Univerzita Karlova v Praze, Filozofická fakulta
Katedra logiky

Karel Chvalovský

Explicitní pevné body v logice dokazatelnosti
Explicit fixed-points in provability logic

Diplomová práce

Vedoucí práce: Doc. RNDr. Vítězslav Švejdar, CSc.

2007

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a že jsem uvedl všechny použité prameny a literaturu.

V Praze 31. srpna 2007

Karel Chvalovský

Abstrakt

Smyslem této diplomové práce je prozkoumat explicitní výpočty pevných bodů v logice dokazatelnosti GL. Věta o pevných bodech zní: „Pro každou modální formuli $A(p)$ v níž každý výskyt atomu p je vázán modálním operátorem $\Box$, existuje formule D obsahující pouze výrokové atomy obsažené v $A(p)$, neobsahující výrokový atom p, a taková, že v GL je dokazatelné $D \equiv A(D)$.“ Formule D je navíc určena až na dokazatelnou ekvivalenci jednoznačně. Nejprve vyslovíme několik speciálních případů věty o pevných bodech a poté podrobněji prozkoumáme větu v plném znění. Dále ukážeme jednu sémantickou a dvě syntaktické konstrukce pevných bodů a dokážeme jejich korektnost. V práci se zabýváme také některými složitostními aspekty konstrukce, především uvádíme jednoduché horní odhady délky a modální složitosti získaných pevných bodů.

Abstract

The aim of this diploma thesis is to discuss the explicit calculations of fixed-points in provability logic GL. The fixed-point theorem reads: For every modal formula $A(p)$ such that each occurrence of p is under the scope of $\Box$, there is a formula D containing only sentence letters contained in $A(p)$, not containing the sentence letter p, such that GL proves $D \equiv A(D)$. Moreover, D is unique up to the provable equivalence. Firstly, we establish some special cases of the theorem and then we will look more closely at the full theorem. We show one semantic and two syntactic full fixed-point constructions and prove their correctness. We also discuss some complexity aspects connected with the constructions and present basic upper bounds on length and modal depth of the constructed fixed-points.

Obsah

Úvod

Zkoumání dokazatelnosti pomocí modální logiky pochází již od Gödela, který si povšiml, že jisté podmínky pro dokazatelnost mohou formovat modální logiku. Důvodem jeho zkoumání byla snaha interpretovat dokazatelnost v intuicionistické logice pomocí modální logiky odpovídající systému S4. Jednoduchá interpretace dokazatelnosti jako nutnosti však v tomto případě selhávala[1]. Cesta k modální logice dokazatelnosti, ve které je dokazatelnost interpretována přímo jako nutnost, byla ještě poněkud složitější. Jak se později ukázalo, velký význam z tohoto pohledu mělo Löbovo kladné řešení [Löb55] Henkinovy otázky, zda sentence tvrdící svojí vlastní dokazatelnost je sama dokazatelná. Navíc v článku [Löb55] byly formulovány podmínky platící pro dokazatelnost v každé dostatečně silné rekurzivně axiomatizovatelné teorii. Například v Peanově aritmetice PA, jejíž Σ-definice v $\mathbf{N}$ je $\pi(z)$, pro libovolnou aritmetickou sentenci φ platí

(D1) $\qquad \mathsf{PA} \vdash \varphi \;\Rightarrow\; \mathsf{PA} \vdash Pr_\pi(\overline{\varphi}),$

(D2) $\qquad \mathsf{PA} \vdash Pr_\pi(\overline{\varphi \to \psi}) \to (Pr_\pi(\overline{\varphi}) \to Pr_\pi(\overline{\psi})),$

(D3) $\qquad \mathsf{PA} \vdash Pr_\pi(\overline{\varphi}) \to Pr_\pi(\overline{Pr_\pi(\overline{\varphi})}).$

Uvážíme-li již navrženou interpretaci formální dokazatelnosti jako nutnosti, získáváme okamžitě z podmínek D2 a D3 axiomy logiky K4 a z podmínky D1 pravidlo necesitace, dostáváme tedy modální logiku K4. Získaný modální systém je proto vůči PA, uvážíme-li rozumnou aritmetickou interpretaci, kterou již lze z výše uvedeného odhadnout a o které se později podrobněji zmíníme, korektní. Lze však ukázat, že není úplný. Překvapivě se však úplným stane, přidáme-li modální znění Löbovy věty

(LR) $\qquad \mathsf{PA} \vdash Pr_\pi(\overline{\varphi}) \to \varphi \;\Rightarrow\; \mathsf{PA} \vdash \varphi,$

ať již v podobě pravidla či axiomu.

V polovině sedmdesátých let minulého století se zkoumáním logiky dokazatelnosti zaobíraly tři významné skupiny badatelů a to v Holandsku, v Itálii a ve Spojených státech amerických. Jedním ze zajímavých výsledků těchto zkoumání byla nepochybně věta o pevných bodech, která říká, že pro libovolnou formuli $A(p, \overrightarrow{q})$, ve které se výrokový atom p vyskytuje výhradně vázaný operátorem nutnosti, existuje formule $D(\overrightarrow{q})$ obsahující pouze výrokové atomy z $A(p, \overrightarrow{q})$ kromě p, pro kterou platí

$$\mathsf{GL} \vdash D(\overrightarrow{q}) \;\equiv\; A(D(\overrightarrow{q}), \overrightarrow{q}).$$

[1] Řešením tohoto problému, které využívá složitější překlad, se stala až logika důkazů. Stručný úvod lze nalézt např. v [AB04].

Navíc platí, že formule $D(\overrightarrow{q})$ je až na dokazatelnou ekvivalenci jednoznačně určena. Nyní se můžeme vrátit zpět k formální dokazatelnosti v jisté teorii, například v PA. V ní platí známá věta o autoreferenci, která v jedné ze svých podob říká, že pro libovolnou aritmetickou formuli $\varphi(x, \overrightarrow{y})$ existuje aritmetická formule $\psi(\overrightarrow{y})$, pro kterou

$$\mathsf{PA} \vdash \psi(\overrightarrow{\overrightarrow{q}}) \equiv \varphi(\overrightarrow{\psi(\overrightarrow{q})}, \overrightarrow{\overrightarrow{q}}).$$

Na první pohled je jasné, že spolu obě věty bezprostředně souvisí, a že věty o pevných bodech v logice dokazatelnosti mají důsledky pro větu o autoreferenci.

V dalším textu se budeme větami o pevných bodech v logice dokazatelnosti GL zabývat podrobněji. Přestože se soustředíme především na to, jak pevné body v logice GL přímo sestrojit a na některé jejich vlastnosti, vrátíme se krátce i k jejich metamatematickému významu.

Podrobnosti o počátcích logiky dokazatelnosti, kterým jsme toto povídání začali, přibližně do poloviny sedmdesátých let, lze získat z článku [BS91], ze kterého jsme také čerpali.

Práce je organizována následujícím způsobem: V první části zavedeme potřebnou terminologii a ukážeme několik základních vlastností, které využijeme později v textu. Ve druhé části se zabýváme studiem pevných bodů v logice dokazatelnosti GL obecně. Podrobněji se věnujeme vlastnosti k-rozložitelnosti, která je pro pozdější konstrukce pevných bodů důležitá. V třetí části ukážeme několik speciálních případů věty o pevných bodech, sestrojíme jednoduché pevné body formulí jistých speciálních vlastností. V poslední hlavní části práce pak studujeme tři metody výpočtu pevného bodu v obecném případě. Snažíme se především ukázat kompletní důkazy těchto tvrzení, které zatím v Čechách nebyly podrobněji zkoumány. To je také hlavním smyslem předkádané práce.

1 Logika dokazatelnosti GL

Jazyk výrokové logiky definujeme standardně, pro naše účely je navíc výhodné, aby obsahoval nulární výrokové konstanty nepravda $\bot$ a pravda $\top$. Jazyk modální logiky získáme rozšířením jazyka klasické výrokové logiky o unární modální operátor nutnosti $\Box$. To provedeme induktivně: všechny formule klasické výrokové logiky jsou formulemi modální výrokové logiky a dále pro každou formuli A modální výrokové logiky platí, že formule $\Box A$ je také formulí modální výrokové logiky. Množina formulí modální výrokové logiky je nejmenší množina uzavřená na předchozí dvě pravidla. Modální operátor možnosti $\Diamond$ definujeme jako zkratku za $\neg\Box\neg$. V dalším textu přijmeme následující úmluvy: Formule modální výrokové logiky budeme značit velkými písmeny latinské abecedy, tedy $A, B, \ldots$, naopak malými písmeny latinské abecedy $p, q, \ldots$ budeme značit výrokové proměnné (výrokové atomy). Zároveň, budeme-li mluvit o formulích či modálních formulích, budeme myslet formule standardní modální výrokové logiky. Množinu podformulí formule A, značíme $\mathsf{Subfl}(A)$, stejně jako množinu modalizovaných podformulí formule A, tedy podformulí tvaru $\Box B$, značíme $\mathsf{Subfl}_{\mathsf{M}}(A)$, definuje standardním způsobem.

Definice 1.0.1. Nechť A a B jsou libovolné modální formule. Minimální modální logika K je tvořena axiomy:

(VL) všechny tautologie výrokové logiky,
(AxK) $\Box(A \to B) \to (\Box A \to \Box B)$.

Její odvozovací pravidla jsou *modus ponens* a *necesitace*:

(MP) $A, A \to B \Rightarrow B$,
(Nec) $A \Rightarrow \Box A$.

Definice má dobrý smysl, neboť výroková logika je rozhodnutelná a máme tedy rekurzivní množinu axiomů. Logiku K jsme označili jako minimální, protože jde o nejslabší z takzvaných *normálních modálních logik*, tedy takových modálních logik, které obsahují všechny instance axiomů VL i AxK a zároveň jsou uzavřeny na pravidla modus ponens i necesitaci. V dalším textu budou hrát hlavní roli normální modální systémy K4 a především GL.

Definice 1.0.2. Nechť A je libovolná modální formule. Modální logika K4 vznikne z modální logiky K přídáním jediného axiomu

(Ax4) $\Box A \to \Box\Box A$.

Definice 1.0.3. Nechť A je libovolná modální formule. Modální logika GL vznikne z modální logiky K4 přidáním *Löbova axiomu*

(AxL) $$\Box(\Box A \to A) \to \Box A.$$

Modální logiku dokazatelnosti GL jsme mohli definovat místo nad logikou K4 přímo nad logikou K, neboť axiom Ax4 je v logice K z Löbova axiomu AxL dokazatelný. Logiku GL jsme mohli také získat přidáním *Löbova pravidla*

(LR) $$\Box A \to A \;\Rightarrow\; A.$$

Explicitně jsme se zatím nezmínili o substituci, platí však pochopitelně níže uvedené lemma. Stačí postupovat podle složitosti důkazu a všude v důkazu nahradit příslušnou proměnnou, za kterou substituujeme, jinou proměnnou či celou formulí. Všechny axiomy i pravidla jsme definovali tak, že se v nich může vyskytovat libovolná formule.

Lemma 1.0.1. *Libovolná substituční instance věty* K, K4 *i* GL *je větou* K, K4 *respektive* GL.

Pro další práci bude výhodné definovat iteraci modálního operátoru nutnosti.

Definice 1.0.4. Definujme zkratku $\Box^i$, která značí i iterací modálního operátoru nutnosti, neboli induktivně $\Box^0 A = A$, $\Box^{n+1} A = \Box\Box^n A$.

Využijeme také jistý omezený jazyk modální logiky bez výrokových proměnných.

Definice 1.0.5. Modální formule A je *bezatomární*, neobsahuje-li žádné výrokové atomy.

Bezatomární modální formule tedy vznikají pouze z výrokových konstant $\bot$ a $\top$ libovolnou kombinací logických spojek a modálního operátoru nutnosti.

1.1 Složitost formule v modální logice

V dalším textu budeme také zkoumat složitost pevných bodů, proto zavedeme několik způsobů měření složitosti formule v modální logice. Pro zjednodušení definice, a především pro snadnější motivaci i názornost, zaveďme nejprve stromovou reprezentaci formulí modální logiky.

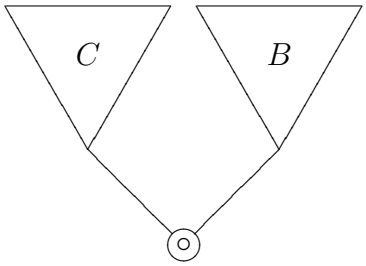
Definice 1.1.1. Pro libovolnou formuli A definujme *stromovou reprezentaci formule* A induktivně podle složitosti formule jako

$A = \top$:

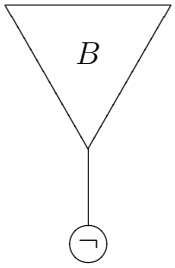
$A = \bot$:

$A = p$:

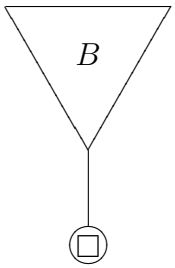
$A = B \circ C$:



$A = \neg B$:



$A = \Box B$:

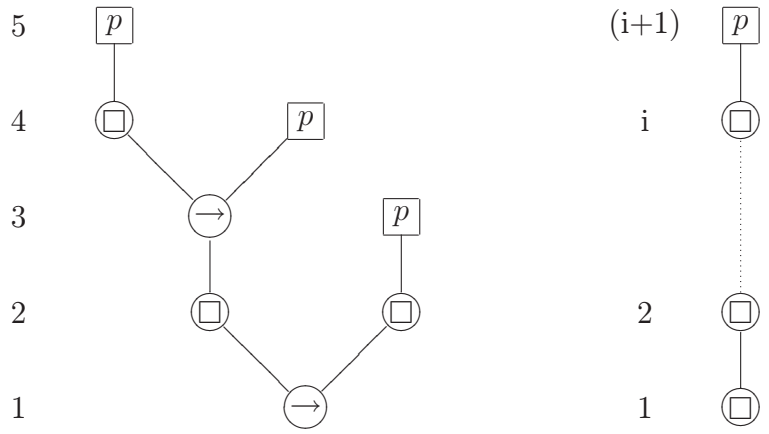


pro $\circ \in \{\wedge, \vee, \rightarrow, \equiv\}$.

Přestože již z definice je patrně jasné, jak stromová reprezentace funguje, uveďme jednoduchý příklad: na obrázku 1 je stromová reprezentace Löbova axiomu $\Box(\Box p \rightarrow p) \rightarrow \Box p$. Zároveň je na obrázku uvedeno také číslování jednotlivých hladin stromu, definujme toto číslování přesně:

Definice 1.1.2. Mějme libovolnou stromovou reprezentaci formule A, *hloubkou stromové reprezentace formule* A či prostě *hloubkou formule* A, značíme $\mathsf{depth}(A)$, rozumíme výšku stromu zvětšenou o jedna, neboli nejmenší číslo $(n+1)$ takové, že pro libovolný list stromu existuje cesta délky nejvýše n z kořene do tohoto listu. *Hladinou* $(h+1)$ *stromové reprezentace* pro $0 \leq h \leq n$ je množina vrcholů, do kterých vede z kořene stromu cesta délky právě h, která neprochází žádným uzlem více než jednou.

Ve výrokové logice se standardně složitost zápisu formule měří *počtem výskytů výrokových proměnných*. To má dobrý smysl, neboť na každý výskyt připadá pouze konstantněkrát dalších symbolů (tj. logických spojek a závorek), neboť jakýkoliv větší počet negací než jedna lze zkrátit. V modální logice ale takový způsob měření dobrý smysl nemá, neboť modální operátory nelze v logice GL na rozdíl od negace krátit. Obecně totiž neplatí, jak se později ukáže, že $\Box p \rightarrow p$. Takto definovaná míra složitosti d' by tedy dávala pro libovolné přirozené číslo i nežádoucí výsledek $\mathsf{d}'(\Box^i p) = 1$, přestože, jak ukazuje obrázek 1, má například její stromová reprezentace $(i+1)$ vrcholů.



Obrázek 1: Stromová reprezentace

Předchozímu problému můžeme předejít, budeme-li měřit složitost formule *počtem výskytů všech symbolů*. S ohledem na to, že v klasické modální logice máme nejvýše binární logické spojky a unární operátor nutnosti a každá logická spojka či modální operátor zanesou do formule nejvýše konstatní počet závorek, liší se míra, která vyjadřuje pouze *počet výskytů výrokových spojek a modálního operátoru nutnosti* od míry vyjadřující počet výskytů všech symbolů pouze konstantněkrát. S užitím stromové reprezentace bychom počet výskytů logických spojek a modálního operátoru nutnosti ve formuli mohli lehce vyjádřit jako počet vrcholů její stromové reprezentace mínus počet listů, neboť ty reprezentují buď výrokové atomy nebo konstanty. Upřednostňovat tuto míru před mírou započítávající i všechny výskyty výrokových atomů a konstant však nemá dobrý smysl, neboť druhá jmenovaná má nejvýše dvakrát tolik vrcholů s jedinou výjimkou, a to formulí obsahující buď pouze výrokový atom nebo konstantu, neboť tam první míra dává hodnutu 0. V dalším textu budeme používat druhou jmenovanou.

Abychom si zjednodušili značení, můžeme využít následující vlastnosti právě definované míry. Pochopitelně předpokládáme, že jak v definici formule, tak v definici stromové reprezentace máme stejné základní výrokové spojky, modální operátory a konstanty.

Lemma 1.1.1. *Pro libovolnou formuli A odpovídá počet vrcholů její stromové reprezentace přesně počtu podformulí A.*

Nyní tedy můžeme zcela korektně definovat délku formule a používat pro ni značení, které intuitivně vyjadřuje počet podformulí.

Definice 1.1.3. Délkou zápisu formule A, značíme $\mathsf{subfl}(A)$, rozumíme počet vrcholů její stromové reprezentace, neboli počet podformulí formule A.

Zaveďme dvě důležité míry složitosti modálních formulí. První počítá, jaký je nejvyšší počet do sebe vnořených modálních operátorů nutnosti a je tedy přirozené nazývat ji modální hloubkou formule.

Definice 1.1.4. Pro libovolnou modální formuli A definujeme její *modální hloubku*, značíme $\mathsf{depth}_{\mathsf{M}}(A)$, induktivně jako

$$\begin{aligned}
&\mathsf{depth}_{\mathsf{M}}(\top) && = 0,\\
&\mathsf{depth}_{\mathsf{M}}(\bot) && = 0,\\
&\mathsf{depth}_{\mathsf{M}}(\neg B) && = \mathsf{depth}_{\mathsf{M}}(B),\\
&\mathsf{depth}_{\mathsf{M}}(B \circ C) && = \max\{\mathsf{depth}_{\mathsf{M}}(B), \mathsf{depth}_{\mathsf{M}}(C)\} \quad \circ \in \{\wedge, \vee, \rightarrow, \equiv\},\\
&\mathsf{depth}_{\mathsf{M}}(\Box B) && = 1 + \mathsf{depth}_{\mathsf{M}}(B).
\end{aligned}$$

Modální hloubku bychom také mohli ekvivalentně definovat jako nejvyšší počet uzlů odpovídajících operátoru nutnosti vyskytující se na libovolné větvi stromové reprezentace formule.

Druhá míra složitosti naopak říká, kolik má formule A podformulí tvaru $\Box B$, neboli jaký má počet modalizovaných podformulí.

Definice 1.1.5. Pro libovolnou modální formuli A definujeme *počet modalizovaných podformulí* formule A, značíme $\mathsf{subfl}_{\mathsf{M}}(A)$, induktivně jako

$$\begin{aligned}
&\mathsf{subfl}_{\mathsf{M}}(\top) && = 0,\\
&\mathsf{subfl}_{\mathsf{M}}(\bot) && = 0,\\
&\mathsf{subfl}_{\mathsf{M}}(\neg B) && = \mathsf{subfl}_{\mathsf{M}}(B),\\
&\mathsf{subfl}_{\mathsf{M}}(B \circ C) && = \mathsf{subfl}_{\mathsf{M}}(B) + \mathsf{subfl}_{\mathsf{M}}(C) \quad \circ \in \{\wedge, \vee, \rightarrow, \equiv\},\\
&\mathsf{subfl}_{\mathsf{M}}(\Box B) && = 1 + \mathsf{subfl}_{\mathsf{M}}(B).
\end{aligned}$$

Znovu bychom mohli počet modalizovaných podformulí definovat pomocí stromové reprezentace jako počet vrcholů stromu reprezentujících operátor nutnosti.

Z induktivní definice, případně z definice pomocí stromové reprezentace, je jasné, že pro obě míry platí následující jednoduchý vztah, do kterého jsme zahrnuli i naši míru pro reprezentaci délky formule.

Lemma 1.1.2. *Pro libovolnou formuli A platí*

$$\mathsf{depth}_{\mathsf{M}}(A) \leq \mathsf{subfl}_{\mathsf{M}}(A) \leq \mathsf{subfl}(A).$$

V dalším textu budeme také studovat složitost jistých algoritmů či spíše pseudoalgoritmů. K tomu bychom měli nějakým způsobem zavést výpočetní model a reprezentaci formulí v něm. My tak explicitně neučiníme, abychom naše odhady nemuseli zbytečně komplikovat. Přesto nebudeme možnosti, které nám tato volnost dává, zneužívat a tam, kde se budeme vyjadřovat ke složitosti algoritmů, budeme pracovat s takovými algoritmy, abychom je případně mohli snadno převést na některý ze standardních výpočetních modelů a aby takový převod zásadním způsobem neovlivnil jejich složitost.

1.2 Kripkovská sémantika

Již jsme definovali kalkuly několika modálních logik, nyní definujeme klasickou kripkovskou sémantiku těchto modálních logik.

Definice 1.2.1. *Kripkovský rámec* $\mathcal{F}$ je dvojice $\langle W, R\rangle$, kde W je neprázdná množina světů a R binární relace dosažitelnosti definovaná na W.

Pro relaci dosažitelnosti R používáme notaci wRw', kterou čteme „svět w' je R-dosažitelný ze světa w“ či nejčastěji prostě „svět w' je dosažitelný ze světa w“. Zároveň poznamenejme, že prvky množiny W nazýváme v dalším textu nejen světy, ale nejčastěji vrcholy.

Nad kripkovským rámcem lze definovat funkci V, která přiřazuje výrokovým atomům množinu světů, ve kterých platí. Tuto funkci lze standardním způsobem rozšířit na pravdivostní relaci $\Vdash$, jak uvádí následující definice:

Definice 1.2.2. Nechť máme funkci V definovanou, jak je uvedeno výše. *Kripkovským modelem* $\mathcal{K}$ nazveme trojici $\langle W, R, \Vdash\rangle$, kde $\mathcal{F} = \langle W, R\rangle$ je kripkovský rámec a $\Vdash$ pravdivostní relace splňující pro libovolnou výrokovou proměnnou p, libovolné formule A a B a libovolný svět $w \in W$ následující podmínky:

$w \Vdash \top$,
$w \nVdash \bot$,
$w \Vdash p$, právě když $w \in V(p)$,
$w \Vdash A \wedge B$, právě když $w \Vdash A$ a $w \Vdash B$,
$w \Vdash A \vee B$, právě když $w \Vdash A$ nebo $w \Vdash B$,
$w \Vdash A \to B$, právě když $w \nVdash A$ nebo $w \Vdash B$,
$w \Vdash A \equiv B$, právě když $w \Vdash A$ tehdy a jen tehdy když $w \Vdash B$,
$w \Vdash \neg A$, právě když $w \nVdash A$,
$w \Vdash \Box A$, právě když pro všechna $w' \in W, wRw'$ platí $w' \Vdash A$.

Zápis $w \Vdash A$ čteme „vrchol w splňuje formuli A“ či prostě „A je splněna v w“, případně používáme také označení „vynucuje“. Budeme-li chtít mluvit

o splňování v konkrétním modelu, můžeme použít značení $w \Vdash_{\mathcal{K}} A$, případně $\mathcal{K}, w \Vdash A$, jejichž význam je zřejmý.

Nyná zavedeme pojem platnosti formule v kripkovském modelu a rámci.

Definice 1.2.3. Nechť $\mathcal{K} = \langle W, R, \Vdash \rangle$ je kripkovský model. Říkáme, že formule A *platí v modelu* $\mathcal{K}$, zapisujeme $\mathcal{K} \models A$, pokud pro každý vrchol $w \in W$ platí $w \Vdash A$. Nechť $\mathcal{F} = \langle W, R \rangle$ je kripkovský rámec. Říkáme, že formule A *platí v rámci* $\mathcal{F}$ neboli $\mathcal{F} \models A$, pokud formule A platí v každém modelu $\mathcal{K} = \langle W, R, \Vdash \rangle$, a tedy platí pro libovolnou definici pravdivostní relace $\Vdash$, nad rámcem $\mathcal{F}$.

Je všeobecně známo, že kripkovské rámce a modely pro jednotlivé námi uvažované logiky nad systémem K získáme omezením relace dosažitelnosti R. Toto omezení přenášíme do názvu rámce, tedy rámec má jistou vlastnost, jestliže ji má jeho relace dosažitelnosti. Logika K je tak úplná vzhledem ke všem kripkovským rámcům a logika K4 vzhledem ke všem tranzitivním rámcům, tedy v logice K není relace dosažitelnosti R nijak omezena, v logice K4 je relace dosažitelnosti R omezena pouze na tranzitivní relace.

Definice 1.2.4. Binární relace $R \subseteq X \times X$ je *obráceně fundovaná*, právě tehdy když každá neprázdná množina $Y \subseteq X$ má R-maximální prvek.

Definice 1.2.5. Kripkovský rámec $\mathcal{F} = \langle W, R \rangle$ je *kripkovským rámcem pro logiku dokazatelnosti* GL, právě tehdy když relace R je tranzitivní a obráceně fundovaná. *Kripkovský model pro logiku* GL získáme z kripkovského rámce pro logiku GL a nějaké pravdivostní funkce V určující pravdivost výrokových atomů ve vrcholech W podle definice 1.2.2.

Protože v dalším textu budeme mluvit téměř výhradně o kripkovských modelech logiky GL, odpustíme si explicitní zmiňování logiky GL a budeme tedy mluvit pouze o kripkovských modelech, případně pouze o modelech. Z kontextu by však mělo být naprosto jasné, že myslíme právě kripkovské modely pro logiku dokazatelnosti GL. Poznamenejme, že platí následující lemma.

Lemma 1.2.1. *Na konečné množině je tranzitivní relace obráceně fundovaná, právě tehdy když je antireflexivní.*

Následující dvě věty o korektnosti a úplnosti kripkovské sémantiky jsou pro nás stěžejní. Můžeme díky nim provádět naše úvahy o logice dokazatelnosti GL syntakticky či sémanticky podle toho, jak budeme v daném okamžiku potřebovat.

Věta 1.2.2 (korektnost vůči kripkovské sémantice)**.** *Nechť A je libovolná formule dokazatelná v logice* GL*, pak formule A platí v každém kripkovském modelu pro logiku dokazatelnosti* GL*.*

Důkaz. Ukážeme pouze platnost Löbova axiomu, ostatní axiomy a všechna odvozovací pravidla se ověřují způsobem standardním v modálních logikách. Mějme libovolný kripkovský model pro logiku dokazatelnosti $\mathcal{K} = \langle W, R, \Vdash\!\!- \rangle$. Nechť tedy $\Box(\Box B \to B) \to \Box B$ je libovolná instance Löbova axiomu a $w \in W$ libovolný vrchol. Stačí dokázat, že kdykoliv platí $w \Vdash\!\!\!\!/\ \Box B$, pak platí také $w \Vdash\!\!\!\!/\ \Box(\Box B \to B)$. Nechť $w \Vdash\!\!\!\!/\ \Box B$, musí tedy existovat vrchol u dosažitelný z w, pro který platí $u \Vdash\!\!\!\!/\ B$. Z vlastnosti obrácené fundovanosti můžeme takové u volit maximální tak, aby pro všechny případné vrcholy v dosažitelné z u, již platilo $v \Vdash\!\!- B$, tedy $u \Vdash\!\!- \Box B$ a v u neplatí implikace $\Box B \to B$. Nyní již dostáváme požadované $w \Vdash\!\!\!\!/\ \Box(\Box B \to B)$. Q.E.D.

Věta 1.2.3 (úplnost vůči kripkovské sémantice)**.** *Nechť formule A platí ve všech kripkovských modelech pro logiku dokazatelnosti* GL*, pak je A dokazatelná v logice* GL*.*

Důkaz úplnosti si odpustíme, lze ho nalézt například v [Šv02, Boo93] či [Smo85]. Základní postup se neliší od standardních důkazů úplnosti ostatních normálních logik, je pouze potřeba ošetřit několik drobností.

Chceme-li ukázat nedokazatelnost formule A v GL, můžeme to provést tak, že se pokusíme zkonstruovat kripkovský protipříklad na A. Pokud se nám to nepodaří, je formule A splnitelná v každém modelu, a tedy z věty 1.2.3 o úplnosti dokazatelná. Kripkovským protipříkladem na formuli A rozumíme takový kripkovský model, ve kterém není A v nějakém jeho vrcholu splněna. Rádi bychom věděli, jaké je omezení velikosti takových modelů, případně by nám pomohlo, pokud bychom se mohli omezit pouze na modely jistého tvaru, například stromy.

Definice 1.2.6. Kripkovský rámec $\mathcal{F} = \langle W, R \rangle$ nazveme *stromový*, právě tehdy když platí

(i) relace dosažitelnosti R je částečné uspořádání, je tedy tranzitivní a antisymetrická,

(ii) pro libovolný prvek $w \in W$ je množina jeho R-předchůdců konečná a lineárně uspořádaná vzhledem k relaci R.

Definice se evidentním způsobem přenáší na kripkovské modely, navíc podotkněme, že z bodu (ii) definice triviálně platí, že existuje kořen stromu, tedy vrchol w, ze kterého jsou všechny ostatní vrcholy dosažitelné.

Následující věta, jejíž důkaz vedeme podle [Smo85], nám poskytuje hledané omezení na velikost i tvar kripkovských modelů.

Věta 1.2.4 (stromová úplnost vůči kripkovské sémantice)**.** *Libovolná modální formule A je dokazatelná v logice* GL*, právě tehdy když platí ve všech konečných stromových kripkovských modelech pro* GL*.*

Důkaz. Jednu stranu ekvivalence dostáváme okamžitě z věty 1.2.2 o korektnosti. Druhou stranu ekvivalence dokazujeme kontrapozicí. Mějme $\mathsf{GL} \nvdash A$, pak z věty 1.2.3 o úplnosti máme kripkovských protipříklad $\mathcal{K} = \langle W, R, \Vdash\rangle$ s vrcholem $w_0, w_0 \nVdash A$. Z tohoto modelu $\mathcal{K}$ vytvoříme stromový konečný kripkovský model $\mathcal{K}_T = \langle W_T, R_T, \Vdash_T\rangle$ s vrcholem $\langle w_0\rangle$.

Popišme nejprve induktivní konstrukci množiny W_T: V kroku 0 přidáme do W_T posloupnost $\langle w_0\rangle$. V kroku $n+1$ uvážíme každou posloupnost $\langle w_0, \ldots, w_n\rangle \in W_T$. Pro každou formuli $\Box B \in \mathsf{Subfl_M}(A)$, pro kterou $w_n \nVdash \Box B$, přidáme prvek do W_T, který bude „dosvědčovat“ v našem konstruovaném stromovém modelu $\mathcal{K}_T$ její neplatnost. Ke každé takové formuli $\Box B$ existuje v $\mathcal{K}$ z obrácené fundovanosti vrchol $u \in W$, $w_n R u$, pro který platí

$$u \Vdash \Box B \text{ a zároveň } u \nVdash B. \tag{1}$$

Do W_T přidáme $\langle w_0, \ldots, w_n, u\rangle$.

Relaci R_T definujeme jako uspořádání prodlužujících se konečných posloupností, tedy například posloupnost $\langle w_0, \ldots, w_n\rangle$ je v takovém uspořádání před posloupností $\langle w_0, \ldots, w_n, u\rangle$. Vrchol $\langle w_0\rangle$ jsme definovali v kroku 0 a relaci $\Vdash_T$ definujeme pro libovolný výrokový atom p vyskytující se ve formuli A jako

$$\langle w_0, \ldots, w_n\rangle \Vdash_T p, \text{ právě tehdy když } w_n \Vdash p.$$

Tvrzení. *Kripkovský rámec $\langle W_T, R_T\rangle$ je konečný stromový kripkovský rámec s vrcholem $\langle w_0\rangle$.*

Že jde o strom s vrcholem $\langle w_0\rangle$ je patrné z kontrukce W_T a relace dosažitelnosti R_T. Z konstrukce je také jasné, že máme strom s konečným větvením, neboť to je omezeno $\mathsf{subfl_M}(A)$. Zároveň nemůže existovat nekonečná větev, neboť z konstrukce na libovolné větvi v každém kroku ubyde alespoň jedna formule $\Box B \in \mathsf{Subfl_M}(A)$, která by mohla vynutit přidání dalšího vrcholu w_i, a tedy délka libovolné posloupnosti respektive délka libovolné větve ve stromu je menší nebo rovna $\mathsf{subfl_M}(A)$.

Tvrzení. *Pro libovolnou podformuli B formule A a libovolnou posloupnost $\langle w_0, \ldots, w_n\rangle \in W_T$ platí*

$$\langle w_0, \ldots, w_n\rangle \Vdash_T B, \textit{ právě tehdy když } w_n \Vdash B.$$

Důkaz provedeme standardně indukcí podle složitosti formule B. Všechny případy kromě $B = \Box C$ jsou triviální, dokazujme tedy pouze tento.

Nejprve ukažme implikaci $w_n \Vdash \Box C \Rightarrow \langle w_0, \ldots, w_n \rangle \Vdash_T \Box C$:

$$
\begin{aligned}
&(2) \quad w_n \Vdash \Box C \Rightarrow \forall u \, (w_n R u \Rightarrow u \Vdash C) \\
&(3) \quad \Rightarrow \forall u \, (\langle w_0, \ldots, w_n, u \rangle \in W_T \Rightarrow u \Vdash C) \\
&(4) \quad \Rightarrow \forall u \, (\langle w_0, \ldots, w_n, u \rangle \in W_T \Rightarrow \langle w_0, \ldots, w_n, u \rangle \Vdash_T C) \, .
\end{aligned}
$$

Formule (3) plyne z (2), protože kdykoliv $\langle w_0, \ldots, w_n, u \rangle \in W_T$, pak z konstrukce určitě platí $w_n R u$. Formule (4) pak plyne z (3) díky indukční hypotéze. Z (4) snadno dostáváme $\langle w_0, \ldots, w_n \rangle \Vdash_T \Box C$.

Ukažme ještě obrácenou implikaci, kterou dokážeme kontrapozicí, dokazujeme tedy implikaci $w_n \nVdash \Box C \Rightarrow \langle w_0, \ldots, w_n \rangle \nVdash_T \Box C$:

$$
\begin{aligned}
&(5) \quad w_n \nVdash \Box C \Rightarrow \exists u \, (w_n R u \,\&\, u \nVdash C) \\
&(6) \quad \Rightarrow \exists u \, (\langle w_0, \ldots, w_n, u \rangle \in W_T \,\&\, u \nVdash C) \\
&(7) \quad \Rightarrow \exists u \, (\langle w_0, \ldots, w_n, u \rangle \in W_T \,\&\, \langle w_0, \ldots, w_n, u \rangle \nVdash_T C) \, .
\end{aligned}
$$

Hned v prvním kroku, kdy z (5) získáváme (6), použijeme zásadním způsobem podmínku (1), neboť pouze skutečnost, že $w_n \nVdash \Box C$ nám zajišťuje existenci u pro které $\langle w_0, \ldots, w_n, u \rangle \in W_T$. Naopak (7) získáme ze (6) znovu z indukční hypotézy. A ze (7) již snadno dostáváme $\langle w_0, \ldots, w_n \rangle \nVdash_T \Box C$.

Nyní již evidentně platí

$$w_0 \nVdash A \Rightarrow \langle w_0 \rangle \nVdash_T A.$$

Q.E.D.

Z důkazu věty můžeme snadno získat slibované odhady, nejprve ale definujeme pojem ranku vrcholu, který budeme používat i dále.

Definice 1.2.7. Nechť $\mathcal{K} = \langle W, R, \Vdash \rangle$ je kripkovský model, pro libovolný vrchol $w \in W$ definujeme *rank* vrcholu w v modelu $\mathcal{K}$, značíme $\mathcal{K}\text{-}\mathsf{rank}\,(w)$, jako

$$\mathcal{K}\text{-}\mathsf{rank}(w) = \begin{cases} 0 & \text{neexistuje } u, \text{ pro které } wRu, \\ 1 + \max\{\mathcal{K}\text{-}\mathsf{rank}(u); wRu\} & \text{jinak.} \end{cases}$$

Důsledek 1.2.5. *Uvažujme libovolnou formuli A a stromový kripkovský model $\mathcal{K}_\mathcal{T} = \langle W_T, R_T, \Vdash_T \rangle$ s kořenem $\langle w_0 \rangle$ z předchozí konstrukce, pak platí*

$$\mathcal{K}_\mathsf{T}\text{-}\mathsf{rank}(\langle w_0 \rangle) \leq \mathsf{subfl}_\mathsf{M}(A),$$

navíc platí $|W_T| \leq (1 + \mathsf{subfl}_\mathsf{M}(A))!$.

Důkaz. Platnost $\mathcal{K}_{\mathsf{T}}\text{-}\mathsf{rank}(\langle w_0 \rangle) \leq \mathsf{subfl}_{\mathsf{M}}(A)$ byla diskutována již v důkazu věty 1.2.4, soustřeďme se tedy na druhý odhad. Vyjdeme-li z kořene $\langle w_0 \rangle$, pak z konstrukce vyplývá, že z něj může vycházet nejvýše $\mathsf{subfl}_{\mathsf{M}}(A)$ přímých následníků. Pro libovolný z těchto přímých následníků pak platí, že může mít tentokráte nejvýše $(\mathsf{subfl}_{\mathsf{M}}(A) - 1)$ přímých následníků a stejným způsobem lze pokračovat. Počet vrcholů W_T tedy můžeme shora odhadnout součtem

$$1 + \mathsf{subfl}_{\mathsf{M}}(A) + \mathsf{subfl}_{\mathsf{M}}(A)(\mathsf{subfl}_{\mathsf{M}}(A) - 1) + \ldots + (\mathsf{subfl}_{\mathsf{M}}(A))!$$

a ten můžeme lehce omezit výrazem $(1 + \mathsf{subfl}_{\mathsf{M}}(A))!$. Q.E.D.

Díky tomu, že k libovolné formuli umíme explicitně určit maximální velikost jejího protipříkladu, máme rozhodovací algoritmus pro logiku GL. Ten postupně generuje všechny modely a zkouší, zda v nich formule platí. Skončí, najde-li protipříklad, nebo pokud vyčerpá všechny modely velikosti menší nebo rovné velikosti maximálního možného protipříkladu. V každém uvažovaném modelu pochopitelně musíme vyzkoušet také všechna možná ohodnocení výrokových atomů vyskytujících se ve formuli. Těch je ale pouze konečný počet, a tedy pro konečný model je pouze konečně mnoho možností ohodnocení.

Důsledek 1.2.6. *Logika* GL *je rozhodnutelná.*

Přestože velikost modelu není omezena polynomem, délka každé větve polynomem od velikosti formule omezena je. Testovací algoritmus lze implementovat tak, že mu stačí vždy zkoušet pouze jednu větev a tedy vystačí s polynomiálním prostorem, proto je logika GL v *PSPACE*. Navíc platí:

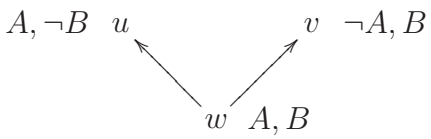
Tvrzení 1.2.7. *Úloha* GLTAUT *je* *PSPACE*-*úplná.*

V článku [Šv03] je ukázáno, že dokonce rozhodovací procedura pro fragment logiky GL s jediným výrokovým atomem je *PSPACE*-úplná.

1.3 Základní vlastnosti logiky GL

V dalším textu budeme potřebovat několik základních vlastností logiky GL. Všechny úvahy budeme provádět v logice K4, přestože bychom mohli samozřejmě uvažovat přímo v logice GL. Jak se však ukáže, bude to pro nás v jistém smyslu výhodné. Všechna námi vyslovená tvrzení pro logiku K4, však pochopitelně platí i v silnější logice GL.

Nejprve uveďme základní vlastnosti distribuce operátoru nutnosti vůči logickým spojkám.



Obrázek 2: Kripkovský protipříklad

Lemma 1.3.1. *Nechť A, B jsou libovolné modální formule, platí*
(i) $\mathsf{K4} \vdash \Box(A \wedge B) \equiv (\Box A \wedge \Box B)$
(ii) $\mathsf{K4} \vdash \Box A \vee \Box B \to \Box(A \vee B)$
(iii) $\mathsf{K4} \vdash \Box(A \to B) \to (\Box A \to \Box B)$
(iv) $\mathsf{K4} \vdash \Box(A \equiv B) \to (\Box A \equiv \Box B)$

Předchozí lemma uvádíme bez důkazu, prokazovalo by se snadno například sémanticky. Upozorněme, že v bodech (ii)–(iv) neplatí obrácená implikace, jak ukazuje pro všechny tři implikace společný kripkovský protipříklad na obrázku 2. Stačí uvážit kořen w. Navíc uvážíme-li formule $\Box(\neg A)$ a $\neg(\Box A)$, pak není obecně dokazatelná ani $\Box(\neg A) \to \neg(\Box A)$, ani $\neg(\Box A) \to \Box(\neg A)$, jak znovu ukazuje obrázek 2, tentokráte uvážíme-li vrchol u či v respektive znovu kořen w.

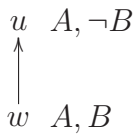
Snadno se, například sémanticky, ukáže i následující lemma.

Lemma 1.3.2. *Nechť A, B jsou libovolné modální formule. Jestliže platí $\mathsf{K4} \vdash \Box A \to B$, pak platí také $\mathsf{K4} \vdash \Box A \to \Box B$.*

V dalším textu bude hrát významnou roli substituční lemma. Ve standardní výrokové logice vystačíme s klasickou ekvivalencí formulí. To nám však v modálním kontextu při uvažování v modelech stačit nebude. Uvažme například kripkovský model na obrázku 3, kde je v kořenu w evidentně splněno $A \equiv B$, uvažme však substituci A a B do formule $\Box p$. Ve vrcholu w je splněno $\Box A$, není však splněno $\Box B$, a tedy není splněno ani $\Box A \equiv \Box B$, a proto ani $(A \equiv B) \to (\Box A \equiv \Box B)$. Díváme-li se na celou věc sémanticky, je jasné, že nestačí, aby substituované formule byly ekvivalentní pouze v jednom vrcholu modelu, ale i ve všech dosažitelných vrcholech, tedy formule musí být nejen ekvivalentní ale i nutně ekvivalentní. To vede k následující definici, takzvané *silné nutnosti*:

Definice 1.3.1. Modální operátor *silně nutně*, značíme $\boxdot A$, je zkratkou za $A \wedge \Box A$, neboli

$$\boxdot A =_{def} A \wedge \Box A.$$



Obrázek 3: Kripkovský protipříklad

Vraťme se na chvíli k logice GL. Zavedení operátoru silné nutnosti má dobrý smysl, neboť obecně

$$\mathsf{GL} \nvdash B \to \Box B$$

ani

$$\mathsf{GL} \nvdash \Box B \to B.$$

Obrázek 3 je kripkovským protipříkladem na obě formule. Ve vrcholu w neplatí první z nich a ve vrcholu u druhá.

K definici silné nutnosti ještě poznamenejme, že stejně jako například v logice K4 neplatí v logice GL standardní podoba věty o dedukci. Z pravidla necesitace triviálně platí $A \vdash \Box A$, ale jak jsme ukázali, obecně neplatí $\vdash A \to \Box A$. Lze však ukázat, stejně jako v logice K4, platnost slabší verze: jestliže $\mathsf{GL}, A \vdash B$, pak $\mathsf{GL} \vdash (A \wedge \Box A) \to B$, neboli $\mathsf{GL} \vdash \boxdot A \to B$.

Uveďme znovu bez důkazu následující jednoduché lemma, které říká, že operátor silně nutně $\boxdot$ splňuje všechny axiomy a pravidla logiky K4.

Lemma 1.3.3. *Nechť A, B jsou libovolné modální formule, pak platí*
(i) $\mathsf{K4} \vdash \boxdot(A \to B) \to (\boxdot A \to \boxdot B)$,
(ii) $\mathsf{K4} \vdash \boxdot A \to \boxdot\boxdot A$,
(iii) jestliže $\mathsf{K4} \vdash \boxdot A$ *a* $\mathsf{K4} \vdash \boxdot(A \to B)$, *pak* $\mathsf{K4} \vdash \boxdot B$,
(iv) jestliže $\mathsf{K4} \vdash A$, *pak* $\mathsf{K4} \vdash \boxdot A$.

Proto můžeme okamžitě vyslovit následující lemma, které je parafrází lemmatu 1.3.1.

Lemma 1.3.4. *Nechť A, B jsou libovolné modální formule, pak platí*
(i) $\mathsf{K4} \vdash \boxdot(A \wedge B) \equiv \boxdot A \wedge \boxdot B$
(ii) $\mathsf{K4} \vdash \boxdot A \vee \boxdot B \to \boxdot(A \wedge B)$
(iii) $\mathsf{K4} \vdash \boxdot(A \to B) \to (\boxdot A \to \boxdot B)$
(iv) $\mathsf{K4} \vdash \boxdot(A \equiv B) \to (\boxdot A \equiv \boxdot B)$

Důkaz. Podle lemmatu 1.3.3 splňuje operátor silné nutnosti $\boxdot$ všechny axiomy logiky K4, a tedy body (i)-(iv) platí podle lemmatu 1.3.1. Q.E.D.

To, že v bodech (ii)–(iv) neplatí obrácené implikace, znovu ukazuje obrázek 2. Opět také není dokazatelné ani $\boxdot(\neg A) \to \neg(\boxdot A)$, ani $\neg(\boxdot A) \to \boxdot(\neg A)$ (znovu obrázek 2), uvážíme-li vrchol u či v respektive kořen w.

Navíc však pro silnou nutnost platí také následující jednoduché vlastnosti:

Lemma 1.3.5. *Nechť A, B jsou libovolné modální formule, pak platí*
(i) $\mathsf{K4} \vdash \boxdot A \to A$,
(ii) $\mathsf{K4} \vdash \boxdot A \to \Box A$,
(iii) $\mathsf{K4} \vdash \boxdot A \equiv \boxdot\boxdot A$,
(iv) $\mathsf{K4} \vdash \Box\boxdot A \equiv \Box A$,
(v) $\mathsf{K4} \vdash \Box\boxdot A \equiv \boxdot\Box A$.

Při dokazování budeme v dalším textu bude často potřebovat následující lemma, které si proto dokážeme.

Lemma 1.3.6. *Nechť A, B jsou modální formule, jestliže $\mathsf{K4} \vdash \boxdot A \to B$, pak $\mathsf{K4} \vdash \Box A \to \Box B$ a také $\mathsf{K4} \vdash \boxdot A \to \boxdot B$.*

Důkaz.

(8)	$\mathsf{K4} \vdash \boxdot A \to B$,	
	$\vdash \Box\boxdot A \to \Box B$,	*Nec*, lemma 1.3.1,
	$\vdash \Box A \to \Box B$,	lemma 1.3.5,
(9)	$\vdash \boxdot A \to \Box B$,	lemma 1.3.5,
	$\vdash \boxdot A \to \boxdot B$,	(8), (9).

Q.E.D.

Již jsme poznamenali, že směřujeme k substitučnímu lemmatu, které lze vyslovit ve dvou základních podobách. Uvedeme obě, ačkoliv druhá je vzhledem k předchozímu lemmatu jednoduchým důsledkem první. V textu však až na drobné výjimky budeme pracovat pouze s prvním zněním.

Lemma 1.3.7 (První substituční lemma)**.** *Mějme modální formuli $A(p)$, pak*

$$\mathsf{K4} \vdash \boxdot(B \equiv C) \to A(B) \equiv A(C).$$

Důkaz. Ukážeme indukcí podle složitosti formule $A(p)$.

Případ, kdy je $A(p)$ rovno p nebo q, $q \neq p$, či $\top$ nebo $\bot$ jsou triviální. Jednoduše se vyřeší také případy pro výrokové spojky, ukažme platnost například pro $A(p) = D(p) \to E(p)$. Z indukční hypotézy víme

$$\mathsf{K4} \vdash \boxdot(B \equiv C) \to D(B) \equiv D(C),$$
$$\mathsf{K4} \vdash \boxdot(B \equiv C) \to E(B) \equiv E(C),$$

navíc následující formule je tautologie výrokové logiky

$$(D(B) \equiv D(C)) \wedge (E(B) \equiv E(C)) \rightarrow (D(B) \rightarrow E(B)) \equiv (D(C) \rightarrow E(C))$$

a nyní již snadno dostáváme požadované

$$\mathsf{K4} \vdash \boxdot (B \equiv C) \rightarrow (D(B) \rightarrow E(B)) \equiv (D(C) \rightarrow E(C)).$$

Klíčovou částí důkazu je samozřejmě případ, kdy $A(p) = \Box D(p)$. Vyjděme znovu z indukční hypotézy a postupujme stejně jako v důkazu lemmatu 1.3.6

$$\begin{aligned}
&\mathsf{K4} \vdash \boxdot (B \equiv C) \rightarrow D(B) \equiv D(C), \\
&\quad \vdash \Box \boxdot (B \equiv C) \rightarrow \Box (D(B) \equiv D(C)), && \text{Nec, lemma 1.3.1,} \\
&\quad \vdash \Box (B \equiv C) \rightarrow \Box (D(B) \equiv D(C)), && \text{lemma 1.3.5,} \\
&\quad \vdash \boxdot (B \equiv C) \rightarrow \Box (D(B) \equiv D(C)), && \text{lemma 1.3.5,} \\
&\quad \vdash \boxdot (B \equiv C) \rightarrow \Box D(B) \equiv \Box D(C), && \text{lemma 1.3.1.}
\end{aligned}$$

Q.E.D.

Sémantický důkaz přechozího lemmatu lze nalézt například v [Šv02].

Lemma 1.3.8 (druhé substituční lemma)**.** *Mějme modální formuli $A(p)$, pak*

$$\mathsf{K4} \vdash \Box (B \equiv C) \rightarrow \Box (A(B) \equiv A(C)).$$

Důkaz. Z prvního substitučního lemmatu použitím lemmatu 1.3.6. Q.E.D.

Substituční lemma budeme v dalším textu často používat, a to jak v syntaktických, tak i sémantických důkazech. Ukažme si obě použití a podrobně je okomentujme. S ohledem na další použití vše demonstrujme v GL, přestože bychom pochopitelně mohli uvažovat i v K4.

Mějme libovolnou formuli $A(p)$ a nejprve předpokládejme, že jsme dospěli k tvzení

$$\mathsf{GL} \vdash B \equiv C,$$

můžeme použít lemma 1.3.3 a získáme

$$\mathsf{GL} \vdash \boxdot (B \equiv C),$$

z prvního substitučního lemmatu 1.3.7 máme

$$\mathsf{GL} \vdash \boxdot (B \equiv C) \rightarrow A(B) \equiv A(C),$$

a tedy snadno použitím pravidla modus ponens (MP) dostáváme

$$\mathsf{GL} \vdash A\,(B) \equiv A\,(C)\,.$$

Sémantické použití je podobné. Máme kripkovský model $\mathcal{K}$ a jeho vrchol w. Dospěli jsme k tvzení

$$w \Vdash \boxdot\,(B \equiv C)\,.$$

Uvědomme si, že v tomto případě je důležité mít $\boxdot\,(B \equiv C)$. Neboli je důležité vědět, že ve w i ve všech z něj dosažitelných vrcholech je splněno $B \equiv C$. První substituční lemma 1.3.7 a úplnost GL nám dává

$$w \Vdash \boxdot\,(B \equiv C) \to A\,(B) \equiv A\,(C)\,,$$

a tedy z definice splňování implikace v modelu dostáváme také

$$w \Vdash A\,(B) \equiv A\,(C)\,.$$

To však není vše. Rozmysleme si, že umíme, jak v předchozím syntaktickém případě, tak nyní, získat dokonce $\boxdot\,(A\,(B) \equiv A\,(C))$. V syntaktickém důkazu můžeme jednak znovu užít lemma 1.3.3, v sémantickém úvahy o tom, že uvedený postup platí také ve všech vrcholech dosažitelných z w, jednak prostě z lemmatu 1.3.6, které nám říká, že kdykoliv máme

$$\mathsf{GL} \vdash \boxdot\,(B \equiv C) \to A\,(B) \equiv A\,(C)\,,$$

máme i

$$\mathsf{GL} \vdash \boxdot\,(B \equiv C) \to \boxdot\,(A\,(B) \equiv A\,(C))\,.$$

Pokud bychom měli pouze

$$w \Vdash \Box\,(B \equiv C)\,,$$

tedy ve w ekvivalence B a C není splněna, respektive o tom nic nevíme, pak stejným způsobem, ale užitím druhého substitučního lemmatu, dostáváme

$$w \Vdash \Box\,(A\,(B) \equiv A\,(C))\,.$$

1.4 Aritmetická interpretace

Modální logika dokazatelnosti GL má, jak jsme se již zmínili, značný metamatematický význam. Uvážíme-li dostatečně silnou formální teorii, například PA a její Σ-definici π v $\mathbf{N}$, pak *aritmetický překlad* $\star$ je funkce z formulí modální výrokové logiky do aritmetických sentencí definovaná tak, že $\star(\bot) = (0 = S(0))$, funkce $\star$ komutuje se všemi výrokovými spojkami, a libovolnou modální formuli $\Box A$ přeložíme na aritmetickou sentenci $\mathrm{Pr}_\pi\left(\overline{\star(A)}\right)$. Uvědomme si, že na výrokových atomech není aritmetický překlad explicitně definován a je tedy libovolný. O modální formuli A řekneme, že je PA-platná, jestliže pro libovolný aritmetický překlad $\star$ platí, že $\mathsf{PA} \vdash \star(A)$.

Význam logiky dokazatelnosti pro PA objasňuje věta o aritmetické korektnosti a úplnosti logiky GL:

Věta 1.4.1 (aritmetická korektnost a úplnost GL)**.** *Každá modální formule A je* PA*-platná, právě tehdy když je dokazatelná v logice* GL*.*

Důkaz aritmetické korektnosti dostáváme téměř okamžitě z podmínek pro dokazatelnost v PA a Löbovy věty, o čemž jsme se již zmínili v úvodu této práce. Solovayův důkaz úplnosti je technicky náročnější a lze ho nalézt buď v původním článku [Sol76], či například v monografiích [Šv02, Boo93, Smo85]. Důkaz probíhá kontrapozicí – ke každé nedokazatelné formuli A sestrojíme takový aritmetický překlad $\star$, že $\star(A)$ není dokazatelná v PA. Tento překlad získáme z kripkovského protipříkladu na formuli A použitím věty o autoreferenci v množném čísle.

Doposud jsme mluvili v souvislosti s logikou dokazatelnosti pouze o aritmetické teorii PA. Má však pochopitelně dobrý smysl ptát se, jak vypadá logika dokazatelnosti jiných formálních teorií, ve kterých lze definovat příslušné pojmy, tedy jak v některých slabších aritmetikách tak například v silnějších teoriích množin. Ukazuje se, že logika GL je společnou logikou dokazatelnosti řady rozumných teorií. Lze ji tedy chápat jako prototypickou logiku dokazatelnosti. Proto se v našich úvahách soustředíme právě na ni. Stejným způsobem je nutno chápat náš přístup k PA. Ta je pro nás také především prototypickým zástupcem, kterého jsme si vybrali pro její význam a pro názornost.

2 Pevné body v logice GL

V úvodu jsme již zmínili věty o pevných bodech – větu o jednoznačnosti a větu o existenci pevných bodů pro formule jistého tvaru. Pevným bodem formule $A(p)$ budeme prozatím rozumět formuli D, která obsahuje pouze výrokové proměnné z $A(p)$ kromě p a platí pro ni

$$\mathsf{GL} \vdash D \equiv A(D).$$

Nemůžeme očekávat, že každá modální formule bude mít pevný bod, uvažme například formuli $A(p) = \neg p$. K takové formuli očividně nemůže existovat žádná bezatomární formule D, pro kterou by platilo

$$\mathsf{GL} \vdash D \equiv \neg D.$$

Přijměme úmluvu, kterou budeme dodržovat dále v textu. Formuli $A(p)$ bychom pochopitelně měli správně zapisovat, například $A(p, \overrightarrow{q})$, abychom zdůraznili, že může mít i další parametry. Nás však většinou zajímá pouze proměnná p, pro kterou hledáme pevný bod a vystačíme si tedy se zápisem $A(p)$. Budeme však mít stále na vědomí, že může obsahovat i další proměnné. V jisté části práce také budeme předpokládat, že se v $A(p)$ jiná proměnná než p nevyskytuje, na to však včas upozorníme. Náš zápis dokonce ani nepředpokládá, že se p musí v $A(p)$ vyskytovat, označení $A(p)$ pak sice nemá úplně dobrý smysl, pro jednotnost značení ho však ponecháváme. Navíc níže uvedené věty, pokud není řečeno jinak, platí i v tomto případě.

Definice 2.0.1. Řekneme, že ve formuli $A(p)$ se výrokový atom p vyskytuje *pouze v modálním kontextu*, jestliže každý výskyt p v $A(p)$ je vázán modálním operátorem nutnosti.

Z pohledu stromové reprezentace formule $A(p)$ předchozí definice vlastně říká, že pokud se p vyskytuje v $A(p)$ pouze v modálním kontextu, pak při libovolné cestě z kořene narazíme dříve na vrchol reprezentující operátor nutnosti než na vrchol reprezentující výrokový atom p, respektive libovolná cesta z kořene do libovolného vrcholu reprezentujícího p vede přes vrchol reprezentující operátor nutnosti. Abychom mohli říci, že je to právě tehdy, musíme kvůli formuli p uvážit i cesty nulové délky.

Jak se ukáže dále, je podmínka výskytu p v $A(p)$ pouze v modálním kontextu postačující podmínkou pro to, aby $A(p)$ měla pevný bod. Nejde však o podmínku nutnou, uvažme například formuli $A(p) = p \vee \Box p$, ta má

evidentně pevný bod $\top$[2], neboť lze snadno ukázat, že $\Box\top$ je v GL ekvivalentní $\top$.

Podmínka výskytu p v $A(p)$ pouze v modálním kontextu má dobrý smysl, připomeneme-li souvislost věty o pevných bodech s větou o autoreferenci. Ve své nejjednodušší podobě věta o autoreferenci říká, že pro libovolnou aritmetickou formuli $\psi(x)$ existuje aritmetická sentence φ a platí

$$\mathsf{PA} \vdash \varphi \equiv \psi(\overline{\varphi}).$$

Formule φ se v ψ vlastně vůbec nevyskytuje, parametrem ψ je totiž pouze její kód $\overline{\varphi}$. Z pohledu aritmetického překladu $\star$ nám tedy podmínka zaručující výskyt p v $A(p)$ pouze v modálním kontextu dává, že v $\star(A(p))$ jsou všechny výskyty $\star(p)$ uvnitř predikátu Pr_π, neboli pro každý výskyt p v $A(p)$ existuje formule $\Box C$, která ho obsahuje a je podformulí $A(p)$, a tedy $\star(A(p))$ obsahuje jako svoji podformuli $Pr_\pi(\overline{\star(C)})$[3].

2.1 k-rozložitelnost modální formule

O formuli $A(p)$, pro kterou hledáme pevné body, předpokládáme, že se v ní proměnná p vyskytuje pouze v modálním kontextu. Můžeme ji tedy chápat jako výrokovou kombinaci výrokových proměnných různých od p a formulí tvaru $\Box E$. Tato vlastnost bude hrát v textu významnou roli, proto se nám vyplatí podrobněji se na ni podívat. Zavedeme rozklad, ve kterém budeme mít výrokovou kombinaci jistých proměnných či formulí, ve kterých se p nevyskytuje, a pak formulí tvaru $\Box E$, ve kterých se p vyskytuje. Směřujeme tedy k definici pojmu k-rozložitelnosti respektive k-rozkladu.

Definice 2.1.1. Modální formuli $A(p)$ nazveme *k-rozložitelnou*, jestliže existuje posloupnost (připouštíme i prázdnou) čerstvých navzájem různých výrokových proměnných $q_1, \ldots, q_k$, formule $B[q_1, \ldots, q_k]$, ve které se nevyskytuje

[2] V dalším textu ukážeme, že se na pevné body nemusíme dívat pouze jako na formule D, které jsou řešeními rovnic typu $p \equiv A(p)$, ale také jako na formule splňující $\boxdot(p \equiv A(p)) \to (p \equiv D)$. Ukážeme, že pokud se p vyskytuje v $A(p)$ pouze v modálním kontextu, tak oba způsoby definice pevného bodu vyjdou nastejno. V tomto případě to tak není, neboť $A(p) = p$ má podle našeho standardního způsobu evidentně za pevné body všechny formule tvořené pouze z konstatnt $\top$, $\bot$. Povšimněme si, že má tedy i neekvivalentní pevné body! Naopak podle druhého způsobu pevný bod nemá, protože triviálně je dokazatelné $\boxdot(p \equiv p)$, a tedy by muselo být dokazatelné i $p \equiv D$ pro nějaké D bez proměnných, ale to pochopitelně nelze. Naopak pro formuli $\Box p \vee p$ je $\top$ pevným bodem podle obou definic. Podrobnosti čtenář najde na straně 113 v knize [Boo93].

[3] Proto se podmínce na výskyt p pouze v modálním kontextu někdy říká (DR) neboli Diagonalisation Restriction. Připomeňme, že v anglosaské literatuře se věta o autoreferenci označuje jako Diagonalisation Theorem. Lze se setkat také se značením „p má pouze modalizovaný výskyt“, jehož význam je jasný.

p a formule $C_1(p), \ldots, C_k(p)$, ve kterých se p naopak vyskytuje, a platí

$$A(p) = B[\Box C_1(p), \ldots, \Box C_k(p)].$$

Navíc předpokládáme, že jednotlivé $C_i(p)$ jsou různé, nepřekrývají se a neobsahují neužitečné výskyty p.

Často budeme místo k-rozložitelnosti hovořit také o k-rozkladu či pouze o rozkladu. Navíc ve většině případů používáme n místo k, abychom upozornili na to, že myslíme konkrétní rozklad. Z kontextu by to mělo býti jasné.

Pochopitelně ne každá modální formule $A(p)$ je k-rozložitelná. Evidentně každá formule, ve které se p vyskytuje také mimo modální kontext není k-rozložitelná, neboť p se musí vyskytovat pouze ve všech $C_i(p)$, tím pádem jsou všechny jeho výskyty v $B[\Box C_1(p), \ldots, \Box C_n(p)]$ tvořené z libovolných formulí $B, C_1(p), \ldots, C_n(p)$ modalizované, a tedy nepochybně $A(p) \neq B[\Box C_1, \ldots, \Box C_n]$.

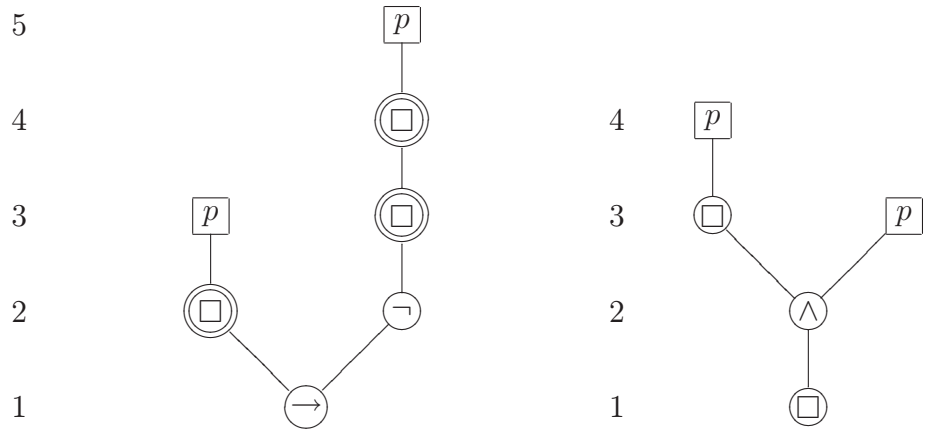
Následující lemma naopak ukazuje, že k tomu, aby formule $A(p)$ byla k-rozložitelná stačí, že se v ní výrokový atom p vyskytuje pouze v modálním kontextu.

Lemma 2.1.1. *Pro každou formuli $A(p)$, v níž se p vyskytuje pouze v modálním kontextu, existuje $k \geq 0$, pro které je $A(p)$ k-rozložitelná.*

Důkaz. Neobsahuje-li formule výrokovou proměnnou p, pak je nepochybně 0-rozložitelná. Jestliže se p v $A(p)$ vyskytuje, uvážíme stromovou reprezentaci formule $A(p)$. Formuli B' konstruujeme tak, že vyjdeme z kořene stromu a postupně procházíme jeho větvení, například zleva, a to tak dlouho, dokud nenarazíme na vrchol reprezentující operátor nutnosti. V tom okamžiku prohledávání příslušné větve zastavíme a vrchol reprezentující operátor nutnosti i celý podstrom na něm navázaný nahradíme vrcholem reprezentujícím čerstvou proměnnou q'_{i+1}, kde i je číslo říkající na kolika větvích jsme již předchozí prohledávání ukončili z důvodu nalezení operátoru nutnosti. Začínáme tedy s $i = 0$. Naopak podstrom napojený na odstraněný vrchol reprezentující nutnost je stromem reprezentujícím formuli C'_{i+1}. Postupným procházením všech větvení až do případného nalezení vrcholu reprezentujícího nutnost získáme pro jisté l formule $B', C'_1, \ldots, C'_l$, pro které platí

$$A(p) = B'[\Box C'_1, \ldots, \Box C'_l],$$

navíc v B' se nemůže p vyskytovat, neboť jsme vždy dříve narazili na operátor nutnosti a případný podstrom obsahující p jsme přesunuli do nějakého C'_i. Jednotlivé C'_i se nám tedy ani nepřekrývají, mohou být však stejné a navíc



Obrázek 4: Strom formule $\Box p \to \neg\Box\Box p$ a strom formule $\Box(\Box p \wedge p)$

se v některých pochopitelně vůbec nemusí vyskytovat p. Upravme tedy postupně naše B' tak, aby ani jedna z těchto variant nastat nemohla. Nejprve projděme jednotlivá $\Box C'_i$, pokud neobsahují p, zasubstituujeme je zpátky do B' za q'_i. Poté pro všechna $i < j$ a formule $C'_i(p)$ a $C'_j(p)$ splňující $C'_i = C'_j$ vybereme například pouze C'_i a v doposud upraveném B' nahraďme všechny výskyty proměnné q'_j proměnnou q'_i. Nakonec zbyde pro nějaké $k \leq l$ množina q'_i a $C'_i(p)$ taková, že z nich lze pouze změnou označení, kterou provedeme i v B' a získáme tedy B, získat posloupnosti $q_1, \ldots, q_k$ a $C_1(p), \ldots, C_k(p)$ pro které platí

$$A(p) = B[\Box C_1, \ldots, \Box C_k]$$

a navíc spňují všechny podmínky pro k-rozklad formule $A(p)$. Q.E.D.

Znovu připomeňme, že k-rozložitelnost bude hrát dále v textu významnou roli, zastavme se tedy ještě u její konstrukce podrobněji. Ukažme nejprve, že rozklad formule nemusí být jednoznačný.

Příklad 2.1.1. Uvažujme formuli $A(p) = \Box p \to \neg\Box\Box p$, její stromová reprezentace je na obrázku 4. Umožňuje dva různé rozklady:

1. $B_1 = q \to \neg\Box q$ a $C(p) = p$, pak evidentně $A(p) = B_1[\Box C(p)]$,
2. $B_2 = q_1 \to \neg q_2$, $C_1 = p$ a $C_2 = \Box p$, pak znovu snadno dostáváme $A(p) = B_2[\Box C_1(p), \Box C_2(p)]$.

Poznamenejme, že postup použitý v důkazu lemmatu 2.1.1 nám pro formuli $\Box p \to \neg\Box\Box p$ dá druhou variantu rozkladu. Při hledání pevných bodů

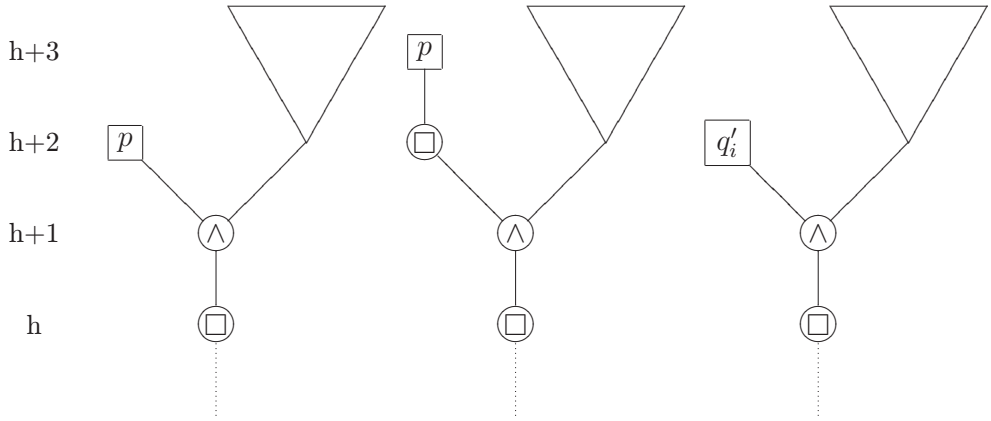
však bude výhodné použít rozklad s co možná nejmenším počtem C_i, to náš postup tedy nezabezpečuje. Popišme proto novou konstrukci, která pro danou formuli najde z tohoto pohledu optimální rozklad.

Stačí pozměnit postup použitý v důkazu věty. Ten tedy postupně prochází strom reprezentující formuli od kořene a zastaví se u prvního operátoru nutnosti, nazvěme tento algoritmus[4] kROZLmax. Navrhněme ještě jeden algoritmus, který se od předešlého liší tím, že se nezastaví u prvního operátoru nutnosti, na který narazí, ale naopak postupuje do maximální hloubky, tedy rozkládá formuli i přes operátory nutnosti a až když narazí na výrokový atom p, pak se vrátí zpět k poslednímu operátoru nutnosti na příslušné větvi, kterým vedla cesta do p. Zatímco předchozí algoritmus mohl formuli rozkládat do hloubky, tedy měla-li formule tvar $B \wedge C$, mohl rozkládat jednotlivé větve podstromu patřícímu B tak dlouho, dokud nenarazil na první operátor nutnosti a to samé pak mohl dělat s podstromem patřícím formuli C a výsledek prohledávání prvního podstromu nijak neovlivnil prohledávání druhého podstromu[5], tak nový algoritmus musí poté, co přejde přes první vrchol reprezentující operátor nutnosti pracovat do šířky – tedy po hladinách. Tím zabráníme zbytečnému procházení. Uvažme například formuli $\Box(\Box p \wedge p)$, reprezentovanou stromem na obrázku 4. Po překročení prvního operátoru nutnosti získáme podstrom formule $\Box p \wedge p$. Nyní již prohledáváme do šířky, tedy přechod na další hladinu vede k tomu, že musíme zkontrolovat, zda se na ní nevyskytuje p. V našem případě algoritmus musí rozložit konjunkci a překontrolovat, zda se oba konjunkty liší od p, což není pravda a tedy se vrátí zpátky v rozkládání k poslednímu operátoru nutnosti a získáme tedy zpět $\Box(\Box p \wedge p)$. V našem příkladu jsme narazili na p okamžitě, u komplikovanějších formulí to však takto jednoduché být nemusí, proto při rozkládání do hloubky musíme na každé hladině překontrolovat, zda jsme již někde nedospěli k p.

Postup je jasný, jedinou komplikací, kterou si musíme vyjasnit, je, jak přesně se budeme chovat při nalezení p, když prohledáváme do šířky. Uvažujme první strom z obrázku 5. Když na hladině $(h + 2)$ narazíme na p, vrátíme se k nejbližšímu vrcholu reprezentujícímu nutnost, ten je na hladině h, a nahradíme ho proměnnou q_i'. V našem případě tedy z celého podstromu zbyde v B' jediný vrchol q_i' a celý podstrom na obrázku 5 začínající konjunkcí na hladině $(h + 1)$ se stane formulí C_i'. Uvažujme teď druhý strom na

[4] Měli bychom mluvit spíše o konstrukci či pseudoalgoritmu, mělo by však býti jasné, jak uvedený postup implementovat například na počítači, a proto si dovolíme používat označení algoritmus.

[5] Samozřejmě necháváme stranou, že číslování q_i' respektive C_i' a případné následné úpravy formule tak, abychom splnili podmínky k-rozložitelnosti, toto nesplňují. Z pohledu toho, co chceme demostrovat, to však není podstatné.



Obrázek 5: Algoritmus kROZLmin

obrázku 5. Nenajdeme-li v pravém podstromu na hladině $(h+2)$ proměnnou p, dostaneme se na hladinu $(h+3)$, kde narazíme na levé větvi na p a vrátíme se k nejbližšímu operátoru nutnosti. Ten je tentokráte na hladině $(h+2)$ a nahradíme ho proměnnou q_i' a za formuli C_i' dosadíme p. Ve výpočtu pak pokračujeme třetím stromem na obrázku 5. Uvědomme si však, že prohledávání pravého podstromu začínajícího na hladině $(h+2)$ a nalezení p v něm může v tomto případě vynutit až návrat k operátoru nutnosti na hladině h, tedy q_i' se může dostat do nějaké C_j', $i < j$. Neboť se do C_j' může dostat pouze tak, že je tam přesunuto, nevyskytuje se tedy vůbec v konečné podobě B'. Při sestavování konečného řešení k-rozkladu z našeho doposud nalezeného pseudořešení musíme toto vzít v úvahu. Naopak si uvědomme, že algoritmus sám o sobě již zaručuje, že žádný člen nemůže být bez výskytu p. Tuto možnost již nemusíme kontrolovat. Stačí tedy kontrolovat pro všechna i, zda se q_i' nevyskytuje v nějakém C_j', $i < j$, a pokud ano, tak C_i' dosadíme za q_i' do C_j'. Nyní ještě musíme, stejně jako v předchozím případě, ošetřit duplicitní C_i' a vytvořit posloupnost k členů $q_1, \ldots, q_k$ a $C_1(p), \ldots, C_k(p)$ pro které platí

$$A(p) = B[\Box C_1, \ldots, \Box C_k]$$

a které splňují všechny podmínky pro k-rozklad formule $A(p)$. Tento druhý algoritmus nazvěme kROZLmin. Názvy algoritmů ospravedlňuje následující lemma, které jinými slovy říká, že algoritmus kROZLmax vytváří takový rozklad, že velikost formulí $\Box C_i(p)$ je maximální a u algoritmu kROZLmin naopak minimální možná.

Lemma 2.1.2. *Nechť $A(p)$ je formule, v níž se p vyskytuje pouze v modálním kontextu a*

$$A(p) = B\left[\Box C_1(p), \ldots, \Box C_n(p)\right]$$

je libovolný její rozklad. Uvažujme rozklad nalezený algoritmem kROZLmax

$$A(p) = B'\left[\Box C'_1(p), \ldots, \Box C'_m(p)\right]$$

a rozklad nalezený algoritmem kROZLmin

$$A(p) = B''\left[\Box C''_1(p), \ldots, \Box C''_l(p)\right],$$

pak platí, že pro libovolné $1 \leq i \leq n$ je $\Box C_i$ podformulí $\Box C'_j$ pro nějaké $1 \leq j \leq m$ a naopak pro libovolné $1 \leq k \leq l$ je $\Box C''_k$ podformulí $\Box C_i$ pro nějaké $1 \leq i \leq n$.

Důkaz. Nejprve uvažujme libovolný člen rozkladu $\Box C_i(p)$ a jeho pozici ve formuli $A(p)$. Uvážíme-li strom reprezentující formuli $A(p)$, pak není-li již sama $\Box C_i(p)$ součástí rozkladu nalezeného algoritmem kROZLmax, pak budeme-li se pohybovat směrem ke kořeni, musíme narazit na uzel, který je kořenem nějaké formule $\Box C'j$. Stejným postupem, budeme-li se naopak pohybovat směrem k listům, dokážeme i druhé tvrzení. Q.E.D.

Předchozí lemma nám omezuje prostor, který musíme projít, abychom nalezli co možná nejmenší rozklad. Uvažujme libovolnou formuli $\Box C''_k$ nalezenou pomocí kROZLmin, pak k ní patří jednoznačně určená formule $\Box C'_j$ nalezená pomocí kROZLmax. Je to ta formule, ke které se dostaneme, vyjdeme-li od $\Box C''_k$ a budeme se vracet zpět přes jednotlivé operátory nutnosti. Samozřejmě nevylučujeme, že $\Box C''_k = \Box C'_j$. Uvědomme si, že pokud narazíme při zpětném průchodu na operátor nutnosti, získali jsme vlastně nového kandidáta[6] pro rozklad. Hledáme-li nejmenší rozklad, stačí tedy uvážit všechny takové formule. Uvědomme si také, že mezi $\Box C''_k$ a $\Box C'_j$ jich

[6]Tím, že jsme získali jeden jiný člen rozkladu C_i, mohli jsme vlastně získat úplně jiné členy i pro ostatní i, neboť tento nový člen mohl umožnit nebo naopak zabránit některým duplicitám mezi C'_j, a tedy zcela změnit počet členů rozkladu. Právě tato vlastnost nás nutí zkoušet mnoho možností, protože dopředu nevíme, jaké duplicity nám která varianta umožní. Je však snadným pozorováním, že máme-li deterministický algoritmus dávající pro dva shodné stromy shodný výsledek a postupujeme-li od listů, má smysl zkoušet pouze takové mezikroky, ve kterých se nám „spojí“ dva podstromy z vyšší hladiny, přičemž oba obsahují p. Lepší algoritmus autorovi zatím není znám. Konkrétně například na obrázku 4 je ve stromě pro formuli $\Box p \rightarrow \neg\Box\Box p$ vyznačen prostor pro prohledávání dvojitým kolečkem. Podle naší poznámky je jasné, že na pravé větvi o variantě, kdy je $C_2 = \Box p$, nemá smysl uvažovat, neboť je možná varianta $C_2 = p$ a pokud má algoritmus výše uvedené vlastnosti, pak i v předchozích případech preferoval druhou variantu, a tedy ji také vybral a případné duplicity mohou vzniknout pouze vzhledem k ní. Tímto omezením jsme k-rozložitelnost

může být nejvýše tolik, jaká je modální hloubka formule $A(p)$. Navíc v algoritmu kROZLmin, který dává rozklad $A(p) = B'[\Box C'_1(p), \ldots, \Box C'_m(p)]$, je m omezeno počtem výskytů p v $A(p)$ či m můžeme omezit počtem modalizovaných podformulí formule $A(p)$, což je zároveň také horní odhad na k-rozložitelnost. Pro nalezení minimálního rozkladu je tedy potřeba vyzkoušet nejvýše $\mathsf{depth}_{\mathsf{M}}(A(p))^{\mathsf{subfl}_{\mathsf{M}}(A(p))}$ variant rozkladů.

Ještě jednou zmiňme, že je možno pro libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, provést horní odhad na k pro její k-rozložitelnost vzhledem k p. Nepochybně musí být k menší nebo rovno počtu modalizovaných podformulí formule, protože nemůže být více formulí tvaru $\Box C_i(p)$ a také musí být menší než počet výskytů proměnné p ve formuli, protože znovu nemůže být více formulí $\Box C_i(p)$, neboť p se musí v každé z nich vyskytovat.

Lemma 2.1.3. *Mějme formuli $A(p)$ a libovolný její k-rozklad, pak platí*

$$k \leq \mathsf{subfl}_{\mathsf{M}}(A(p)),$$
$$k \leq \textit{počet výskytů } p \textit{ v } A(p).$$

Nyní bychom mohli počítat časovou i prostorovou složitost algoritmu. Museli bychom se tedy zaobírat reprezentací stromů a operacemi s nimi. To však dělat nebudeme, neboť následující příklad ukáže, že obecně stejně nemůžeme počítat s tím, že by nám byť ideální rozklad zlepšil odhad u složitosti algoritmů pro hledání pevného bodu. Můžeme tedy vzít buď algoritmus kROZLmin nebo především algoritmus kROZLmax, které v závislosti na složitosti práce se stromy mají nízkou složitost a použít jejich výsledek. Ukažme tedy, že existují netriviální formule, jejichž rozložitelnost dokonce přímo odpovídá velikosti formule a je přesně počtem jejich modálních podformulí.

Příklad 2.1.2. Uvažujme formule tvaru

$$\Box(p \vee q_1) \wedge \Box(p \vee q_2) \wedge \ldots \wedge \Box(p \vee q_n),$$

nemohli zvýšit. Jediné, co jsme mohli pokazit, je zvýšená složitost formule B na úkor zjednodušení C_i, to nám ale příliš nevadí. Rozhodující je pro nás totiž pro jaké k je formule k-rozložitelná, složitost výsledné formule B a formulí C_i má pochopitelně také svůj význam, ale jak uvidíme později s ohledem na naše odhady nijak zásadní.

Upozorněme také, že i zdánlivě jednoduchá 1-rozložitelnost vyžaduje potenciálně zkoušení řady variant. Mohlo by se totiž zdát, že algoritmus kROZLmin již pro každou 1-rozložitelnou formuli nalezne její 1-rozklad. To však není pravda, stačí uvážit například formuli

$$\Box(\Box p \vee \Box(\neg p \wedge q)) \rightarrow \neg\Box\Box(\Box p \vee \Box(\neg p \wedge q)),$$

pro kterou nenalezne 1-rozklad ani kROZLmax.

$$\Box(p \wedge q_1) \vee \Box(p \wedge q_2) \vee \ldots \vee \Box(p \wedge q_n).$$

Taková formule je evidentně pouze n-rozložitelná, dokonce až na eventuální permutace C_i jednoznačně. Délka těchto formulí je evidentně $\mathcal{O}(n)$, počet jejich modálních podformulí právě n a jsou navíc právě n-rozložitelné. Protože však lze díky lemmatu 1.3.1 distribuovat operátor nutnosti přes konjunkci oběma směry, můžeme k první formuli získat (ještě po drobné úpravě) ekvivalentní formuli

$$\Box(p \vee (q_1 \wedge q_2 \wedge \ldots \wedge q_n)),$$

která je 1-rozložitelná. U druhé formule existuje také ekvivalentní formule, která je 1-rozložitelná a to

$$\Box p \wedge (\Box q_1 \vee \Box q_2 \vee \ldots \vee \Box q_n).$$

Jak se ukáže, sestrojovat pevné body 1-rozložitelných formulí je mnohem jednodušší než n-rozložitelných s velkým n. Tedy ani optimální rozklad nám nemusí přinést optimální výpočet. Mohli bychom totiž výpočet provést pro jednodušší ekvivalentní formuli a sestrojený pevný bod je nepochybně i pevným bodem každé s ní dokazatelně ekvivalentní formule.

2.2 Jednoznačnost pevných bodů

Nejprve ukažme jednoduché tvrzení: libovolná formule E splňující parametry pro pevný bod formule $A(p)$, která je dokazatelně ekvivalentní s nějakým pevným bodem D formule $A(p)$, je také pevným bodem formule $A(p)$.

Lemma 2.2.1. *Nechť $A(p)$ a B jsou libovolné modální formule, pro které platí*

$$\mathsf{GL} \vdash B \equiv A(B),$$

pak pro libovolnou formuli C dokazatelně ekvivalentní s B platí

$$\mathsf{GL} \vdash C \equiv A(C).$$

Důkaz. Z předpokladu věty víme, že

(10)	$\mathsf{GL} \vdash B \equiv C,$	
(11)	$\vdash \boxdot(B \equiv C),$	lemma 1.3.3,
(12)	$\vdash \boxdot(B \equiv C) \to A(B) \equiv A(C),$	lemma 1.3.7,
(13)	$\vdash A(B) \equiv A(C),$	(11), (12),
(14)	$\vdash B \equiv A(B),$	
(15)	$\vdash B \equiv A(C),$	(13), (14),
	$\vdash C \equiv A(C),$	(10), (15).

Q.E.D.

Z předchozího lemmatu nyní již snadno plyne požadovaný důsledek:

Důsledek 2.2.2. *Nechť B je pevným bodem formule $A(p)$, pak pro libovolnou formuli C dokazatelně ekvivalentní s B, ve které se vyskytují pouze výrokové proměnné z $A(p)$ kromě p, platí, že C je pevným bodem $A(p)$.*

Mnohem zajímavější je však platnost opačného tvrzení, tedy že libovolné dva pevné body jsou spolu ekvivalentní. Tentokrát však na rozdíl od předchozího případu požadujeme, aby se p vyskytovalo v $A(p)$ pouze v modálním kontextu. Důkaz provádíme podle [Smo85] syntakticky, ale mohli bychom ho pochopitelně vésti i sémanticky.

Věta 2.2.3 (o jednoznačnosti pevných bodů)**.** *Nechť se p vyskytuje v $A(p)$ pouze v modálním kontextu a q je nová proměnná, pak platí*

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \wedge \boxdot(q \equiv A(q)) \to p \equiv q.$$

Důkaz. Díky předpokladům o p existuje n, pro které je $A(p)$ n-rozložitelná, a tedy $A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)]$, kde v $B[q_1, \ldots, q_n]$ se p vůbec nevyskytuje.

Uvažujme nyní libovolnou formuli $C_i(p)$, druhé substituční lemma 1.3.8 nám dává

$$\mathsf{GL} \vdash \Box(p \equiv q) \to \Box(C_i(p) \equiv C_i(q)) \tag{16}$$

a body (iv) a (v) lemmatu 1.3.5 nám navíc umožňují odvodit $\Box E \to \boxdot\Box E$, v našem případě tedy

$$\begin{aligned} &\vdash \Box(C_i(p) \equiv C_i(q)) \to \boxdot\Box(C_i(p) \equiv C_i(q)), \\ &\vdash \Box(C_i(p) \equiv C_i(q)) \to \boxdot(\Box C_i(p) \equiv \Box C_i(q)), \quad \text{lemma 1.3.1.} \end{aligned} \tag{17}$$

Z (16) a (17) již snadno dostaneme

$$\vdash \Box(p \equiv q) \to \boxdot(\Box C_i(p) \equiv \Box C_i(q)) \tag{18}$$

a nyní stačí uvážit první substituční lemma 1.3.7 na formuli $B[q_1, \ldots, q_n]$ a dostáváme

$$\vdash \Box(p \equiv q) \to A(p) \equiv A(q). \tag{19}$$

Teď již přistoupíme k důkazu tvrzení věty. Z (19) snadno přepsáním několika ekvivalencí dostáváme

(20)
$$\begin{aligned}
&\vdash (p \equiv A(p)) \wedge (q \equiv A(q)) \to \Box(p \equiv q) \to (p \equiv q), \\
&\vdash \Box(p \equiv A(p)) \wedge \Box(q \equiv A(q)) \to \Box(\Box(p \equiv q) \to (p \equiv q)), && \text{Nec, 1.3.1,} \\
&\vdash \Box(p \equiv A(p)) \wedge \Box(q \equiv A(q)) \to \Box(p \equiv q), && \text{AxL,} \\
&\vdash \boxdot(p \equiv A(p)) \wedge \boxdot(q \equiv A(q)) \to p \equiv q, && (20).
\end{aligned}$$

Q.E.D.

Důsledek 2.2.4. *Nechť se p vyskytuje ve formuli $A(p)$ pouze v modálním kontextu, pak libovolné dva její pevné body jsou ekvivalentní.*

Díky lemmatu 1.3.6, neboť operátor nutnosti lze distribuovat přes konjunkci oběma směry, či prostudováním důkazu věty snadno dostáváme následující podobu předchozí věty.

Důsledek 2.2.5. *Nechť se p vyskytuje ve formuli $A(p)$ pouze v modálním kontextu a q je nová proměnná, pak platí*

$$\mathsf{GL} \vdash \Box(p \equiv A(p)) \wedge \Box(q \equiv A(q)) \to \Box(p \equiv q).$$

Poznamenejme znovu, že podmínka na p je důležitá, v poznámce pod čarou 2 jsme diskutovali pevné body formule $A(p) = p$. Těmi jsou jak konstanta $\top$, tak i $\bot$ a jsou tedy evidentně neekvivalentní.

Předpokládejme nyní na chvilku platnost věty o existenci pevných bodů. Tu dokážeme o něco později, v jejím důkazu však nebudeme nijak využívat následující lemma, které je přímým zobecněním věty 2.2.3 o jednoznačnosti pevných bodů až na dokazatelnou ekvivalenci. Toto zobecnění by šlo také dokazovat podobně jako věta 2.2.3, my však uvádíme jiný důkaz podle [Lin06].

Lemma 2.2.6. *Pro libovolné n a všechna $1 \leq i \leq n$ a $1 \leq j \leq n$ mějme formule $A_i(p_1, \ldots, p_n)$, ve kterých se všechna p_j vyskytují pouze v modálním kontextu. Pak pro libovolné $D_1, \ldots, D_n$ a $E_1, \ldots, E_n$, jestliže*

$$\begin{aligned}
&\mathsf{GL} \vdash D_i \equiv A_i(D_1, \ldots, D_n), && 1 \leq i \leq n, \\
&\mathsf{GL} \vdash E_i \equiv A_i(E_1, \ldots, E_n), && 1 \leq i \leq n,
\end{aligned}$$

pak platí

$$\mathsf{GL} \vdash D_i \equiv E_i, \qquad 1 \leq i \leq n.$$

Důkaz. Mějme tedy libovolné $D_1, \ldots, D_n$ a $E_1, \ldots, E_n$ splňující předpoklady věty. Pro důkaz stačí ukázat posloupnost formulí $F_1, \ldots, F_n$ splňující

$$\mathsf{GL} \vdash F_i \equiv A_i(F_1, \ldots, F_n), \qquad 1 \leq i \leq n,$$

a především

$$\mathsf{GL} \vdash F_i \equiv D_i, \qquad 1 \leq i \leq n.$$

Neboť $D_1, \ldots, D_n$ jsou libovolné platí tedy také

$$\mathsf{GL} \vdash F_i \equiv E_i, \qquad 1 \leq i \leq n,$$

a tedy také požadované

$$\mathsf{GL} \vdash D_i \equiv E_i, \qquad 1 \leq i \leq n.$$

Důkaz povedeme indukcí podle n, nechť nejprve $n = 1$, pak stačí užít standardní větu 2.2.3 o jednoznačnosti pevných bodů.

Nechť tedy $n > 1$ a předpokládejme, že pro $n - 1$ již tvrzení platí. Nyní, neboť všechna p_j se vyskytují ve všech A_i pouze v modálním kontextu, můžeme použít větu o existenci pevných bodů a její $n-1$ násobnou aplikací pro každé $1 \leq i < n$ získáme formule $G_i(p_n)$, pro které platí

$$\mathsf{GL} \vdash G_i(p_n) \equiv A_i(G_1(p_n), \ldots, G_{n-1}(p_n), p_n), \qquad 1 \leq i < n, \tag{21}$$

a ještě jednou aplikací věty o existenci pevných bodů, tentokráte na formuli $A_i(G_1(p_n), \ldots, G_{n-1}(p_n), p_n)$ získáváme

$$\mathsf{GL} \vdash G_n \equiv A_n(G_1(G_n), \ldots, G_{n-1}(G_n), G_n). \tag{22}$$

Hledané formule $F_1, \ldots, F_n$ definujme

$$F_i =_{def} \begin{cases} G_i(G_n), & 1 \leq i < n, \\ G_n, & i = n. \end{cases}$$

Ukažme, že opravdu mají požadované vlastnosti. Z předpokladu věty máme

$$\mathsf{GL} \vdash D_i \equiv A_i(D_1, \ldots, D_n), \qquad 1 \leq i \leq n, \tag{23}$$

a tedy D_n, pro které

$$\mathsf{GL} \vdash D_n \equiv A_n(D_1, \ldots, D_n). \tag{24}$$

Nyní dosaďme toto D_n za p_n do (21) a dostáváme

$$\mathsf{GL} \vdash G_i\left(D_n\right) \equiv A_i\left(G_1\left(D_n\right), \ldots, G_{n-1}\left(D_n\right), D_n\right), \qquad 1 \leq i < n. \tag{25}$$

Uvažujme nyní formule $A_i\left(p_1, \ldots, p_{n-1}, D_n\right)$, na ně lze použít induktivní hypotézu a z (23) a (25) tedy dostáváme

$$\mathsf{GL} \vdash D_i \equiv G_i\left(D_n\right), \qquad 1 \leq i < n, \tag{26}$$

a z toho a z (24) pak díky prvnímu substitučnímu lemmatu 1.3.7 platí

$$\mathsf{GL} \vdash D_n \equiv A_n\left(G_1\left(D_n\right), \ldots, G_{n-1}\left(D_n\right), D_n\right). \tag{27}$$

Nyní však z (22) a (27) snadno vidíme, že D_n a G_n jsou pevné body formule $A_n\left(G_1\left(p_n\right), \ldots, G_{n-1}\left(p_n\right), p_n\right)$, a jsou tedy dokazatelně ekvivalentní díky standardní větě 2.2.3 o jednoznačnosti pevných bodů. Uvědomme si navíc, že F_n jsme definovali jako G_n. Máme tedy

$$\mathsf{GL} \vdash D_n \equiv G_n \equiv F_n.$$

Navíc z ekvivalence D_n a G_n lze znovu díky prvnímu substitučnímu lemmatu 1.3.7 v libovolné formuli „nahradit“ D_n formulí G_n při zachování dokazatelnosti, to použijeme na (26). Navíc, neboť F_i pro $1 \leq i < n$ jsme definovali jako $G_i\left(G_n\right)$, dostaneme

$$\mathsf{GL} \vdash D_i \equiv G_i\left(G_n\right) \equiv F_i, \qquad 1 \leq i < n.$$

Q.E.D.

Jak se později ukáže, lze navíc opakovaným užitím věty o pevných bodech vždy $D_1, \ldots, D_n$ požadované v předchozím lemmatu sestrojit, a tedy až na dokazatelnou ekvivalenci je právě jedna posloupnost takových formulí.

2.2.1 Metamatematické důsledky

Věta o jednoznačnosti pevných bodů má svoje metamatematické důsledky. Pro tyto účely bývá zvykem používat ji spíše v podobě důsledku 2.2.5, kde operátor nutnosti snadno interpretujeme jako dokazatelnost. My však metamatematické důsledky ukážeme přímo na větě 2.2.3. Uvažujme nějaký aritmetický překlad $\star$ pro který platí $\varphi_1 = \star(p), \varphi_2 = \star(q), \psi(\overline{\varphi_1}) = \star(A(p))$

a $\psi(\overline{\varphi_2}) = \star(A(q))$. Nyní jestliže se p respektive q vyskytuje v $A(p)$ respektive $A(q)$ pouze v modálním kontextu, pak z aritmetické korektnosti GL a z důsledku 2.2.5 dostáváme

$$\mathsf{PA} \vdash \mathrm{Pr}_\pi(\overline{\varphi_1 \equiv \psi(\overline{\varphi_1})}) \wedge \mathrm{Pr}_\pi(\overline{\varphi_2 \equiv \psi(\overline{\varphi_2})}) \to \mathrm{Pr}_\pi(\overline{\varphi_1 \equiv \varphi_2}).$$

Z věty 2.2.3 naopak dostáváme

(28)
$$\mathsf{PA} \vdash (\varphi_1 \equiv \psi(\overline{\varphi_1})) \wedge \mathrm{Pr}_\pi(\overline{\varphi_1 \equiv \psi(\overline{\varphi_1})}) \wedge (\varphi_2 \equiv \psi(\overline{\varphi_2})) \wedge \mathrm{Pr}_\pi(\overline{\varphi_2 \equiv \psi(\overline{\varphi_2})}) \to \varphi_1 \equiv \varphi_2.$$

Mějme tedy autoreferenční rovnici $\varphi \equiv \psi(\overline{\varphi})$ pro nějakou aritmetickou formuli $\psi(x)$, která je vyjádřitelná takovou modální formulí $A(p)$ logiky GL, že se v ní p vyskytuje pouze v modálním kontextu. Nazvěme takové autoreferenční rovnice v souladu s [Šv02] *gödelovské*. Jinak bychom je mohli definovat jako autoreferenční rovnice pro aritmetické formule, ve kterých se proměnná x vyskytuje pouze vázaná predikátem Pr_π, a fakticky tedy pouze uvnitř jistého numerálu. Pojem *gödelovských* autoreferenčních rovnic pochopitelně snadno rozšíříme i na aritmetické formule s více parametry. Vezměme si jako příklad právě Gödelovu formuli $\psi(x)$, kterou můžeme v GL interpretovat jako $\neg\Box p$. Předpokládejme, že máme dvě řešení φ_1, φ_2 autoreferenční rovnice pro Gödelovu formuli $\psi(x)$, a tedy platí

$$\mathsf{PA} \vdash \varphi_1 \equiv \psi(\overline{\varphi_1}),$$
$$\mathsf{PA} \vdash \varphi_2 \equiv \psi(\overline{\varphi_2}).$$

Z podmínky (D1) pro dokazatelnost okamžitě dostáváme

$$\mathsf{PA} \vdash \mathrm{Pr}_\pi(\overline{\varphi_1 \equiv \psi(\overline{\varphi_1})}),$$
$$\mathsf{PA} \vdash \mathrm{Pr}_\pi(\overline{\varphi_2 \equiv \psi(\overline{\varphi_2})}).$$

Nyní stačí použít (28) a získáváme

$$\mathsf{PA} \vdash \varphi_1 \equiv \varphi_2,$$

neboli libovolná dvě řešení autoreferenční rovnice pro Gödelovu formuli $\psi(x)$ jsou spolu dokazatelně ekvivalentní. V tomto konkrétním případě jsme to již vědeli z Druhé Gödelovy věty, předchozí postup však platí pro všechny gödelovské autoreferenční rovnice, a tedy všechna řešení těchto autoreferenčních rovnic jsou až na dokazatelnou ekvivalenci jednoznačná. To však neznamená, že všechny aritmetické formule mají jednoznačné řešení. Takové tvrzení totiž neplatí. V článku [GS79] je o jisté variantě Rosserovy formule dokázáno, že řešení její autoreferenční rovnice nejsou jednoznačná. Omezení na gödelovské formule je tedy podstatné.

2.3 Existence pevných bodů

Stěžejním tématem naší práce je věta o existenci pevných bodů. V této části ukážeme, že ji lze vyslovit dvojím způsobem a zároveň ukážeme, že za daných okolností jsou oba způsoby ekvivalentní.

Věta 2.3.1 (VARIANTA 1)**.** *Pro libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, existuje formule D, obsahující pouze výrokové atomy z $A(p)$ a neobsahující p, pro kterou platí*

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \to (p \equiv D).$$

Ukážeme, že splňuje-li pevný bod D podmínku z předchozí věty, splňuje i silnější podmínku. Nejprve konstatujme jednoduché lemma, ke kterému potřebujeme následující jednoduchou definici:

Definice 2.3.1. Mějme kripkovský model $\mathcal{K} = \langle W, R, \Vdash\!- \rangle$ a vrchol $w \in W$, *kripkovským podmodelem generovaným vrcholem w* nazvěme kripkovský model $\mathcal{K}_w = \langle W_w, R_w, \Vdash\!-_w \rangle$, kde

$$W_w = \{u; u = w \vee wRu\},$$
$$R_w = R \cap (W_w \times W_w),$$
$$u \Vdash\!-_w q \equiv u \Vdash\!- q \text{ a } u \in W_w.$$

Lemma 2.3.2. *Mějme libovolné kripkovské modely $\mathcal{K} = \langle W_\mathcal{K}, R_\mathcal{K}, \Vdash\!-_\mathcal{K} \rangle$ a $\mathcal{L} = \langle W_\mathcal{L}, R_\mathcal{L}, \Vdash\!-_\mathcal{L} \rangle$ a jejich vrcholy $w \in W_\mathcal{K}$ respektive $u \in W_\mathcal{L}$, pak je-li podmodel modelu $\mathcal{K}$ generovaný vrcholem w izomorfní podmodelu modelu $\mathcal{L}$ generovaného vrcholem u, platí pro libovolnou formuli B*

$$w \Vdash\!-_\mathcal{K} B, \text{ právě tehdy když } u \Vdash\!-_\mathcal{L} B.$$

Důkaz probíhá indukcí podle složitosti formule, je však více než jasný, proto ho neuvádíme. Podrobnosti lze případně nalézt například v [Boo93].

Teď již můžeme přistoupit k zesílení podmínky z věty 2.3.1. V důkazu budeme často používat předchozí lemma a ne vždy to budeme explicitně zmiňovat, z kontextu by to však mělo býti jasné. Postupujeme podle [Boo93].

Lemma 2.3.3. *Nechť D neobsahuje p, pak pro libovolnou formuli $A(p)$ platí, jestliže*

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \to (p \equiv D),$$

pak také

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \equiv \boxdot(p \equiv D).$$

Důkaz. Podle lemmatu 1.3.6 kdykoliv máme $\mathsf{GL} \vdash \boxdot B \to C$, pak platí také $\mathsf{GL} \vdash \boxdot B \to \boxdot C$. Pro důkaz $\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \equiv \boxdot (p \equiv D)$ tedy stačí ukázat $\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to (p \equiv D)$ a $\mathsf{GL} \vdash \boxdot (p \equiv D) \to (p \equiv A(p))$. Pro dokončení důkazu lemmatu tedy potřebujeme ukázat, že kdykoliv

$$\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to (p \equiv D),$$

pak již

$$\mathsf{GL} \vdash \boxdot (p \equiv D) \to (p \equiv A(p)).$$

Důkaz provedeme kontrapozicí. Předpokládáme tedy, že máme kripkovský protipříklad $\mathcal{K} = \langle \mathcal{W}, \mathcal{R}, \Vdash_{\mathcal{K}} \rangle$, ve kterém neplatí $\boxdot(p \equiv D) \to (p \equiv A(p))$. Mějme nějaký jeho svět $w \in W$ takový, že $\mathcal{K}$-$\mathsf{rank}(w)$ je minimální a

$$\begin{aligned} &w \Vdash_{\mathcal{K}} \boxdot(p \equiv D), \\ &w \nVdash_{\mathcal{K}} p \equiv A(p). \end{aligned} \tag{29}$$

Protože jsme w volili minimální, a protože ve w je splněno $\boxdot(p \equiv D)$, musí pro každý vrchol v dosažitelný z w platit

$$\begin{aligned} &v \Vdash_{\mathcal{K}} \boxdot(p \equiv D), \\ &v \Vdash_{\mathcal{K}} p \equiv A(p). \end{aligned}$$

Sestrojme nyní model $\mathcal{L} = \langle \mathcal{W}, \mathcal{R}, \Vdash_{\mathcal{L}} \rangle$, který se od $\mathcal{K}$ liší pouze tím, že ve vrcholu w změníme definici splňování p, tedy

$$w \Vdash_{\mathcal{L}} p, \text{ právě tehdy když } w \nVdash_{\mathcal{K}} p.$$

Ve všech ostatních případech je definice splňování $\Vdash_{\mathcal{L}}$ shodná s $\Vdash_{\mathcal{K}}$. Díky tomu, že se ve formuli $A(p)$ vyskytuje p pouze v modálním kontextu, můžeme se na $A(p)$ dívat jako na výrokovou kombinaci proměnných různých od p a formulí tvaru $\Box C$, v nichž se již p může vyskytovat. Protože pro všechny výrokové proměnné různé od p je splňování v $\mathcal{K}$ i $\mathcal{L}$ stejné, mají-li se tedy modely $\mathcal{K}$ a $\mathcal{L}$ lišit splňováním $A(p)$ ve vrcholu w, musí se lišit splňováním nějaké podformule tvaru $\Box C$. O jejím splňování ve w však rozhodují všechny vrcholy dosažitelné z w. V nich je ale splňování v $\mathcal{K}$ i $\mathcal{L}$ definována naprosto stejně a z lemmatu 2.3.2 se tedy nemohou lišit splňováním žádné formule. Tedy všechny formule tvaru $\Box C$ jsou splněny ve w v modelu $\mathcal{K}$, právě tehdy když jsou splněny v $\mathcal{L}$. Tedy pro oba modely platí, že se neliší splňováním

formule $A(p)$ ve vrcholu w[7]. Víme však, že ve vrcholu w modelu $\mathcal{K}$ není splněno $p \equiv A(p)$, z definice splňování p v modelu $\mathcal{L}$ ale dostáváme, že ve vrcholu w modelu $\mathcal{L}$ je naopak $p \equiv A(p)$ splněno. Neboť se $\mathcal{K}$ s $\mathcal{L}$ neliší splňováním ve všech vrcholech dosažitelných z w a ve všech takových vrcholech v $\mathcal{K}$ je splněno $p \equiv A(p)$, máme

$$w \Vdash_{\mathcal{L}} \Box(p \equiv A(p)),$$

a tedy pokud by

$$w \Vdash_{\mathcal{L}} \Box(p \equiv A(p)) \to (p \equiv D),$$

pak bychom měli

$$w \Vdash_{\mathcal{L}} p \equiv D.$$

Protože se však v D nevyskytuje p, neliší se $\mathcal{K}$ a $\mathcal{L}$ jeho splňováním, a tím spíše ve w. Splňováním p se však ve w liší, musí se tedy ve w lišit i splňováním $p \equiv D$, my jsme však vycházeli z (29), tedy

$$w \Vdash_{\mathcal{K}} \Box(p \equiv D),$$

což je spor. Musí tedy být

$$w \nVdash_{\mathcal{L}} \Box(p \equiv A(p)) \to (p \equiv D),$$

což jsme chtěli ukázat. Q.E.D.

S ohledem na to, že již máme dokázánu větu o jednoznačnosti pevných bodů, která říká

$$\mathsf{GL} \vdash \Box(p \equiv A(p)) \wedge \Box(q \equiv A(q)) \to p \equiv q, \tag{30}$$

pak dokážeme-li, že existuje D splňující „standardní podobu“ věty o pevných bodech

$$\vdash D \equiv A(D), \tag{31}$$

máme již

$$\vdash \Box(p \equiv A(p)) \to (p \equiv D),$$

[7]Poznamenejme, že nic neříkáme o splňování v případných vrcholech, ze kterých je dosažitelný vrchol w, tam uvedená vlastnost pochopitelně platit nemusí.

neboť stačí uvážit substituci D do (30) za q a získáme

$$\vdash \boxdot(p \equiv A(p)) \wedge \boxdot(D \equiv A(D)) \rightarrow p \equiv D. \tag{32}$$

Z (31) a z lemmatu 1.3.3 máme

$$\vdash \boxdot(D \equiv A(D)) \tag{33}$$

a teď již snadno z (32) a (33) získáváme

$$\vdash \boxdot(p \equiv A(p)) \rightarrow (p \equiv D).$$

Dokažme, že lze postupovat i obráceně, a tedy obě znění věty o pevných bodech jsou za daných podmínek navzájem ekvivalentní.

Věta 2.3.4 (VARIANTA 2)**.** *Pro libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, existuje formule D obsahující pouze výrokové atomy z $A(p)$ a neobsahující p, pro kterou platí*

$$\mathsf{GL} \vdash D \equiv A(D).$$

Důkaz. Formule $A(p)$ splňuje předpoklady první varianty věty 2.3.1 o pevných bodech, a tedy existuje formule D požadovaných vlastností, pro kterou platí

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \rightarrow (p \equiv D)$$

a z lemmatu 2.3.3 tedy máme

$$\vdash \boxdot(p \equiv A(p)) \equiv \boxdot(p \equiv D).$$

Nyní můžeme substituovat D za p a získáme

$$\vdash \boxdot(D \equiv A(D)) \equiv \boxdot(D \equiv D),$$

kde pravá strana ekvivalence je evidentně vždy pravdivá a z definice silné nutnosti již okamžitě dostáváme hledané

$$\vdash D \equiv A(D).$$

Q.E.D.

Ukázali jsme tedy, že obě znění věty o pevných bodech jsou navzájem ekvivalentní.

Ukažme nyní, že lze znění věty o existenci pevných bodů zobecnit v tom smyslu, v jakém bylo lemma 2.2.6 zobecněním věty o jednoznačnosti pevných bodů.

Lemma 2.3.5. *Pro libovolné n a všechna $1 \leq i \leq n$ a $1 \leq j \leq n$ mějme formule $A_i(p_1, \ldots, p_n)$, ve kterých se všechna p_j vyskytují pouze v modálním kontextu. Pak existují formule $D_1, \ldots, D_n$, pro které platí*

$$\mathsf{GL} \vdash D_i \equiv A_i(D_1, \ldots, D_n), \qquad 1 \leq i \leq n.$$

Důkaz. Tvrzení prokážeme indukcí. Pro $n = 1$ jde o standardní větu o existenci pevných bodů. Nyní předpokládejme platnost tvrzení pro n a snažme se dokázat tvrzení pro $n + 1$. Máme tedy $n + 1$ formulí

$$A_i(p_1, \ldots, p_n, p_{n+1}), \qquad 1 \leq i \leq n + 1,$$

a v každé z nich se proměnné $p_1, \ldots, p_n, p_{n+1}$ vyskytují pouze v modálním kontextu. Nyní můžeme použít indukční předpoklad na prvních n formulí a proměnné $p_1, \ldots, p_n$ a dostáváme n částečných pevných bodů $D'_i(p_{n+1})$, pro které platí

(34)
$$\mathsf{GL} \vdash D'_i(p_{n+1}) \equiv A_i(D'_1(p_{n+1}), \ldots, D'_n(p_{n+1}), p_{n+1}), \qquad 1 \leq i \leq n.$$

Nyní můžeme do formule $A_{n+1}(p_1, \ldots, p_n, p_{n+1})$ dosadit za jednotlivé proměnné $p_1, \ldots, p_n$ formule $D'_1(p_{n+1}), \ldots, D'_n(p_{n+1})$ a dostáváme formuli

$$A_{n+1}(D'_1(p_{n+1}), \ldots, D'_n(p_{n+1}), p_{n+1}),$$

na kterou lze použít standardní větu o pevných bodech a dostaneme pevný bod D_{n+1}, pro který platí

(35)
$$\mathsf{GL} \vdash D_{n+1} \equiv A_{n+1}(D'_1(D_{n+1}), \ldots, D'_n(D_{n+1}), D_{n+1}).$$

Ostatní formule D_i definujme jako

$$D_i =_{def} D'_i(D_{n+1}), \qquad 1 \leq i \leq n.$$

Nyní stačí uvážit substituce D_{n+1} za p_{n+1} do (34), platnost (35) a předchozí definici. Okamžitě dostáváme požadované

$$\mathsf{GL} \vdash D_i \equiv A_i(D_1, \ldots, D_n, D_{n+1}), \qquad 1 \leq i \leq n+1.$$

Q.E.D.

K předchozímu postupu se ještě vrátíme. Na podobném principu bude založena jedna z našich metod pro počítání pevných bodů.

Nejčastěji je v literatuře věta o existenci pevných bodů dokazována pomocí Craigovy věty o interpolaci. To má tu výhodu, že důkaz je jednoduchý a věta o interpolaci je důležitá i sama o sobě.

Věta 2.3.6 (Craigova interpolační)**.** *Pro libovolné formule E a F, pro které platí*

$$\mathsf{GL} \vdash E \to F,$$

existuje formule G, nazýváme ji interpolant, ve které se vyskytují pouze proměnné společné E a F, pro kterou platí

$$\mathsf{GL} \vdash E \to G \text{ a } \mathsf{GL} \vdash G \to F.$$

Větu uvádíme bez důkazu, čtenáře odkazujeme na knihy [Šv02, Boo93] či disertaci [Bí07]. Ve výše uvedené literatuře lze také nalézt interpolací jaké formule lze pevný bod získat a pochopitelně také důkaz, že tento interpolant je opravdu pevným bodem. V druhé z citovaných knih je postup trochu odlišný, pomocí věty o interpolaci je dokázána Bethova věta o explicitní definovatelnosti, ze které dostaneme větu o existenci pevných bodů jako jednoduchý důsledek.

Věta 2.3.7 (Bethovská definovatelnost)**.** *Pro libovolnou formuli $E(p)$ a nové proměnné r_1 a r_2 nevyskytující se v $E(p)$ platí, jestliže*

$$\mathsf{GL} \vdash (E(r_1) \wedge E(r_2)) \to (r_1 \equiv r_2),$$

pak existuje formule G obsahující pouze výrokové proměnné z $E(p)$ kromě p, pro kterou platí

$$\mathsf{GL} \vdash E(p) \to (p \equiv G).$$

Pro logiku GL platí, že pro libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, a libovolný konečný model $\mathcal{K}$, ve kterém je splňování omezeno pouze na výrokové proměnné různé od p, umíme splňování rozšířit jednoznačným způsobem tak, aby v $\mathcal{K}$ platilo $p \equiv A(p)$. K této

vlastnosti se ještě vrátíme v lemmatu 3.3.1, kde ji také dokážeme. Nyní z jednoznačnosti takového řešení a z Bethovy věty okamžitě plyne věta o existenci pevných bodů na základě standardních úvah.

Oba výše uvedené postupy mají zásadní nevýhodu, že nám neposkytují konkrétní formuli D, o které bychom mohli tvrdit, že je pevným bodem, tedy že pevný bod nekonstruují, respektive není na první pohled vidět, jak ho z výše uvedeného získat. Máme-li ale konstruktivní důkaz věty o interpolaci, což můžeme mít, pak pevný bod umíme dokonce spočítat i výše uvedeným postupem. My se zde však zkoumáním konstruktivních důkazů věty o interpolaci zabývat nebudeme a pouze konstatujeme, že se taková konstrukce pevných bodů ukazuje značně neefektivní [SV82] a budeme se tedy věnovat algoritmům, které naopak přímo pevné body konstruují.

Na druhou stranu částečně překvapivě, častečně proto, že měl autor již přichystány téměř všechny potřebné podklady, je jediný autorovi této práce známý počítačový program počítající pevné body založen na interpolaci. Jeho autorem je Melvin Fitting a podrobnosti lze nalézt v [Fit96]. Program je psán v programovacím jazyce Prolog a konstruktivní metoda hledání interpolantů je založena na sémantických tabulkách[8]. Autor této práce se snažil pomocí Fittingova programu ověřovat výpočty pevných bodů v této práci uvedené, přesto na řadu z nich, ačkoliv jsou všechny velmi jednoduché, program nenalezl v rozumném čase žádnou odpověď. Naopak se ukazuje, že pro některé zdánlivě složité formule počítá program velmi rychle. Žádné podrobnější zkoumání však autor neprováděl, proto je nutno výše uvedené brát spíše jako poznámku.

2.3.1 Metamatematické důsledky

Již jsme zavedli pojem gödelovských autoreferenčních rovnic a ukázali jsme pomocí věty 2.2.3 o jednoznačnosti pevných bodů v logice GL, že mají až na dokazatelnou ekvivalenci jednoznačná řešení. Nyní můžeme podobně využít i větu o existenci pevných bodů v logice GL. V PA nám říká, že gödelovské autoreferenční rovnice mají vždy řešení. To už jsme ale věděli z věty o autoreferenci. Podstatné je, že taková řešení lze vyjádřit bez použití autoreference, mají tedy explicitní řešení. Pro Gödelovu autoreferenční formuli a Henkinovu autoreferenční formuli, které mluví o své nedokazatelnosti respektive dokazatelnosti, jsme toto již vědeli z Druhé Gödelovy věty respektive z Löbovy

[8]Konkrétně je hledán interpolant formule

$$(p \wedge A(p) \wedge \Box(p \equiv A(p))) \rightarrow (\Box(q \equiv A(q)) \rightarrow (q \vee A(q))).$$

věty. Nyní to víme pro všechny gödelovské autoreferenční rovnice. Navíc, až ukážeme konstrukci pevných bodů, budeme umět taková řešení i explicitně vypočítat. Všechny příklady uvedené dále v textu lze tedy chápat nejen jako hledání pevných bodů jistých formulí v logice dokazatelnosti GL, ale také jako hledání explicitního řešení jistých autoreferenčních rovnic v PA.

2.4 Jiné logiky než GL

Můžeme se samozřejmě ptát, zda platí věta o pevných bodech také v jiných logikách než je GL. Takovou otázku lze zdůvodnit několika způsoby, jedním z nich může být zkoumání „nestandardních“ predikátů dokazatelnosti respektive zkoumání dokazatelnosti v „nestandardních“ teoriích. Z triviálních důvodů pochopitelně věta o pevných bodech platí ve všech logikách silnějších než GL, tedy například i v Solovayově [Sol76] systému GL^{ω}[9]. Přesto bychom i takové případy mohli z rozumných důvodů zkoumat. Zajímavé by například mohlo být, zda se pevné body v takových systémech výrazně nezjednodušší. My se však budeme pouze velmi stručně zabývat vlastností existence pevných bodů i v jiných modálních logikách než je GL. Ukážeme logiky nad modálním systémem K, které mají vlastnost existence pevných bodů. Zároveň se také zmíníme o pevných bodech v bimodálních logikách.

2.4.1 Logiky nad systémem K

V této části stručně ukážeme několik výsledků Lorenza Sacchetiho týkajících se vlastnosti existence pevných bodů v modálních logikách. Čtenáře lze odkázat na trojici článků [Sac99, Sac01, Sac02], ze kterých vycházíme. Autorův zájem o danou problematiku vychází ze zkoumání „nestandardních“ predikátů dokazatelnosti, které splňují větu o autoreferenci. K tomuto zkoumání využívá různé modální logiky nad systémem K. Ve všech případech totiž předpokládá přijetí podmínek pro dokazatelnost D1 a D2.

Uvažme logiku K rozšířenou o axiom $\Box A \equiv A$. Víme, že pokud přidáme tento axiom k logice GL, získáme spornou teorii. Stačí si uvědomit, že formule implikuje formuli $\Box A \to A$ a uvážit například instanci $\Box\bot \to \bot$. Použitím pravidla necesitace Nec a Löbova axiomu AxL totiž dostáváme, že je dokazatelné $\Box\bot$ a stačí znovu použít výchozí instanci a získáváme $\bot$. Vraťme se zpět k logice K s přidaným axiomem $\Box A \equiv A$. Tato logika nemá vlastnost

[9] Ten získáme, prohlásíme-li všechny dokazatelné formule logiky GL za axiomy. To můžeme, neboť GL je rozhodnutelná a dostáváme tak rekurzivní množinu axiomů. Přidáme axiom reflexe, tedy $\Box A \to A$, a systém uzavřeme pouze na pravidlo modus ponens. Nikoliv však na necesitaci, výsledný systém tedy není normální modální logikou. Přesto se dá ukázat, že je úplný vůči standardnímu modelu aritmetiky.

pevných bodů, stačí uvážit formuli $\neg\Box p$, ta je ekvivalentní formuli $\neg p$ a ta z pochopitelných důvodů nemůže mít v bezesporné logice pevný bod.

Naopak rozšíření K o libovolný axiom tvaru $\Box^n\bot$, $n \geq 1$, nám dává logiku s vlastností existence pevných bodů. To samé platí pro logiku K rozšířenou o libovolný z axiomů $\Box(\Box^n A \to A) \to \Box A$, $n \geq 1$. Obě tvrzení lze dokázat pomocí věty o interpolaci v příslušných logikách. To je také obecná metoda, jak lze tvrzení o existenci pevných bodů v příslušné logice získat. Druhé z tvrzení lze v jistém smyslu zesílit, pro naše účely však postačí v této podobě.

Je známo [Boo93], že přidáním axiomu $\Box(\Box A \equiv A) \to \Box A$ k logice K4 získáme logiku GL a naopak přidáním k logice K dostaneme logiku, která je nekompletní vůči své charakteristické třídě. Pro logiku K rozšířenou o libovolný z axiomů $\Box(\Box A^n \equiv A) \to \Box A$, $n \geq 1$, je navíc v [Sac02] ukázáno, že nemá vlastnost pevných bodů. Poznamenejme, že tvrzení lze znovu formulovat silněji.

2.4.2 Bimodální logiky

Vedle standardních modálních logik s jediným modálním operátor nutnosti (možnost bereme pouze jako zkratku) můžeme uvažovat také modální logiky s více modálními operátory. V případě logiky dokazatelnosti tímto způsobem můžeme vyjádřit řadu zajímavých metamatematických vlastností. Nebudeme se pouštět do bližších podrobností, čtenáře odkazujeme na monografie [Smo85, Boo93]. Poznamenejme pouze, že pro některé takové systémy platí věta o pevných bodech. Dokonce díky tomu, že ji v naší práci dokážeme i čistě syntaktickými prostředky, lze v některých systémech po ukázání několika základních vlastností prakticky převzít náš syntaktický důkaz z logiky GL.

3 Speciální případy věty o pevných bodech

V této části ukážeme konstrukci pevných bodů pro formule jistých speciálních tvarů či vlastností. Překvapivě již těmito metodami získáme nástroj pro řešení většiny zajímavých autoreferenčních rovnic.

Uvážíme-li dokazatelné formule v normální modální logice K, jsou všechny dokazatelně ekvivalentní a díky pravidlu necesitace dokonce dokazatelně silně nutně ekvivalentní. Nejde pochopitelně o žádnou speciální vlastnost logiky K, pro nás je však důležité, že ji tím pádem mají i logiky K4 a především GL. Všechny dokazatelné formule jsou tak ekvivalentní formuli $\top$. Nabízí se okamžitě následující jednoduchá věta:

Věta 3.0.1. *Nechť $A(p)$ je dokazatelná formule v logice* K, K4 *respektive* GL*, pak jejím pevným bodem v logice* K, K4 *respektive* GL *je formule $\top$.*

Důkaz. Platnost ukážeme pro logiku K, v ostatních případech postupujeme zcela stejně. Nechť $\mathsf{K} \nvdash \top \equiv A(\top)$, pak, neboť $\mathsf{K} \vdash \top$, musí být $\mathsf{K} \nvdash A(\top)$. To ale nemůže nastat, neboť $A(p)$ je dokazatelná a každá substituční instance dokazatelné formule v K je v K dokazatelná. Q.E.D.

Pro libovolnou „rozumnou“, a tedy i neklesající míru složitosti formule, platí následující jednoduché lemma, které má však pro naše zkoumání poměrně podstatný důsledek.

Lemma 3.0.2. *V logice* K, K4 *respektive* GL *existují dokazatelné formule s neomezenou konečnou délkou, modální hloubkou, počtem podformulí i počtem modalizovaných podformulí.*

Důkaz. Chceme-li sestrojit dokazatelnou formuli délky větší než n, stačí vzít libovolnou formuli A délky alespoň n, ta pro každou rozumnou míru složitosti musí existovat, a uvážit formuli $\Box^{(n+1)}A \to \Box^{(n+1)}A$. Ta má délku určitě větší než n, neboť už A mělo délku větší než n, modální hloubku alespoň $(n+1)$, počet modalizovaných podformulí nejméně $2 \cdot (n+1)$, a tedy i nejméně tolik podformulí. Q.E.D.

Důsledek 3.0.3. *Existují formule s neomezenou konečnou délkou, modální hloubkou, počtem podformulí i počtem modalizovaných podformulí, které mají triviální pevný bod $\top$.*

Získali jsme tedy spodní odhad na složitost pevných bodů formulí, v logice GL ukážeme, že existují i nedokazatelné formule mající pevný bod $\top$, a to například formule $\Box p$, a tím pádem i formule $q \vee \Box p$. Neboť $\Box\top$ je v GL ekvivalentní $\top$, můžeme toto zobecnit i na $\Box^i p$ a $q_1 \vee \ldots \vee q_i \vee \Box p$. Máme

tedy nedokazatelné formule s libovolnou délkou i modální hloubkou, počtem podformulí i modalizovaných podformulí mající triviální pevný bod $\top$.

Poznamenejme, že podobně jako jsme uvažovali o dokazatelných formulích a pevný bodu $\top$, mohli jsme uvažovat také o nesplnitelných formulích a jejich pevném bodu $\bot$.

3.1 Pevné body 1-rozložitelných formulí

Zatím jsme pouze ukázali, že dokazatelné (a případně i nesplnitelné) formule mají pevné body. Nyní ukážeme, jak sestrojit pevné body k 1-rozložitelným formulím. Již nyní poznamenejme, že následující lemma a věta, která je jeho důsledkem, jsou stěžejní pro všechny naše další syntaktické konstrukce pevných bodů. Autorem lemmatu je Sambin [Sam74], který ho však dokázal v trochu silnější podobě, ke které se ještě vrátíme. My uvádíme de Jonghův důkaz podle [Smo85].

Lemma 3.1.1. *Nechť $C(p)$ je libovolná formule, pak $\Box C(\top)$ je pevným bodem $\Box C(p)$.*

Důkaz. Nejprve ukažme implikaci $\Box C(\top) \to \Box C(\Box C(\top))$. Evidentně platí

$$
\begin{array}{lll}
(36) & \mathsf{GL} \vdash \Box C(\top) \to (\top \equiv \Box C(\top)), & \\
 & \quad \vdash \Box\Box C(\top) \to \Box(\top \equiv \Box C(\top)), & \mathit{Nec}, 1.3.1, \\
(37) & \quad \vdash \Box C(\top) \to \Box(\top \equiv \Box C(\top)), & \text{axiom } \mathit{Ax4}, \\
(38) & \quad \vdash \Box C(\top) \to \boxdot(\top \equiv \Box C(\top)), & (36), (37),
\end{array}
$$

použitím (38) a prvního substitučního lemmatu 1.3.7 na formuli $\Box C(p)$ dostáváme

$$
\begin{array}{l}
\vdash \Box C(\top) \to (\Box C(\top) \equiv \Box C(\Box C(\top))), \\
\vdash \Box C(\top) \to \Box C(\Box C(\top)).
\end{array}
$$

Pro druhou implikaci užijeme (38) a z prvního substitučního lemmatu 1.3.7, tentokrát však na formuli $C(p)$, dostáváme

$$
\begin{array}{lll}
(39) & \mathsf{GL} \vdash \Box C(\top) \to (C(\top) \equiv C(\Box C(\top))), & \\
(40) & \quad \vdash (E \to (F \equiv G)) \to (G \to (E \to F)), & \mathit{VL}, \\
 & \quad \vdash C(\Box C(\top)) \to (\Box C(\top) \to C(\top)), & (39), (40), \\
 & \quad \vdash \Box C(\Box C(\top)) \to \Box(\Box(C(\top) \to C(\top))), & \mathit{Nec}, \ 1.3.1, \\
 & \quad \vdash \Box C(\Box C(\top)) \to \Box C(\top), & \text{axiom } \mathit{AxL}.
\end{array}
$$

Celkově tedy máme $\Box C(\top) \equiv \Box C(\Box C(\top))$, což bylo dokázat. Q.E.D.

Důsledek 3.1.2. *Pro libovolnou formuli tvaru $\Box C(p)$ sestrojí předchozí konstrukce pevný bod D, pro který platí*

$$\mathsf{subfl}(D) = \mathsf{subfl}(\Box C(p)),$$
$$\mathsf{depth}_{\mathsf{M}}(D) = \mathsf{depth}_{\mathsf{M}}(\Box C(p)).$$

Důkaz. Stačí si uvědomit, že pevný bod vznikne dosazením konstanty $\top$ do formule za p. Její délka ani modální hloubka se tak nezmění. K sestrojenému pevnému bodu D však pochopitelně může existovat ekvivalentní formule D', která má délku či modální hloubku ostře nižší. Q.E.D.

Ukažme aplikaci předchozího lemmatu.

Příklad 3.1.1 (Henkin)**.** Mějme formuli $A(p) = \Box p$. Předchozí lemma nám říká, že jejím pevným bodem je formule $\Box\top$, která je však v GL ekvivalentní $\top$, a tedy získáváme $D = \top$.

Příklad 3.1.2. Mějme formuli $A(p) = \Box\neg p$. Znovu snadno zjistíme, že jejím pevným bodem je formule $\Box\neg\top$ neboli $\Box\bot$.

V předchozím důkazu jsme při dokazování druhé implikace použili Löbův axiom, důkaz tedy neprojde například v logice $\mathsf{K4}$, což ostatně ukazuje i následující příklad.

Příklad 3.1.3 (Kreisel[10])**.** Mějme formuli $A(p) = \Box(p \to g)$. Jejím pevným bodem je $\Box(\top \to g)$, což je z výrokové logiky ekvivalentní $\Box g$. Platí tedy

$$\mathsf{GL} \vdash \Box g \equiv \Box(\Box g \to g).$$

Ostatně implikace zprava doleva je vlastně Löbův axiom AxL, ale pro něj pochopitelně platí

$$\mathsf{K4} \nvdash \Box(\Box g \to g) \to \Box g.$$

Našli jsme tedy formuli, pro kterou v $\mathsf{K4}$ znění lemmatu neplatí.

Předchozí lemma však lze téměř okamžitě použít k hledání pevných bodů složitějších formulí, neboť následující věta je jeho poměrně přímočarým důsledkem.

Věta 3.1.3. *Nechť $A(p)$ je 1-rozložitelná formule, tedy*

$$A(p) = B[\Box C(p)],$$

pak $A(B[\top])$ je jejím pevným bodem.

[10] Jde o Kreiselovu variantu Löbovy formule.

Důkaz. Uvažme formuli $\Box C\,(B\,[q])$, ta má podle lemmatu 3.1.1 pevný bod $\Box C\,(B\,[\top])$, a tedy platí

$$\mathsf{GL} \vdash \Box C\,(B\,[\top]) \;\equiv\; \Box C\,(B\,[\Box C\,(B\,[\top])])\,.$$

Nyní použitím lemmatu 1.3.3 získáváme

$$\mathsf{GL} \vdash \boxdot\,(\Box C\,(B\,[\top]) \;\equiv\; \Box C\,(B\,[\Box C\,(B\,[\top])]))$$

a můžeme tedy použít první substituční lemma 1.3.7 na formuli $B\,[q]$, což nám dává

$$\mathsf{GL} \vdash B\,[\Box C\,(B\,[\top])] \;\equiv\; B\,[\Box C\,(B\,[\Box C\,(B\,[\top])]]\,. \tag{41}$$

Protože $A\,(p)$ je vlastně $B\,[\Box C\,(p)]$ pouze přepsáním (41) dostáváme požadované

$$\mathsf{GL} \vdash A\,(B\,[\top]) \;\equiv\; A\,(A\,(B\,[\top]))\,.$$

Q.E.D.

Důsledek 3.1.4. *Mějme libovolnou* 1*-rozložitelnou formuli* $A(p)$*, pak předchozí konstrukce nalezne pevný bod* D*, pro který platí*

$$\begin{array}{rcccl} \mathsf{subfl}(A(p)) & \leq & \mathsf{subfl}(D) & \leq & \mathsf{subfl}(A(p)) \cdot \mathsf{subfl}(A(p)), \\ \mathsf{depth}_{\mathsf{M}}(A(p)) & \leq & \mathsf{depth}_{\mathsf{M}}(D) & \leq & 2 \cdot \mathsf{depth}_{\mathsf{M}}(A(p)). \end{array}$$

Důkaz. Zabývejme se nejprve horním odhadem délky pevného bodu D. Ten vznikne ve dvou krocích. Nejprve dosazením $\top$ do formule B, ta má délku nejvýše $\mathsf{subfl}(A(p))$. Získáváme formuli B', která má tedy také délku nejvýše $\mathsf{subfl}(A(p))$. Nyní každý výskyt p v $A(p)$ nahradíme formulí B'. Neboť se p vyskytuje v $A(p)$ nejvýše $\mathsf{subfl}(A(p))$-krát, získáváme již požadovaný odhad[11]. Pro spodní odhad délky pevného bodu D okamžitě vidíme, že ji náš postup nemůže snížit, pokud tedy pochopitelně v průběhu neprovádíme záměny jednoduššími ekvivalentními formulemi.

Při určování horního odhadu modální hloubky pevného bodu budeme postupovat jako v předchozím kroku, akorát si uvědomíme, že oba odhady nenásobíme, nýbrž sčítáme. Pro dolní odhad znovu evidentně platí, že bez zjednodušení v průběhu výpočtu se modální hloubka nemůže snížit. Q.E.D.

[11] Počet výskytů p v $A(p)$ bychom mohli odhadnout lépe například výrazem $\frac{\mathsf{subfl}(A(p))}{2}$. To vyplývá z toho, že se p vyskytuje v $A(p)$ pouze v modálním kontextu a z úvah o tom, kolik z délky formule zabírají logické spojky a operátory. Jde však pouze o konstantní zrychlení, proto vystačíme s jednodušším odhadem.

S využitím předchozí věty nyní můžeme ukázat pevné body dalších zajímavých formulí.

Příklad 3.1.4 (Gödel)**.** Mějme $A(p) = \neg\Box p$, pak je $B = \neg q_1$ a $C_1(p) = p$, pevným bodem je tedy po dosazení $\neg\top = \bot$ do $A(p)$ formule $\neg\Box\bot$.

Příklad 3.1.5 (Löb [Smo79])**.** Mějme $A(p) = \Box p \to g$, pak je $B = q_1 \to g$ a $C_1(p) = p$, tentokráte dosazujeme do $A(p)$ formuli $\top \to g = g$, a tedy dostáváme pevný bod $\Box g \to g$.

Pokusme se dále rozšířit třídu formulí, pro které umíme jednoduchým způsobem hledat pevné body i na formule, které jsou n-rozložitelné pro $n > 1$, ale mají jistý speciální tvar.

Nechť pro $n \geq 1$ existuje n-rozklad

$$A\left(p\right) = B\left[\Box C_1\left(p\right), \ldots, C_n\left(p\right)\right]$$

takový, že v $B\left[q_1, \ldots, q_n\right]$ se kromě výrokových atomů $q_1, \ldots, q_n$, výrokových konstant a operátoru nutnosti vyskytuje pouze konjunkce, pak existuje k $A\left(p\right)$ ekvivalentní formule $A'\left(p\right)$, která je 1-rozložitelná, neboť díky lemmatu 1.3.1 platí

$$\mathsf{GL} \vdash \Box E \wedge \Box F \to \Box\left(E \wedge F\right), \tag{42}$$

a tedy lze postupnou aplikací (42) distribuovat operátor nutnosti tolikrát, až získáme formuli $A'\left(p\right)$ v požadovaném tvaru a pro ni již pomocí věty 3.1.3 jednoduše nalezneme její pevný bod a snadno dostáváme, že platí

$$D \equiv A'(D) \equiv A(D),$$

a tedy nalezený pevný bod formule $A'\left(p\right)$ je i pevným bodem formule $A\left(p\right)$.

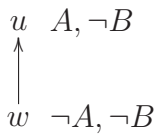
Distribuce operátoru nutnosti tímto způsobem však neplatí pro ostatní spojky, proto nelze použít tuto konstrukci k nalezení pevného bodu obecné formule.

3.2 Téměř nutné formule

V této části ukážeme, že pevné body lze snadno určovat i pro formule jiného tvaru než jsou pouze 1-rozložitelné formule. Výklad vedeme podle [Smo79], přestože klíčové lemma pochází od Sambiniho.

Definice 3.2.1. O libovolné formuli A řekneme, že je *téměř nutná*, jestliže platí

$$\mathsf{GL} \vdash A \to \Box A.$$



Obrázek 6: Kripkovský protipříklad

Již jsme ukázali, že uvedený vztah obecně neplatí. Ukažme, že přesto existuje třída formulí, pro které platí. Definujeme ji induktivně.

Lemma 3.2.1. *Pro libovolnou formuli A jsou všechny formule $\bot, \top, \Box A$ i $\boxdot A$ téměř nutné.*

Důkaz. Tvrzení věty okamžitě vyplývá, napíšeme-li si podmínky, které je potřeba ověřit:

$$\begin{aligned}
&\mathsf{GL} \vdash \bot \to \Box\bot,\\
&\mathsf{GL} \vdash \top \to \Box\top,\\
&\mathsf{GL} \vdash \Box A \to \Box\Box A,\\
&\mathsf{GL} \vdash (A \wedge \Box A) \to \Box(A \wedge \Box A).
\end{aligned}$$

Q.E.D.

Lemma 3.2.2. *Jsou-li formule A a B téměř nutné, pak jsou téměř nutné i formule $A \wedge B$ a $A \vee B$.*

Důkaz. Tvrzení znovu snadno dostáváme, stačí si uvědomit, že podle lemmatu 1.3.1 platí

$$\begin{aligned}
&\mathsf{GL} \vdash (\Box A \wedge \Box B) \to \Box(A \wedge B),\\
&\mathsf{GL} \vdash (\Box A \vee \Box B) \to \Box(A \vee B).
\end{aligned}$$

Q.E.D.

Poznamenejme navíc, že pro libovolnou téměř nutnou formuli A platí

$$\mathsf{GL} \vdash A \equiv \boxdot A.$$

Naopak téměř nutné formule nejsou uzavřeny na implikaci ani na negaci, stačí uvážit kripkovský protipříklad na obrázku 6 a formule $A \to B$ a $\neg A$ v kořeni w.

Získali jsme tedy množinu formulí uzavřenou na konjunkci a disjunkci. Navíc, neboť libovolná formule $\Box C$ je také téměř nutná, je níže uvedená věta zesílením lemmatu 3.1.1. Nejprve však dokažme stěžejní lemma.

Lemma 3.2.3. *Nechť $A(p)$ je libovolná téměř nutná formule, ve které se p vyskytuje pouze v modálním kontextu, pak pro libovolné formule E a F platí*

$$\mathsf{GL} \vdash A(E) \to E \equiv F \Rightarrow \mathsf{GL} \vdash A(E) \equiv A(F).$$

Důkaz. Předpokládejme tedy, že platí

$$\mathsf{GL} \vdash A(E) \to E \equiv F, \tag{43}$$

musíme dokázat dvě implikace:

1) $\mathsf{GL} \vdash A(E) \to A(F)$:

$$\mathsf{GL} \vdash \Box A(E) \to \Box(E \equiv F), \qquad (43), Nec, 1.3.1,$$

nyní využijeme toho, že A je téměř nutná, tedy

$$\mathsf{GL} \vdash A(E) \to \Box(E \equiv F), \tag{44}$$
$$\mathsf{GL} \vdash A(E) \to \boxdot(E \equiv F), \qquad (43), (44), \tag{45}$$

z (45) a prvního substitučního lemmatu 1.3.7 na formuli $A(p)$ získáváme

$$\mathsf{GL} \vdash A(E) \to A(E) \equiv A(F),$$
$$\mathsf{GL} \vdash A(E) \to A(F).$$

2) $\mathsf{GL} \vdash A(F) \to A(E)$:

Využijeme předpokladu, že se p vyskytuje v $A(p)$ pouze v modálním kontextu. Pro nějaké n tedy existuje n-rozklad $A(p)$, neboli formule $B[q_1, \ldots, q_n], C_1(p), \ldots, C_n(p)$, pro které platí

$$A(p) = B[\Box C_1(p), \ldots, C_n(p)].$$

Použitím (45) a prvního substitučního lemmatu 1.3.7 na libovolnou formuli $C_i(p)$ dostáváme

$$\mathsf{GL} \vdash A(E) \to C_i(E) \equiv C_i(F),$$
$$\mathsf{GL} \vdash \Box A(E) \to \Box C_i(E) \equiv \Box C_i(F), \qquad Nec, 1.3.1, \tag{46}$$
$$\mathsf{GL} \vdash \Box A(E) \to \Box(\Box C_i(E) \equiv \Box C_i(F)), \qquad 1.3.2, \tag{47}$$
$$\mathsf{GL} \vdash \Box A(E) \to \boxdot(\Box C_i(E) \equiv \Box C_i(F)), \qquad (46), (47),$$

můžeme tedy na všechny $\Box C_i(p)$ pro p rovno E respektive F použít první substituční lemma 1.3.7 na formuli $B[q_1, \ldots, q_n]$ a dostáváme

$$\mathsf{GL} \vdash \Box A(E) \to (A(E) \equiv A(F)),$$
$$\mathsf{GL} \vdash \Box A(E) \to (A(F) \to A(E)),$$

nyní použijeme výrokovou tautologii $(K \to (L \to M)) \to (L \to (K \to M))$ a máme

$$\begin{array}{lll} (48) & \mathsf{GL} \vdash A(F) \to (\Box A(E) \to A(E)), & \\ & \mathsf{GL} \vdash \Box A(F) \to \Box(\Box A(E) \to A(E)), & \mathit{Nec}, 1.3.1, \end{array}$$

znovu použijeme, že $A(p)$ je téměř nutná, tedy

$$\begin{array}{lll} & \mathsf{GL} \vdash A(F) \to \Box(\Box A(E) \to A(E)), & \\ (49) & \mathsf{GL} \vdash A(F) \to \Box A(E)), & \text{Löbův axiom } \mathit{Ax}L, \\ & \mathsf{GL} \vdash A(F) \to A(E), & (48), (49). \end{array}$$

Q.E.D.

Věta 3.2.4. *Nechť $A(p)$ je libovolná téměř nutná formule, ve které se p vyskytuje pouze v modálním kontextu, pak formule $D = A(\top)$ je jejím pevným bodem.*

Důkaz. Použitím lemmatu 3.2.3 pro $E = \top$ a $F = A(\top)$ dostáváme

$$\mathsf{GL} \vdash A(\top) \to \top \;\equiv\; A(\top) \;\Rightarrow\; \mathsf{GL} \vdash A(\top) \;\equiv\; A(A(\top)),$$

nyní si jen stačí uvědomit, že platí

$$\mathsf{GL} \vdash A(\top) \to \top \;\equiv\; A(\top).$$

Q.E.D.

Důsledek 3.2.5. *Nechť $A(p)$ je libovolná téměř nutná formule ve které se p vyskytuje pouze v modálním kontextu, pak podle předchozí konstrukce má $A(p)$ pevný bod D, pro který platí*

$$\begin{aligned} \mathsf{subfl}(D) &= \mathsf{subfl}(A(p)), \\ \mathsf{depth}_{\mathsf{M}}(D) &= \mathsf{depth}_{\mathsf{M}}(A(p)). \end{aligned}$$

Důkaz. Dosazením konstanty $\top$ do formule $A(p)$ se délka formule ani její modální hloubka nezmění. Q.E.D.

Vraťme se k lemmatům 3.2.1 a 3.2.2 definujícím třídu téměř nutných formulí. Víme, že všechny formule tvaru $\Box C$ jsou téměř nutné a navíc téměř nutné formule jsou uzavřené na disjunkci a konjunkci. Platí proto následující snadné důsledky.

Důsledek 3.2.6. *Mějme libovolnou formuli $A(p)$ jednoho z následujících tvarů*

$$A(p) = \bigvee_{i=1}^{n} \Box C_i(p),$$
$$A(p) = \bigwedge_{i=1}^{n} \Box C_i(p),$$
$$A(p) = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \Box C_{i,j}(p),$$
$$A(p) = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m} \Box C_{i,j}(p),$$

pak $D = A(\top)$ je jejím pevným bodem.

Poznamenejme, že podmínka na výskyt p pouze v modálním kontextu je skryta ve tvaru $A(p)$, neboť p se vyskytuje pouze ve formulích $\Box C_i(p)$ respektive $\Box C_{i,j}(p)$.

Později ukážeme, že uvedený výsledek nelze zlepšit v tom smyslu, že by pevný bod obecné formule $E \wedge F$ nebo $E \vee F$ byl konjunkcí respektive disjunkcí pevných bodů formulí E a F.

Ukažme aplikaci předchozích tvzení na několika formulích.

Příklad 3.2.1. V příkladu 2.1.2 jsme uvažovali o k-rozložitelnosti následujících formulí

$$\Box(p \vee q_1) \wedge \Box(p \vee q_2) \wedge \ldots \wedge \Box(p \vee q_n),$$
$$\Box(p \wedge q_1) \vee \Box(p \wedge q_2) \vee \ldots \vee \Box(p \wedge q_n),$$

nyní snadno dostáváme, že pevným bodem první z nich je formule

$$\Box(\top \vee q_1) \wedge \Box(\top \vee q_2) \wedge \ldots \wedge \Box(\top \vee q_n),$$

která je evidentně ekvivalentní $\top$ a pevným bodem druhé je formule

$$\Box(\top \wedge q_1) \vee \Box(\top \wedge q_2) \vee \ldots \vee \Box(\top \wedge q_n),$$

kterou můžeme zjednodušit na

$$\Box(q_1) \vee \Box(q_2) \vee \ldots \vee \Box(q_n).$$

Příklad 3.2.2. Podle lemmatu 3.2.1 je i každá formule tvaru $\boxdot E$ téměř nutnou, uvažme tedy formuli $A(p) = \neg\Box p \wedge \Box\neg\Box p$, neboli $A(p) = \boxdot\neg\Box p$. Jejím pevným bodem D je formule $\boxdot\neg\Box\top$, kterou lze snadno zjednodušit na $\bot$.

Získali jsme tedy další třídu formulí, pro které umíme velmi efektivně určit pevné body.

3.3 Pevné body bez parametrů

Většina známých a používaných metamatematických formulí hovořících o dokazelnosti v jisté formální teorii, které můžeme převést do logiky GL, abychom spočítali jejich pevný bod, je tvořena pouze jediným výrokovým atomem. Neboť se tento jediný atom v pevném bodu nevyskytuje, nevyskytuje se v něm žádný výrokový atom, a mluvíme tedy o pevných bodech bez parametrů.

Klíčové pozorování pro konstrukci pevných bodů bez parametrů vystihuje následující lemma. Dokážeme ho v obecnější podobě, než bychom momentálně potřebovali, později se nám to však bude hodit.

Lemma 3.3.1. *Nechť $A(p)$ je libovolná formule, ve které se p vyskytuje pouze v modálním kontextu a $\mathcal{K} = \langle W, R, \Vdash\!\!- \rangle$ je libovolný konečný stromový kripkovský model, ve kterém je definováno splňování všech výrokových atomů z $A(p)$ kromě p. Pak lze $\Vdash\!\!-$ jednoznačně rozšířit na $\Vdash\!\!-_p$ tak, aby pro libovolný vrchol $w \in W$ platilo*

$$w \Vdash\!\!-_p p, \text{ právě tehdy když } w \Vdash\!\!- A(p),$$

a tedy pro libovolný vrchol $v \in W$ platí

$$v \Vdash\!\!- \boxdot(p \equiv A(p)).$$

Důkaz. Nejprve pro všechny vrcholy $w \in W$ a všechny výrokové proměnné $q_1, \ldots, q_k$ z $A(p)$ kromě p definujeme

$$w \Vdash\!\!-_p q_i, \text{ právě tehdy když } w \Vdash\!\!- q_i.$$

Mějme kořen w stromu $\mathcal{K}$, $\mathcal{K}\text{-}\mathsf{rank}(w) = n$. Pro p dodefinujeme splňování postupně od listů, tedy vrcholů v, jejichž $\mathcal{K}\text{-}\mathsf{rank}(v) = 0$. Využijeme skutečnosti, že se p vyskytuje v $A(p)$ pouze v modální kontextu, tedy pokud se výroková proměnná p v $A(p)$ vyskytuje, je vázána operátorem nutnosti, tedy ve všech takových vrcholech v můžeme určit splněnost $A(p)$ bez ohledu na to, že ve v není definováno splňování p, neboť p se vyskytuje v $A(p)$ pouze v podformulích tvaru $\Box B$. Z libovolného v však není dosažitelný žádný svět, tedy ve v jsou všechny takové podformule triviálně splněné a umíme tedy určit splněnost $A(p)$ ve v prostě ze splněnosti výrokových proměnných $q_1, \ldots, q_k$ ve v a výrokové logiky. Definujme

$$v \Vdash\!\!-_p p, \text{ právě tehdy když } v \Vdash\!\!-_p A(p).$$

Uvažme nyní všechny vrcholy u, $\mathcal{K}\text{-}\mathsf{rank}(u) = 1$. Argument můžeme opakovat s tím rozdílem, že tentokráte pro vrcholy u platí, že jsou z nich dostupné

nějaké vrcholy v. V nich je ale splňování p již definováno, tedy můžeme určit splňování všech podformulí $A(p)$, v nichž se p vyskytuje, neboť jsou tvaru $\Box B$ a na splňování p v u nezáleží. Umíme tedy určit splňování $A(p)$ v u. Znovu definujme

$$u \Vdash\!\!\!-_p p, \text{ právě tehdy když } u \Vdash\!\!\!-_p A(p).$$

Postup můžeme opakovat. Po $n+1$ krocích máme takto definováno splňování p ve všech vrcholech $\mathcal{K}$ a navíc všude je splněno $p \equiv A(p)$, a tedy opravdu pro libovolný vrchol $v \in W$ dostáváme

$$v \Vdash\!\!\!- \boxdot(p \equiv A(p)).$$

Z konstrukce je jasné, že definice je jednoznačná, neboť v žádném kroku jsme splňování p nemohli definovat jinak, protože pak by nebylo splněno $p \equiv A(p)$. Q.E.D.

Co nám předchozí věta říká o formuli $A(p)$, ve které se vyskytuje z výrokových atomů pouze p, a to výhradně v modálním kontextu? Říká nám, že libovolný model $\mathcal{K}$, ve kterém není definováno splňování pro žádný výrokový atom, je v něm tedy pouze definováno splňování konstant $\bot$ a $\top$, umíme rozšířit jednoznačně na model $\mathcal{K}_p$, ve kterém platí $p \equiv A(p)$. Jinými slovy, máme-li libovolný model $\mathcal{L}_p$, ve kterém je definováno pouze splňování p a platí v něm $p \equiv A(p)$, pak ho umíme získat z nějakého modelu $\mathcal{L}$, ve kterém splňování výrokové proměnné p definováno není. Stačí prostě zapomenout splňování p a získáme požadovaný model $\mathcal{L}$, neboť ten umíme jediným způsobem rozšířit na model, ve kterém platí $p \equiv A(p)$, a tím musí být model $\mathcal{L}_p$.

Myšlenka naší konstrukce je následující. Chceme sestrojit formuli D, pro kterou platí

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \to (p \equiv D).$$

Tedy pro libovolný model $\mathcal{K}$ a jeho vrchol w platí

$$w \Vdash\!\!\!- \boxdot(p \equiv A(p)) \to (p \equiv D).$$

Pokud navíc platí

$$w \Vdash\!\!\!- \boxdot p \equiv A(p)), \tag{50}$$

pak musíme zajistit

$$w \Vdash\!\!\!- p \equiv D.$$

Pro konstrukci pevného bodu D nás pochopitelně zajímají právě varianty, kdy ve vrcholu platí (50). Samozřejmě se můžeme zabývat pouze modely, jejichž je w kořenem, pak se podmínka (50) vlastně redukuje na platnost $p \equiv A(p)$ v modelu. Můžeme se tedy zaobírat pouze modely, ve kterých platí $p \equiv A(p)$. Nyní budeme směřovat k tomu, že se můžeme omezit ještě na specifičtější modely, vlastně na jeden model. V něm určíme, ve kterých vrcholech je p splněno, a formuli D definujeme jako popis těchto vrcholů.

Mějme tedy libovolný model $\mathcal{K}$, ve kterém platí $\boxdot(p \equiv A(p))$ a libovolný jeho vrchol w. Chceme ukázat, že splňování formule obsahující pouze výrokové atomy p záleží pouze na $\mathcal{K}$-$\mathsf{rank}(w)$ a nikoliv na tvaru modelu.

Lemma 3.3.2. *Nechť B je formule, ve které se vedle $\top$ a $\bot$ vyskytuje pouze výrokový atom p. Pak pro libovolné dva konečné modely $\mathcal{K} = \langle W_\mathcal{K}, R_\mathcal{K}, \Vdash_\mathcal{K}\rangle$ a $\mathcal{L} = \langle W_\mathcal{L}, R_\mathcal{L}, \Vdash_\mathcal{L}\rangle$, ve kterých platí $p \equiv A(p)$, a libovolné jejich vrcholy $w \in W_\mathcal{K}$ a $u \in W_\mathcal{K}$, pro které platí $\mathcal{K}$-$\mathsf{rank}(w) = \mathcal{L}$-$\mathsf{rank}(u)$, dostáváme*

$$w \Vdash_\mathcal{K} B, \text{ právě tehdy když } u \Vdash_\mathcal{L} B.$$

Důkaz. Neboť modely $\mathcal{K}$ a $\mathcal{L}$ jsou libovolné, stačí dokazovat jednu implikaci, tedy například

$$w \Vdash_\mathcal{K} B \Rightarrow u \Vdash_\mathcal{L} B.$$

Dokazujme dvojitou indukcí, podle $\mathcal{K}$-$\mathsf{rank}(w)$ a podle složitosti formule B. Pro vrchol w, pro který $\mathcal{K}$-$\mathsf{rank}(w) = 0$ tvrzení platí okamžitě, stačí postupovat indukcí podle složitost formule B, to si však s ohledem na jednoduchost tvrzení odpustíme. Připomeňme pouze, že definice splňování p je dána splňováním $A(p)$. Náš vrchol w je listem, v $A(p)$ se p vyskytuje pouze v modálním kontextu, tedy pouze uvnitř formule tvaru $\Box C$. Ty jsou však v listech triviálně splněny. Zbytek je dán pouze výrokovou logikou.

Mějme tedy nějaký vrchol w, pro který platí $\mathcal{K}$-$\mathsf{rank}(w) = n + 1$ a pro všechny vrcholy w' dosažitelné z w již tvrzení platí z indukčního předpokladu, neboť $\mathcal{K}$-$\mathsf{rank}(w') \leq n$. Postupujme indukcí podle složitosti B. Jestliže je $B = \top$ nebo $B = \bot$, stejně jako v případě $B = E \wedge F$, $B = E \vee F$, $B = E \rightarrow F$ i $B = \neg E$ platí tvrzení triviálně.

Předpokládejme tedy, že $B = p$. Splňování p je dáno splňováním $A(p)$, to však kromě výrokové logiky závisí pouze na splňování formulí tvaru $\Box C$, neboť p se vyskytuje v $A(p)$ pouze v modálním kontextu. Pokud je ve w formule $\Box C$ splněna, pak je C splněna ve všech vrcholech w' dosažitelných z w. Protože však $\mathcal{K}$-$\mathsf{rank}(w') \leq n$ platí z indukčního předpokladu také pro všechny vrcholy u' modelu $\mathcal{L}$, pro které $\mathcal{L}$-$\mathsf{rank}(u') \leq n$, že u' splňuje C. Z definice splňování nutnosti v modelu, tedy pro libovolný vrchol u, $\mathcal{L}$-$\mathsf{rank}(u) = n + 1$ dostáváme požadované u splňuje $\Box C$. Nyní nechť naopak

formule $\Box C$ ve w splněna není, pak musí existovat vrchol w' dosažitelný z w, ve kterém není C splněna. Stejným způsobem jako před chvílí dostáváme z indukčního předpokladu také vrchol u' dosažitelný z u, ve kterém není splněna formule C, a tedy v u také není splněna formule $\Box C$. Vrcholy w a u se tedy neliší splňováním formule $A(p)$, a tedy ani splňováním výrokového atomu p.

Poslední případ, který nám zbývá, je $B = \Box C$, ten jsme však již vlastně vyřešili, když jsme se zabývali $B = p$. Q.E.D.

Zaveďme nyní předpokládaným způsobem pojem lineárního kripkovského modelu.

Definice 3.3.1. Kripkovský model $\mathcal{L} = \langle W, R, \Vdash \rangle$ nazveme *lineárním modelem*, právě tehdy když pro libovolné dva vrcholy $v, w \in W$ platí vRw nebo wRv.

Předchozí úvahy a právě dokázané lemma nám vlastně říkají, že se můžeme omezit pouze na lineární kripkovské modely, ve kterých platí $p \equiv A(p)$. Mějme pevně dánu nějakou konečnou hloubku modelu, pak evidentně existuje, až na izomorfismus, právě jeden lineární model, ve kterém není definováno splňování pro žádný výrokový atom. Takový model umíme jednoznačně rozšířit na model, ve kterém platí $p \equiv A(p)$, tedy až na izomorfismus existuje také pouze jeden lineární model pevné konečné hloubky, ve kterém je definováno pouze splňování p a platí v něm $p \equiv A(p)$. Navíc takový lineární model hloubky n obsahuje jako své podmodely všechny modely hloubek $0, \ldots, n$.

Pokud bychom tedy věděli, že se můžeme omezit také na modely jisté maximální hloubky, stačilo by se vlastně pohybovat v jediném modelu. V tom bychom postupně počínaje jeho jediným listem definovali splňování p a mohli z takového modelu vyčíst pevný bod D. Abychom takto mohli postupovat, je pro nás stěžejní následující vlastnost.

Definice 3.3.2. O libovolné formuli B, ve které se vyskytuje pouze výrokový atom p, řekneme, že je *nakonec konstantní řádu* k, jestliže pro libovolný lineární model $\mathcal{L}$, ve kterém platí $p \equiv A(p)$, a libovolné jeho dva vrcholy w a w', pro které $\mathcal{L}\text{-}\mathsf{rank}(w) = k$ a $\mathcal{L}\text{-}\mathsf{rank}(w') > k$, platí

$$w \Vdash B, \text{ právě tehdy když } w' \Vdash B.$$

Jinými slovy, formule B je nakonec konstantní řádu k, právě tehdy když se její splňování v lineárním modelu $\mathcal{L}$, ve kterém platí $p \equiv A(p)$, od jistého vrcholu w, pro který platí $\mathcal{L}\text{-}\mathsf{rank}(w) = k$, pro všechny vrcholy w', pro které $\mathcal{L}\text{-}\mathsf{rank}(w') > k$, nemění.

Lemma 3.3.3. *Libovolná formule $A(p)$, ve které se vyskytuje pouze výrokový atom p, a to výhradně v modálním kontextu, je nakonec konstantní řádu n, kde $n = \mathsf{subfl}_{\mathsf{M}}(A(p))$.*

Důkaz. Z předpokladu věty lze $A(p)$ chápat jako výrokovou složeninu formulí tvaru $\Box C_1, \ldots, \Box C_k$. Zvolme libovolně pevně nějakou formuli $\Box C_i, 1 \leq i \leq k$. Pak mohou nastat dvě varianty. Nejprve jednodušší z nich, nechť

$$\mathsf{GL} \vdash \boxdot(p \equiv A(p)) \rightarrow \Box C_i,$$

pak je $\Box C_i$ nakonec konstantní řádu 0.

Nyní tedy nechť

$$\mathsf{GL} \nvdash \boxdot(p \equiv A(p)) \rightarrow \Box C_i,$$

pak chceme sestrojit kripkovský protipříklad $\mathcal{K}$ s nějakým vrcholem w, ve kterém je splněno $\boxdot(p \equiv (Ap))$, ale není splněno $\Box C_i$. Z věty o stromové úplnosti 1.2.4 a z důsledku 1.2.5 dostáváme omezení na $\mathcal{K}\text{-}\mathsf{rank}(w)$ daný počtem modalizovaných podformulí formule $\boxdot(p \equiv A(p)) \rightarrow C_i$. Připomeneme-li si důkaz věty 1.2.4, zvyšují $\mathcal{K}\text{-}\mathsf{rank}$ pouze formule tvaru $\Box E$, které nejsou v nějakém vrcholu konstruovaného protipříkladu splněny, jenže po formuli $\Box(p \equiv A(p))$ chceme, aby byla splněna všude, tedy ta nám $\mathcal{K}\text{-}\mathsf{rank}$ nezvýší a máme tak $\mathcal{K}\text{-}\mathsf{rank}(w) \leq \mathsf{subfl}_{\mathsf{M}}(A(p))$. To je dáno tím, že všechny modalizované podformule formule $\Box C_i$ jsou zároveň podformulemi $A(p)$. Navíc se při hledání kripkovského protipříkladu na základě úvah, které jsme provedli po důkazu lemmatu 3.3.2, můžeme omezit pouze na lineární modely.

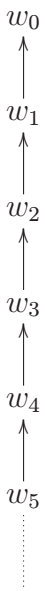
Pro libovolnou podformuli $\Box C_i$ formule $A(p)$ jsme tedy získali, že je nakonec konstantní řádu $\mathsf{subfl}_{\mathsf{M}}(A(p))$, a tedy i celá $A(p)$ je nakonec konstantní řádu $\mathsf{subfl}_{\mathsf{M}}(A(p))$, neboť vzniká z formulí $\Box C_i$ pouze na základě výrokové logiky. Q.E.D.

Nyní již víme všechno, co potřebujeme k výpočtu pevného bodu. Víme, že stačí zkoumat lineární modely s nejvýše $(\mathsf{subfl}_{\mathsf{M}}(A(p)) + 1)$ vrcholy. Stačí tedy uvažovat vlastně pouze jediný lineární model $\mathcal{L}$, jehož kořen má $\mathcal{L}\text{-}\mathsf{rank}$ roven $\mathsf{subfl}_{\mathsf{M}}(A(p))$. Od listu budeme postupně dodefinovávat splňování p a poté se podíváme v jakých vrcholech je p splněno a podle toho sestrojíme pevný bod. Ještě než přesně popíšeme algoritmus, ukažme si obecný výpočet osvětlující celou předchozí konstrukci.

Příklad 3.3.1. Mějme model jako na obrázku 7 a formuli

$$A(p) = \Box(\neg p \rightarrow \Box\bot) \rightarrow \Box(p \rightarrow \Box\bot).$$

Ukažme, jak výpočet probíhá. Budeme postupovat od listu k dalším vrcholům:



Obrázek 7: Kripkovský model

w_0 :
Chceme pochopitelně zjistit, zda ve w_0 je splněna $A(p)$, abychom věděli, jak máme definovat splňování p. Formule $A(p)$ je implikace. Podíváme se nejprve, zda je ve w_0 splněn její sukcedent, pak by byla splněna i celá implikace. Sukcedent je formule $\Box(p \to \Box\bot)$, neboť z w_0 není dosažitelný žádný vrchol, je splněna triviálně, a tedy je splněna i $A(p)$. Definujme

$$w_0 \Vdash p.$$

w_1 :
Znovu zjišťujeme, zda ve w_1 je splněna $A(p)$, zkusíme opět vyjít od sukcedentu, ten je $\Box(p \to \Box\bot)$, tedy v každém dosažitelném vrcholu musí být splněno $p \to \Box\bot$. Dosažitelný vrchol je pouze jeden, a to w_0. V něm je p splněno, ale neboť z něj není dosažitelný žádný vrchol, je v něm splněno i $\Box\bot$. Ve w_1 je tedy splněn sukcedent, a tedy i celá implikace. Znovu definujme

$$w_1 \Vdash p.$$

w_2 :
Postup opakujeme, z předchozího kroku již patrně vysvítá, že tentokráte sukcedent $A(p)$ splněn nebude. Uvažujme jako v minulém kroku.

Dosažitelný vrchol je tentokráte ale i w_1, v něm musí být splněno $p \to \Box\bot$, p v něm je splněno, ale $\Box\bot$ nikoliv, neboť z w_1 je dosažitelný vrchol w_0 a v něm pochopitelně nemůže být splněno $\bot$. Musíme se tedy poprvé zabývat i antecedentem $A(p)$, ten je $\Box(\neg p \to \Box\bot)$, tedy ve všech dosažitelných vrcholech musí být splněno $\neg p \to \Box\bot$, ale neboť ve všech dosažitelných vrcholech, totiž ve w_1 a w_0 není splněno p, je implikace $\neg p \to \Box\bot$ triviálně splněna, a tedy také antecedent $A(p)$ je ve vrcholu w_2 splněn, a tedy celkem $A(p)$ není ve w_2 splněna a definujeme tedy tentokráte

$$w_2 \Vdash\!\!\!\!/\ p.$$

w_3 :
Sukcedent $A(p)$ znovu nebude splněn. Díky tranzitivitě modelu můžeme opakovat stále stejný argument, musíme se tedy znovu zabývat antecedentem. V minulém případě splněn nebyl, neboť nebyl dostupný žádný vrchol, ve kterém by nebylo splněno p, to se však v minulém kroku změnilo. Zkusíme tedy ověřit splněnost implikace $\neg p \to \Box\bot$ ve w_2, jak jsme již řekli $\neg p$ je ve w_2 splněna, ale není v něm splněno $\Box\bot$, neboť z w_2 je dostupný například vrchol w_1, takže $\neg p \to \Box\bot$ ve w_2 není splněna, a tedy antecedent $A(p)$ není splněn ve w_3, a tedy celá formule $A(p)$ je ve vrcholu w_3 splněna a definujeme tedy

$$w_3 \Vdash p.$$

w_4 :
Stejně jako jsme v předchozím kroku poznamenali, že sukcedent $A(p)$ již v žádném dalším vrcholu splněn nebude, můžeme to samé nyní říci i o jejím antecedentu, neboť z tranzitivity lze znovu opakovat argument použitý u w_3. Tedy ve w_4 i v každém dalším vrcholu je určitě splněna $A(p)$, a tedy také definujeme

$$\begin{aligned} w_4 &\Vdash p, \\ w_5 &\Vdash p, \\ &\vdots \end{aligned}$$

Celkově jsme tedy získali, že

$$w \Vdash p, \text{ právě tehdy když } \mathcal{L}\text{-}\mathsf{rank}(w) \neq 2,$$

neboli je roven 0 či 1 nebo 3 a více. To však umíme říci jednoduše formulí. První variantu vystihuje, jak se snadno nahlédne, formule $\Box\Box\bot$ a druhou

variantu formule $\neg\Box\Box\Box\bot$. Definujeme-li tedy D jako $\Box\Box\bot \vee \neg\Box\Box\Box\bot$, pak nepochybně v každém modelu $\mathcal{L}$, ve kterém platí $\boxdot(p \equiv A(p))$, a v libovolném jeho vrcholu w máme

$$p \equiv D,$$

což jsme chtěli.

V příkladu jsme viděli, že umíme sestrojit bezatomární formule, které jsou splnitelné právě ve vrcholech jistého pevného ranku. Základními konstrukčními prvky jsou formule, pro které platí

$$\begin{aligned} w &\Vdash \Box^i\bot, && \text{právě tehdy když } \mathcal{K}\text{-}\mathsf{rank}(w) < i,\\ w &\Vdash \neg\Box^i\bot, && \text{právě tehdy když } \mathcal{K}\text{-}\mathsf{rank}(w) \geq i. \end{aligned}$$

Z výše uvedeného tedy můžeme snadno konstruovat následující varianty

$$\begin{aligned} w &\Vdash \Box^{i+1}\bot \wedge \neg\Box^i\bot, && \text{právě tehdy když } \mathcal{K}\text{-}\mathsf{rank}(w) = i,\\ w &\Vdash \Box^{k+1}\bot \wedge \neg\Box^l\bot, && \text{právě tehdy když } l \leq \mathcal{K}\text{-}\mathsf{rank}(w) \leq k. \end{aligned}$$

Nyní již můžeme přistoupit ke konstrukci konkrétního pevného bodu.

Věta 3.3.4. *Nechť $A(p)$ je formule, ve které se vyskytuje pouze výrokový atom p, a to výhradně v modálním kontextu, pak existuje pevný bod D formule $A(p)$.*

Důkaz. Nechť $n = \mathsf{subfl}_{\mathsf{M}}(A(p))$, uvažujme lineární model $\mathcal{L} = \langle W, R, \Vdash\rangle$, ve kterém platí $p \equiv A(p)$. Navíc uvažujme $W = \{w_0, \ldots, w_n\}$ a pro každé $0 \leq i < j \leq n$ platí $w_j R w_i$. Definujme množinu

$$P = \{k : k \leq n \text{ a } w_k \Vdash p\}.$$

Pevný bod D pro $k, l \geq 0$ nyní definujme jako disjunkci maximálních intervalů. Nejprve pokud v P existuje posloupnost $k, \ldots, n$, pak pro minimální k, tedy nejdelší takovou posloupnost, přidáme do disjunkce člen $\neg\Box^k\bot$ zajišťující splnění v každém vrcholu, jehož rank je alespoň k. Prvky $k, \ldots, n$, pokud taková posloupnost existovala, z P odstraňme. Dále se postarejme o začátek posloupnosti prvků v P, tedy o posloupnost typu $0, \ldots, k$. V takovém případě přidáme do disjunkce člen $\Box^{k+1}\bot$ zajišťující splnění ve všech vrcholech, jejichž rank je menší nebo roven k. Znovu odstraňme případné prvky $0, \ldots, k$ z P. V P nám již mohly zbýt pouze intervaly $k, \ldots, l$, kde $k \neq 0$ a $l \neq n$, navíc platí $k \leq l$. Připouštíme i intervaly, kde $k = l$, tedy jednobodové intervaly. Pro každý takový interval $k, \ldots, l$ v P přidejme do disjunkce konjunkci $\Box^{l+1}\bot \wedge \neg\Box^k\bot$, která je splněna, jestliže rank vrcholu je mezi k a

l včetně. Volme vždy maximální takové intervaly. Pro jednoduchost znovu prvky odstraňujme, končíme tedy s $P = \emptyset$. Definici pevného bodu ještě uveďme přehledně s tím, že poznamenejme, že volíme maximální intervaly a prvky z P, které se již na tvorbě pevného bodu podílely odstraňujeme.

$$D = \bigvee \begin{cases} \neg\Box^k\bot & k, \ldots, n \in P, \\ \Box^{k+1}\bot & 0, \ldots, k \in P, \\ \bigvee(\Box^{k+l+1}\bot \wedge \neg\Box^k\bot), & k, \ldots, (k+l) \in P. \end{cases} \tag{51}$$

Korektnost konstrukce vyplývá z úvah, které jsme již provedli. Q.E.D.

V důkazu jsme tedy pevný bod definovali jako disjunkci jistých intervalů. Poznamenejme, že pokud p není nikde splněno, pak nevybereme ani jeden disjunkt, neboť množina P je prázdná, a tedy výsledný pevný bod je $\bot$ z definice prázdné disjunkce. Naopak pokud je p splněno všude, pak hned v prvním kroku vybereme posloupnost $0, \ldots, n$, a tedy do disjunkce přidáme jediný člen, a to $\neg\Box^0\bot$ neboli $\top$.

Stěžejní ke konstrukci pevného bodu je pochopitelně sestavení množiny P, zbytek konstrukce již tvoří pouze její projití a vytvoření formule podle návodu daného v důkazu. Popišme tedy, jakým způsobem můžeme množinu P získat. Vytvoříme vlastně tabulkovou metodu na její počítání. Vycházíme zde částečně z [Boo93] a částečně z [Smo79].

Mějme bez újmy na obecnosti kripkovský model jako na obrázku 7, tedy s $W = \{w_0, \ldots, w_n\}$, kde $n = \mathsf{subfl}_{\mathsf{M}}(A(p))$ a $w_i R w_j$, právě tehdy když $j < i$. Nyní potřebujeme pro každý vrchol w_i rozhodnout splňování p, tedy splňování $A(p)$. Spočítat splňování $A(p)$ znamená spočítat splňování logického výrazu bez proměnných a splňování podformulí tvaru $\Box C$. Zaveďme si tabulku, která bude pro každou takovou podformuli tvaru $\Box C$ obsahovat sloupce C a $\Box C$ a to tak, že sloupce všech formulí tvaru $\Box C$ jsou před sloupci jejich podformulí C[12]. Přidáme ještě sloupec p, ze kterého získáme množinu P a do kterého budeme počítat splňování $A(p)$, ten v tabulce umístíme mezi formule tvaru $\Box C$ a jejich podformule C. Řádky tabulky očíslujeme $0, \ldots, n$. Toto číslo odpovídá příslušnému vrcholu modelu. Tabulku nyní naplníme hodnotami $\top$ a $\bot$, a to podle toho, zda je formule v příslušném vrcholu splněna či není.

Tabulku jsme koncipovali tak, že chceme-li určit splňování formule v příslušném řádku, stačí použít výrokovou logiku a případně již spočítané výsledky na témže řádku. Jedinou výjimkou jsou formule tvaru $\Box C$, tam mu-

[12] Pro algoritmické zpracování by mohlo býti užitečné, aby se sloupce všech formulí tvaru $\Box C$ nacházely až za případnými sloupci jejich podformulí tvaru $\Box C'$ respektive především, aby toto platilo také pro sloupce formulí C a C'.

	$\Box\bot$	$\Box(\neg p \to \Box\bot)$	$\Box(p \to \Box\bot)$	p	$\bot$	$\neg p \to \Box\bot$	$p \to \Box\bot$
0	$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
1	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\bot$
2	$\bot$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$	$\top$
3	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$
4	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Tabulka 1: Výpočet pevného bodu formule $\Box(\neg p \to \Box\bot) \to \Box(p \to \Box\bot)$.

síme zkontrolovat splňování i na předchozích řádcích. Popišme induktivně, jak naplníme tabulku.

Nultý řádek získáme snadno. Všechny formule tvaru $\Box C$ jsou pochopitelně splněny, označme si je tedy rovnou $\top$. To nám stačí k tomu, abychom z výrokové logiky spočítali splňování $A(p)$, a tedy i p. Ostatní formule tvaru C nezačínající operátorem nutnosti počítáme zleva. To snadno můžeme z výrokové logiky, ze splňování p v nultém řádku a z hodnot formulí tvaru $\Box C'$ na nultém řádku.

Mějme tedy již tabulku naplněnu do řádku i. Chceme určit hodnoty na řádku $i+1$. Klíčové na celé konstrukci je počítání formulí tvaru $\Box C$. Ty záleží pouze na předchozích řádcích. Nejprve se podíváme, zda na předchozím řádku i byla formule $\Box C$ splněna. Pokud nebyla, má tedy hodnotu $\bot$, což znamená, že v nějakém předchozím řádku $j < i$ nebyla splněna formule C. Tedy formule $\Box C$ již nemůže být nikdy splněna a označme si ji tedy znovu $\bot$. Jestliže je však na předchozím řádku i hodnota $\top$, znamená to, že na všech řádcích $j < i$ je u formule C také hodnota $\top$. Jestliže je hodnota $\top$ u C také na řádku i, pak je formule $\Box C$ splněna i na řádku $i+1$ a poznamenáme si do tabulky $\top$. Je-li naopak hodnota u C v řádku i rovna $\bot$, pak si musíme u $\Box C$ v řádku $i+1$ pochopitelně poznamenat $\bot$. Hodnotu $A(p)$ respektive p v řádku $i+1$ nyní snadno získáme z výrokové logiky a hodnot formulí tvaru $\Box C$ na řádku $i+1$. Zbývá nám tedy spočítat hodnotu formulí C, které nezačínají operátorem nutnosti a jsou různé od $A(p)$. Známe již splňování p v řádku $i+1$ i všech formulí tvaru $\Box C'$, k určení splňování C nám tedy stačí pouze výroková logika.

Výše uvedeným způbem umíme zaplnit celou tabulku. Množinu P snadno vyčteme ze sloupce pro p. Ukažme si jednoduchý příklad.

Příklad 3.3.2. Spočítejme pevný bod stejné formule jako v příkladu 3.3.1, tedy formule $A(p) = \Box(\neg p \to \Box\bot) \to \Box(p \to \Box\bot)$. Formule má evidentně

	$\Box p$	$\Box\neg p$	p	p	$\neg p$
0	$\top$	$\top$	$\top$	$\top$	$\bot$
1	$\top$	$\bot$	$\bot$	$\bot$	$\top$
2	$\bot$	$\bot$	$\top$	$\top$	$\bot$

Tabulka 2: Výpočet pevného bodu formule $\Box p \to \Box\neg p$.

pouze tři různé modalizované podformule, tedy bude nám stačit[13], a to $\Box\bot, \Box(\neg p \to \Box\bot)$ a $\Box(p \to \Box\bot)$. Nyní již můžeme přistoupit k výpočtu, který nám ukazuje tabulka 1. Spočítali jsme i řádek 4, abychom ukázali, že se výpočet již opravdu od řádku 3 nezmění. Množina P má prvky $0, 1, 3$ a pevný bod D je tedy podle definice $\neg\Box^3\bot \vee \Box^2\bot$, což můžeme napsat

$$D = \Box\Box\Box\bot \to \Box\Box\bot.$$

Příklad 3.3.3. Mějme formuli $A(p) = \Box p \to \Box\neg p$. Jejími modalizovanými podformulemi jsou $\Box p$ a $\Box\neg p$, stanovme tedy $n = 2$. Výpočet P uvádí tabulka 2. Poznamenejme, že jsme získali dva sloupce obsahující p, neboť p je také zároveň podformulí formule $\Box p$. Z P snadno získáme pevný bod $\neg\Box^2\bot \vee \Box\bot$, který můžeme přepsat lépe jako $\Box\Box\bot \to \Box\bot$.

Zajímavým důsledkem věty o pevných bodech bez parametrů je věta o normální formě pro bezatomární formule.

Definice 3.3.3. Řekneme, že bezatomární formule A je v *normální formě*, jestliže je pouze výrokovou kombinací sentencí tvaru $\Box^i\bot$.

Základní myšlenka vychází z toho, že libovolná bezatomární formule A je zároveň formulí, ve které se vyskytuje nejvýše jeden výrokový atom. Můžeme použít naši konstrukci a nalézt k ní pevný bod D, který je s A ekvivalentní. Zbývá zdůvodnit, že pevný bod D má vždy požadovaný charakter, to lze ukázat rozborem naší konstrukce. Lze dokázat silnější podobu věty o normální formě, stačí si například všimnout, že formule je vlastně v disjunktivní normální formě. Navíc je možné ukázat, že lze formuli reprezentovat jistým jedinečným způsobem. Čtenáře odkazujeme na knihu [Smo85] a částečně také na [Boo93].

Věta 3.3.5 (o normální formě bezatomárních formulí)**.** *Pro libovolnou bezatomární formuli A existuje bezatomární formule B v normální formě, pro kterou platí* $\mathsf{GL} \vdash A \equiv B$.

[13] Při odhadu n jsme použili stromovou variantu věty o úplnosti 1.2.4 a důsledek 1.2.5 $n = 3$. Z důkazu věty lze vyčíst, že kripkovský protipříklad má výšku nejvýše takovou jako je počet různých modalizovaných podformulí formule.

Poznamenejme, že pro jiné než bezatomární formule obdoba věty o normální formě v logice GL neplatí, zájemce znovu odkazujeme na výše uvedené publikace.

3.3.1 Složitost pevných bodů

Ukázali jsme tabulkovou metodu k sestrojení pevného bodu. Mějme formuli $A(p)$, nejprve potřebujeme nalézt všechny jeji podformule tvaru $\Box C$, abychom mohli sestrojit tabulku. To lze například opakovaným použitím algoritmu kROZLmax. Poté sestrojíme tabulku o nejvýše $2 \cdot \mathsf{subfl}_{\mathsf{M}}(A(p)) + 1$ sloupcích. Pro každou modalizovanou podformuli $A(p)$ potřebujeme dva a jeden pro p, duplicitní sloupce můžeme případně vynechat. Tabulka má navíc nejvýše $\mathsf{subfl}_{\mathsf{M}}(A(p)) + 1$ řádků. Velikost tabulky tedy roste kvadraticky vzhledem k počtu modalizovaných podformulí formule $A(p)$).

K vyplnění jednoho políčka tabulky potřebujeme spočítat hodnotu příslušné formule. Jde-li o formuli tvaru $\Box C$, pak se stačí podívat do nejvýše dvou políček na předchozím řádku a podle toho se rozhodnout. Vystačíme tedy s konstatním počtem operací. Na všechny formule takového tvaru tedy v jednom řádku spotřebujeme čas $\mathcal{O}(\mathsf{subfl}_{\mathsf{M}}(A(p)))$. Složitější situace nastane v případě, kdy máme pro každou takovou formuli $\Box C$ spočítat také splňování formule C. To musíme projít celou formuli, abychom mohli pomocí výrokové logiky určit její hodnotu. To nám zabere čas $\mathcal{O}(\mathsf{subfl}(C))$. Délku všech takových formulí C můžeme shora odhadnout délkou $A(p)$, celkově tedy na spočítání všech sloupců pro formule tohoto tvaru potřebujeme čas nejvýše $\mathcal{O}(\mathsf{subfl}(A(p)))$. Spočítání splňování p nás pak vyjde také na $\mathcal{O}(\mathsf{subfl}(A(p)))$.

Pro výpočet pochopitelně potřebujeme také prostor k reprezentaci formulí, jejichž splňování počítáme a také potřebujeme prostor pro pomocné operace. Pro všechno toto vystačíme s prostorem $\mathcal{O}(A(p))$. Celkově tedy dostáváme následující větu.

Věta 3.3.6. *Tabulku pro výpočet pevného bodu formule $A(p)$ umíme sestrojit v čase $\mathcal{O}(\mathsf{subfl}_{\mathsf{M}}(A(p)) \cdot \mathsf{subfl}(A(p)))$ a vystačíme přitom s prostorem $\mathcal{O}(\mathsf{subfl}_{\mathsf{M}}(A(p))^2 + \mathsf{subfl}(A(p)))$.*

Ze sloupce p nyní snadno získáme množinu P a z ní okamžitě sestrojíme pevný bod D. Již jsme konstatovali, že pokud P obsahuje všechna k od 0 až do n, pak získáváme jako pevný bod formuli $\neg\Box^0\bot = \neg\bot = \top$, tedy formuli délky jedna či dva (bereme-li jako pevný bod formuli $\neg\bot$). Naopak pokud je P prázdná, dostáváme prázdnou disjunkci, kterou nahradíme formulí $\bot$. Máme tedy spodní odhad na délku pevného bodu, zároveň jsem získali i spodní odhad na jeho modální hloubku. Horní odhad na modální hloubku se snadno ukáže z konstrukce, může být nejvýše n a tedy $\mathsf{subfl}_{\mathsf{M}}(A(p))$. Délka

formule je dána počtem prvků P, těch může být nejvýše $n+1$. Protože však pevné body máme definovany jako intervaly, nemusí s rostoucí velikostí P růst délka pevného bodu. Z (51) se dá nahlédnout, že nejhorším případem z pohledu maximální velikosti formule je případ, kdy jsou buď prvky P všechna lichá nebo všechna sudá čísla do n. Neboť krajní body lze reprezentovat formulí o jediném konjunktu, je nejhorším možným případem situace, kdy prvky P jsou všechna lichá čísla do n a navíc n je sudé. V takovém případě má disjunkce $\frac{n}{2}$ členů. Z (51) každý z nich určitě obsahuje dva symboly $\bot$, jeden symbol $\wedge$ a jistý počet operátorů nutnosti $\Box$. Ten je dán hodnotou čísla z množiny P. Pro číslo i jich je $2i+1$, spočítejme tedy součet $2i+1$ pro všechna lichá i od 1 do $n-1$, kdy n je sudé. To můžeme provést řadou způsobů, asi nejjednodušším je uvědomit si, že pro každé liché i dostáváme z (51) jednu formuli s i operátory nutnosti a jednu s $i+1$ operátory nutnosti, tedy můžeme počítat součet všech čísel od 1 do n, což je

$$s_n = \frac{n}{2}(1+n) = \frac{n^2+n}{2}.$$

Protože počet všech ostatních symbolů je lineární vzhledem k n, a protože n je vlastně $\mathsf{subfl}_{\mathsf{M}}(A(p))$, dostáváme následující větu.

Věta 3.3.7. *Pro pevný bod D formule $A(p)$ vypočtený předchozí metodou platí*

$$\begin{array}{rcccl} 0 & \leq & \mathsf{subfl}(D) & \leq & c_1 \cdot \mathsf{subfl}(A(p))^2 + c_2, \\ 0 & \leq & \mathsf{depth}_{\mathsf{M}}(D) & \leq & \mathsf{subfl}_{\mathsf{M}}(A(p)), \end{array}$$

pro nějaké konstanty $c_1, c_2 > 0$.

Později ve větě 4.1.5 dokážeme, že odhad na modální hloubku pevného bodu ani lepší býti nemůže. Tato metoda nám tedy v tomto směru poskytuje pevné body s optimální modální hloubkou. Navíc přihlédneme-li k větě 3.3.5 o normální formě, můžeme si uvědomit, že získáváme jako pevné body v jistém smyslu optimální formule.

Předvedli jsme metodu sestrojování pevných bodů bez parametrů s rozumnou složitostí. V další části se již zaměříme na postupy dávající výsledek pro libovolnou formuli, ve které se p vyskytuje pouze v modálním kontextu. Složitost těchto metod bude výrazně vyšší, tedy alespoň co se týká horních odhadů na složitost výsledného pevného bodu. Přesto se ukáže, že pro některé formule nabízí obecná metoda rychlejší způsob sestrojení pevného bodu. Příkladem takové formule je $A(p) = \Box^k p \to \Box^l \bot$. Pro velká k a l získáme velkou tabulku. Syntaktické metody, které představíme, naopak pro formuli tohoto tvaru naleznou pevný bod při vhodném předzpracování formule téměř okamžitě, neboť výpočet bude v tomto případě probíhat stejně, jako bychom použili větu 3.1.3 pro 1-rozložitelné formule.

4 Výpočty pevných bodů

Některé matematické konstrukce vznikající metodou pokusů a omylů mají bohužel tu vlastnost, že jsou jako takové dosti neproniknutelné. Buď je to dáno tím, že sám autor si není zcela jist důvody, které vedou k výsledku či tím, že jsou tyto důvody natolik komplikované, že není možno je rozumným způsobem předat ostatním. Takové výsledky pak často u čtenářů vzbuzují dojem, že sice věří důkazu, nejsou však schopni pochopit, jak se na takový důkaz dalo přijít. Jak napovídá článek [BS91] osvětlující počátky logiky dokazatelnosti, můžeme se setkat s takovými výsledky i v případě věty o pevných bodech. Obě základní syntaktické[14] konstrukce pevných bodů jsou výsledkem rozsáhlých pokusů svých autorů a o jejich neprostupnosti nejlépe svědčí fakt, že de Jongh se bál publikovat svůj původní důkaz a Sambin nebyl po jistou dobu schopen přenést svoji schopnost počítat libovolné pevné body na nikoho jiného.

Přestože se oba syntaktické důkazy podařilo postupně zjednodušovat, nelze říci, že by se tím nějakým způsobem projasnily důvody, které k nim vedou a zůstávají tak do značné míry nejasné, a to zvláště třetí (Sambinova) metoda výpočtu pevných bodů. Projasnily se pouze důkazy korektnosti konstrukcí nikoliv způsob, jak k nim dospět. Zmínka v předchozím odstavci o de Jonghovi a Sambinim není náhodná, jsou autory prvních důkazů věty o existenci pevných bodů v GL, proto se také tato věta někdy nazývá de Jonghova, Sambinova věta.

4.1 První metoda výpočtu

Tato metoda výpočtu pevných bodů pochází původně od Boolose [Boo79], a přestože jde o čistě sémantickou metodu a v jistém smyslu je dosti podobná hledání pevných bodů s jediným výrokovým atomem, nelze ji považovat za její zobecnění. U formulí s nejvýše jednou výrokovou proměnnou lze pevný bod, který je bez parametrů, snadno vyčíst z jistého modelu, jehož velikost je dobře omezena větou o úplnosti. Máme-li parametry, je situace o poznání složitější, musíme proto postupovat trochu jinak.

Mějme formuli $A(p)$, ve které se p vyskytuje jako vždy pouze v modálním kontextu. Již víme z lemmatu 3.3.1, že každý kripkovský model $\mathcal{K} = \langle W, R, \Vdash \rangle$, ve kterém je definováno splňování všech výrokových pro-

[14] Máme zde na mysli syntaktické charakterem nikoliv tím, zda důkaz samotný je syntaktický či sémantický. V již citovaném článku [BS91] de Jongh ve svém dopise přiznává, že jeho první důkaz věty o pevných bodech, ačkoliv vedený sémanticky, byl ve své podstatě syntaktický. Tím myslíme, že byl založen na syntaktických konstrukcích, pouze jejich korektnost byla dokazována sémanticky.

měnných z $A(p)$ kromě p, umíme rozšířit o definici splňování pro p na model $\mathcal{K}_p = \langle W, R, \Vdash_p \rangle$ tak, aby v modelu $\mathcal{K}_p$ platilo $p \equiv A(p)$. Zda je $A(p)$ potažmo p splněno v jistém vrcholu $w \in W$ modelu $\mathcal{K}_p$ je pak dáno splňováním výrokových proměnných z $A(p)$ kromě p v w a splňováním všech formulí tvaru $\Box B$ ve vrcholech dosažitelných z w. Tedy liší-li se dva vrcholy splňováním $A(p)$, a tedy i p, musí se lišit buď splňováním nějaké výrokové proměnné z $A(p)$ kromě p nebo splňováním nějaké modalizované podformule formule $A(p)$. Na tomto pozorování je založena celá následující konstrukce. Již jsme zmínili, že pochází od Boolose [Boo79], my však výklad vedeme podle článku [GG90], který přišel s jistými zjednodušeními, která přejal i Boolos do své druhé monografie o logice dokazatelnosti [Boo93].

Definujme pro množinu výrokových atomů S a libovolné n formule speciálního tvaru. Jsou-li splnitelné, pak jde v jistém smyslu o formule s maximální vyjadřovací silou skládající se z atomů S a mající modální hloubku maximálně n. Pro přehlednost definice a ve shodě s [GG90] ještě nejprve zaveďme značení

$$\pm A,$$

kde $\pm$ znamená A pozitivně či negativně, neboli bez negace, tedy A, či s negací, tedy $\neg A$.

Definice 4.1.1. Pro libovolnou konečnou množinu výrokových proměnných $S = \{q_1, \ldots, q_n\}$ definujme *n-S-charaktery* induktivně:

0-S-charaktery:

Všechny formule tvaru

$$\pm q_1 \wedge \pm q_2 \wedge \ldots \wedge \pm q_n.$$

Jediný 0-$\emptyset$-charakter je tedy konstanta $\top$, což vyplývá z definice splňování prázdné konjunkce.

$(n+1)$-S-charaktery:

Nechť formule $K_1, \ldots, K_m$ reprezentují všechny n-S-charaktery, pak $(n+1)$-S-charaktery jsou všechny formule tvaru

$$\pm q_1 \wedge \pm q_2 \wedge \ldots \wedge \pm q_n \wedge \pm\Diamond K_1 \wedge \pm\Diamond K_2 \wedge \ldots \wedge \pm\Diamond K_m.$$

Příklad 4.1.1. Nechť $S = \{q_1, q_2\}$, pak všemi 1-S-charaktery jsou všechny formule tvaru:

$$\pm q_1 \wedge \pm q_2 \wedge \pm\Diamond (q_1 \wedge q_2) \wedge \pm\Diamond (q_1 \wedge \neg q_2) \wedge \pm\Diamond (\neg q_1 \wedge q_2) \wedge \pm\Diamond (\neg q_1 \wedge \neg q_2),$$

jde tedy celkem o $2^6 = 64$ formulí.

Z předchozího příkladu je jasné, že počet formulí se vzrůstajícím n a počtem výrokových atomů v S prudce roste, lze ho totiž rekurzivně definovat jako

$$\mathsf{count}\,(0, |S|) = 2^{|S|},$$
$$\mathsf{count}\,(n+1, |S|) = 2^{|S|} \cdot 2^{\mathsf{count}(n,|S|)}.$$

Z definice navíc vyplývá, že disjunkce všech n-S-charakterů je tautologie a naopak konjunkce libovolných dvou je nesplnitelná. Tím jsme ospravedlnili tvrzení, o kterém jsme se zmínili, že tedy sestrojíme formule s v jistém smyslu maximální vyjadřovací silou. Z výše uvedeného plyne, že pro libovolný kripkovský model $\mathcal{K}$ a jeho vrchol w existuje právě jeden n-S-charakter C, pro který platí

$$w \Vdash C.$$

Definice 4.1.2. Nechť $\mathcal{K} = \langle W, R, \Vdash \rangle$ je kripkovský model a $w \in W$ jeho vrchol. Pak *n-S-charakterem vrcholu w* nazveme jednoznačně určený n-S-charakter C, pro který

$$w \Vdash C.$$

Předpokládejme na chvíli $n > 1$. Uvažme libovolný stromový[15] model $\mathcal{K}$, ve kterém je definováno splňování pro výrokové atomy z S. V libovolném jeho vrcholu w je splněn právě jeden n-S-charakter C. Uvažujme navíc libovolný stromový model $\mathcal{L}$, ve kterém je také definováno splňování pro výrokové atomy z S, a jeho kořen u, ve kterém je splněn stejný n-S-charakter jako ve w, tedy C. Existuje-li v $\mathcal{K}$ vrchol w' dosažitelný z w, pak je v něm určitě z obecných vlastností splněn právě jeden $(n-1)$-S-charakter C'. V konjunkci n-S-charakteru C se z jeho konstrukce musí vyskytovat buď $\Diamond C'$, nebo $\neg\Diamond C'$. Protože ale existuje w', ve kterém je splněno C', musí nastat první možnost, tedy C obsahuje v konjunkci $\Diamond C'$. Neboť je ale C splněno i v u, musí v u být splněno i $\Diamond C'$, a tedy z u musí být dosažitelný nějaký vrchol u', ve kterém je také splněno C'. Připomeňme, že jsme $\mathcal{K}, \mathcal{L}$ a w volili obecně. Výše uvedenou úvahu použijeme v důkazu následujícího lemmatu.

Předpokládejme n a S jako výše, tedy n je počet modalizovaných podformulí formule $A(p)$ a S je množina všech výrokových atomů vyskytujících se v $A(p)$ kromě p. Platí následující klíčové lemma.

Lemma 4.1.1. *Nechť $\mathcal{K} = \langle W_\mathcal{K}, R_\mathcal{K}, \Vdash_\mathcal{K} \rangle$ a $\mathcal{L} = \langle W_\mathcal{L}, R_\mathcal{L}, \Vdash_\mathcal{L} \rangle$ jsou libovolné kripkovské modely, ve kterých platí $p \equiv A(p)$ a nechť $w \in W_\mathcal{K}$ respektive $u \in W_\mathcal{L}$ jsou jejich vrcholy, které mají stejný n-S-charakter, pak*

$$w \Vdash_\mathcal{K} p, \text{ právě tehdy když } u \Vdash_\mathcal{L} p.$$

[15] Z věty 1.2.4 víme, že se v našich úvahách můžeme omezit na modely tohoto tvaru.

Důkaz. Označme si nejprve w jako w_0 a u jako u_0, to se nám bude v konstrukci hodit. Dokazujme sporem. Tedy pokud se w_0 a u_0 liší splňováním p, pak, neboť všude je splněno $p \equiv A(p)$, se musí lišit také splňováním $A(p)$, a tedy splňováním nějaké podformule $A(p)$. Formuli $A(p)$ znovu můžeme chápat jako výrokovou kombinaci atomů z S a formulí tvaru $\Box B$, které jsou podformulemi $A(p)$. Protože w_0 a u_0 mají stejný n-S-charakter, nemohou se lišit splňováním výrokových atomů z S, musí se tedy lišit splňováním nějaké formule tvaru $\Box B$, například $\Box B_0$. Bez újmy na obecnosti nechť je $\Box B_0$ splněna ve w a není splněna v u, pak tedy existuje vrchol u_1, jehož $\mathcal{L}$-rank je minimální, dosažitelný z u_0, ve kterém není splněno B_0. To ale znamená, díky úvahám, které jsme provedli před vyslovením lemmatu, že musí existovat vrchol w_1 dosažitelný z w, který má stejný $(n-1)$-S-charakter jako u_1 a je v něm splněno B_1. Protože oba vrcholy u_1 i w_1 mají stejný $(n-1)$-S-charakter, nemohou se znovu lišit splňováním atomů z S, liší se však splňováním B_0, tedy musí se buď lišit splňováním nějaké její podformule tvaru $\Box B_1'$ (ta je zároveň podformulí $A(p)$) či splňováním p, tedy také splňováním $A(p)$. Díky stejnému $(n-1)$-S-charakteru u_1 a w_1 se pak musí lišit splňováním nějaké podformule formule $A(p)$ tvaru $\Box B_1''$. Bez újmy na obecnosti máme jeden z předchozích dvou případů, tedy buď formuli $\Box B_1'$ nebo $\Box B_1''$ označme za B_1 a můžeme pokračovat v konstrukci stejně jako v prvním kroku a to až do doby než dosáhneme vrcholů w_n a u_n. Ty mají sice stejný 0-S-charakter, zde již naše úvaha ale pokračovat nemůže. Ukažme však, že to není potřeba. Naše konstrukce nám obstarala posloupnosti vrcholů $w_0, \ldots, w_n$ a $u_0, \ldots, u_n$ a také posloupnost formulí $\Box B_0, \ldots, \Box B_n$. Zatím jsme nevyužili skutečnosti, že jsme vždy vybírali vrchol w_{i+1} či u_{i+1}, bez újmy na obecnosti například u_{i+1}, který dosvědčuje nesplněnost $\Box B_i$, jako vrchol s minimálním rankem. To znamená, že v každém vrcholu dosažitelném z u_{i+1} již je B_i splněno. Neboť ve w_i bylo splněno $\Box B_i$, je B_i splněno i v každém vrcholu z něj dosažitelném, tedy i v každém dosažitelném z w_{i+1}, tedy $\Box B_i$ je splněno jak v u_{i+1} tak i ve w_{i+1}. Z toho je jasné, že vybíráme-li formuli $\Box B_{i+1}$, jejímž splňováním se liší w_{i+1} a u_{i+1}, musí být různá od $\Box B_0, \ldots, \Box B_i$, neboť ty všechny jsou ve w_{i+1} i u_{i+1} splněny. Konstrukce nám dává posloupnost $\Box B_0, \ldots, \Box B_n$, tedy posloupnost $n+1$ různých formulí tvaru $\Box B$, které jsou podformulemi formule $A(p)$, ale ta má podle toho, jak jsme volili n, pouze n podformulí tohoto tvaru. Q.E.D.

Nyní již máme všechno připraveno, abychom dokázali větu o existenci pevných bodů a zároveň ukázali první konstrukci pevných bodů v obecném případě.

Věta 4.1.2. *Pro libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu existuje pevný bod D standardních vlastností, pro který*

$$\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to (p \equiv D)\,.$$

Důkaz. Definujme n a S k formuli $A(p)$ jako výše. S ohledem na předchozí lemma lze pevný bod D definovat jako disjunkci všech n-S-charakterů C, pro které existuje model $\mathcal{K}$, ve kterém platí $p \equiv A(p)$ a jeho vrchol w splňující

$$w \Vdash_{\mathcal{K}} C,$$
$$w \Vdash_{\mathcal{K}} p.$$

Uvažujme libovolný model $\mathcal{L} = \langle W_{\mathcal{L}}, R_{\mathcal{L}}, \Vdash_{\mathcal{L}} \rangle$ a jeho vrchol $u \in W_{\mathcal{L}}$, v němž i ve všech z něj dosažitelných vrcholech je splněno $p \equiv A(p)$. Chceme ukázat, že v u je pak splněno také $p \equiv D$. Pro u existuje nějaký n-S-charakter E. Dokažme postupně obě implikace v $p \equiv D$:

$\mathsf{p} \to \mathsf{D}$:

> Předpokládejme, že p je splněné v u, z konstrukce D je však nepochybně E prvkem pevného bodu D, a D je tedy splněno v u.

$\mathsf{D} \to \mathsf{p}$:

> Naopak předpokládejme, že v u je splněno D. Pak musí být E členem disjunkce pevného bodu D, neboť všechny n-S-charaktery jsou vzájemně neslučitelné a n-S-charakter E je v u splněn. Z definice pevného bodu D existuje nějaký model $\mathcal{M}$, ve kterém platí $p \equiv A(p)$ a jeho vrchol v, ve kterém je p splněno a zároveň n-S-charakterem v je E. Nyní stačí uvážit model generovaný vrcholem u, v němž nepochybně platí $p \equiv A(p)$. Z předchozího lemmatu tedy dostáváme, že splňování p je shodné v u i v a tedy p je splněno i v u.

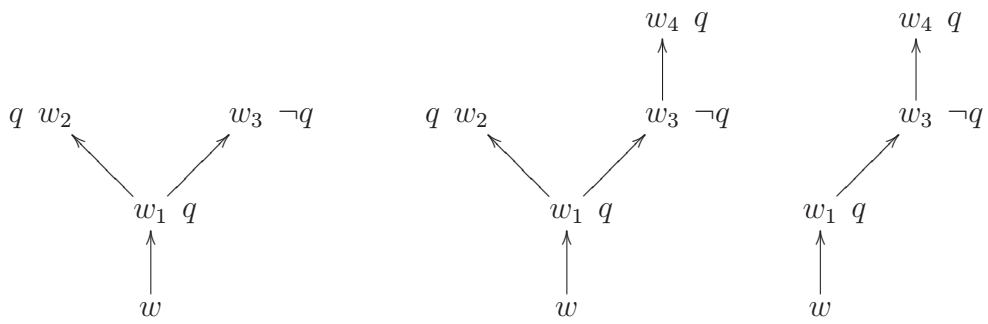
Model $\mathcal{L}$ i jeho vrchol u jsme volili libovolně, víme tedy, že platí

$$\boxdot (p \equiv A(p)) \to (p \equiv D)\,,$$

a tedy z úplnosti dostáváme požadované

$$\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to (p \equiv D)\,.$$

Q.E.D.



Obrázek 8: Kripkovské modely

Poznamenejme, že některé n-S-charaktery jsou nesplnitelné.

Podívejme se podrobněji na fungování metody, o které jsme právě dokázali, že nám umožňuje sestrojit pevný bod. Mějme formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu. Stanovíme n jako počet modalizovaných podformulí $A(p)$ a S jako množinu všech výrokových proměnných vyskytujících se v $A(p)$ kromě p. Nyní pro všechny n-S-charakter C provádíme následující postup. Snažíme se sestrojit kripkovský model $\mathcal{K} = \langle W, R, \Vdash\!\!- \rangle$, ve kterém by byl splněn n-S-charakter C v nějakém jeho vrcholu $w \in W$. Bez újmy na obecnosti to může být kořen modelu a navíc v modelu stačí mít definováno splňování pouze pro výrokové atomy z S. Pokud se nám podaří nějaký takový model najít, umíme v něm jediným možným způsobem dodefinovat splňování p tak, aby v modelu platilo $p \equiv A(p)$. Poté se ptáme, zda ve w je splněno p neboli, zda ve w je splněno $A(p)$. Pokud ano, pak příslušný n-S-charakter přidáme do disjunkce, která nám tvoří pevný bod. Pokud nám do disjunkce nepřibyde ani jeden n-S-charakter, je pevným bodem $\bot$, pokud naopak všechny splnitelné n-S-charaktery, je pevným bodem $\top$.

Podstatné pro naši konstrukci je lemma 4.1.1, které nám říká, že pro každý n-S-charakter C stačí uvážit libovolný model a vrchol, ve kterém je C splněno, neboť po dodefinovaní splňování p tak, aby platilo $p \equiv A(p)$, již vyjde splňování p ve všech ostatních modelech a vrchol, ve kterých je splněno C stejně. Stačí tedy najít libovolný model, ve kterém je příslušný n-S-charakter splnitelný.

Pro konkrétní výpočty však zůstává nezodpovězena otázka, jak velké modely musíme prohledávat, abychom našli model splňující C. Poznamenejme, že všechny n-S-charaktery nemusí být splnitelné, stačí uvážit 2-$\emptyset$-charakter

$$\top \wedge \Diamond(\top \wedge \Diamond\top) \wedge \neg\Diamond(\top \wedge \neg\Diamond\top),$$

který lze po zjednodušení vyjádřit $\Diamond\Diamond\top \wedge \neg\Diamond\neg\Diamond\top$, kde první člen konjunkce vynucuje posloupnost dvou dosažitelných vrcholů a druhý za takových předpokladů vynucuje nekonečnou větev.

Horní odhad velikosti modelu, který dosvědčuje splnitelnost libovolného n-S-charakteru, nás tedy zajímá nejen z důvodů odhadu složitosti algoritmu, ale také z důvodu jeho fungování. První odhad na výšku modelu vychází z věty o úplnosti, ta je tedy nejvýše rovna počtu modalizovaných podformulí příslušného n-S-charakteru. Uvědomíme-li si, jakým způsobem je n-S-charakter definován, má nepochybně alespoň tolik modalizovaných podformulí kolik je $(n-1)$-S-charakterů. O funkci, která vyjadřuje počet n-S-charakterů, však již víme, že roste velmi rychle. Odhad na výšku modelu lze zlepšit. Přirozeným odhadem by mohlo být n, ukažme však, že tomu tak není. Stačí uvážit 2-$\{q\}$-charakter obsahující

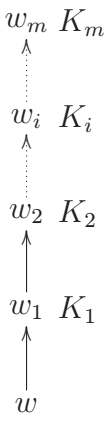
$$\Diamond(q \wedge \Diamond q \wedge \Diamond\neg q) \wedge \neg\Diamond(\neg q \wedge \neg\Diamond q \wedge \neg\Diamond\neg q).$$

Sestrojme nejmenší model, ve kterém je splněn první člen konjunkce, jde o první strom na obrázku 8. Chceme nyní splnit druhý konjunkt, ten nám vlastně říká, že z w nesmí být dosažitelný žádný takový vrchol u, ve kterém je splněno $\neg q$ a z u není dosažitelný žádný vrchol, ve kterém by bylo splněno q ani žádný vrchol, ve kterém by bylo splněno $\neg q$. V našem modelu však takový vrchol u máme, je to vrchol w_3. Splněnost $\neg q$ v něm změnit nemůžeme, musíme tedy přidat jeden vrchol dosažitelný z w_3, ve kterém je splněno buď q, nebo $\neg q$. Přidejme třeba takový, ve kterém je splněno q, jak ukazuje druhý strom na obrázku 8. Pokud bychom naopak přidali $\neg q$, byl by nový vrchol z tranzitivity dosažitelný z w a měli bychom stejný problém. Náš model lze ještě zjednodušit ubráním vrcholu w_2, jak ukazuje třetí strom na obrázku 8, neboť jeho funkci v modelu zastal vrchol w_4. Tento nový model jsme mohli volit jako alternativní pro splnění prvního konjunktu již v prvním kroku, zdálo se to však jako zbytečné prodlužování ranku. Nakonec se ukázalo, že se tomuto podstromu stejně nevyhneme. Ukázali jsme tedy 2-$\{q\}$-charakter splnitelný až v modelech výšky nejméně tři.

Výška modelu možná trochu překvapivě záleží na velikosti množiny S, definujme $s = |S|$, pak existuje splnitelný 2-S-charakter C nesplnitelný v libovolném modelu $\mathcal{K}$ a jeho vrcholu w, pro který platí $\mathcal{K}$-$\mathsf{rank}(w) \leq 2^s$. Oproti postupu v [GG90] neuvádíme důkaz tohoto tvrzení, ale pouze náznak konstrukce, která k němu vede. Její výhodou je, že objasní tvrzení další věty. Nechť $S = \{q_1, \ldots, q_s\}$, můžeme uvážit všechny 0-S-charaktery

$$\pm q_1 \wedge \pm q_2 \wedge \ldots \wedge \pm q_s.$$

Těch je $m = 2^s$, můžeme si je tedy očíslovat například $K_1, \ldots, K_m$. Každé K_i vlastně reprezentuje jednu z možných definic splňování $q_1, \ldots, q_s$, Definujme



Obrázek 9: Kripkovský model

nové vrcholy w_i, $1 \leq i \leq m$, tak, že v w_i je splněno K_i, tedy $w_1, \ldots, w_m$ jsou vrcholy, z nichž každý reprezentuje jednu možnou variantu splňování $q_1, \ldots, q_s$. Cíle bychom dosáhli, pokud bychom měli nějaký vrchol w a nějaký 2-S-charakter C, který by vynucoval, že z w je dosažitelný vrchol w_1 a z něj vrchol w_2 a takto až k w_m, jak ukazuje obrázek 9. To umíme. Splňování všech q_j, $1 \leq j \leq s$, ve w volme libovolně. Dále musíme specifikovat, jaké 1-S-charaktery mají mít $\Diamond$ a jaké $\neg\Diamond$, tedy jinými slovy jaké 1-S-charaktery chceme vynutit a jaké naopak zakázat. Pro každé K_i chceme vynutit jediný 1-S-charakter, který obsahuje jako úvodní konjunkci q_j právě K_i, ve zbylých členech pak obsahuje formuli, která výše uvedeným způsobem říká, že z něj nemají být dosažitelné všechny w_0 až w_i a naopak všechny w_{i+1} až w_m z něj dosažitelné být mají. Všechny ostatní 1-S-charaktery chceme zakázat. Právě popsaná konstrukce nám dává jistý 2-S-charakter C, který pro svoji splnitelnost vyžaduje model z obrázku 9 a evidentně model s nižším rankem K nesplňuje.

Předchozí odhad byl nejlepší možný, neboť jak ukazuje následující věta, ke splnitelnému n-S-charakteru C musí existovat model $\mathcal{L}$ a jeho vrchol v, $\mathcal{L}\text{-}\mathsf{rank}(v) = 2^s + 1$, pro který platí $v \Vdash C$.

Věta 4.1.3. *Mějme libovolnou konečnou množinu S a $n \geq 2$, pak pro libovolný splnitelný n-S-charakter C existuje model $\mathcal{K}$ a jeho vrchol w takový, že*

$$w \Vdash C$$

a $\mathcal{K}\text{-}\mathsf{rank}(w) \leq x + 1$, kde x je počet splnitelných $(n-2)$-S-charakterů.

Pro důkaz čtenáře odkazujeme na článek [GG90]. Z předchozích úvah je

však jasné, že opravdu musíme mít $x+1$, jinak bychom mohli použít postup naznačený výše. Pro $n = 0$ a $n = 1$ je naopak okamžitě jasné, že situace je velmi jednoduchá – stačí uvažovat modely výšky nula respektive jedna.

Již nyní je pravděpodobně jasné, že praktické hledání pevných bodů touto metodou není příliš vhodné, neboť i jednoduché příklady vyžadují značné úsilí[16]. Ke složitosti algoritmu se ještě krátce vrátíme. Ukažme si přesto jeden příklad na hledání pevného bodu metodou, která sice neodpovídá naší metodě, její souvislost je však více než zřejmá.

Příklad 4.1.2. Uvažujme formuli $A(p) = \Box(p \rightarrow g) \vee \Box(p \rightarrow \neg g)$[17]. Její pevný bod můžeme najít tak, že uvážíme jaké všechny n-S-charaktery by potenciálně mohly splňovat podmínky, aby se staly disjunkty pevného bodu podle výše popsaného postupu. Budeme však uvažovat trochu obecněji. Mějme libovolný model $\mathcal{K}$, ve kterém platí $p \equiv A(p)$ a jeho vrchol w. Jak musí takový vrchol w vypadat, aby v něm bylo splněno p, tedy z platnosti $p \equiv A(p)$, aby v něm bylo splněno $A(p) = \Box(p \rightarrow g) \vee \Box(p \rightarrow \neg g)$? Předně je jasné, že pokud $\mathcal{K}\text{-}\mathsf{rank}(w) = 0$, pak okamžitě platí

$$w \Vdash \Box(p \rightarrow g) \vee \Box(p \rightarrow \neg g),$$

a tedy, neboť $\Box(p \rightarrow g) \vee \Box(p \rightarrow \neg g)$ je $A(p)$, dostáváme

$$w \Vdash p.$$

Máme tedy první podmínku. Nechť nyní $\mathcal{K}\text{-}\mathsf{rank}(w) > 0$, pak abychom zajistili

$$w \Vdash A(p),$$

musí v každém vrcholu v dosažitelném z w platit jedno z

$$v \Vdash p \rightarrow g,$$
$$v \Vdash p \rightarrow \neg g.$$

[16] Čtenář, který by přesto měl zájem vidět krátký příklad, může ho nalézt na straně 122 v knize [Smo85]. Poznamenejme, že terminologie je v této knize trochu jiná. Zároveň upozorňujeme, že právě v této části knihy je chyba. Jak jsme ukázali, existují pro $n > 2$ i n-S-charaktery, které jsou splnitelné až v modelech výšky větší než je počet modalizovaných podformulí formule, pro kterou hledáme pevný bod. Na tuto chybu upozornili ve svém článku [GG90] Gleit a Goldfarb.

[17] Předem poznamenejme, že pevný bod formule můžeme snadno najít pomocí důsledku 3.2.6, to však nic nemění na významu příkladu jako takového.

Musí to tedy platit i v každém u dosažitelném z w, pro které $\mathcal{K}\text{-}\mathsf{rank}(u) = 0$, pro takové u snadno dostáváme

$$u \Vdash \Box(p \to g) \vee \Box(p \to \neg g),$$

a tedy také

$$u \Vdash p.$$

V u nyní musí platit jedno z

$$u \Vdash g,$$
$$u \Vdash \neg g.$$

Nechť je v u splněno například g, pak ze splněnosti $A(p)$ v w musí platit

$$w \Vdash \Box(p \to g),$$

a tedy v každém v dosažitelném z w musí platit

$$v \Vdash p \to g.$$

Neboť i v každém v' dosažitelném z v platí

$$v' \Vdash p \to g,$$

ve v tedy platí

$$v \Vdash \Box(p \to g),$$

a tedy ve v je splněno $A(p)$, a musí v něm tedy být splněno i p, a tedy aby bylo splněno $p \to g$, musí platit

$$v \Vdash g.$$

Pokud bychom uvažovali v u splňování $p \to \neg g$, měli bychom všude splněno $\neg g$, postup by však byl zcela stejný. Máme-li tedy $\mathcal{K}\text{-}\mathsf{rank}(w) > 0$, pak platí jedno z

$$w \Vdash \Box g,$$
$$w \Vdash \Box \neg g.$$

Tím jsme pokryli všechny možnosti, stačí tedy uvažované modely „zakódovat“ pomocí modální formule, ta pak bude pevným bodem. První možnost, tedy $\mathcal{K}\text{-}\mathsf{rank}(w) = 0$, nám snadno zajistí formule $\Box\bot$. Druhou možnost, tedy $\mathcal{K}\text{-}\mathsf{rank}(w) > 0$ a platnost $\Box g$ nebo $\Box\neg g$ nám zajistí formule $\Diamond g \wedge \Box g$ nebo $\Diamond\neg g \wedge \Box\neg g$. Pevný bod je tedy disjunkce všech těchto formulí, tedy

$$\Box\bot \vee (\Diamond g \wedge \Box g) \vee (\Diamond\neg g \wedge \Box\neg g).$$

Všechny uvažované modely však můžeme popsat i jednodušeji, jsou to právě ty, ve kterých platí

$$\Box g \vee \Box\neg g.$$

Z dokazatelné jednoznačnosti pevných bodů musí být obě formule v GL ekvivalentní, což lze snadno ověřit.

4.1.1 Složitost pevných bodů

Naše konstrukce předpokládá, že se pro každý n-S-charakter K pokusíme sestrojit model, ve kterém je K splněno. To podle věty 4.1.3 pro $n \geq 2$ v nejhorším případě znamená zkoušet modely až do hloubky o jedna větší než je počet splnitelných $(n-2)$-S-charakterů. V každém takovém modelu pak musíme postupně od listů dodefinovat splňování p a zjistit, zda je splněno v jeho kořeni. Pokud ano, přidáme příslušný n-S-charakter do disjunkce.

Pokusme se tedy odhadnout složitost našeho postupu. Nejprve připomeňme, že počet n-S-charakterů K lze spočítat pomocí rekurzivní funkce

$$\begin{aligned}\mathsf{count}\,(0, |S|) &= 2^{|S|},\\ \mathsf{count}\,(n+1, |S|) &= 2^{|S|} \cdot 2^{\mathsf{count}(n,|S|)}.\end{aligned}$$

Rozepíšeme-li uvedený rekurzivní zápis dostáváme

$$\mathsf{count}\,(n+1, |S|) = 2^{|S| \cdot 2^{|S| \cdot 2^{\cdot^{\cdot^{\cdot^{2^{|S|}}}}}}} \Big\}{\scriptstyle n\text{-krát}}.$$

Popisovat podrobně algoritmus pro konstrukci pevných bodů touto metodou a odhadovat jeho složitost se nyní zdá zbytečné. Navíc si musíme uvědomit, že pro $n > 1$ každý n-S-charakter v sobě obsahuje jako podformule všechny $(n-1)$-S-charaktery, a tedy i formule dosahuje astronomických rozměrů. Tím pádem i velikost pevného bodu lze omezit pouze astronomickým výrazem. Navíc pro formule, jejichž pevným bodem je $\top$, musí mít v disjunkci všechny splnitelné n-S-charaktery. Naopak pro formule jejichž

pevným bodem je $\bot$, neobsahuje disjunkce žádný člen a máme tak triviální spodní odhad na složitost pevného bodu, který tato konstrukce dává.

Popsaný způsob výpočtu pevných bodů se tedy pro praktické použití nehodí. Přesto má konstrukce jednu velmi důležitou vlastnost, kterou shrnuje následující věta.

Věta 4.1.4. *Nechť D je pevný bod formule $A(p)$ sestrojený předchozí metodou, pak platí*

$$0 \leq \mathsf{depth}_{\mathsf{M}}(D) \leq \mathsf{subfl}_{\mathsf{M}}(A(p)).$$

Důkaz. Pro formule, jejichž pevným bodem je $\bot$, dostáváme jako pevný bod prázdnou disjunkci, neboli $\bot$. Tím jsme získali také triviální spodní odhad modální hloubky pevného bodu nalezeného naší konstrukci.

Předpokládejme nyní pevný bod D s alespoň jedním disjunktem. Víme, že jde o disjunkci jistých n-S-charakterů C. Z definice libovolného pevného n-S-charakteru C okamžitě dostáváme, že pro všechna C platí

$$\mathsf{depth}_{\mathsf{M}}(C) = n,$$

a tedy nepochybně také

$$\mathsf{depth}_{\mathsf{M}}(D) = n.$$

Tvrzení pro horní odhad modální hloubky D teď již jednoduše plyne z toho, že n je právě $\mathsf{subfl}_{\mathsf{M}}(A(p))$. Q.E.D.

Poznamenejme, že jsme vlastně ukázali, že modální hloubka pevného bodu D nalezeného touto metodou je 0 nebo n, pokud tedy neuvažujeme zjednodušování formulí. Získali jsme tedy horní odhad na modální hloubku pevných bodů obecně. Ukažme, že jde-li o horní odhad modální hloubky pevného bodu, je námi podaný odhad nejlepší možný.

Věta 4.1.5. *Pro libovolné přirozené číslo n existuje formule $A(p)$ splňující $\mathsf{subfl}_{\mathsf{M}}(A(p)) = n$, pro jejíž každý pevný bod D platí*

$$\mathsf{depth}_{\mathsf{M}}(D) = \mathsf{subfl}_{\mathsf{M}}(A(p)).$$

Důkaz. Uvažujme pro libovolné n formuli $A(p) = \neg\Box^n p$, ta je 1-rozložitelná. Vyberme jeden z těchto rozkladů, například $B = \neg q$ a $C = \Box^{n-1}p$. Podle věty 3.1.3 je jejím pevným bodem formule $A(B[\top])$. Dosazením $\top$ do B získáme $\bot$ a jeho dosazením do $A(p)$ dostáváme pevný bod $D = \neg\Box^n\bot$. Ten má jistě modální hloubku právě n, navíc k ní neexistuje žádná ekvivalentní formule bez výrokových atomů, která by měla menší hloubku. Formule $\neg\Box^n\bot$ je totiž splněna v takovém vrcholu modelu, ze kterého je dosažitelná posloupnost vrcholů délky alespoň n. Tuto vlastnost nepochybně nelze vyjádřit žádnou formulí bez výrokových proměnných s nižší modální hloubkou. Q.E.D.

Z důkazu předchozí věty by se ale mohlo zdát, že bychom mohli modální hloubku pevných bodů odhadnout i lépe, a to modální hloubkou $A(p)$. Ukažme, že to není možné.

Věta 4.1.6. *Existuje taková formule $A(p)$, že pro každý její pevný bod D platí*

$$\mathsf{depth}_{\mathsf{M}}(D) > \mathsf{depth}_{\mathsf{M}}(A(p)).$$

Důkaz. Zvolme formuli $A(p) = \Box p \rightarrow \Box\neg p$, ta má evidentně modální hloubku jedna. Ukážeme, že pro každý její pevný bod platí, že má hloubku alespoň dva. Jejím pevným bodem je podle příkladu 3.3.3 formule $\Box\Box\bot \rightarrow \Box\bot$. Uvažujme libovolnou formuli bez výrokových proměnných modální hloubky jedna. Díky větě 3.3.5 o normální formě bezatomárních formulí a její konstrukci víme, že všechny takové formule jsou ekvivalentní jedné z formulí $\bot, \top, \Box\bot$ nebo $\neg\Box\bot$. To však $\Box\Box\bot \rightarrow \Box\bot$ není. Q.E.D.

Přestože se výše uvedená metoda výpočtu pevných bodů ukázala prakticky nepoužitelnou, získali jsme díky ní důležitý odhad maximální modální hloubky pevných bodů. Neboť se ukáže, že ostatní metody nám takový odhad nenabízí, měla pro nás konstrukce význam i z pohledu složitosti pevných bodů obecně. Její síla však spočívá především v průhlednosti hlavní myšlenky.

4.2 Druhá metoda výpočtu

Od sémantické metody konstrukce pevných bodů se nyní přesuneme k první ze syntaktických metod. Je vlastně přímým zobecněním syntaktických konstrukcí pevných bodů pro 1-rozložitelné formule a pevný bod počítá iterativním použitím tohoto algoritmu. Máme-li libovolnou formuli $A(p)$ příslušných vlastností a její n-rozklad

$$A(p) = B\left[\Box C_1(p), \ldots, \Box C_n(p)\right],$$

můžeme v každé jednotlivé formuli $C_i(p), 1 \leq i \leq n$, přejmenovat všechny výskyty p na novou proměnnou p_i, takto získáme novou formuli

$$A(p_1, \ldots, p_n) = B\left[\Box C_1(p_1), \ldots, \Box C_n(p_n)\right]$$

a nyní můžeme použít n-krát větu 3.1.3 o pevných bodech pro 1-rozložitelné formule. Podrobnosti ukazuje důkaz níže uvedené věty. Poznamenejme, že výklad vedeme podle článku [Smo79] a knihy [Smo85]. Metoda samotná pochází z nepublikované práce de Jongha. Základní myšlenka je shodná

s důkazem lemmatu 2.3.5, důkaz však povedeme trochu jinak, aby byl jasný také algoritmus sestrojení pevného bodu.

Nejprve připomeňme konstrukci pevných bodů 1-rozložitelných formulí z věty 3.1.3. Mějme tedy libovolnou 1-rozložitelnou formuli

$$A(p) = B\left[\Box C_1(p)\right],$$

pak jejím pevným bodem je formule $A(B\left[\top\right])$.

Věta 4.2.1. *Každá formule $A\left(p\right)$, ve které se p vyskytuje pouze v modálním kontextu, má pevný bod.*

Důkaz. Víme, že pro každou formuli $A\left(p\right)$ splňující předpoklady věty existuje n takové, že $A\left(p\right)$ je n-rozložitelná, uvažme tedy nějaký takový rozklad

$$A\left(p\right) = B\left[\Box C_1\left(p\right), \ldots, \Box C_n\left(p\right)\right].$$

Je-li formule 0-rozložitelná, pak se p v $A(p)$ nevyskytuje a můžeme za pevný bod vzít rovnou formuli $A(p)$. Je-li $A(p)$ 1-rozložitelná, pak nalezneme pevný bod okamžitě díky větě 3.1.3 o existenci pevných bodů pro 1-rozložitelné formule. Předpokládejme tedy $n \geq 2$. Převedeme problém, jak jsme již naznačili, tak, abychom mohli použít opakovaně větu 3.1.3 umožňující nám nalézt pevné body pro 1-rozložitelné formule. Proto v jednotlivých formulích $C_i\left(p\right)$ přejmenujeme všechny výskyty p na čerstvé proměnné p_i, o kterých předpokládáme, že se v $A(p)$ nevyskytují. Přeneseme-li tuto změnu i do formule $A\left(p\right)$, získáme novou formuli

$$A_1\left(p_1, \ldots, p_n\right) = B\left[\Box C_1\left(p_1\right), \ldots, \Box C_n\left(p_n\right)\right]. \tag{52}$$

Ta je však již pro všechny p_i triviálně 1-rozložitelná, neboť p_i se vyskytuje pouze v C_i, a stačí tedy pro libovolné i použít výše uvedený rozklad s tím, že na $B\left[\Box C_1\left(p_1\right), \ldots, \Box C_n\left(p_n\right)\right]$ se můžeme dívat jako na $B_1\left[\Box C_1\left(p_1\right)\right]$, pro které

$$\begin{aligned} B_1\left[\Box C_1\left(p_1\right)\right] &= B\left[\Box C_1\left(p_1\right), \ldots, \Box C_n\left(p_n\right)\right], \\ &= A_1\left(p_1, \ldots, p_n\right), \end{aligned}$$

a které se od $B\left[q_1, \ldots, q_n\right]$ liší pouze tím, že má pro všechna i, $1 < i \leq n$, dosazeny za q_i přímo formule $\Box C_i\left(p_i\right)$, tedy

$$B_1\left[q_1\right] = B\left[q_1, \Box C_2(p_2), \ldots, \Box C_n\left(p_n\right)\right].$$

Teď již umíme snadno nalézt pevný bod D_1, pro který platí

$$\mathsf{GL} \vdash D_1 \;\equiv\; A_1\left(D_1\right).$$

Z konstrukce D_1 také víme, že platí

$$\begin{aligned} D_1(p_2,\ldots,p_n) &= A_1(B_1[\top],p_2,\ldots,p_n), \\ &= A_1(B[\top,\Box C_2(p_2),\ldots,\Box C_n(p_n)],p_2,\ldots,p_n), \\ &= B[\Box C_1(B[\top,\Box C_2(p_2),\ldots,\Box C_n(p_n)]), \\ &\qquad\qquad \Box C_2(p_2),\ldots,\Box C_n(p_n)]. \end{aligned}$$

Vezměme nyní za $A_2(p_2,\ldots,p_n)$ pevný bod $D_1(p_2,\ldots,p_n)$, tedy

$$A_2(p_2,\ldots,p_n) =_{def} D_1(p_2,\ldots,p_n)$$

a postup opakujme. Nakonec tímto způsobem získáme D_n, což bude náš hledaný pevný bod, neboli

$$D =_{def} D_n.$$

Obecně tedy definujeme

$$A_{k+1}(p_{k+1},\ldots,p_n) =_{def} D_k(p_{k+1},\ldots,p_n) \tag{53}$$

a také z konstrukce pevných bodů D_k obecně platí

$$\mathsf{GL} \vdash D_k(p_{k+1},\ldots,p_n) \equiv A_k(D_k(p_{k+1},\ldots,p_n),p_{k+1},\ldots,p_n). \tag{54}$$

Tvrdíme, že D je hledaný pevný bod formule $A(p)$. Přitom využijeme, že jsme konstruovali pevné body specifických formulí. Ukažme indukcí podle k od n do 1, že pro libovolné k, $1 \leq k \leq n$ platí

$$\mathsf{GL} \vdash D \equiv A_k(D,\ldots,D).$$

Pro $k = n$ chceme ukázat

$$\mathsf{GL} \vdash D \equiv A_n(D),$$

což s ohledem na skutečnost, že $D = D_n$ plyne přímo z kontrukce D_n jako pevného bodu formule A_n. Podstata celé konstrunce se však ukáže až v indukčním kroku. Z indukční hypotézy máme

$$\mathsf{GL} \vdash D \equiv A_{k+1}(D,D,\ldots,D).$$

Nyní z definice A_{k+1}, tedy použitím (53) dostáváme

$$\mathsf{GL} \vdash D \equiv D_k(D,D,\ldots,D) \tag{55}$$

a dále pak substitucí D za $p_{k+1}, \ldots, p_n$ do (54) máme

$$\text{(56)} \quad \mathsf{GL} \vdash D_k\left(D, \ldots, D\right) \equiv A_k\left(D_k\left(D, \ldots, D\right), D, \ldots, D\right)$$

a nyní, využijeme-li ekvivalenci (55) a první substituční lemma 1.3.7 na formuli $q \equiv A_k\left(q, D, \ldots, D\right)$, získáváme

$$\begin{aligned}\mathsf{GL} \vdash \left(D \equiv A_k\left(D, D, \ldots, D\right)\right) \\ \equiv \left(D_k\left(D, \ldots, D\right) \equiv A_k\left(D_k\left(D, \ldots, D\right), D, \ldots, D\right)\right),\end{aligned}$$

pak s využitím (56) dostáváme požadované

$$\mathsf{GL} \vdash D \equiv A_k\left(D, D, \ldots, D\right).$$

Nyní tedy víme, že platí

$$\mathsf{GL} \vdash D \equiv A_1\left(D, \ldots, D\right),$$

ale $A_1(D, \ldots, D)$ je vlastně $A(D)$, neboť

$$A_1\left(D, \ldots, D\right) = B\left[\Box C_1\left(D\right), \ldots, \Box C_n\left(D\right)\right] = A\left(D\right),$$

a tedy

$$\mathsf{GL} \vdash D \equiv A\left(D\right).$$

Q.E.D.

V předchozí větě jsme popsali postup, jak nalézt pevný bod libovolné formule $A(p)$, ve které se p vyskytuje pouze v modálním kontextu. Popišme nyní na základě této konstrukce konkrétní algoritmus[18], který budeme dále zkoumat a který můžeme použít k výpočtům. Jde o algoritmus 1 a nazveme jej FP1.

Mějme tedy formuli $A(p)$. Vstupem algoritmu je její n-rozklad, tedy konkrétně číslo n, formule B a formule $C_1(p), \ldots, C_n(p)$. Algoritmus v naprostém souladu s důkazem nejprve testuje, zda není n rovno nule, pokud ano, vrací jako pevný bod formuli B. Výpočet je pochopitelně zajímavý

[18]Bylo by pravděpodobně lepší mluvit o pseudoalgoritmu. Odpustili jsme si těžkosti, které by vznikly s reprezentací formulí a také operaci dosazování, značíme $\leftarrow$, považujeme za primitivní operaci. K tomu nás vedla snaha o názornost. Přepsaní algoritmu, například v podobě počítačového programu, by však nemělo činit výraznější problémy.

Algoritmus 1 FP1$(n, B[q_1, \ldots, q_n], \langle C_1, \ldots, C_n \rangle)$

Vstup: Libovolný n-rozklad $B[\Box C_1(p), \ldots, \Box C_n(p)]$, konkrétně hodnota n a formule $B[q_1, \ldots, q_n], C_1, \ldots, C_n$.
Výstup: Pevný bod formule $B[\Box C_1(p), \ldots, \Box C_n(p)]$.

```
if n = 0 then
  return B
else
  B_1 ⇐ B
  for i = 1 to n do
    B'_i ⇐ B_i [q_i ← ⊤]
    □C'_i ⇐ □C_i [p ← B'_i]
    B_{i+1} ⇐ B_i [q_i ← □C'_i]
  end for
  return B_{n+1}
end if
```

především v ostatních případech. Ty bychom mohli řešit jednak rekurzivně, jednak jistým cyklem. Znovu v souladu s důkazem a zároveň i z důvodu názornosti volíme druhý způsob, volíme i značení používané v předchozím důkazu.

Námi uvedený algoritmus se přesto od postupu v důkazu drobně liší. V důkazu jsme za formuli B_1 volili formuli, která měla za všechny proměnné $q_2, \ldots, q_n$ dosazeny formule $\Box C_2, \ldots, \Box C_n$. Tentokráte bereme za formuli B_1 přímo formuli B, ponecháváme tedy proměnné $q_2, \ldots, q_n$. To si můžeme dovolit, neboť pečlivým prostudováním konstrukce v důkazu věty zjistíme, že formule $\Box C_i$ se zapojí do konstrukce až v kroku i. V předchozích krocích se na konstrukci pevného bodu nijak nepodílí, ten totiž vzniká dosazením příslušné formule B_i, ve které jsme nahradili q_i konstantou $\top$, do formule A_i. V našem algoritmu dosazením konstanty $\top$ do formule B_i vzniká nová formule B'_i. Nyní bychom ji podle důkazu měli dosadit do A_i za příslušné p_i, my však proměnné p_i ani formule A_i vůbec nezavádíme. Stačí si uvědomit, že stejného výsledku dosáhneme, pokud dosadíme B'_i pouze do $\Box C_i$ za p a výsledek, v našem případě formuli $\Box C'_i$, do formule B_i. V důkazu jsme výsledek prohlásili za formuli A_{i+1}, nyní ho však prohlásíme za formuli B_{i+1}. To souvisí s již zmíněnou skutečností, že v algoritmu pracujeme pouze s formulemi B_i. Jde však opravdu o čistě kosmetický rozdíl, neboť A_i získáme z B_i, uvážíme-li všechna $\Box C_i, \ldots, \Box C_n$.

Zdůrazněme znovu hlavní rozdíl oproti konstrukci v důkazu. V něm pracujeme s celými formulemi A_i včetně všech podformulí tvaru $\Box C_i, \ldots, \Box C_n$,

které k této formuli patří. Při konstrukci pevného bodu však tyto formule využijeme až v kroku i, můžeme místo nich tedy do té doby nechávat všude proměnné $q_i, \ldots, q_n$ a pracovat tak s formulemi B_i. V i-tém kroku pak použijeme i příslušnou formuli $\Box C_i$ a nahradíme jí všechny výskyty q_i. Uvědomme si, že se nám v průběhu výpočtu proměnné $q_i, \ldots, q_n$ ve formuli B_i hromadí, neboť každý krok výpočtu znamená dosazení příslušné formule B_i s dosazenou konstantou $\top$ za q_i, ale obsahující všechny proměnné $q_{i+1}, \ldots, q_n$. Poté příslušný krok výpočtu pokračuje dosazením takto obdržené formule do formule $\Box C_i$ za proměnnou p a dále dosazením získané formule do B_i a končí výslednou formulí B_{i+1}, ve které se nám výskyt všech $q_{i+1}, \ldots, q_n$ vlastně zvětší a to tolikrát, kolikrát se p vyskytovalo v $\Box C_i$.

Po n krocích algoritmu dostáváme formuli B_{n+1}, která již neobsahuje žádné q_i, a tedy do ní ani nelze dosadit žádné $\Box C_i$ za q_i a zanést tak do ní proměnnou p. Formule B_{n+1} je tedy pevným bodem. To je také výstupem algoritmu, jehož korektnost ukazuje důkaz předchozí věty a výše uvedené ospravedlnění rozdílů.

Než se pustíme do počítání příkladů, uvědomme si jednoduchou skutečnost, která nám, jak se ukáže, počítání velmi zjednoduší. V každém kroku můžeme získanou formuli nahradit formulí dokazatelně ekvivalentní, a dokonce i podformule získaných formulí můžeme nahradit dokazatelně ekvivalentními formulemi. Jedním z ospravedlnění by mohlo být, že pokud jsou dvě formule dokazatelně ekvivalentní, pak jsou i silně nutně dokazatelně ekvivalentní a můžeme tedy použít první substituční lemma 1.3.7, a tedy v libovolné formuli můžeme zaměňovat její podformule jinými formulemi s nimi dokazatelně ekvivalentními při zachování dokazatelné ekvivalence původní a výsledné formule. Neboť evidentně dokazatelně ekvivalentní formule mají stejné pevné body a pevné body jsou až na dokazatelnou ekvivalenci jednoznačné, můžeme tedy libovolný výpočet dávající nám pevné body vhodně měnit tak, abychom pracovali s co možná nejmenšími formulemi.

Přijměme zároveň jednoduchou konvenci ke značení těchto úprav. Pro názornost budeme záměny ekvivalentními formulemi značit rovností, čímž chceme zdůraznit použití předchozích úvah, přestože bychom zcela správně měli používat ekvivalenci.

Poznamenejme však, že takové úpravy formulí jsou velmi problematické, uvažujeme-li čistě algoritmické řešení úlohy. Šlo by je pochopitelně implementovat zkoušením, zda není nějaká „jednodušší“ formule ekvivalentní formuli vznikající během výpočtu. Takové testování je však algoritmicky velmi náročné, neboť pro složité formule by bylo potřeba testovat velké množství kandidátů na zjednodušení, a navíc testování dokazatelnosti v logice GL, tedy v našem případě ekvivalence dvojice formulí, je *PSPACE*-úplná úloha. Navíc není jisté, že by se nám nějaké zjednodušení podařilo nalézt.

Máme	**Nahradíme**
$\Box\top$	$\top$
$\top \to E$	E
$E \to \top$	$\top$
$E \wedge \top$	E
$E \vee \top$	$\top$
$E \equiv \top$	E
$\bot \to E$	$\top$
$E \to \bot$	$\neg E$
$E \wedge \bot$	$\bot$
$E \vee \bot$	E
$E \equiv \bot$	$\neg E$
$\neg\top$	$\bot$
$\neg\bot$	$\top$
$\neg\neg E$	E

Tabulka 3: Tabulka základních zjednodušení

Na druhou stranu lze říci, že řadu často používaných zjednodušení by bylo možno implementovat poměrně snadno. Z charakteru konstrukce pevných bodů, kdy dosazujeme konstantnu $\top$, se pochopitelně často vyskytují formule obsahující $\top$ eventuálně $\bot$, které lze okamžitě zjednodušit, jak uvádí tabulka 3.

Uveďme důležité příklady, které demonstrují, že pro konjunkci, disjunkci nebo implikaci dvou formulí majících pevné body neplatí, že by pevným bodem vzniklé formule byla konjunkce, disjunkce respektive implikace pevných bodů jednotlivých formulí.

Příklad 4.2.1. Mějme formuli $A(p) = \neg\Box p \wedge \Box p$, pevným bodem $\neg\Box p$ je $\neg\Box\bot$ a pevným bodem $\Box p$ je $\top$, to již víme. Konjunce těchto pevných bodů je tedy $\neg\Box\bot$. Spočítejme pevný bod formule $A(p)$, ta je však evidentně ekvivalentní $\bot$, a tedy její pevný bod je také $\bot$. Dostáváme však

$$\mathsf{GL} \not\vdash \bot \equiv \neg\Box\bot,$$

neboť evidentně neplatí implikace zprava doleva.

Příklad 4.2.2. Mějme formuli $A(p) = \neg\Box p \vee \Box\neg p$, pevným bodem $\neg\Box p$ je $\neg\Box\bot$ a pevným bodem $\Box\neg p$ je $\Box\bot$. Disjunkce těchto pevných bodů je tedy $\top$. Naopak spočítejme pevný bod formule $A(p)$, mějme $B = \neg q_1 \vee q_2$ a

Obrázek 10: Kripkovský protipříklad na $(\Box\Box\bot \to \Box\bot) \to \Box\bot$

$C_1 = p, C_2 = \neg p$. Postupujme podle algoritmu FP1:

$$\begin{aligned} B_1 &= \neg q_1 \vee q_2, \\ B_1' &= \neg\top \vee q_2 = \bot \vee q_2 = q_2, \\ \Box C_1' &= \Box q_2, \\ B_2 &= \neg\Box q_2 \vee q_2 \\ B_2' &= \neg\Box q_2 \vee \top = \top, \\ \Box C_2' &= \Box\neg\top = \Box\bot, \\ B_3 &= \neg\Box\Box\bot \vee \Box\bot, \\ D &= \neg\Box\Box\bot \vee \Box\bot. \end{aligned}$$

Formule D rozhodně v GL není dokazatelná, a tedy

$$\mathsf{GL} \nvdash \top \equiv (\neg\Box\Box\bot \vee \Box\bot).$$

Příklad 4.2.3. Mějme formuli $A(p) = \Box p \to \Box\neg p$, pevným bodem $\Box p$ je $\top$ a pevným bodem $\Box\neg p$ je $\Box\bot$. Uvažovaná implikace těchto pevných bodů je tedy ekvivalentní $\Box\bot$. Spočítejme pevný bod $A(p)$, k tomu můžeme využít předchozí příklad, neboť máme vlastně stejnou formuli $A(p)$, stačí uvážit zápis implikace jako disjunkce. Naopak, přepíšeme-li předchozí pevný bod do implikace, dostáváme $\Box\Box\bot \to \Box\bot$. Lehce však ukážeme, že

$$\mathsf{GL} \nvdash \Box\bot \equiv (\Box\Box\bot \to \Box\bot),$$

neboť model na obrázku 10 je kripkovským protipříkladem na implikaci zprava doleva.

Naopak pro negaci pochopitelně platí, že kdykoliv D je pevným bodem $A(p)$, pak $\neg D$ je pevným bodem $\neg A(p)$. Stačí užít výrokovou logiku a snadno dostáváme

$$\mathsf{GL} \vdash D \equiv A(D), \text{ právě tehdy když } \mathsf{GL} \vdash \neg D \equiv \neg A(D).$$

Poznamenejme, že jsme předchozí příklady mohli počítat již pomocí postupu pro pevné body bez parametrů. Naší hlavní náplní je však sestrojování pevných bodů v obecném případě, a proto jsme je počítali až nyní. Uveďme přesto také jeden příklad na výpočet s parametry.

Příklad 4.2.4. Mějme formuli $A(p) = \Box(\Box p \to g) \wedge \neg\Box p$. Formule má dva možné rozklady, spočítejme oba.

1) $B = q_1 \wedge \neg q_2, C_1 = \Box p \to g, C_2 = p$:

$$\begin{aligned} B_1 &= q_1 \wedge \neg q_2, \\ B_1' &= \top \wedge \neg q_2 = \neg q_2, \\ \Box C_1' &= \Box(\Box\neg q_2 \to g), \\ B_2 &= \Box(\Box\neg q_2 \to g) \wedge \neg q_2, \\ B_2' &= \Box(\Box\neg\top \to g) \wedge \neg\top = \bot \\ \Box C_2' &= \Box\bot, \\ B_3 &= \Box(\Box\neg\Box\bot \to g) \wedge \neg\Box\bot, \\ D &= \Box(\Box\neg\Box\bot \to g) \wedge \neg\Box\bot. \end{aligned}$$

2) $B = \Box(q_1 \to g) \wedge \neg q_1, C_1 = p$:

$$\begin{aligned} B_1 &= \Box(q_1 \to g) \wedge \neg q_1, \\ B_1' &= \Box(\top \to g) \wedge \neg\top = \bot, \\ \Box C_1' &= \Box\bot, \\ B_2 &= \Box(\Box\bot \to g) \wedge \neg\Box\bot, \\ D &= \Box(\Box\bot \to g) \wedge \neg\Box\bot. \end{aligned}$$

Získali jsme dva různé pevné body, ty však musí být ekvivalentní, což snadno ukážeme, uvědomíme-li si, že platí

$$\mathsf{GL} \vdash \Box\neg\Box\bot \equiv \Box\bot.$$

Předchozí příklad nám ukazuje skutečnost, o které jsme se již zmínili u k-rozložitelnosti. Menší rozklady jsou pro nás při výpočtu výhodnější. Především evidentně méněkrát projdeme cyklem výpočtu, ale jak ukazuje předchozí příklad, můžeme dostat i kratší pevný bod. U velikosti pevného bodu to nebylo příliš znát, neboť během výpočtu formule zkracujeme. Pokud bychom to nedělali, byl by vidět mnohem podstatnější rozdíl.

Abychom lépe pochopili fungování algoritmu, zkusme si rozepsat jeho postup pro nějaký obecný n-rozklad. Volme $n = 2$, pro větší n by byl totiž výpočet neúměrně velký a menší n nejsou zajímavá.

Příklad 4.2.5. Mějme formuli

$$A(p) = B\left[\Box C_1(p), \Box C_2(p)\right],$$

máme tedy $B[q_1, q_2]$. Postupujme podle algoritmu FP1:

$$\begin{aligned}
B_1 &= B[q_1, q_2],\\
B_1' &= B[\top, q_2],\\
\Box C_1' &= \Box C_1(B[\top, q_2]),\\
B_2 &= B[\Box C_1(B[\top, q_2]), q_2],\\
B_2' &= B[\Box C_1(B[\top, \top]), \top],\\
\Box C_2' &= \Box C_2(B[\Box C_1(B[\top, \top]), \top]),\\
B_3 &= B[\Box C_1(B[\top, \Box C_2(B[\Box C_1(B[\top, \top]), \top])]), \Box C_2(B[\Box C_1(B[\top, \top]), \top])]\\
D &= B[\Box C_1(B[\top, \Box C_2(B[\Box C_1(B[\top, \top]), \top])]), \Box C_2(B[\Box C_1(B[\top, \top]), \top])]
\end{aligned}$$

Předchozí příklad nám poskytuje několik zajímavých pozorování. Předně si můžeme všimnout, že formule

$$\Box C_1(B[\top, \Box C_2(B[\Box C_1(B[\top, \top]), \top])]),$$

kterou substituujeme do B za q_1 je evidentně složitější než formule

$$\Box C_2(B[\Box C_1(B[\top, \top]), \top]),$$

kterou substiujeme za q_2. Protože jsme předchozí příklad řešili zcela obecně, musí to být dáno tím, v jakém pořadí jsme „eliminovali“ proměnné q_1 a q_2. Co kdybychom tedy pořadí obrátili? To můžeme udělat jednoduše, stačí v B zaměnit proměnné q_1 a q_2, dále pak vyměnit formule $C_1(p)$ a $C_2(p)$ a můžeme znovu použít stejný algoritmus. Dostali jsme vlastně jinou formuli B, měli bychom ji značit například B', ale protože evidentně platí

$$B[\Box C_1(p), \Box C_2(p)] = B'[\Box C_2(p), \Box C_1(p)],$$

tedy kdykoliv při dosazování do B prohodíme členy, dostáváme to samé, nemusíme takové značení zavádět, jen stačí mít toto na paměti. Využijeme-li předchozího příkladu, pak touto záměnou dostáváme, že pevným bodem je vlastně i formule

$$D' = B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \Box C_2(B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \top])],$$

která vznikne z D akorát záměnou pořadí parametrů v B a záměnou $C_1(p)$ za $C_2(p)$ a naopak. Situace se nyní obrátila. Celkově tedy máme dva možné postupy výpočtu, které obecně dávají jiné výsledky.

Srovnejme oba výpočty. Dostáváme tedy pevný bod

$$D = B[\Box C_1(B[\top, \Box C_2(B[\Box C_1(B[\top, \top]), \top])]), \Box C_2(B[\Box C_1(B[\top, \top]), \top])],$$

nebo

$$D' = B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \Box C_2(B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \top])].$$

V prvním případě se nám ve výsledném pevném bodu vyskytuje „navíc“ formule C_2, ve druhém naopak C_1. Z toho můžeme usoudit, že v závislosti na velikosti a tvaru formulí C_1 a C_2 může být jeden z výpočtů výrazně výhodnější. To však záleží na řadě faktorů – složitosti formulí C_1 a C_2, počtu výskytů p v nich, ale také na počtu výskytů q_1 a q_2 v B. Mluvíme tedy pouze o relativní složitost v obecném případě, pro konkrétní formule může být vše zcela jinak.

Zmiňme se ještě o tom, ja by se situace změnila, kdyby se n zvýšilo. Vždy máme k dispozici tolik možných postupů, kolik je permutací (pořadí) na n prvcích, tedy konkrétně $n!$. Z příkladu lze vypozorovat, jak by situace probíhala pro $n = 3$ a také pro další n. Získáme tedy vždy jeden v obecném případě „nejjednodušší“ člen, další složitější, další ještě složitější a tak dále v závisloti na pořadí eliminace proměnných q_i. Složitost členů se v obecném případě postupně snižuje, tedy nejjednodušší bude ten odpovídající posledně eliminované proměnné.

Nyní se můžeme oprávněně ptát, zda by nešlo všechny výpočty nějakým způsobem spojit. Jinými slovy najít si pro každý parametr formule B nejjednodušší možnou variantu a uvažovat výslednou formuli. Jistou odpověď na tuto otázku nabídne algoritmus FP2, který budeme studovat poté, co krátce prozkoumáme složitostní aspekty algoritmu FP1.

4.2.1 Složitost pevných bodů

Náš algoritmus FP1 je velmi jednoduchý. Prostudujme nyní podrobněji jeho běh, abychom získali odhad jeho složitosti. Nejprve odhadneme velikost konstruovaného pevného bodu a následně si uvědomíme, jaký má tento odhad vztah k časové a prostorové složitosti algoritmu.

Klíčová je následující věta, ze které všechny uvedené odhady získáme jako jednoduché důsledky.

Věta 4.2.2. *Mějme libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, a její n-rozklad*

$$A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)],$$

pak algoritmus FP1B *nalezne pevný bod D, pro který platí*

$$\begin{array}{rcccl} \mathsf{subfl}(A(p)) & \leq & \mathsf{subfl}(D) & \leq & \mathsf{subfl}(A(p))^{2^n}, \\ \mathsf{depth}_{\mathsf{M}}(A(p)) & \leq & \mathsf{depth}_{\mathsf{M}}(D) & \leq & 2^n \cdot \mathsf{depth}_{\mathsf{M}}(A(p)). \end{array}$$

Důkaz. Ošetřeme jediný speciální případ a to $n = 0$. Pak je pevným bodem přímo $A(p)$ a tvrzení věty platí triviálně. V ostatních případech probíhá výpočet.

Abychom zjednodušili odhad složitosti, použijeme konstrukci spíše podobnou původnímu důkazu korektnosti než algoritmu FP1. Nový algoritmus 2 nazveme FP1B[19]. Místo formule B budeme během výpočtu pracovat s formulí $A(p)$ respektive s formulí B, která bude mít na pozicích q_i dosazenu příslušnou formuli $\Box C_i$. Máme tedy formuli A_1, to je formule $A(p)$. Ukažme, jak probíhá i-tý průchod cyklem v našem pozměněném algoritmu. V původním algoritmu nejprve získáváme formuli B'_i, v našem pozměněném bude tento krok reprezentovat nahrazení podformule $\Box C_i$ konstantou $\top$. Vzniklou formuli označme A'_i. Krok ve kterém vytváříme formuli $\Box C'_i$ vypouštíme a vznik formule B_{i+1} je pro nás nahrazením proměnné p ve formuli A_i formulí A'_i a to pouze na pozicích uvnitř příslušné formule $\Box C_i$. Dostáváme tak formuli A_{i+1}. Ekvivalentně lze předchozí vyjádřit jako nahrazení formule $\Box C_i(p)$ v A_i formulí $\Box C_i(A'_i)$. V této podobě je také zapsán algoritmus.

Nyní již odhady získáme snadno. Spodní odhady získáme okamžitě. Vycházíme od formule $A(p)$ a uvážíme-li oba kroky cyklu, délka formule ani modální hloubka neklesnou, neboť v druhém kroku cyklu vzrostou minimálně o tolik, o kolik v prvním kroku klesnou.

Horní odhady budou vyžadovat složitější úvahu. Nejprve odhadněme délku pevného bodu. Projděme si i-tý cyklus algoritmu. Máme jistou formuli A_i, jejíž velikost můžeme odhadnout například konstantnou d, nyní v ní podformuli $\Box C_i(p)$ nahradíme konstantnou $\top$, tím délku formule rozhodně nezvýšíme, formule A'_i má tedy stále délku nejvýše d. Nyní získáme formuli

[19] Význam dosazení, značíme $\leftarrow$, je v tomto případě, jak osvětlí text, spíše nahrazení než dosazení. Tedy $E\,[F \leftarrow G]$ má význam: „ve formuli E nahraď všechny výskyty F formulí G“. To není z algoritmického hlediska příliš šťastné, neboť testování na výskyt F v E může být s ohledem na složitost formule výpočetně dosti náročné. Navíc práce s formulemi $\Box C_i$ se v novém algoritmu také velmi komplikuje, neboť z prosté reprezentace výsledné formule není při nahrazování jasné, kterou podformuli máme přesně nahradit. Tyto technické detaily, které by implementaci velmi komplikovaly, nám však nyní pro účely odhadu složitosti výsledné formule nevadí.

Algoritmus 2 FP1B$(n, B[q_1, \ldots, q_n], \langle C_1, \ldots, C_n \rangle)$

Vstup: Libovolný n-rozklad $B[\Box C_1(p), \ldots, \Box C_n(p)]$, konkrétně hodnota n a formule $B[q_1, \ldots, q_n], C_1, \ldots, C_n$.

Výstup: Pevný bod formule $B[\Box C_1(p), \ldots, \Box C_n(p)]$.

```
if n = 0 then
  return B
else
  A_1 ⇐ B[□C_1(p), ..., □C_n(p)]
  for i = 1 to n do
    A'_i ⇐ A_i [□C_i(p) ← ⊤]
    A_{i+1} ⇐ A_i [□C_i(p) ← □C_i(A'_i)]
  end for
  return A_{n+1}
end if
```

A_{i+1} tak, že všechna p uvnitř podformule $C_i(p)$ formule A_i nahradíme formulí A'_i. Takových p rozhodně není více než je velikost A_i, tedy d a velikost A'_i jsme také odhadli pomocí d, velikost A_{i+1} je tedy nejvýše kvadratická vzhledem k d.

Vyjdeme-li od formule $A(p)$, která má velikost právě $\mathsf{subfl}(A(p))$, pak po každém průchodu cyklem dostaneme formuli nejvýše kvadratické velikosti, tedy po n průchodech cyklem dostáváme pevný bod D, pro který platí

$$\mathsf{subfl}(D) \leq \mathsf{subfl}(A(p))^{\overbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}^{n\text{-krát}}} = \mathsf{subfl}(A(p))^{2^n}.$$

Horní odhad modální hloubky pevného bodu získáme podobně. Předpokládejme, že jsme v i-tém cyklu. Modální hloubku A_i odhadněme pomocí konstanty h, nyní nahrazení $\Box C_i$ konstantou $\top$ rozhodně modální hloubku nezvýší, formule A'_i má tedy stále modální hloubku nejvýše h. Nyní dosazujeme do A_i, která má modální hloubku nejvýše h, za některé výskyty p, totiž ty uvnitř C_i, formuli A'_i. Tím se modální hloubka formule v nejhorším případě zdvojnásobí.

Vyjdeme-li znovu od formule $A(p)$, dostáváme po každém průchodu cyklem maximálně dvojnásobné zvětšení modální hloubky, a tedy po n krocích získáváme pevný bod D, pro který platí

$$\mathsf{depth}_{\mathsf{M}}(D) \leq 2^n \cdot \mathsf{depth}_{\mathsf{M}}(A(p)).$$

Q.E.D.

Předchozí věta má následující jednoduchý důsledek.

Důsledek 4.2.3. *Mějme libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, a její n-rozklad*

$$A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)],$$

pak algoritmus FP1B *nalezne pevný bod D, pro který platí*

$$\begin{array}{rcccl} \mathsf{subfl}(A(p)) & \leq & \mathsf{subfl}(D) & \leq & \mathsf{subfl}(A(p))^{2^{\mathsf{subfl}_{\mathsf{M}}(A(p))}}, \\ \mathsf{depth}_{\mathsf{M}}(A(p)) & \leq & \mathsf{depth}_{\mathsf{M}}(D) & \leq & 2^{\mathsf{subfl}_{\mathsf{M}}(A(p))} \cdot \mathsf{depth}_{\mathsf{M}}(A(p)). \end{array}$$

Důkaz. Z lemmatu 2.1.3 můžeme n triviálně omezit hodnotou $\mathsf{subfl}_{\mathsf{M}}(A(p))$. Q.E.D.

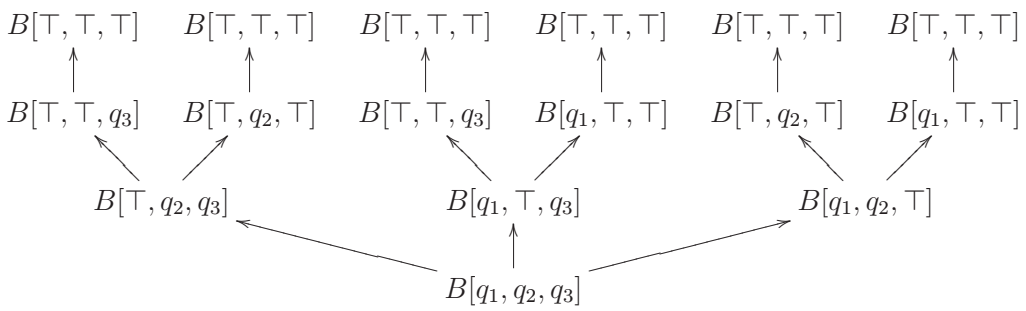
Předchozí odhad má dobrý smysl pouze pokud umíme pomocí algoritmu sestrojit příslušný n-rozklad. Na to můžeme využít například algoritmus kROZLmax. Ten sice nevydá optimální rozklad, pro náš odhad to však nehraje roli. Jeho výhodou je naopak nízká výpočtová složitost.

Z našich horních odhadů plyne, že maximální složitost konstruovaného pevného bodu roste velmi dramaticky vzhledem k počtu modalizovaných podformulí formule $A(p)$. V našich výpočtech jsme si toho neměli možnost všimnout, protože byly příliš krátké a zároveň jsme konstruované formule vhodně zkracovali. Nepopíráme, že náš odhad není zcela optimální a bylo by možné jej nepochybně zlepšit. Například při určování maximální modální hloubky dochází při dosazování konstanty $\top$ za $\Box C_i(p)$ ke snížení modální hloubky této formule o jedna. Ve výsledku tedy můžeme mít odhad lepší o $\mathsf{subfl}_{\mathsf{M}}(A(p))$, což je však zlepšení v daném případě zanedbatelné.

Mohli bychom pochopitelně odhadnout časovou a prostorovou složitost algoritmu. Pro tyto účely se však vrátíme k algoritmu FP1. Jeho prostudováním snadno zjistíme, že jeho časová a prostorová složitost je vlastně dána formulemi, se kterými pracuje, neboť jediné, co provádí, je dosazování formulí za proměnné do formulí . Navíc si můžeme všimnout, že žádná konstruovaná formule se během výpočtu „neztrácí“, tedy časová a prostorová složitost algoritmu pro vhodnou konstantu odpovídá délce konstruovaného pevného bodu pouze s přihlédnutím k použité reprezentaci formulí[20]. Délku pevného bodu jsme již odhadli, to že jsme k tomu použili algoritmus FP1B nevadí, neboť výsledná formule je v obou případech naprosto shodná. Naše pozorování tedy můžeme shrnout do následujícího tvrzení.

Tvrzení 4.2.4. *Časová a prostorová složitost algoritmu* FP1 *je dána horním odhadem délky pevného bodu s přihlédnutím k použité reprezentaci formulí.*

[20]Předpokládáme například, že k dosazení jedné formule do jiné formule za všechny výskyty nějaké proměnné vyžaduje nejvýše konstantněkrát více operací než je délka výsledné formule v použité reprezentaci.



Obrázek 11: Strom výpočtu

4.3 Třetí metoda výpočtu

Jako poslední popišme Sambinovu [Sam76, SV82] rekurzivní konstrukci pevných bodů podle n-rozložitelnosti formule $A(p)$. Mějme formuli $A(p)$, v níž se p vyskytuje pouze v modálním kontextu. Předpokládejme, že formule $A(p)$ je n-rozložitelná.

Jestliže je naše formule 0-rozložitelná, pak se v ní p vůbec nevyskytuje, a tedy sama formule $A(p)$ je pevným bodem. Je-li naopak n nenulové, budeme chtít problém převést na hledání pevných bodů pro jisté $(n-1)$-rozložitelné formule a z těchto n nalezených pevných bodů poté sestrojíme hledaný pevný bod. Tento postup můžeme iterovat, neboť vždy narazíme na 0-rozložitelné formule, pro které umíme pevný bod triviálně určit. Uvažujme libovolný pevný rozklad pro $n \neq 0$

$$A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)]$$

a definujme pro všechna i, $1 \leq i \leq n$, formule $A_i(p)$ jako

$$A_i(p) = B[\Box C_1(p), \ldots, \Box C_{i-1}(p), \top, \Box C_{i+1}(p), \ldots, \Box C_n(p)],$$

tím jsme získali n formulí, z nichž každá je $(n-1)$-rozložitelná a můžeme o nich předpokládat, že pro každé $A_i(p)$ umíme sestrojit pevný bod D_i, což jsme přesně plánovali. Pevný bod D pro formuli $A(p)$ definujeme jako

$$D =_{def} B[\Box C_1(D_1), \ldots, \Box C_n(D_n)].$$

Uvědomme si, že pro $n = 1$ je výpočet zcela shodný s větou 3.1.3 o sestrojování pevných bodů 1-rozložitelných formulí, lze se na něj tedy znovu dívat jako na jisté její přímé zobecnění. Předchozí metoda výpočtu pevných

bodů eliminovala postupně jednotlivé členy n-rozkladu za cenu neustálého zvětšování formule. Jednalo se v jistém smyslu o lineární postup. Tentokrát naopak sestrojujeme vlastně jistý strom výpočtu hloubky $(n+1)$, kde na i-té hladině má každý uzel $(n+1-i)$ následovníků, jak ukazuje pro $n=3$ obrázek 11, demostrující zároveň „průchod“ konstanty $\top$ stromem výpočtu. Velikost stromu je přesně dána. Kořen má n přímých následníků, každý z těchto n následníků pak $(n-1)$ přímých následníků a tak dále. Strom má tedy celkem $n!$ listů. Jeho hloubka je také snadno odhadnutelná z výše uvedené úvahy a to $(n+1)$, jedničku musíme přičíst kvůli kořeni.

Je vidět, že všechny listy v našem stromu jsou stejné, to však neznamená, že by byl stejný i výpočet. Jádrem výpočtu je totiž dosazování částečných pevných bodů, a to se již řídí tím, za které q_i se má dosazovat.

Dokažme, že Sambinova konstrukce opravdu dává pevný bod. Z konstrukce to zatím není příliš jasné. Použijeme jednoduchý sémantický důkaz, který navrhla Reidhaar-Olson [RO90]. Lze také použít poměrně jednoduchý syntaktický Lindströmův [Lin06] důkaz využívající lemma 2.2.6 o zobecněné jednoznačnosti pevných bodů.

Věta 4.3.1. *Nechť formule $A(p)$ je taková, že se v ní p vyskytuje pouze v modálním kontextu, pak existuje pevný bod D požadovaných parametrů, pro který platí*

$$\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to (p \equiv D).$$

Důkaz. S ohledem na to, že konstrukce je rekurzivní, bude se její korektnost dokazovat nejlépe indukcí podle n-rozložitelnosti formule. Pro $n=0$ vše platí triviálně z konstrukce.

Předpokládejme tedy, že pro n-rozložitelné formule již tvrzení věty platí a mějme libovolnou formuli $A(p)$, která je $(n+1)$-rozložitelná, a tedy

$$A(p) = B[\Box C_1(p), \ldots, \Box C_{n+1}(p)].$$

Z konsktruce máme pro libovolné $i \in \langle 1, n+1 \rangle$ pevný bod D_i. Ukažme, že platí následující klíčová vlastnost:

Tvrzení 4.3.2.

$$\mathsf{GL} \vdash \boxdot (p \equiv A(p)) \to \boxdot (\Box C_i(p) \equiv \Box C_i(D_i))$$

To dokážeme sémanticky. Zvolme tedy libovolně pevně kripkovský model $\mathcal{K} = \langle W, R, \Vdash \rangle$, jeho vrchol $w \in W$ a $i \in \langle 1, n+1 \rangle$. Ukažme, že kdykoliv

$$w \Vdash \boxdot (p \equiv A(p)), \tag{57}$$

pak již

$$w \Vdash \boxdot (\Box C_i (p) \equiv \Box C_i (D_i)) . \tag{58}$$

Z definice silné nutnosti a nutnosti je to ale to samé jako ukázat pro libovolné pevné u, které je w nebo je z w dosažitelné, tedy $u \in \{v; v = w \vee wRv\}$, platnost

$$u \Vdash \Box C_i (p) \equiv \Box C_i (D_i) . \tag{59}$$

Rozlišme dva případy:

1) $\mathsf{u} \Vdash \Box \mathsf{C_i} (\mathsf{p})$:
V tom případě triviálně platí

$$u \Vdash \Box C_i (p) \equiv \top .$$

To však také platí ve všech vrcholech dosažitelných z u, neboť ve všech je splněno $\Box C_i(p)$. Dostáváme tedy

$$u \Vdash \boxdot (\Box C_i (p) \equiv \top) .$$

Z prvního substitučního lemmatu 1.3.7 tak lze do libovolné formule substituovat $\top$ za $\Box C_i (p)$ při zachování splněnosti ve vrcholu u. Vezměme nyní do hry konstrukci pevných bodů. Z definice víme, že $A_i (p)$ vznikne z $A (p)$ tak, že do jeho rozkladu dosadíme místo $\Box C_i (p)$ prostě $\top$. V u tedy platí

$$u \Vdash A_i (p) \equiv A (p)$$

a navíc, neboť u je w či libovolný vrchol dosažitelný z w, máme

$$w \Vdash \boxdot (A_i (p) \equiv A (p)) ,$$

a tedy evidentně také

$$u \Vdash \boxdot (A_i (p) \equiv A (p)) ,$$

navíc z (57) můžeme odvodit

$$u \Vdash \boxdot (p \equiv A (p)) .$$

Prozkoumáním definice silné nutnosti, která sémanticky vlastně říká, že formule je splněna v daném vrcholu i ve všech dosažitelných, pak z předchozího snadno dostáváme

$$u \Vdash \boxdot (p \equiv A_i (p)) .$$

Z konstrukce je jasné, že A_i je n-rozložitelná a z indukční hypotézy pro ni tedy existuje pevný bod D_i, pro který platí

$$\mathsf{GL} \vdash \boxdot (p \equiv A_i (p)) \rightarrow (p \equiv D_i) ,$$

a tedy díky úplnosti dostáváme

$$u \Vdash p \equiv D_i,$$

navíc znovu z definice u a z toho, že bylo voleno libovolně platí

$$u \Vdash \boxdot (p \equiv D_i) .$$

Uvažme první substituční lemma 1.3.7 pro formuli $\Box C_i (p)$, pak dostáváme

$$u \Vdash \Box C_i (p) \equiv \Box C_i (D_i) ,$$

což dokončuje důkaz prvního případu, stačí vzít v úvahu, jak jsme volili u. Uvažíme-li ještě použití prvního substitučního lemmatu 1.3.7 na formuli $C_i (p)$, dostáváme vztah

$$u \Vdash C_i (p) \equiv C_i (D_i) , \tag{60}$$

který se nám bude hodit v důkazu druhého případu.

2) $u \nVdash \Box C_i (p)$:
Z definice nutnosti to znamená existenci vrcholu v dosažitelného z u, pro který

$$v \nVdash C_i (p) .$$

Můžeme volit vrchol v takový, že jeho $\mathcal{K}$-rank je minimální, tedy ve všech vrcholech v' dosažitelných z v je $C_i(p)$ splněno, a tedy

$$v \Vdash \Box C_i(p).$$

Nyní použijeme platnost vztahu (60), to můžeme, neboť jsme k jeho důkazu potřebovali pouze $u \Vdash \Box C_i(p)$ a neboť toto u bylo libovolné dosažitelné z w (či w), můžeme za něj volit v a dostáváme tak

$$\begin{aligned} v &\Vdash C_i\,(p) \;\equiv\; C_i\,(D_i)\,, \\ v &\nVdash C_i\,(D_i)\,, \end{aligned}$$

a neboť v je dosažitelné z u, máme hledané

$$u \nVdash \Box C_i\,(D_i)\,.$$

Důkaz celé věty teď již dokončíme poměrně jednoduše. Předpokládejme znovu libovolně pevně model $\mathcal{K} = \langle W, R, \Vdash\!\!-\rangle$ a svět $w \in W$, pro který

(61)
$$w \Vdash \boxdot\,(p \;\equiv\; A\,(p))\,,$$

pro libovolné i tedy z právě dokázaného tvrzení máme

$$w \Vdash \boxdot\,(\Box C_i\,(p) \;\equiv\; \Box C_i\,(D_i))\,.$$

Nyní uvažme $n+1$ aplikací prvního substitučního lemmatu 1.3.7 na formuli $B\,[q_1, \ldots, q_{n+1}]$ a dostáváme

$$w \Vdash B\,[\Box C_1\,(p)\,, \ldots, \Box C_{n+1}\,(p)] \;\equiv\; B\,[\Box C_1\,(D_1)\,, \ldots, \Box C_{n+1}\,(D_{n+1})]\,.$$

Uvědomíme-li si, že levá strana předchozí ekvivalence je vlastně $A\,(p)$ a pravá strana definice D, můžeme vše přepsat jako

$$w \Vdash A\,(p) \;\equiv\; D$$

a nyní z (61) dostáváme požadované

$$w \Vdash p \;\equiv\; D.$$

Neboť model $\mathcal{K}$ i vrchol w byly libovolné, dostáváme z úplnosti

$$\mathsf{GL} \vdash \boxdot\,(p \;\equiv\; A\,(p)) \to (p \;\equiv\; D)\,.$$

Q.E.D.

Algoritmus 3 FP2$(n, B, \langle q_1, \ldots, q_n \rangle, \langle C_1, \ldots, C_n \rangle)$

Vstup: Libovolný n-rozklad $B[\Box C_1(p), \ldots, \Box C_n(p)]$, konkrétně hodnota n a formule $B, C_1, \ldots, C_n$ a proměnné $\langle q_1, \ldots, q_n \rangle$.
Výstup: Pevný bod formule $B[\Box C_1(p), \ldots, \Box C_n(p)]$.

```
if n = 0 then
  return B
else
  for i = 1 to n do
    B'_i ⇐ B[q_i ← ⊤]
    Q'_i ⇐ ⟨q_1, ..., q_{i-1}, q_{i+1}, ..., q_n⟩
    C'_i ⇐ ⟨C_1, ..., C_{i-1}, C_{i+1}, ..., C_n⟩
    D_i ⇐ FP2(n − 1, B'_i, Q'_i, C'_i)
  end for
  return B [q_1 ← □C_1(D_1), ..., q_n ← □C_n(D_n)]
end if
```

Vraťme se zpět ke konstrukci pevného bodu a popišme si algoritmus, který ho počítá. Přijímáme stejné úmluvy jako v předchozím případě u algoritmu FP1. Algoritmus 3 nazvěme FP2. Mějme jistý n-rozklad formule $A(p)$, tedy

$$A(p) = B\left[\Box C_1(p), \ldots, \Box C_n(p)\right].$$

Vstupem algoritmu je znovu číslo n, formule $B\left[q_1, \ldots, q_n\right]$ a posloupnost formulí $C_1(p), \ldots, C_n(p)$. Navíc však také posloupnost proměnných $q_1, \ldots, q_n$. Program pracuje rekurzivně a tato posloupnost se nám bude hodit k tomu, abychom mohli pracovat s dosazováním konstanty $\top$ za příslušné q_i do B. Připomeňme znovu, že formule $A(p)$ není přímo vstupem algoritmu, ale je rozložena na formuli B a formule $C_1(p), \ldots, C_n(p)$, a lze ji tedy kdykoliv z těchto formulí získat.

Již jsme zmínili, že program bude fungovat rekurzivně. To odpovídá definici konstrukce, kterou jsme podali, neboť ta byla také rekurzivní. Jestliže je tedy $n = 0$, nevyskytuje se v B již žádné q_i a pevným bodem je samo B, to odpovídá přesně popisu konstrukce. Nechť je naopak $n \geq 1$, pak musíme postupovat stromem výpočtu, tedy vytvoříme n větví, na každé dosadíme do B za příslušné q_i konstantu $\top$ a rekurzivně voláme algoritmus na tuto novou formuli. V algoritmu provádíme pomocné operace, nejprve získáme pomocnou formuli B'_i, která vznikne dosazením $\top$ za q_i do B. Poté následují dva technické kroky, které nám z posloupností $q_1, \ldots, q_n$ a $C_1, \ldots, C_n$ odstraní q_i respektive C_i, to se nám hodí k rekurzivnímu zápisu algoritmu. Nyní rekurzivně voláme algoritmus, abychom zjistili pevný bod D_i pro každou z n

formulí B'_i. Těchto n pevných bodů D_i pak dosadíme do příslušné formule $\Box C_i$ za proměnnou p a výsledek pak za q_i do formule B. To přesně odpovídá konstrukci.

Připomeňme ještě jednou, že algoritmus je rekurzivní. Tedy dosadíme-li za jistou proměnnou q_i konstantu $\top$ a následně ji před rekurzivním voláním odstraníme z posloupnosti $q_1, \ldots, q_n$, pak po rekurzivním zavolání algoritmu již indexy neodpovídají, neboť posloupnost $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n$ se po zavolání vlastně stane posloupností $q_1, \ldots, q_{i-1}, q_i, \ldots, q_{n-1}$. To samé platí pro posloupnost $C_1, \ldots, C_n$.

Fungování algoritmu nejlépe osvětlí jednoduchý příklad. Stejně jako u algoritmu FP1 formule během výpočtu vhodně zkracujeme.

Příklad 4.3.1. Mějme formuli $A(p) = \Box(p \to g) \to \Box\neg p$, máme $B = q_1 \to q_2$, $C_1 = p \to g$ a $C_2 = \neg p$. Postupujme podle algoritmu FP2:

$$
\begin{aligned}
B &= q_1 \to q_2 \\
&\quad B'_1 = \top \to q_2 = q_2 \\
&\quad Q'_1 = \langle q_2 \rangle \\
&\quad C'_1 = \langle C_2 \rangle = \langle \neg p \rangle \\
&\quad D_1 = \mathrm{FP2}(1, q_2, \langle q_2 \rangle, \langle \neg p \rangle) \\
&\qquad\quad B'_1 = \top \\
&\qquad\quad Q'_1 = \langle \emptyset \rangle \\
&\qquad\quad C'_1 = \langle \emptyset \rangle \\
&\qquad\quad D_1 = \mathrm{FP2}(0, \top, \langle \emptyset \rangle, \langle \emptyset \rangle) \\
&\qquad\qquad\quad D = \top \\
&\qquad\qquad = \top \\
&\qquad\quad D = \Box\neg\top = \Box\bot \\
&\quad = \Box\bot \\
&\quad B'_2 = q_1 \to \top = \top \\
&\quad Q'_2 = \langle q_1 \rangle \\
&\quad C'_2 = \langle C_1 \rangle = \langle p \to g \rangle \\
&\quad D_2 = \mathrm{FP2}(1, \top, \langle q_1 \rangle, \langle p \to g \rangle) \\
&\qquad\quad B'_1 = \top \\
&\qquad\quad Q'_1 = \langle \emptyset \rangle \\
&\qquad\quad C'_1 = \langle \emptyset \rangle \\
&\qquad\quad D_1 = \mathrm{FP2}(0, \top, \langle \emptyset \rangle, \langle \emptyset \rangle) \\
&\qquad\qquad\quad D = \top \\
&\qquad\qquad = \top \\
&\qquad\quad D = \top \\
&\quad = \top \\
D &= \Box(\Box\bot \to g) \to \Box\neg\top = \Box(\Box\bot \to g) \to \Box\bot.
\end{aligned}
$$

Pevným bodem D je tedy formule $\Box(\Box\bot \to g) \to \Box\bot$.

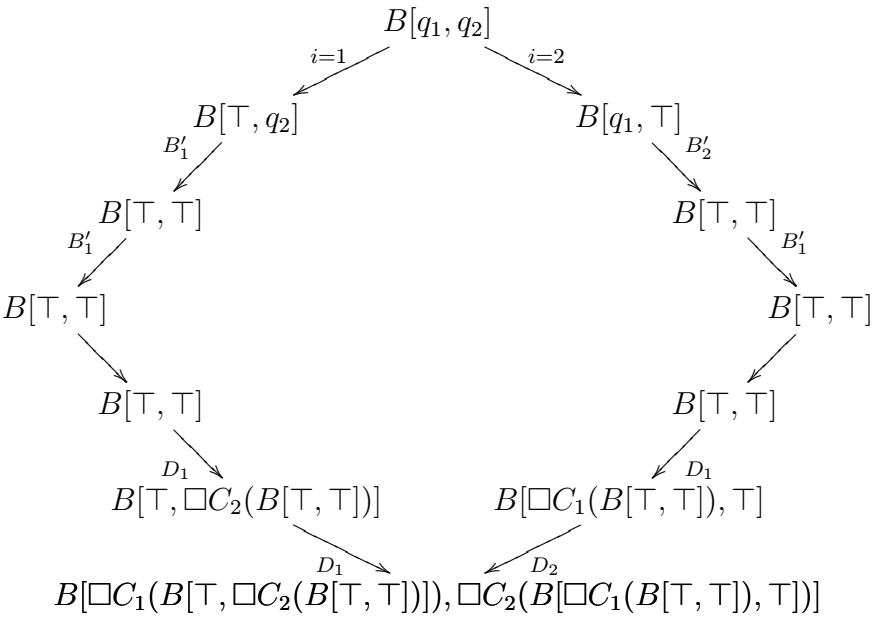
Poznamenejme, že jsme si druhou půlku výpočtu v předchozím příkladě mohli zcela ušetřit, neboť v okamžiku, kdy jsme rekurzivně volali algoritmus s hodnotou B rovnou $\top$, nemohli jsme získat jinou odpověď než $\top$, neboť libovolným dosazováním do této formule získáme znovu pouze $\top$.

Přestože se předchozí výpočet může zdát ve srovnání s výpočty pomocí algoritmu FP1 dlouhý, je to způsobeno především množstvím operací spojených s rekurzí. Srovnejme nyní algoritmus FP2 s algoritmem FP1. U algoritmu FP1 jsme uvedli příklad 4.2.5, který demonstroval výpočet pro obecnou 2-rozložitelnou formuli. Proveďme stejný výpočet i pro algoritmus FP2. Navíc poznamenejme, že pro $n = 0$ a $n = 1$ se výsledek algoritmů FP1 a FP2 očividně neliší.

Příklad 4.3.2. Mějme formuli

$$A(p) = B\left[\Box C_1(p), \Box C_2(p)\right],$$

máme tedy $B[q_1, q_2]$. Postupujme podle algoritmu FP2 a dostáváme výpočet, který můžeme reprezentovat následujícím obrázkem, kde první větvení symbolizuje dvě větve výpočtu pro $n = 2$, rozšiřování pak průchod rekurzí a sbíhání naopak návrat rekurzí.



Srovnejme nyní výpočet s příkladem 4.2.5, a tedy výpočtem pomocí algoritmu FP1. Nejprve poznamenejme, že zatímco u algoritmu FP1 jsme

mohli výpočet provádět v závislosti na pořadí eliminace proměnných dvěma způsoby, tentokrát takovou možnost nemáme. Výpočet nemůže v žádném případě ovlivnit pořadí paramentrů v rozkladu, respektive dojde pouze k permutaci větví výpočtu, ale výsledek bude vždy stejný. Připomeňme, že jsme algoritmem FP1 dostali dvě varianty pevného bodu, buď

$$D_a = B[\Box C_1(B[\top, \Box C_2(B[\Box C_1(B[\top, \top]), \top])]), \Box C_2(B[\Box C_1(B[\top, \top]), \top])],$$

nebo

$$D_b = B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \Box C_2(B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \top])].$$

Uvážíme-li pevný bod získaný algoritmem FP2

$$D = B[\Box C_1(B[\top, \Box C_2(B[\top, \top])]), \Box C_2(B[\Box C_1(B[\top, \top]), \top])],$$

zjistíme, že jde o kombinaci obou předchozích výsledků, tedy první parametr B v D je prvním parametrem B v D_b a druhý parametr B v D je druhým parametrem B v D_a. Na otázku, kterou jsme si položili na konci zkoumání příkladu 4.2.5, zda by šlo výpočty kombinovat a dostat tak menší pevný bod, je tedy alespoň pro $n = 2$ odpověď kladná.

Nyní bychom se mohli pokusit tento výsledek zobecnit a ukázat, že tomu tak bude i pro větší n. Poznamenejme však, že vztah nebude tak jednoduchý, jak by se mohlo zdát z případu $n = 2$, neboť pro vyšší n nám algoritmus FP2 nabízí stále jedinou variantu výpočtu, zatímco FP1 jich v závislosti na pořadí C_i nabízí $n!$. Nemůžeme proto předpokládat, že by pevný bod FP2 byl znovu kombinací „nejlepších částí“ pevných bodů vydávaných algoritmem FP1. Například pro $n = 3$ lze částečně vypozorovat, budeme-li zkoumat oba příklady 4.2.5 a 4.3.2, že algoritmus FP2 již bude v obecném případě dávat výsledky takové, že všechny tři parametry B ve výsledném pevném bodu budou v obecném případě kratší než příslušné parametry B v pevném bodu vydaném algoritmem FP1. Podrobně dokazovat to však nebudeme, neboť by takový důkaz byl dosti pracný. Jistou částečnou odpověď na tuto otázku nám poskytne srovnání horních odhadů složitosti pevných bodů.

4.3.1 Složitost pevných bodů

Pokusme se nyní, stejně jako v případě algoritmu FP1, určit spodní a horní odhady délky a modální hloubky pevných bodů konstruovaných algoritmem FP2. Pomocí tohoto výsledku se také znovu pokusíme odhadnout časovou a prostorovou složitost algoritmu.

Stěžejní pro naše další zkoumání je tedy následující věta.

Věta 4.3.3. *Mějme libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, a její n-rozklad*

$$A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)],$$

pak algoritmus FP2 *nalezne pevný bod D, pro který platí*

$$\begin{array}{rcccl} \mathsf{subfl}(A(p)) & \leq & \mathsf{subfl}(D) & \leq & \mathsf{subfl}(A(p))^{n+1}, \\ \mathsf{depth_M}(A(p)) & \leq & \mathsf{depth_M}(D) & \leq & (n+1) \cdot \mathsf{depth_M}(A(p)). \end{array}$$

Důkaz. Pro $n = 0$ platí věta triviálně, předpokládejme tedy $n \geq 1$. Nejprve proveďme spodní odhady. Ty získáváme okamžitě, pokud se podíváme na poslední instrukci programu, která vydává výsledný pevný bod. Nahrazení proměnných p v $A(p)$ pevnými body $D_1, \ldots, D_n$, tak je nutno instrukci chápat, nepochybně nesníží délku ani modální hloubku formule.

Oba horní odhady budeme provádět s využitím stromu výpočtu, připomeňme obrázek 11. Označme číslo udávající kolik q_i zůstává v B, tedy kolik jich ještě nebylo nahrazeno konstantou $\top$, jako hladinu výpočtu. Na nulté hladině máme formuli $B[\top, \top, \ldots, \top]$ a jsme tedy v listech stromu výpočtu.

Odhadněme nejprve délku pevného bodu. Každý z listů stromu výpočtu, neboli formule $B[\top, \top, \ldots, \top]$, má délku, kterou můžeme omezit délkou $A(p)$. Zvolme si nyní libovolně pevně jednu větev výpočtu a postupujme až do kořene. Z nulté hladiny se přesuneme na hladinu jedna, tam výsledek D_1 z minulé hladiny vlastně dosazujeme za p do formule $B[\top, \ldots, \Box C_i(p), \ldots, \top]$, jejíž délka rozhodně není větší než délka $A(p)$. Dosazením formule délky nejvýše $A(p)$ tedy dostáváme formuli délky nejvýše kvadratické vzhledem k délce $A(p)$. Na hladině dva již dosazujeme dva výsledky D_1 a D_2, o každém můžeme předpokládat, že má délku nejvýše kvadratickou vzhledem k $A(p)$. Nyní dosazujeme do formule $B[\top, \ldots, q_i, \ldots, q_j, \ldots, \top]$, jejíž délku lze znovu odhadnout velikostí $A(p)$. Dosazováním formulí, které mají kvadratickou délku vzhledem k $A(p)$, tedy dostáváme formuli délky nejvýše $\mathsf{subfl}(A(p))^3$.

Takto bychom mohli pokračovat dále, na i-té hladině máme formuli délky maximálně

$$\mathsf{subfl}(A(p))^{i+1},$$

tedy na n-té hladině dostáváme hledaný pevný bod D, pro který platí

$$\mathsf{subfl}(D) \leq \mathsf{subfl}(A(p))^{n+1}.$$

Modální hloubku pevného bodu odhadneme analogicky. Na nulté hladině máme formuli $B[\top, \top, \ldots, \top]$, ta má modální hloubku nejvýše takovou jako formule $A(p)$. Na hladině jedna dosazujeme formuli hloubky nejvýše $A(p)$ do formule $B[\top, \ldots, \Box C_i(p), \ldots, \top]$, která má také modální hloubku

nejvýše $A(p)$, výsledná formule má tedy modální hloubku nejvýše dvojnásobek modální hloubky $A(p)$. Na hladině dva dosazujeme do formule $B[\top, \ldots, q_i, \ldots, q_j, \ldots, \top]$, která má modální hloubku znovu nejvýše $A(p)$, dvě formule, obě s modální hloubkou nejvýše dvakrát větší než $A(p)$, celkově tedy dostáváme formuli hloubky nejvýše $3 \cdot \mathsf{depth}_{\mathsf{M}}(A(p))$.

Obecně pak na i-té hladině dostáváme formuli modální hloubky nejvýše

$$(i+1) \cdot \mathsf{depth}_{\mathsf{M}}(A(p)),$$

a tedy na n-té hladině pro výsledný pevný bod D platí

$$\mathsf{depth}_{\mathsf{M}}(D) \leq (n+1) \cdot \mathsf{depth}_{\mathsf{M}}(A(p)).$$

Q.E.D.

Uveďme nyní jednoduchý důsledek předchozí věty.

Důsledek 4.3.4. *Mějme libovolnou formuli $A(p)$, ve které se p vyskytuje pouze v modálním kontextu, a její n-rozklad*

$$A(p) = B[\Box C_1(p), \ldots, \Box C_n(p)],$$

pak algoritmus FP2 *nalezne pevný bod D, pro který platí*

$$\begin{array}{rcccl} \mathsf{subfl}(A(p)) & \leq & \mathsf{subfl}(D) & \leq & \mathsf{subfl}(A(p))^{\mathsf{subfl}_{\mathsf{M}}(A(p))+1}, \\ \mathsf{depth}_{\mathsf{M}}(A(p)) & \leq & \mathsf{depth}_{\mathsf{M}}(D) & \leq & (\mathsf{subfl}_{\mathsf{M}}(A(p))+1) \cdot \mathsf{depth}_{\mathsf{M}}(A(p)). \end{array}$$

Důkaz. Z lemmatu 2.1.3 můžeme n triviálně omezit hodnotou $\mathsf{subfl}_{\mathsf{M}}(A(p))$.
Q.E.D.

Znovu poznamenejme, že předchozí odhad má dobrý smysl pouze pokud umíme pomocí algoritmu sestrojit příslušný n-rozklad. K tomu můžeme využít například algoritmus kROZLmax. Ten sice nevydá optimální rozklad, pro náš odhad to však nehraje roli. Jeho výhodou je naopak nízká výpočtová složitost.

Ve srovnání s algoritmem FP1 jsme získali výrazně lepší horní odhady. Přesto můžeme stále pozorovat, že délka pevného bodu roste velmi dramaticky se vzrůstajícím počtem modalizovaných podformulí, a to exponenciálně vzhledem k délce $A(p)$. Růst modální hloubky není tak drastický, přesto nedosahuje odhadu, který jsme získali u sémantické metody sestrojování pevných bodů.

V případě algoritmu FP1 jsme nyní pomocí jednoduchého pozorování odhadli také časovou a prostorovou složitost algoritmu. Pokusme se stejným

způsobem odhadnout i složitost algoritmu FP2. Na první pohled je situace tentokráte komplikovanější, neboť máme rekurzivní algoritmus.

Jeho pečlivým prozkoumáním však znovu zjistíme, že podstatou výpočtu je opět pouze dosazování formulí za proměnné do jiných formulí a že se nám formule během výpočtu „neztrácejí“. Provádíme sice některé další pomocné operace, délka formulí, které do nich vstupují, je však odhadnutelná délkou formulí účastnících se přímo výpočtu pevného bodu, případně odhadnutelná délkou $A(p)$. Pomocné operace a rekurze tak prodlouží s přihlédnutím k použité reprezentaci formulí výpočet pouze konstantněkrát. Můžeme tedy stejně jako v případě algoritmu FP1 vyslovit následující tvrzení.

Tvrzení 4.3.5. *Časová a prostorová složitost algoritmu* FP2 *je dána horním odhadem na délky pevného bodu s přihlédnutím k použité reprezentaci formulí.*

Závěr

V předchozím textu jsme se snažili poměrně podrobně diskutovat explicitní výpočty pevných bodů v logice dokazatelnosti GL. Postupně jsme získali pevné body následujících formulí:

Formule	**Pevný bod**
$\Box p$	$\top$
$\Box\neg p$	$\Box\bot$
$\Box(p \to g)$	$\Box g$
$\neg\Box p$	$\neg\Box\bot$
$\Box p \to g$	$\Box g \to g$
$\Box(p \vee g_1) \wedge \ldots \wedge \Box(p \vee g_2)$	$\top$
$\Box(p \wedge g_1) \vee \ldots \vee \Box(p \wedge g_2)$	$\Box g_1 \vee \ldots \vee \Box g_n$
$\neg\Box p \wedge \Box\neg\Box p$	$\bot$
$\Box(\neg p \to \Box\bot) \to \Box(p \to \Box\bot)$	$\Box\Box\Box\bot \to \Box\Box\bot$
$\Box p \to \Box\neg p$	$\Box\Box\bot \to \Box\bot$
$\Box(p \to g) \vee \Box(p \to \neg g)$	$\Box g \vee \Box\neg g$
$\neg\Box p \wedge \Box p$	$\bot$
$\Box(\Box p \to g) \wedge \neg\Box p$	$\Box(\Box\bot \to g) \wedge \neg\Box\bot$
$\Box(p \to g) \to \Box\neg p$	$\Box(\Box\bot \to g) \to \Box\bot$

Nyní můžeme číst formule v levém sloupci metamatematicky. Modální operátor nutnosti interpretujeme jako dokazatelnost, tedy $\Box$ čteme jako „dokazuje“, $\neg\Box$ čteme „nedokazuje“ a konstantu $\bot$ čteme „spor“.

První formule $\Box p$, zapsaná v podobě autoreferenční rovnice $p \equiv \Box p$, tvrdí vlastní dokazatelnost, jde tedy o Henkinovu formuli. Jejím řešením je konstanta $\top$, neboli dokazatelná sentence, což již víme z Löbova výsledku. Přirozeným řešením autoreferenční formule $\Box\neg p$, která tvrdí, že je dokazatelná její vlastní negace, je pochopitelně $\Box\bot$, tedy sentence ekvivalentní dokazatelnosti sporu. Formuli $\neg\Box p$ tvrdící vlastní nedokazatelnost známe dobře, jde o Gödelovu formuli. Z Druhé Gödelovy věty víme, jaké má tato formule řešení autoreferenční rovnice. Je jím sentence ekvivalentní s $\neg\Box\bot$, neboli nedokazatelností sporu, tedy konzistencí teorie. Formule $\Box p \to g$ je použita v důkazu Löbovy věty, jejím pevným bodem je formule $\Box g \to g$.

Přestože umíme prostřednictvím logiky GL spočítat pevný bod libovolné gödelovské autoreferenční rovnice, není autorovi známo, že by tak někdo ve větším měřítku činil. Význam našich výpočtů tak nelze z metamatematického hlediska přeceňovat. To souvisí také s tím, že zajímavé gödelovské auto-

referenční rovnice již byly zkoumány dříve jinými prostředky. Podle [JdJ98] lze dokonce věty o pevných bodech v logice GL chápat v jistém smyslu také jako negativní výsledek. Chceme-li totiž pomocí věty o autoreferenci sestrojit formuli se zajímavými novými vlastnostmi, nezískáme je jako řešení gödelovských autoreferenčních rovnic. Jediné dvě výjimky jsou Gödelova a Löbova sentence. To je také jeden z důvodů, proč většina zajímavých pevných bodů využívá Rosserovy konstrukce, neboť jak jsme se již zmínili, některé takové rovnice nemají jednoznačná řešení [GS79].

Podařilo se nám získat několik způsobů, jak počítat pevné body. Některé jsou velmi efektivní, použitelné však pouze ve speciálních případech. Pro obecné formule jsme získali tři postupy. První nám poskytl cenný odhad na maximální modální hloubku pevného bodu, ukázal se však výpočetně zcela neefektivní. Další dva přístupy mají hodně společného. Přestože odhady sestrojené pro druhou metodu nebyly příliš optimistické, dosáhli jsme ve všech našich jednoduchých příkladech vhodným zkracováním velmi krátkých výpočtů. Se vzrůstající složitostí formule by se pochopitelně situace komplikovala. Ukázala by se také výhoda třetí metody, která se na jednoduchých příkladech mohla jevit náročnější než metoda druhá. Třetí metoda nám navíc poskytla výrazně lepší odhad maximální délky pevného bodu.

V tématech studovaných v této práci by bylo možné pokračovat mnoha způsoby. Bylo by možno například podrobněji prozkoumat k-rozložitelnost a především její vypočtovou složitost při hledání minimálního rozkladu. V naší práci jsme se celkově explicitním zkoumáním výpočtové složitosti algoritmů nevěnovali příliš podrobně. Dalším zajímavým tématem by mohlo být zkoumání souvislosti druhé a třetí obecné výpočetní metody pro $n \geq 3$. My jsme jistý částečný výsledek pouze naznačili. Neukázali jsme také žádný příklad formule, která má pevné body například pouze exponenciálně delší než je sama. Navíc nevíme, zda takové tvrzení vůbec platí, tedy zda například nelze k libovolné formuli sestrojit pevný bod pouze polynomiální délky vzhledem k původní formuli.

Zcela jsme pominuli algebraický přístup k logice dokazatelnosti, který pochází od Magariho a jeho skupiny z univerzity v Sieně. Algebraické postupy využívají například původní Sambinovy konstrukce [Sam74, Sam76]. Existuje celá řada na sebe navazujících článků studujících logiku dokazatelnosti algebraicky, čtenář může některé reference získat například z monografie [Smo85]. Podobně jsme mohli některé naše úvahy provádět v gentzenovském kalkulu, který se v naší práci vůbec neobjevil.

Nepochybně zajímavé by také mohlo být konkrétní implementování zde uvedených algoritmů pro výpočet pevných bodů. Bylo by tak například

možno zkoušet jejich chování na velkých souborech automaticky generovaných formulí. S ohledem na vysokou výpočtovou složitost těchto algoritmů a obecné zkušenosti s těmito postupy by však nebylo rozumné vkládat do nich přehnané naděje. Na druhou stranu může jít o užitečné pomocníky při testování různých hypotéz. Ostatně věty o pevných bodech jsou vlastně do značné míry výsledkem různých pokusů a náročných výpočtů.

Literatura

[AB04] S. Artemov a L. Beklemishev. Provability logic. V D. Gabbay a F. Guenthner, editoři, *Handbook of Philosophical Logic*, str. 229–403. Kluwer, Dordrecht, 2. vydání, 2004.

[Bek90] L. D. Beklemishev. On the classification of propositional provability logics. *Math. USSR Izvestiya*, 35:247–275, 1990.

[Boo79] G. Boolos. *The Unprovability of Consistency.* Cambridge University Press, 1979.

[Boo93] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1993.

[BS91] G. Boolos a G. Sambin. Provability: the emergence of a mathematical modality. *Studia Logica*, L(1):1–23, 1991.

[Bí07] M. Bílková. *Interpolation in Modal Logics.* Ph.D. disertace, Filozofická fakulta Univerzity Karlovy, 2007.

[Fit96] M. Fitting. A program to compute gödel-löb fixpoints. *Bulletin EATCS*, 58:118–130, 1996.

[GG90] Z. Gleit a W. Goldfarb. Characters and fixed points in provability logic. *Notre Dame J. Formal Logic*, 31:26–36, 1990.

[GS79] D. Guaspari a R. M. Solovay. Rosser sentences. *Annals of Math. Logic*, 16:81–99, 1979.

[ChZ97] A. Chagrov a M. Zakharyaschev. *Modal Logic.* Oxford University Press, 1997.

[JdJ98] G. Japaridze a D. de Jongh. The logic of provability. V S. R. Buss, editor, *Handbook of Proof Theory*, str. 475–536. Elsevier Science Publishers, Amsterdam, 1998.

[Kra99] M. Kracht. *Tools and Techniques in Modal Logic.* Číslo 142 řady Studies in Logic and the Foundations of Mathematics. Elsevier, 1999.

[Lad77] R. E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal of Computation*, 6:3:467–480, 1977.

[Lin06] P. Lindström. Note on some fixed point constructions in provability logic. *J. Philosophical Logic*, 35:225–230, 2006.

[Löb55] M. H. Löb. Solution of a problem of Leon Henkin. *J. Symbolic Logic*, 20:115–118, 1955.

[Mon93a] F. Montagna. Characters and fixed points in provability logic. by Zachary Gleit, Warren Goldfarb. *J. Symbolic Logic*, 58(2):715, 1993. (recenze).

[Mon93b] F. Montagna. A new proof of the fixed-point theorem of provability logic. by Lisa Reidhaar-Olson. *J. Symbolic Logic*, 58(2):714–715, 1993. (recenze).

[RO90] L. Reidhaar-Olson. A new proof of the fixed-point theorem of provability logic. *Notre Dame J. Formal Logic*, 31:37–43, 1990.

[Sac99] L. Sacchetti. Modal logics with the fixed-point property. *Bollettino della Unione Matematica Italiana*, 2:279–90, 1999.

[Sac01] L. Sacchetti. The fixed point property in modal logic. *Notre Dame J. Formal Logic*, 42(2):65–86, 2001.

[Sac02] L. Sacchetti. Incompleteness and fixed points. *Math. Log. Q*, 48(1):15–28, 2002.

[Sam74] G. Sambin. Un estensione del theorema di Löb. *Rend. Sem. Math. Univ. Padova*, 52, 1974.

[Sam76] G. Sambin. An effective fixed-point theorem in intuitionistic diagonalizable algebras. *Studia Logica*, 35(4):345–361, 1976.

[Smo79] C. Smoryński. Calculating self-referential statements, I: Explicit calculations. *Studia Logica*, 38, 1979.

[Smo85] C. Smoryński. *Self-Reference and Modal Logic.* Springer, New-York, 1985.

[Sol76] R. M. Solovay. Provability interpretations of modal logic. *Israel J. Math.*, 25, 1976.

[SV82] G. Sambin a S. Valentini. The modal logic of provability: The sequential approach. *Journal of Philosophical Logic*, 11:311–342, 1982.

[Šv00] V. Švejdar. On Provability Logic. *Nordic J. Philosophical Logic*, 4(2):95–116, 2000.

[Šv02] V. Švejdar. *Logika: neúplnost, složitost a nutnost.* Academia, 2002.

[Šv03] V. Švejdar. The decision problem of provability logic with only one atom. *Archive for Math. Logic*, 42:763–768, 2003.