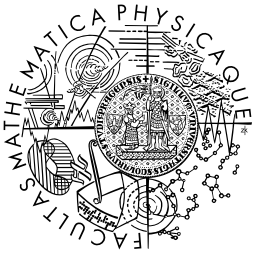

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Jan Kolář

Dosvědčování existenčních vět

Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Jan Krajíček, DrSc.
Studijní program: Matematika
Studijní obor: Matematické struktury

Praha 2021

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Rád bych na tomto místě poděkoval vedoucímu své diplomové práce prof. RNDr. Janu Krajíčkovi, DrSc. za nabídku zajímavého tématu, vysvětlení problematiky, cenné rady a věnovaný čas.

Název práce: Dosvědčování existenčních vět

Autor: Jan Kolář

Katedra: Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Jan Krajíček, DrSc., Katedra algebry

Abstrakt: Tato práce formuluje a dokazuje dosvědčovací větu pro tvrzení dokazatelná v teorii S_{PV} tvaru $\forall x \exists y A(x, y)$, kde A odpovídá relaci rozhodnutelné v polynomiálním čase. Teorií S_{PV} se zde rozumí rozšíření teorie T_{PV} (univerzální teorie $\mathbb{N}_0$ v jazyce reprezentujícím polynomiální algoritmy) o přidané axiomy zajišťující existenci minima lineárního uspořádání definovaného polynomiální relací na počátečním úseku. Jelikož tyto přidané axiomy nejsou univerzální sentence, vyžaduje teorie S_{PV} netriviální použití dosvědčovacích vět Herbrandovy a KPT, které mají přímé použití pouze pro teorie univerzální. Na základě dokázané dosvědčovací věty je odvozen NP vyhledávací problém charakterizující složitost nalezení y pro zadané x tak, aby platilo $A(x, y)$. Část práce je věnována argumentům podporujícím domněnku, že teorie S_{PV} je ostře silnější než T_{PV}.

Klíčová slova: formální teorie, polynomiální algoritmus, složitost, dosvedčování

Title: Witnessing of existential statements

Author: Jan Kolář

Department: Department of Algebra

Supervisor: prof. RNDr. Jan Krajíček, DrSc., Department of Algebra

Abstract: The thesis formulates and proves a witnessing theorem for S_{PV}-provable formulas in the form $\forall x \exists y A(x, y)$ where A corresponds to a polynomial time decidable relation. By S_{PV} we understand an extension of the theory T_{PV} (the universal theory of $\mathbb{N}$ in the language representing polynomial algorithms) by additional axioms ensuring the existence of a minimum of a linear ordering defined by a polynomial time decidable relation on an initial segment. As these additional axioms are not universal sentences, the theory S_{PV} requires nontrivial use of witnessing Herbrand's and KPT theorems which have direct application only for universal theories. Based on the proven witnessing theorem, we derive a NP search problem characterizing complexity of finding y for a given x such that $A(x, y)$. A part of the thesis is dedicated to arguments supporting the conjecture that S_{PV} is strictly stronger than T_{PV}.

Keywords: formal theory, polynomial algorithm, complexity, witnessing

Obsah

Úvod

Dosvědčování existenčních vět tvaru $\forall x \exists y A(x, y)$ a $\forall x \exists y \forall z B(x, y, z)$, kde A je otevřená formule (bez kvantifikátorů) a B je existenční formule, lze v univerzálních teoriích (axiomatizovaných univerzálními sentencemi) zkoumat pomocí Herbrandovy věty (v. 3) a KPT věty (v. 5). Tyto věty použitím na teorii T_{PV}, tedy univerzální teorii $\mathbb{N}_0$ v jazyce L_{PV} reprezentujícím polynomiální algoritmy, viz def. 2, dávají do přímé souvislosti dokazatelnost existenční věty a algoritmickou složitost dosvědčitelnosti, tedy nalezení y pro zadané x. Již v případě teorií rozšiřujících univerzální teorii o jedno schéma axiomů se však situace může stát podstatně komplikovanější a zmíněné věty nelze použít přímo.

Cílem této práce je ukázat souvislost mezi dokazatelností existenční formule tvaru $\forall x \exists y A(x, y)$ v teorii S_{PV} (tj. T_{PV} s axiomy existence minima lineárního uspořádání definovaného polynomiální relací na počátečním úseku, viz def. 13) a konkrétní třídou NP vyhledávacích problémů (def. 7) jakožto třídou složitosti nalezení x pro zadané y, tak aby platilo $A(x, y)$. Tato snaha je inspirována podobnou již dokázanou souvislostí mezi teorií $NP - IND$ (T_{PV} s omezenou indukcí) a třídou PLS (polynomiální lokální vyhledávání), viz (Krajíček, 2010), (Buss a Krajíček, 1994).

Kapitola 1 shrnuje základní poznatky o dosvědčování existenčních vět v univerzálních teoriích včetně důsledků pro teorii T_{PV}.

Kapitola 2 slouží jako krátké seznámení s NP vyhledávacími problémy.

V kapitole 3 je prezentována teorie S_{PV}, její síla a argumenty podporující domněnku, že tato teorie je silnější než T_{PV}. Z opačného předpokladu $T_{PV} = S_{PV}$ jsou odvozeny jen těžko uvěřitelné důsledky pro teorii složitosti a kryptografii. Dále je dokázána analogie této domněnky pro teorie s orákulem pro binární relaci.

V kapitole 4 je pak odvozena samotná dosvědčovací věta (v. 30) pro teorii S_{PV} a její slovní popis jako hry mezi studentem a učitelem odvozený od hry popisující KPT větu. Dále je pomocí této věty odvozeno (důsl. 31), že složitost problému dosvědčování formule $\forall x \exists y A(x, y)$ dokazatelné v S_{PV} je složitostí konkrétní třídy NP vyhledávacích problémů.

1. Dosvědčování v teorii $\mathbf{T_{PV}}$

1.1 Jazyk $\mathbf{L_{PV}}$

Uvažujme pevně zvolený polynomiální deterministický algoritmus, který dvojici (T, p), kde T označuje Turingův stroj a p je polynom v jedné proměnné s kladnými koeficienty, přiřadí Turingův stroj T^p. Turingův stroj T^p odsimuluje pro vstup i v polynomiálním čase prvních $p(|i|)$ kroků (kde $|i|$ značí délku vstupu i v binárním zápisu) Turingova stroje T nad i a následně zastaví. Takový algoritmus lze zkonstruovat podobně jako univerzální Turingův stroj, technickými detaily této konstrukce se nebudeme zabývat. *Turingovými stroji s polynomiálními hodinami* budeme rozumět Turingovy stroje tvaru T^p.

Definice 1 (L_{PV}, Krajíček, 2019)**.** *Symbolem L_{PV} rozumíme jazyk (predikátové logiky prvního řádu) sestávající z funkčních symbolů všech arit pro každý Turingův stroj s polynomiálními hodinami. To jest pro libovolnou aritu n a T^p Turingův stroj s polynomiálními hodinami L_{PV} obsahuje symbol příslušný T^p arity n.*

Všimněme si, že symboly jazyka L_{PV} odpovídají výhradně Turingovým strojům, které zastaví v polynomiálním čase, neboť jsou to symboly příslušné Turingovým strojům s polynomiálními hodinami. Naopak máme-li pevně zvolený způsob kódování k-tic přirozených čísel s kódováním i dekódováním v polynomiálním čase, pak každý polynomiální algoritmus $\mathbb{N}_0^k \to \mathbb{N}_0$ (kde $\mathbb{N}_0 = \{0, 1, 2, \dots\}$) je při tomto kódování vstupu počítán nějakým Turingovým strojem s polynomiálními hodinami, a tedy odpovídá k-árnímu symbolu jazyka L_{PV}. Na L_{PV} tedy můžeme nahlížet jako na konstruktivně definovaný jazyk všech polynomiálních algoritmů.

Ačkoliv L_{PV} neobsahuje relační symboly, můžeme pro relace rozhodnutelné v polynomiálním čase uvažovat jejich charakteristické funkce, tedy polynomiální algoritmus, který vrátí hodnotu 1, je-li zadaná k-tice přirozených čísel v relaci a hodnotu 0 v opačném případě. Relace definované charakteristickou funkcí budeme pro přehlednost zapisovat jako relační symboly. Například $R(x, y)$ je zkráceně $\neg(f_R(x, y) = 0_{L_{PV}})$, kde L_{PV}-symbol f_R odpovídá charakteristické funkci relace R a $0_{L_{PV}}$ je L_{PV}-symbol odpovídající polynomiálnímu algoritmu vracejícímu vždy 0. Všimněme si, že funkce f_R nemusí v konkrétním modelu nabývat jenom dvou hodnot, jedná se pouze o formální symbol označený nějakou charakteristickou funkcí na $\mathbb{N}_0$.

1.2 Teorie $\mathbf{T_{PV}}$

Uvažujme pevně zvolený způsob kódování k-tic (s kódováním i dekódováním v polynomiálním čase, pro všechna $k \in \mathbb{N}$), pak mají všechny L_{PV}-symboly přirozenou interpretaci na $\mathbb{N}_0$. To jest pro k-ární funkční symbol f jazyka L_{PV} definujeme hodnotu $f(n_1, \dots, n_k)$, kde $n_1, \dots, n_k \in \mathbb{N}_0$, jako výstup Turingova stroje (posloupnost bitů získanou přečtením pásky zleva doprava po prázdný symbol interpretujeme jako prvek $\mathbb{N}_0$) příslušnému f pro (na pásce) zakódovanou k-tici $n_1, \dots, n_k$. Touto interpretací symbolů jazyka L_{PV} na množině $\mathbb{N}_0$ získáme L_{PV}-strukturu, kterou budeme nazývat *standardní model*.

Definice 2 (T_{PV}, Krajíček, 2019)**.** *Symbolem T_{PV} budeme značit univerzální teorii standardního modelu, tedy L_{PV}-teorii axiomatizovanou všemi univerzálními sentencemi, které jsou pravdivé ve standardním modelu.*

1.3 Věty Herbrandova a KPT

Důležitými větami pro dosvědčování existenčních tvrzení v univerzálních teoriích jsou věty Herbrandova a KPT, jejichž jednodušší verze si nyní uvedeme. Tyto věty v jen minimálně odlišném znění lze najít v knize Krajíčka (Krajíček, 2019, podkap. 12.2) jako důsledky obecnější verze Herbrandovy věty.

Pro přehlednost budeme zapisovat bloky kvantifikátorů tvaru $\forall x_1 \forall x_2 \dots \forall x_n$ a $\exists x_1 \exists x_2 \dots \exists x_n$ jako $\forall \bar{x}$, respektive $\exists \bar{x}$. Například formuli

$$\forall x_1 \forall x_2 \dots \forall x_k \exists y_1 \exists y_2 \dots \exists y_l A(x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_l)$$

zapíšeme stručně jako $\forall \bar{x} \exists \bar{y} A(\bar{x}, \bar{y})$, kde $\bar{x}$ a $\bar{y}$ jsou bloky proměnných. Obdobně budeme zkracovat i bloky termů, například ve formuli $\forall \bar{x} A(\bar{x}, \bar{t}(\bar{x}))$ značí $\bar{t}(\bar{x})$ blok termů vhodné velikosti v proměnných bloku $\bar{x}$.

Věta 3 (Herbrand, 1930)**.** *Nechť T je univerzální teorie v jazyce L a nechť*

$$T \vdash \forall \bar{x} \exists \bar{y} A(\bar{x}, \bar{y}),$$

kde A je otevřená. Pak existuje $k \in \mathbb{N}$ a termy (bloky termů) $\bar{t}_1(\bar{x}), \dots, \bar{t}_k(\bar{x})$, splňující

$$T \vdash \forall \bar{x} \bigvee_{i=1}^{k} A(\bar{x}, \bar{t}_i(\bar{x})).$$

Důkaz. Uvažujme jazyk $L' := L + \{\bar{c}\}$, kde $\bar{c}$ jsou nové konstanty, respektive blok konstant svou velikostí odpovídající bloku $\forall \bar{x}$ a L'-teorii $T' \supseteq T$, která má oproti T navíc axiomy $\neg A(\bar{c}, \bar{t}(\bar{c}))$ pro všechny bloky L-termů $\bar{t}$ (vhodné velikosti a počtu proměnných).

Pro spor předpokládejme, že T' je bezesporná, a tudíž existuje model $\mathcal{A} \vDash T'$ (z věty o úplnosti). Definujme strukturu $\mathcal{B} \subseteq \mathcal{A}$ jako podstrukturu $\mathcal{A}$ s nosnou množinou $\{t(\bar{c}) \mid t \text{ je } L\text{-term}\}$. Jelikož T je univerzální a $\mathcal{A} \vDash T$, tak také $\mathcal{B} \vDash T$. Pro všechny bloky L'-termů $\bar{t}$ plyne z $\mathcal{B} \subseteq \mathcal{A}$ a $\mathcal{A} \vDash \neg A(\bar{c}, \bar{t}(\bar{c}))$, že $\mathcal{B} \vDash \neg A(\bar{c}, \bar{t}(\bar{c}))$ (neboť A je otevřená). Celkem tedy dostáváme $\mathcal{B} \vDash T'$. Dále platí $\mathcal{B} \vDash \neg \exists \bar{y} A(\bar{c}, \bar{y})$, jelikož každý blok $\bar{y}$ v $\mathcal{B}$ je tvaru $\bar{t}(\bar{c})$ pro nějaké $\bar{t}$ a $\mathcal{B} \vDash \neg A(\bar{c}, \bar{t}(\bar{c}))$. Ovšem $\mathcal{B} \vDash T$, a tedy dle předpokladu věty také $\mathcal{B} \vDash \forall \bar{x} \exists \bar{y} A(\bar{x}, \bar{y})$, volbou $\bar{x} := \bar{c}$ dostáváme spor s $\mathcal{B} \vDash \neg \exists \bar{y} A(\bar{c}, \bar{y})$.

T' je tedy sporná, to jest existuje důkaz sporu z axiomů T'. Jelikož důkazy používají pouze konečně mnoho axiomů teorie, tak existují termy $\bar{t}_1(\bar{x}), \dots, \bar{t}_k(\bar{x})$ takové, že L'-teorie T je ve sporu s axiomy $\neg A(\bar{c}, \bar{t}_i(\bar{c}))$, $i \in \{1, \dots, k\}$. Tedy v každém modelu L'-teorie T není alespoň jedna z formulí $\neg A(\bar{c}, \bar{t}_i(\bar{c}))$, $i \in \{1, \dots, k\}$ splněna, a platí tedy $\bigvee_{i=1}^{k} A(\bar{c}, \bar{t}_i(\bar{c}))$.

Nechť nyní $\mathcal{M}$ je modelem L-teorie T a $\bar{x}$ blok libovolných prvků modelu $\mathcal{M}$. Volbou $\bar{c} := \bar{x}$ získám model $\mathcal{M}'$ L'-teorie T, a tedy $\mathcal{M}' \vDash \bigvee_{i=1}^{k} A(\bar{c}, \bar{t}_i(\bar{c}))$, tudíž i $\mathcal{M} \vDash \bigvee_{i=1}^{k} A(\bar{x}, \bar{t}_i(\bar{x}))$. Jelikož model $\mathcal{M}$ L-teorie T stejně tak i blok prvků $\bar{x} \in \mathcal{M}$ byly zvoleny libovolně, je věta dokázána.

□

Důsledek 4. *Nechť*

$$T_{PV} \vdash \forall \bar{x} \exists \bar{y} A(\bar{x}, \bar{y}), \tag{1.1}$$

kde A je otevřená. Pak existuje blok termů $\bar{t}(\bar{x})$ takový, že

$$T_{PV} \vdash \forall \bar{x} A(\bar{x}, \bar{t}(\bar{x})),$$

speciálně blok polynomiálních algoritmů příslušný L_{PV}-symbolům $\bar{t}(\bar{x})$ splňuje

$$\mathbb{N}_0 \vDash \forall \bar{x} A(\bar{x}, \bar{t}(\bar{x}))$$

(kde $\mathbb{N}_0$ značí standardní model).

Důkaz. Volbou $L := L_{PV}$ a $T := T_{PV}$ Hebrandova věta implikuje existenci termů (polynomiálních algoritmů) $\bar{t}_1(\bar{x}), \ldots, \bar{t}_k(\bar{x})$ takových, že $\mathbb{N}_0 \vDash \forall \bar{x} \bigvee_{i=1}^{k} A(\bar{x}, \bar{t}_i(\bar{x}))$. Otevřená formule $A(\bar{x}, \bar{y})$ je rozhodnutelná v polynomiálním čase, tudíž formuli $A(\bar{x}, \bar{t}_i(\bar{x}))$ lze také rozhodnout v polynomiálním čase. Existuje tedy polynomiální algoritmus, který pro zadané $\bar{x}$ postupně testuje $A(\bar{x}, \bar{t}_1(\bar{x})), A(\bar{x}, \bar{t}_2(\bar{x})), \ldots$ až najde $\bar{t}_i(\bar{x})$ takové, že $A(\bar{x}, \bar{t}_i(\bar{x}))$. Označme $\bar{t}(\bar{x})$ blok algoritmů, který pro zadané $\bar{x}$ takto spočte svědka $\bar{y}$, tedy ve standardním modelu platí $\forall \bar{x} A(\bar{x}, \bar{t}(\bar{x}))$, což je univerzální sentence, tudíž axiom T_{PV}.

□

Důsledek 4 speciálně říká, že pro relaci $A(x, y)$ rozhodnutelnou v polynomiálním čase splňující (1.1) existuje polynomiální algoritmus, který pro zadané x spočte y takové, že platí $A(x, y)$.

Věta 5 (KPT, Krajíček, Pudlák a Takeuti, 1991)**.** *Nechť T je univerzální teorie v jazyce L a nechť*

$$T \vdash \forall \bar{x} \exists \bar{y} \forall \bar{z} B(\bar{x}, \bar{y}, \bar{z}),$$

kde B je existenční formule, tedy formule tvaru $\exists \bar{w} C(\bar{x}, \bar{y}, \bar{z}, \bar{w})$, pro nějakou otevřenou formuli C. Pak existuje $k \in \mathbb{N}$ a termy (bloky termů)

$$\bar{t}_1(\bar{x}), \bar{t}_2(\bar{x}, \bar{z}_1), \bar{t}_3(\bar{x}, \bar{z}_1, \bar{z}_2), \ldots, \bar{t}_k(\bar{x}, \bar{z}_1, \bar{z}_2, \ldots, \bar{z}_{k-1})$$

takové, že T dokazuje

$$\forall x, \bar{z}_1, \ldots, \bar{z}_k [B(\bar{x}, \bar{t}_1(\bar{x}), \bar{z}_1) \vee B(\bar{x}, \bar{t}_2(\bar{x}, \bar{z}_1), \bar{z}_2) \vee \cdots \vee B(\bar{x}, \bar{t}_k(\bar{x}, \bar{z}_1, \ldots, \bar{z}_{k-1}), \bar{z}_k)].$$

Důkaz. (Krajíček, 1995, podkap. 7.6) Uvažujme induktivně definované jazyky $L'_0 := L + \{\bar{c}\}$, $L'_i := L'_{i-1} + \{\bar{d}^i_j \mid j \in \mathbb{N}\}$, $i \in \mathbb{N}$, kde $\bar{c}$ je blok nových konstant velikostí odpovídající bloku $\forall \bar{x}$ ve znění věty a $\bar{d}^i_j$, $j \in \mathbb{N}$, jsou bloky nových konstant přidaných do jazyka L'_i navíc oproti jazyku L'_{i-1} velikostí odpovídající bloku $\forall \bar{z}$ ve znění věty. Označme $T'_0 := T$ a pro všechna $i \in \mathbb{N}$ induktivně definujme L'_i-teorii $T'_i \supseteq T'_{i-1}$, která má oproti T'_{i-1} navíc axiomy $\neg B(\bar{c}, \bar{s}^i_j(\bar{c}), \bar{d}^i_j)$, $j \in \mathbb{N}$, kde $\bar{s}^i_1(\bar{x})$,$\bar{s}^i_2(\bar{x}), \ldots$ jsou všechny bloky $(L'_{i-1} \setminus \{\bar{c}\})$-termů (očíslované) vhodné velikosti. Všimněme si, že tyto axiomy jsou přirozeně „číslované“ dvojicemi (i, j). Definujme jazyk $L^* := \bigcup_{i=1}^{\infty} L'_i$ a L^*-teorii $T^* := \bigcup_{i=1}^{\infty} T'_i$.

Pro spor předpokládejme, že T^* je bezesporná, a tudíž existuje model $\mathcal{A} \vDash T^*$. Definujme strukturu $\mathcal{B} \subseteq \mathcal{A}$ jako podstrukturu $\mathcal{A}$ s nosnou množinou $\{t(\bar{h}) \mid$

t je L-term, $\bar{h}$ konstanty L^*}. Jelikož T je univerzální a $\mathcal{A} \vDash T$, tak také $\mathcal{B} \vDash T$. Pro všechna $i, j \in \mathbb{N}$ plyne z $\mathcal{B} \subseteq \mathcal{A}$ a $\mathcal{A} \vDash \neg B(\bar{c}, \bar{s}^i_j(\bar{c}), \bar{d}^i_j)$, že $\mathcal{B} \vDash \neg B(\bar{c}, \bar{s}^i_j(\bar{c}), \bar{d}^i_j)$. Celkem tedy dostáváme $\mathcal{B} \vDash T^*$. Dále platí $\mathcal{B} \vDash \neg\exists\bar{y}\forall\bar{z}B(\bar{c}, \bar{y}, \bar{z})$, jelikož každý blok $\bar{y}$ v $\mathcal{B}$ je tvaru $\bar{t}(\bar{h})$ pro nějaké L-termy $\bar{t}$ a L^*-konstanty $\bar{h}$ a platí $\mathcal{B} \vDash \neg B(\bar{c}, \bar{s}^{i+1}_j(\bar{c}), \bar{d}^{i+1}_j)$, kde i je nejvyšší index $\bar{d}^i_j$ obsaženého v $\bar{h}$ a j je takové, že $\bar{s}^{i+1}_j(\bar{c}) = \bar{t}(\bar{h})$. Ovšem $\mathcal{B} \vDash T$, a tedy také $\mathcal{B} \vDash \forall\bar{x}\exists\bar{y}\forall\bar{z}B(\bar{x}, \bar{y}, \bar{z})$ dle předpokladu věty. Volbou $\bar{x} \coloneqq \bar{c}$ dostáváme spor s $\mathcal{B} \vDash \neg\exists\bar{y}\forall\bar{z}B(\bar{c}, \bar{y}, \bar{z})$.

T^* je tedy sporná, to jest existuje důkaz sporu z axiomů T^*. Jelikož důkazy používají pouze konečně mnoho axiomů teorie, existuje k axiomů tvaru $\neg B(\bar{c}, \bar{s}^i_j(\bar{c}), \bar{d}^i_j)$ (pro nějaké $k \in \mathbb{N}$), které jsou ve sporu s L^*-teorií T. Tedy v každém modelu L^*-teorie T není alespoň jedna z těchto k formulí splněna.

Nechť nyní $\mathcal{M}$ je modelem L-teorie T, $\bar{x}, \bar{z} \in \mathcal{M}$, bloky libovolných prvků $\mathcal{M}$, $\bar{x}$ velikosti bloku $\forall\bar{x}$ a $\bar{z} = z_1, \dots\ z_k$. Volbou $\bar{c} \coloneqq \bar{x}$, $\bar{d} \coloneqq \bar{z}$, kde $\bar{d}$ je blok lexikograficky seřazených $\bar{d}^i_j$, (i, j) odpovídajících nějakému z výše zmíněných k axiomů, zbylé $\bar{d}^i_j$ definujme jako c_1 (první z konstant $\bar{c}$), získáme model $\mathcal{M}^*$ L^*-teorie T. A tedy některý z k axiomů tvaru $\neg B(\bar{c}, \bar{s}^i_j(\bar{c}), \bar{d}^i_j)$ neplatí v $\mathcal{M}^*$, tudíž $\mathcal{M}^* \vDash B(\bar{c}, \bar{t}_l(\bar{g}), \bar{z}_l)$ (kde $l \in \{1, \dots, k\}$ je číslo axiomu při lexikografickém uspořádání dle (i, j)), $\bar{t}_l$ je blok L-termů společně s L'_{i-1}-konstantami $\bar{g}$ přirozeně interpretující výraz $\bar{s}^i_j(\bar{c})$, kde d^i_j pro (i, j) neodpovídající žádnému z k axiomů jsou nahrazena c_1, a tedy nejsou součástí $\bar{g}$. Jelikož model $\mathcal{M}$ L-teorie T stejně tak i bloky prvků $\bar{x}, \bar{z} \in \mathcal{M}$ byly zvoleny libovolně a termy t_l jsou na této volbě nezávislé, seřazením (dle l) členů $B(\bar{c}, \bar{t}_l(\bar{g}), \bar{z}_l)$ v disjunkci a rozepsáním $\bar{g}$ je věta dokázána.

□

KPT větu, respektive její závěr, lze chápat jako hru mezi studentem a učitelem (Krajíček, Pudlák a Sgall, 1990), kdy učitel zadá $\bar{x}$ a student se snaží najít $\bar{y}$ takové, že pro všechna $\bar{z}$ platí $B(\bar{x}, \bar{y}, \bar{z})$. Student postupuje tak, že pro zadané $\bar{x}$ spočte $\bar{t}_1(\bar{x})$ jakožto kandidáta na hledané $\bar{y}$. Platí-li pro všechna $\bar{z}$ $B(\bar{x}, \bar{t}_1(\bar{x}), \bar{z})$, hra končí, student uspěl. Existuje-li $\bar{z}_1$ takové, že $\neg B(\bar{x}, \bar{t}_1(\bar{x}), \bar{z}_1)$, učitel jej ukáže studentovi a vyzve ho, aby svou odpověď přehodnotil. Student vezme v úvahu učitelův protipříklad $\bar{z}_1$ a spočte $\bar{t}_2(\bar{x}, \bar{z}_1)$ jakožto kandidáta na hledané $\bar{y}$. Situace se opakuje, buď student uspěl (hra končí), nebo mu učitel ukáže protipříklad, a student dále počítá přičemž bere v úvahu všechny již získané učitelovy protipříklady. V i-té *interakci* (pokusu studenta) student počítá kandidáta na $\bar{y}$ jako $\bar{t}_i(\bar{x}, \bar{z}_1, \dots, \bar{z}_{i-1})$. Dle věty student uspěje nejpozději v k-tém pokusu.

Důsledek 6. *Nechť*

$$T_{PV} \vdash \forall\bar{x}\exists\bar{y}\forall\bar{z}B(\bar{x}, \bar{y}, \bar{z}),$$

kde B je existenční formule. Pak existuje $k \in \mathbb{N}$ a polynomiální interaktivní algoritmus („polynomiální student“), který pro zadané $\bar{x}$ nanejvýš v k interakcích („pokusech s učitelovými protipříklady“) najde $\bar{y}$ takové, že $\forall\bar{z}B(\bar{x}, \bar{y}, \bar{z})$.

Důkaz. Důsledek dostáváme přímou aplikací KPT věty na $L \coloneqq L_{PV}$ a $T \coloneqq T_{PV}$ interpretováním bloků polynomiálních algoritmů jako jeden polynomiální algoritmus počítající blok neznámých a následnou interpretací sady získaných k algoritmů jako jeden polynomiální interaktivní algoritmus.

□

Obecně je praktické využití takového „polynomiálního studenta“ omezeno neexistencí výpočetně dostupného „učitele“ schopného hledat protipříklady na „studentova“ nesprávná řešení. Naopak pokud by pro nějaký problém existoval polynomiální „student“, který nalezne řešení v k interakcích i polynomiální „učitel“, pak je tento problém zjevně řešitelný v polynomiálním čase, a to společnými silami „učitele“ a „studenta“.

2. NP vyhledávací problémy

Definice 7 (NP vyhledávací problém, Papadimitriou, 1994)**.** *Nechť $R(x, y)$ je relace rozhodnutelná v polynomiálním čase, splňující*

$$\forall x \exists y R(x, y) \wedge \forall x, y[R(x, y) \rightarrow |y| \leq |x|^{\mathcal{O}(1)}]$$

(kde $|\cdot|$ značí délku binárního zápisu), pak úloha nalezení y (ne nutně jednoznačného) pro zadané x je NP vyhledávácí problém.

Definice 8 (p-redukce, Papadimitriou, 1994)**.** *Nechť $R(x, y)$ a $S(x, y)$ jsou definující relace dvou NP vyhledávacích problémů a existují v polynomiálním čase spočítatelné funkce $f(x)$ a $g(x, v)$ takové, že*

$$S(f(x), v) \rightarrow R(x, g(x, v)),$$

pak řekneme, že dvojice f, g je p-redukcí *R na S.*

Definici p-redukce lze chápat následovně: chceme-li vyřešit pro zadané x NP vyhledávací problém definovaný relací R, můžeme vyřešit NP vyhledávací problém definovaný relací S pro zadání $f(x)$, a z tohoto řešení a zadaného x pomocí g spočteme řešení NP vyhledávacího problému definovaného relací R. Více o NP vyhledávacích problémech a jejich významu se lze dočíst v kapitole 19.3 v (Krajíček, 2019).

Definice 9 (PLS, Johnson, Papadimitriou a Yannakakis, 1988)**.** *Polynomiálním lokálním vyhledáváním, zkráceně* PLS*, rozumíme třídu NP vyhledávacích problémů definovaných následujícími daty: v polynomiálním čase rozhodnutelnou relací $S(x, y)$, v polynomiálním čase spočitatelnými funkcemi „ceny“ $c(x, y)$ (chápeme jako přirozené číslo) a „souseda“ $N(x, y)$, splňujícími pro všechna x, y: $S(x, 0)$, $S(x, y) \rightarrow |y| \leq |x|^{\mathcal{O}(1)}$ a*

$$S(x, y) \rightarrow \Big(S(x, N(x, y)) \wedge \Big(N(x, y) \neq y \rightarrow \big(c(x, N(x, y)) < c(x, y)\big)\Big)\Big).$$

Cílem PLS *úlohy je pro zadané x najít y takové, že*

$$S(x, y) \wedge N(x, y) = y.$$

PLS lze chápat jako hledání y pro zadané x takového, že funkce „souseda“ nenajde pro toto y prvek s nižší „cenou“.

Relací $R(x, y)$ z definice NP vyhledávacího problému (def. 7) je v případě PLS $S(x, y) \wedge N(x, y) = y$ vlastností popsaných v definici 9.

Pozorování 10. *Podmínky kladené na S, c, N v definici PLS jsou univerzální sentence, tedy axiomy T_{PV} pro příslušné L_{PV}-symboly. Například podmínka $S(x, 0)$ jako axiom $\forall x\, S(x, 0_{L_{PV}})$, kde $0_{L_{PV}}$ je L_{PV}-konstanta odpovídající algoritmu vracejícímu vždy 0. Obdobně $|y| \leq |x|^{\mathcal{O}(1)}$ lze přepsat jako $y \leq b(x)$ (kde omezující funkce $b(x)$ je spočítatelná v polynomiálním čase v závislosti na $|x|$).*

3. Teorie S_{PV}

3.1 Definice a základní vlastnosti S_{PV}

Pro zkrácení zápisu axiomů lineárních uspořádání definujme následující značení:

Definice 11 ($\mathcal{L}$). *Symbolem $\mathcal{L}_w^{u,v}(R(u,v,\bar{z}))$, kde R je relace a u,v,w jsou libovolné (jednosložkové) prvky, budeme rozumět formuli*

$$R(u,u,\bar{z}) \wedge \Big(\Big(R(u,v,\bar{z}) \wedge R(v,w,\bar{z})\Big) \to R(u,w,\bar{z})\Big) \\ \wedge \Big(\Big(R(u,v,\bar{z}) \wedge R(v,u,\bar{z})\Big) \to u = v\Big) \wedge \Big(R(u,v,\bar{z}) \vee R(v,u,\bar{z})\Big). \quad (3.1)$$

Pozorování 12. *L_{PV}-symbol $\leq$ je lineárním uspořádáním v teorii T_{PV}, neboť univerzální sentence $\forall u,v,w\, \mathcal{L}_w^{u,v}(u \leq v)$ platí ve standardním modelu, a je tudíž axiomem T_{PV}.*

Nyní rozšíříme T_{PV} o axiomy vyjadřující, že relace, která je lineárním uspořádáním na nějakém počátečním úseku, má na tomto počátečním úseku také minimum (počátečním úsekem myslíme množinu prvků menších než nějaké x při uspořádání L_{PV}-relací $\leq$). Výslednou teorii budeme nazývat S_{PV}.

Definice 13 (S_{PV}). *Symbolem S_{PV} budeme značit L_{PV}-teorii axiomatizovanou axiomy T_{PV} (viz def. 2) společně s* axiomy minima *tvaru*

$$\forall x\Big[\Big(\forall u,v,w \leq x\, \mathcal{L}_w^{u,v}(R(u,v,x))\Big) \to \exists m \leq x \forall m' \leq x\, R(m,m',x)\Big]$$

pro všechny L_{PV}-relace R.

Chápeme-li $R(u,v,x)$ v definici 13 jako binární relace v u,v, pak tyto jsou závislé na jednosložkovém parametru x. V lemmatu 17 dokážeme, že teorie S_{PV} dokazuje „axiomy minima“ i pro binární relace závislé na vícesložkovém parametru.

Problém najít minimum polynomiálně rozhodnutelného lineárního uspořádání na $[0,x]$ byl studován (Chiari a Krajíček, 1998) v souvislosti s charakterizací Σ_2^b-důsledků jisté teorie omezené aritmetiky.

Pozorování 14. *Teorie S_{PV} je bezesporná, neboť standardní model ($\mathbb{N}_0$) je modelem S_{PV}.*

Pozorování 15. *T_{PV} přirozeně reprezentuje prvky $\mathbb{N}_0$ jako L_{PV}-konstanty splňující T_{PV}-axiomy $n_{L_{PV}} \leq m_{L_{PV}}$ a $n_{L_{PV}} \neq m_{L_{PV}}$ (ekvivalentně $n_{L_{PV}} < m_{L_{PV}}$) pro všechna $n,m \in \mathbb{N}_0$ splňující $n < m$.*

Nechť $\langle x,y\rangle := \frac{(x+y)(x+y+1)}{2} + y$ (Cantorova párující funkce), pak teorie T_{PV} dokazuje, že $\langle x,y\rangle$ kóduje dvojice prvků, tedy že existují L_{PV}-symboly odpovídající dekódujícím funkcím p_1,p_2 takové, že $\forall x,y[p_1(\langle x,y\rangle) = x \wedge p_2(\langle x,y\rangle) = y]$ a $\forall x,y[x,y \leq \langle x,y\rangle]$ jsou jakožto univerzální sentence T_{PV}-axiomy.

Definice 16 (posloupnost)**.** *Symbolem* $Seq_n(x_1, \dots, x_n)$ *budeme rozumět*

$$\langle n_{L_{PV}}, \langle x_1, \langle x_2, \langle x_3, \langle x_4, \langle \dots, \langle x_{n-1}, \langle x_n, 0_{L_{PV}} \underbrace{\rangle\rangle \dots \rangle\rangle}_{(n+1)krát}.$$

Dále definujeme binární funkční symbol $(s)_i$ *jako ten algoritmus, který ve standardním modelu iterováním projekce spočte* i*-tý člen posloupnosti* s*, tedy*

$$\underbrace{p_2(p_2(p_2(\dots p_2(}_{i\text{-krát}} p_1(s)) \dots))). \tag{3.2}$$

Pro $i \in \mathbb{N}_0$ *(nikoliv prvek modelu či* L_{PV}*-konstantu) budeme unárním symbolem* $(s)_i$ *rozumět přímo term (3.2). Dále definujme délku posloupnosti jako* $len(s) \coloneqq (s)_0 = p_1(s)$*.*

Lemma 17. *Teorie* S_{PV} *dokazuje*

$$\forall x \forall \bar{z} \Big[\Big(\forall u, v, w \leq x \, \mathcal{L}_w^{u,v}(B(u, v, x, \bar{z})) \Big) \to \exists m \leq x \forall m' \leq x \, B(m, m', x, \bar{z}) \Big]$$

pro všechny otevřené (bez kvantifikátorů) L_{PV}*-formule* $B(u, v, x, \bar{z})$*.*

Důkaz. Označme k velikost bloku $\forall \bar{z}$, nechť $\overline{(s)_*}$ značí následující blok prvků posloupnosti s: $(s)_2, \dots, (s)_{(k+1)}$. Nyní označme R L_{PV}-symbol splňující

$$\begin{aligned} T_{PV} \vdash \forall u, v, s \Big[R(u, v, s) = \Big(u \leq (s)_1 \wedge v > (s)_1 \Big) \vee \\ \vee \Big(u, v \leq (s)_1 \wedge B(u, v, (s)_1, \overline{(s)_*}) \Big) \vee \Big(u, v > (s)_1 \wedge u \leq v \Big) \Big], \end{aligned} \tag{3.3}$$

který existuje, neboť existuje algoritmus počítající tuto relaci ve standardním modelu a ve (3.3) je univerzální sentence, tedy axiom T_{PV} ($\subseteq S_{PV}$). Dále v T_{PV} platí:

$$\forall s \forall u, v, w \Big[\Big(u, v, w > (s)_1 \Big) \to \mathcal{L}_w^{u,v}(R(u, v, s)) \Big], \tag{3.4}$$

$$\forall s \forall u, v \Big[\Big(u \leq (s)_1 \wedge v > (s)_1 \Big) \to (R(u, v, s)) \Big], \tag{3.5}$$

$$\forall x \forall \bar{z} \forall u, v \Big[\Big(u, v \leq x \Big) \to \Big(B(u, v, x, \bar{z}) \leftrightarrow R(u, v, Seq_{(k+1)}(x, \bar{z})) \Big) \Big], \tag{3.6}$$

neboť se jedná o univerzální sentence platné ve standardním modelu.

Zvolme nyní libovolný model S_{PV} a v něm libovolné prvky $x, \bar{z}$. Platí-li

$$\forall u, v, w \leq x \, \mathcal{L}_w^{u,v}(B(u, v, x, \bar{z})), \tag{3.7}$$

pak dle (3.6) platí také

$$\forall u, v, w \leq x \, \mathcal{L}_w^{u,v}(R(u, v, Seq_{(k+1)}(x, \bar{z}))),$$

což v kombinaci s (3.4) a (3.5) implikuje

$$\forall u, v, w \, \mathcal{L}_w^{u,v}(R(u, v, Seq_{(k+1)}(x, \bar{z}))),$$

tedy linearitu $R(u, v, Seq_{(k+1)}(x, \bar{z}))$ v proměnných u, v na všech prvcích. Speciálně

$$\forall u, v, w \leq Seq_{(k+1)}(x, \bar{z}) \, \mathcal{L}_w^{u,v}(R(u, v, Seq_{(k+1)}(x, \bar{z}))).$$

Tudíž aplikací S_{PV}-axiomu minima na R a prvek $Seq_{(k+1)}(x, \bar{z})$ (jakožto x z definice S_{PV} (def. 13)) dostaneme existenci prvku minima m splňujícího

$$\forall m' \leq Seq_{(k+1)}(x, \bar{z})\, R(m, m', Seq_{(k+1)}(x, \bar{z})). \tag{3.8}$$

V kombinaci s podmínkou (3.5) víme, že $m \leq x$ (jinak spor s volbou $m' \coloneqq x$).

Pro spor předpokládejme existenci $m' \leq x$ takového, že $\neg B(m, m', x, \bar{z})$. Z podmínky (3.6) plyne, že také $\neg R(m, m', Seq_{(k+1)}(x, \bar{z}))$, což je spor s (3.8).

V libovolném modelu S_{PV} a pro libovolné $x, \bar{z}$ jsme ukázali, že z podmínky (3.7) plyne existence minima relace $B(u, v, x, \bar{z})$ (v proměnných u, v) na prvcích menších než x.

□

3.2 $\mathbf{T_{PV}}$ versus $\mathbf{S_{PV}}$

Přirozenou otázkou je, zda je teorie S_{PV} silnější než T_{PV}, nebo zda lze axiomy S_{PV} dokázat z T_{PV}, tedy $T_{PV} = S_{PV}$. Tato otázka zůstává nadále otevřeným problémem, my si však ukážeme důvody domnívat se, že S_{PV} je silnější než T_{PV}.

Tvrzení 18. *S_{PV} dokazuje, že každý PLS problém má řešení, to jest, pokud $S(x, y)$, $c(x, y)$ a $N(x, y)$ určují PLS problém (viz definici 9), pak*

$$S_{PV} \vdash \forall x \exists y [S(x, y) \wedge N(x, y) = y],$$

kde S, c, N, jsou L_{PV}-symboly příslušné algoritmům počítajícím funkce určujících daný PLS.

Důkaz. Abychom se vyhnuli ještě komplikovanějšímu rozboru případů než ve formuli (3.3) důkazu lemmatu 17, definujeme tentokrát relaci R slovy. Uvažujme relaci $R(u_1, u_2, x)$, reprezentující algoritmus, který pro zadané x, u_1, u_2 spočte a porovná (neostře lexikograficky) následující dvě trojice $(\neg S(x, u_i), c(x, u_i), u_i)$, $i = 1, 2$, kde $\neg S(x, u_i)$ interpretujeme jako 0, pokud platí $S(x, u_i)$ a jako 1 v opačném případě. Tyto vlastnosti relace R lze podobně jako v (3.3) důkazu lemmatu 17 vyjádřit univerzální sentencí a jsou tedy axiomem T_{PV}. Platí

$$\forall x \forall u, v, w\, \mathcal{L}_w^{u,v}(R(u, v, x)), \tag{3.9}$$

tedy R definuje lineární uspořádání pro všechna x, a tato vlastnost popsaná univerzální sentencí je také axiomem $T_{PV} \subseteq S_{PV}$.

Jelikož pro $S(x, y)$ je $|y|$ odhadnuto polynomem v $|x|$ (viz def. 9), tak existuje polynomiální algoritmus $b(x)$, který počítá horní odhad na hledaná y, a formule

$$\forall x \forall y [S(x, y) \rightarrow y \leq b(x)] \tag{3.10}$$

je tedy, jakožto univerzální sentence, axiomem $T_{PV} \subseteq S_{PV}$.

Nyní pro zadané x v libovolném modelu T_{PV} dle (3.9) máme $\forall u, v, w \leq b(x)\, \mathcal{L}_w^{u,v}(R(u, v, x))$, a tudíž dle lemmatu 17 (volbou $x \coloneqq b(x), \bar{z} \coloneqq x$) existuje minimum m takové, že $\forall m' \leq b(x)\, R(m, m', x)$. Z pozorování 10 dostáváme (viz definici PLS, def. 9), že $S(x, m)$, jinak by $R(0_{L_{PV}}, m, x)$ a $b(x) \geq 0_{L_{PV}} \neq m$,

pak m není minimum, spor. Nechť nyní pro spor $N(x,m) \neq m$, pak $S(x,N(x,m))$, $c(x,N(x,m)) < c(x,m)$, tedy $R(N(x,m),m,x)$, a jelikož $N(x,m) \leq b(x)$ (dle (3.10)), m není minimum, spor.

Celkem tedy platí $S(x,m) \wedge N(x,m) = m$.

□

Důsledek 19. *Pokud platí $T_{PV} = S_{PV}$, pak každý PLS problém je řešitelný nějakým polynomiálním algoritmem.*

Důkaz. Pokud $T_{PV} = S_{PV}$, pak dle tvrzení 18 T_{PV} dokazuje, že každý PLS problém má řešení. Aplikací Herbrandovy věty (v. 3), respektive jejího důsledku (důsl. 4) na

$$T_{PV} \vdash \forall x \exists y [S(x,y) \wedge N(x,y) = y],$$

kde S, c, N definují PLS problém (viz definici 9), dostáváme existenci polynomiálního algoritmu, který pro zadané x najde y takové, že $S(x,y) \wedge N(x,y) = y$.

□

Možnost (implikovaná $T_{PV} = S_{PV}$), že by PLS problémy byly řešitelné v polynomiálním čase, by byla významným, avšak nečekaným zjištěním. Třída PLS by pak byla totožná s třídou polynomiálních problémů.

Podobně jako v kapitole 9.1 (Krajíček, 2019) definujeme:

Definice 20 (posloupnost libovolné konečné délky)**.** *Zvolme pevně čtveřici: konstanta λ, unární funkce $len(w)$, binární funkce $(w)_i$ a binární funkce $ext(w,a)$ které splňují:*

1. $len(\lambda) = 0_{L_{PV}}$,
2. $\forall w [len(w) \leq |w| \wedge (w)_i \leq w]$,
3. $\forall w,a,i \Big[ext(w,a) \leq (w \cdot a)^{10} \wedge len(ext(w,a)) = len(w)+1 \wedge \Big((i < len(w)) \rightarrow (ext(w,a))_i = (w)_i\Big) \wedge (ext(w,a))_{len(ext(w,a))} = a\Big]$,

kde $|\cdot|$ rozumíme délku binárního zápisu.

Funkce $len(w)$ představuje délku posloupnosti w, funkce $ext(w,a)$ rozšíření posloupnosti w o prvek a a funkce $(w)_i$ představuje i-tý člen posloupnosti w.

Existenci čtveřice funkcí splňujících 1.-3. můžeme uvažovat, neboť existují ve standardním modelu jako polynomiální algoritmy a podmínky 1.-3. jsou univerzální sentence.

Kódování posloupností, které umožňují funkce z def. 20 budeme uvažovat v následujícím tvrzení.

Tvrzení 21. *S_{PV} dokazuje, že každý prvek má rozklad na prvočinitele. To jest pro symbol $\tilde{\Pi}(s)$, odpovídající algoritmu roznásobujícímu posloupnosti rozkladu čísla na činitele (tedy validní posloupnosti, bez 1 v případě vícečlenné posloupnosti, jinak vracejícímu 0) a binární symbol dělitelnosti $|$, platí*

$$\forall x > 0_{L_{PV}} \exists s \Big[\tilde{\Pi}(s) = x \wedge \forall i \in [1_{L_{PV}}, len(s)] \forall d \Big(d|(s)_i \rightarrow (d = 1_{L_{PV}} \vee d = (s)_i)\Big)\Big],$$

kde $(i \in [1_{L_{PV}}, len(s)]) \equiv (i \geq 1_{L_{PV}} \wedge i \leq len(s))$.

Důkaz. Uvažujme funkci $b(x)$ horního odhadu velikosti zakódované posloupnosti rozkladu x, to jest

$$\forall x \forall s \Big[\Big(x > 0_{L_{PV}} \wedge \tilde{\Pi}(s) = x \Big) \rightarrow s \leq b(x) \Big]. \tag{3.11}$$

Taková funkce ve standardním modelu existuje, neboť zvolené kódování je spočítatelné v polynomiálním čase, pro zadané x je počet prvků rozkladu menší nebo roven $\log_2(x)$ a členy posloupnosti jsou menší než x. Dále existuje ve standardním modelu funkce $q(s, i, d)$, která pro posloupnost rozkladu s prvku x a dělitele d i-tého členu rozkladu spočte delší rozklad, tedy

$$\begin{aligned} &\forall x \forall s \forall i, d \\ &\quad \Big[\Big(x > 0_{L_{PV}} \wedge \tilde{\Pi}(s) = x \wedge i \in [1_{L_{PV}}, len(s)] \wedge d | (s)_i \wedge d \neq 1_{L_{PV}} \wedge d \neq (s)_i \Big) \\ &\qquad \rightarrow \Big(\tilde{\Pi}(q(s,i,d)) = x \wedge len(q(s,i,d)) > len(s) \Big) \Big]. \end{aligned} \tag{3.12}$$

Podmínky (3.11) a (3.12) jsou, jakožto univerzální sentence, axiomy T_{PV} ($\subseteq S_{PV}$). Nyní uvažujme relaci $R(s_1, s_2, x)$, která lexikograficky řadí podle uspořádané trojice $(\neg\tilde{\Pi}(s_i) = x, -len(s_i), s_i)$ (pravdu chápeme jako 1, nepravdu jako 0). Tuto relaci lze popsat univerzální sentencí (s využitím symbolu $\leq$) obdobně jako ve formuli (3.3) důkazu lemmatu 17, tedy axiomem T_{PV}.

Relace $R(s_1, s_2, x)$ je pro zadané x lineární, což je popsáno univerzální sentencí $\forall x \forall u, v, w \, \mathcal{L}^{u,v}_w(R(u, v, x))$, tedy axiomem T_{PV}. Dle lemmatu 17 ($x \coloneqq b(x)$, $\bar{z} \coloneqq x$) S_{PV} dokazuje, že pro zadané $x \neq 0_{L_{PV}}$ má relace $R(s_1, s_2, x)$ minimum na prvcích menších než $b(x)$. Označme toto minimum m. Platí $\tilde{\Pi}(m) = x$, jinak by $Seq_1(x)$ byl menší (při $R(s_1, s_2, x)$), neboť $\forall x [x \neq 0_{L_{PV}} \rightarrow \tilde{\Pi}(Seq_1(x)) = x]$ je axiom T_{PV}.

Nechť nyní pro spor existují i, d takové, že $i \in [1_{L_{PV}}, len(s)]$, $d|(m)_i$ a $1_{L_{PV}} \neq d \neq (m)_i$, pak $q(s, i, d)$ je dle (3.12) a (3.11) menší než $b(x)$ (při $\leq$) a (ostře) menší než minimum m při $R(s_1, s_2, x)$, spor. Taková i, d tedy pro m neexistují, a m je hledaný rozklad na prvočinitele.

□

Důsledek 22. *Pokud platí $T_{PV} = S_{PV}$, existuje $k \in \mathbb{N}$ pevné a polynomiální interaktivní algoritmus („polynomiální student“ viz podkapitolu 1.3 za KPT větou, v. 5), který pro libovolné zadané $x \in \mathbb{N}$ v k interakcích, kde jako protipříklad v každé interakci dostane nevlastního dělitele nějakého členu rozkladu naposledy spočítaného kandidáta na rozklad, nalezne rozklad x na prvočísla.*

Důkaz. $T_{PV} = S_{PV}$ dle tvrzení 21 implikuje, že T_{PV} dokazuje

$$\forall x > 0_{L_{PV}} \exists s \Big[\tilde{\Pi}(s) = x \wedge \forall i \in [1_{L_{PV}}, len(s)] \forall d \Big(d | (s)_i \rightarrow (d = 1 \vee d = (s)_i) \Big) \Big],$$

což lze přepsat jako

$$\begin{aligned} &\forall x \exists s \forall i, d \Big[x \neq 0_{L_{PV}} \\ &\quad \rightarrow \Big[\tilde{\Pi}(s) = x \wedge i \in [1_{L_{PV}}, len(s)] \rightarrow \Big(d | (s)_i \rightarrow (d = 1 \vee d = (s)_i) \Big) \Big] \Big]. \end{aligned} \tag{3.13}$$

Aplikací KPT věty (v. 5), respektive důsledku 6 na formuli (3.13), dostáváme existenci hledaného algoritmu.

□

Pokud by tedy platilo $T_{PV} = S_{PV}$, pak existuje polynomiální interaktivní algoritmus, který v k interakcích najde prvočíselný rozklad. To by bylo velice překvapivé, neboť pro $k+1$ či více roznásobených „kryptograficky silných“ prvočísel by takový algoritmus ve snaze najít prvočíselný rozklad částečně uspěl. Když by nenašel napoprvé rozklad, tak mu napovíme jedno prvočíslo, když opět neuspěje, tak napovíme další prvočíslo, atd. Ovšem nejpozději v k-krocích takový algoritmus najde celý rozklad, tedy někdy musel samostatně najít dělitele v polynomiálním čase. To odporuje kryptografické intuici.

Příklad. Nechť $s = p_1 \cdot p_2$, kde p_1, p_2 jsou kryptograficky silná, nám neznámá prvočísla. Předpokládejme, že máme „polynomiálního studenta“, který uspěje v $k = 30$ krocích. Pak zadáme „studentovi“ rozložit $n \coloneqq s \cdot p'_3 \cdot p'_4 \cdot \ldots \cdot p'_{100}$, kde $p'_3, \ldots, p'_{100}$ jsou námi zvolená kryptograficky silná prvočísla. Budeme-li mu napovídat námi zvolená p'_i, tak pravděpodobně nejpozději ve 30 krocích a polynomiálním čase rozloží n, tedy i s. Problém nastane, pokud by v některém z prvních 29 kroků rozložil vše vyjma s, to je ovšem nepravděpodobné, protože mezi prvočísly p_1, p_2 a ostatními nevidí rozdíl.

3.3 $\mathbf{T_{PV(\alpha)}}$ versus $\mathbf{S_{PV(\alpha)}}$

Podobně, jako jsme v kapitole 1 formálně definovali jazyk polynomiálních algoritmů, definujeme nyní jazyk $L_{PV(\alpha)}$ jako jazyk polynomiálních algoritmů s orákulem pro binární relaci $\alpha(u, v)$ a $T_{PV(\alpha)}$ jako analogii T_{PV}.

Definice 23 ($L_{PV(\alpha)}$)**.** *Symbolem $L_{PV(\alpha)}$ rozumíme jazyk sestávající z funkčních symbolů všech arit pro každý Turingův stroj s orákulem pro relaci $\alpha(u, v)$ a s polynomiálními hodinami (obdobně jako v definici 1).*

Definice 24. Expanzí $(\mathbb{N}_0, R)$*, kde $R(x, y)$ je konkrétní relace na $\mathbb{N}_0$, budeme rozumět $T_{PV(\alpha)}$-model vzniklý přirozenou interpretací $L_{PV(\alpha)}$ na $\mathbb{N}_0$, interpretujeme-li symbol α jako R.*

Definice 25 ($T_{PV(\alpha)}$)**.** *Symbolem $T_{PV(\alpha)}$ budeme značit $L_{PV(\alpha)}$-teorii axiomatizovanou všemi univerzálními sentencemi, které jsou pravdivé v každé expanzi tvaru $(\mathbb{N}_0, R)$, kde R je binární relace na $\mathbb{N}_0$.*

Definice 26 ($S_{PV(\alpha)}$)**.** *Symbolem $S_{PV(\alpha)}$ budeme značit teorii $T_{PV(\alpha)}$ rozšířenou o axiomy minima analogicky k definici 13.*

Tvrzení 27. $T_{PV(\alpha)} \neq S_{PV(\alpha)}$.

Důkaz. Dokážeme, že $T_{PV(\alpha)}$ nedokazuje konkrétní $S_{PV(\alpha)}$-axiom, tedy

$$T_{PV(\alpha)} \nvdash \forall x \Big[\Big(\forall u, v, w \leq x \, \mathcal{L}_w^{u,v}(\alpha(u, v)) \Big) \to \exists m \leq x \forall m' \leq x \, \alpha(m, m') \Big].$$

Pro spor předpokládejme opak, tedy že $T_{PV(\alpha)}$ dokazuje axiom minima pro relační symbol α. To lze přepsat jako

$$T_{PV(\alpha)} \vdash$$
$$\forall x \exists m, u, v, w \forall m' \Big[m, u, v, w \leq x \wedge \Big(m' \leq x \to \Big(\neg \mathcal{L}_w^{u,v}(\alpha(u, v)) \vee \alpha(m, m') \Big) \Big) \Big].$$

Použitím KPT věty (v. 5) získáme analogicky k důsledku 6 bloky (čtveřice) $L_{PV(\alpha)}$-termů

$$\bar{t}_1(x), \bar{t}_2(x, z_1), \bar{t}_3(x, z_1, z_2), \ldots, \bar{t}_k(x, z_1, z_2, \ldots, z_{k-1})$$

reprezentující interaktivní algoritmus, o kterém $T_{PV(\alpha)}$ dokazuje, že pro zadané $x \in \mathbb{N}_0$ najde v k interakcích buď protipříklad na linearitu α, nebo číslo $m \leq x$ takové, že $\alpha(m, m')$ pro všechna $m' \leq x$.

Označme symbolem t_i^m první term bloku $\bar{t}_i$, tedy term počítající kandidáta na minimum a předpokládejme $x \in \mathbb{N}_0$ dostatečně velké, pak můžeme provést následující konstrukci.

Nechme počítat výše získaný interaktivní algoritmus hodnotu $\bar{t}_1(x)$ až do momentu, než se poprvé zeptá orákula α na pravdivost $\alpha(u, v)$ pro nějaká u, v. Definujme částečné uspořádání $R_1 \coloneqq \{(u, v)\} \cup \{(u, u)\} \cup \{(v, v)\}$ a nechme algoritmus počítat dále za předpokladu $\alpha = R_1$. Postupně zkonstruujme $R_1 \subsetneq R_2 \subsetneq R_3 \subsetneq \ldots$, tak, že kdykoliv se algoritmus bude chtít zeptat na hodnotu $\alpha(u, v)$, kde jedno z čísel u, v ještě nikdy α-neporovnával, definujeme částečné uspořádání $R_{j+1} \supsetneq R_j$ jako (nejmenší) rozšíření naposledy zkonstruovaného R_j tak, že toto číslo je R_{j+1}-menší než všechna čísla, na která jsme se již α dotazovali, a také je R_{j+1}-menší samo sobě. Je-li α prvně dotazováno na obě čísla u, v, pak částečné uspořádání R_{j+1} definujeme jako (nejmenší) rozšíření R_j tak, že u je R_{j+1}-menší než v a obě tato čísla jsou menší než všechna čísla, na která jsme se α dotazovali při konstrukci R_j, a také jsou R_{j+1}-menší samy sobě. Dále pokračujme ve výpočtu za předpokladu $\alpha = R_{j+1}$. Takto postupujeme, dokud algoritmus nevrátí $\bar{t}_1(x)$.

Termy (čtveřice termů) $\bar{t}_1$ reprezentují polynomiální algoritmy s orákulem pro α, a ty používají pouze polynomiální počet dotazů na hodnoty relace α. Jelikož jsme zvolili dostatečně velké x, existují čísla menší než x a zároveň různá od $t_1^m(x)$, na jejichž hodnoty α (společně s jiným číslem) se $\bar{t}_1$ orákula nedotazoval. Označme n_1 libovolné takové číslo a definujme částečné uspořádání $R_{j'+1} \supsetneq R_{j'}$, kde $R_{j'}$ je poslední získané částečné uspořádání po spočtení $\bar{t}_1(x)$, tak, že n_1 je $R_{j'+1}$-menší než všechna čísla, která se objevují v uspořádaných dvojicích relace $R_{j'}$ (tedy na která jsme se již α dotazovali) a než $t_1^m(x)$ a n_1 samotné.

Předpokládejme opět $\alpha = R_{j'}$ a pokračujme obdobným způsobem s výpočtem $\bar{t}_2(x, n_1), \bar{t}_3(x, n_1, n_2), \ldots$. Tedy konstruujeme další částečná uspořádání $R_{j'} \subseteq R_{j'+1} \subseteq \ldots$ tak, že nově α-porovnávaná čísla, která nejsou jedním z již zvolených $n_1, n_2, \ldots$, jsou menší než všechny dříve α-porovnávaná a než předchozí spočtení kandidáti na minimum (čísla tvaru $t_l^m(x, n_1, \ldots, n_{l-1})$, $l < i$, $\bar{t}_i$ naposledy počítající algoritmus) a také než již zvolená čísla $n_1, n_2, \ldots, n_{i-1}$. Dále při výpočtu uvažujeme $\alpha = R_{j''+1}$, j'' takové, že $R_{j''}$ je naposledy rozšiřovaná relace. Vždy po doběhnutí algoritmu $\bar{t}_i$ nalezneme v minulosti α-neporovnávaná $n_i \leq x$ různá od spočtených hodnot t_l^m, $l \leq i$ a již zvolených n_l, $l < i$. To lze, neboť jsme volili x dostatečně velké a máme $4k$ polynomiálních algoritmů s orákulem a maximálně k vstupy $\leq$-menšími x. Zkonstruujeme další rozšiřující částečné uspořádání $R_{j'''}$ tak, že n_i je nejmenší a pokračujeme s $\bar{t}_{i+1}(x, n_1, \ldots, n_i)$ za předpokladu $\alpha = R_{j'''}$.

Po doběhnutí celého interaktivního algoritmu rozšíříme uspořádání o informaci, že $n_k \leq x$ dosud nezmíněné (dotaz na α nebo výstup algoritmu nebo n_i, $i < k$) číslo je menší než všechna dříve zmíněná čísla. Nakonec získáme lineární uspořádání R rozšířením získaného částečného uspořádání $R_{j''''}$ tak, aby dosud nezmíněná čísla (při konstrukci $R_{j''''}$) byla navzájem srovnána pomocí $\leq$ a zároveň

byla R-větší všem číslům zmíněným při konstrukci $R_{j''''}$ (tedy číslům obsaženým v nějaké uspořádané dvojici v $R_{j''''}$).

Výše získaný interaktivní algoritmus selže v expanzi $(\mathbb{N}_0, R)$ pro vstup x, neboť jeho průběh bude totožný s průběhem při výše popsané konstrukci, tudíž nenalezne číslo R-menší $n_k \leq x$, i když mu poskytneme validní protipříklady $n_1, n_2, \ldots, n_{k-1}$.

□

4. Dosvědčování v S_{PV}

Cílem této kapitoly je odvodit dosvědčovací větu pro teorii S_{PV} a zformulovat souvislost mezi S_{PV}-dokazatelnými existenčními tvrzeními ve vhodném tvaru s nějakým NP vyhledávacím problémem (def. 7), tedy podobnou souvislost jako byla odvozena mezi dokazatelnými existenčními formulemi tvaru $\forall x \exists y A(x,y)$ (A otevřená) v teorii $NP - IND$ ($\supseteq T_{PV}$, navíc axiomy omezené indukce pro E_1-formule) a třídou PLS (def. 9), viz články (Krajíček, 2010), (Buss a Krajíček, 1994).

Lemma 28. *Nechť $S_{PV} \vdash \phi$, kde ϕ je L_{PV}-formule, pak existuje důkaz ϕ z teorie S_{PV} používající pouze jediný S_{PV}-axiom, který není T_{PV}-axiomem (tedy axiom minima). To jest existuje L_{PV}-relace $R(u,v,x)$ taková, že*

$$T_{PV} + \forall x \Big[\Big(\forall u,v,w \leq x \, \mathcal{L}_w^{u,v}(R(u,v,x)) \Big) \rightarrow \exists m \leq x \forall m' \leq x \, R(m,m',x) \Big] \vdash \phi. \tag{4.1}$$

Důkaz. Uvažujme jeden konkrétní S_{PV}-důkaz formule ϕ. Jelikož důkaz používá jen konečně mnoho axiomů, můžeme označit $R_i(u,v,x)$ $i \in \{1,\ldots,k\}$ všechny relace takové, že v S_{PV}-důkazu ϕ je použit S_{PV}-axiom minima pro relaci R_i. Dále označme $B(u,v,x,z)$ relaci splňující formule

$$\forall x \forall u,v [B(u,v,x,i_{L_{PV}}) \leftrightarrow R_i(u,v,x)], i \in \{1,\ldots,k\}. \tag{4.2}$$

Taková relace existuje ve standardním modelu jako kombinace polynomiálních algoritmů příslušných jednotlivým R_i. Jelikož (4.2) jsou univerzální sentence, jsou i axiomy T_{PV}.

Nyní uvažujme formuli

$$\forall x \forall z \Big[\Big(\forall u,v,w \leq x \, \mathcal{L}_w^{u,v}(B(u,v,x,z)) \Big) \rightarrow \exists m \leq x \forall m' \leq x \, B(m,m',x,z) \Big]. \tag{4.3}$$

Tedy speciálně

$$\forall x \Big[\Big(\forall u,v,w \leq x \, \mathcal{L}_w^{u,v}(B(u,v,x,i_{L_{PV}})) \Big) \rightarrow \exists m \leq x \forall m' \leq x \, B(m,m',x,i_{L_{PV}}) \Big],$$

pro všechna $i \in \{1,\ldots,k\}$, což společně s (4.2) implikuje

$$\forall x \Big[\Big(\forall u,v,w \leq x \, \mathcal{L}_w^{u,v}(R_i(u,v,x)) \Big) \rightarrow \exists m \leq x \forall m' \leq x \, R_i(m,m',x) \Big]$$

pro všechna $i \in \{1,\ldots,k\}$, a to jsou právě ty S_{PV}-axiomy použité v důkazu ϕ, které nejsou T_{PV}-axiomy.

Celkem tedy máme, že $T_{PV} + (4.3) \vdash \phi$. Dle lemmatu 17 platí $S_{PV} \vdash (4.3)$, navíc v důkazu lemmatu 17 jsme dokázali (4.3) z S_{PV} pouze za použití jediného S_{PV}-axiomu minima. To jest axiomu tvaru jako ve (4.1) pro relaci R definovanou ve (3.3) důkazu lemmatu 17. Pro tuto volbu R pak platí (4.1).

□

Lemma 29. *Nechť*

$$S_{PV} \vdash \forall x \exists y A(x,y), \tag{4.4}$$

kde $A(x,y)$ je otevřená formule. Pak existuje term $b(x)$ a relace $R(u,v,x)$ taková, že teorie T_{PV} dokazuje, že pro všechna x formule

$$\forall a \leq b(x)\Big[\Big(\forall u,v,w \leq a\, \mathcal{L}_w^{u,v}(R(u,v,a))\Big) \to \exists m \leq a \forall m' \leq a\, R(m,m',a)\Big]$$

implikuje

$$\exists y \leq b(x) A(x,y).$$

Důkaz. Z (4.4) a lemmatu 28 plyne (s použitím lemmatu o dedukci) existence L_{PV}-relace $R(u,v,x)$ takové, že T_{PV} dokazuje, že

$$\forall a\Big[\Big(\forall u,v,w \leq a\, \mathcal{L}_w^{u,v}(R(u,v,a))\Big) \to \exists m \leq a \forall m' \leq a\, R(m,m',a)\Big] \tag{4.5}$$

implikuje

$$\forall x \exists y A(x,y). \tag{4.6}$$

Přepsáním implikace v (4.5) $\to$ (4.6) na tvar $\neg(4.5) \vee (4.6)$ a přesunutím kvantifikátoru $\forall x$ na začátek formule $\neg(4.5) \vee (4.6)$ dostáváme ekvivalentní formu

$$\forall x\Big[\exists a\Big[\Big(\forall u,v,w \leq a\, \mathcal{L}_w^{u,v}(R(u,v,a))\Big) \wedge \forall m \leq a \exists m' \leq a\, \neg R(m,m',a)\Big] \vee \exists y A(x,y)\Big], \tag{4.7}$$

což lze celé přepsat jako

$$\forall x \exists a,y \forall m,u,v,w \leq a \exists m' \leq a\Big[\Big(\mathcal{L}_w^{u,v}(R(u,v,a)) \wedge \neg R(m,m',a)\Big) \vee A(x,y)\Big]. \tag{4.8}$$

Označme $L'_{PV} \coloneqq L_{PV} + \{c\}$, kde c je nová konstanta. Označme T'_{PV} L'_{PV}-teorii axiomatizovanou axiomy T_{PV} společně s axiomy tvaru

$$\forall a,y \leq t(c) \neg \forall m,u,v,w \leq a \exists m' \leq a\Big[\Big(\mathcal{L}_w^{u,v}(R(u,v,a)) \wedge \neg R(m,m',a)\Big) \vee A(c,y)\Big], \tag{4.9}$$

pro všechny L_{PV}-termy t.

Pro spor předpokládejme, že T'_{PV} je bezesporná, a tudíž existuje model $\mathcal{A} \vDash T'_{PV}$. Uvažujme strukturu $\mathcal{B} \subseteq \mathcal{A}$ jako podstrukturu $\mathcal{A}$ s nosnou množinou $\{q \mid q \leq t(c),\ t \text{ je } L_{PV}\text{-term}\}$ (což je podstruktura, neboť každý polynomiální algoritmus je shora odhadnut nějakým polynomiálním algoritmem počítajícím rostoucí funkci, a tyto vlastnosti jsou T_{PV}-axiomy). Jelikož je T_{PV} univerzální teorie, $\mathcal{A} \vDash T_{PV}$, tak také $\mathcal{B} \vDash T_{PV}$. V $\mathcal{A}$ jsou splněny axiomy tvaru (4.9), kde po omezených ($t(c)$) kvantifikátorech následuje (v hranaté závorce) otevřená formule, tudíž je jejich pravdivost ovlivněná pouze pravdivostí této otevřené formule na prvcích nosné množiny $\mathcal{B}$. Tyto axiomy tedy platí také v $\mathcal{B}$, celkem tedy $\mathcal{B} \vDash T'_{PV}$. Speciálně $\mathcal{B} \vDash$ (4.8), ovšem všechna a, y v $\mathcal{B}$ jsou menší než $t(c)$ pro nějaký term t, tedy volbou $x \coloneqq c$ ve (4.8) dostáváme spor s (4.9).

T'_{PV} je tedy sporná. Jelikož důkazy využívají jen konečný počet axiomů, existuje pro nějaké $k \in \mathbb{N}$ množina k axiomů tvaru (4.9) (z důkazu sporu) sporná s L'_{PV}-teorií T_{PV}. Existují tedy termy $t_1, \ldots, t_k$ takové, že L'_{PV}-teorie T_{PV} dokazuje, že alespoň pro jeden z těchto termů (4.9) neplatí. Uvažujme term $b(x)$, který

shora odhaduje všechna $t_1, \ldots, t_k$ (například součet, vlastnost odhadu je univerzální sentence), pak pro tento term neplatí (4.9) (volba $t \coloneqq b$), a to v každém modelu L'_{PV}-teorie T_{PV}.

Nyní vezměme libovolný T_{PV}-model $\mathcal{M}$ a prvek x tohoto modelu. Volbou $c \coloneqq x$ v $\mathcal{M}$ dostáváme L'_{PV}-model $\mathcal{M}'$ L'_{PV}-teorie teorie T_{PV}. Pro $t \coloneqq b$ neplatí (4.9), tedy platí

$$\exists a, y \leq b(x) \forall m, u, v, w \leq a \exists m' \leq a \Big[\Big(\mathcal{L}_w^{u,v}(R(u, v, a)) \wedge R(m, m', a) \Big) \vee A(x, y) \Big],$$

což lze zpět přepsat na tvrzení ze znění lemmatu.

□

Věta 30. *Nechť $A(x, y)$ je otevřená L_{PV}-formule, pak*

$$S_{PV} \vdash \forall x \exists y A(x, y) \tag{4.10}$$

právě tehdy, když existuje $k \in \mathbb{N}$, L_{PV}-relace $R(u, v, z)$, L_{PV}-termy

$$z_1(x), z_2(x, m_1, u_1, v_1, w_1), z_3(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2), \ldots \\ \ldots, z_k(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_{k-1}, u_{k-1}, v_{k-1}, w_{k-1})$$

a termy

$$m'(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k), \\ y(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_{k-1}, u_{k-1}, v_{k-1}, w_{k-1})$$

takové, že teorie T_{PV} dokazuje

$$\forall x \forall m_1, u_1, v_1, w_1 \leq z_1(x) \forall m_2, u_2, v_2, w_2 \leq z_2(x, m_1, u_1, v_1, w_1) \ldots \\ \ldots \forall m_k, u_k, v_k, w_k \leq z_k(x, \ldots, w_{k-1}) \Big[A\Big(x, y(x, \ldots, w_{k-1})\Big) \\ \vee \bigvee_{i=1}^{k} D\Big(z_i(x, \ldots, w_{i-1}), m_i, u_i, v_i, w_i, m'(x, \ldots, w_k)\Big) \Big], \tag{4.11}$$

kde $D(z, m, u, v, w, m')$ značí formuli

$$(m' \leq z) \wedge \mathcal{L}_w^{u,v}(R(u, v, z)) \wedge \neg R(m, m', z).$$

Navíc pak axiom minima (viz definici 13) pro R společně s T_{PV} dokazuje $\forall x \exists y A(x, y)$ a za R můžeme zvolit libovolnou relaci takovou, že axiom minima pro tuto relaci společně T_{PV} dokazuje $\forall x \exists y A(x, y)$.

Důkaz. ($\Rightarrow$) Použitím lemmatu 28 a lemmatu o dedukci na (4.10) odvodíme, že existuje relace $R(x, y, z)$ o které teorie T_{PV} dokazuje

$$\forall z \Big[\Big(\forall u, v, w \leq z \, \mathcal{L}_w^{u,v}(R(u, v, z)) \Big) \rightarrow \exists m \leq z \forall m' \leq z \, R(m, m', z) \Big] \\ \rightarrow \forall x \exists y A(x, y),$$

což můžeme přepsat jako

$$\forall x \exists y \Big[\forall z \Big[\Big(\forall u, v, w \leq z \, \mathcal{L}_w^{u,v}(R(u,v,z)) \Big) \to \exists m \leq z \forall m' \leq z \, R(m,m',z) \Big] \\ \to A(x,y) \Big],$$

dále rozepsáním implikací dostaneme

$$\forall x \exists y \Big[\exists z \Big[\forall u, v, w \leq z \, \mathcal{L}_w^{u,v}(R(u,v,z)) \wedge \forall m \leq z \exists m' \leq z \neg R(m,m',z) \Big] \vee A(x,y) \Big],$$

což přepíšeme jako

$$\forall x \exists z, y \forall m, u, v, w \leq z \exists m' \leq z \Big[\Big(\mathcal{L}_w^{u,v}(R(u,v,z)) \wedge \neg R(m,m',z) \Big) \vee A(x,y) \Big]$$

a nakonec upravíme na tvar

$$\forall x \exists z, y \forall m, u, v, w \exists m' \Big[m, u, v, w \leq z \\ \to \Big((m' \leq z) \wedge \Big[\Big(\mathcal{L}_w^{u,v}(R(u,v,z)) \wedge \neg R(m,m',z) \Big) \vee A(x,y) \Big] \Big) \Big]. \quad (4.12)$$

Pro přehledost označme

$$D''(x,z,y,m,u,v,w,m') \coloneqq \\ m,u,v,w \leq z \to \Big((m' \leq z) \wedge \Big[\Big(\mathcal{L}_w^{u,v}(R(u,v,z)) \wedge \neg R(m,m',z) \Big) \vee A(x,y) \Big] \Big).$$

Použitím KPT věty (v. 5) na (4.12), kde ve znění věty uvažujeme, $\bar{x} \coloneqq x$, $\bar{y} \coloneqq z, y$, $\bar{z} \coloneqq m, u, v, w$, $B(\bar{x}, \bar{y}, \bar{z}) \coloneqq \exists m' D''(x,z,y,m,u,v,w,m')$, dostaneme, že existuje k přirozené a bloky (velikosti 2) termů

$$\bar{t}_1(x), \bar{t}_2(x, m_1, u_1, v_1, w_1), \bar{t}_3(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2), \ldots \\ \ldots, \bar{t}_k(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_{k-1}, u_{k-1}, v_{k-1}, w_{k-1}),$$

takové, že platí

$$\forall x \forall m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k \\ \bigvee_{i=1}^{k} \exists m' D'' \Big(x, \bar{t}_i(x, m_1, u_1, v_1, w_1, \ldots, m_{i-1}, u_{i-1}, v_{i-1}, w_{i-1}), m_i, u_i, v_i, w_i, m' \Big),$$

což můžeme dále přepsat jako

$$\forall x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k \exists m' \\ \bigvee_{i=1}^{k} D'' \Big(x, \bar{t}_i(x, m_1, u_1, v_1, w_1, \ldots, m_{i-1}, u_{i-1}, v_{i-1}, w_{i-1}), m_i, u_i, v_i, w_i, m' \Big).$$

Nyní použitím Herbrandovy věty (v. 3) dostáváme existenci termu

$$m'(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k),$$

takového, že

$$\forall x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k$$
$$\bigvee_{i=1}^{k} D''\Big(x, \bar{t}_i(x, m_1, u_1, v_1, w_1, \ldots, m_{i-1}, u_{i-1}, v_{i-1}, w_{i-1}), m_i, u_i, v_i, w_i,$$
$$m'(x, m_1, u_1, v_1, w_1, \ldots, m_k, u_k, v_k, w_k)\Big).$$

Označením složek bloků termů (velikosti dva) $\bar{t}_i$ jako z_i, y_i, dostaneme

$$\forall x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k$$
$$\bigvee_{i=1}^{k} D''\Big(x, z_i(x, \ldots, w_{i-1}), y_i(x, \ldots, w_{i-1}), m_i, u_i, v_i, w_i, m'(x, \ldots, w_k)\Big). \quad (4.13)$$

Existuje term

$$y(x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_{k-1}, u_{k-1}, v_{k-1}, w_{k-1}),$$

odpovídající algoritmu testujícímu pro zadané x, zda některé $y_i, i \in \{1, \ldots, k\}$ nesplňuje $A(x, y_i(x, \ldots, w_{i-1}))$, a vracejícímu případnou splňující hodnotu, tudíž ve standardním modelu platí

$$\forall x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k$$
$$\Big[\Big(\bigvee_{i=1}^{k} A\Big(x, y_i(x, v_1, \ldots, w_{i-1})\Big)\Big) \to A\Big(x, y(x, v_1, \ldots, w_{k-1})\Big)\Big],$$

což je univerzální sentence a tedy axiom T_{PV}.
Kdykoliv pro $x, m_1, u_1, v_1, w_1, m_2, \ldots, m_k, u_k, v_k$ (v libovolném T_{PV} modelu) neplatí $A(x, y(x, \ldots, w_{i-1}))$, pak neplatí ani kterékoliv $A(x, y_i(x, \ldots, w_{i-1}))$, $i \leq k$, a tudíž dle (4.13) platí

$$\bigvee_{i=1}^{k} D'\Big(z_i(x, \ldots, w_{i-1}), m_i, u_i, v_i, w_i, r(x, \ldots, w_k)\Big),$$

kde $D'(z, m, u, v, w, m')$ značí formuli

$$m, u, v, w \leq z \to \Big((m' \leq z) \wedge \mathcal{L}_w^{u,v}(R(u, v, z)) \wedge \neg R(m, m', z)\Big).$$

Celkem tedy máme

$$\forall x, m_1, u_1, v_1, w_1, m_2, u_2, v_2, w_2, \ldots, m_k, u_k, v_k, w_k \Big[A\Big(x, y(x, \ldots, w_{k-1})\Big)$$
$$\vee \bigvee_{i=1}^{k} D'\Big(z_i(x, \ldots, w_{i-1}), m_i, u_i, v_i, w_i, m'(x, \ldots, w_k)\Big)\Big],$$

z čehož již snadno odvodíme (4.11).

($\Leftarrow$) Uvažujme libovolný S_{PV} model $\mathcal{M}$ a libovolný prvek $x \in \mathcal{M}$. Spočtěme prvek $z_1(x)$, pak dle axiomů T_{PV} společně s axiomem minima pro relaci R buď $R(u, v, z_1(x))$ není lineární (v u, v a na prvcích menších než $z_1(x)$ při $\leq$), nebo existuje minimum této relace. Můžeme tedy zvolit prvky $m_1, u_1, v_1, w_1 \leq z_1(x)$ takové,

že $\mathcal{L}_{w_1}^{u_1,v_1}(R(u_1,v_1,z_1(x))) \to \forall m' \leq z_1(x) R(m_1,m',z_1(x))$. Obdobně budeme pokračovat, tedy v i-tém kroku najdeme prvky $m_i, u_i, v_i, w_i \leq z_i(x, m_1, \ldots, w_{i-1})$, takové, že

$$\mathcal{L}_{w_i}^{u_i,v_i}(R(u_i,v_i,z_i(x,\ldots))) \to \forall m' \leq z_i(x,\ldots) R(m_i,m',z_i(x,\ldots)).$$

Takto zvolíme všechny prvky $m_1, u_1, v_1, w_1 \ldots, m_k, u_k, v_k, w_k$. Z platnosti (4.11) a volby $m_1, u_1, v_1, w_1 \ldots, m_k, u_k, v_k, w_k$ plyne

$$A(x, y(x, m_1, u_1, v_1, w_1, \ldots, m_{k-1}, u_{k-1}, v_{k-1}, w_{k-1})).$$

A jelikož S_{PV} model $\mathcal{M}$ a prvek x tohoto modelu byly zvoleny libovolně, platí $S_{PV} \vdash \forall x \exists y A(x,y)$.

Poslední část věty 30 plyne z důkazů implikací.

□

Podobně jako v případě věty 5 lze formuli (4.10) ve znění věty 30 chápat jako hru mezi studentem a učitelem (respektive existenci takového polynomiálního studenta), kdy se student pro zadané x snaží buď najít z takové, že $R(u,v,z)$ je lineární v u, v na prvcích menších než z (při $\leq$) a zároveň na těchto prvcích nemá minimum (tedy porušuje axiom minima konkrétně pro $x \coloneqq z$ v definici 13), nebo najít y takové, že $A(x,y)$.

Student tedy pro zadané x spočte $z_1(x)$ a od učitele dostane čtveřici prvků $m_1, u_1, v_1, w_1 \leq z_1(x)$, o které učitel tvrdí, že buď u_1, v_1, w_1 je protipříkladem na linearitu relace $R(u,v,z_1(x))$ (v u, v a na prvcích menších než z při $\leq$), nebo m_1 je minimum $R(u,v,z_1(x))$. Dále student s učitelem postupují obdobně. V i-té interakci student spočte $z_i(x,\ldots,w_{i-1})$ a učitel ukáže studentovi čtveřici m_i, u_i, v_i, w_i, o které tvrdí, že buď dosvědčuje nelinearitu relace $R(u,v,z_i(\ldots))$ (v $u, v \leq z_i(\ldots)$), nebo je m_i minimum této relace.

Obecně není v moci studenta ověřit v i-tém kroku pro $i < k$, zda jsou učitelovy protipříklady validní (pokud učitel nenajde protipříklad na linearitu, student nepozná, zda je skutečně m_i minimem). Ovšem po poslední, tedy k-té interakci student vždy buď spočte hledané y splňující $A(x,y)$ (pomocí termu $y(\ldots)$), nebo dosvědčí učiteli, že některý z jeho protipříkladů nebyl validní, neboť $m'(x,\ldots,w_k)$ nebude větší nebo rovno (při $R(u,v,z_i(\ldots))$) než učitelem navrhované minimum v některé z předchozích interakcí (takové kde učitel nenašel protipříklad na linearitu). Všimněme si, že věta nevylučuje možnost, kdy student dostane nesprávné protipříklady od učitele, ani po k-té interakci není schopen učitele opravit (termem m'). Pokud se učitel opraví, pak pochopitelně může hra od dané interakce pokračovat.

Platí-li $S_{PV} \vdash \forall x \exists y A(x,y)$, pak existenci „studenta“ z věty 30 můžeme použít při hledání y pro zadané x tak aby, platilo $A(x,y)$. Umíme-li najít „učitelovy“ protipříklady, tak aby v nich student nedokázal najít chybu ani po k-té interakci, pak už dokážeme (respektive „student“ dokáže) najít v polynomiálním čase hledané y. To vede k formulaci třídy NP vyhledávacích problémů (viz def. 7) spjatou s teorií S_{PV} v následujícím smyslu.

Důsledek 31. *Nechť $A(x,y)$ je relace na $\mathbb{N}_0$ rozhodnutelná v polynomiálním čase a platí*

$$S_{PV} \vdash \forall x \exists y A(x,y).$$

Pak existuje term $b(x)$ takový, že úloha nalezení y pro zadané x takového, aby platilo $A(x,y) \wedge y \leq b(x)$, je NP vyhledávacím problémem p-redukovatelným na NP vyhledávací problém nalezení (pro zadané x) posloupnosti s kódující validní sadu „učitelových protipříkladů“ takových, že je příslušný „student“ nedokáže opravit. Formálně je tedy tento NP vyhledávací problém definovaný relací tvaru

$$\begin{aligned} Q(x,s) = \bigwedge_{i=1}^{k} \Big[& (s)_{4i-3}, (s)_{4i-2}, (s)_{4i-1}, (s)_{4i} \leq z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \\ & \wedge \Big(\neg \Big(m'(x, (s)_1, \ldots, (s)_{4i}) \leq z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \Big) \\ & \vee \neg \mathcal{L}^{(s)_{4i-2}, (s)_{4i-1}}_{(s)_{4i}} \Big(R\Big((s)_{4i-2}, (s)_{4i-1}, z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \Big) \Big) \\ & \vee R\Big((s)_{4i-3}, m'(x, (s)_1, \ldots, (s)_{4i}), z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \Big) \Big) \Big] \wedge len(s) = 4k, \end{aligned} \tag{4.14}$$

kde k je přirozené číslo, $R(u,v,z)$ je relace na $\mathbb{N}_0$ rozhodnutelná v polynomiálním čase, z_i jsou funkce $\mathbb{N}_0^{(4i-3)} \to \mathbb{N}_0$ spočitatelné v polynomiálním čase, $i \in \{1, \ldots, k\}$ a m' je funkce $\mathbb{N}_0^{(4k+1)} \to \mathbb{N}_0$ spočitatelná v polynomiálním čase.

Nechť naopak $\forall x \forall v [Q(f(x), v) \to A(x, g(x,v))]$, kde f, q jsou polynomiální algoritmy, A je relace na $\mathbb{N}_0$ rozhodnutelná v polynomiálním čase a Q je relace na $\mathbb{N}_0$ tvaru (4.14), pak $S_{PV} \vdash \forall x \exists y A(x,y)$.

Důkaz. S použitím lemmatu 29 dostáváme, že kdykoliv $S_{PV} \vdash \forall x \exists y A(x,y)$, pak $S_{PV} \vdash \forall x \exists y \leq b(x) A(x,y)$ pro nějaký L_{PV}-term $b(x)$ odpovídající polynomiálnímu algoritmu. Teorie S_{PV} tedy dokazuje polynomiální odhad $|y|$ v závislosti na $|x|$, jak požaduje definice NP vyhledávacího problému (def. 7). Relace $A(x,y) \wedge y \leq b(x)$ tudíž definuje NP vyhledávací problém.

Pro libovolnou relaci Q tvaru (4.14) platí $S_{PV} \vdash \forall x \exists s Q(x,s)$, neboť stačí induktivně zvolit hodnoty čtveřic z posl. s, tedy $(s)_{4i-3}, (s)_{4i-2}, (s)_{4i-1}, (s)_{4i} \leq z_i(x, (s)_1, \ldots, (s)_{4(i-1)})$ tak, aby platilo buď

$$\neg \mathcal{L}^{(s)_{4i-2}, (s)_{4i-1}}_{(s)_{4i}} \Big(R\Big((s)_{4i-2}, (s)_{4i-1}, z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \Big) \Big),$$

nebo

$$\forall m' \neg R\Big((s)_{4i-3}, m', z_i(x, (s)_1, \ldots, (s)_{4(i-1)}) \Big) \Big),$$

což lze dle axiomů S_{PV}. Zakódováním do posloupnosti s (pomocí termu kódujícího posloupnosti délky $4k$) pak dostáváme hledaný prvek splňující $Q(x,s)$. Jelikož pro zadané x z odhadu $(s)_{4i-3}, (s)_{4i-2}, (s)_{4i-1}, (s)_{4i} \leq z_i(x, (s)_1, \ldots, (s)_{4(i-1)})$ indukcí dostaneme polynomiální odhad (v závislosti na x) velikosti všech členů posloupnosti s splňující $Q(x,s)$, máme i polynomiální odhad velikosti posloupnosti s (délky $4k$) samotné. Relace Q tedy definuje NP vyhledávací problém.

Nechť nyní $S_{PV} \vdash \forall x \exists y A(x,y)$, pak věta 30 implikuje existenci termů $z_i, i \in \{1, \ldots, k\}$, m', y splňujících (4.11). Definujme relaci Q přirozeně pomocí těchto termů (bez y). Buď s takové, že $Q(x,s)$. Označme pro $i \in \{1, \ldots, k\}$ $m_i \coloneqq (s)_{4i-3}$, $u_i \coloneqq (s)_{4i-2}$, $v_i \coloneqq (s)_{4i-1}$, $w_i \coloneqq (s)_{4i}$. Pak přirozeným použitím (4.11) v kombinaci s platností $Q(x,s)$ dostáváme $A(x, y(x, (s)_1, \ldots, (s)_{4(i-1)}))$. Volbou $f(x) \coloneqq x$ a $g(x,v) \coloneqq y(x, (v)_1, \ldots, (v)_{4(i-1)})$ v definici 8 dostáváme hledanou p-redukci.

Nechť naopak $\forall x \forall v[Q(f(x), v) \to A(x, g(x, v))]$, kde A je relace na $\mathbb{N}_0$ rozhodnutelná v polynomiálním čase a Q je tvaru (4.14). Pak tato formule je jakožto univerzální sentence T_{PV}-axiomem. Dále již víme, že $S_{PV} \vdash \forall x \exists s Q(x, s)$. V každém S_{PV}-modelu pro libovolné zadané x tedy existuje s splňující $Q(f(x), s)$, a platí tudíž $A(x, g(x, s))$. Celkem tedy $S_{PV} \vdash \forall x \exists y A(x, y)$.

□

Závěr

Podařilo se odvodit dosvědčovací větu (v. 30), která dává do souvislosti S_{PV}-dokazatelnost (viz def. 13) formule tvaru $\forall x \exists y A(x, y)$, kde $A(x, y)$ je relace rozhodnutelná v polynomiálním čase, s konkrétní třídou složitosti problému nalezení y pro zadané x takového, že platí $A(x, y)$.

Tento výsledek lze asi nejsnáze pochopit jako hru mezi studentem a učitelem. Učitel zadá x a student se snaží učitele buď přesvědčit, že pro vhodně zvolené z je konkrétní relace $R(u, v, z)$ lineární v u, v na prvcích $\leq$-menších než z, a přesto zde nemá minimum, nebo najít y takové, že platí $A(x, y)$. Student tedy spočte z a doufá, že $R(u, v, z)$ má požadované vlastnosti. Učitel se pokusí studenta přesvědčit o opaku tím, že najde buď prvky dosvědčující nelinearitu $R(u, v, z)$, a nebo tím, že najde minimum této relace (obojí myšleno v u, v a na prvcích $\leq z$). Ačkoli student v případě minima nepozná, zda se jedná skutečně o minimum, předpokládá, že se učitel nebude mýlit, a pokusí se najít jiný prvek z požadovaných vlastností. Takto učitel se studentem pokračují, přičemž student k výpočtu dalších z používá jak x, tak všechny domnělé protipříklady, které od učitele v minulosti dostal. Potom, co student dostane od učitele k-tý ($k \in \mathbb{N}$ je pevná vlastnost studenta) domnělý protipříklad, nastane alespoň jedna ze dvou možností. Buď student uspěje v nalezení y takového, že $A(x, y)$, nebo dokáže učiteli, že některý z jeho domnělých protipříkladů minimem byl chybný, tím, že spočte prvek, který není větší ani roven učitelovu protipříkladu. Student tedy volil již prvky z i v závislosti na x, aby mu učitelovy protipříklady mohly případně pomoci ke spočtení y. Možnost, že student dostane chybné protipříklady a není schopen opravit učitele ani po k-tém pokusu, avšak dokáže spočítat hledané y (byť na základě nesprávných protipříkladů), není vyloučena. Věta 30 říká, že $S_{PV} \vdash \forall x \exists y A(x, y)$ (kde $A(x, y)$ je rozhodnutelná v polynomiálním čase), právě tehdy, když takovýto student existuje (společně s příslušnou relací $R(u, v, z)$) jako sada konečně mnoha polynomiálních algoritmů.

V důsledku 31 je třída problémů řešitelných takovýmto studentem zformulovaná jako třída NP vyhledávacích problémů p-redukovatelných na NP vyhledávací problémy konkrétního tvaru (viz def. 7, 8). Zjednodušeně řečeno, za předpokladů věty k nalezení y pro zadané x tak, aby platilo $A(x, y)$, stačí nalézt kompletní validní (v kontextu studentem počítaných z) sadu učitelových protipříkladů takových, že příslušný student není schopen žádný z nich opravit (a tedy umí najít řešení y).

V kapitole 3 jsou demonstrovány důvody domnívat se, že teorie S_{PV} je silnější než T_{PV} („příliš silné“ důsledky v opačném případě, relativizovaná verze), a tedy výsledky kapitoly 4 tak nejspíš nejsou triviální. Samotná otázka, zda je skutečně S_{PV} ostře silnější než T_{PV}, však nadále zůstává otevřeným problémem.

Seznam použité literatury

Buss, S. R. a Krajíček, J. (1994). An application of boolean complexity to separation problems in bounded arithmetic. *Proceedings of the London Mathematical Society*, **69(3)**, 1–21.

Chiari, M. a Krajíček, J. (1998). Witnessing functions in bounded arithmetic and search problems. *Journal of Symbolic Logic*, **63**(3), 1095–1115.

Herbrand, J. (1930). Recherches sur la théorie de la démonstration. *Travaux historiques de la Société des sciences et des lettres de Varsovie*, **33**.

Johnson, D. S., Papadimitriou, C. H. a Yannakakis, M. (1988). How easy is local search? *Journal of Computer and System Sciences*, **37**(1), 79–100.

Krajíček, J. (1995). *Bounded arithmetic, propositional logic, and complexity theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press. ISBN 0-521-45205-8.

Krajíček, J. (2010). From feasible proofs to feasible computations. *Computer Science Logic*, **LNCS 6247**, 22–31.

Krajíček, J. (2019). *Proof Complexity*, volume 170 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press. ISBN 9781108416849.

Krajíček, J., Pudlák, P. a Sgall, J. (1990). Interactive computations of optimal solutions. *Mathematical Foundations of Computer Science*, **LNCS 452**, 48–60.

Krajíček, J., Pudlák, P. a Takeuti, G. (1991). Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, **52**, 143–153.

Papadimitriou, C. H. (1994). On the complexity of the parity argument and other inefficient proofs of existence. *Journal of Computer and System Sciences*, **48**(3), 498–532.