

Metode interpretacije, kvazimodela i mozaika za dokazivanje odlučivosti modalnih logika

Sokolaj, Iva

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:217:536360>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-08-16**



Repository / Repozitorij:

[Repository of the Faculty of Science - University of Zagreb](#)



SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Iva Sokolaj

**METODE INTERPRETACIJE,
KVAZIMODELA I MOZAIKA ZA
DOKAZIVANJE ODLUČIVOSTI
MODALNIH LOGIKA**

Diplomski rad

Voditelji rada:
prof. dr. sc. Mladen Vuković
izv. prof. dr. sc. Tin Perkov

Zagreb, studeni, 2023.

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. _____

Sadržaj

Sadržaj	iii
Uvod	1
1 Osnovne definicije i činjenice	2
1.1 Sintaksa modalne logike	2
1.2 Semantika modalne logike	3
1.3 Normalne modalne logike	10
2 Metoda konačnih modela	12
2.1 Svojstvo konačnih modela i svojstvo konačnih okvira	12
2.2 Aksiomatizabilnost	15
2.3 Logika KvB nema svojstvo konačnih modela	16
3 Metode interpretacije i kvazimodela	19
3.1 Teorije SnS	19
3.2 Rabinov teorem	21
3.3 Dokaz odlučivosti logike KvB metodom kvazimodela	35
4 Metoda mozaika	41
4.1 Osnovni temporalni jezik	41
4.2 Odlučivost logike K_tN	43
Bibliografija	50

Uvod

Logika je jedna od najstarijih disciplina u znanosti s počecima razvoja iz drevnih vremena. Prvi su logičari htjeli uspostaviti pravila koja bi omogućila razlikovanje valjanih i nevaljanih argumenata. Logika se nastavljala razvijati te je u 20. stoljeću imala veliki utjecaj na razvoj računalne znanosti.

Modalna logika nastala je u 20. stoljeću iz potrebe za formalizacijom izraza poput nužnosti i mogućnosti koje ne možemo prikazati klasičnom logikom sudova. U današnje vrijeme modalne logike čine familiju logika sa sličnim pravilima i nizom različitih simbola. Jedna od njih je temporalna logika koja formalizira izraze o prošlosti i budućnosti, kao što su "uvijek će biti" i "uvijek je bilo". Modalni su jezici jednostavni, ali dovoljno izražajni za opis relacijskih struktura te imaju veliki značaj u računalnoj znanosti. U ovom radu bavimo se metodama za dokazivanje odlučivosti modalnih logika.

Pitanje odlučivosti problema ekvivalentno je pitanju mogućnosti stvaranja računalnog programa koji za svaku instancu tog problema uvijek ispiše rješenje. Kao takvo, posebno je bitno u današnjem dobu konstantnog razvoja računala.

Prvo poglavlje pruža uvod u normalne modalne logike. Definiramo sintaksu i semantiku osnovnog modalnog jezika te neke sisteme modalne logike.

Zatim, u drugom poglavlju definiramo svojstvo konačnih modela te pokazujemo korisnost tog svojstva za dokazivanje odlučivosti modalnih logika. Metoda dokazivanja odlučivosti koja koristi svojstvo konačnih modela naziva se metoda konačnih modela. Navest ćemo i neka ograničenja te metode. Točnije, dokazat ćemo da ne posjeduju svi odlučivi sistemi modalne logike svojstvo konačnih modela. Navedeno ograničenje prirodno povlači da trebamo razmotriti i neke druge metode.

U trećem poglavlju dajemo dvije alternative metodi konačnih modela. To su metoda interpretacije i metoda kvazimodela. Dokazujemo odlučivost logike KvB na dva načina upravo koristeći te dvije metode.

U zadnjem, četvrtom poglavlju prvo definiramo sintaksu i semantiku osnovnog temporalnog jezika. Zatim, definiramo temporalnu logiku K_tN i metodom mozaika dokazujemo odlučivost te logike.

Poglavlje 1

Osnovne definicije i činjenice

U ovom poglavlju definiramo osnovne pojmove vezane uz modalnu logiku. Poglavlje se sastoji od tri potpoglavlja. U prvom potpoglavlju definiramo sintaksu modalne logike, u drugom semantiku, a u trećem definiramo normalne modalne logike. Uz pojedine definicije dat ćemo i primjere definiranih pojmova tamo gdje je to potrebno radi boljeg razumijevanja.

1.1 Sintaksa modalne logike

Potpoglavlje započinjemo definiranjem alfabeta osnovnog modalnog jezika. Zatim definiramo formulu osnovnog modalnog jezika i stupanj formule.

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

- skup prebrojivo mnogo propozicionalnih varijabli $Prop = \{p, q, r, \dots\}$;
- skup logičkih veznika, modalnih operatora i logičkih konstanti $\{\neg, \vee, \square, \perp\}$;
- skup pomoćnih simbola $\{(,)\}$ (zagrada).

U nastavku koristimo i logičke veznike \wedge, \rightarrow i \leftrightarrow . Oni nisu navedeni u definiciji budući da se mogu iskazati pomoću navedenih logičkih veznika. Primjerice, znamo iz logike sudova da je formula $A \wedge B$ logički ekvivalentna formuli $\neg(\neg A \vee \neg B)$. Također, koristimo unarni modalni operator \diamond kao pokratu za $\neg\square\neg$ i logičku konstantu \top kao pokratu za $\neg\perp$. Operatore \square i \diamond čitamo redom "nužno" i "moguće", a nazivamo ih operator nužnosti i operator mogućnosti.

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

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

Pojam formule osnovnog modalnog jezika definiramo rekurzivno:

1. svaka atomarna formula je formula
2. ako su φ i ψ formule, tada su i riječi $\neg\varphi$, $\varphi \vee \psi$ i $\Box\varphi$ također formule.

Riječ alfabeta logike sudova je formula ako je nastala primjenom konačno mnogo koraka 1 i 2. Formule obično označavamo simbolima φ, ψ, χ .

Primjer 1.1.3. *Primjeri modalnih formula su riječi $\Box\Box\Box(p \vee \neg\Box q)$, \top i $\neg\neg\perp \wedge p$, dok riječi $p\neg$, pq i $\Diamond p \wedge \vee\perp$ nisu formule.*

Složenost modalne formule, analogno logici sudova, definira se kao broj veznika i modalnih operatora u formuli. Za razliku od logike sudova, u modalnoj logici definiramo i stupanj modalne formule. Intuitivno, stupanj formule je maksimalni broj ugniježđenih modalnih operatora.

Definicija 1.1.4. *Stupanj modalne formule φ , u oznaci $\text{deg}(\varphi)$, definiramo rekurzivno na sljedeći način:*

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

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

Primjer 1.1.5. 1. *Stupanj formule $\neg\Box(\Box\Box\top \vee (\Box\neg\Box\Box p \wedge \Box q))$ je 4.*

2. *Stupanj skupa formula $\{\Box\perp, \Diamond\Box\Diamond p, \neg p \vee q, \Box(\neg\Box p \vee \Diamond q \wedge \Box r)\}$ je 3.*

1.2 Semantika modalne logike

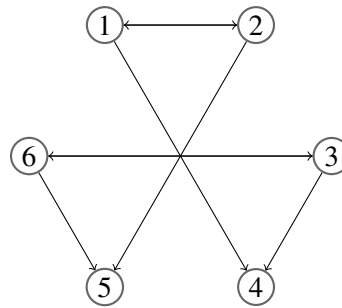
Prvo ćemo definirati pojmove relacijskih struktura koje se nazivaju Kripkeov okvir i Kripkeov model. Zatim ćemo definirati pojam istinitosti i valjanosti formule na Kripkeovom okviru, odnosno Kripkeovom modelu čime ćemo povezati modalni jezik s navedenim relacijskim strukturama. Na kraju definiramo pojam filtracije modela u odnosu na skup formula te iznosimo teorem o filtracijama.

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

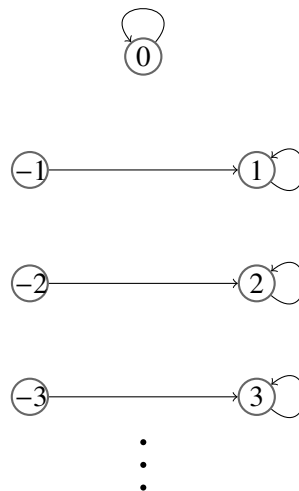
Umjesto $(w, v) \in R$ pisat ćemo wRv te kažemo da je svijet v sljedbenik svijeta w .

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

1. Neka je $\mathfrak{F} = (W, R)$ Kripkeov okvir gdje je nosač $W = \{1, 2, 3, 4, 5, 6\}$, a relacija $R = \{(1, 4), (1, 2), (2, 1), (2, 5), (3, 4), (3, 6), (6, 3), (6, 5)\}$. Na sljedećoj slici ilustriramo upravo definirani okvir.



2. Neka je $\mathfrak{F} = (W, R)$ gdje je nosač $W = \mathbb{Z}$ i relacija R je definirana ovako: xRy ako i samo ako je $|x| = y$. Slijedi ilustracija navedenog okvira.



U nastavku definiramo strukturu koja se naziva Kripkeov model. Nakon toga ćemo moći definirati istinitost formule na nekom svijetu i na Kripkeovom modelu. Već sada možemo pretpostaviti da će formule poput \top i $p \rightarrow p$ biti istinite na svim svjetovima i okvirima kao što su uvijek istinite u logici sudova bez obzira na interpretaciju. Kao što u logici sudova istinitost formule ovisi o funkciji interpretacije, ovdje će nam od važnosti biti funkcija zvana valuacija. No, za razliku od logike sudova, u modalnoj logici ne možemo definirati istinitost formule isključivo putem funkcije već nam je bitan i Kripkeov okvir.

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 $V: Prop \rightarrow \mathcal{P}(W)$ funkcija koju nazivamo *valuacija*. Kažemo da je model \mathfrak{M} baziran na okviru \mathfrak{F} .

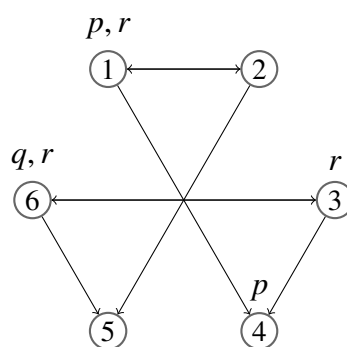
U nastavku umjesto Kripkeov okvir i Kripkeov model pišemo samo kratko okvir, odnosno model. Zatim, umjesto $\mathfrak{M} = ((W, R), V)$ pišemo $\mathfrak{M} = (W, R, V)$.

Primjer 1.2.4. *Za primjere okvira iz 1.2.2, navodimo primjere modela baziranih na njima.*

1. *Neka je $\mathfrak{M} = (W, R, V)$ model baziran na prvom okviru iz prošlog primjera, a definicija valuacije V je sljedeća:*

- $V(p) = \{1, 4\}$
- $V(q) = \{6\}$
- $V(r) = \{1, 6, 3\}$,
- $V(s) = \emptyset$ za preostale $s \in Prop$

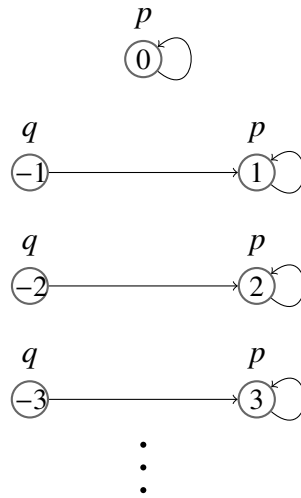
Tada model \mathfrak{M} ilustriramo na sljedeći način:



2. Neka je $\mathfrak{F} = (W, R)$ okvir kao u prošlom primjeru, a $\mathfrak{M} = (\mathfrak{F}, V)$ model, gdje je valuacija V definirana ovako:

- $V(p) = \{n \mid n \in \mathbb{N}\}$
- $V(q) = \{n \mid n \in \mathbb{Z}^-\}$
- $V(r) = \emptyset$, za preostale $r \in Prop$

Na sljedećoj slici ilustriramo upravo definirani model.



Vidimo da valuacija preslikava propozicionalnu varijablu u skup svih svjetova na kojima je ta varijabla istinita. Iz toga se na očekivan način definicija istinitosti na svijetu proširuje na proizvoljne formule. Slijedi formalna definicija istinitosti formule na svijetu.

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 $p \in Prop$
- $\mathfrak{M}, w \not\Vdash \perp$
- $\mathfrak{M}, w \Vdash \neg \varphi$ 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 $\mathfrak{M}, w \Vdash \psi$
- $\mathfrak{M}, w \Vdash \Box \varphi$ ako i samo ako za svaki svijet $v \in W$ takav da vrijedi wRv vrijedi i $\mathfrak{M}, v \Vdash \varphi$

Kažemo da je formula φ **istinita na modelu** \mathfrak{M} ako je istinita na svakom svijetu modela \mathfrak{M} .
Oznaka: $\mathfrak{M} \models \varphi$.

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} . Oznaka: $\mathfrak{M} \not\models \varphi$.

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

Iako smo modalni operator \diamond definirali kao pokratu operatora \Box , radi boljeg razumijevanja i razvijanja snažnije intuicije slijedi formalna definicija.

Napomena 1.2.7. Iz ekvivalencija operatora \diamond i izraza $\neg\Box\neg$, lako se pokaže da vrijedi sljedeća tvrdnja:

$\mathfrak{M}, w \Vdash \diamond\varphi$ ako i samo ako postoji svijet $v \in W$ takav da wRv i vrijedi $\mathfrak{M}, v \Vdash \varphi$.

Sada nam je jasnije zašto operatore \Box i \diamond čitamo redom "nužno" i "moguće". Uzmimo model $\mathfrak{M} = (W, R, V)$, svijet $w \in W$ i njegovog proizvoljnog sljedbenika v . Ako vrijedi $\mathfrak{M}, w \Vdash \Box\varphi$, tada za sljedbenika v od w *nužno* vrijedi $\mathfrak{M}, v \Vdash \varphi$, a ako vrijedi $\mathfrak{M}, w \Vdash \diamond\varphi$ tada je *moguće* da vrijedi $\mathfrak{M}, v \Vdash \varphi$.

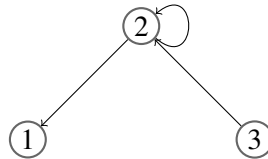
Definicija 1.2.8. Kažemo da je formula φ **valjana na svijetu** w u okviru \mathfrak{F} ako za svaku valuaciju V vrijedi $(\mathfrak{F}, V), w \Vdash \varphi$. Oznaka: $\mathfrak{F}, w \Vdash \varphi$.

Kažemo da je formula φ **valjana na okviru** \mathfrak{F} ako je valjana na svakom svijetu okvira \mathfrak{F} .
Oznaka: $\mathfrak{F} \Vdash \varphi$

Kažemo da je formula φ **valjana** ako je valjana na svakom okviru.

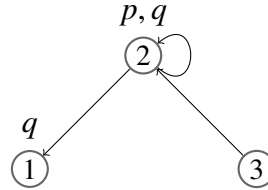
Kažemo da je formula φ **valjana na klasi okvira** F ako je valjana na svakom okviru iz F .
Oznaka: $F \Vdash \varphi$.

Primjer 1.2.9. Prvo ćemo dati primjer okvira te pokazati koje formule jesu i nisu valjane na okviru. Zatim dajemo primjer modela baziranog na definiranom okviru te pokazujemo primjere formula koje jesu i nisu istinite na modelu, odnosno na svjetovima. Neka je $\mathfrak{F} = (W, R)$ okvir gdje je $W = \{1, 2, 3\}$ i relacija dostiživosti je zadana sa $R = \{(2, 1), (3, 2), (2, 2)\}$.



Osim tautologija, primijetimo da vrijedi i $\mathfrak{F} \models \diamond p \rightarrow \diamond\diamond p$ jer je ta formula valjana na svakom svijetu bez obzira na valuaciju.

Međutim, formula $\Box p \rightarrow \Box\Box p$ nije valjana na okviru \mathfrak{F} jer za valuaciju V takvu da $V(p) = \{2\}$ vrijedi $(\mathfrak{F}, V), 3 \not\models \Box p \rightarrow \Box\Box p$. Proširimo definiciju valuacije V sa $V(q) = \{1, 2\}$ te ilustrirajmo model $\mathfrak{M} = (\mathfrak{F}, V)$.



Primijetimo da vrijede sljedeće tvrdnje o istinitosti formula:

- $\mathfrak{M} \models \Box q \rightarrow \Box\Box q$
- $\mathfrak{M} \not\models \diamond q$
- $\mathfrak{M}, 1 \models \neg\diamond p \wedge \Box p$
- $\mathfrak{M}, 2 \models p \wedge q \wedge \diamond p \wedge \neg(\Box p)$
- $\mathfrak{M}, 3 \models \Box\diamond\Box q$

Napomena 1.2.10. Definicije ispunjivosti i valjanosti možemo proširiti i na skupove formula.

Skup formula Γ istinit je na nekom svijetu w modela \mathfrak{M} ako je svaka formula iz Γ istinita na w . Oznaka: $\mathfrak{M}, w \models \Gamma$.

Skup formula Γ ispunjiv je na modelu \mathfrak{M} ako je istinit na nekom svijetu modela \mathfrak{M} .

Skup formula Γ valjan je na nekom okviru \mathfrak{F} ako je svaka formula iz Γ valjana na \mathfrak{F} . Oznaka: $\mathfrak{F} \models \Gamma$.

Skup formula Γ valjan je na klasi okvira F ako je svaka formula iz Γ valjana na F . Oznaka: $F \models \Gamma$.

Primjer 1.2.11. Primijetimo da smo u prethodnom primjeru umjesto $\mathfrak{M}, 2 \models p \wedge q \wedge \diamond p \wedge \neg(\Box p)$ mogli napisati $\mathfrak{M}, 2 \models \{p, q, \diamond p, \neg(\Box p)\}$.

Definicija 1.2.12. Kažemo da je skup formula Γ **zatvoren na potformule** ako za sve formule φ, ψ vrijedi:

- ako $\neg\varphi \in \Gamma$, onda $\varphi \in \Gamma$,
- ako $\varphi \vee \psi$, onda $\varphi, \psi \in \Gamma$,
- ako $\Box\varphi \in \Gamma$, onda $\varphi \in \Gamma$.

Navodimo dva primjera skupa formula, jedan koji je zatvoren na potformule i jedan koji nije zatvoren na potformule.

Primjer 1.2.13. Skup formula $\{\neg\Box(p \wedge \Diamond q), \neg\neg\Diamond q, \Box(p \wedge \Diamond q), p \wedge \Diamond q, p, \Diamond q, q, \neg\Diamond q\}$ je zatvoren na potformule. Skup formula $\{\neg\top, \neg\perp, \perp, p\}$ nije zatvoren na potformule. Nedostaje formula \top da bude zatvoren na potformule, iako je formula $\neg\perp$ koja je ekvivalentna formuli \top element skupa formula.

Definicija 1.2.14. Neka je $\mathfrak{M} = (W, R, V)$ model i neka je Γ skup formula zatvoren na potformule.

Definiramo binarnu relaciju \sim_Γ na svim svjetovima $w, v \in W$ na sljedeći način:

$$w \sim_\Gamma v \iff \text{za svaku formulu } \varphi \in \Gamma \text{ vrijedi } \mathfrak{M}, w \Vdash \varphi \text{ ako i samo ako } \mathfrak{M}, v \Vdash \varphi.$$

Lako se pokaže da je relacija \sim_Γ relacija ekvivalencije. Klasu ekvivalencije svijeta $w \in W$ označavamo sa $[w]_\Gamma$.

Neka je $W_\Gamma = \{[w]_\Gamma \mid w \in W\}$, a preslikavanje $V_\Gamma : Prop \rightarrow \mathcal{P}(W_\Gamma)$ takvo da za svaku propozicionalnu varijablu $p \in \Gamma$ vrijedi:

$$V_\Gamma(p) = \{[w]_\Gamma \mid w \in V(p)\}.$$

Kažemo da je neki model $\tilde{\mathfrak{M}} = (W_\Gamma, \tilde{R}, V_\Gamma)$ **filtracija modela \mathfrak{M} u odnosu na skup Γ** ako za relaciju \tilde{R} i sve svjetove $w, v \in W$ vrijede sljedeća svojstva:

(MIN): ako je wRv , onda je $[w]_\Gamma \tilde{R} [v]_\Gamma$,

(MAX): ako je $[w]_\Gamma \tilde{R} [v]_\Gamma$, onda za svaku formulu $\Diamond\varphi \in \Gamma$ koja zadovoljava $\mathfrak{M}, v \Vdash \varphi$ vrijedi $\mathfrak{M}, w \Vdash \Diamond\varphi$.

Iskazujemo teorem o filtracijama. Dokaz se može pronaći u [1] kao Filtration Theorem.

Teorem 1.2.15. Neka je Γ skup formula zatvoren na potformule te neka je model $\tilde{\mathfrak{M}} = (W_\Gamma, \tilde{R}, V_\Gamma)$ filtracija modela $\mathfrak{M} = (W, R, V)$ u odnosu na skup Γ . Za svaku formulu $\varphi \in \Gamma$ i svaki svijet $w \in W$ vrijedi:

$$\mathfrak{M}, w \Vdash \varphi \text{ ako i samo ako } \tilde{\mathfrak{M}}, [w]_\Gamma \Vdash \varphi.$$

1.3 Normalne modalne logike

Sada imamo sve potrebne definicije koje nam omogućuju definiciju sistema modalne logike. Prvo definiramo pojam normalne modalne logike, zatim definiramo najmanju normalnu modalnu logiku te dodavanjem aksioma definiramo i neke druge sisteme.

Definiramo i modalnu logiku **KvB** koja se bitno razlikuje od ostalih definiranih, ne samo u načinu definicije, već i u jednom zanimljivom svojstvu koji ćemo obraditi u sljedećem poglavlju.

Definicija 1.3.1. *Normalna modalna logika Λ je svaki skup formula koji sadrži sve tautologije, sve formule oblika $\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi)$ 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**.

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

$$(4) \equiv \Box p \rightarrow \Box\Box p$$

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

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

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

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

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

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

Definicija logike **KvB** nešto je složenija te zahtjeva da prethodno definiramo još nekoliko pojmova.

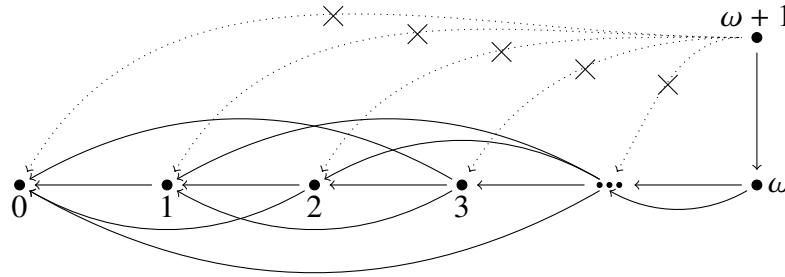
Definicija 1.3.3. *Neka je Λ normalna modalna logika i $\mathfrak{F} = (W, R)$ proizvoljan okvir. Okvir \mathfrak{F} nazivamo Λ -okvir ako vrijedi $\mathfrak{F} \models \Lambda$. Model baziran na Λ -okviru nazivamo Λ -model. Ako je formula φ ispunjiva na nekom Λ -modelu, kažemo da je formula φ jedna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

Definicija 1.3.4. Neka je $\mathfrak{F} = (W, R)$ okvir s nosačem W i relacijom dostiživosti R . Kažemo da je (\mathfrak{F}, A) **opći okvir** ako je A neprazna familija podskupova od W zatvorena na:

1. konačne unije: ako je $X, Y \in A$, onda $X \cup Y \in A$
2. komplemente: ako je $X \in A$, onda je $W \setminus X \in A$
3. prasluku po relaciji R : ako je $X \in A$, onda je $\{w \in W \mid wRv, \text{ za neki } v \in X\} \in A$.

Skupove koji su elementi od A nazivamo **dopustivima**. **Model nad općim okvirom** (\mathfrak{F}, A) je trojka (\mathfrak{F}, A, V) gdje je V valuacija sa svojstvom da za svaku proposicionalnu varijablu p vrijedi $V(p) \in A$. Valuacije s ovim svojstvom isto tako zovu se **dopustive** za opći okvir (\mathfrak{F}, A) .

Napomena 1.3.5. Valjanost formule na općim okvirima i na modelima nad općim okvirima definiramo analogno definiciji valjanosti na Kripkeovim okvirima i modelima.



Slika 1.1: Opći okvir \mathfrak{F} nad kojim je definirana logika KvB

Definicija 1.3.6. Neka je $\mathfrak{F} = (J, R, A)$ opći okvir takav da redom imamo:

- $J = \mathbb{N} \cup \{\omega, \omega + 1\}$,
- $xRy : \Leftrightarrow y < x \neq \omega + 1$ ili $x = \omega + 1$ i $y = \omega$,
- $A = \{X \subseteq J \mid X \text{ konačan i } \omega \notin X \text{ ili } X \text{ kofinitan i } \omega \in X\}$ je familija svih dopustivih skupova.

Logiku koja se sastoji od svih formula valjanih na općem okviru \mathfrak{F} označavamo **KvB**.

U sljedećem poglavlju navest ćemo neke primjere modalnih formula koje su valjane na upravo definiranom općem okviru.

Poglavlje 2

Metoda konačnih modela

U ovom poglavlju razmatramo metodu konačnih modela za dokazivanje odlučivosti modalnih logika. Definirat ćemo svojstvo konačnih modela i pojam aksiomatizabilnosti, a zatim ćemo navesti teoreme koji iskazuju korisnost uvedenih pojmova za dokazivanje odlučivosti modalnih logika.

Želimo istaknuti da u ovom poglavlju nećemo dokazivati niti jednu tvrdnju. Ovo poglavlje trebalo bi poslužiti kao motivacija za sljedeće poglavlje. Naime, u zadnjem potpoglavlju ovog poglavlja navest ćemo neka ograničenja metode konačnih modela za dokazivanje odlučivosti modalnih logika. To prirodno povlači da razmotrimo i neke druge metode.

2.1 Svojstvo konačnih modela i svojstvo konačnih okvira

Ovo potpoglavlje započet ćemo definicijama svojstva konačnih modela i svojstva konačnih okvira. Zatim ćemo definirati nekoliko pojmova vezanih uz izračunljivost. Definirane pojmove ćemo koristiti u definiciji jakog svojstva konačnih modela. Potpoglavlje završavamo teoremom koji povezuje jako svojstvo konačnih modela s odlučivosti modalne logike.

Definicija 2.1.1. *Za logiku Λ kažemo da ima svojstvo konačnih modela (eng. finite model property; kratko: fmp) ako postoji klasa modela \mathbf{M} takva da $\mathbf{M} \models \Lambda$ i da za svaku ispunjivu formulu postoji konačan model $\mathfrak{M} \in \mathbf{M}$ na kojem je istinita.*

Primjer 2.1.2. *Sve logike koje smo definirali aksiomima imaju svojstvo konačnih modela. Dokaz da logika \mathbf{K} ima svojstvo konačnih modela može se pronaći u 5. poglavlju knjige [8], dokaz za logiku $\mathbf{K4}$ može se pronaći u [3] kao teorem 3.22, za logike \mathbf{T} i $\mathbf{S4}$ u [6] redom kao leme 2.6.4 i 2.6.5, a za logiku $\mathbf{S4.3}$ u [1] kao Bullov teorem.*

Definicija 2.1.3. Za logiku Λ kažemo da ima svojstvo **konačnih okvira** (eng. *finite frame property*) ako postoji klasa konačnih okvira \mathbf{F} takva da vrijedi $\mathbf{F} \models \Lambda$ i da je svaka formula $\varphi \notin \Lambda$ oboriva na nekom okviru $\mathfrak{F} \in \mathbf{F}$.

Teorem 2.1.4. Modalna logika Λ ima svojstvo konačnih modela ako i samo ako ima svojstvo konačnih okvira.

Dokaz prethodnog teorema može se pronaći u [1] kao teorem 3.28.

Sada slijedi nekoliko definicija pojmova koji će nam biti od važnosti za definiranje jakog svojstva konačnih modela. Više o navedenim pojmovima možete pročitati u [9].

Turingov stroj matematički je model koji opisuje rad apstraktnog stroja. Stroj se sastoji od beskonačne trake na kojoj u svakom polju može biti zapisan neki simbol i od glave stroja koja čita i manipulira simbole na traci. Slijedi formalna definicija.

Definicija 2.1.5. *Turingov stroj je uređena sedmorka $(Q, \Sigma, \sqcup, \Gamma, \delta, q_0, F)$ gdje:*

- Q je konačan skup stanja
- Σ je konačan skup koji nazivamo **ulazna abeceda**
- $\Gamma \supset \Sigma$ je **radna abeceda** s istaknutim znakom $\sqcup \in \Gamma \setminus \Sigma$ koji, kada je napisan na traci, označava **prazno mjesto**
- $\delta : (Q \setminus F) \times \Gamma \rightarrow Q \times \Gamma \times \{L, S, D\}$ je **funkcija prijelaza**
- $q_0 \in Q$ je **početno stanje**
- $F \subseteq Q$ je skup **završnih stanja**.

Turingov odlučitelj je Turingov stroj s dva završna stanja: **stanje prihvatanja** (oznaka: q_{\checkmark}) i **stanje odbijanja** (oznaka: q_{\times}), te sa svojstvom da svako izvršavanje s ulaznim podatkom iz skupa Σ^* stane u jednom od navedenih završnih stanja. Zato za probleme za koje postoji Turingov odlučitelj kažemo da su odlučivi.

Definicija 2.1.6. Neka je Σ abeceda. Za funkciju $f : \Sigma^* \rightarrow \Sigma^*$ kažemo da je **Turing-izračunljiva** (ili **kraće izračunljiva**) ako postoji Turingov stroj koji je računa. To znači da za svaki ulazni podatak $w \in \Sigma^*$ Turingov stroj na traku ispiše $f(w)$.

Neka je Λ normalna modalna logika. Pojmovi Λ -dokaza i Λ -dokazive formule definiraju se standardno kao i u logici sudova. Pišemo $\vdash_{\Lambda} \varphi$ ako je formula φ jedna Λ -dokaziva formula. Budući da definicija Λ -izvedive formule iz danog skupa formula nije sasvim ista kao definicija tog pojma u klasičnim logikama (primjerice, logici sudova i logici prvog

reda), ovdje je navodimo. Pojam Λ -izvedivosti treba nam kako bismo mogli definirati pojam Λ -konzistentnog skupa.

Definicija 2.1.7. *Neka je Γ skup formula, a φ proizvoljna formula. Neka je Λ normalna modalna logika. Kažemo da je formula φ izvediva iz skupa Γ u logici Λ ili Λ -izvediva iz skupa Γ ako vrijedi jedno od sljedećeg:*

1. $\vdash_{\Lambda} \varphi$
2. postoje formule $\psi_1, \dots, \psi_n \in \Gamma$ takve da vrijedi $\vdash_{\Lambda} (\psi_1 \wedge \dots \wedge \psi_n) \rightarrow \varphi$.

U tom slučaju pišemo $\Gamma \vdash_{\Lambda} \varphi$. U suprotnom pišemo $\Gamma \not\vdash_{\Lambda} \varphi$.

Za skup formula Γ kažemo da je Λ -konzistentan ako vrijedi $\Gamma \not\vdash_{\Lambda} \perp$. Inače kažemo da je Λ -nekonzistentan.

Formula φ je Λ -konzistentna ako za skup $\{\varphi\}$ vrijedi da je Λ -konzistentan.

Definicija 2.1.8. *Neka je Λ normalna modalna logika, $f : \mathbb{N} \rightarrow \mathbb{N}$ neka funkcija i \mathbf{M} skup modela takav da svaki model sadrži konačno mnogo svjetova i nepraznu relaciju dostiživosti te vrijedi $\Lambda = \Lambda_{\mathbf{M}}$, gdje $\Lambda_{\mathbf{M}}$ označava skup svih formula koje su valjane na svim modelima iz \mathbf{M} .*

Kažemo da logika Λ ima svojstvo konačnih modela reda $f(n)$ u odnosu na skup \mathbf{M} ako je svaka Λ -konzistentna formula φ ispunjiva na nekom modelu iz \mathbf{M} koji sadrži najviše $f(|\varphi|)$ svjetova, gdje $|\varphi|$ označava duljinu reprezentacije formule φ na Turingovom stroju.

Ako je funkcija f izračunljiva, tada kažemo da logika Λ ima jako svojstvo konačnih modela u odnosu na skup \mathbf{M} .

Primijetimo da iz prethodne definicije slijedi da svaka modalna logika koja ima jako svojstvo konačnih modela ima i "obično" svojstvo konačnih modela. Naime, $\Lambda = \Lambda_{\mathbf{M}}$ povlači $\mathbf{M} \models \Lambda$.

Primjer 2.1.9. *Multiplikativni aditivni fragment intuicionističke linearne logike primjer je logike koja ima svojstvo konačnih modela, no nema jako svojstvo konačnih modela. (Vidi: [2].)*

Definicija 2.1.10. *Turingov enumerator je jedna verzija Turingovog stroja koji je "spojen na printer" te koji nema završna stanja. No, ima jedno istaknuto izlazno stanje q_{\leftarrow} koje služi za „ispis“ sadržaja trake kad god se stroj nađe u tom stanju. Kako stroj nema završno stanje, ispis traje beskonačno, a prelazak na ispis iduće trake može se shvatiti kao prelazak u novi red u beskonačno dugoj listi.*

Definicija 2.1.11. *Za skup kažemo da je rekurzivan ako postoji Turingov odlučitelj koji za dani ulazni podatak stane u stanju prihvaćanja ako je taj ulazni podatak element skupa, a u suprotnom stane u stanju odbijanja.*

Za neki skup kažemo da je **rekurzivno prebrojiv** ako postoji Turingov enumerator koji na traku ispisuje sve i samo elemente tog skupa.

Dokaz sljedećeg teorema dan je u [1] (kao teorem 6.7).

Teorem 2.1.12. *Neka je Λ normalna modalna logika i M rekurzivan skup modela. Ako logika Λ ima jako svojstvo konačnih modela u odnosu na skup M , tada je logika Λ odlučiva.*

Prije nego što iskažemo još neke teoreme koji povezuju svojstvo konačnih modela i odlučivost modalne logike, trebamo definirati pojam aksiomatizabilnosti. To ćemo napraviti u sljedećem potpoglavlju.

2.2 Aksiomatizabilnost

Slijede definicije konačno aksiomatizabilne logike i aksiomatizabilne logike. Nakon definicija navodimo teoreme koji povezuju (konačnu) aksiomatizabilnost i svojstvo konačnih modela s odlučivosti modalne logike.

U čitavom ovom potpoglavlju neka je sa Λ označena proizvoljna normalna modalna logika.

Definicija 2.2.1. *Za skup formula Γ kažemo da je **skup aksioma** za logiku Λ ako je Λ najmanja logika koja sadrži Γ .*

Definicija 2.2.2. *Kažemo da je logika Λ **konačno aksiomatizabilna** ako postoji konačan skup aksioma za logiku Λ .*

*Kažemo da je logika Λ **aksiomatizabilna** ako postoji skup aksioma za Λ koji je rekurzivno prebrojiv skup.*

Pogledajmo još rezultata koji nam dokazuju korisnost svojstva konačnih modela za dokazivanje odlučivosti modalnih logika. Sljedeća dva teorema su iskazana i dokazana u [1] kao teoremi 6.15 i 6.13.

Teorem 2.2.3. *Ako je Λ konačno aksiomatizabilna logika sa svojstvom konačnih modela, onda je odlučiva.*

Teorem 2.2.4. *Ako je Λ aksiomatizabilna logika koja ima svojstvo konačnih modela u odnosu na rekurzivno prebrojiv skup modela \mathbf{M} , onda je logika Λ jedna odlučiva logika.*

2.3 Logika KvB nema svojstvo konačnih modela

U prethodnom potpoglavlju vidjeli smo da je svojstvo konačnih modela korisno za dokazivanje odlučivosti modalnih logika. No, postavlja se pitanje što je s logikama koje nemaju svojstvo konačnih modela, ali su odlučive. Jedna takva je logika KvB . U nastavku slijedi dokaz da logika KvB nema svojstvo konačnih modela, a u sljedećem poglavlju ćemo nekim drugim metodama dokazati da je logika KvB odlučiva.

U propozicijama koje slijede koristimo opći okvir \mathfrak{J} koji je definiran u definiciji 1.3.6 u prethodnom poglavlju.

Propozicija 2.3.1. *Formula $\Box\Diamond\top \rightarrow \Box(\Box(\Box p \rightarrow p) \rightarrow p)$ je valjana na općem okviru \mathfrak{J} .*

Dokaz. Pretpostavimo suprotno. Tada postoji dopustiva valuacija V i svijet $w \in J$ takvi da $w \Vdash \Box\Diamond\top$, ali $w \not\Vdash \Box(\Box(\Box p \rightarrow p) \rightarrow p)$. Iz potonjeg slijedi da postoji svijet $v \in J$ takav da je wRv i $v \not\Vdash \Box(\Box p \rightarrow p) \rightarrow p$, odnosno $v \Vdash \Box(\Box p \rightarrow p)$ i $v \not\Vdash p$. Promotrimo sada mogućnosti za svjetove w i v .

Primijetimo prvo da svijet v ne može biti $\omega + 1$ budući da po definiciji relacije R ne postoji svijet w takav da vrijedi $wR(\omega + 1)$.

Pretpostavimo sada da je $w = \omega + 1$. Tada je $v = \omega$ te iz $v \not\Vdash p$ i dopustivosti valuacije slijedi da je $V(p)$ konačan (jer ne sadrži svijet ω). Stoga je skup $\omega \setminus V(p)$ neprazan te kao podskup od ω koji je dobro uređen, ima najmanji element m . Zbog $\omega \Vdash \Box(\Box p \rightarrow p)$ i ωRm vrijedi $m \Vdash \Box p \rightarrow p$, ali kako je $m \in \omega \setminus V(p)$, znamo da vrijedi $m \not\Vdash p$. Kako je m najmanji element skupa $\omega \setminus V(p)$, svaki svijet $n < m$ (što je po definiciji relacije R iz 1.3.6 ekvivalentno mRn) zadovoljava $n \Vdash p$. Stoga vrijedi $m \Vdash \Box p$. Međutim, ovo zajedno s $m \not\Vdash p$ je u kontradikciji s $m \Vdash \Box p \rightarrow p$. Dakle, svijet w ne može biti $\omega + 1$.

Primijetimo da ne može vrijediti $w = 0$ jer ne postoji svijet $v \in J$ takav da je $0Rv$. Iz toga slijedi da je $w = \omega$ ili neki element iz ω različit od 0. U oba slučaja imamo $wR0$. Iz činjenice $w \Vdash \Box\Diamond\top$ bi trebalo vrijediti $0 \Vdash \Diamond\top$, ali 0 nema sljedbenika, pa je ovo isto kontradikcija. Kako smo u oba slučaja došli do kontradikcije, početna je pretpostavka bila pogrešna. \square

Propozicija 2.3.2. *Na svakom okviru na kojem je valjana $\Box\Diamond\top \rightarrow \Box(\Box(\Box p \rightarrow p) \rightarrow p)$, valjana je i formula $\Box\Diamond\top \rightarrow \Box\perp$.*

Dokaz. Pretpostavimo suprotno. Tada postoji okvir $\mathfrak{J} = (WR)$ tako da imamo $\mathfrak{J} \Vdash \Box\Diamond\top \rightarrow \Box(\Box(\Box p \rightarrow p) \rightarrow p)$ i $\mathfrak{J} \not\Vdash \Box\Diamond\top \rightarrow \Box\perp$. Iz potonjeg slijedi da postoji svijet $\alpha \in W$ takav da $\alpha \not\Vdash \Box\Diamond\top \rightarrow \Box\perp$ (primijetimo da je ta formula neovisna o valuaciji), to jest $\alpha \Vdash \Box\Diamond\top$ i $\alpha \Vdash \neg\Box\perp$. Iz prvo navedenog i početne pretpostavke slijedi $\alpha \Vdash \Box(\Box(\Box p \rightarrow p) \rightarrow p)$. Činjenica $\alpha \Vdash \neg\Box\perp$ ekvivalentna je $\alpha \Vdash \neg\neg\Diamond\neg\perp$. Nakon što pokratimo dvostruku negaciju

i $\neg\perp$ dobijemo $\alpha \Vdash \diamond\top$. To povlači da postoji svijet $\beta \in W$ tako da vrijedi $\alpha R\beta$. Sada iz $\alpha \Vdash \Box(\Box p \rightarrow p) \rightarrow p$ i $\alpha R\beta$ imamo da vrijedi sljedeće:

$$\beta \Vdash \Box(\Box p \rightarrow p) \rightarrow p \quad (*)$$

Po definiciji valjanosti formule na okviru, početne pretpostavke trebaju biti valjane na svim modelima koji sadrže okvir \mathfrak{F} neovisno o valuaciji. Uzmimo valuaciju V za koju vrijedi $V(p) = \{\gamma : \beta R\gamma\} \setminus \{\beta\}$. Tada za svaki svijet γ koji je dostiživ iz β vrijedi $\gamma \Vdash p$, a onda očito vrijedi i $\gamma \Vdash \Box p \rightarrow p$. Stoga vrijedi $\beta \Vdash \Box(\Box p \rightarrow p)$. Budući da po definiciji valuacije vrijedi $\beta \nVdash p$ tada imamo $\beta \nVdash \Box(\Box p \rightarrow p) \rightarrow p$, što je kontradikcija s dokaznom činjenicom (*). \square

Propozicija 2.3.3. Formula $\Box\diamond\top \rightarrow \Box\perp$ nije valjana na općem okviru \mathfrak{F} .

Dokaz. Primijetimo da zbog $\omega R0$ vrijedi $\omega \Vdash \diamond\top$. Iz svijeta $(\omega + 1)$ dostiživ je samo svijet ω . Tada vrijedi $(\omega + 1) \Vdash \Box\diamond\top$. Zbog $(\omega + 1)R\omega$ vrijedi $(\omega + 1) \nVdash \Box\perp$ te zato formula $\Box\diamond\top \rightarrow \Box\perp$ nije valjana na općem okviru \mathfrak{F} . \square

Definicija 2.3.4. Modalna logika Λ je **potpuna u odnosu na okvire** ako postoji klasa okvira \mathbf{F} takva da je $\Lambda = \Lambda_{\mathbf{F}}$, gdje $\Lambda_{\mathbf{F}}$ označava skup svih formula koje su valjane na svim okvirima u klasi \mathbf{F} .

Dajemo primjere logika koje su potpune u odnosu na okvire.

Primjer 2.3.5. Logika \mathbf{K} potpuna je u odnosu na klasu svih okvira, $\mathbf{K4}$ u odnosu na klasu tranzitivnih okvira, a $\mathbf{S4}$ u odnosu na klasu okvira koji su tranzitivni i reflektivni.

Dokazi se mogu pronaći u [1] (kao dokazi teorema 4.23, 4.27, 4.29.)

Teorem 2.3.6. Logika \mathbf{KvB} nije potpuna u odnosu na okvire.

Dokaz. Kada bi postojala klasa okvira \mathbf{F} iz definicije 2.3.4, onda bi po definiciji 1.3.6 i propoziciji 2.3.1 na svakom od okvira $\mathfrak{F} \in \mathbf{F}$ bila valjana formula $\Box\diamond\top \rightarrow \Box(\Box p \rightarrow p) \rightarrow p$. Tada iz propozicije 2.3.2 slijedi da je na okviru \mathfrak{F} valjana i formula $\Box\diamond\top \rightarrow \Box\perp$. Međutim, sada bi iz definicija 2.3.4 i 1.3.6 slijedilo da je formula $\Box\diamond\top \rightarrow \Box\perp$ valjana na općem okviru \mathfrak{F} , što je u kontradikciji s propozicijom 2.3.3. \square

Napomena 2.3.7. Modalna logika \mathbf{KvB} nema svojstvo konačnih modela.

Dokaz. Zbog teorema 2.1.4 dovoljno je dokazati da logika \mathbf{KvB} nema svojstvo konačnih okvira. U tu svrhu pretpostavimo da ima, te neka je \mathbf{F} klasa konačnih okvira iz definicije 2.1.3. Tada iz činjenice da je svaka formula modalne logike \mathbf{KvB} valjana na okviru \mathbf{F} slijedi $\mathbf{KvB} \subseteq \mathcal{L}_{\mathbf{F}}$, a iz uvjeta da nijedna formula $\varphi \notin \mathbf{KvB}$ nije valjana na cijeloj klasi \mathbf{F}

dobivamo da vrijedi $KvB^c \subseteq \mathcal{L}_F^c$. Ovo posljednje povlači $\mathcal{L}_F \subseteq KvB$. Koristeći i prije dokazanu obratnu inkluziju, dobivamo $KvB = \mathcal{L}_F$, što je u kontradikciji s prethodnim teoremom 2.3.6. \square

Poglavlje 3

Metode interpretacije i kvazimodela

U prošlom poglavlju uvjerali smo se u korisnost svojstva konačnih modela za dokazivanje odlučivosti modalnih logika. Na primjeru logike KvB vidjeli smo i da sve modalne logike ne posjeduju to svojstvo. Prirodno se postavlja pitanje odlučivosti takvih logika.

U ovom poglavlju dokazat ćemo da je logika KvB odlučiva pomoću dvije različite metode: metode interpretacije i metode kvazimodela. Iako je u ovom poglavlju naglasak na dokazivanju odlučivosti logike KvB , metode koje ćemo obraditi primjenjive su i na druge logike koje nemaju svojstvo konačnih modela.

Poglavlje započinjemo razmatranjem metode interpretacije. To je metoda za dokazivanje odlučivosti problema u kojoj učinkovito svodimo jedan problem na drugi problem koji je već dokazano odlučiv. Budući da postoji puno odlučivih problema cilj nam je pronaći problem, ili klasu problema, na koje se problem odlučivosti modalnih logika može prirodno svesti. Štoviše, željeli bismo da svođenje bude što općenitije: da je primjenjivo na veliki broj problema modalne ispunjivosti i da postupak svođenja bude uniforman. Prikladna grupa problema je problem odlučivosti monadske logike drugog reda SnS koja je definirana na beskonačno dubokim stablima gdje svaki čvor ima n sljedbenika.

Prvo ćemo formalno definirati SnS , zatim ćemo dati skicu dokaza Rabinovog teorema koji dokazuje da je SnS odlučiva, a zatim obrađujemo metodu kvazimodela. Za veći dio ovog poglavlja koristili smo seminar [5].

3.1 Teorije SnS

Prvo definiramo monadsku teoriju drugog reda funkcija n sljedbenika, to jest teoriju koju označavamo sa SnS . Razumijevanje definicije bitno je za sljedeće potpoglavlje u kojem dokazujemo Rabinov teorem koji ćemo koristiti u dokazu odlučivosti logike KvB .

Definicija 3.1.1. Za alfabet \mathcal{A} sa \mathcal{A}^* označavamo skup svih konačnih riječi generiranih tim alfabetom. Definiramo sljedeće pojmove:

1. *Parcijalan uređaj \leq na \mathcal{A}^* : $x \leq y$ ako $y = xz$ za neki $z \in \mathcal{A}^*$. Ako vrijedi $x \leq y$ i $x \neq y$ tada pišemo $x < y$.*
2. *Pretpostavimo da je \mathcal{A} totalno uređen nekom relacijom $<_{\mathcal{A}}$. Tada definiramo **leksikografski uređaj** \leqslant na \mathcal{A}^* kao $x \leqslant y : \Leftrightarrow x \leq y$ ili je $x = zau$ i $y = zbv$, gdje je $a <_{\mathcal{A}} b$.*
3. *Za svaki $a \in \mathcal{A}$ definiramo **funkciju a -tog sljedbenika** $r_a : \mathcal{A}^* \rightarrow \mathcal{A}^*$ kao $r_a(x) = xa$.*

Definicija 3.1.2. Neka je n prirodan broj ili $n = \omega$, i neka je $T_n := \{i \in \omega \mid i < n\}^*$. Definiramo strukturu $\mathfrak{N}_n := (T_n, r_i, \leq, \leqslant)_{i < n}$, gdje za leksikografski uređaj \leqslant koristimo standardni uređaj prirodnih brojeva. \mathfrak{N}_n nazivamo **strukturu funkcija n sljedbenika**.

Monadna teorija drugog reda funkcija n sljedbenika, u oznaci S_nS , je teorija drugog reda u kojoj postoje samo jednomjesni predikati drugog reda, to jest samo pripadnost skupu, i koristi signaturu koja odgovara strukturi \mathfrak{N}_n (dakle, funkcijske simbole i -tog sljedbenika r_i te relacijske simbole uređaja).

Primjer 3.1.3. Neka je $n = 17$. Tada je T_n skup svih riječi oblika $a_0a_1a_2\dots a_m$ gdje su $a_i \in \{0, 1, 2, \dots, 16\}$, $i \leq m$. Primijetimo da ne možemo razlikovati riječ poput $a_0a_1a_2a_3 = 3516$ gdje su $a_0 = 3$, $a_1 = 5$, $a_2 = 1$ i $a_3 = 6$ od riječi $a_0a_1a_4 = 3516$ gdje je $a_4 = 16$. Taj problem rješiv je stavljanjem točaka iznad prve i zadnje znamenke višeznamenkastih elemenata skupa T_n . Tada je riječ $a_0a_1a_4$ jednaka $35\overset{\cdot}{1}\overset{\cdot}{6}$.

Primjer 3.1.4. Neka je

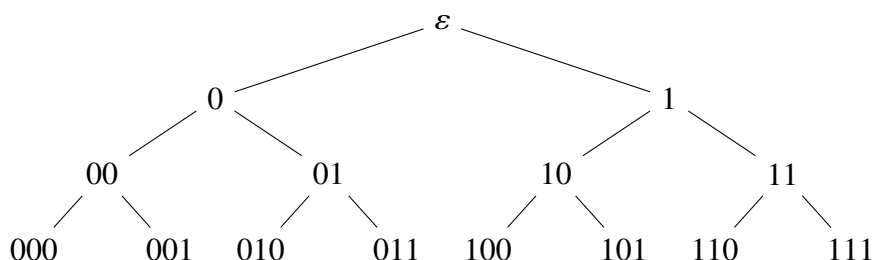
- $n = 0$. Tada je $\mathfrak{N}_0 = (\emptyset, \leq, \leqslant)$.
- $n = 1$. Tada je $\mathfrak{N}_1 = (T_0, r_0, \leq, \leqslant)$. Vidimo da je $T_0 = \{\varepsilon, 0, 00, 000, 0000, \dots\}$ gdje je ε oznaka za praznu riječ. Funkcija $r_0 : T_0 \rightarrow T_0$ preslika jedan čvor u drugi čvor koji ima točno jednu nulu više. Struktura \mathfrak{N}_1 beskonačno je stablo s korijenom ε u kojem svaki čvor $x \in T_0$ ima točno jedno dijete $r_0(x)$.
- $n = 2$. Tada je struktura $\mathfrak{N}_2 = (\{0, 1\}^*, r_0, r_2, \leq, \leqslant)$ beskonačno binarno stablo. Prve četiri razine beskonačnog binarnog stabla prikazane su na slici 3.1. Beskonačno binarno stablo ćemo formalno definirati u definiciji 3.2.2 sljedećeg potpoglavlja.
- $n = 3$. Tada je struktura $\mathfrak{N}_3 = (\{0, 1, 2\}^*, r_0, r_1, r_2, \leq, \leqslant)$ beskonačno stablo u kojem svaki čvor ima točno tri djeteta. Uzmimo čvor $12 \in T_2$. Prvo, drugo i treće dijete čvora 12 redom su čvorovi $r_0(12) = 120$, $r_1(12) = 121$ i $r_2(12) = 122$. Primijetimo da za svaki čvor $x \in T_2$ i njegovo dijete $y \in T_2$ vrijedi $x < y$ i $x \leqslant y$.

3.2 Rabinov teorem

Ovo potpoglavlje sadži redom definicije sljedećih pojmova: stablo, beskonačno binarno stablo, tablica, automat označen alfabetom te pojma izvršavanja. Sve te definicije će biti potrebne u dokazu Rabinovog teorema. Nakon što dokažemo jednu instancu Rabinovog teorema, dokazat ćemo da je logika **KvB** odlučiva.

Teorem 3.2.1 (Rabin). *Za bilo koji prirodan broj n ili za $n = \omega$, S_nS je odlučiva.*

Dokaz Rabinovog teorema može se pronaći u [7]. Mi ovdje dajemo skicu dokaza Rabinovog teorema za slučaj $n = 2$, odnosno za problem S_2S . Osim što nam je ovaj slučaj jedini nužan za dokaz odlučivosti logike **KvB**, ostali slučajevi za $n \in \omega$ dokazuju se sasvim analogno ovom, jedino je problem $S_\omega S$ nešto zahtjevniji. Za ovaj dokaz potrebno je uvesti pojam automata na beskonačnim binarnim stablima, a za to je prvo potrebno definirati beskonačna binarna stabla.



Slika 3.1: Prve četiri razine beskonačnog binarnog stabla

Definicija 3.2.2. *Neka su $r_0, r_1 : \{0, 1\}^* \rightarrow \{0, 1\}^*$ redom funkcije 0-tog i 1-tog sljedbenika. **Beskonačno binarno stablo** je uređeni par (T, R) , pri čemu je $T := \{0, 1\}^*$ skup svih konačnih nizova (riječi) nula i jedinica, a $R \subset T \times T$ relacija takva da za svaki $x \in T$ vrijedi $xRr_0(x)$ i $xRr_1(x)$. Elemente skupa T zovemo **čvorovima** stabla. Za svaki $x \in T$, čvorove $r_0(x)$ i $r_1(x)$ nazivamo **djecom** čvora x , a čvor x **roditeljem** čvorova $r_0(x)$ i $r_1(x)$. Praznu riječ ε zovemo **korijenom** stabla T .*

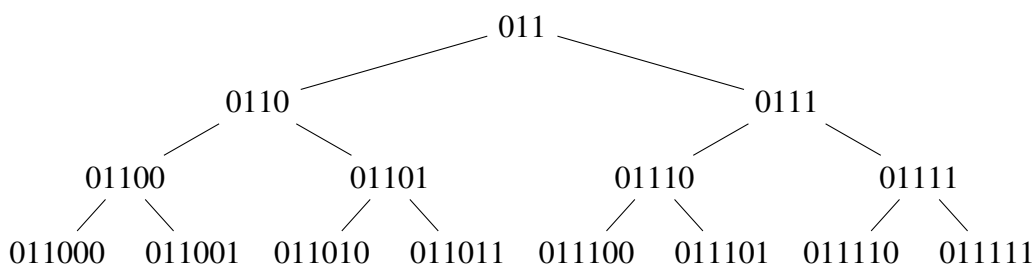
Za svaki čvor $x \in T$, **podstablo** u čvoru x je stablo $T_x := \{y \in T \mid x \leq y\}$, gdje je uređaj kao u definiciji 3.1.1. Samo stablo T je isto podstablo oblika T_ε , stoga poistovjećujemo ta dva zapisa. **Put** u stablu T_x je skup $\pi \subset T_x$ koji sadži korijen x , za svaki $y \in \pi$ vrijedi točno jedno od $r_0(y) \in \pi$ ili $r_1(y) \in \pi$ te ako $y \neq x$, onda je y roditelj od x u π .

Navodimo nekoliko primjera definiranih pojmova.

Primjer 3.2.3. Pogledajmo sliku 3.1. Čvorovi 0 i 1 djeca su korijena ε , dok je korijen ε roditelj djece 0 i 1. Također, čvorovi 010 i 011 imaju istog roditelja: čvor 01. Kažemo da su 010 i 011 djeca čvora 01.

Skupovi $\pi_0 = \{\varepsilon, 1, 11, 111, \dots\}$ i $\pi_1 = \{\varepsilon, 1, 10, 101, 1010, \dots\}$ primjeri su puteva u beskonačnom binarnom stablu. Navedeni putevi imaju logički slijed što, naravno, nije uvjet.

Primjer 3.2.4. Na sljedećoj slici ilustriramo prve četiri razine podstabla u čvoru 011.



Slika 3.2: Prve četiri razine podstabla u čvoru 011

Neka je $r_0 : T_{011} \rightarrow T_{011}$ funkcija 0-tog sljedbenika, skup $\pi_0 = \{011\}$ i za svaki $n \in \mathbb{N}$ definiramo skup $\pi_{n+1} = \{r_0(x) \mid x \in \pi_n\}$. Tada je $\pi = \bigcup_{n \in \mathbb{N}} \pi_n$ put u podstablu T_{011} .

Propozicija 3.2.5. Neka je T_z stablo, π neki u stablu T_z i $x, y \in \pi$. Tada vrijedi $x \leq y$ ili $y \leq x$.

Dokaz. Pretpostavimo da ne vrijedi $x \leq y$ niti $y \leq x$. Znamo da su čvorovi x i y oblika $x = a_1 a_2 \dots a_n$ i $y = b_1 b_2 \dots b_m$ za neke $a_1, \dots, a_n, b_1, \dots, b_m \in \{0, 1\}$. Za svaki čvor puta vrijedi da je i roditelj tog čvora u putu. Slijedi da za svaki $i \leq n$ i svaki $j \leq m$ vrijedi $a_1 \dots a_i \in \pi$ i $b_1 \dots b_j \in \pi$. Iz početne pretpostavke slijedi da postoji $k \leq \min\{n, m\}$ takav da $a_k \neq b_k$. Označimo najmanji takav sa l . Ako je $l = 1$, onda su $0, 1 \in \pi$ što je u kontradikcijom s time da vrijedi ili $r_0(\varepsilon) \in \pi$ ili $r_1(\varepsilon) \in \pi$. Ako je $l > 1$, onda $a_1 \dots a_{l-1} = b_1 \dots b_{l-1}$. Činjenice $a_l \neq b_l$ i $a_1 \dots a_l, b_1 \dots b_l \in \pi$ zajedno s prethodnom tvrdnjom povlače $a_1 \dots a_{l-1} 0, a_1 \dots a_{l-1} 1 \in \pi$. No, to je u kontradikciji s činjenicom da vrijedi ili $r_0(a_1 a_2 \dots a_{l-1}) \in \pi$ ili $r_1(a_1 a_2 \dots a_{l-1}) \in \pi$. \square

Definicija 3.2.6. Za proizvoljnu funkciju $f : A \rightarrow B$ označimo s $In(f)$ skup

$$In(f) := \{b \in B \mid \text{card}(f^{-1}(b)) \geq \aleph_0\}.$$

Elemente ovog skupa nazovimo **gomilišta** ili **akumulacijske točke** funkcije f .

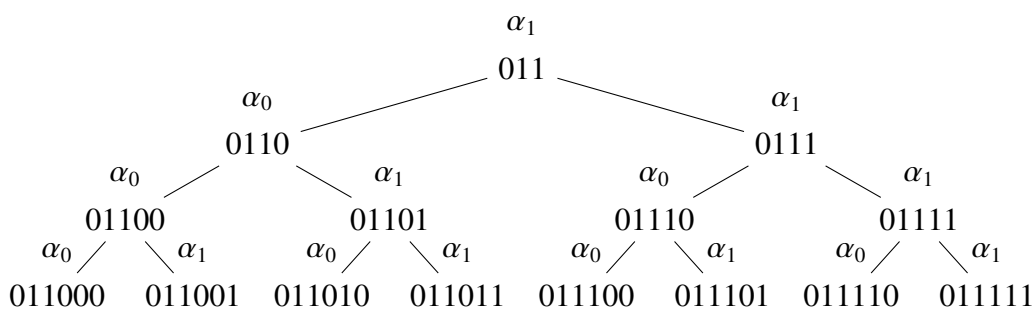
U idućim definicijama podrazumijevamo da je zadan konačan skup Σ koji zovemo **alfabet**.

Definicija 3.2.7. Neka je T_x stablo s korijenom x . Σ -označeno stablo (ili kraće Σ -stablo) je uređeni par (v, T_x) , gdje je $v : T_x \rightarrow \Sigma$. Preslikavanje v nazivamo valuacijom stabla. Σ -podstablo u x nekog Σ -stabla (v, T) je uređeni par $(v|_{T_x}, T_x)$. Umjesto toga kraće pišemo (v, T_x) .

Primjer 3.2.8. Neka je alfabet $\Sigma = \{\alpha_0, \alpha_1\}$, stablo T_{011} iz primjera 3.2.3, r_0 funkcija 0-tog sljedbenika i valuacija v definirana na sljedeći način:

$$v(x) = \begin{cases} \alpha_0, & \text{ako } x = r_0(y) \text{ za neki } y \in T_{011} \\ \alpha_1, & \text{inače.} \end{cases}$$

Tada je (v, T_{011}) jedno Σ -stablo. Ilustriramo Σ -stablo (v, T_{011}) na sljedećoj slici.



Slika 3.3: Prve četiri razine Σ -stabla (v, T_{011})

Ako je zadano stablo T i neki njegov čvor x , onda skup svih Σ -stabala (v, T_x) označavamo s V_x^Σ . Primijetimo da je drugi član uređenog para (v, T_x) konstantan, tako da ustvari nabrajamo samo po svim mogućim funkcijama v . Uvedimo i oznaku $V^\Sigma := \bigcup_{x \in T} V_x^\Sigma$.

Definicija 3.2.9. *Tablica nad Σ -stablina* (ili kraće Σ -tablica) je uređeni par $\mathfrak{A} = (S, M)$, gdje je S konačan skup čije elemente zovemo *stanja*, a $M : S \times \Sigma \rightarrow \mathcal{P}(S \times S)$ je (nedeterministička) *funkcija prijelaza*.

Konačni automat nad Σ -stablina (Σ -automat) je uređena četvorka $\mathfrak{A} = (S, M, S_0, F)$, gdje su S i M isto definirani kao u definiciji Σ -tablice, $S_0 \subseteq S$ je skup *početnih stanja* i $F \subseteq \mathcal{P}(S)$ je skup *označenih podskupova* od S .

Primjer 3.2.10. Razlog naziva Σ -tablica leži u tome što je stvarno možemo prikazati kao tablicu. Primjerice, Σ -tablicu $\mathfrak{A} = (S, M)$ gdje su $\Sigma = \{\alpha_0, \alpha_1\}$, $S = (s_0, s_1, s_2)$, a M je definirana kao $M(\alpha_i, s_j) = \{(s_k, s_k) : i \leq k \leq j\}$ možemo prikazati na sljedeći način:

$\Sigma \setminus S$	s_0	s_1	s_2
α_0	$\{(s_0, s_0)\}$	$\{(s_0, s_0), (s_1, s_1)\}$	$\{(s_0, s_0), (s_1, s_1), (s_2, s_2)\}$
α_1	\emptyset	$\{(s_1, s_1)\}$	$\{(s_1, s_1), (s_2, s_2)\}$

Neka je $S_0 = \{s_0, s_1\}$ skup početnih stanja i $F = \{\{s_0\}, \{s_0, s_2\}\}$ skup označenih podskupova podskupova od S . Tada je $\mathfrak{A} = (S, M, S_0, F)$ primjer jednog Σ -automata.

Definicija 3.2.11. Neka je $t = (v, T_x)$ neko Σ -stablo te $\mathfrak{A}' = (S, M)$ neka Σ -tablica. **Izvršavanje** Σ -tablice \mathfrak{A}' na Σ -stablu t je preslikavanje $r : T_x \rightarrow S$ gdje za svaki $y \in T_x$ vrijedi $(r(y_0), r(y_1)) \in M(r(y), v(y))$. Na isti način definiramo izvršavanje automata \mathfrak{A} na stablu. Skup svih takvih izvršavanja označavamo s $Rn(\mathfrak{A}, t)$.

Prije nego što ćemo navesti daljnje definicije važno je razviti intuiciju oko Σ -automata i njihovih izvršavanja na stablima. Kao prvo, riječ "konačni" u nazivu automata ne znači da izvršavanje traje konačno mnogo koraka, kao što je slučaj kod automata na riječima nekog jezika. Isto kao i kod automata nad riječima, naziv "konačni" odnosi se na to da ima samo konačno mnogo stanja. Štoviše, svako izvršavanje automata na stablima trajat će beskonačno.

Stroj kreće od korijena označenog stabla te u svakom koraku na temelju stanja i oznake u trenutnom čvoru nedeterministički "bira" dozvoljena stanja za djecu tog čvora na temelju funkcije prijelaza M . Važno je uočiti da svaki čvor ima svoju oznaku i svoje stanje. Dakle, u n -tom koraku istovremeno se nalazimo u 2^{n-1} stanja, ovisno o čvoru koji promatramo na n -toj razini stabla. Također, stanja čvorova x_0 i x_1 ovise isključivo o oznaci i stanju čvora x .

Slijedi konkretan primjer jednog izvršavanja.

Primjer 3.2.12. Neka je skup $\Sigma = \{\alpha_0, \alpha_1\}$ alfabet, $t = (v, T_{011})$ Σ -stablo iz primjera 3.2.8 i $\mathfrak{A}' = (S, M)$ Σ -tablica iz primjera 3.2.10. Definiramo preslikavanje $r : T_{011} \rightarrow S$ na sljedeći način:

$$r(x) = s_1 \text{ za svaki čvor } x \in T_{011}.$$

Preslikavanje r jedno je izvršavanje Σ -tablice \mathfrak{A}' na Σ -stablu t .

Definicija 3.2.13. Kažemo da automat $\mathfrak{A} = (S, M, S_0, F)$ **prihvća** Σ -stablo $t = (v, T_x)$ ako postoji izvršavanje $r \in Rn(\mathfrak{A}, t)$ takvo da je $r(x) \in S_0$ i za svaki put $\pi \subset T_x$ vrijedi $In(r|_\pi) \in F$. Uvedimo oznaku

$$T(\mathfrak{A}) := \{(v, T_x) \mid x \in T, \mathfrak{A} \text{ prihvaća } (v, T_x)\}.$$

Kažemo da je skup $A \subseteq V^\Sigma$ **definabilan** ako postoji automat \mathfrak{A} takav da je $A = T(\mathfrak{A})$.

Proširimo sada intuiciju o konačnim automatima iz prethodnih razmatranja. Da bi automat prihvaćao neko stablo, odnosno da bi neko izvršavanje bilo "ispravno", mora započeti nekim od početnih stanja u korijenu. Međutim, kako se stroj nikad ne zaustavlja, situacija sa završnim stanjima je dosta neobično definirana. Naime, umjesto završnih stanja imamo **označene skupove** stanja, te kretanjem od korijena prema dolje, neovisno o odabiru puta, skup onih stanja koja posjetimo beskonačno mnogo puta mora biti označen skup.

Napomena 3.2.14. Za skup $A \subseteq V^\Sigma$ kažemo da je **invarijantan** ako za svako Σ -stablo $t = (v, T)$ i svaki $x \in T$ vrijedi da je $t \in A$ ako i samo ako je $(v', T_x) \in A$, gdje je $v'(xy) := v(y)$, $y \in T$. Drugim riječima, invarijantne skupove stabala "ne zanima" koji je koji čvor, što je korijen i slično, nego samo relativni raspored čvorova i njihove oznake. Dakle, ako bismo oznake čitavog stabla "translatirali" od korijena prema nekom čvoru x tako da odnos roditelja i djece ostane očuvan, onda bi podstablo s korijenom u x bilo "ekvivalentno" originalnom stablu.

Primijetimo da familija svih invarijantnih podskupova od V^Σ čini Booleovu algebru, to jest zatvorena je na uniju, presjek i komplement. S obzirom na to da pitanje prihvaćanja označenih stabala kod automata ovisi isključivo o oznakama tog stabla, za svaki automat \mathfrak{A} skup $T(\mathfrak{A})$ je invarijantan. Dakle, da bismo za neki drugi invarijantan skup A dokazali da je definabilan, dovoljno je konstruirati automat \mathfrak{A} takav da je $(v, T) \in T(\mathfrak{A})$ ako i samo ako je $(v, T) \in A$, to jest dovoljno je promatrati samo cijelo stablo T jer nas ne zanima koja podstabla prihvaća \mathfrak{A} .

Sada, koristeći ove zaključke možemo dokazati sljedeća dva rezultata.

Lema 3.2.15. Za svaki definabilan skup A postoji automat $\mathfrak{A} = (S, M, \{s_0\}, F)$ takav da je $T(\mathfrak{A}) = A$.

Dokaz. Zbog definabilnosti skupa A postoji automat $\mathfrak{A}' = (S', M', S'_0, F')$ takav da je $T(\mathfrak{A}') = A$. Neka su $s_1, s_2, \dots, s_k \in S'_0$ sva početna stanja automata kojima započinju izvršavanja koja prepoznaju stabla iz A . Sada definiramo $\mathfrak{A} := (S := (S')^k, M, \{s_0 := (s_1, \dots, s_k)\}, F)$, gdje je

$$M((q_1, \dots, q_k), \alpha) := \bigcup_{i=1}^k M'(q_i, \alpha), \quad q_1, \dots, q_k \in S', \alpha \in \Sigma$$

te vrijedi da je $\{(q_1^1, \dots, q_k^1), \dots, (q_1^n, \dots, q_k^n)\} \in F$ ako i samo ako postoje stanja $q_{i_1}^1, q_{i_2}^2, \dots, q_{i_n}^n$ takva da je $\{q_{i_1}^1, q_{i_2}^2, \dots, q_{i_n}^n\} \in F'$. Budući da je M nedeterministična funkcija, izvršavanja automata \mathfrak{A} su zapravo sva izvršavanja automata \mathfrak{A}' po bilo kojoj od k komponenti. Iz definicija stanja s_0 i skupa F slijedi da automat \mathfrak{A} prihvaća ona stabla koja prihvaća automat \mathfrak{A}' u **bilo kojem** od svih mogućih izvršavanja s početkom u nekom od k početnih stanja. Iz toga vidimo da vrijedi $T(\mathfrak{A}) = T(\mathfrak{A}') = A$. \square

S obzirom na rezultat prethodne leme, od sada pa nadalje za konačne automate ćemo koristiti i oznaku (S, M, s_0, F) umjesto $(S, M, \{s_0\}, F)$ kad je riječ o automatu sa samo jednim početnim stanjem.

Teorem 3.2.16. *Ako su skupovi A i B definabilni, onda su i skupovi $A \cup B$ i $A \cap B$ definabilni.*

Dokaz. Neka su dani skupovi $A = T(\mathfrak{A})$ i $B = T(\mathfrak{B})$, za neke konačne automate $\mathfrak{A} = (S, M, s_0, F)$ i $\mathfrak{B} = (S', M', s'_0, F')$. Bez smanjenja općenitosti možemo pretpostaviti da je skup $S \cap S' = \emptyset$, inače gledamo konačne automate sa skupovima stanja $S \times \{0\}$ i $S' \times \{1\}$. Sada je jasno da automat

$$\mathfrak{A} \cup \mathfrak{B} := (S \cup S', M \cup M', \{s_0, s'_0\}, F \cup F')$$

prepoznaje upravo skup $A \cup B$. Uz iste oznake definiramo i automat

$$\mathfrak{A} \times \mathfrak{B} := (S \times S', \tilde{M}, (s_0, s'_0), \tilde{F} := \{G \subseteq S \times S' \mid p_1(G) \in F, p_2(G) \in F'\}),$$

gdje je $\tilde{M}((s, s'), \alpha) := M(s, \alpha) \times M'(s', \alpha)$, te p_1 i p_2 koordinatne projekcije $(x, y) \mapsto x$ i $(x, y) \mapsto y$, redom. Uočavamo da automat $\mathfrak{A} \times \mathfrak{B}$ prepoznaje skup $A \cap B$. \square

Definicija 3.2.17. *Neka je $t = (v, T)$ neko $\Sigma_1 \times \Sigma_2$ -označeno stablo te p_1 projekcija $(x, y) \mapsto x$. Definiramo projekciju označenog stabla kao $p_1(t) := (p_1(v), T) \in V^{\Sigma_1}$. Projekciju skupa stabala definiramo po elementima, odnosno $p_1(A) := \{p_1(t) \mid t \in A\}$, $A \in V^{\Sigma_1 \times \Sigma_2}$.*

Neka je skup $B \subseteq V^{\Sigma_1}$ i Σ_2 neki alfabet. Najveći skup $A \subseteq V^{\Sigma_1 \times \Sigma_2}$ takav da je $p_1(A) = B$ nazivamo Σ_2 -cilindrifikacija skupa B .

Ako su čvorovi stabla označeni uređenim parovima koji su elementi skupa $\Sigma_1 \times \Sigma_2$, onda projekciju p_1 označenog stabla dobivamo tako što umjesto uređenih parova promatramo samo prve članove uređenih parova kao oznake čvorova. Slično vrijedi i za skupove označenih stabala.

S druge strane, ako imamo skup stabala B čiji su čvorovi označeni znakovima iz nekog alfabeta Σ_1 , onda njegovu Σ_2 -cilindrifikaciju dobivamo tako da umjesto znakova iz Σ_1 kao oznake promatramo uređene parove iz $\Sigma_1 \times \Sigma_2$. Σ_2 -cilindrifikacija je tada skup svih mogućih uređenih parova gdje su prvi članovi parova iz skupa A .

Razlog naziva **cilindrifikacija** geometrijske je prirode. Ako imamo neki skup točaka u ravnini (npr. krivulja) $B \subseteq \mathbb{R}^2$, onda je cilindar nad skupom B upravo najveći skup $A \subseteq \mathbb{R}^3$ takav da je $p_{1,2}(A) = B$, gdje je $p_{1,2}$ koordinatna projekcija $(x, y, z) \mapsto (x, y)$. U ovom slučaju taj skup možemo definirati jednostavnije kao $A := B \times \mathbb{R}$, ali ovaj pristup nije primjenjiv u definiciji 3.2.17 jer je tamo $p_1(A)$ "dodefinirana" na elementima skupa A , dakle $B \times V^{\Sigma_2}$ ima drugo značenje.

Teorem 3.2.18. *Ako je skup $A \subseteq V^{\Sigma_1 \times \Sigma_2}$ definabilan, onda je i skup $p_1(A) \subseteq V^{\Sigma_1}$ definabilan. Obratno, ako je skup $B \subseteq V^{\Sigma_1}$ definabilan, onda je njegova Σ_2 -cilindrifikacija $C \subseteq V^{\Sigma_1 \times \Sigma_2}$ definabilna.*

Dokaz. Neka su dani skupovi $A = T(\mathfrak{A})$ i $B = T(\mathfrak{B})$, za neke konačne automate $\mathfrak{A} = (S, M, s_0, F)$ i $\mathfrak{B} = (S', M', s'_0, F')$. Sada je jasno da za automat

$$\mathfrak{A}_g := (S, M_1, s_0, F),$$

gdje je $M_1(s, \alpha) = \bigcup_{\beta \in \Sigma_2} M(s, (\alpha, \beta))$, vrijedi $T(\mathfrak{A}_g) = p_1(A)$, a za automat

$$\mathfrak{B}_g = (S', M'_1, s'_0, F'),$$

gdje je $M'_1(s, (\alpha, \beta)) = M'(s, \alpha)$, vrijedi $T(\mathfrak{B}_g) = C$. □

Sljedeću definiciju uvodimo radi opisivanja komplementa definabilnih skupova.

Definicija 3.2.19. *Neka je $\Omega = ((L_i, U_i))_{1 \leq i \leq k}$ niz uređenih parova skupova stanja, T_x neko stablo i S skup stanja. Za preslikavanje $\phi : T_x \rightarrow S$ kažemo da je **tipa Ω** (oznaka: $\phi \in [\Omega]$) ako postoji $i, 1 \leq i \leq k$, takav da $In(\phi) \cap L_i = \emptyset$ i $In(\phi) \cap U_i \neq \emptyset$.*

*Ako je ϕ tipa Ω i za neki $j, 1 \leq j \leq k$, vrijedi $\phi(T_x) \cap L_j = \emptyset$, kažemo da je ϕ **tipa Ω -prazno** (oznaka: $\phi \in [\Omega, e]$).*

*Neka je $\mathfrak{A} = (S, M)$ Σ -tablica i $s \in S$ neko stanje. Kažemo da \mathfrak{A} **dualno prihvaća** Σ -stablo (v, T_x) (oznaka: $(v, T_x) \in \mathcal{D}(\mathfrak{A}, \Omega, s)$) ako za svaki $r \in Rn(\mathfrak{A}, (v, T_x))$ za koji vrijedi $r(x) = s$ postoji put $\pi \subset T_x$ takav da $r|_{\pi} \in [\Omega]$.*

Sljedeće dvije leme su ključne za dokaz Rabinovog teorema, no nećemo ih dokazivati. Dokazi se mogu pronaći u [7].

Lema 3.2.20. *Za svaki Σ -automat \mathfrak{A} postoji Σ -tablica $\mathfrak{A}' = (S, M)$, niz Ω i stanje $s \in S$ takvi da*

$$(v, T) \in V^{\Sigma} \setminus T(\mathfrak{A}) \text{ ako i samo ako } (v, T) \in \mathcal{D}(\mathfrak{A}', \Omega, s).$$

Lema 3.2.21. *Neka je $\mathfrak{A} = (S, M)$ Σ -tablica, $\bar{s} \in S$ stanje, $\bar{\Sigma} = \Sigma \times P(S)$ produkt alfabeti i partitivnog skupa stanja, $\Omega = ((L_i, U_i))_{1 \leq i \leq k}$ niz i A skup svih $\bar{\Sigma}$ -stabla takav da*

$$\bar{i} = (\bar{v}, T_x) \in A \text{ ako i samo ako}$$

$$\forall r[r \in Rn(\mathfrak{A}, p_1(\bar{i})) \wedge r(x) = \bar{s} \rightarrow \exists \pi(\pi \subset T_x \wedge r|_{\pi} \in [\Omega, e]) \vee \exists y(y \in T_x \wedge \bar{v}(y) = (\alpha, q) \wedge r(y) \in q)].$$

Tada postoji tablica $\mathfrak{B} = (S^{\mathfrak{B}}, M^{\mathfrak{B}})$, stanje $s^{\mathfrak{B}}$ i niz $\Omega^{\mathfrak{B}} = ((L_i^{\mathfrak{B}}, U_i^{\mathfrak{B}}))_{1 \leq i \leq k}$, gdje je $L_k^{\mathfrak{B}} = \emptyset$ takvi da vrijedi $A = \mathcal{D}(\mathfrak{B}, \Omega^{\mathfrak{B}}, s^{\mathfrak{B}})$.

Lema 3.2.22. *Neka je $\mathfrak{A} = (S, M)$ Σ -tablica, $s_0 \in S$ stanje, $\Omega = ((L_i, U_i))_{1 \leq i \leq k}$ i $\Omega_{k-1} = ((L_i, U_i))_{1 \leq i \leq k-1}$ nizovi uređenih parova skupova stanja. Ako za Σ -stablo $t = (v, T)$ vrijedi $t \in \mathcal{D}(\mathfrak{A}, \Omega, s_0)$, onda postoji skup $H \subseteq (T \setminus \{\varepsilon\}) \times U_k$ takav da:*

$$\forall r[r \in Rn(\mathfrak{A}, t) \wedge r(\varepsilon) = s_0 \rightarrow [\forall \pi(r|_{\pi} \notin [\Omega_{k-1}]) \rightarrow \exists x((x, r(x)) \in H)]].$$

Pokušat ćemo dati neku ideju dokaza prethodne leme. Uzmimo proizvoljno stablo $t = (v, T)$ takvo da $t \in \mathcal{D}(\mathfrak{A}, \Omega, s_0)$ za neki automat \mathfrak{A} , niz Ω i stanje s_0 . Ako za neko izvršavanje $r \in Rn(\mathfrak{A}, t)$, koje zadovoljava $r(\varepsilon) = s_0$, vrijedi da za svaki put π $r|_{\pi}$ nije tipa Ω_{k-1} , tada iz činjenice $t = (v, T) \in \mathcal{D}(\mathfrak{A}, \Omega, s_0)$ zaključujemo da postoji put π_0 takav da vrijedi $In(r|_{\pi_0}) \cap L_k = 0$ i $In(r|_{\pi_0}) \cap U_k \neq 0$. Iz $In(r|_{\pi_0}) \cap U_k \neq 0$ zaključujemo da postoji čvor x takav da $r(x) = s \in U_k$. Skup H će sadržavati takve parove (x, s) .

Primijetimo da formulu iz iskaza prethodne leme možemo napisati i u obliku:

$$\forall r[r \in Rn(\mathfrak{A}, t) \wedge r(\varepsilon) = s \rightarrow \exists \pi(r|_{\pi} \in [\Omega_{k-1}]) \vee \exists x(r(x) \in H)].$$

Naredna lema važna je za dokaz Rabinovog teorema. Dokaz leme izostavljamo, a može se pronaći u [7].

Lema 3.2.23. *Neka je $\mathfrak{A} = (S, M)$ Σ -tablica, $s_0 \in S$ stanje te T stablo. Ako postoji skup $H_0 \subseteq T \times S$ takav da za svako izvršavanje $r \in Rn(\mathfrak{A}, T)$, takvo da $r(\varepsilon) = s_0$, postoji čvor $x \in T$ takav da vrijedi $(x, r(x)) \in H_0$, onda postoji konačan skup $H_1 \subseteq H_0$ s istim svojstvom.*

Idući teorem ima složeniji dokaz koji se može pronaći u trećem poglavlju [7] kao 3.11.

Teorem 3.2.24. *Komplement $V^{\Sigma} \setminus T(\mathfrak{A})$ definabilnog skupa je definabilan.*

Sljedeći teorem nužan je za dokaz Rabinovo teorema. No, prije nego što prijedemo na teorem, bitno je uvesti još par definicija pojmova koje ćemo koristiti u dokazu teorema.

Definicija 3.2.25. *Neka je $\mathfrak{A} = (S, M)$ Σ -tablica, te $S' \subseteq S$. Definiramo **ograničenje tablice \mathfrak{A} na S'** kao $\mathfrak{A}|_{S'} = (S, M')$, gdje je $M'(\alpha, s) = M(\alpha, s) \cap \Sigma \times S'$.*

Primijetimo da su izvršavanja r tablice $\mathfrak{A}|_{S'}$ na stablu T_x upravo ona izvršavanja tablice \mathfrak{A} za koja vrijedi $r(y) \in S'$ za svaki $y > x$.

Definicija 3.2.26. *Slabu monadsku teoriju drugog reda funkcija n sljedbenika, u oznaci $WSnS$, definiramo analogno kao SnS sa jedinom razlikom da su varijable ograničene na konačne skupove.*

J. E. Doner 1965. godine je dokazao odlučivost teorije $WS2S$. Dokaz se može se pronaći u [4].

Teorem 3.2.27. *Pitanje vrijedi li $T(\mathfrak{A}) = \emptyset$ za zadani automat \mathfrak{A} je odlučivo. Navedeno pitanje nazivamo problem praznosti za konačne automate nad stablima.*

Dokaz. Za sve automate oblika $\mathfrak{A} = (S, M, s_0, \{\emptyset\})$ vrijedi $T(\mathfrak{A}) = \emptyset$, pa postoji automat \mathfrak{A} za koji vrijedi $T(\mathfrak{A}) = \emptyset$.

Cilj nam je pronaći algoritam kojim za svaki Σ -automat $\mathfrak{A} = (S, M, s_0, F)$ možemo odrediti vrijedi li $T(\mathfrak{A}) = \emptyset$.

Promotrimo jednočlan alfabet $\bar{\Sigma} = \{\alpha\}$ i $\bar{\Sigma}$ -automat $\bar{\mathfrak{A}} = (S, \bar{M}, s_0, F)$, gdje je $\bar{M}(s, \alpha) = \bigcup_{\beta \in \Sigma} M(s, \beta)$. Za stabla nad jednočlanim alfabetima postoji samo jedna valuacija stoga ćemo izostavljati alfabet i valuaciju dok pričamo o navedenim stablima. To jest, umjesto $\bar{\Sigma}$ -stabla (v, T) pisat ćemo stablo T . Također, umjesto $\bar{M}(s, \alpha)$ pisat ćemo $\bar{M}(s)$.

Primijetimo da je svako izvršavanje automata \mathfrak{A} na Σ -stablu (v, T) ujedno i izvršavanje automata $\bar{\mathfrak{A}}$ na stablu T . Također, za svako izvršavanje $r \in Rn(\mathfrak{A}, T)$ postoji valuacija v takva da $r \in Rn(\mathfrak{A}, (v, T))$. Ta zapažanja i činjenica da je skup svih podstabla stabla T invarijantan povlače:

$$T(\mathfrak{A}) \neq \emptyset \text{ ako i samo ako } T(\bar{\mathfrak{A}}) \neq \emptyset \text{ ako i samo ako } T(\bar{\mathfrak{A}}) = \{T_x : x \in T\}.$$

Zato se možemo, radi jednostavnosti, fokusirati samo na automate nad jednočlanim stablima.

Po teoremu 3.2.24 znamo da je skup $V^{\bar{\Sigma}} \setminus T(\bar{\mathfrak{A}})$ definabilan što povlači da postoji automat \mathfrak{B} takav da vrijedi $T(\mathfrak{B}) = V^{\bar{\Sigma}} \setminus T(\bar{\mathfrak{A}})$, to jest $T(\bar{\mathfrak{A}}) = V^{\bar{\Sigma}} \setminus T(\mathfrak{B})$. Sada po lemi 3.2.20 znamo da postoje tablica \mathfrak{C} , niz Ω i stanje s' za koje vrijedi:

$$T \in T(\bar{\mathfrak{A}}) \text{ ako i samo ako } T \in \mathfrak{D}(\mathfrak{C}, \Omega, s').$$

Iz te tvrdnje slijedi da ako za proizvoljnu $\bar{\Sigma}$ -tablicu $\mathfrak{A} = (S, M)$, proizvoljni niz $\Omega = ((L_i, U_i))_{1 \leq i \leq k}$ i proizvoljno stanje $s_0 \in S$ možemo utvrditi vrijedi li $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$ tada je problem praznosti za konačne automate nad stablima odlučiv. Zato u nastavku dajemo algoritam kako odrediti vrijedi li $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$.

Algoritam je ovaj: prvo ćemo pitanje $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$ svesti na konačno mnogo pitanja vrijedi li $T \in \mathfrak{D}(\mathfrak{A}', \Omega', s)$, gdje je \mathfrak{A}' neka tablica, niz $\Omega' = ((L'_i, U'_i))_{1 \leq i \leq k}$ i skup $L_k = \emptyset$. Zatim ćemo ta pitanja svesti na konačno mnogo pitanja oblika $T \in \mathfrak{D}(\mathfrak{A}'', \Omega_{k-1}, s')$. Budući da je prethodna dva koraka moguće ponavljati sve dok ne dođemo do konačno problema oblika $T \in \mathfrak{D}(\mathfrak{A}, ((\emptyset, U)), s)$, na kraju će preostati pokazati da je taj problem svediv na dokazano odlučiv problem. Preciznije, svest ćemo problem $T \in \mathfrak{D}(\mathfrak{A}, ((\emptyset, U)), s)$ na konačno mnogo problema $WS2S$.

Krenimo s reduciranjem na konačno problema $T \in \mathcal{D}(\mathfrak{A}, \Omega', s)$, gdje je $\Omega' = ((L'_i, U'_i))_{1 \leq i \leq k}$ i $L_k = \emptyset$. U tu svrhu definiramo niz $(H_m)_{m < l}$ podskupova skupa stanja S na sljedeći način:

- $s \in H_0$ ako i samo ako $\forall r[r \in Rn(\mathfrak{A}, T) \wedge r(\varepsilon) = s \rightarrow \exists \pi(r|_\pi \in [\Omega, e])]$,
- $s \in H_{m+1}$ ako i samo ako $s \notin \bigcup_{i \leq m} H_i$ i vrijedi:

$$\forall r[r \in Rn(\mathfrak{A}, T) \wedge r(\varepsilon) = s \rightarrow \exists \pi(r|_\pi \in [\Omega, e]) \vee \exists y(r(y) \in \bigcup_{i \leq m} H_i)]. \quad (3.1)$$

Primijetimo da zbog uvjeta $s \notin \bigcup_{i \leq m} H_i$ prilikom definiranja skupa H_{m+1} vrijedi da se svako stanje može nalaziti u samo jednom skupu niza. Ako kardinalnost skupa S označimo s n , tada za sve skupove H_m , gdje je $m > n$, vrijedi $H_m = \emptyset$.

Po definiciji skupa H_0 vidimo da se u njemu nalaze se sva moguća početna stanja s za koja bi svako izvršavanje r stabla T na automatu \mathfrak{A} postojao put π takav da je $r|_\pi \in [\Omega, e]$. Budući da $r|_\pi \in [\Omega, e]$ povlači $r|_\pi \in [\Omega]$, vidimo da vrijedi $T \in \mathcal{D}(\mathfrak{A}, \Omega, s)$.

Promotrimo skupove H_{m+1} , za $m \in \mathbb{N}$, počevši od skupa H_1 . Za stanje $s \in H_1$ vrijedi da za svako izvršavanje za koje je s početno stanje postoji put π takav da je $r|_\pi \in [\Omega, e]$ ili postoji čvor y takav da $r(y) \in H_0$.

Primijetimo da će od te dvije opcije vrijediti samo:

$$\forall r[r \in Rn(\mathfrak{A}, T) \wedge r(\varepsilon) = s \rightarrow \exists y(r(y) \in \bigcup_{i \leq m} H_i)]$$

jer da vrijedi:

$$\forall r[r \in Rn(\mathfrak{A}, T) \wedge r(\varepsilon) = s \rightarrow \exists \pi(r|_\pi \in [\Omega, e])]$$

bi stanje s bilo element skupa H_0 te se ne bi moglo nalaziti u H_1 .

To znači da postoji put $\pi' \subset T_y$ takav da vrijedi $r|_{\pi'} \in [\Omega, e]$. Budući da do čvora y možemo imati samo konačno mnogo drugih čvorova vidimo da postoji put $\pi \subset T$, $\pi' \subset \pi$, takav da $r|_\pi \in [\Omega]$ te zato i za stanja $s \in H_1$ vrijedi $T \in \mathcal{D}(\mathfrak{A}, \Omega, s)$. Analogno zaključujemo da za svako stanje $s' \in H_{m+1}$ vrijedi $T \in \mathcal{D}(\mathfrak{A}, \Omega, s')$. Na sličan način možemo dokazati da za svako stanje s za koje vrijedi $T \in \mathcal{D}(\mathfrak{A}, \Omega, s)$, vrijedi i $s \in \bigcup_{m \leq n} H_m$. Zbog sličnosti dokaza ćemo izostaviti dokaz te tvrdnje.

Time smo dobili da vrijedi:

$$T \in \mathcal{D}(\mathfrak{A}, \Omega, s_0) \text{ ako i samo ako } s_0 \in \bigcup_{m \leq n} H_m$$

ako i samo ako $s_0 \in H_j$ za neki $j, 0 \leq j \leq n$

ako i samo ako za s_0 i neki H_j vrijedi 3.1.

Iz leme 3.2.21 slijedi da postoje tablice $\mathfrak{B}_i = (S^{\mathfrak{B}_i}, M^{\mathfrak{B}_i})$, stanja $s^{\mathfrak{B}_i}$ i nizovi $\Omega^{\mathfrak{B}_i} = ((L_i^{\mathfrak{B}_i}, U_i^{\mathfrak{B}_i}))_{1 \leq i \leq k}$, takvi da $L_k^{\mathfrak{B}_i} = \emptyset$, $0 \leq j \leq n$, takvi da vrijedi $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s)$ ako i samo ako $T \in \mathfrak{D}(\mathfrak{B}_j, \Omega^{\mathfrak{B}_j}, s^{\mathfrak{B}_j})$ za neki $j \leq n$.

Sada nam je cilj svako od pitanja vrijedi li $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$, gdje je Ω duljine k , a $L_k = \emptyset$ svesti na konačno mnogo pitanja vrijedi li $T \in \mathfrak{D}(\mathfrak{A}, \Omega_{k-1}, s_0)$, gdje je $\Omega_{k-1} = ((L_i, U_i))_{1 \leq i \leq k-1}$. Primjenjujući lemu 3.2.22 na naš slučaj dobivamo da ako vrijedi $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$, tada postoji skup $H \subseteq U_k$ takav da za svako stanje $s \in H \cup \{s_0\}$ vrijedi:

$$\forall r[r \in \text{Rn}(\mathfrak{A}, T)] \wedge r(\varepsilon) = s \rightarrow \exists \pi(r|_{\pi} \in [\Omega_{k-1}]) \vee \exists x(\varepsilon < x \wedge r(x) \in H). \quad (3.2)$$

Ukratko ćemo objasniti zašto za naš slučaj vrijedi i obrnuta implikacija. Ako za izvršavanje r , za koje $r(\varepsilon) = s_0$, vrijedi da postoji put π takav da $r|_{\pi} \in [\Omega_{k-1}]$, onda sigurno vrijedi i $r|_{\pi} \in [\Omega]$. No, što je s izvršavanjima za koje ne postoji takav put već vrijedi da postoji čvor $x_1 > \varepsilon$, takav da $r(x_1) = s_1 \in H$?

Uzmimo takvo izvršavanje r , navedeni čvor x_1 i stanje s_1 . Neka je π_1 put u T_{x_1} . Vidimo da ne može vrijediti $r|_{\pi_1} \in [\Omega_{k-1}]$ jer bi tada postojao put π u T takav da $r|_{\pi} \in [\Omega_{k-1}]$. Budući da je skup podskupova od T invarijantan i jer za stanje s_1 vrijedi formula 3.2, dolazimo do zaključka da postoji čvor $x_2 \neq x_1$ takav da $r(x_2) \in H$. Analogno dolazimo do zaključka da postoji beskonačno čvorova x takvih da $r(x) \in H \subset U_k$. Zato vrijedi $\text{In}(r|_{\pi}) \cap U_k \neq \emptyset$. Vidimo da za svaki r i svaki π vrijedi $\text{In}(r|_{\pi}) \cap L_k = \emptyset$ jer je $L_k = \emptyset$ iz čega slijedi $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$. Time smo dokazali da vrijedi i obrnuta implikacija.

Ograničavanjem na skup $S \setminus H$ otklonili bi mogućnost da vrijedi $r(x) \in H$ za neki čvor x , zato slijedi da za izvršavanja tablice $\mathfrak{A}' = \mathfrak{A}|_{(S \setminus H)}$ vrijedi:

$$\forall r'[r' \in \text{Rn}(\mathfrak{A}', T)] \wedge r'(\varepsilon) = s \rightarrow \exists \pi(r'|_{\pi} \in [\Omega_{k-1}]) \text{ ako i samo ako vrijedi 3.2} \quad (3.3)$$

Pitanje vrijedi li 3.3 ekvivalentno je pitanju vrijedi li $T \in \mathfrak{D}(\mathfrak{A}', \Omega_{k-1}, s)$ te smo time uspješno sveli pitanje $T \in \mathfrak{D}(\mathfrak{A}, \Omega, s_0)$ na konačno mnogo pitanja $T \in \mathfrak{D}(\mathfrak{A}', \Omega_{k-1}, s)$, gdje su \mathfrak{A}' ograničenja tablice \mathfrak{A} skupovima oblika $S' = (S \setminus H)$ za skup $H \in P(S)$, to jest $S' \in P(S)$.

Još nam je preostalo pitanje vrijedi li $T \in \mathfrak{D}(\mathfrak{A}, ((\emptyset, U)), s_0)$ za neku tablicu \mathfrak{A} , jednočlan niz $((\emptyset, U))$ i stanje s_0 svesti na odlučiv problem.

Primijetimo da za svako izvršavanje $r \in \text{Rn}(\mathfrak{A}, T)$ i svaki put π u T vrijedi $r|_{\pi} \notin [\emptyset]$. Zato primjenjujući lemu 3.2.22 na ovaj slučaj dobivamo da vrijedi $T \in \mathfrak{D}(\mathfrak{A}, ((\emptyset, U)), s_0)$ ako i samo ako postoji skup $H_0 \subset U$ takav da za svako izvršavanje $r \in \text{Rn}(\mathfrak{A}, T)$, za koje je početno stanje $s \in H \cup \{s_0\}$, postoji čvor $x > \varepsilon$ takav da $r(x) \in H_0$. Po lemi 3.2.23 slijedi da postoji neprazan skup $H_1 = \{s_1, s_2, \dots, s_m\} \subseteq H_0$ i konačna stabla E_i , $1 \leq i \leq m$ takva da za svaki i , $1 \leq i \leq m$, vrijedi da ako je $r \in \text{Rn}(\mathfrak{A}, E_i)$, $r(\varepsilon) = s_i$, tada $r(E_i \setminus \{\varepsilon\}) \cap H_1 \neq \emptyset$.

Pitanje da li za proizvoljan skup $H_1 \subseteq H_0$ i stanje $s \in S$ postoji konačno stablo E takvo da za svako \mathfrak{A} -izvršavanje r na konačnom stablu E , $r(s)$ povlači $r(E \setminus \{\varepsilon\}) \cap H_1 \neq \emptyset$ izrazivo je u WS2S što ga čini odlučivim po [4].

□

Napomena 3.2.28. Neka je $\chi_A : T \rightarrow \{0, 1\}$ karakteristična funkcija skupa $A \subseteq T$. Za svaki $n \in \omega$ nadalje ćemo koristiti oznaku $\Sigma_n := \{0, 1\}^n$. Uvedimo za proizvoljni $n \in \omega$ i skupove $A_1, A_2, \dots, A_n \subseteq T$ oznaku $\tilde{A} := (A_1, A_2, \dots, A_n)$ te promotrimo Σ_n -stablo $(v_{\tilde{A}}, T)$, pri čemu je

$$v_{\tilde{A}}(x) := (\chi_{A_1}(x), \chi_{A_2}(x), \dots, \chi_{A_n}(x)), \quad x \in T.$$

Uočimo da je preslikavanje koje danoj uređenoj n -torki \tilde{A} pridružuje stablo $(v_{\tilde{A}}, T)$ bijekcija između $\mathcal{P}(T)^n$ i $V_\varepsilon^{\Sigma_n} := \{(v, T) \mid v : T \rightarrow \Sigma_n\}$. Označimo to preslikavanje s $\tau : \mathcal{P}^n \rightarrow V_\varepsilon^{\Sigma_n}$.

Intuitivno, preslikavanje τ prima uređenu n -torku \tilde{A} podskupova stabla T i "označava" stablo T tako da oznaka svakog čvora bude niz nula i jedinica koje upućuju na to je li taj čvor član pojedinog skupa iz \tilde{A} . Jasno je da je to bijekcija jer je svaki niz podskupova od T jedinstveno određen označenim stablom gdje oznaka čvora određuje članstvo tog čvora u pojedinom skupu.

U ostatku ovog potpoglavlja promatrat ćemo monadsku teoriju drugog reda S2S. Za formule logike drugog reda koristit ćemo oznake oblika $F(A_1, A_2, \dots, A_n)$ što znači da se u formuli pojavljuju slobodne skupovne varijable A_1, A_2, \dots, A_n . Konkretno skupove označavamo isto kao i skupovne varijable, a slobodne individualne varijable x_i , $i \in \omega$ zamjenjujemo singletonima $\{x_i\}$, $i \in \omega$ kako bi sve slobodne varijable bile skupovne. Shodno tomu, relacijske i funkcijske simbole koji se javljaju uz slobodne individualne varijable oblika npr. $R(x, y)$ zamjenjujemo formulama oblika $\exists x \exists y (x \in X \wedge y \in Y \wedge R(x, y))$ gdje su x i y sada vezane, a X i Y slobodne varijable za singletone koji sadrže samo x odnosno y .

Teorem 3.2.29. Neka je $n \in \omega$. Postoji Turingov odlučitelj koji na traku kao ulaz prima proizvoljnu formulu drugog reda $F(A_1, A_2, \dots, A_n) \in S2S$ te ulazi u stanje q_\checkmark ako je to ispravno napisana formula, pri čemu na traci kao izlaz ostavlja zapisan Σ_n -automat \mathfrak{A}_F tako da vrijedi

$$T(\mathfrak{A}_F) \cap V_\varepsilon^{\Sigma_n} = \tau(\{(A_1, A_2, \dots, A_n) \in \mathcal{P}(T)^n \mid \mathfrak{A}_2 \models F(A_1, A_2, \dots, A_n)\}). \quad (3.4)$$

Za svaki automat koji zadovoljava jednadžbu 3.4 kažemo da **reprezentira** formulu $F(A_1, \dots, A_n)$.

Desna strana 3.4 zapravo je slika skupa po funkciji τ . Teorem kaže da za svaku formulu S2S s n skupovnih varijabli postoji automat koji prepoznaje sva ona Σ_n -stabla t za koja je

ta formula istinita uz valuaciju koja i -toj skupovnoj varijabli pridružuje i -tu komponentu uređene n -torke $\tau^{-1}(t)$, te da je problem pronalaska tog automata odlučiv.

Teorem 3.2.29 dokazuje se svođenjem proizvoljne formule na preneksnu normalnu formu drugog reda, gdje "vanjski" kvantifikatori idu po skupovnim varijablama, a "unutarnji" po individualnima. Međurezultat o postojanju ovakve normalne forme za svaku formulu drugog reda ključan je za konačni dokaz Rabinovog teorema. Dokaz teorema 3.2.29 može se pronaći u [7] kao teorema 1.7.

Teorem 3.2.30 (Rabin). *Teorija drugog reda $S2S$ je odlučiva.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da je zadana formula iz $S2S$ oblika $G \equiv \exists A_1 \exists A_2 \dots \exists A_n F(A_1, A_2, \dots, A_n)$. Naime, ako je neka skupovna varijabla A pod univerzalnim kvantifikatorom u preneksnoj normalnoj formi, jednostavno ga možemo zamijeniti egzistencijalnim, a skup A "idejno" zamijenimo njegovim komplementom, to jest sve potformule oblika $x \in A$ zamijenimo s $x \notin A$, i obratno. S obzirom na to da je $S2S$ **monadska** logika drugog reda, ovo su jedine potformule u kakvima se skupovna varijabla A može pojaviti.

Ovakva će zamjena potformulu pretvoriti u njenu negaciju. Tu negaciju primjenom De Morganovih pravila možemo izlučiti ispred idućeg kvantifikatora te ako je on sada univerzalni ponovno primijenimo isti postupak. Ako na kraju pretvaranja svih kvantifikatora u egzistencijalne i kraćenja dvostrukih negacija na početku formule ostane negacija, nju možemo zanemariti jer je pitanje odlučivosti bilo koje formule ekvivalentno odlučivosti njene negacije.

Neka je \mathfrak{A}_F neki automat koji reprezentira formulu $F(A_1, A_2, \dots, A_n)$. Sada iz 3.4 slijedi da je $\mathfrak{R}_2 \models \exists A_1 \exists A_2 \dots \exists A_n F(A_1, A_2, \dots, A_n)$ ako i samo ako je $T(\mathfrak{A}_F) \neq \emptyset$. Međutim, prema teoremu 3.2.27 postoji Turingov odlučitelj koji odlučuje vrijedi li $T(\mathfrak{A}_F) \neq \emptyset$ ili ne. Dakle, on isto tako odlučuje vrijedi li $\mathfrak{R}_2 \models \exists A_1 \exists A_2 \dots \exists A_n F(A_1, A_2, \dots, A_n) \equiv G$. \square

Za dokazati varijantu teorema S_nS za neki drugi $n \in \omega$ dovoljno je umjesto beskonačnih **binarnih** stabala promatrati beskonačna " n -mjesna" stabla te sve definicije i tvrdnje iz ovog dijela prilagoditi njima. Slučaj $S_\omega S$ dokazuje se uspostavljanjem ekvivalencije između čvorova beskonačnog " ω -mjesnog" stabla i podstabala beskonačnog binarnog stabla, uz očuvanje relacije roditelj-dijete. Cjelovit dokaz dan je u točki 1.9 [7] kao teorem 1.12.

Teorem 3.2.31. *Logika KvB je odlučiva.*

Dokaz. Ovdje dajemo skicu dokaza. Prisjetimo se da je logika KvB definirana nad općim okvirom $\mathfrak{F} = (J, R, A)$, gdje je redom:

- $J = \mathbb{N} \cup \{\omega, \omega + 1\}$,
- $xRy : \Leftrightarrow y < x \neq \omega + 1$ ili $x = \omega + 1$ i $y = \omega$,
- $A = \{X \subseteq J \mid X \text{ konačan i } \omega \notin X \text{ ili } X \text{ kofinitan i } \omega \in X\}$ je familija svih dopustivih skupova.

Cilj ovog dokaza je svesti problem ispunjivosti modalne formule na općem okviru \mathfrak{F} na problem ispunjivosti određene formule monadske logike drugog reda $S2S$.

Za dokaz su važne sljedeće dvije tvrdnje:

1. Postoji izomorfizam koji preslika opći okvir \mathfrak{F} u podstrukturu strukture funkcija 2 sljedbenika $\mathfrak{R}_2 = (T_2, r_0, r_2, \leq, \leq)$. Označimo tu izomorfnu sliku s $\mathfrak{F}' = (J', R', A')$.
2. Navedena izomorfna slika je definabilna u jeziku logike $S2S$, odnosno postoje formule monadske logike drugog reda $\tilde{J}(x)$, $\tilde{R}(x, y)$ i $\tilde{A}(P)$ takve da:

$$J' = \{t \in T_2 \mid \mathfrak{R}_2 \models \tilde{J}(x)[t]\},$$

$$R' = \{(t_1, t_2) \in T_2 \times T_2 \mid \mathfrak{R}_2 \models \tilde{R}(x, y)[t_1, t_2]\},$$

$$A' = \{U \subseteq T_2 \mid \mathfrak{R}_2 \models \tilde{A}(P)[U]\},$$

pri čemu $\tilde{J}(x)[t]$ znači da uvrštavamo riječ $t \in \{0, 1\}^*$ u slobodnu varijablu x formule \tilde{J} , značenje $\tilde{R}(x, y)[t_1, t_2]$ je da uvrštavamo t_1 i t_2 redom u slobodne varijable x i y formule \tilde{R} , a $\tilde{A}(P)[U]$ da uvrštavamo skup U u slobodnu predikatnu varijablu P formule \tilde{A} .

Dokaz ovih tvrdnji, koji se bazira na pronalasku navedenog izomornog preslikavanja, detaljno je raspisan u [1] kao teorem o odlučivosti logike KvB .

Preostalo je definirati preslikavanje modalne formule u formulu monadske logike drugog reda. U tu svrhu ćemo prvo definirati preslikavanje T_x koje preslika modalnu formulu u formulu logike drugog reda, a zatim ćemo iskoristiti funkciju T_x za definiciju preslikavanja modalne formule u formulu monadske logike drugog reda.

Preslikavanje T_x definiramo ovako:

$$\begin{aligned} T_x(p) &= Px, \\ T_x(\neg \varphi) &= \neg T_x(\varphi), \\ T_x(\varphi \vee \psi) &= T_x(\varphi) \vee T_x(\psi), \\ T_x(\Box \varphi) &= \forall y(xRy \rightarrow T_y(\varphi)). \end{aligned}$$

Za svaku modalnu formulu φ sastavljenu od propozicionalnih varijabli p_1, p_2, \dots, p_n , svaku valuaciju V i svaki svijet $w \in J$ vrijedi sljedeća ekvivalencija:

$$(\mathfrak{S}, V) \models \varphi \text{ ako i samo ako } \mathfrak{R}_2 \models T_x(\varphi)[w, V(p_1), V(p_2), \dots, V(p_n)],$$

gdje $T_x(\varphi)[w, V(p_1), V(p_2), \dots, V(p_n)]$ znači da u formulu logike drugog reda $T_x(\varphi)$ uvrstimo svijet w u slobodnu varijablu x , a skupove svjetova $V(p_i)$ u slobodne predikatne varijable P_i za svaki i , $1 \leq i \leq n$.

Za svaku modalnu formulu φ sastavljenu od propozicionalnih varijabli p_1, p_2, \dots, p_n definiramo formulu monadske logike drugog reda $Sat - KvB(\varphi)$ na sljedeći način:

$$\exists P_1 \dots \exists P_n \exists x (\tilde{A}(P_1) \wedge \dots \wedge \tilde{A}(P_n) \wedge \tilde{J}(x) \wedge T_x(\varphi)).$$

Slijedi da je modalna formula φ ispunjiva na okviru \mathfrak{S} ako i samo ako $\mathfrak{R}_2 \models Sat - KvB(\varphi)$. Time smo uspješno sveli problem odlučivosti logike KvB na problem odlučivosti teorije $S2S$. Budući da je po teoremu 3.2.30 teorija $S2S$ odlučiva zaključujemo da je i logika KvB odlučiva. \square

3.3 Dokaz odlučivosti logike KvB metodom kvazimodela

U ovom potpoglavlju dokazujemo odlučivost logike KvB pomoću metode **kvazimodela**. Kvazimodeli su strukture vrlo slične modelima koje smo do sada promatrali. No, kvazimodeli umjesto valuacije imaju tzv. **opisnik**.

Naime, neka je $\mathfrak{S} = (J, R, A)$ opći okvir nad kojim je definirana logika KvB u definiciji 1.3.6. Primijetimo da uklanjanjem točke $\omega + 1$ iz općeg okvira \mathfrak{S} dobivamo tranzitivnu strukturu te na njoj možemo primijeniti metodu filtracije kako bi nova struktura opet bila tranzitivna.

Definicija 3.3.1. *Kažemo da je skup formula Γ zatvoren ako je zatvoren na potformule i jednostruke negacije, odnosno za svaku formulu $\varphi \in \Gamma$ koja nije oblika $\varphi \equiv \neg\psi$ vrijedi $\neg\varphi \in \Gamma$.*

Zatvarač skupa formula Γ , u oznaci $Cl(\Gamma)$, je presjek svih zatvorenih skupova formula koji sadrže Γ .

Definicija 3.3.2. Neka je Γ skup formula zatvoren na potformule. **Hintikkin skup** H nad skupom Γ je maksimalan podskup od skupa Γ koji zadovoljava uvjete:

1. $\perp \notin H$;
2. ako je $\neg\varphi \in \Gamma$, onda je $\neg\varphi \in H$ ako i samo ako $\varphi \notin H$
3. ako je $\varphi \wedge \psi \in \Gamma$, onda je $\varphi \wedge \psi \in H$ ako i samo ako je $\varphi \in H$ i $\psi \in H$.

Napomena 3.3.3. Uočimo da za Hintikkine skupove vrijedi analogon 3. uvjeta za ostale Booleove veznike jer se svi oni mogu izraziti pomoću negacije i konjunkcije.

Iako bi se iz 1. i 2. uvjeta dalo naslutiti da Hintikkini skupovi moraju biti konzistentni, zapravo je moguće pronaći primjer inkonzistentnih Hintikkinih skupova.

Primjer 3.3.4. Skup formula $\{\Box p \wedge \Box q, \Box p, \Box q, p, q\}$ je zatvoren na potformule, a istodobno i konzistentan Hintikkin skup nad samim sobom. Primijetimo da je to ujedno i jedini Hintikkin skup nad njim te da ista stvar vrijedi i za sve ostale skupove koji ne sadrže nijednu negaciju ni \perp .

Skup formula $S = \{\Box(p \wedge q), p \wedge q, \neg\Box p, \neg\Box q, \Box p, \Box q, p, q\}$ je zatvoren na potformule, a njegov podskup $\{\Box(p \wedge q), p \wedge q, \neg\Box p, \neg\Box q, p, q\}$ je Hintikkin skup nad skupom S koji nije konzistentan. Naime, uzmimo proizvoljan model $\mathfrak{M} = (W, R, V)$ i svijet $w \in W$ takav da $w \Vdash \Box(p \wedge q)$. Za svakog sljedbenika $v \in W$ svijeta w vrijedi $v \Vdash p \wedge q$ što povlači $v \Vdash p$ i $v \Vdash q$. Budući da navedene tvrdnje vrijede za svakog sljedbenika svijeta w slijedi $w \Vdash \Box p$ i $w \Vdash \Box q$. Zaključujemo da iz $\Box(p \wedge q)$ možemo izvesti $\Box p$ i $\Box q$, stoga skup formula S nije konzistentan.

Definicija 3.3.5. Neka je φ modalna formula. **KvB kvazimodel** za φ je par $\mathfrak{Q} = (\mathfrak{F}, \lambda)$, gdje je $\mathfrak{F} = (Q, S)$ konačan okvir koji sadrži dva istaknuta svijeta c i ∞ te zadovoljava:

- (F1) na skupu $Q \setminus \{\infty\}$ relacija S je tranzitivna i linearna¹;
- (F2) $cS w$ ako i samo ako je $w \neq \infty$;
- (F3) wSc ako i samo ako je $w = c$ ili $w = \infty$;
- (F4) $\infty S w$ ako i samo ako je $w = c$;
- (F5) ne postoji $w \in Q$ takav da je $wS \infty$,

¹Za sve x, y vrijedi barem jedno od sljedećeg: xSy , ySx , $x = y$

a $\lambda : Q \rightarrow \mathcal{P}(Cl(\varphi))$ je funkcija koju zovemo **opisnik** te zadovoljava:

- (L0) postoji $w \in Q$ takav da je $\varphi \in \lambda(w)$;
- (L1) za sve $w \in Q$, $\lambda(w)$ je Hintikkin skup;
- (L2) za sve $\diamond\psi \in Cl(\varphi)$ je $\diamond\psi \in \lambda(w)$ ako i samo ako postoji $v \in Q$ takav da je wSv i $\psi \in \lambda(v)$;
- (L3) ako je $\diamond\psi \in \lambda(w)$, onda postoji $v \in Q$ takav da je $\psi \in \lambda(v)$ i wSv , ali nije vSw .

Prije nego što dokažemo lemu iz koje će direktno slijediti odlučivost logike **KvB**, dokažat ćemo jedan pomoćni rezultat u vezi tranzitivnih filtracija.

Propozicija 3.3.6. *Neka je Γ skup zatvoren na potformule i neka je $\mathfrak{M} = (W, R, V)$ model na kojem je relacija R tranzitivna. Neka su kvocijenti skup \tilde{W} i valuacija \tilde{V} definirani kao kod filtracije modela \mathfrak{M} u odnosu na skup Γ te neka je relacija \tilde{R} definirana kao:*

$$[u]\tilde{R}[w] : \Leftrightarrow \text{za svaku formulu } \psi \text{ takvu da je } \diamond\psi \in \Gamma \text{ i } v \Vdash \psi \vee \diamond\psi \text{ vrijedi } u \Vdash \diamond\psi. \quad (3.5)$$

Tada je $\tilde{\mathfrak{M}} := (\tilde{W}, \tilde{R}, \tilde{V})$ doista filtracija te je relacija \tilde{R} tranzitivna na \tilde{W} .

Dokaz. Dokažimo da je $\tilde{\mathfrak{M}}$ uistinu filtracija. U tu svrhu provjeravamo ispunjenost sljedećih uvjeta na svim svjetovima $w, v \in W$:

(MIN) ako je wRv , onda je $[w]\tilde{R}[v]$;

(MAX) ako je $[w]\tilde{R}[v]$, onda za svaku formulu $\diamond\psi \in \Gamma$ koja zadovoljava $\mathfrak{M}, v \Vdash \psi$ vrijedi $\mathfrak{M}, w \Vdash \diamond\psi$.

Neka je wRv te uzmimo formulu ψ takvu da je $\diamond\psi \in \Gamma$ i $v \Vdash \psi \vee \diamond\psi$. Iz potonjeg slijedi da je $v \Vdash \psi$ ili $v \Vdash \diamond\psi$. U prvom slučaju odmah imamo $u \Vdash \diamond\psi$ zbog wRv , a u drugom dobivamo da postoji $u \in W$ takav da je vRu i $u \Vdash \psi$. No sad zbog tranzitivnosti R vrijedi wRu te stoga $w \Vdash \diamond\psi$. Dakle, u oba slučaja prema 3.5 vrijedi $[w]\tilde{R}[v]$, stoga je uvjet (MIN) dokazan.

Neka je sada $[w]\tilde{R}[v]$ i uzmimo formulu $\diamond\psi \in \Gamma$ takvu da vrijedi $\mathfrak{M}, v \Vdash \psi$. Iz potonjeg naravno slijedi i $v \Vdash \psi \vee \diamond\psi$, te sad iz 3.5 imamo $\mathfrak{M}, w \Vdash \diamond\psi$, što dokazuje svojstvo (MAX).

Iz svojstava (MIN) i (MAX) slijedi da je uistinu riječ o filtraciji. Dokažimo sada da je \tilde{R} tranzitivna na \tilde{W} . Neka je $[u]\tilde{R}[v]\tilde{R}[w]$. Uzmimo proizvoljnu formulu $\diamond\psi \in \Gamma$ takvu da $w \Vdash \psi \vee \diamond\psi$. Iz toga i iz $[v]\tilde{R}[w]$ po 3.5 slijedi $v \Vdash \diamond\psi$, pa vrijedi i $v \Vdash \psi \vee \diamond\psi$. Zbog toga i $[u]\tilde{R}[v]$ opet po 3.5 imamo $u \Vdash \diamond\psi$, iz čega slijedi $[u]\tilde{R}[w]$, dakle relacija \tilde{R} je tranzitivna. \square

Lema 3.3.7. *Neka je $\mathfrak{S} = (J, R, A)$ opći okvir nad kojim je definirana logika **KvB**. Modalna formula φ je ispunjiva na općem okviru \mathfrak{S} ako i samo ako postoji kvazimodel za formulu φ veličine najviše $2^n + 1$, gdje je n broj elemenata u skupu $Cl(\varphi)$.*

Dokaz. Ideja dokaza je sljedeća: uklonimo svijet $\omega + 1$ iz nosača, napravimo filtraciju ostatka u odnosu na neki skup zatvoren na potformule, te opet dodamo svijet $\omega + 1$ i po potrebi proširimo relaciju dostiživosti. Rezultat toga neće nužno biti filtracija, ali svejedno možemo iz njega dobiti kvazimodel.

Neka je φ jedna proizvoljna formula koja je ispunjiva na modelu čiji je okvir \mathfrak{S} . Tada postoji svijet $w \in J$ i dopustiva valuacija V takva da vrijedi $(\mathfrak{S}, V), w \Vdash \varphi$. Prisjetimo se, valuaciju V nazivamo dopustivom ako za svaku propozicionalnu varijablu p vrijedi $V(p) \in A$.

Neka je skup $J_0 := J \setminus \{\omega + 1\}$, relacija $R_0 := R \cap J_0 \times J_0$ (primijetimo da je relacija R_0 tranzitivna) te $\mathfrak{S}_0 := (J_0, R_0, V|_{J_0})$. Uzmimo filtraciju $\tilde{\mathfrak{S}} := (\tilde{J}, \tilde{R}, \tilde{V})$ modela \mathfrak{S}_0 u odnosu na skup $Cl(\varphi)$. Nosač \tilde{J} i valuaciju \tilde{V} definiramo standardno, a relaciju \tilde{R} isto kao u 3.5. Iz propozicije 3.3.6 znamo da je relacija \tilde{R} tranzitivna.

Sada definiramo kvazimodel (Q, S, λ) tako da je $Q = \tilde{J}_0 \cup \{\omega + 1\}$, pri čemu je $c = [\omega]$ i $\infty = \omega + 1$, $S = \tilde{R} \cup \{(\omega + 1, [\omega])\}$, te opisnik λ jednostavno svakom svijetu $w \in Q$ pridružuje skup svih formula koje su istinite na w . Iz propozicije 3.3.6, svojstva (MIN), tranzitivnosti relacije \tilde{R} i definicije kvazimodela trivijalno slijede sva svojstva iz definicije 3.3.5 osim **(L3)** i toga da je $c\tilde{R}c$, stoga njih dokazujemo u nastavku.

Da bismo dokazali da je $c\tilde{R}c$, uzmimo neku formulu ψ takvu da je $\diamond\psi \in Cl(\varphi)$ i $c \Vdash \psi \vee \diamond\psi$. Ako vrijedi $c \Vdash \diamond\psi$ tada ne trebamo ništa više dokazivati. Promotrimo slučaj kada vrijedi $c \Vdash \psi$. Uočimo da je svijet c kofinitan kao konačan presjek kofinitnih skupova, zbog dopustivosti valuacije V . To znači da ima barem dva elementa: ω i neki $n \in \omega$. Tada imamo $\omega R n$ i $n \Vdash \psi$, dakle $\omega \Vdash \diamond\psi$, te je stoga i $c \Vdash \diamond\psi$, što dokazuje tvrdnju $c\tilde{R}c$.

Preostaje dokazati svojstvo **(L3)**. Neka je $\diamond\psi \in \lambda(u)$, odnosno $u \Vdash \diamond\psi$. Ako je $u = \infty$, onda vrijedi $c \Vdash \psi$, odnosno $\psi \in \lambda(c)$ te po definiciji relacije S imamo $\infty S c$, ali ne i $c S \infty$. Ako je $u \neq \infty$, onda mora postojati najmanji element $m \in u$ za koji vrijedi $m \Vdash \diamond\psi$. Dakle, postoji svijet $k < m$ takav da $k \Vdash \psi$, ali taj k ne može biti iz skupa u jer je on manji od m . Stoga vrijedi $[k] \neq u$ i $u\tilde{R}[k]$, ali ne vrijedi $[k]\tilde{R}u$, dakle uvjet **(L3)** je opet zadovoljen za skup $[k]$.

Primijetimo da je funkcija $\lambda|_{\tilde{\mathfrak{S}}_0}$ injekcija u skup $\mathcal{P}(Cl(\varphi))$ čija je kardinalnost 2^n te da skup Q ima jedan element više od skupa $\tilde{\mathfrak{S}}_0$. Time direktno slijedi tvrdnja leme o gornjoj međi veličine kvazimodela.

Dokažimo sada obratnu implikaciju iz iskaza leme. Neka je (Q, S, λ) neki kvazimodel na kojem je ispunjiva formula φ te neka je $Q_0 := Q \setminus \{\infty\}$.

Definirajmo binarnu relaciju \sim na skupu Q_0 ovako:

$$w \sim v \quad :\Leftrightarrow \quad w = v \text{ ili } (wSv \text{ i } vSw), \quad (3.6)$$

Lako je provjeriti da je \sim jedna relacija ekvivalencije. Zatim, definiramo binarnu relaciju $>$ nad kvocijntnim skupom Q_0/\sim ovako:

$$[w] > [v] \quad :\Leftrightarrow \quad wSv \text{ i nije } vSw. \quad (3.7)$$

Iz svojstva **(F1)** slijedi da je relacija $>$ strogi totalni uređaj. Neka su svi elementi skupa Q_0 poredani u niz q_0, q_1, \dots, q_N tako da prvo dolaze elementi iz najmanje klase ekvivalencije, onda iz druge najmanje, i tako sve do najveće u odnosu na uređaj $>$. Sada definiramo funkciju $f : J \rightarrow Q$ na sljedeći način:

$$f(w) := \begin{cases} q_w, & w \leq N \\ c, & w > N \text{ i } w < \omega + 1 \\ \infty, & w = \omega + 1 \end{cases}$$

Tvrdimo da za sve svjetove w i v takve da je wRv , vrijedi $f(w)Sf(v)$. U tu svrhu prvo promotrimo slučaj $w = \omega + 1$. Iz wRv slijedi $v = \omega$, dakle treba dokazati ∞Sc , a to slijedi direktno iz **(F4)**. Neka je sad $w = \omega$. Iz wRv slijedi da je $v \in \omega$, dakle treba dokazati $\omegaSn, n \in \omega$, a to slijedi iz **(F2)**. Još je ostao slučaj kad je $w \in \omega$. Tada je i $v \in \omega$ te je $v < w$. Ako je $N < w$, onda je $f(w) = c$, te tražena tvrdnja $cSn, n \in \omega$ ili cSc slijedi iz **(F2)**, a ako je $w \leq N$, onda treba dokazati q_wSq_v . Iz $v < w$ i zadanog poretka elemenata niza q dobivamo $[w] \geq [v]$, dakle $[w] > [v]$ ili $q_w \sim q_v$, ali kako je $v \neq w$, u oba slučaja vrijedi q_wSq_v . Time smo dokazali da je funkcija f homomorfizam koji preslikava opći okvir (J, R) u strukturu (Q, S) .

Promotrimo valuaciju na (J, R) definiranu kao $V(p) := \{w \in J \mid p \in \lambda(f(w))\}$. Ona je dopustiva na općem okviru \mathfrak{F} jer ako je $\omega \in V(p)$, onda je $n \in V(p)$ za sve $n > N$ zbog $f(n) = f(\omega)$, dakle $V(p)$ je kofinitan. Sasvim analogno se vidi da vrijedi i obrat.

Tvrdimo da za svaku formulu $\psi \in Cl(\varphi)$ i svaki svijet $w \in J$ vrijedi sljedeća ekvivalencija:

$$(\mathfrak{F}, V), w \Vdash \psi \text{ ako i samo ako } \psi \in \lambda(f(w))$$

Navedenu tvrdnju dokazujemo indukcijom po složenosti formule ψ . Baza indukcije slijedi direktno iz definicije valuacije V , dok u koraku indukcije slučajevi s Booleovim veznicima slijede trivijalno iz toga da je $\lambda(f(w))$ Hintikkin skup. Promotrimo još slučaj kada je $\psi \equiv \diamond\chi$ za neku formulu $\chi \in Cl(\varphi)$. Pretpostavimo prvo da vrijedi $(\mathfrak{F}, V), w \Vdash \diamond\chi$. Tada postoji svijet $v \in J$ takav da je wRv i $v \Vdash \chi$. Kako je funkcija f homomorfizam, imamo $f(w)Sf(v)$, dok je po pretpostavci indukcije $\chi \in \lambda(f(w))$. Iz ovoga i **(L2)** slijedi da vrijedi

$\diamond\chi \in \lambda(f(w))$. Dokažimo sada obratnu implikaciju. U tu svrhu pretpostavimo da vrijedi $\diamond\chi \in \lambda(f(w))$ za neki $w \in J$. Trebamo dokazati da vrijedi $(\mathfrak{J}, V), w \Vdash \diamond\chi$. Ako je $w = \omega + 1$, onda je $f(w) = \infty$. Tada iz **(F4)** i **(L2)** slijedi $\chi \in \lambda(c)$. Iz $c = f(\omega)$ i pretpostavke indukcije sada imamo $\omega \Vdash \chi$, a onda i $\omega + 1 \Vdash \diamond\chi$. Ako je $w \neq \omega + 1$, onda prema **(L3)** postoji svijet $q \in Q$ takav da vrijedi $\chi \in \lambda(q)$ i $f(w)S q$, a ne vrijedi $qS f(w)$. Iz **(F5)** i $f(w)S q$ slijedi da $q \neq \infty$. To znači da za $v \in f^{-1}(q)$ vrijedi $v \neq \omega + 1$. Primijetimo da ne vrijedi vRw , jer bi inače vrijedilo $f(w) = qS f(w)$. Zatim, ne vrijedi $w = v$, jer tada ne bismo mogli imati $f(v)S f(w)$ i ne $f(w)S f(v)$. Budući da je relacija R linearna na skupu $J \setminus \{\omega + 1\}$ tada vrijedi wRv . Po pretpostavci indukcije imamo $v \Vdash \chi$, dakle opet dobivamo $w \Vdash \diamond\chi$.

Sada iz upravo dokazane tvrdnje i svojstva **(L0)** dobivamo da postoji svijet $w \in J$ takav da $(\mathfrak{J}, V), w \Vdash \psi$, što smo i trebali dokazati. \square

Teorem 3.3.8. *Logika **KvB** je odlučiva.*

Dokaz. Neka je $\mathfrak{J} = (J, R, A)$ opći okvir nad kojim je definirana logika **KvB**, to jest vrijedi:

- $J = \mathbb{N} \cup \{\omega, \omega + 1\}$,
- $xRy : \Leftrightarrow y < x \neq \omega + 1$ ili $x = \omega + 1$ i $y = \omega$,
- $A = \{X \subseteq J \mid X \text{ konačan i } \omega \notin X \text{ ili } X \text{ kofinitan i } \omega \in X\}$ je familija svih dopustivih skupova.

Neka je zadana formula φ za koju treba odrediti postoje li svijet $w \in J$ i dopustiva valuacija V takva da je $(\mathfrak{J}, V), w \Vdash \varphi$. Prema lemi 3.3.7 to pitanje ekvivalentno je pitanju postojanja kvazimodela za formulu φ veličine najviše $2^{Cl(\varphi)} + 1$.

Konstruirajmo Turingov enumerator koji radi sljedeće: za svaki prirodni broj n , počevši od $n = 1$ i inkrementirajući n za 1 nakon svakog koraka, u pojedinom koraku pobrojavamo sve uređene trojke (Q, S, λ) takve da je $|Q| = n$, $S \subseteq Q \times Q$ i $\lambda : Q \rightarrow \mathcal{P}(Cl(\varphi))$ kojih ima konačno mnogo. S obzirom na to da vrijednosti samih elemenata iz Q nisu bitne, možemo uzeti, primjerice, $Q = \{1, 2, \dots, n\}$.

Sada za provjeru ispunjivosti formule φ pokrećemo zadani enumerator i u svakom koraku provjeravamo je li generirana uređena trojka kvazimodel za φ . Ako naidemo na neku koja je, onda je formula ispunjiva, a ako dostignemo $n = 2^{Cl(\varphi)} + 1$ bez da smo našli ijednu takvu formulu, onda nije ispunjiva. Automat koji obavlja opisanu provjeru je Turingov odlučitelj jer se zaustavlja i u slučaju potvrdnog i negativnog odgovora. Dakle, problem ispunjivosti formula logike **KvB** je odlučiv, stoga je logika **KvB** odlučiva. \square

Poglavlje 4

Metoda mozaika

Glavni je cilj ovog poglavlja upoznati se s metodom mozaika za dokazivanje odlučivosti modalne logike. U tu svrhu ćemo dokazati odlučivost logike K_tN pomoću te metode. Prvo ćemo definirati osnovni temporalni jezik, nakon čega dokazujemo odlučivost logike K_tN .

4.1 Osnovni temporalni jezik

U ovom potpoglavlju definirat ćemo sintaksu i semantiku osnovnog temporalnog jezika te istinitost formule u svijetu modela.

Definicija 4.1.1. *Alfabet osnovnog temporalnog jezika je unija sljedećih skupova:*

- skup prebrojivo mnogo propozicionalnih varijabli $Prop = \{p, q, r, \dots\}$;
- skup logičkih veznika, modalnih operatora i logičkih konstanti $\{\neg, \vee, \langle F \rangle, \langle P \rangle, \perp\}$;
- skup pomoćnih simbola $\{(\, , \,)\}$ (zagrada).

Formulu osnovnog temporalnog jezika definiramo analogno kao formulu osnovnog modalnog jezika. Također, složenost temporalne formule, analogno složenosti modalne formule, definira se kao broj veznika i modalnih operatora u formuli.

Primijetimo da se alfabet osnovnog temporalnog jezika razlikuje od alfabeta osnovnog modalnog jezika samo u modalnim operatorima. Umjesto jednog modalnog operatora \Box imamo dva modalna operatora $\langle F \rangle$ i $\langle P \rangle$. Umjesto $\langle F \rangle$ i $\langle P \rangle$ često pišemo redom F i P .

Oznake F i P dolaze od engleskih riječi "future" (budućnost) i "past" (prošlost). Naime, formulu $F\varphi$ shvaćamo kao "formula φ će biti istinita u nekom trenutku u budućnosti", a formulu $P\varphi$ kao "formula φ je bila istinita u nekom trenutku u prošlosti".

U nastavku definiramo nekoliko pojmova semantike temporalne logike.

Definicija 4.1.2. *Dvosmjerni okvir je uređena trojka $\mathfrak{F} = (W, R_P, R_F)$, gdje je W nosač, a R_P i R_F binarne relacije takve da $R_P = \{(v, w) \mid wR_Fv\}$.*

Kažemo da je relacija R_P inverzna relacija relacije R_F .

Definicija 4.1.3. *Dvosmjerni model je uređen par $\mathfrak{M} = (\mathfrak{F}, V)$, gdje je $\mathfrak{F} = (W, R_P, R_F)$ dvosmjerni okvir te $V: Prop \rightarrow \mathcal{P}(W)$ funkcija koju nazivamo valuacija.*

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

Sljedeće definicije istinitosti formula dobivenih primjenom modalnih operatora budućnosti i prošlosti.

Definicija 4.1.4. *Istinitost formule u svijetu modela definira se analogno osnovnom modalnom jeziku. Navodimo samo slučajeve modalnih operatora. Neka je $\mathfrak{M} = (W, R_P, R_F, V)$ model. Tada za svaki svijet $w \in W$ vrijedi:*

$\mathfrak{M}, w \models F\varphi$ ako i samo ako postoji svijet $v \in W$ takav da wR_Fv i vrijedi $\mathfrak{M}, v \models \varphi$.

$\mathfrak{M}, w \models P\varphi$ ako i samo ako postoji svijet $v \in W$ takav da wR_Pv i vrijedi $\mathfrak{M}, v \models \varphi$.

Primijetimo da, budući da je relacija R_P uvijek inverzna relacija relacije R_F , možemo izostaviti spominjanje relacije R_P . Štoviše, možemo definirati istinitost formule dobivene primjenom modalnog operatora P bez upotrebe relacije R_P na sljedeći način:

$\mathfrak{M}, w \models P\varphi$ ako i samo ako postoji svijet $v \in W$ takav da vR_Fw i vrijedi $\mathfrak{M}, v \models \varphi$.

Dajemo primjer modela i formula osnovnog temporalnog jezika koje su ispunjive na tom modelu. Tim primjerom pokazat ćemo zašto navedeni jezik zovemo temporalnim.

Primjer 4.1.5. *Pretpostavimo da želimo opisati odnose godina s nekim događajima. Primjerice, neka je $\mathfrak{M} = (W, <, V)$ model, gdje je nosač W skup godina od 1900. do danas (2023.), relacija $<$ je standardni uređaj na skupu prirodnih brojeva, a skup $V(p)$ tumačimo kao skup svih godina za koje vrijedi da je događaj p istinit.*

Nikola Tesla rođen je 1856. godine. Ako označimo događaj njegovog rođenja s propozicionalnom varijablom r , vidimo da vrijedi $\mathfrak{M}, 1856. \models r$. Zatim, za sve godine $g \in W$ takve da $g < 1856$ vrijedi: $\mathfrak{M}, g \models Fr$. Primjerice, za 1850. godinu vrijedi $\mathfrak{M}, 1850 \models Fr$, što možemo pročitati kao "za 1850. godinu vrijedi da će se Nikola Tesla roditi u nekoj budućoj godini". U drugu ruku za sve godine $g \in W$ takve da $g > 1856$ vrijedi $\mathfrak{M}, g \models Pr$. To uključuje i današnju 2023. godinu, tj. posebno vrijedi $\mathfrak{M}, 2023 \models Pr$. To možemo pročitati i kao: "Nikola Tesla se rodio u nekoj prošloj godini u odnosu na 2023. godinu".

Naš drugi primjer vezan je uz otkriće interneta 1983. godine. Neka propozicionalna varijabla p predstavlja tvrdnju "postoji internet". Tada za sve godine $g \geq 1983$ vrijedi $\mathfrak{M}, g \models p$. Primijetimo da za 1982. godinu vrijedi $\mathfrak{M}, 1982 \models \neg F\neg p$. To možemo pročitati i ovako: "Za 1982. godinu vrijedi da ne postoji buduća godina u kojoj neće postojati internet" odnosno u afirmativnom obliku: "Svake godine poslije 1982. godine postojat će internet".

Pokratu za $\neg F\neg$ označavamo s G i čitamo "uvijek će biti slučaj da vrijedi" (eng. "it is always *Going* to be the case").

Pokratu za $\neg P\neg$ označavamo s H te čitamo "uvijek je bio slučaj da vrijedi" (eng. "it always *Has* been the case"). Primjer upotrebe operatora H je $\mathfrak{M}, 1983. \models H\neg p$. Navedenu tvrdnju čitamo: "za sve godine prije 1983. vrijedi da nije postojao internet".

4.2 Odlučivost logike K_tN

U ovom potpoglavlju dokazat ćemo odlučivost logike K_tN metodom mozaika.

Potpoglavlje započinjemo definicijom temporalne logike K_tN . Definiramo i sljedeće pojmove: pločica, put pločica, zasićen skup pločica za formulu, povijest formule te proširenje povijesti. Nakon svih potrebnih definicija, dokazat ćemo dvije leme iz kojih će slijediti odlučivost logike K_tN .

Definicija 4.2.1. Logika K_tN je skup formula osnovnog temporalnog jezika valjanih na okviru $(\mathbb{N}, <)$.

U sljedećem primjeru navodimo nekoliko formula logike K_tN i svojstva okvira $(\mathbb{N}, <)$ iz kojih te formule slijede.

Primjer 4.2.2. Ovo su neke od formula logike K_tN :

- $FFp \rightarrow Fp$ (tranzitivnost)
- $H\perp \vee PH\perp$ (postoji najmanji element)
- $F\top$ (ne postoji najveći element)
- $Fp \wedge Fq \rightarrow F(p \wedge q) \vee F(Fp \wedge q) \vee F(p \wedge Fq)$ (linearna uređenost)
- $H(Hp \rightarrow p) \rightarrow Hp$ (dobra uređenost skupa \mathbb{N}).

Logika K_tN još je jedan primjer logike koja nema svojstvo konačnih modela, ali je odlučiva. Slijedi dokaz da logika K_tN nema svojstvo konačnih modela, nakon čega dokazujemo njezinu odlučivost metodom mozaika.

Teorem 4.2.3. *Logika K_tN nema svojstvo konačnih modela.*

Dokaz. Iz teorema 2.1.4 slijedi da ako logika K_tN ima svojstvo konačnih modela, onda ima i svojstvo konačnih okvira. Po definiciji 2.1.3, to znači da onda postoji klasa konačnih okvira \mathbf{F} takva da vrijedi $\mathbf{F} \models K_tN$. Pokazat ćemo da ne postoji konačan okvir \mathfrak{F} takav da $\mathfrak{F} \models K_tN$ iz čega će slijediti da logika K_tN nema svojstvo konačnih okvira, stoga ni svojstvo konačnih modela.

Uzmimo proizvoljan konačan okvir $\mathfrak{F} = (W, R_F)$. Iz konačnosti okvira \mathfrak{F} slijedi da postoji niz svjetova $w_1, w_2, \dots, w_n \in W$, $n > 0$, takav da vrijedi $w_1 R_F w_2 R_F \dots R_F w_n R_F w_1$ (takav niz nazivamo ciklus) ili postoji svijet $w \in W$ bez sljedbenika. Ako okvir \mathfrak{F} sadrži ciklus, onda na tom okviru nije valjana formula $H(Hp \rightarrow p) \rightarrow Hp \in K_tN$ koja je valjana samo na dobro uređenim okvirima. Ako okvir \mathfrak{F} sadrži svijet bez sljedbenika, onda formula $F\top \in K_tN$ nije valjana na okviru \mathfrak{F} budući da ta formula nije istinita na svjetovima bez sljedbenika. Zaključujemo $\mathfrak{F} \not\models K_tN$ te smo time završili dokaz teorema. \square

U nastavku dokazujemo odlučivost logike K_tN metodom mozaika, no prije toga trebamo uvesti još nekoliko definicija i par lema.

Definicija 4.2.4. *Pločica je uređeni par (Φ, Λ) , gdje su Φ i Λ Hintikini skupovi koji zadovoljavaju sljedeće uvjete:*

(B0) *ako $F\varphi \in \Lambda$ ili $\varphi \in \Lambda$, onda $F\varphi \in \Phi$*

(B1) *ako $P\varphi \in \Phi$ ili $\varphi \in \Phi$, onda $P\varphi \in \Lambda$*

(B2) *$F\top \in \Lambda$.*

Za pločicu kažemo da je mala ako zadovoljava:

(B3) *ako $F\varphi \in \Phi$, onda $\varphi \in \Lambda$ ili $F\varphi \in \Lambda$*

(B4) *ako $P\varphi \in \Lambda$, onda $\varphi \in \Phi$ ili $P\varphi \in \Phi$.*

Definicija 4.2.5. *Put (malih) pločica od Hintikkinog skupa Φ do Hintikkinog skupa Λ je bilo koji niz $(\Phi_i, \Lambda_i)_{0 \leq i \leq n}$ (malih) pločica takav da $\Phi_0 = \Phi$, $\Lambda_n = \Lambda$ te za svaki $i < n$ vrijedi $\Lambda_i = \Phi_{i+1}$.*

Definicija 4.2.6. Neka je φ neka formula osnovnog temporalnog jezika.

Za skup pločica B kažemo da je **zasićen skup pločica za formulu φ** (eng. *saturated set of bricks for φ* ; kratko: φ -SSB) ako zadovoljava sljedeće uvjete:

(S0) postoji pločica $(\Phi, \Lambda) \in B$ takva da $\neg P\top \in \Phi$ i $\varphi \in \Phi \cup \Lambda$

(S1) za sve $(\Phi, \Lambda) \in B$, ako $F\varphi \in \Lambda$, onda postoji pločica $(\Lambda, \Gamma) \in B$ takva da $\varphi \in \Gamma$

(S2) za svaku pločicu $(\Phi, \Lambda) \in B$ postoji put malih pločica od Φ do Λ u skupu B .

Definicija 4.2.7. Kažemo da je skup formula Γ **zatvoren** ako je:

- zatvoren na potformule
- zatvoren na jednostruke negacije
- za svaku formulu $\varphi \in \Gamma$ koja nije oblika $F\psi$ niti $P\psi$ vrijedi $F\varphi \in \Gamma$ i $P\varphi \in \Gamma$.

Zatvarač skupa formula Γ , u oznaci $Cl(\Gamma)$, je presjek svih zatvorenih skupova formula koji sadrže Γ .

Primijetimo da smo time promijenili definiciju zatvorenog skupa formula temporalnog jezika u odnosu na zatvoreni skup formula osnovnog modalnog jezika, a samim time i definiciju zatvarača (usporedi s 3.3.1.)

Lema 4.2.8. Ako je formula φ osnovnog temporalnog jezika ispunjiva na okviru $(\mathbb{N}, <)$, onda postoji φ -SSB kardinaliteta najviše 2^{2^n} , gdje je n broj elemenata u skupu $Cl(\{\varphi, \top\})$.

Dokaz. Uzmimo proizvoljnu formulu φ koja je ispunjiva na nekom modelu $(\mathbb{N}, <, V)$. Za svaki $n \in \mathbb{N}$ definiramo skup Γ_n na sljedeći način:

$$\Gamma_n = \{\psi \in Cl(\{\varphi, \top\}) \mid (\mathbb{N}, <, V), n \Vdash \psi\}.$$

Skup B definiramo na sljedeći način:

$$B = \{(\Gamma_n, \Gamma_m) \mid n < m\}.$$

Tvrdimo da je skup B jedan φ -SSB skup. Prvo ćemo dokazati da su elementi skupa B pločice. Očito su skupovi Γ_n Hintikkini skupovi.

Pokažimo da za proizvoljan par $(\Gamma_n, \Gamma_m) \in B$ vrijedi uvjet **(B0)**.

Pretpostavimo da vrijedi $F\psi \in \Gamma_m$ ili $\psi \in \Gamma_m$ za neku proizvoljnu formulu ψ . Oba slučaja povlače da postoji svijet $k \geq m$ takav da $(\mathbb{N}, <, V), k \Vdash \psi$. Relacija $<$ je tranzitivna, stoga $n < m$ i $m \leq k$ povlače $n < k$ iz čega slijedi $(\mathbb{N}, <, V), n \Vdash F\psi$. Iz pretpostavke da vrijedi

$F\psi \in \Gamma_m$ ili $\psi \in \Gamma_m$ slijedi $F\psi \in Cl(\{\varphi, \top\})$ ili $\psi \in Cl(\{\varphi, \top\})$. Oba slučaja povlače $F\psi \in Cl(\{\varphi, \top\})$. Zaključujemo $F\psi \in \Gamma_n$. Uvjet **(B1)** dokazuje se analogno.

Iz $\top \in Cl(\{\varphi, \top\})$ slijedi $F\top \in Cl(\{\varphi, \top\})$. Budući da svaki svijet okvira $(\mathbb{N}, <)$ ima sljedbenika, zaključujemo $F\top \in \Gamma_m$. Time smo dokazali i uvjet **(B2)** te završili dokaz da su elementi skupa B pločice.

Pokažimo da za skup B vrijedi uvjet **(S0)**. Po pretpostavci leme formula φ je ispunjiva pa postoji svijet k takav da $(\mathbb{N}, <, V), k \models \varphi$ iz čega slijedi $\varphi \in \Gamma_k$. Iz definicije skupa $Cl(\{\varphi, \top\})$ slijedi $\neg P\top \in Cl(\{\varphi, \top\})$. Iz definicije operatora P slijedi $(\mathbb{N}, <, V), 0 \models \neg P\top$, stoga zaključujemo $\neg P\top \in \Gamma_0$. Ako je $k = 0$, onda je uvjet **(S0)** ispunjen za pločicu (Γ_0, Γ_1) , inače za pločicu (Γ_0, Γ_k) .

Kako bi dokazali ispunjenost uvjeta **(S1)** uzmimo proizvoljnu pločicu $(\Gamma_n, \Gamma_m) \in B$ te pretpostavimo da vrijedi $F\psi \in \Gamma_m$. Zaključujemo da vrijedi $(\mathbb{N}, <, V), m \models F\psi$ iz čega slijedi da postoji svijet $k \in \mathbb{N}$ takav da $m < k$ i $(\mathbb{N}, <, V), k \models \psi$. Zatvarač $Cl(\{\varphi, \top\})$ zatvoren je na potformule, stoga $F\psi \in Cl(\varphi, \top)$ povlači $\psi \in Cl(\varphi, \top)$. Zaključujemo da za pločicu $(\Gamma_m, \Gamma_k) \in B$ vrijedi $\psi \in \Gamma_k$.

Uvjet **(S2)** bit će dokazan ako pokažemo da su pločice oblika (Γ_n, Γ_{n+1}) male pločice. Ako to dokažemo, onda izravno slijedi da je svaki niz $(\Gamma_i, \Gamma_{i+1})_{n \leq i < m}$ put malih pločica od Γ_n do Γ_m .

Kako bi dokazali da uvjet **(B3)** vrijedi za svaku pločicu $(\Gamma_n, \Gamma_{n+1}) \in B$ uzmimo proizvoljnu formulu $F\psi$ takvu da vrijedi $F\psi \in \Gamma_n$. Iz $(\mathbb{N}, <, V), n \models F\psi$ slijedi da postoji $k \in \mathbb{N}$, $n < k$ takav da vrijedi $(\mathbb{N}, <, V), k \models \psi$. Imamo dva slučaja: $k = n + 1$ i $k > n + 1$. Ako vrijedi $k = n + 1$, onda slijedi $\psi \in \Gamma_{n+1}$. Pretpostavimo da vrijedi $n + 1 < k$. Onda iz $(\mathbb{N}, <, V), k \models \psi$ slijedi $(\mathbb{N}, <, V), n + 1 \models F\psi$ te zaključujemo $F\psi \in \Gamma_{n+1}$.

Uvjet **(B4)** dokazuje se analogno, stoga izostavljamo dokaz. Time smo dokazali da je skup B jedan φ -SSB skup.

Preostalo je dokazati da je skup B kardinaliteta najviše $2^{2^{Cl(\{\varphi, \top\})}}$. Vidimo da za svaki n vrijedi $\Gamma_n \subseteq Cl(\{\varphi, \top\})$, stoga možemo imati najviše $2^{|Cl(\{\varphi, \top\})|}$ takvih skupova te najviše $(2^{|Cl(\{\varphi, \top\})|})^2 = 2^{2^{Cl(\{\varphi, \top\})}}$ različitih pločica sastavljenih od tih skupova. Time smo završili dokaz leme. \square

Kako bismo dokazali odlučivost logike $K_t N$, valja dokazati da vrijedi i obrnuta implikacija prethodne leme. No, prije nego što dokažemo obrnutu implikaciju trebamo uvesti još par definicija.

Definicija 4.2.9. Neka je φ formula osnovnog temporalnog jezika. **Povijest formule** φ je uređen par (L, λ) , gdje je $L \in \mathbb{N}$, a funkcija $\lambda : \{0, 1, \dots, L\} \rightarrow Cl(\{\varphi, \top\})$ zadovoljava sljedeće uvjete:

$$(H0) \quad \neg P\top \in \lambda(0)$$

(H1) za sve $n < L$ je $\lambda(n)$ Hintikkin skup

(H2) za svaki $n < L$ je $(\lambda(n), \lambda(n+1))$ mala pločica.

Može se pokazati da za proizvoljnu formulu $\psi \in Cl(\{\varphi, \top\})$ vrijedi:

(H3) ako za neki $n < L$ vrijedi $F\psi \in \lambda(n)$, onda ili postoji $m \in \mathbb{N}$ takav da $n < m \leq L$ i $\psi \in \lambda(m)$ ili vrijedi $F\psi \in \lambda(L)$

(H4) ako za neki $n \leq L$ vrijedi $P\psi \in \lambda(n)$, onda postoji $m \in \mathbb{N}$ takav da $m < n$ i $\psi \in \lambda(m)$.

Ako je jasno za koju formulu definiramo povijest ili ako je ta informacija suvišna, govorimo samo "povijest" umjesto "povijest formule φ ".

Definicija 4.2.10. Kažemo da je povijest (L', λ') **proširenje** povijesti (L, λ) ako vrijedi $L < L'$ i za svaki prirodan broj $n \in \{0, 1, \dots, L\}$ vrijedi $\lambda'(n) = \lambda(n)$. Oznaka: $(L, \lambda) \triangleleft (L', \lambda')$.

Lema 4.2.11. Ako za formulu φ postoji φ -SSB, onda je φ ispunjiva na okviru $(\mathbb{N}, <)$.

Dokaz. Uzmimo formulu φ takvu da postoji skup B koji je φ -SSB. Koristit ćemo pločice iz skupa B za izgradnju modela nad $(\mathbb{N}, <)$ na kojem je formula φ ispunjiva. Ideja je sljedeća: uzet ćemo jednu pločicu iz skupa B koja zadovoljava uvjet (S0) te pomoću nje izgraditi povijest. Koristit ćemo tu povijest i pločice iz skupa B da kreiramo proširenja te povijesti. Ponavljajući postupak kreirat ćemo niz povijesti. Koristit ćemo definirani niz povijesti da definiramo model na kojem je formula φ ispunjiva.

Uzmimo proizvoljnu povijest (L, λ) formule φ . Iz uvjeta (H2) zaključujemo da je $(\lambda(L-1), \lambda(L))$ pločica. Ako vrijedi $(\lambda(L-1), \lambda(L)) \in B$, onda za proizvoljnu formulu ψ vrijedi:

$$\text{ako } F\psi \in \lambda(L), \text{ onda postoji } (L', \lambda') \text{ takva da } (L, \lambda) \triangleleft (L', \lambda') \text{ i } \psi \in \lambda'(L'). \quad (4.1)$$

Kako bi dokazali prethodnu tvrdnju pretpostavimo da vrijedi $(\lambda(L-1), \lambda(L)) \in B$ i $F\psi \in \lambda(L)$. Iz uvjeta (S1) zaključujemo da postoji pločica $(\Lambda, \Gamma) \in B$ takva da je $\Lambda = \lambda(L)$ i $\psi \in \Gamma$. Zbog uvjeta (S2) zaključujemo da postoji put pločica $(\Sigma_i, \Sigma_{i+1})_{0 \leq i < k}$ takav da $\Sigma_0 = \Lambda$ i $\Sigma_k = \Gamma$. Taj put "zalijepimo" na povijest (L, λ) , to jest definiramo $L' = L + k$ te funkciju λ' definiramo na sljedeći način:

$$\lambda'(n) = \begin{cases} \lambda(n), & \text{za } n \leq L, \\ \Sigma_i, & \text{za } n = L + i. \end{cases}$$

Time je za povijest (L', λ') ispunjeno 4.1.

Koristeći 4.1 možemo konstruirati niz $(L_0, \lambda_0) \triangleleft (L_1, \lambda_1) \triangleleft \dots$ povijesti formule φ takav da $\neg P \top \in \lambda_0(0)$, $\varphi \in \lambda_0(0) \cup \lambda_0(L_0)$ te da za svaki i i svaku formulu $F\psi \in \lambda_i(L_i)$ postoji $j > i$ i svijet $L_i < m \leq L_j$ takav da $\psi \in \lambda_j(m)$. Za kreiranje niza povijesti koristili smo uvjet da za svaku funkciju λ_i povijesti (L_i, λ_i) vrijedi $(\lambda_i(L_i - 1), \lambda_i(L_i)) \in B$. Primijetimo da je bitno ispuniti taj uvjet samo za prvi član niza jer je za ostale uvjet ispunjen zbog načina na koji smo definirali funkcije λ_i za $i > 0$. Pokažimo da možemo pronaći pločicu (L_0, λ_0) za koju vrijedi $(\lambda(L_0 - 1), \lambda_0(L_0)) \in B$.

Uzmimo pločicu $(\Phi, \Lambda) \in B$ koja ispunjava uvjet **(S0)**. Definirajmo $L_0 = 1$ te $\lambda(0) = \Phi$ i $\lambda_0(1) = \Lambda$. Time smo pokazali da uistinu možemo definirati takav niz povijesti.

Promotrimo valuaciju $V : Prop \rightarrow \mathcal{P}(\mathbb{N})$ definiranu na sljedeći način:

$$V(p) = \{n \in \mathbb{N} \mid p \in \lambda_i(n) \text{ za neki } i \in \mathbb{N}\}.$$

Tvrdimo da za svaku formulu $\psi \in Cl(\{\varphi, \top\})$ i svaki $n \in \mathbb{N}$ vrijedi:

$$(\mathbb{N}, <, V), n \Vdash \psi \text{ ako i samo ako } \psi \in \lambda_i(n) \text{ za neki } i \in \mathbb{N}. \quad (4.2)$$

Navedenu tvrdnju dokazujemo indukcijom po složenosti formule ψ . Baza indukcije slijedi direktno iz definicije valuacije V .

Pretpostavimo da 4.2 vrijedi za sve formule složenosti $k > 0$. Uzmimo proizvoljnu formulu ψ složenosti $k + 1$. Vrijednosti funkcija λ su Hintikkini skupovi, stoga slučajevi kada je formula ψ nastala Booleovim veznicima slijede izravno.

Promotrimo slučaj kada je ψ oblika $F\chi$ za neku formulu χ složenosti k . Pretpostavimo da za neki svijet $n \in \mathbb{N}$ vrijedi $(\mathbb{N}, <, V), n \Vdash F\chi$. Znači da postoji svijet $m > n$ takav da $(\mathbb{N}, <, V), m \Vdash \chi$. Po pretpostavci indukcije postoji $i \in \mathbb{N}$ takav da vrijedi $\chi \in \lambda_i(m)$. Po uvjetu **(H2)** i činjenici da za sve pločice vrijedi **(B0)** vidimo da za svaki $l < m$ vrijedi $F\psi \in \lambda_i(l)$ što uključuje i $F\chi \in \lambda_i(n)$.

Pokažimo da vrijedi i obrnuti smjer tvrdnje 4.2. Pretpostavimo da vrijedi $F\chi \in \lambda_i(n)$ za neki i . Po definiciji povijesti, preciznije uvjetu **(H3)**, vidimo da ili postoji svijet m takav da $n < m \leq L$ i $\chi \in \lambda_i(m)$ ili vrijedi $F\chi \in \lambda(L_i)$. Promotrimo prvi slučaj. Po pretpostavci

indukcije vrijedi $(\mathbb{N}, <, V), m \Vdash \chi$ iz čega slijedi $(\mathbb{N}, <, V), n \Vdash F\chi$. Ako ne postoji takav m , već vrijedi $F\chi \in \lambda(L_i)$, onda znamo da u našem nizu povijesti postoji povijest (L_j, λ_j) , $j > i$, i svijet m takav da $\chi \in \lambda_j(m)$. Po pretpostavci indukcije vrijedi $(\mathbb{N}, <, V), m \Vdash \chi$ iz čega slijedi $(\mathbb{N}, <, V), n \Vdash F\chi$. Slučaj kada je formula ψ oblika $P\chi$ dokazuje se analogno.

Budući da smo definirali niz povijesti tako da vrijedi $\varphi \in \lambda_0(0) \cup \lambda_0(L_0)$ iz 4.2 slijedi da za valuaciju V vrijedi $(\mathbb{N}, <, V), 0 \Vdash \varphi$ ili $(\mathbb{N}, <, V), L_0 \Vdash \varphi$ te smo time završili dokaz. \square

Teorem 4.2.12. *Logika K_tN je odlučiva.*

Dokaz. Neka je zadana formula φ za koju treba odrediti postoje li svijet $w \in J$ i valuacija V takva da je $(\mathbb{N}, <, V), w \Vdash \varphi$. Prema lemapa 4.2.8 i 4.2.11 to pitanje ekvivalentno je pitanju postojanja φ -SSB kardinaliteta najviše $2^{2|Cl(\varphi, \tau)|}$.

Kreiranje Turingovog enumeratora kojim odgovaramo na pitanje postojanja φ -SSB veličine najviše $2^{2|Cl(\varphi, \tau)|}$ analogno je kreiranju Turingovog enumeratora u dokazu odlučivosti logike KvB pomoću kvazimodela (3.3.8), stoga ćemo taj dio izostaviti. \square

Bibliografija

- [1] P. Blackburn, M. de Rijke i Y. Venema, *Modal Logic*, Cambridge University Press, 2002.
- [2] W. J. Blok i C. J. van Alten, *On the finite embeddability property for residuated lattices, pocrimms and bck-algebras*, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 2000.
- [3] G. Corsi, M. L. Dalla Chiara i G. C. Ghirardi (ur.), *Bridging the Gap: Philosophy, Mathematics, and Physics*, Boston Studies in the Philosophy and History of Science, br. 140, Kluwer Academic Publishers, 1992.
- [4] J. E. Doner, *Decidability of the weak second-order theory of two successors*, Notices Amer. Math. Soc. **12** (1965.), 819.
- [5] J. Ivica, *Odlučivost logike KvB, seminar za kolegij Modalna logika*, 2023.
- [6] M. Mukund i S. P. Suresh, *An Introduction to Logic*, Chennai Mathematical Institute, 1997.
- [7] M. O. Rabin, *Decidability of second-order theories and automata on infinite trees*, Transactions of the American Mathematical Society **141** (1969.), 1–35.
- [8] Z. Richard, *Boxes and Diamonds, An Open Introduction to Modal Logic*, Nezavisno objavljeno, 2019.
- [9] V. Čačić, *Komputonomikon, Izračunljivost za računare*, Prirodoslovno-matematički fakultet u Zagrebu - Matematički odsjek, 2022.

Sažetak

U ovom radu predstavljani su neki osnovni pojmovi sintakse i semantike modalne logike. Zatim su definirani neki sistemi modalne logike poput sistema KvB .

Definirano je svojstvo konačnih modela te prezentirana metoda konačnih modela za dokazivanje odlučivosti modalnih logika. Istaknut je nedostatak te metode, a to je da ne posjeduju sve odlučive logike svojstvo konačnih modela. Logika KvB primjer je jedne takve logike. Zato su predložene druge metode za dokazivanje odlučivosti modalnih logika. Riječ je o metodama interpretacije, kvazimodela i mozaika.

Predstavljena je teorija SnS te je iskazan Rabinov teorem o odlučivosti teorije SnS . Metodom interpretacije dokazana je odlučivost logike KvB . To je ostvareno tako da je problem odlučivosti logike KvB sveden na problem odlučivosti teorije SnS . Odlučivost logike KvB dokazana je i pomoću kvazimodela.

Definirano je jedno proširenje osnovnog modalnog jezika naziva temporalni jezik. Zatim je definirana temporalna logika K_tN . Metodom mozaika dokazana je odlučivost logike K_tN .

Iako su metode interpretacije, kvazimodela i mozaika predstavljene kroz dokaz odlučivosti logika KvB i K_tN , ove metode primjenjive su i na neke druge modalne logike.

Summary

In this master thesis, some basic concepts of syntax and semantics of modal logic are presented. Then, certain systems of modal logic, such as the system \mathbf{KvB} , are defined.

The finite model property is defined, and the technique for proving the decidability of modal logics via finite models is presented. A shortcoming of this technique is highlighted: not all decidable logics possess the finite model property. Logic \mathbf{KvB} serves as an example of such a logic. Therefore, some other techniques for proving the decidability of modal logics are proposed. Those are the decidability via interpretations, quasi-models and mosaics.

The theory S_nS is introduced, and Rabin's theorem on the decidability of the theory S_nS is expressed. The decidability of logic \mathbf{KvB} is proven using interpretations. This is achieved by reducing the decidability problem of logic \mathbf{KvB} to the decidability problem of the theory S_nS . The decidability of logic \mathbf{KvB} is also demonstrated using quasi-models.

An extension of the basic modal language called temporal language is defined. Then, the temporal logic \mathbf{K}_tN is defined. The decidability of the logic \mathbf{K}_tN is proven via mosaics.

Although the decidability via interpretations, quasi-models, and mosaics are presented through the proof of decidability of logics \mathbf{KvB} and \mathbf{K}_tN , these methods are applicable to other modal logics as well.

Životopis

Rođena sam 1998. godine u Zagrebu. Završila sam Osnovnu školu Stenjevec i Osnovnu glazbenu školu Ivana Zajca gdje sam svirala flautu. Srednjoškolsko obrazovanje završila sam u V. gimnaziji u Zagrebu. Tijekom srednjoškolskog obrazovanja sudjelovala sam na državnim natjecanjima iz matematike. Godine 2017. upisala sam preddiplomski sveučilišni studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, a zatim diplomski studij Računarstvo i matematika na istom odsjeku. Tijekom fakultetskog obrazovanja volontirala sam u Dječjem domu Antun Gustav Matoš gdje sam podučavala matematiku.