula $\forall pF$ logički ekvivalentna formuli $F(\bot/p) \wedge F(\top/p)$, a formula $\exists pF$ logički je ekvivalentna formuli $F(\bot/p) \vee F(\top/p)$. Reći ćemo da je zatvorena **QBF**-formula $\forall pF$ istinita ako je istinita formula $F(\bot/p) \wedge F(\top/p)$. Slično, reći ćemo da je zatvorena **QBF**-formula $\exists pF$ istinita ako je istinita formula $F(\bot/p) \vee F(\top/p)$.

Definiramo problem određivanja istinitosti **QBF**-formula:

$$\mathsf{TQBF} = \{F \mid F \text{ je istinita zatvorena } \mathbf{QBF}\text{-formula}\}$$

Problem TQBF prvi je problem za kojeg je dokazano da je PSPACE-potpun, a dokaz se može pročitati u [5].

Primjer 2.2.14. *a) Formula $\forall p_1 \exists p_2(\neg p_1 \leftrightarrow p_2)$ je istinita **QBF**-formula*

*b) Formula $\forall p(p \wedge \neg p)$ nije istinita **QBF**-formula*

Svakoj **QBF**-formuli F možemo pridružiti neko označeno stablo. Ako je F formula logike sudova, to jest nema kvantifikatora, tada joj pridružujemo stablo koje ima samo korijen bez oznake.

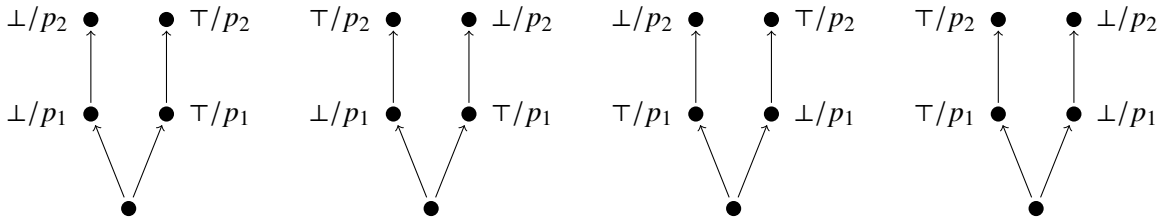
Pretpostavimo da je $F \equiv Q_1 p_1, \ldots, Q_n p_n G(p_1, \ldots, p_n)$. Na razini nula nalazi se neoznačeni korijen. Ako je $Q_i = \forall$, tada svaki čvor na razini $i-1$ ima dva sljedbenika - jedan označen s $\bot/p_i$, drugi označen s $\top/p_i$. Ako je $Q_i = \exists$, tada svaki čvor na razini $i-1$ ima jednog sljedbenika označenog s $\bot/p_i$ ili $\top/p_i$. Ovakva stabla nazivat ćemo **kvantifikacijska stabla**. Primijetimo da oznaka svakog čvora na razini i predstavlja supstituciju varijable p_i u formuli G logičkom konstantom $\bot$ ili $\top$.

Neka je $F \equiv Q_1 p_1, \ldots, Q_n p_n G(p_1, \ldots, p_n)$ prozvoljna **QBF**-formula i neka je T neko kvantifikacijsko stablo za F. Neka je r korijen stabla te neka su $l_1, \ldots, l_m$ listovi. Uvrštavanjem supstitucija kojima su označeni čvorovi na jedinstvenom putu od korijena do lista l_j u formulu G dobivamo formulu G_j u kojoj su sve propozicionalne varijable $p_1, \ldots, p_n$ zamijenjene konstantama $\bot$ ili $\top$, ovisno o oznakama čvorova u putu. Formula G_j je ili istinita ili lažna. Ako su sve formule G_j za $j = 1, \ldots, m$ istinite, tada kažemo da stablo T **potvrđuje istinitost formule** F.

Vrijedi sljedeća ekvivalencija:

formula F je istinita ako i samo ako postoji kvantifikacijsko stablo koje potvrđuje istinitost od F.

Primjer 2.2.15. *Ovdje navodimo kvantifikacijska stabla T_1, T_2, T_3 i T_4 za **QBF**-formulu $F \equiv \forall p_1 \exists p_2 (\neg p_1 \leftrightarrow p_2)$.*



Stabla T_2 i T_3 potvrđuju istinitost formule F. Naime, uvrštavanjem supstitucija kojima su označeni čvorovi stabla T_2 u formulu $\neg p_1 \leftrightarrow p_2$ dobivamo formule $\neg\bot \leftrightarrow \top$ i $\neg\top \leftrightarrow \bot$ koje su istinite, a uvrštavanjem supstitucija kojima su označeni čvorovi stabla dobivamo formule $\neg\top \leftrightarrow \bot$ i $\neg\bot \leftrightarrow \top$ koje su također istinite.

S druge strane, uvrštavanjem supstitucija kojima su označeni čvorovi stabla T_1 u formulu $\neg p_1 \leftrightarrow p_2$ dobivamo formule $\neg\bot \leftrightarrow \bot$ i $\neg\top \leftrightarrow \top$ koje nisu istinite, a uvrštavanjem supstitucija kojima su označeni čvorovi stabla T_4 dobivamo formule $\neg\top \leftrightarrow \top$ i $\neg\bot \leftrightarrow \bot$ koje također nisu istinite.

Sada koristeći problem TQBF dokazujemo Ladnerov teorem.

Teorem 2.2.16 (Ladnerov teorem)**.** *Neka je* Λ *normalna modalna logika takva da* $\mathbf{K} \subseteq \Lambda \subseteq \mathbf{S4}$*. Problem ispunjivosti logike* Λ *je* PSPACE*–težak problem.*

Dokaz. Dokazat ćemo da je problem TQBF polinomno reducibilan na problem ispunjivosti logike Λ.

Neka je $F \equiv Q_1 p_1 \dots Q_m p_m G(p_1, \dots, p_m)$ proizvoljna zatvorena **QBF**-formula. Definirat ćemo modalnu formulu φ_F takvu da vrijedi sljedeće:

QBF–fromula F je istinita ako i samo ako modalna formula φ_F je Λ-ispunjiva.

U formuli φ_F koristimo propozicionalne varijable $q_0, \dots, q_m$ i $p_1, \dots, p_m$ te pokrate 2.1 i 2.2 definirane u dokazu teorema 2.2.2. Najprije definiramo pomoćne formule:

$$\varphi_1(F) \equiv \bigwedge_{i=0}^{m} \Box^{(m)} \left(q_i \to \wedge_{j \neq i} \neg q_j \right)$$

$$\varphi_2(F) \equiv \bigwedge_{i=0}^{m-1} \Box^{(m)} (q_i \to \Diamond q_{i+1})$$

$$\varphi_3(F) \equiv \bigwedge_{\{i \mid Q_i = \forall\}} \Box^{i-1} B_{i-1}$$

$$\begin{aligned} \varphi_4(F) \equiv \Box S(p_1, \neg p_1) \wedge \Box^2 S(p_1, \neg p_1) \wedge \Box^2 S(p_1, \neg p_1) \wedge \dots \wedge \Box^{m-1} S(p_1, \neg p_1) \\ \wedge \Box^2 S(p_2, \neg p_2) \wedge \Box^3 S(p_2, \neg p_2) \wedge \dots \wedge \Box^{m-1} S(p_2, \neg p_2) \\ \wedge \Box^3 S(p_3, \neg p_3) \wedge \dots \wedge \Box^{m-1} S(p_3, \neg p_3) \\ \vdots \\ \wedge \Box^{m-1} S(p_{m-1}, \neg p_{m-1}) \end{aligned}$$

$$\varphi_5(F) = \Box^m (q_m \to G)$$

U nastavku dokaza dat ćemo intutitivne opise upravo definiranih formula.

Definiramo traženu formulu φ_F ovako:

$$\varphi_F \equiv q_0 \wedge \varphi_1(F) \wedge \varphi_2(F) \wedge \varphi_3(F) \wedge \varphi_4(F) \wedge \varphi_5(F).$$

Pretpostavimo prvo da je zatvorena **QBF**–formula F istinita. Tada postoji kvantifikacijsko stablo $T = (S, P)$ koje potvrđuje istinitost formul F. Dokazat ćemo da postoji **S4**-model $\mathfrak{M} = (W, R, V)$ i svijet $w_0 \in W$ takav da vrijedi $\mathfrak{M}, w_0 \Vdash \varphi_F$. Iz $\Lambda \subseteq \mathbf{S4}$ će slijediti da je model $\mathfrak{M}$ i Λ-model te da je modalna formula φ_F Λ-ispunjiva.

Primijetimo da su formule $\varphi_1(F)$ i $\varphi_4(F)$ jednake redom formulama $\varphi_1(m)$ i $\varphi_3(m)$ iz dokaza teorema 2.2.2. Formula $\varphi_1(F)$ osigurava da je varijabla q_i istinita samo na svjetovima na i-toj razini stabla. Formula $\varphi_4(F)$ "čuva" istinitost varijable p_i na sljedećim razinama stabla - ako je p_i istinita na nekom svijetu w na k-toj razini stabla, tada je p_i istinita na svim svjetovima v na razini $k+1$ za koje je wRv. Obratno, ako p_i nije istinita na nekom svijetu w na k-toj razini, tada p_i nije istinita ni na svjetovima v na razini $k+1$ takvim da wRv. Iz istinitosti formule $\varphi_5(F)$ slijedi da je formula G istinita na svim svjetovima na m-toj razini.

Iz kvantifikacijskog stabla T za formulu F možemo konstruirati okvir za model $\mathfrak{M}$. Definiramo nosač W kao skup S te definiramo relaciju dostiživosti R kao refleksivno i tranzitivno zatvorenje relacije P. Kako je R refleksivna i tranzitivna relacija, slijedi da je okvir (W, R) jedan **S4**-okvir. Valuaciju V definiramo na sljedeći način:

- $V(q_i) = \{w \in W \mid w \text{ se nalazi na } i\text{-toj razini stabla } T\}$, za $i \in \{0, \ldots, m\}$
- Ako u stablu T postoji čvor w označen s $\top/p_i$, tada je $V(p_i) = \{w\} \cup \{v \in W \mid wRv\}$. U suprotnom je $V(p_i) = \emptyset$

Neka je w_0 korijen stabla T. Lako se provjeri da vrijedi $\mathfrak{M}, w_0 \Vdash \varphi_F$ iz čega slijedi da je formula φ_F istinita na **S4** modelu. No, tada je istinita i na Λ-modelu.

Doakžimo sada obratnu implikaciju. U tu svrhu pretpostavimo da je modalna formula φ_F Λ-ispunjiva. Iz pretpostavke teorema $\mathbf{K} \subseteq \Lambda$ slijedi da je modalna formula φ_F također i $\mathbf{K}$-ispunjiva. Primijetimo da je stupanj formule φ_F jednak m. Iz dokaza leme 2.2.11 slijedi da je formula φ_F istinita na korijenu w_0 nekog stablastog modela $\mathfrak{M} = (W, R, V)$ visine najviše m. Sada iz stabla (W, R) možemo dobiti kvantifikacijsko stablo za formulu F. Naime, iz istinitosti formule $\varphi_2(F)$ na w_0 slijedi da svaki čvor osim listova ima barem jednog sljedbenika. Iz istinitosti formule $\varphi_3(F)$ na svijetu w_0 slijedi da ako je kvantifikator Q_i u formuli F jednak $\forall$, tada svaki čvor na razini $i-1$ ima barem dva sljedbenika te je na barem jednom od njih istinita varijabla p_i, a na barem jednom od njih nije istinita varijabla p_i.

Neka je $S = \{w_0\}$ te $P = \emptyset$. Razinu po razinu gradimo kvantifikacijsko stablo za formulu F. Za svaki $i = 1, \ldots, m$ promatramo dva slučaja:

- $Q_i = \exists$
  Za svaki čvor w na razini $i-1$ stabla (W, R) takav da $w \in S$ odaberemo neki njegov sljedbenik v te skupu S dodajemo v, a relaciji P dodajemo par (w, v). Takav sljedbenik v sigurno postoji zbog istinitosti formule $\varphi_2(F)$ na svijetu w_0. Čvor v označimo sa $\top/p_i$ ako $v \in V(p_i)$, inače ga označimo sa $\bot/p_i$.
- $Q_i = \forall$
  Za svaki čvor w na razini $i-1$ stabla (W, R) takav da $w \in S$ odaberemo njegova dva sljedbenika v_1 i v_2 takvi da $v_1 \in V(p_i)$ i $v_2 \notin V(p_i)$. Takvi sljedbenici postoje

zbog istinitosti formule $\varphi_3(F)$ na svijetu w_0. Skupu S dodajemo v_1 i v_2, a relaciji P dodajemo parove (w, v_1) i (w, v_2). Čvor v_1 označimo sa $\top/p_i$, a čvor v_2 označimo sa $\bot/p_i$

Primijetimo da u oba slučaja postoji barem jedan, a najviše dva svijeta w na razini $i-1$ stabla (W, R) takvi da $w \in S$.

Definiramo označeno stablo $T = (S, P)$. Lako se vidi da je T kvantifikacijsko stablo za F koje potvrđuje istinitost od F.

Preostalo je još dokazati da formulu φ_F možemo konstruirati u polinomnom vremenu u odnosu na $|F|$. Kao i u dokazu teorema 2.2.2, vrijedi $|\varphi_1(F)| \in O(m^3)$ te $|\varphi_4(F)| \in O(m^3)$ gdje je m broj propozicionalnih varijabli u F. Na sličan se način može pokazati da je $|\varphi_2(F)| \in O(m^3)$ i $|\varphi_3(F)| \in O(m^3)$. U formuli $\varphi_5(F)$ je m nastupa operatora $\Box$ pa je $|\varphi_5(F)| \in O(m+|G|)$. Sada za formulu φ_F vrijedi $|\varphi_F| \in O(m^3+|G|)$. Kako je $|F| \in O(m+|G|)$ slijedi da se formula φ_F može konstruirati u polinomnom vremenu u odnosu na $|F|$. $\Box$

Primjer 2.2.17. *Promotrimo primjer formule φ_F iz prethodnog teorema 2.2.16 za $F \equiv \forall p_1 \exists p_2(\neg p_1 \leftrightarrow p_2)$.*

$$\begin{aligned}\varphi_1(F) \equiv\ & q_0 \to (\neg q_1 \wedge \neg q_2) \wedge \Box(q_0 \to (\neg q_1 \wedge \neg q_2)) \wedge \Box\Box(q_0 \to (\neg q_1 \wedge \neg q_2)) \wedge \\ & q_1 \to (\neg q_0 \wedge \neg q_2) \wedge \Box(q_1 \to (\neg q_0 \wedge \neg q_2)) \wedge \Box\Box(q_1 \to (\neg q_0 \wedge \neg q_2)) \wedge \\ & q_2 \to (\neg q_0 \wedge \neg q_1) \wedge \Box(q_2 \to (\neg q_0 \wedge \neg q_1)) \wedge \Box\Box(q_2 \to (\neg q_0 \wedge \neg q_1))\end{aligned}$$

$$\begin{aligned}\varphi_2(F) \equiv\ & (q_0 \to \Diamond q_1) \wedge \Box(q_0 \to \Diamond q_1) \wedge \Box\Box(q_0 \to \Diamond q_1) \wedge \\ & (q_1 \to \Diamond q_2) \wedge \Box(q_1 \to \Diamond q_2) \wedge \Box\Box(q_1 \to \Diamond q_2)\end{aligned}$$

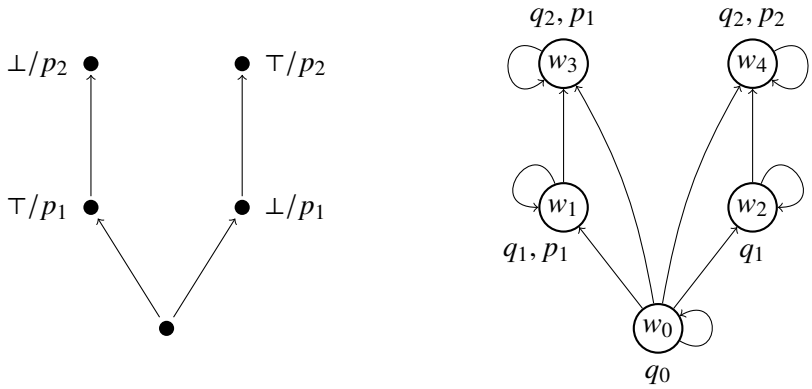
$$\varphi_3(F) \equiv q_0 \to (\Diamond(q_1 \wedge p_1) \wedge \Diamond(q_1 \wedge \neg p_1))$$

$$\varphi_4(F) \equiv \Box((p_1 \to \Box p_1) \wedge (\neg p_1 \to \Box\neg p_1))$$

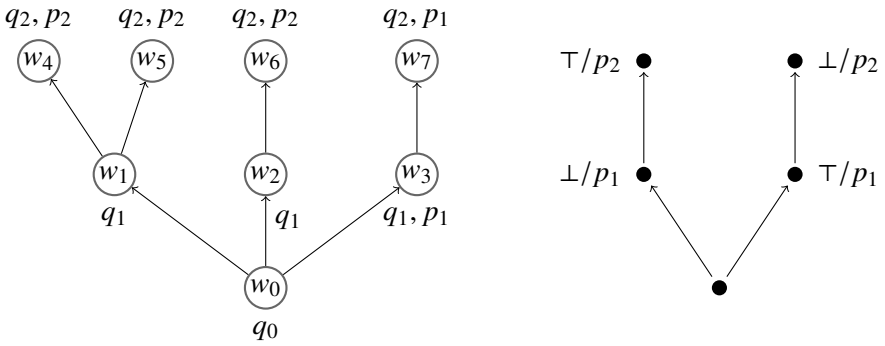
$$\varphi_5(F) \equiv \Box\Box(q_2 \to (\neg p_1 \leftrightarrow p_2))$$

Imamo $\varphi_F = q_0 \wedge \varphi_1(F) \wedge \varphi_2(F) \wedge \varphi_3(F) \wedge \varphi_4(F) \wedge \varphi_5(F)$.

*a) Lako se vidi je F istinita formula. Na sljedećoj slici ilustrirano je kvantifikacijsko stablo koje potvrđuje istinitost od F te **S4**-model dobiven postupkom iz dokaza teorema 2.2.16.*



*b) Obratno, lako je pronaći **K**-model na kojemu je φ_F ispunjiva. Na sljedećoj slici ilustrirani je jedan takav **K**-model te kvantifikacijsko stablo koje potvrđuje istinitost od F dobiveno postupkom iz dokaza teorema 2.2.16.*



Čvorovi kvantifikacijskog stabla su svjetovi w_0, w_1, w_3, w_5 te w_7.

Iz teorema 2.2.16 slijedi da su problemi ispunjivosti logika **K**, **T**, **K4** te **S4** PSPACE-teški problemi. Kako problemi ispunjivosti navedenih logika pripadaju klasi PSPACE, slijedi da su PSPACE-potpuni. Iz PSPACE = co-PSPACE slijedi i da je problem valjanosti navedenih logika PSPACE-potpun.

2.3 Umjesto zaključka

Spomenimo još neke modalne logike te ukratko komentirajmo njihovu složenost. Linearna temporalna logika, kratko: LTL, definirana je 1977. godine kao sredstvo za formalnu verifikaciju računalnih programa. Dokazano je da je ona PSPACE–potpuna. Da bi se to dokazalo, prvo se dokaže da je tzv. problem provjere modela za LTL (eng. *model checking problem*) jedan PSPACE–težak problem. Nakon toga dokaže se da je taj problem polinomno reducibilan na problem ispunjivosti za logiku LTL. Iz toga odmah slijedi da je problem ispunjivosti za logiku LTL također PSPACE–težak. Zatim se definira nedeterministički Turingov stroj polinomne prostorne složenosti koji odlučuje problem ispunjivosti logike LTL. Iz toga slijedi da problem ispunjivosti za logiku LTL pripada klasi složenosti NPSPACE. Iz Savitchevog teorema slijedi da problem ispunjivosti logike LTL pripada klasi složenosti PSPACE. Detaljan dokaz može se pročitati u [6].

Propozicionalna dinamička logika, kratko: PDL, dobivena je iz dinamičke logike, također u svrhu formalne verifikacije programa, a primjenjuje se još i u umjetnoj inteligenciji, filozofiji i lingvistici. Logika PDL je EXPTIME–potpuna, a detaljan dokaz nalazi se u [1]. Svođenjem na varijantu problema popločavanja, zvane i igra popločavanja koridora za dva igrača, dokaže se da je problem ispunjivosti za logiku PDL jedan EXPTIME–težak problem. Postupkom koji se naziva eliminacija Hintikkinih skupova, dokazuje se da problem ispunjivosti za logiku PDL pripada klasi složenosti EXPTIME.

Kao što smo spomenuli na početku ovog poglavlja, više je neodlučivih modalnih logika nego onih odlučivih. Primjer neodlučive modalne logike je logika Tile. Pripadni alfabet sadrži modalne operatore $\Diamond_r$ i $\Diamond_u$ koji se interpretiraju na standardni način te univerzalni modalni operator E. Formula $\mathsf{E}\varphi$ istinita je na nekom svijetu modela $\mathfrak{M}$ ako je formula φ istinita na nekom svijetu modela $\mathfrak{M}$. Neodlučivost logike Tile dokazuje se svođenjem na poznati neodlučivi problem popločavanje $\mathbb{N}\times\mathbb{N}$ ravnine. Micanjem operatora E iz alfabeta dobivamo NP–potpunu logiku $\mathtt{Tile}^{-}$. Više o neodlučivosti logike Tile te složenosti logike $\mathtt{Tile}^{-}$ može se pronaći u [4].

Bibliografija

[1] P. Blackburn, M. de Rijke i Y. Venema, *Modal Logic*, Cambrdige University Press, 2001.

[2] R. E. Ladner, *The Computational Complexity of Provability in Systems of Modal Propositional Logic*, SIAM J. Comput. **6** (1977), 467–480.

[3] M. Marx, *Complexity of Modal Logic*, Handbook of Modal Logic (P. Blackburn, J. van Benthem i F. Wolter, ur.), Elsevier, 2007.

[4] M. Marx i Y. Venema, *Local Variations on a Loose Theme: Modal Logic and Decidability*, 2007.

[5] M. Sipser, *Introduction to the Theory of Computation*, Cengage Learning, 2013.

[6] A. Sistla i E. Clarke, *The Complexity of Propositional Linear Temporal Logics*, J. ACM **32** (1985), 733–749.

[7] E. Spaan, *Complexity of Modal Logics*, Disertacija, University of Amsterdam, 1993.

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

Sažetak

Glavni cilj ovog rada je dokazati nekoliko rezultata o složenosti modalnih logika. Rad je podijeljen u dva poglavlja. U prvom se poglavlju bavimo sintaksom i semantikom osnovnog modalnog jezika. Definiramo pojmove alfabeta i formula, Kripkeovih okvira i modela te istinitost i valjanost modalnih formula. Zatim definiramo najmanju normalnu modalnu logiku **K** te neka njezina proširenja - logike **K4**, **T**, **S4**, **S5** te **S4.3**. U prvom poglavlju dajemo i osnovne pojmove i rezultate teorije modela modalne logike. Definiramo redom sljedeće pojmove: generirani podmodel, izomorfizam i ograničeni morfizam. Za svaku od upravo navedenih konstrukcija modela dokazujemo da čuva istinitost. Definiramo i svojstvo konačnih modela i okvira. Na kraju poglavlja opisujemo karakteristične klase okvira pojedinih modalnih logika.

U drugom poglavlju razmatramo složenost normalnih modalnih logika koje smo definirali u prvom poglavlju. Prvo definiramo pojam polinomnog svojstva konačnih modela te pojam definabilnosti klase okvira u logici prvog reda. Ti su pojmovi ključni za dokaz NP–potpunost logike **S5** te za dokaz Hemaspaandrinog teorema o NP–potpunosti modalnih logika koje proširuju **S4.3**.

U drugom dijelu ovog poglavlja prvo definiramo pojam stabla koji će biti važan u ostatku poglavlja. Zatim dokazujemo da logika **K** nema polinomno svojstvo konačnih modela. Iz tog rezultata možemo naslutiti da logika **K** nije NP–potpuna modalna logika. U nastavku definiramo pojam Hintikkinog skupa i pojam skupova svjedoka. Zatim dokazujemo tvrdnje koje nam daju sintaktički kriterij za provjeru ispunjivosti formule. Prvo navodimo algoritam *Svjedok*, a onda opisujemo rad Turingovog stroja koji provjerava **K**–ispunjivost koristeći taj algoritam. Time dokazujemo da je logika **K** PSPACE–složena modalna logika. Zatim definiramo pojam **QBF**-formule te definiramo problem određivanja istinitosti **QBF**-formula, u oznaci TQBF, za koji se zna da je PSPACE–potpun. Svođenjem problema TQBF na problem ispunjivosti proizvoljne normalne modalne logike Λ takve da je $\mathbf{K} \subseteq \Lambda \subseteq \mathbf{S4}$ dokazujemo Ladnerov teorem koji govori da je svaka logika između **K** i **S4** PSPACE–teška. Na kraju poglavlja ukratko opisujemo složenost logika `LTL` i `PDL`. Također dajemo primjer neodlučive modalne logike `Tile`.

Summary

The main goal of this thesis is to present some results about the complexity of modal logics. The thesis consists of two chapters. In the first chapter, we describe the syntax and semantics of the basic modal language. We define alphabet, formulas, Kripke frames and models, satisfiability, and validity. We then define smallest normal modal logic **K** and its extensions - **K4**, **T**, **S4**, **S5** and **S4.3**. In this chapter we also present basic notions and results of the model theory of modal logic. We define the following notions: generated submodel, isomorphism and bounded morphism. We prove that each of the defined constructions preserves satisfiability. We also define a finite model and finite frame property. At the end of the first chapter, we describe characteristic frame classes of some modal logics.

The second chapter is about the complexity of normal modal logics defined in the first chapter. First, we define polysize model property and frame definability by a first-order sentence. These are key notions for proving NP-completeness of **S5** and for proving Hemaspaandra's theorem about the NP–completeness of normal modal logics extending **S4.3**. The second part of the second chapter starts with the definition of trees as they are very useful in the rest of the chapter. Then we show that **K** lacks polysize model property. From this result we can assume that **K** is not **NP**–complete. Furthermore, we define Hintikka sets and witness sets and give a syntactic criterion for the satisfiability of a formula. We also present an algorithm called *Witness* and describe a Turing machine that decides **K**-satisfiability using *Witness*. This show that **K** has PSPACE complexity. Moreover, we define **QBF**-formulas and **QBF**-validity problem, or TQBF problem, which is a known PSPACE-complete problem. By reducing the TQBF problem to the Λ-satisfiability problem, for normal modal logic Λ such that $\mathbf{K} \subseteq \Lambda \subseteq \mathbf{S4}$, we prove that every normal modal logic between **K** and **S4** is PSPACE-hard. At the end of this chapter, we mention the complexity of logics LTL and PDL. We also give an example of an undecidable modal logic called Tile.

Životopis

Rođena sam 25. travnja 1998. u Čakovcu. Odrasla sam u Nedelišću gdje sam pohađala osnovnu školu. Gimnaziju Josipa Slavenskog u Čakovecu upisala sma 2013. godine. Tijekom osnovnošolskog i srednjoškolskog obrazovanja sudjelovala sam na natjecanjima iz matematike, geografije i hrvatskog jezika.

Nakon završetka srednje škole 2017. godine upisujem preddiplomski studij *Matematika* na Prirodoslovno-matematičkom fakultetu u Zagrebu. Po završetku preddiplomskog studija 2020. godine upisujem diplomski studij *Računarstvo i matematika* na istome fakultetu.

Tijekom cijelog studija bila sam član Veslačke sekcije PMF-a s kojom sam na desetak natjecanja osvojila jedno od prva tri mjesta.