DIPLOMARBEIT

Decidability of Diophantine equations in a theory adjacent to IOpen

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Technische Mathematik

eingereicht von

Fabian Achammer, BSc BSc

Matrikelnummer 01621489

unter der Anleitung von

Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

ausgeführt am

Institut für Diskrete Mathematik und Geometrie
der Fakultät für Mathematik und Geoinformation
der Technischen Universität Wien

Wien, am 28.04.2023

Fabian Achammer	Stefan Hetzl

Kurzfassung

Hilberts zehntes Problem ist die Frage, ob es einen Algorithmus gibt, der für ein gegebenes Polynom mit ganzzahligen Koeffizienten bestimmt, ob es ganzzahlige Nullstellen hat. Als Folgerung aus dem MRDP-Theorem wurde gezeigt, dass kein solcher Algorithmus existiert. Anders ausgedrückt: Diophantische Erfüllbarkeit is unentscheidbar für die Arithmetik der natürlichen Zahlen. Eine naheliegende Fragestellung ist nun das Problem der Entscheidbarkeit der Diophantischen Erfüllbarkeit für schwächere arithmetische Theorien.

In dieser Arbeit präsentieren wir einen neuen beweistheoretischen Ansatz, um Diophantische Erfüllbarkeitsprobleme zu entscheiden. Wir arbeiten in einer arithmetischen Theorie A, deren Sprache Nachfolger, Vorgänger, Addition und Multiplikation enthält. Ein Resultat von Shepherdson erlaubt es uns, eine Theorie AB zu definieren, die sich nur um ein Axiomenschema von der Theorie der offenen Induktion über A unterscheidet. Wir zeigen, dass das Diophantische Erfüllbarkeit für AB entscheidbar ist.

Abstract

Hilbert's 10th problem is the question whether there is an algorithm which, given a polynomial with integer coefficients, determines whether it has integer roots. It has been shown that no such algorithm exists as a consequence of the MRDP theorem. In other words: Diophantine satisfiability is undecidable for arithmetic. One can now ask whether the problem of Diophantine satisfiability is decidable for weaker theories of arithmetic.

In this thesis we present a novel proof-theoretic approach for deciding Diophantine satisfiability problems. We work in a base arithmetical theory A in the language with successors, predecessors, addition and multiplication and use a result by Shepherdson to define a theory AB which is one axiom schema short of the theory of open induction over A. We show that Diophantine satisfiability of AB is decidable.

Acknowledgement

My biggest thanks goes to my advisor Stefan Hetzl who provided me with an interesting and challenging problem, worked with me through major and minor steps in its proof and helped me shape this thesis during countless discussions.

I also thank my friends and family who have always supported me in my endeavors and helped me through a challenging time in my life.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am 27. April 2023

Fabian Achammer

Contents

1 Introduction

Hilbert's 10th problem is the question whether there is an algorithm which, given a polynomial with integer coefficients, determines whether it has integer roots. It has been shown that no such algorithm exists as a consequence of the MRDP theorem, named after Matiyasevič, Robinson, Davis and Putnam.

A generalization of Hilbert's 10th problem is this: Given an arithmetical theory T, is there an algorithm which decides for every Diophantine equation, whether one can prove its unsolvability in T? We call such problems *Diophantine satisfiability problems*. Some variations of the MRDP theorem show the undecidability of Diophantine satisfiability problems for theories weaker than Peano arithmetic. A positive result has been obtained by Jeřábek, who showed in [3] that Diophantine satisfiability in the Robinson arithmetic Q is decidable. The decidability for IOpen, the theory of open induction over Q has remained an open problem since it was posed by Shepherdson [4].

In this thesis we present a new proof-theoretic approach for deciding Diophantine satisfiability. We work in an arithmetical base theory A whose language consists of successors, predecessors, addition and multiplication, but does not contain inequality. Using a result by Shepherdson [5] we extract a subtheory AB of the theory of open induction over A and show decidability of Diophantine satisfiability for AB.

The rest of this thesis is structured as follows: In chapter 2 we introduce definitions and notations for the rest of the thesis and mention basic results from proof theory and the study of arithmetical theories. Chapter 3 introduces the main result of this thesis, defines the specialized proof calculus $\mathcal{P}_T$, outlines the proof strategy and shows the soundness of $\mathcal{P}_T$ as a first result. In chapters 4 and 5 respectively we show completeness and decidability of $\mathcal{P}_T$. The thesis concludes in chapter 6 by giving an outline for future work.

2 Preliminaries

2.1 Logic and proof theory

In this thesis we will use several different proof calculi, so we introduce a general notion of proof calculus which fits these different scenarios:

Definition 2.1. *Let X be a set. For $n \in \mathbb{N}$ an* inference rule of arity n on X *is a relation $I \subseteq X^{n+1}$. Elements of I are called* I-inferences *and for $(S, S_1, \ldots, S_n) \in I$ we also write*

$$\frac{S_1 \quad \cdots \quad S_n}{S} \; I \; .$$

Furthermore, S is called the conclusion *of the inference and $S_1, \ldots, S_n$ are called the* premises *of the inference. A non-empty inference rule of arity 0 is called* initial.

A proof calculus on X *is a set $\mathcal{C}$ of inference rules on X. The relation π* is a $\mathcal{C}$-proof of S *(in symbols: $\pi \vdash_{\mathcal{C}} S$) is inductively defined as the smallest relation with the following closure property: If $I \in \mathcal{C}$ is an n-ary inference rule, $S_1, \ldots, S_n \in X$, $\pi_1 \vdash_{\mathcal{C}} S_1, \ldots, \pi_n \vdash_{\mathcal{C}} S_n$ such that $(S, S_1, \ldots, S_n) \in I$, then $(S, I, \pi_1, \ldots, \pi_n) \vdash_{\mathcal{C}} S$.*

Instead of $(S, I, \pi_1, \ldots, \pi_n) \vdash_{\mathcal{C}} S$ we also write

$$\frac{\pi_1 \quad \cdots \quad \pi_n}{S} \; I,$$

and instead of $\pi_1 \vdash_{\mathcal{C}} S_1, \ldots, \pi_n \vdash_{\mathcal{C}} S_n, (S, I, \pi_1, \ldots, \pi_n) \vdash_{\mathcal{C}} S$ we write

$$\frac{\begin{matrix}(\pi_1) & & (\pi_n) \\ S_1 & \cdots & S_n\end{matrix}}{S} \; I.$$

We say π is a $\mathcal{C}$-proof *if there exists an $S \in X$ such that $\pi \vdash_{\mathcal{C}} S$. By definition, we have that if π is a $\mathcal{C}$-proof then there is a unique S such that $\pi \vdash_{\mathcal{C}} S$. If $\pi \vdash_{\mathcal{C}} S$, we say that S is the* conclusion of π. *We say that π* ends in an inference rule I *if $\pi = (S, I, \pi_1, \ldots, \pi_n)$ for some $\mathcal{C}$-proofs $\pi_1, \ldots, \pi_n$ and $S \in X$. We inductively define that* a $\mathcal{C}$-proof π uses an inference rule I *if π ends in I or $\pi = (S, J, \pi_1, \ldots, \pi_n)$ and any of the proofs $\pi_1, \ldots, \pi_n$ uses I. If $\pi = (S, I, \pi_1, \ldots, \pi_n)$, then $\pi_1, \ldots, \pi_n$ are called* direct subproofs of π. *Further, we inductively define that ρ* is a subproof of π *if $\rho = \pi$ or ρ is a subproof of a direct subproof ρ' of π. If $\pi = (S, I, \pi_{\text{left}}, \pi_{\text{right}})$ we call π_{left} the* left direct subproof of π *and π_{right} the* right direct subproof of π. *Further let ρ, σ be subproofs of π. We say ρ* is between π and σ *if σ is a subproof of ρ. We say ρ* is strictly between π and σ *if ρ is between π and σ, $\rho \neq \sigma$ and $\rho \neq \pi$. We say a subproof ρ of π with a certain property is a* lowermost *such subproof if the only subproof between π and ρ with that property is ρ itself. We say that ρ*

is an uppermost *such subproof, if the only subproof of ρ with that property is ρ itself. We inductively define the number of inferences in $\pi = (S, I, \pi_1, \ldots, \pi_n)$, written as $\#(\pi)$ by $\#(\pi) := 1 + \sum_{i=1}^{n} \#(\pi_i)$. We define the* number of I-inferences in π *(denoted by $\#_I(\pi)$) as the number of subproofs of π that end in an I-inference.*

We write $\vdash_{\mathcal{C}} S$ or $\mathcal{C} \vdash S$ to mean there exists a $\mathcal{C}$-proof π with $\pi \vdash_{\mathcal{C}} S$. If $\mathcal{C}$ is a proof calculus on X and J is an inference rule on X we write $\mathcal{C}+J$ for the proof calculus $\mathcal{C} \cup \{J\}$.

In this thesis we will only use languages with equality. Therefore, we will just use *language* when we mean *language with equality.*

Definition 2.2. *We define the set of variables as $V := \{\mathsf{x}_n \mid n \in \mathbb{N}\}$. Let L be a language. We call $T(L)$ the set of L-terms. Further we write $A(L)$ for the set of L-atoms, $N(L)$ for the set of negated L-atoms and $\mathrm{Lit}(L)$ for the set of L-literals. For $\varphi \in \mathrm{Lit}(L)$ we write $\varphi^\perp$ for the dual literal of φ, i.e. for φ we set $\varphi^\perp :\equiv \neg\varphi$ and for $\varphi \equiv \neg\psi$ we set $\varphi^\perp :\equiv \psi$.*

$F(L)$ denotes set of L-formulas built from $\neg$ (negation), $\wedge$ (conjunction), $\vee$ (disjunction), $\supset$ (implication), $\forall x$ (universal quantification) and $\exists x$ (existential quantification). $F_{\mathrm{qf}}(L)$ is the set of quantifier-free L-formulas. For L-formulas φ, ψ we write $\varphi \leftrightarrow \psi$ as a shorthand for $(\varphi \supset \psi) \wedge (\psi \supset \varphi)$.

Definition 2.3. *Let X be a set. A* multiset over X *is a function $X \to \mathbb{N}$. Let Γ be a multiset. For $x \in X$ we write $x \in \Gamma$, if $\Gamma(x) > 0$. Let Δ be another multiset. We write $\Gamma \subseteq \Delta$ if $\Gamma(x) \leq \Delta(x)$ for all $x \in X$. We write $\Gamma \cup \Delta$ for the multiset $x \mapsto \Gamma(x) + \Delta(x)$, $\Gamma \cap \Delta$ for the multiset $x \mapsto \min(\Gamma(x), \Delta(x))$ and $\Gamma - \Delta$ for the multiset $x \mapsto \Gamma(x) \dot{-} \Delta(x)$ where $n \dot{-} m$ is $n - m$ if $n \geq m$ and 0 otherwise. We define the* support of Γ, *denoted by* $\mathrm{supp}(\Gamma)$, *as the set $\{x \in X \mid \Gamma(x) > 0\}$. We say Γ* is finite *if $\Gamma(x) > 0$ only for finitely many $x \in X$. If Γ is finite we denote by $|\Gamma|$* size of Γ, *defined as $\sum_{x \in X} \Gamma(x)$. We write $\emptyset$ for the multiset $x \mapsto 0$. We write $\mathcal{M}(X)$ for the set of finite multisets over X.*

Definition 2.4 (sequent)**.** *Let L be a language and let Γ, Δ be finite multisets of formulas in $F(L)$. Then the tuple (Γ, Δ) is called a L-sequent, written as $\Gamma \longrightarrow \Delta$. Γ is called the* antecedent *of the sequent and Δ is called the* succedent *of the sequent. If $\Gamma = \{\varphi_1, \ldots, \varphi_n\}$ and $\Delta = \{\psi_1, \ldots, \psi_m\}$ we often omit the curly braces and write $\varphi_1, \ldots, \varphi_n \longrightarrow \psi_1, \ldots, \psi_m$ for the sequent $\Gamma \longrightarrow \Delta$. We also mix these notations and e.g. write $\varphi, \Gamma \longrightarrow \Delta, \psi$ for the sequent $\Gamma \cup \{\varphi\} \longrightarrow \Delta \cup \{\psi\}$. The set of L-sequents is denoted by $\mathrm{Seq}(L)$.*

Definition 2.5. *Let L be a language and $\varphi \in F(L)$. We denote the set of free variables of φ by $\mathrm{FV}(\varphi)$. If $\mathrm{FV}(\varphi) = \emptyset$, we say that φ* is closed. *We extend these notions to multisets of formulas Γ by $\mathrm{FV}(\Gamma) := \bigcup_{\varphi \in \Gamma} \mathrm{FV}(\varphi)$ and sequents $\Gamma \longrightarrow \Delta$ by $\mathrm{FV}(\Gamma \longrightarrow \Delta) := \mathrm{FV}(\Gamma \cup \Delta)$.*

Notation 2.6. *Let L be a language, $t \in T(L)$ and let $x_1, \ldots, x_n$ be variables. We write $t(x_1, \ldots, x_n)$ to mean that the variables $x_1, \ldots, x_n$ may occur in t. Further, if we have $u_1, \ldots, u_n \in T(L)$ we write $t(u_1, \ldots, u_n)$ for the term which results from simultaneously substituting the variables x_i in t by the terms u_i. We extend this notation for substitution to substituting free variables in formulas, multisets of formulas, sequents and proofs. Instead of writing $u_1, \ldots, u_n$ we often abbreviate to $\bar{u}$, if n is clear from the context or irrelevant.*

Definition 2.7. *Let L be a language, $\varphi, \psi \in F(L)$. We write $\psi \preceq \varphi$ if ψ is a subformula of φ and also say φ* contains *ψ. We say φ* contains *$\neg$, if there is a $\psi \in F(L)$ with*

$(\neg\psi) \preceq \varphi$. *Similarly, for* $\odot \in \{\wedge, \vee, \supset\}$, *we say* φ contains $\odot$, *if there are* $\psi, \chi \in F(L)$ *with* $(\psi \odot \chi) \preceq \varphi$. *For* $Q \in \{\forall, \exists\}$ *we also say* φ contains Q, *if there is a* $\psi \in F(L)$ *and a variable* x *with* $(Qx\psi) \preceq \varphi$. *Now let* Γ, Δ *be multisets of L-formulas and* $s \in \{\neg, \wedge, \vee, \supset, \forall, \exists\}$. *We say* Γ contains s *if there is a* $\varphi \in \Gamma$ *such that* φ *contains* s. *We say* $\Gamma \longrightarrow \Delta$ contains s *if* $\Gamma \cup \Delta$ *contains* s.

Definition 2.8. *Let* L *be a language. In the following,* Γ, Δ, Π *and* Λ *denote arbitrary multisets of* L- *formulas,* φ *and* ψ *denote arbitrary* L*-formulas,* A *denotes an arbitrary atomic* L*-formula,* t *denotes an arbitrary* L*-term and* x, y *denote variables. We now define inference rules on* $\mathrm{Seq}(L)$ *by their inferences:*

(i) logical axiom*:*

$$\frac{}{A \longrightarrow A}\ \text{axiom.}$$

A *is called the* principal occurrence.

(ii) weakening*:*

$$\frac{\Gamma \longrightarrow \Delta}{\varphi, \Gamma \longrightarrow \Delta}\ \mathrm{w}_{\mathrm{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \varphi}\ \mathrm{w}_{\mathrm{right}}.$$

φ *is called the* principal occurrence, Γ, Δ *is called the* context.

(iii) contraction*:*

$$\frac{\varphi, \varphi, \Gamma \longrightarrow \Delta}{\varphi, \Gamma \longrightarrow \Delta}\ \mathrm{c}_{\mathrm{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi, \varphi}{\Gamma \longrightarrow \Delta, \varphi}\ \mathrm{c}_{\mathrm{right}}.$$

φ *in the conclusion is called the* principal occurrence, *The* φ*-occurrences in the premises are called* auxiliary occurrences. Γ, Δ *is called the* context.

(iv) cut*:*

$$\frac{\Gamma \longrightarrow \Delta, \varphi \quad \varphi, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}\ \text{cut.}$$

We call φ *the* cut formula. *The occurrences of* φ *in the premises are called* auxiliary occurrences. cut *has no principal occurrence.* $\Gamma, \Pi, \Delta, \Lambda$ *is called the* context

If φ *is atomic we call the* cut*-inference* atomic.

(v) negation*:*

$$\frac{\Gamma \longrightarrow \Delta, \varphi}{\neg\varphi, \Gamma \longrightarrow \Delta}\ \neg_{\mathrm{left}} \qquad \textit{and} \qquad \frac{\varphi, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg\varphi}\ \neg_{\mathrm{right}}.$$

The occurrence of φ *in the premise is called* auxiliary occurrence. *The occurrence of* $\neg\varphi$ *in the conclusion is called* principal occurrence. Γ, Δ *is called the context.*

(vi) conjunction*:*

$$\frac{\varphi, \psi, \Gamma \longrightarrow \Delta}{\varphi \wedge \psi, \Gamma \longrightarrow \Delta}\ \wedge_{\mathrm{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi \quad \Pi \longrightarrow \Lambda, \psi}{\Gamma, \Pi \longrightarrow \Delta, \Lambda, \varphi \wedge \psi}\ \wedge_{\mathrm{right}}.$$

The occurrences of φ, ψ *in the premises are called* auxiliary occurrences. *The occurrences of* $\varphi \wedge \psi$ *in the conclusion are called* principal occurrences. Γ, Δ *and* $\Gamma, \Pi, \Delta, \Lambda$ *are called the* context *respectively.*

(vii) disjunction:

$$\frac{\varphi, \Gamma \longrightarrow \Delta \quad \psi, \Pi \longrightarrow \Lambda}{\varphi \vee \psi, \Gamma, \Pi \longrightarrow \Delta, \Lambda} \vee_{\text{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi, \psi}{\Gamma \longrightarrow \Delta, \varphi \vee \psi} \vee_{\text{right}}.$$

The occurrences of φ, ψ *in the premises are called* auxiliary occurrences. *The occurrences of* $\varphi \vee \psi$ *in the conclusion are called* principal occurrences. Γ, Δ *and* $\Gamma, \Pi, \Delta, \Lambda$ *are called the* context *respectively.*

(viii) implication:

$$\frac{\Gamma \longrightarrow \Delta, \varphi \quad \psi, \Pi \longrightarrow \Lambda}{\varphi \supset \psi, \Gamma, \Pi \longrightarrow \Delta, \Lambda} \supset_{\text{left}} \qquad \textit{and} \qquad \frac{\varphi, \Gamma \longrightarrow \Delta, \psi}{\Gamma \longrightarrow \Delta, \varphi \supset \psi} \supset_{\text{right}}.$$

The occurrences of φ, ψ *in the premises are called* auxiliary occurrences. *The occurrences of* $\varphi \supset \psi$ *in the conclusion are called* principal occurrences. Γ, Δ *and* $\Gamma, \Pi, \Delta, \Lambda$ *are called the* context *respectively.*

(ix) universal quantification:

$$\frac{\varphi(t), \Gamma \longrightarrow \Delta}{\forall x\, \varphi(x), \Gamma \longrightarrow \Delta} \forall_{\text{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi(y)}{\Gamma \longrightarrow \Delta, \forall x\, \varphi(x)} \forall_{\text{right}}$$

where $y \notin \mathrm{FV}(\Gamma \longrightarrow \Delta, \forall x\, \varphi(x))$. *The occurrence of* φ *in the premise is called* auxiliary occurrence. *The occurrence of* $\forall x\, \varphi$ *in the conclusion is called* principal occurrence. Γ, Δ *is called the context.* y *is called* eigenvariable. *The condition that* y *does not occur in the lower sequent is called the* eigenvariable condition.

(x) existential quantification:

$$\frac{\varphi(y), \Gamma \longrightarrow \Delta}{\exists x\, \varphi(x), \Gamma \longrightarrow \Delta} \exists_{\text{left}} \qquad \textit{and} \qquad \frac{\Gamma \longrightarrow \Delta, \varphi(t)}{\Gamma \longrightarrow \Delta, \exists x\, \varphi(x)} \exists_{\text{right}}$$

where $y \notin \mathrm{FV}(\exists x\, \varphi(x), \Gamma \longrightarrow \Delta)$. *The occurrence of* φ *in the premise is called* auxiliary occurrence. *The occurrence of* $\exists x\, \varphi$ *in the conclusion is called* principal occurrence. Γ, Δ *is called the context.* y *is called* eigenvariable. *The condition that* y *does not occur in the lower sequent is called the* eigenvariable condition.

(xi) reflexivity*:*

$$\frac{}{\longrightarrow t = t}\ \text{refl.}$$

$t = t$ *is called the* principal occurrence.

(xii) equality*:*

$$\frac{\Gamma \longrightarrow \Delta, t = u \quad A(t), \Pi \longrightarrow \Lambda}{A(u), \Gamma, \Pi \longrightarrow \Delta, \Lambda}\ \text{eq}{\rightarrow}_{\text{left}},$$

$$\frac{\Gamma \longrightarrow \Delta, t = u \quad \Pi \longrightarrow \Lambda, A(t)}{\Gamma, \Pi \longrightarrow \Delta, \Lambda, A(u)}\ \text{eq}{\rightarrow}_{\text{right}},$$

$$\frac{\Gamma \longrightarrow \Delta, t = u \quad A(u), \Pi \longrightarrow \Lambda}{A(t), \Gamma, \Pi \longrightarrow \Delta, \Lambda}\ \text{eq}{\leftarrow}_{\text{left}},$$

$$\frac{\Gamma \longrightarrow \Delta, t = u \quad \Pi \longrightarrow \Lambda, A(u)}{\Gamma, \Pi \longrightarrow \Delta, \Lambda, A(t)}\ \text{eq}{\leftarrow}_{\text{right}}.$$

In all the equality inferences we call $t = u$ *the* auxiliary equality *and* A *the* principal equality. *We also call the occurrences of* $t = u$, $A(u)$, $A(t)$ *in the premises* auxiliary occurrences *and the occurrences of* A *in the conclusion* principal occurrences. $\Gamma, \Pi, \Delta, \Lambda$ *is called the* context. *We call the rules* $\mathrm{eq}{\rightarrow}_{\mathrm{left}}$ *and* $\mathrm{eq}{\rightarrow}_{\mathrm{right}}$ *the* left-to-right equality rules *and* $\mathrm{eq}{\leftarrow}_{\mathrm{left}}$ *and* $\mathrm{eq}{\leftarrow}_{\mathrm{right}}$ *the* right-to-left equality rules.

We also define sets of inference rules:

(i) structural rules $\mathcal{S} := \{\mathrm{axiom}, \mathrm{w}_{\mathrm{left}}, \mathrm{w}_{\mathrm{right}}, \mathrm{c}_{\mathrm{left}}, \mathrm{c}_{\mathrm{right}}, \mathrm{cut}\}$,

(ii) propositional rules $\mathcal{B} := \{\neg_{\mathrm{left}}, \neg_{\mathrm{right}}, \wedge_{\mathrm{left}}, \wedge_{\mathrm{right}}, \vee_{\mathrm{left}}, \vee_{\mathrm{right}}, \supset_{\mathrm{left}}, \supset_{\mathrm{right}}\}$,

(iii) quantifier rules $\mathcal{Q} := \{\forall_{\mathrm{left}}, \forall_{\mathrm{right}}, \exists_{\mathrm{left}}, \exists_{\mathrm{right}}\}$,

(iv) equational rules $\mathcal{E} := \{\mathrm{refl}, \mathrm{eq}{\rightarrow}_{\mathrm{left}}, \mathrm{eq}{\rightarrow}_{\mathrm{right}}, \mathrm{eq}{\leftarrow}_{\mathrm{left}}, \mathrm{eq}{\leftarrow}_{\mathrm{right}}\}$,

(v) sequent calculus with equality $\mathrm{LK}^{=}(L) := \mathcal{S} \cup \mathcal{B} \cup \mathcal{Q} \cup \mathcal{E}$.

If the language L is known from the context, we just write $\mathrm{LK}^{=}$ instead of $\mathrm{LK}^{=}(L)$. It is well-known that $\mathrm{LK}^{=}$ is a reasonable proof calculus for first order logic with equality by the following

Theorem 2.9. *(soundness and completeness of* $\mathrm{LK}^{=}$*) Let* L *be a language. Then for all closed* L*-sequents* $\Gamma \longrightarrow \Delta$ *there holds:* $\mathrm{LK}^{=}(L)$ *derives* $\Gamma \longrightarrow \Delta$ *if and only if*

$$\bigwedge_{\varphi \in \Gamma} \varphi \supset \bigvee_{\psi \in \Delta} \psi$$

is valid in first order logic with equality.

Proof. It is straightforward to see that all rules in $\mathrm{LK}^{=}$ are sound.

For completeness we use the fact the the equality calculus LK_e in [6] is complete and note that it is straightforward to show that the equality axioms can be proven in $\mathrm{LK}^{=}$ using the equality rules in $\mathrm{LK}^{=}$. More precisely, let $n \in \mathbb{N}$, $t_1, \ldots, t_n, u_1, \ldots, u_n \in T(L)$, let $f \in L$ be an n-ary function symbol and let $R \in L \cup \{=\}$ be an n-ary relation symbol. It is straightforward to show the following in $\mathrm{LK}^{=}$:

$$\begin{aligned}
&\mathrm{LK}^{=} \vdash \longrightarrow t = t,\\
&\mathrm{LK}^{=} \vdash t_1 = u_1, \ldots, t_n = u_n \longrightarrow f(t_1, \ldots, t_n) = f(u_1, \ldots, u_n),\\
&\mathrm{LK}^{=} \vdash t_1 = u_1, \ldots, t_n = u_n, R(t_1, \ldots, t_n) \longrightarrow R(u_1, \ldots, u_n).
\end{aligned}$$

□

Definition 2.10. *Let* L *be a language. An* L-theory *is a set of closed* L*-formulas. For* $\Gamma \longrightarrow \Delta \in \mathrm{Seq}(L)$ *we write* $T \vdash \Gamma \longrightarrow \Delta$ *if* $\mathrm{LK}^{=} \vdash T_0, \Gamma \longrightarrow \Delta$ *for a finite set* $T_0 \subseteq T$. *For a formula* $\varphi \in F(L)$ *we write* $T \vdash \varphi$, *if* $T \vdash \longrightarrow \varphi$. *If* $T = \{\sigma_1, \ldots, \sigma_n\}$ *is finite we often omit the curly braces and write* $\sigma_1, \ldots, \sigma_n \vdash \Gamma \longrightarrow \Delta$ *or* $\sigma_1, \ldots, \sigma_n \vdash \varphi$. *Let* $\Phi \subseteq F(L)$. *The* deductive closure of T in Φ *is* $T^{\vdash}(\Phi) := \{\varphi \in \Phi \mid T \vdash \varphi\}$. *Further, the* deductive closure of T *is* $T^{\vdash} := T^{\vdash}(F(L))$. *We say* T is consistent *if* $T \nvdash \longrightarrow$. *Let* $\mathcal{M}$ *be an* L*-structure. For an* L*-term we write* $t^{\mathcal{M}}$ *for the interpretation of the term* t *in* $\mathcal{M}$. *For an* L*-formula* φ *we write* $\mathcal{M} \models \varphi$ *if* $\mathcal{M}$ *satisfies* φ. *The* theory of $\mathcal{M}$ *is* $\mathrm{Th}(\mathcal{M}) := \{\varphi \in F(L) \mid \varphi \text{ is closed and } \mathcal{M} \models \varphi\}$.

When showing statements of the form $T \vdash \varphi$ where T is a theory, it is often cumbersome and less readable to write out a $\mathrm{LK}^{=}$-proof explicitly. In those situations we will instead carry out the proof in ordinary mathematical reasoning, prefix it with the phrase "Work in T" and be cautious to only use the axioms given in T. Since $\mathrm{LK}^{=}(L)$ is complete by Theorem 2.9, an explicit $\mathrm{LK}^{=}(L)$-proof can be constructed.

Even in cases where we provide an explicit proof in a proof calculus it is often useful to shorten some straightforward inferences. To this end we introduce the following notation: Let I be a unary inference rule. We write

$$\frac{\pi}{S}\ I^*$$

to mean that from a proof π of we can construct a proof of S by repeated application of the inference rule I. For rules where there is a left and right variant say I_{left} and I_{right} we also just write

$$\frac{\pi}{S}\ I^*$$

to mean that from a proof π of we can construct a proof of S by repeated application of the inference rules I_{left} and I_{right}. We will mostly use this notation for the rules $\mathrm{w}_{\text{left}}, \mathrm{w}_{\text{right}}, \mathrm{c}_{\text{left}}$ and $\mathrm{c}_{\text{right}}$.

In a few cases we use the notation

$$\frac{\pi}{S}\ I, J$$

to denote that we first apply I to π and then J to the resulting proof.

In this thesis we will also use some standard definitions and results of proof theory:

Definition 2.11. *Let L be a language. A variable x is called* eigenvariable of an $\mathrm{LK}^{=}(L)$-proof π *if x is eigenvariable of an inference which is used by π. An $\mathrm{LK}^{=}(L)$-proof π is called* regular*, if all eigenvariables of π are pairwise different.*

Lemma 2.12. *Let L be a language and $\pi \vdash_{\mathrm{LK}^{=}(L)} S$. Then there exists a regular proof $\pi' \vdash_{\mathrm{LK}^{=}(L)} S$.*

Proof sketch. Rename the eigenvariables appropriately. □

Lemma 2.13. *Let L be a language $S(\bar{x}) \in \mathrm{Seq}(L)$ and $\bar{t} \in T(L)$. If $\mathrm{LK}^{=}(L) \vdash S(\bar{x})$, then $\mathrm{LK}^{=}(L) \vdash S(\bar{t})$.*

Proof sketch. Let $\pi(\bar{x}) \vdash_{\mathrm{LK}^{=}(L)} S(\bar{x})$. Without loss of generality $\bar{t}$ does not contain an eigenvariable of π and no variable in $\bar{x}$ is an eigenvariable of π (otherwise rename eigenvariables in π accordingly). Replacing $\bar{x}$ by $\bar{t}$ in all sequents of π yields a proof $\pi(\bar{t}) \vdash_{\mathrm{LK}^{=}(L)} S(\bar{t})$. □

Theorem 2.14 (cut elimination)**.** *Let L be a language. If $\mathrm{LK}^{=}(L) \vdash \Gamma \longrightarrow \Delta$, then there exists an $\mathrm{LK}^{=}(L)$-proof π of $\Gamma \longrightarrow \Delta$ where all cuts are atomic.*

Proof. See [6]. □

An important corollary of the cut elimination theorem is the subformula property. For $\mathrm{LK}^{=}$ we will use the following form:

Theorem 2.15 (subformula property)**.** *Let L be a language and let $s \in \{\neg, \wedge, \vee, \supset, \forall, \exists\}$, $S \in \mathrm{Seq}(L)$ and $\pi \vdash_{\mathrm{LK}^{=}(L)} S$ where all cuts are atomic. If π uses the inference rule s_{left} or s_{right}, then S contains s.*

Proof sketch. Since s can only occur in non-atomic formulas and all cuts are atomic, there is no inference rule where s is in the upper sequent, but not in the lower sequent. Thus, the statement can be shown by a straightforward induction on π. □

2.2 Arithmetical theories

Definition 2.16. *We define the language $S_{\mathsf{p}} := \{0, \mathsf{s}, \mathsf{p}, +, \cdot\}$ where 0 is a constant symbol, s, p are unary function symbols and $+$, $\cdot$ are binary function symbols. Furthermore we set $S := S_{\mathsf{p}} \setminus \{\mathsf{p}\}$.*

Definition 2.17 (theory A)**.** *Consider the formulas*

$$\forall x \;\; \mathsf{s}(x) \neq 0, \tag{A_1}$$
$$\mathsf{p}(0) = 0, \tag{A_2}$$
$$\forall x \;\; \mathsf{p}(\mathsf{s}(x)) = x, \tag{A_3}$$
$$\forall x \;\; x + 0 = x, \tag{A_4}$$
$$\forall x \, \forall y \;\; x + \mathsf{s}(y) = \mathsf{s}(x + y), \tag{A_5}$$
$$\forall x \;\; x \cdot 0 = 0, \tag{A_6}$$
$$\forall x \, \forall y \;\; x \cdot \mathsf{s}(y) = x \cdot y + x. \tag{A_7}$$

We define $A := \{A_1, \ldots, A_7\}$.

Definition 2.18 (induction axiom)**.** *Let L be a language with $L \supset S$. Let $\varphi(x, \bar{z}) \in F(L)$. Then the* induction axiom for φ with respect to x *is the formula*

$$I_x(\varphi) :\equiv \forall \bar{z} \; (\varphi(0, \bar{z}) \supset \forall x \, (\varphi(x, \bar{z}) \supset \varphi(\mathsf{s}(x), \bar{z})) \supset \forall x \, \varphi(x, \bar{z})) \, .$$

For $F \subseteq F(L)$ we define $I(F) := \{I_x(\varphi) \,|\, \varphi \in F, \; x \text{ is a variable}\}$.

In this thesis, by $\mathrm{IOpen}_{\mathsf{p}}$, we refer to the theory of open induction in the language S_{p}. Consequently we define:

Definition 2.19 ($\mathrm{IOpen}_{\mathsf{p}}$)**.** *We define* $\mathrm{IOpen}_{\mathsf{p}} := A \cup I(F_{\mathrm{qf}}(S_{\mathsf{p}}))$.

Notation 2.20. *Let $t \in T(S_{\mathsf{p}})$ and $n \in \mathbb{N}$. We inductively define the term $nt \in T(S_{\mathsf{p}})$ by $0t :\equiv 0$ and $(n+1)t :\equiv t + nt$.*

$\mathrm{IOpen}_{\mathsf{p}}$ has a characterization due to Shepherdson (see [5]):

Theorem 2.21. *Over the theory A the set of formulas $I(F_{\mathrm{qf}}(S_{\mathsf{p}}))$ is equivalent to the formulas*

$$\forall x \ (x = 0 \vee x = \mathsf{s}(\mathsf{p}(x))), \tag{B_1}$$
$$\forall x \forall y \ \ x + y = y + x, \tag{B_2}$$
$$\forall x \forall y \forall z \ \ (x + y) + z = x + (y + z), \tag{B_3}$$
$$\forall x \forall y \forall z \ \ (x + y = x + z \supset y = z), \tag{B_4}$$
$$\forall x \forall y \ \ x \cdot y = y \cdot x, \tag{B_5}$$
$$\forall x \forall y \forall z \ \ x \cdot (y \cdot z) = (x \cdot y) \cdot z, \tag{B_6}$$
$$\forall x \forall y \forall z \ \ x \cdot (y + z) = x \cdot y + x \cdot z \tag{B_7}$$

and

$$\forall x \forall y \forall z \left(mx = my \supset \bigvee_{i=0}^{m-1} (z + i) \cdot x = (z + i) \cdot y \right), \quad \text{for } m \geq 2. \tag{C'_m}$$

This allows us to consider variations of $\mathrm{IOpen}_{\mathsf{p}}$:

Definition 2.22. *We define $AB := A \cup \{B_1, \ldots, B_7\}$. Further, consider the formulas:*

$$\forall x \forall y \, (mx = my \supset x = y) \quad \text{for } m \geq 2. \tag{C_m}$$

Then we define $ABC_m := AB \cup \{C_m \mid m \geq 2\}$.

Remark 2.23. *It is straightforward to show $ABC_m \vdash C'_m$ for $m \geq 2$. Thus we have $AB^{\vdash} \subseteq \mathrm{IOpen}_{\mathsf{p}}{}^{\vdash} \subseteq ABC_m{}^{\vdash}$.*

Let $L \supseteq S$ be a language and let T be an L-theory. The *Diophantine satisfiability problem for T* is the question whether the set

$$\mathrm{D}_T := \{(t(\bar{x}), u(\bar{x})) \in T(S) \times T(S) \mid T \cup \{\exists \bar{x} \, t(\bar{x}) = u(\bar{x})\} \text{ is consistent}\}$$

is decidable. Two results in this area are that D_Q is decidable where Q is the Robinson arithmetic (see [3]) and $\mathrm{D}_{\mathrm{Th}(\mathbb{N})}$ is undecidable as a consequence of the MRDP theorem. The decidability of $\mathrm{D}_{\mathrm{IOpen}}$ is a long-standing open problem (see [4]). In this thesis we show that D_{AB} is decidable as a consequence of the decidability of $AB^{\vdash}(N(S))$.

3 The main result

Our goal in this thesis is to show

Theorem 3.1. *$AB^{\vdash}(N(S))$ is decidable.*

In the remainder of this short chapter we briefly outline our proof strategy: We will first introduce a specialized proof calculus $\mathcal{P}_T$, show its soundness and completeness with respect to $AB^{\vdash}(N(S))$ and then prove its decidability.

3.1 Calculus $\mathcal{P}_T$

Our calculus is based on the observation that the axioms in AB without A_1, A_2, A_3 and B_1 allow us to more or less work with terms as with polynomials. We will expand on this observation later, but now introduce a notion of equivalence to factor out this polynomial part and present a simple calculus based only on A_1 and B_1.

Definition 3.2. *Let L be a language and Γ a multiset of L-formulas. We define the relation $\Leftrightarrow_\Gamma^{\mathrm{at}}$ on $A(L)$ by*

$$\varphi \Leftrightarrow_\Gamma^{\mathrm{at}} \psi :\iff \mathrm{LK}^{=} \vdash \Gamma, \varphi \longrightarrow \psi \text{ and } \mathrm{LK}^{=} \vdash \Gamma, \psi \longrightarrow \varphi.$$

We extend $\Leftrightarrow_\Gamma^{\mathrm{at}}$ to $\mathrm{Lit}(L)$ by setting

$$\Leftrightarrow_\Gamma := \Leftrightarrow_\Gamma^{\mathrm{at}} \cup \left\{ (\neg\varphi, \neg\psi) \,|\, \varphi, \psi \in A(L) \text{ and } \varphi \Leftrightarrow_\Gamma^{\mathrm{at}} \psi \right\}.$$

Lemma 3.3. *$\Leftrightarrow_\Gamma$ is a congruence relation with respect to $^{\perp}$.*

Proof. (i) Reflexivity: If $\varphi \in A(L)$, then $\varphi \Leftrightarrow_\Gamma^{\mathrm{at}} \varphi$ and thus $\varphi \Leftrightarrow_\Gamma \varphi$ by

$$\frac{}{\varphi \longrightarrow \varphi}\ \text{axiom.}$$

If $\varphi \in N(L)$, then $\varphi^{\perp} \Leftrightarrow_\Gamma^{\mathrm{at}} \varphi^{\perp}$ by what has been just shown. Thus $\varphi \Leftrightarrow_\Gamma \varphi$.

(ii) Symmetry: Follows immediately from the definition.

(iii) Transitivity: Let $\varphi, \psi, \chi \in \mathrm{Lit}(L)$ with $\varphi \Leftrightarrow_\Gamma \psi$ and $\psi \Leftrightarrow_\Gamma \chi$. By the definition of $\Leftrightarrow_\Gamma$ we have either $\varphi, \psi, \chi \in A(L)$ or $\varphi, \psi, \chi \in N(L)$. In the first case we have proofs $\pi_1 \vdash_{\mathrm{LK}=} \Gamma, \varphi \longrightarrow \psi$ and $\pi_2 \vdash_{\mathrm{LK}=} \Gamma, \psi \longrightarrow \chi$. Now $\Gamma \vdash \varphi \longrightarrow \chi$ by

$$\dfrac{\dfrac{\begin{matrix}(\pi_1)\\ \Gamma, \varphi \longrightarrow \psi\end{matrix} \quad \begin{matrix}(\pi_2)\\ \Gamma, \psi \longrightarrow \chi\end{matrix}}{\Gamma, \Gamma, \varphi \longrightarrow \chi}\ \mathrm{cut}}{\Gamma, \varphi \longrightarrow \chi}\ \mathrm{c}^{*}_{\mathrm{left}}\ .$$

$\Gamma \vdash \chi \longrightarrow \varphi$ follows similarly.

If $\varphi, \psi, \chi \in N(L)$, then the statement follows by what has just been shown and the definition of $\Leftrightarrow_\Gamma$.

(iv) Congruence: By the definition of $\Leftrightarrow_\Gamma$ we have $\varphi \Leftrightarrow_\Gamma \psi$ if and only if $\varphi^\perp \Leftrightarrow_\Gamma \psi^\perp$.

□

Definition 3.4. *For $\varphi \in \mathrm{Lit}(L)$ we denote its equivalence class with respect to $\Leftrightarrow_\Gamma$ by $[\varphi]_\Gamma$. For a multiset $\Phi \subseteq \mathrm{Lit}(L)$ we set $[\Phi]_\Gamma := \{[\varphi]_\Gamma \mid \varphi \in \Phi\}$, i.e. the multiset of equivalence classes of literals in Φ.*

The following shows that substitution is well-defined for equivalence classes:

Lemma 3.5. *Let L be a language, Γ a multiset of L-formulas, $\varphi(\bar{x}), \psi(\bar{x}) \in \mathrm{Lit}(L)$ with $\varphi(\bar{x}) \Leftrightarrow_\Gamma \psi(\bar{x})$ and $\bar{t} \in T(L)$. Then $\varphi(\bar{t}) \Leftrightarrow_\Gamma \psi(\bar{t})$.*

Proof. Follows from Lemma 2.13. □

Definition 3.6. *Let $T := AB \setminus \{A_1, A_2, A_3, B_1\}$. The calculus $\mathcal{P}_T$ acts on $[N(S)]_T$ and has the inference rules*

$$\frac{}{[\mathsf{s}(t) \neq 0]_T}\, A_1^{\mathrm{ax}} \qquad \text{and} \qquad \frac{[\varphi(0)]_T \quad [\varphi(\mathsf{s}(x))]_T}{[\varphi(x)]_T}\, B_1^{\mathrm{var}}$$

where $t \in T(S)$, $\varphi \in N(S)$ and x is a variable.

Remark 3.7. *Note that the theory T implies the laws of a commutative semiring. By B_4 and congruence of $+$ we have that $T \vdash \forall x \forall y \forall z \;\; x + y = x + z \leftrightarrow y = z$.*

Example 3.8. *Let $\varphi(x) :\equiv x \cdot x \neq x + \mathsf{s}(0)$. We show $\mathcal{P}_T \vdash [\varphi(x)]_T$. It is straightforward to show $\varphi(0) \Leftrightarrow_T \mathsf{s}(0) \neq 0$ and $\varphi(\mathsf{s}(x)) \Leftrightarrow_T x \cdot x + x \neq \mathsf{s}(0)$. Furthermore, we have $\varphi(\mathsf{s}(0)) \Leftrightarrow_T \mathsf{s}(0) \neq 0$ and $\varphi(\mathsf{s}(\mathsf{s}(x))) \Leftrightarrow_T \mathsf{s}(x \cdot x + x + x + x) \neq 0$. Thus we get a $\mathcal{P}_T$-proof of $[\varphi(x)]_T$ by*

$$\dfrac{\dfrac{}{[\mathsf{s}(0) \neq 0]_T}\, A_1^{\mathrm{ax}} \quad \dfrac{\dfrac{}{[\mathsf{s}(0) \neq 0]_T}\, A_1^{\mathrm{ax}} \quad \dfrac{}{[\mathsf{s}(x \cdot x + x + x + x) \neq 0]_T}\, A_1^{\mathrm{ax}}}{[x \cdot x + x \neq \mathsf{s}(0)]_T}\, B_1^{\mathrm{var}}}{[\varphi(x)]_T}\, B_1^{\mathrm{var}}.$$

We reduce our main result to the following three results:

Theorem 3.9 (soundness of $\mathcal{P}_T$)**.** *Let $\varphi \in N(S)$. If $\mathcal{P}_T \vdash [\varphi]_T$, then $AB \vdash \varphi$.*

Theorem 3.10 (completeness of $\mathcal{P}_T$)**.** *Let $\varphi \in N(S)$. If $AB \vdash \varphi$, then $\mathcal{P}_T \vdash [\varphi]_T$.*

Theorem 3.11 (decidability of $\mathcal{P}_T$)**.** *The set $\mathcal{P}_T{}^{\vdash} := \{\varphi \in N(S) \mid \mathcal{P}_T \vdash [\varphi]_T\}$ is decidable.*

Now the main result follows by

Proof of Theorem 3.1. By soundness (Theorem 3.9) and completeness (Theorem 3.10) we have that $AB \vdash \varphi$ if and only if $\mathcal{P}_T \vdash [\varphi]_T$. Thus $AB^{\vdash}(N(S))$ is decidable by the decidability of $\mathcal{P}_T$ (Theorem 3.11). □

A straightforward corollary of Theorem 3.1 is

Corollary 3.12. D_{AB} *is decidable.*

Proof. By Theorem 3.1 we get that $AB^{\vdash}(N(S))$ is decidable. Now the statement follows from

$$\begin{aligned}\mathrm{D}_{AB} &= \{\varphi(\bar{x}) \in A(S) \mid AB \cup \{\exists \bar{x}\, \varphi(\bar{x})\} \not\vdash \longrightarrow\}\\ &= \{\varphi(\bar{x}) \in A(S) \mid AB \not\vdash \exists \bar{x}\, \varphi(\bar{x}) \longrightarrow\}\\ &= \{\varphi(\bar{x}) \in A(S) \mid AB \not\vdash \varphi(\bar{x}) \longrightarrow\}\\ &= \{\varphi(\bar{x}) \in A(S) \mid AB \not\vdash \neg\varphi(\bar{x})\}\\ &= \{\psi(\bar{x}) \in N(S) \mid AB \not\vdash \psi(\bar{x})\}\\ &= N(S) \setminus AB^{\vdash}(N(S)).\end{aligned}$$

□

We show Theorem 3.9 in the next section. The following two chapters are dedicated to proving theorems 3.10 and 3.11 respectively.

3.2 Soundness of $\mathcal{P}_T$

We show soundness of $\mathcal{P}_T$ by transforming proofs in $\mathcal{P}_T$ into $\mathrm{LK}^{=}$-proofs. For this we use

Lemma 3.13. *Let* $\varphi(x) \in N(S_{\mathsf{p}})$ *and* $t \in T(S_{\mathsf{p}})$. *Then*

$$\{B_1\} \vdash \varphi(\mathsf{0}), \forall x\, \varphi(\mathsf{s}(x)) \longrightarrow \varphi(t).$$

Proof. Work in $\{B_1\}$: By B_1 we have $t = \mathsf{0} \vee t = \mathsf{s}(\mathsf{p}(t))$. In the first case we can use $\varphi(\mathsf{0})$ to prove $\varphi(t)$. In the other case we use $\forall x\, \varphi(\mathsf{s}(x))$ for $x = \mathsf{p}(t)$. □

Proof of Theorem 3.9. Let $\pi \vdash_{\mathcal{P}_T} [\varphi]_T$. Since $\varphi \in N(S)$ we have $\varphi^{\perp} \in A(S)$. We proceed by induction on π. If $\pi =$

$$\frac{}{[\varphi]_T}\, A_1^{\mathrm{ax}},$$

then, $\varphi \Leftrightarrow_T \mathsf{s}(t) \neq \mathsf{0}$ for some $t \in T(S)$. Since $\Leftrightarrow_T$ is congruent we have $\varphi^{\perp} \Leftrightarrow_T \mathsf{s}(t) = \mathsf{0}$. Therefore we have a proof $\pi' \vdash_{\mathrm{LK}^{=}} T, \varphi^{\perp} \longrightarrow \mathsf{s}(t) = \mathsf{0}$. Now $\mathrm{LK}^{=} \vdash AB \longrightarrow \varphi$ by

$$\dfrac{\dfrac{\dfrac{(\pi')}{T, \varphi^{\perp} \longrightarrow \mathsf{s}(t) = \mathsf{0}} \quad \dfrac{\dfrac{\dfrac{}{\mathsf{s}(t) = \mathsf{0} \longrightarrow \mathsf{s}(t) = \mathsf{0}}\,\text{axiom}}{\mathsf{s}(t) \neq \mathsf{0}, \mathsf{s}(t) = \mathsf{0} \longrightarrow}\,\neg_{\text{left}}}{A_1, \mathsf{s}(t) = \mathsf{0} \longrightarrow}\,\forall_{\text{left}}}{T, A_1, \varphi^{\perp} \longrightarrow}\,\text{cut}}{AB, \varphi^{\perp} \longrightarrow}\,\mathrm{w}_{\text{left}}}{AB \longrightarrow \varphi}\,\neg_{\text{right}}.$$

If $\pi =$

$$\frac{\begin{matrix}(\pi_0) & (\pi_{\mathsf{s}})\\ [\varphi_0]_T & [\varphi_{\mathsf{s}}]_T\end{matrix}}{[\varphi]_T}\, B_1^{\mathrm{var}},$$

then there is a variable x such that for $\varphi = \varphi(x)$ we have $\varphi_0 \Leftrightarrow_T \varphi(0)$ as well as $\varphi_{\mathsf{s}} \Leftrightarrow_T \varphi(\mathsf{s}(x))$. Using the induction hypothesis we have proofs $\pi_{\varphi(0)} \vdash_{\mathrm{LK}=} AB \longrightarrow \varphi(0)$ and $\pi_{\varphi(\mathsf{s}(x))} \vdash_{\mathrm{LK}=} AB \longrightarrow \varphi(\mathsf{s}(x))$. By applying Lemma 3.13 we get a proof

$$\pi' \vdash_{\mathrm{LK}=} B_1, \varphi(0), \forall x\, \varphi(\mathsf{s}(x)) \longrightarrow \varphi.$$

Now we have $\mathrm{LK}^{=} \vdash AB \longrightarrow \varphi$ by

$$\dfrac{\dfrac{\dfrac{(\pi_{\varphi(\mathsf{s}(x))})}{AB \longrightarrow \varphi(\mathsf{s}(x))}}{AB \longrightarrow \forall x\, \varphi(\mathsf{s}(x))}\,\forall_{\mathrm{right}} \quad \dfrac{\dfrac{(\pi_{\varphi(0)})}{AB \longrightarrow \varphi(0)} \quad \dfrac{(\pi')}{B_1, \varphi(0), \forall x\, \varphi(\mathsf{s}(x)) \longrightarrow \varphi}}{AB, B_1, \forall x\, \varphi(\mathsf{s}(x)) \longrightarrow \varphi}\,\mathrm{cut}}{\dfrac{AB, AB, B_1 \longrightarrow \varphi}{AB \longrightarrow \varphi}\,\mathrm{c}^{*}_{\mathrm{left}}}\,\mathrm{cut}.$$

□

4 Completeness

Our goal for this chapter is to show completeness of $\mathcal{P}_T$ with respect to provability of negated equations in AB, i.e. for $\varphi \in N(S)$ with $AB \vdash \varphi$ there holds $\mathcal{P}_T \vdash [\varphi]_T$.

First we observe that we can remove the predecessor axioms A_2 and A_3 by using a "deskolemized" version of B_1:

Definition 4.1. *We define* $B_1^\exists :\equiv \forall x\,(x = 0 \vee \exists y\, x = \mathsf{s}(y))$ *and*

$$AB^\exists := (AB \setminus \{A_2, A_3, B_1\}) \cup \left\{B_1^\exists\right\}.$$

$AB^\exists$ proves that s is injective:

Lemma 4.2. $A_4, A_5, B_2, B_4 \vdash \forall x\, \forall y\, (\mathsf{s}(x) = \mathsf{s}(y) \supset x = y)$

Proof. Work in $AB^\exists$:

$$\begin{aligned} \mathsf{s}(x) = \mathsf{s}(y) &\overset{A_4}{\Longrightarrow} \mathsf{s}(x + 0) = \mathsf{s}(y + 0) \\ &\overset{A_5}{\Longrightarrow} x + \mathsf{s}(0) = y + \mathsf{s}(0) \\ &\overset{B_2}{\Longrightarrow} \mathsf{s}(0) + x = \mathsf{s}(0) + y \\ &\overset{B_4}{\Longrightarrow} x = y. \end{aligned}$$

□

Lemma 4.3. *Let* $\varphi \in F(S)$. *If* $AB \vdash \varphi$, *then* $AB^\exists \vdash \varphi$.

Proof. We show this statement by contraposition. If $AB^\exists \nvdash \varphi$, then there is a model $\mathcal{M} = (M, 0^\mathcal{M}, \mathsf{s}^\mathcal{M}, +^\mathcal{M}, \cdot^\mathcal{M})$ of $AB^\exists$ such that $\mathcal{M} \not\models \varphi$. We now construct a model $\mathcal{M}_\mathsf{p}$ of AB such that $\mathcal{M}_\mathsf{p} \not\models \varphi$. We set $\mathcal{M}_\mathsf{p} = (M, 0^\mathcal{M}, \mathsf{s}^\mathcal{M}, +^\mathcal{M}, \cdot^\mathcal{M}, \mathsf{p}^{\mathcal{M}_\mathsf{p}})$ where $\mathsf{p}^{\mathcal{M}_\mathsf{p}} : M \to M$ is defined as

$$\mathsf{p}^{\mathcal{M}_\mathsf{p}}(a) = \begin{cases} 0^\mathcal{M} & \text{if } a = 0^\mathcal{M} \\ b & \text{if } a = \mathsf{s}^\mathcal{M}(b) \text{ for some } b \in M. \end{cases}$$

Note that this is well-defined: Since $\mathcal{M} \models A_1$, the two cases are distinct. Because $\mathcal{M} \models B_1^\exists$ we have that for all $a \in M$ that either $a = 0^\mathcal{M}$ or there is a $b \in M$ such that $a = \mathsf{s}^\mathcal{M}(b)$. Furthermore, by Lemma 4.2 we have that there is at most one such b.

By construction we have that $\mathcal{M}_\mathsf{p} \models AB \setminus \{A_2, A_3, B_1\}$. It remains to show $\mathcal{M}_\mathsf{p} \models A_2$, $\mathcal{M}_\mathsf{p} \models A_3$, $\mathcal{M}_\mathsf{p} \models B_1$ and $\mathcal{M}_\mathsf{p} \not\models \varphi$. Clearly, by definition of $\mathsf{p}^{\mathcal{M}_\mathsf{p}}$ we have $\mathsf{p}^{\mathcal{M}_\mathsf{p}}(0^\mathcal{M}) = 0^\mathcal{M}$, therefore $\mathcal{M}_\mathsf{p} \models A_2$. Now let $b \in M$, then we also have $\mathsf{p}^{\mathcal{M}_\mathsf{p}}(\mathsf{s}^\mathcal{M}(b)) = b$ by definition, therefore $\mathcal{M}_\mathsf{p} \models A_3$. Also, if $b \neq 0^\mathcal{M}$, then there is a $c \in M$ such that $b = \mathsf{s}^\mathcal{M}(c)$ since $\mathcal{M} \models B_1^\exists$. Then $\mathsf{s}^\mathcal{M}(\mathsf{p}^{\mathcal{M}_\mathsf{p}}(b)) = \mathsf{s}^\mathcal{M}(c) = b$. Therefore $\mathcal{M}_\mathsf{p} \models B_1$. Since φ is a formula without predecessors and $\mathcal{M}_\mathsf{p}$ has the same interpretation as $\mathcal{M}$ on formulas without predecessors, we get that $\mathcal{M}_\mathsf{p} \not\models \varphi$. □

Also note the following reduction:

Lemma 4.4. *Let $\varphi \in A(S)$. If $AB^{\exists} \vdash \neg\varphi$, then $AB^{\exists} \vdash \varphi \longrightarrow$.*

Proof. Let $\pi \vdash_{\mathrm{LK}^{=}} AB^{\exists} \longrightarrow \neg\varphi$. Then we have $AB^{\exists} \vdash \varphi \longrightarrow$ by

$$\dfrac{\dfrac{(\pi)}{AB^{\exists} \longrightarrow \neg\varphi} \qquad \dfrac{\dfrac{}{\varphi \longrightarrow \varphi}\,\text{axiom}}{\neg\varphi, \varphi \longrightarrow}\,\neg_{\text{left}}}{AB^{\exists}, \varphi \longrightarrow}\,\text{cut}.$$

□

Thus it suffices to transform $\mathrm{LK}^{=}$-proofs of $AB^{\exists}, \varphi \longrightarrow$ into $\mathcal{P}_T$-proofs of $[\neg\varphi]_T$. We do this in a series of steps and introduce intermediate proof calculi where the axioms of $AB^{\exists}$ are replaced by rules in the calculus: We then extend $\mathrm{LK}^{=}$ with rules that resemble A_1^{ax} and B_1^{var} of $\mathcal{P}_T$ to get a calculus called $\mathrm{LK}\mathcal{P}_T^{=}$. This allows us to get rid of the axioms A_1 and B_1. Next, we get rid of quantifier and propositional rules as well as the remaining theory T in a calculus called $\mathcal{P}_T^{=}$. We then introduce a notion of normality for $\mathcal{P}_T^{=}$-proofs which will allow us to get rid of equational and structural rules to only be left with rules from $\mathcal{P}_T$.

4.1 From $\mathrm{LK}^{=}$ to $\mathrm{LK}\mathcal{P}_T^{=}$

We extend $\mathrm{LK}^{=}$ by two inference rules which resemble the inference rules of $\mathcal{P}_T$:

Definition 4.5. *The inference rules A_1^{ax} and B_1^{var} are given by*

$$\dfrac{}{\mathsf{s}(t) = 0 \longrightarrow}\,A_1^{\mathrm{ax}} \qquad \text{and} \qquad \dfrac{x = 0, \Gamma_1 \longrightarrow \Delta_1 \qquad x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\,B_1^{\mathrm{var}}$$

where $t \in T(S)$, $x \neq y \in V$ and $y \notin \mathrm{FV}(\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2)$, i.e. B_1^{var} has an eigenvariable condition. Furthermore we set $\mathrm{LK}\mathcal{P}_T^{=}$ to be the proof calculus $\mathrm{LK}^{=} + A_1^{\mathrm{ax}} + B_1^{\mathrm{var}}$.

The goal for this section is to prove a completeness result for $\mathrm{LK}\mathcal{P}_T^{=}$:

Proposition 4.6. *Let $\varphi \in A(S)$. If $AB \vdash \neg\varphi$, then $\mathrm{LK}\mathcal{P}_T^{=} \vdash T, \varphi \longrightarrow$.*

In particular we want to get rid of A_1 and B_1 in the theory and instead use the rules A_1^{ax} and B_1^{var}. To do this for A_1^{ax} is straightforward, but to do this for B_1^{var} we need some groundwork. To simplify the following proofs, we introduce a notation for instantiating universal quantifiers in a formula:

Definition 4.7. *Let L be a language, $\varphi \in F(L)$ and $t \in T(L)$. We define*

$$\varphi[t] := \begin{cases} \psi(t) & \text{if } \varphi \equiv \forall x\, \psi(x) \text{ for some } \psi(x) \in F(L), \\ \varphi & \text{otherwise.} \end{cases}$$

We call every formula of the form $\varphi[t]$ a partial instance of φ.

A first important observation is that, even though B_1^{var} only does a case distinction on variables, this is enough to prove $B_1^{\exists}[t]$ from axioms in T for an arbitrary term $t \in T(S)$. To show this we need some closure properties of provability of partial instances of $B_1^{\exists}$:

Lemma 4.8. *For $x \in V$ and $t, u \in T(S)$ we have:*

(i) $\mathrm{LK}^{=} + B_1^{\mathrm{var}} \vdash \longrightarrow B_1^{\exists}[x]$,

(ii) $\mathrm{LK}^{=} \vdash \longrightarrow B_1^{\exists}[\mathsf{0}]$,

(iii) $\mathrm{LK}^{=} \vdash \longrightarrow B_1^{\exists}[\mathsf{s}(t)]$,

(iv) $\mathrm{LK}^{=} \vdash A_4, A_5, B_1^{\exists}[t], B_1^{\exists}[u] \longrightarrow B_1^{\exists}[t+u]$,

(v) $\mathrm{LK}^{=} \vdash A_5, A_6, A_7, B_5, B_1^{\exists}[t], B_1^{\exists}[u] \longrightarrow B_1^{\exists}[t \cdot u]$.

Proof. (i) It is straightforward to find proofs $\pi_1 \vdash_{\mathrm{LK}^{=}} x = \mathsf{0} \longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y)$ and $\pi_2 \vdash_{\mathrm{LK}^{=}} x = \mathsf{s}(y) \longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y)$. Thus the statement is given by

$$\dfrac{\dfrac{(\pi_1) \qquad\qquad (\pi_2)}{x = \mathsf{0} \longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y) \quad x = \mathsf{s}(y) \longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y)}\, B_1^{\mathrm{var}}}{\dfrac{\longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y), x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y)}{\longrightarrow x = \mathsf{0} \vee \exists y\, x = \mathsf{s}(y)}\, \mathrm{c}_{\mathrm{right}}}.$$

(ii) By

$$\dfrac{\dfrac{\dfrac{}{\longrightarrow \mathsf{0} = \mathsf{0}}\,\mathrm{refl}}{\longrightarrow \mathsf{0} = \mathsf{0}, \exists y\, \mathsf{0} = \mathsf{s}(y)}\,\mathrm{w}_{\mathrm{right}}}{\longrightarrow \mathsf{0} = \mathsf{0} \vee \exists y\, \mathsf{0} = \mathsf{s}(y)}\,\vee_{\mathrm{right}}.$$

(iii) By

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\longrightarrow \mathsf{s}(t) = \mathsf{s}(t)}\,\mathrm{refl}}{\longrightarrow \exists y\, \mathsf{s}(t) = \mathsf{s}(y)}\,\exists_{\mathrm{right}}}{\longrightarrow \mathsf{s}(t) = \mathsf{0}, \exists y\, \mathsf{s}(t) = \mathsf{s}(y)}\,\mathrm{w}_{\mathrm{right}}}{\longrightarrow \mathsf{s}(t) = \mathsf{0} \vee \exists y\, \mathsf{s}(t) = \mathsf{s}(y)}\,\vee_{\mathrm{right}}.$$

(iv) Work in $\{A_4, A_5, B_1^{\exists}[t], B_1^{\exists}[u]\}$: We do a case distinction on $B_1^{\exists}[u]$. If $u = \mathsf{0}$, then by A_4 we have $t + u = t$. Thus, the conclusion follows from $B_1^{\exists}[t]$. If $u = \mathsf{s}(y)$ for some y, then $t + u = \mathsf{s}(t + y)$ by A_5. Thus, the conclusion follows from (iii).

(v) Work in $\{A_5, A_6, A_7, B_5, B_1^{\exists}[t], B_1^{\exists}[u]\}$: We do a case distinction on $B_1^{\exists}[u]$. If $u = \mathsf{0}$, then by A_6 we have $t \cdot u = \mathsf{0}$ and the conclusion follows from (ii). If $u = \mathsf{s}(x)$ for some x, we do a case distinction on $B_1^{\exists}[t]$. If $t = \mathsf{0}$, then by B_5 we have $t \cdot u = u \cdot \mathsf{0}$ and by A_6 we get $t \cdot u = \mathsf{0}$. Thus, the conclusion follows from (ii). Now let $t = \mathsf{s}(y)$ for some y. We have $t \cdot u = t \cdot x + t$ by A_7 since $u = \mathsf{s}(x)$. By A_5 we have $t \cdot u = \mathsf{s}(t \cdot x + y)$. Thus, the conclusion follows from (iii).

□

Lemma 4.9. *Let $t \in T(S)$. Then* $\mathrm{LK}^{=} + B_1^{\mathrm{var}} \vdash A \setminus \{A_1, A_2, A_3\}, B_5 \longrightarrow B_1^{\exists}[t]$.

Proof. We proceed by induction on t. The case $t \in V$ follows from Proposition 4.8 (i). The case $t \equiv \mathsf{0}$ follows from Proposition 4.8 (ii). The case $t \equiv \mathsf{s}(u)$ for some $u \in T(S)$ follows from Proposition 4.8 (iii).

If $t \equiv u + v$ for some $u, v \in T(S)$, then by induction hypothesis, there are proofs

$$\pi_u \vdash_{\mathrm{LK}^{=}+B_1^{\mathrm{var}}} A \setminus \{A_1\} \longrightarrow B_1^{\exists}[u]$$
$$\pi_v \vdash_{\mathrm{LK}^{=}+B_1^{\mathrm{var}}} A \setminus \{A_1\} \longrightarrow B_1^{\exists}[v].$$

By Proposition 4.8 (iv), there is a proof

$$\pi_{u+v} \vdash_{\mathrm{LK}^{=}} A_4, A_5, B_1^{\exists}[u], B_1^{\exists}[v] \longrightarrow B_1^{\exists}[u+v].$$

Now the statement is follows from

$$\dfrac{\pi_v \qquad \dfrac{\pi_u \qquad \pi_{u+v}}{A \setminus \{A_1\}, A_4, A_5, B_1^{\exists}[v] \longrightarrow B_1^{\exists}[u+v]}\,\mathrm{cut}}{\dfrac{A \setminus \{A_1\}, A \setminus \{A_1\}, A_4, A_5 \longrightarrow B_1^{\exists}[u+v]}{A \setminus \{A_1\} \longrightarrow B_1^{\exists}[u+v]}\,\mathrm{c}^{*}_{\mathrm{left}}}\,\mathrm{cut}.$$

If $t \equiv u \cdot v$ for some $u, v \in T(S)$, then the proof is analogous to the previous case but we use Proposition 4.8 (v) instead of Proposition 4.8 (iv). □

Now we can replace A_1 and $B_1^{\exists}$ by the rules A_1^{ax} and B_1^{var}:

Lemma 4.10. *If* $\mathrm{LK}\mathcal{P}_T^{=} \vdash \Pi, \Gamma \longrightarrow \Delta$, *where* Π *is a multiset with* $\mathrm{supp}(\Pi) \subseteq \{B_1^{\exists}, A_1\}$, *then* $\mathrm{LK}\mathcal{P}_T^{=} \vdash A \setminus \{A_1, A_2, A_3\}, B_5, \Gamma \longrightarrow \Delta$.

Proof. For this proof we set $A' := A \setminus \{A_1, A_2, A_3\}$. Let $\pi \vdash_{\mathrm{LK}\mathcal{P}_T^{=}} \Pi, \Gamma \longrightarrow \Delta$. We show the statement by induction on π. We first consider the cases where A_1 is introduced as an element of Π:

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ \Pi', \Gamma \longrightarrow \Delta\end{matrix}}{\underbrace{A_1, \Pi'}_{=\Pi}, \Gamma \longrightarrow \Delta}\,\mathrm{w}_{\mathrm{left}},$$

then apply the induction hypothesis to π_1 to get the desired proof.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ A_1, A_1, \Pi', \Gamma \longrightarrow \Delta\end{matrix}}{\underbrace{A_1, \Pi'}_{=\Pi}, \Gamma \longrightarrow \Delta}\,\mathrm{c}_{\mathrm{left}},$$

then again apply the induction hypothesis to π_1 to get the desired proof.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ \mathsf{s}(t) \neq \mathsf{0}, \Pi', \Gamma \longrightarrow \Delta\end{matrix}}{\underbrace{A_1, \Pi'}_{=\Pi}, \Gamma \longrightarrow \Delta}\,\forall_{\mathrm{left}},$$

then apply the induction hypothesis to π_1 to get a proof

$$\pi_1' \vdash_{\mathrm{LK}^{=}+\mathcal{P}_T} \mathsf{s}(t) \neq \mathsf{0}, A', B_5, \Gamma \longrightarrow \Delta.$$

Now the statement follows by

$$\dfrac{\dfrac{\dfrac{}{\mathsf{s}(t) = \mathsf{0} \longrightarrow}\, A_1^{\mathrm{ax}}}{\longrightarrow \mathsf{s}(t) \neq \mathsf{0}}\, \neg_{\mathrm{right}} \qquad \begin{matrix}(\pi_1')\\ \mathsf{s}(t) \neq \mathsf{0}, A', B_5, \Gamma \longrightarrow \Delta\end{matrix}}{A', B_5, \Gamma \longrightarrow \Delta}\ \mathrm{cut}.$$

There are no other rules that can introduce A_1 on the left.

Now consider the cases where $B_1^{\exists}$ is introduced in the last inference as an element of Π. The cases where $B_1^{\exists}$ is introduced via $\mathrm{w}_{\mathrm{left}}$ or $\mathrm{c}_{\mathrm{left}}$ are analogous to the cases for A_1. Therefore we only consider the case where $B_1^{\exists}$ is introduced by $\forall_{\mathrm{left}}$, i.e. $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ B_1^{\exists}[t], \Pi', \Gamma \longrightarrow \Delta\end{matrix}}{\underbrace{B_1^{\exists}, \Pi'}_{=\Pi}, \Gamma \longrightarrow \Delta}\ \forall_{\mathrm{left}},$$

then by induction hypothesis and Lemma 4.9 we have proofs

$$\pi_1' \vdash_{\mathrm{LK}\mathcal{P}_T^{=}} A', B_5, B_1^{\exists}[t], \Gamma \longrightarrow \Delta,$$
$$\pi_t \vdash_{\mathrm{LK}^{=}+B_1^{\mathrm{var}}} A', B_5 \longrightarrow B_1^{\exists}[t].$$

Now the statement follows by

$$\dfrac{\dfrac{\pi_t \qquad \pi_1'}{A', B_5, A', B_5, \Gamma \longrightarrow \Delta}\ \mathrm{cut}}{A', B_5, \Gamma \longrightarrow \Delta}\ \mathrm{c}^*_{\mathrm{left}}.$$

The remaining cases are all very similar: We apply the induction hypothesis to the premises of the last inference, reapply the inference to the resulting proofs and do contractions. Consider for example the case where π ends in $\vee_{\mathrm{left}}$, i.e. $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ \varphi, \Pi_1', \Gamma_1 \longrightarrow \Delta_1\end{matrix} \qquad \begin{matrix}(\pi_2)\\ \psi, \Pi_2', \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\varphi \vee \psi, \Pi', \Gamma \longrightarrow \Delta}\ \vee_{\mathrm{left}}.$$

Then by induction hypothesis we get proofs

$$\pi_1' \vdash_{\mathrm{LK}\mathcal{P}_T^{=}} A', B_5, \varphi, \Gamma_1 \longrightarrow \Delta_1,$$
$$\pi_2' \vdash_{\mathrm{LK}\mathcal{P}_T^{=}} A', B_5, \psi, \Gamma_2 \longrightarrow \Delta_2.$$

Note that in the induction hypothesis we always consider φ and ψ as elements of Γ, not of Π, even if they equal A_1 or $B_1^{\exists}$. Now the statement follows by

$$\dfrac{\dfrac{\pi_1' \qquad \pi_2'}{A', B_5, A', B_5, \varphi \vee \psi, \Gamma \longrightarrow \Delta}\ \vee_{\mathrm{left}}}{A', B_5, \varphi \vee \psi, \Gamma \longrightarrow \Delta}\ \mathrm{c}^*_{\mathrm{left}}.$$

If π ends in an initial sequent, then $\Pi = \emptyset$ since all initial sequents only contain atomic formulas and thus cannot introduce A_1 or $B_1^\exists$. We then apply appropriate weakenings. □

This leads us to the main result of this section:

Proof of Proposition 4.6. Let $AB \models \neg\varphi$. Then by Lemma 4.3 we have $AB^\exists \models \neg\varphi$. Using Lemma 4.4 we get $AB^\exists \models \varphi \longrightarrow$. By Lemma 4.10 we have a proof

$$\pi' \vdash_{\mathrm{LK}\mathcal{P}_T^=} \underbrace{A \setminus \{A_1, A_2, A_3\}, B_5}_{\subseteq T}, \underbrace{AB^\exists \setminus \{A_1, B_1^\exists\}}_{=T}, \varphi.$$

Now by applying $\mathrm{c}_{\mathrm{left}}$ a few times we get a $\pi'' \vdash_{\mathrm{LK}\mathcal{P}_T^=} T, \varphi \longrightarrow$ which concludes the proof. □

We conclude this section by showing cut-elimination and a subformula property for $\mathrm{LK}\mathcal{P}_T^=$.

Definition 4.11. *An $\mathrm{LK}\mathcal{P}_T^=$-proof π is called* regular *if all inferences with eigenvariable conditions have pairwise different eigenvariables. Note that this includes the eigenvariable condition for B_1^{var}.*

Proposition 4.12. *If $\mathrm{LK}\mathcal{P}_T^= \vdash \Gamma \longrightarrow \Delta$. Then there exists a regular $\mathrm{LK}\mathcal{P}_T^=$-proof π of $\Gamma \longrightarrow \Delta$*

Proof sketch. Very similar to the $\mathrm{LK}^=$ case. □

Proposition 4.13. *If $\mathrm{LK}\mathcal{P}_T^= \vdash \Gamma \longrightarrow \Delta$. Then there exists a $\mathrm{LK}\mathcal{P}_T^=$-proof π of $\Gamma \longrightarrow \Delta$ where all cuts are atomic.*

Proof. The proof follows the standard cut-elimination procedure for $\mathrm{LK}^=$. We can assume that the proof is regular because of Proposition 4.12. We have to show that we can perform rank- and degree-reduction in the presence of B_1^{var}. Since B_1^{var} does not introduce a formula in the lower sequent, it suffices to show rank-reduction. There are four cases to consider: B_1^{var} can be the left or right inference above cut and the cut formula can be in the left or right inference above B_1^{var}. We only consider the case where B_1^{var} is the left inference above cut and the cut formula occurs in the right inference above B_1^{var}. The other cases are similar. Now consider

$$\dfrac{\dfrac{\overset{(\pi_1)}{x = 0, \Gamma_1 \longrightarrow \Delta_1} \quad \overset{(\pi_2)}{x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2, \varphi}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2, \varphi}\, B_1^{\mathrm{var}} \quad \overset{(\pi_3)}{\varphi, \Gamma_3 \longrightarrow \Delta_3}}{\Gamma_1, \Gamma_2, \Gamma_3 \longrightarrow \Delta_1, \Delta_2, \Delta_3}\ \mathrm{cut}.$$

Because of the eigenvariable condition on B_1^{var} we have $y \notin \mathrm{FV}(\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2, \varphi)$. We can rewrite this proof into

$$\dfrac{\overset{(\pi_1)}{x = 0, \Gamma_1 \longrightarrow \Delta_1} \quad \dfrac{\overset{(\pi_2)}{x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2, \varphi} \quad \overset{(\pi_3)}{\varphi, \Gamma_3 \longrightarrow \Delta_3}}{x = \mathsf{s}(y), \Gamma_2, \Gamma_3 \longrightarrow \Delta_2, \Delta_3}\ \mathrm{cut}}{\Gamma_1, \Gamma_2, \Gamma_3 \longrightarrow \Delta_1, \Delta_2, \Delta_3}\ B_1^{\mathrm{var}}.$$

Since the proof is regular we have that $y \notin \mathrm{FV}(\Gamma_3 \longrightarrow \Delta_3)$, thus the eigenvariable condition still holds for B_1^{var}. Also, the resulting cut has lower rank. □

Next we state a subformula property for LK$\mathcal{P}_T^=$:

Proposition 4.14. *Let $s \in \{\neg, \wedge, \vee, \supset, \forall, \exists\}$, $S \in \mathrm{Seq}(S)$ and $\pi \vdash_{\mathrm{LK}\mathcal{P}_T^=} S$ where all cuts are atomic. If π uses s_{left} or s_{right}, then S contains s.*

Proof. The proof is similar to the proof of Theorem 2.15: Since s can only occur in non-atomic formulas and all cuts are atomic, there is no inference rule where s is in the upper sequent, but not in the lower sequent. This also applies to B_1^{var} since $x = 0$ and $x = \mathsf{s}(y)$ are atomic. Thus, the statement can be shown by a straightforward induction on π. □

4.2 From LK$\mathcal{P}_T^=$ to $\mathcal{P}_T^=$

We now introduce a calculus which operates on $[A(S)]_T$ and only uses A_1^{ax}, B_1^{var}, equational and structural rules. This serves as an intermediate step towards our goal calculus $\mathcal{P}_T$ which allows us to get rid of quantifier and propositional rules and the premise of T in the proof of the previous lemma.

Definition 4.15. *$\mathcal{P}_T^=$ is the proof calculus acting on $[A(S)]_T$ where for every inference*

$$\frac{\Gamma_1 \longrightarrow \Delta_1 \quad \dots \quad \Gamma_n \longrightarrow \Delta_n}{\Gamma \longrightarrow \Delta}\ I$$

with $I \in \mathcal{S} \cup \mathcal{E} \cup \{A_1^{\mathrm{ax}}, B_1^{\mathrm{var}}\}$ we have the corresponding inference

$$\frac{[\Gamma_1]_T \longrightarrow [\Delta_1]_T \quad \dots \quad [\Gamma_n]_T \longrightarrow [\Delta_n]_T}{[\Gamma]_T \longrightarrow [\Delta]_T}\ [I]_T$$

in $\mathcal{P}_T^=$.

In proofs we will often omit the $[\cdot]_T$ around multisets and formulas for ease of notation and instead imply it by the use of $[\cdot]_T$ in the inference rule. So, instead of the above we will often just write

$$\frac{\Gamma_1 \longrightarrow \Delta_1 \quad \dots \quad \Gamma_n \longrightarrow \Delta_n}{\Gamma \longrightarrow \Delta}\ [I]_T.$$

We also inherit the notions of auxiliary/principal occurrence/equality *and* cut formula *from* LK$\mathcal{P}_T^=$ *into this calculus. Since we are now dealing with equivalence classes of formulas, we have to modify the notion of* eigenvariable (condition) *in $[B_1^{\mathrm{var}}]_T$. Consider an inference*

$$\frac{x = 0, \Gamma \longrightarrow \Delta \quad x = \mathsf{s}(y), \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}\ [B_1^{\mathrm{var}}]_T.$$

We say that the eigenvariable condition is satisfied *if for all $[\varphi]_T \in [\Gamma]_T \cup [\Pi]_T \cup [\Delta]_T \cup [\Lambda]_T$ there exists a $\psi \in [\varphi]_T$ such that ψ does not contain y.*

Remark 4.16. *An alternative calculus is the calculus* $\mathcal{S} \cup \mathcal{E} \cup \{A_1^{\text{ax}}, B_1^{\text{var}}\}$ *on* $A(S)$ *extended with the rules*

$$\frac{A, \Gamma \longrightarrow \Delta}{A', \Gamma \longrightarrow \Delta} \Leftrightarrow_{T\text{left}} \qquad \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A'} \Leftrightarrow_{T\text{right}}$$

where $A, A' \in A(S)$ *and* $A \Leftrightarrow_T A'$*. This too allows us to exchange atoms with* T*-equivalent atoms which is implicit in the calculus we introduced before.*

For this section we formalize the notion of *quantifier-free instance* by expanding on Definition 4.7:

Definition 4.17. *Let* L *be a language and* $\varphi \in F(L)$*. A* $\psi \in F_{\text{qf}}(L)$ *is called a* quantifier-free instance of φ*, if there are terms* $t_1, \ldots, t_n \in T(L)$ *such that* $\psi \equiv \varphi[t_1] \ldots [t_n]$*.*

We show that we can transform $\text{LK}\mathcal{P}_T^=$-proofs of $T, t = u \longrightarrow$ into $\mathcal{P}_T^=$-proofs. For this we use a few lemmas:

Lemma 4.18. *Let* φ *be a quantifier-free instance of a formula in* $T \setminus \{B_4\}$ *and* $t \in T(S)$*. Then* $\varphi \in A(S)$ *and* $\varphi \Leftrightarrow_T t = t$*.*

Proof. Checking the formulas in T we see that the only axiom with non-atomic quantifier-free instances is B_4. Thus $\varphi \in A(S)$.

Now we have $\text{LK}^= \vdash T, \varphi \longrightarrow t = t$ by

$$\dfrac{\dfrac{}{\longrightarrow t = t}\,\text{refl}}{T, \varphi \longrightarrow t = t}\,\text{w}^*_{\text{left}}.$$

Let $\psi \in T$ be the formula that φ is a quantifier-free instance of. Then $\text{LK}^= \vdash T, t = t \longrightarrow \varphi$ by

$$\dfrac{\dfrac{\dfrac{}{\varphi \longrightarrow \varphi}\,\text{axiom}}{\psi \longrightarrow \varphi}\,\forall^*_{\text{left}}}{T, t = t \longrightarrow \varphi}\,\text{w}^*_{\text{left}}.$$

□

Lemma 4.19. *Let* $\varphi, \psi \in F(S)$ *such that* $\varphi \supset \psi$ *is a quantifier-free instance of* B_4*. Then* $\varphi, \psi \in A(S)$ *and* $\varphi \Leftrightarrow_T \psi$*.*

Proof. Since $\varphi \supset \psi$ is an instance of B_4, there are $t, u, v \in T(S)$ such that $\varphi \equiv t + u = t + v$ and $\psi \equiv u = v$. We have $\text{LK}^= \vdash T, u = v \longrightarrow t + u = t + v$ by

$$\dfrac{\dfrac{\dfrac{}{u = v \longrightarrow u = v}\,\text{axiom} \quad \dfrac{}{\longrightarrow t + u = t + u}\,\text{refl}}{u = v \longrightarrow t + u = t + v}\,\text{eq}{\rightarrow}_{\text{right}}}{T, u = v \longrightarrow t + u = t + v}\,\text{w}^*_{\text{left}}$$

and $\text{LK}^= \vdash T, t + u = t + v \longrightarrow u = v$ by

$$\dfrac{\dfrac{\dfrac{\dfrac{}{t + u = t + v \longrightarrow t + u = t + v}\,\text{axiom} \quad \dfrac{}{u = v \longrightarrow u = v}\,\text{axiom}}{t + u = t + v \supset u = v, t + u = t + v \longrightarrow u = v}\,\supset_{\text{left}}}{B_4, t + u = t + v \longrightarrow u = v}\,\forall^*_{\text{left}}}{T, t + u = t + v \longrightarrow u = v}\,\text{w}^*_{\text{left}}.$$

□

Lemma 4.20. *If* $\mathrm{LK}\mathcal{P}^{=}_{T} \vdash \Pi, \Gamma_{\mathrm{at}} \longrightarrow \Delta_{\mathrm{at}}$ *such that* $\mathrm{supp}(\Gamma_{\mathrm{at}} \cup \Delta_{\mathrm{at}}) \subseteq A(S)$ *and* Π *is a multiset of partial instances of formulas in* T*, then* $\mathcal{P}^{=}_{T} \vdash [\Gamma_{\mathrm{at}}]_T \longrightarrow [\Delta_{\mathrm{at}}]_T$.

Proof. Let $\pi \vdash_{\mathrm{LK}\mathcal{P}^{=}_{T}} \Pi, \Gamma_{\mathrm{at}} \longrightarrow \Delta_{\mathrm{at}}$. We can assume that the cuts in π are atomic because of Proposition 4.13. By Lemma 4.14 we then have that π does not use any of the rules $\neg_{\mathrm{left}}$, $\neg_{\mathrm{right}}$, $\wedge_{\mathrm{left}}$, $\wedge_{\mathrm{right}}$, $\vee_{\mathrm{left}}$, $\vee_{\mathrm{right}}$, $\exists_{\mathrm{left}}$ and $\exists_{\mathrm{right}}$. We show that there is a proof $\pi' \vdash_{\mathcal{P}^{=}_{T}} [\Gamma_{\mathrm{at}}]_T \longrightarrow [\Delta_{\mathrm{at}}]_T$.

If π ends in axiom, then $\pi =$

$$\frac{}{\varphi \longrightarrow \varphi}\ \text{axiom}.$$

for an atomic formula φ. If $\varphi \in \Gamma_{\mathrm{at}}$, then $\pi' =$

$$\frac{}{\varphi \longrightarrow \varphi}\ [\text{axiom}]_T.$$

Otherwise $\varphi \in \Pi$ and since φ is atomic, it is quantifier-free and we have $\varphi \Leftrightarrow_T \mathsf{0} = \mathsf{0}$ by Lemma 4.18. Thus $\pi' =$

$$\frac{}{\longrightarrow \varphi}\ [\text{refl}]_T.$$

If $\pi =$

$$\frac{}{\longrightarrow t = t}\ \text{refl},$$

then $\pi' =$

$$\frac{}{\longrightarrow t = t}\ [\text{refl}]_T.$$

If $\pi =$

$$\frac{}{\mathsf{s}(t) = \mathsf{0} \longrightarrow}\ A^{\mathrm{ax}}_1,$$

note that no formula of the form $\mathsf{s}(t) = \mathsf{0}$ is an instance of a formula in T and therefore $\Pi = \emptyset$. Thus $\pi' =$

$$\frac{}{\mathsf{s}(t) = \mathsf{0} \longrightarrow}\ [A^{\mathrm{ax}}_1]_T.$$

If $\pi =$

$$\frac{\begin{matrix}(\pi_1)\\ \varphi, \varphi, \Gamma \longrightarrow \Delta_{\mathrm{at}}\end{matrix}}{\varphi, \Gamma \longrightarrow \Delta_{\mathrm{at}}}\ \mathrm{c}_{\mathrm{left}},$$

with Γ such that $\Gamma \cup \{\varphi\} = \Pi \cup \Gamma_{\mathrm{at}}$. If $\varphi \in \Pi$, we apply the induction hypothesis to π_1 to get a proof π'_1 of $[\Gamma_{\mathrm{at}}]_T \longrightarrow [\Delta_{\mathrm{at}}]_T$. Then $\pi' = \pi'_1$. If $\varphi \in \Gamma_{\mathrm{at}}$, then we apply the induction hypothesis to π_1 to get a proof π'_1 of $[\varphi]_T, [\varphi]_T, [\Gamma \cap \Gamma_{\mathrm{at}}]_T \longrightarrow [\Delta_{\mathrm{at}}]_T$. Then $\pi' =$

$$\frac{\begin{matrix}(\pi'_1)\\ \varphi, \varphi, \Gamma \cap \Gamma_{\mathrm{at}} \longrightarrow \Delta_{\mathrm{at}}\end{matrix}}{\underbrace{\varphi, \Gamma \cap \Gamma_{\mathrm{at}}}_{=\Gamma_{\mathrm{at}}} \longrightarrow \Delta_{\mathrm{at}}}\ [\mathrm{c}_{\mathrm{left}}]_T.$$

The cases where π ends in $\mathrm{c}_{\mathrm{right}}$, $\mathrm{w}_{\mathrm{left}}$ or $\mathrm{w}_{\mathrm{right}}$ are argued similarly.

Now consider the case $\pi =$

$$\frac{\begin{matrix}(\pi_1)\\ \Gamma_1 \longrightarrow \Delta_1, \varphi\end{matrix} \quad \begin{matrix}(\pi_2)\\ \varphi, \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\ \text{cut}$$

with $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ such that $\Gamma_1 \cup \Gamma_2 = \Pi \cup \Gamma_{\text{at}}$ and $\Delta_1 \cup \Delta_2 = \Delta_{\text{at}}$. Since φ is atomic we can apply the induction hypothesis to π_1 and π_2 to get proofs $\pi_1' \vdash_{\mathcal{P}_T^=} [\Gamma_1 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_1]_T, [\varphi]_T$ and $\pi_2' \vdash_{\mathcal{P}_T^=} [\varphi]_T, [\Gamma_2 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_2]_T$. Now, $\pi' =$

$$\dfrac{\begin{matrix}(\pi_1') \\ \Gamma_1 \cap \Gamma_{\text{at}} \longrightarrow \Delta_1, \varphi\end{matrix} \quad \begin{matrix}(\pi_2') \\ \varphi, \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \Delta_2\end{matrix}}{\underbrace{\Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}}}_{=\Gamma_{\text{at}}} \longrightarrow \underbrace{\Delta_1, \Delta_2}_{=\Delta_{\text{at}}}} \; [\text{cut}]_T.$$

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) \\ \Gamma_1 \longrightarrow \Delta_1, t = u\end{matrix} \quad \begin{matrix}(\pi_2) \\ \varphi(t), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\varphi(u), \Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2} \; \text{eq}{\rightarrow_{\text{left}}}$$

with φ atomic and $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ such that $\Gamma_1 \cup \Gamma_2 \cup \{\varphi(u)\} = \Pi \cup \Gamma_{\text{at}}$ and $\Delta_1 \cup \Delta_2 = \Delta_{\text{at}}$. Since $\varphi(t)$ and $t = u$ are atomic we can apply the induction hypothesis to π_1 and π_2 to get proofs π_1' of $[\Gamma_1 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_1]_T, [t = u]_T$ and π_2' of $[\varphi(u)]_T, [\Gamma_2 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_2]_T$. Now let $\pi_3' :=$

$$\dfrac{\begin{matrix}(\pi_1') \\ \Gamma_1 \cap \Gamma_{\text{at}} \longrightarrow \Delta_1, t = u\end{matrix} \quad \begin{matrix}(\pi_2') \\ \varphi(t), \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \Delta_2\end{matrix}}{\varphi(u), \Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \underbrace{\Delta_1, \Delta_2}_{=\Delta_{\text{at}}}} \; [\text{eq}{\rightarrow_{\text{left}}}]_T.$$

If $\varphi(u) \in \Gamma_{\text{at}}$ we have $\Gamma_{\text{at}} = \{\varphi(u)\} \cup (\Gamma_1 \cap \Gamma_{\text{at}}) \cup (\Gamma_2 \cap \Gamma_{\text{at}})$ and $\pi' = \pi_3'$. Otherwise, $\varphi(u) \in \Pi$ and we have $\varphi(u) \Leftrightarrow_T \mathsf{0} = \mathsf{0}$ by Lemma 4.18. Thus, $\pi' =$

$$\dfrac{\dfrac{}{\longrightarrow \varphi(u)}\,[\text{refl}]_T \quad \begin{matrix}(\pi_3') \\ \varphi(u), \Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \Delta_1, \Delta_2\end{matrix}}{\underbrace{\Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}}}_{=\Gamma_{\text{at}}} \longrightarrow \underbrace{\Delta_1, \Delta_2}_{=\Delta_{\text{at}}}} \; [\text{cut}]_T.$$

If π ends in other equality rules, we perform a similar transformation.

Now consider $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) \\ x = \mathsf{0}, \Gamma_1 \longrightarrow \Delta_1\end{matrix} \quad \begin{matrix}(\pi_2) \\ x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2} \; B_1^{\text{var}},$$

with $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ where $\Gamma_1 \cup \Gamma_2 = \Pi \cup \Gamma_{\text{at}}$, $\Delta_1 \cup \Delta_2 = \Delta_{\text{at}}$ and $y \notin \text{FV}(\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2)$. Since $x = \mathsf{0}$ and $x = \mathsf{s}(y)$ are atomic we can apply the induction hypothesis to π_1 and π_2 to get proofs π_1' of $[x = \mathsf{0}]_T, [\Gamma_1 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_1]_T$ and π_2' of $[x = \mathsf{s}(y)]_T, [\Gamma_2 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_2]_T$. Then $\pi' =$

$$\dfrac{\begin{matrix}(\pi_1) \\ x = \mathsf{0}, \Gamma_1 \cap \Gamma_{\text{at}} \longrightarrow \Delta_1\end{matrix} \quad \begin{matrix}(\pi_2) \\ x = \mathsf{s}(y), \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \Delta_2\end{matrix}}{\underbrace{\Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}}}_{=\Gamma_{\text{at}}} \longrightarrow \underbrace{\Delta_1, \Delta_2}_{=\Delta_{\text{at}}}} \; [B_1^{\text{var}}]_T.$$

Now consider $\pi =$

$$\dfrac{\dfrac{(\pi_1)}{\Gamma_1 \longrightarrow \Delta_1, \varphi} \quad \dfrac{(\pi_2)}{\psi, \Gamma_2 \longrightarrow \Delta_2}}{\varphi \supset \psi, \Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2} \supset_{\text{left}},$$

with $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ such that $\{\varphi \supset \psi\} \cup \Gamma_1 \cup \Gamma_2 = \Pi \cup \Gamma_{\text{at}}$. Since $\varphi \supset \psi$ is not atomic, it is an instance of a formula in T. The only formula in T which contains $\supset$ is B_4, therefore we have $\varphi \equiv t + u = t + v$ and $\psi \equiv u = v$ for some $t, u, v \in T(S)$. There holds $\varphi \Leftrightarrow_T \psi$ by Lemma 4.19. Since φ and ψ are atomic we can apply the induction hypothesis to π_1 and π_2 to get proofs π_1' of $[\Gamma_1 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_1]_T, [\varphi]_T$ and π_2' of $[\psi]_T, [\Gamma_2 \cap \Gamma_{\text{at}}]_T \longrightarrow [\Delta_2]_T$. Since $[\varphi]_T = [\psi]_T$, we can replace $\supset_{\text{left}}$ by a cut to get $\pi' =$

$$\dfrac{\dfrac{(\pi_1')}{\Gamma_1 \cap \Gamma_{\text{at}} \longrightarrow \Delta_1, \varphi} \quad \dfrac{(\pi_2')}{\psi, \Gamma_2 \cap \Gamma_{\text{at}} \longrightarrow \Delta_2}}{\underbrace{\Gamma_1 \cap \Gamma_{\text{at}}, \Gamma_2 \cap \Gamma_{\text{at}}}_{=\Gamma_{\text{at}}} \longrightarrow \underbrace{\Delta_1, \Delta_2}_{=\Delta_{\text{at}}}} [\text{cut}]_T \ .$$

π cannot end in $\supset_{\text{right}}$ since all formulas in Δ_{at} are atomic.

Now consider $\pi =$

$$\dfrac{\dfrac{(\pi_1)}{\varphi(t), \Gamma \longrightarrow \Delta_{\text{at}}}}{\forall x\, \varphi(x), \Gamma \longrightarrow \Delta_{\text{at}}} \forall_{\text{left}}$$

with $\{\forall x\, \varphi(x)\} \cup \Gamma = \Pi \cup \Gamma_{\text{at}}$. Since $\forall x\, \varphi(x)$ is not atomic we have that $\forall x\, \varphi(x)$ and $\varphi(t)$ are instances of a formula in T. Thus we can apply the induction hypothesis to π_1 to get a proof π_1' of $[\Gamma_{\text{at}}]_T \longrightarrow [\Delta_{\text{at}}]_T$. Now, $\pi' = \pi_1'$.

Note that π cannot end in $\forall_{\text{right}}$ since all formulas in Δ_{at} are atomic. □

Now, the main result for this section follows:

Proposition 4.21. *Let $\varphi \in A(S)$ and $\text{LK}\mathcal{P}_T^= \vdash T, \varphi \longrightarrow$. Then $\mathcal{P}_T^= \vdash [\varphi]_T \longrightarrow$.*

Proof. Follows directly from Lemma 4.20 for $\Pi = T$, $\Gamma_{\text{at}} = \{\varphi\}$ and $\Delta_{\text{at}} = \emptyset$. □

4.3 From $\mathcal{P}_T^=$ to $[B_1^{\text{var}}]_T$-normal proofs

In this section we discuss the notion of $[B_1^{\text{var}}]_T$-normal proofs which will allow us to extract the $\mathcal{P}_T$-proof structure from $\mathcal{P}_T^=$-proofs. Further, $[B_1^{\text{var}}]_T$-normal proofs will give us the ability to substitute free variables in $\mathcal{P}_T^=$-proofs: Note that the $[B_1^{\text{var}}]_T$-rule is not preserved under substitutions of variables by arbitrary terms in proofs. Since the rule requires that we use a variable x in the antecedent of the premises we cannot substitute x by arbitrary terms since then the corresponding $[B_1^{\text{var}}]_T$-inference might not be valid anymore. To do this, we first need to be able to uniquely identify the variables associated with a $[B_1^{\text{var}}]_T$-inference.

Lemma 4.22. *Let x, y be variables. If $x = 0 \Leftrightarrow_T y = 0$, then $x = y$.*

Proof. By assumption we have $T \vdash x = 0 \longrightarrow y = 0$. Now further assume that $x \neq y$. Since $\mathbb{N}$ is a model of T we have that $\mathbb{N} \models x = 0 \supset y = 0$. However, under the variable mapping b with $b(x) = 0$ and $b(y) = 1$ we have that $x = 0$ is satisfied, but $y = 0$ is not. Therefore we have a contradiction and $x = y$. □

Lemma 4.23. *Let x, y, z, w be variables with $x \neq z$ and $y \neq w$. If $x = \mathsf{s}(z) \Leftrightarrow_T y = \mathsf{s}(w)$, then $x = y$ and $z = w$.*

Proof. By assumption we have $T \vdash x = \mathsf{s}(z) \longrightarrow y = \mathsf{s}(w)$. Since $\mathbb{N}$ is a model of T we have $\mathbb{N} \models x = \mathsf{s}(z) \supset y = \mathsf{s}(w)$. Now assume $x \neq y$. Under the variable mapping b with $b(x) = 1$ and $b(y) = b(z) = b(w) = 0$ we have $\mathbb{N} \models x = \mathsf{s}(z)$, but $\mathbb{N} \not\models y = \mathsf{s}(w)$ which is a contradiction. Therefore $x = y$. Now assume $z \neq w$, then under the variable mapping b with $b(x) = b(y) = 1, b(z) = 0$ and $b(w) = 1$ we have that $\mathbb{N} \models x = \mathsf{s}(z)$, but $\mathbb{N} \not\models y = \mathsf{s}(w)$, which is a contradiction. Therefore $w = z$. □

This means the following is well-defined:

Definition 4.24. *Consider a $[B_1^{\text{var}}]_T$-inference*

$$\frac{x = 0, \Gamma \longrightarrow \Delta \quad x = \mathsf{s}(y), \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}\,[B_1^{\text{var}}]_T.$$

We call x the split variable *and y the* eigenvariable *of this inference. For a $\mathcal{P}_T^=$-proof π we write* $\mathrm{EV}(\pi)$ *for the set of variables which are eigenvariable of a $[B_1^{\text{var}}]_T$-inference in π and* $\mathrm{SV}(\pi)$ *for the set of variables which are split variables of a $[B_1^{\text{var}}]_T$-inference in π. We say* π is EV-regular *if all eigenvariables of $[B_1^{\text{var}}]_T$-inferences in π are pairwise distinct.*

This allows us to formulate conditions under which substitution of terms is allowed:

Lemma 4.25. *Let $\pi(x) \vdash_{\mathcal{P}_T^=} [\Gamma(x)]_T \longrightarrow [\Delta(x)]_T$. Further let x be a variable such that $x \notin \mathrm{SV}(\pi(x))$ and let $t \in T(S)$ such that $\mathrm{FV}(t) \cap \mathrm{EV}(\pi) = \emptyset$. Then there exists a proof $\pi(t) \vdash_{\mathcal{P}_T^=} [\Gamma(t)]_T \longrightarrow [\Delta(t)]_T$ with $\#_{[B_1^{\text{var}}]_T}(\pi(t)) = \#_{[B_1^{\text{var}}]_T}(\pi(x))$.*

Proof. We proceed by induction on π.

If $\pi(x) =$

$$\frac{}{\mathsf{s}(u(x)) = 0 \longrightarrow}\,[A_1^{\text{ax}}]_T,$$

then $\pi(t) =$

$$\frac{}{\mathsf{s}(u(t)) = 0 \longrightarrow}\,[A_1^{\text{ax}}]_T$$

is a $\mathcal{P}_T^=$-proof of $[\Gamma(t)]_T \longrightarrow [\Delta(t)]_T$. A similar argument holds, if π ends in $[\text{refl}]_T$ or $[\text{axiom}]_T$.

If $\pi(x)$ ends in a contraction or weakening we can apply the induction hypothesis to the direct subproof $\pi'(x)$ of $\pi(x)$. We can then reapply the contraction or weakening to $\pi'(t)$ to get the desired proof.

If $\pi(x) =$

$$\frac{\begin{matrix}(\pi_1(x)) \\ \Gamma_1(x) \longrightarrow \Delta_1(x), u(x) = v(x)\end{matrix} \quad \begin{matrix}(\pi_2(x)) \\ \varphi(u(x), x), \Gamma_2(x) \longrightarrow \Delta_2(x)\end{matrix}}{\varphi(v(x), x), \Gamma_1(x), \Gamma_2(x) \longrightarrow \Delta_1(x), \Delta_2(x)}\,[\text{eq}{\rightarrow_{\text{left}}}]_T,$$

then by induction hypothesis we have $\pi_1(t) \vdash_{\mathcal{P}_T^=}, [\Gamma_1(t)]_T \longrightarrow [\Delta_1(t)]_T, [u(t) = v(t)]_T$ and $\pi_2(t) \vdash_{\mathcal{P}_T^=} [\varphi(u(t), t)]_T, [\Gamma_2(t)]_T \longrightarrow [\Delta_2(t)]_T$. Thus, applying $[\text{eq}{\rightarrow_{\text{left}}}]_T$ to $\pi_1(t)$ and $\pi_2(t)$ gives the desired result. A similar arguments works for the other equality rules and $[\text{cut}]_T$.

If $\pi(x) =$

$$\dfrac{\begin{array}{cc}(\pi_1(x)) & (\pi_2(x))\\ y = 0, \Gamma_1(x) \longrightarrow \Delta_1(x) & y = \mathsf{s}(z), \Gamma_2(x) \longrightarrow \Delta_2(x)\end{array}}{\Gamma_1(x), \Gamma_2(x) \longrightarrow \Delta_1(x), \Delta_2(x)}\ [B_1^{\text{var}}]_T,$$

then note that $y \neq x$ since $x \notin \mathrm{SV}(\pi(x))$ and $z \neq x$ since z is an eigenvariable and x is a free variable in π. By induction hypothesis we have proofs

$$\pi_1(t) \vdash_{\mathcal{P}_T^=} [y = 0]_T, [\Gamma_1(t)]_T \longrightarrow [\Delta_1(t)]_T$$

and

$$\pi_2(t) \vdash_{\mathcal{P}_T^=} [y = \mathsf{s}(z)]_T, [\Gamma_2(t)]_T \longrightarrow [\Delta_2(t)]_T.$$

Thus, applying $[B_1^{\text{var}}]_T$ to $\pi_1(t)$ and $\pi_2(t)$ gives the desired result. Note that the eigenvariable condition is satisfied since $\mathrm{FV}(t) \cap \mathrm{EV}(\pi(x)) = \emptyset$.

Note than in all cases the number of $[B_1^{\text{var}}]_T$-inferences was preserved. □

The following property makes it easier to fulfill the conditions for Lemma 4.25.

Definition 4.26. *Let* $\pi \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$. *We say* π is $[B_1^{\text{var}}]_T$-regular *if for all subproofs* ρ *of* π *and all subproofs* ρ' *of* ρ *there holds: If* ρ *and* ρ' *end in* $[B_1^{\text{var}}]_T$ *and both their last* $[B_1^{\text{var}}]_T$*-inferences have the same split variable, then* $\rho = \rho'$.

To extract the $\mathcal{P}_T$-proof structure from $\mathcal{P}_T^=$-proofs we transform $\mathcal{P}_T^=$-proofs into proofs where $[B_1^{\text{var}}]_T$-inferences occur after all $[\text{cut}]_T$ and equality inferences. To do this, the following definitions are useful.

Definition 4.27. *Let* $\mathcal{C}$ *be a proof calculus and* $\mathcal{I}, \mathcal{J} \subseteq \mathcal{C}$. *We say a* $\mathcal{C}$-proof π is $\frac{\mathcal{I}}{\mathcal{J}}$-formed *if all subproofs* ρ *of* π *which end in one of the rules in* $\mathcal{I}$*, do not use any of the rules in* $\mathcal{J}$. *We say a* $\mathcal{C}$-proof π is $\mathcal{I}\downarrow$-formed *if* π *is* $\frac{\mathcal{C}\setminus\mathcal{I}}{\mathcal{I}}$*-formed. Let* ρ *be a subproof of* π*, and let* ρ' *be a subproof of* ρ. *Further let* ρ' *end in a rule from* $\mathcal{J}$ *and let* ρ *end in a rule from* $\mathcal{I}$. *Then we call* (ρ', ρ) *an* $\frac{\mathcal{I}}{\mathcal{J}}$-violating pair of π. *If* ρ' *is a direct subproof of* ρ *we call* (ρ', ρ) *a* direct $\frac{\mathcal{I}}{\mathcal{J}}$-violating pair of π. *If* $\mathcal{I} = \{I\}$ *we often omit the braces and write* $\frac{I}{\mathcal{J}}$-violating pair. *Similarly if* $\mathcal{J}$ *is a singleton set.*

Remark 4.28. *It is straightforward to show that a proof is* $\frac{\mathcal{I}}{\mathcal{J}}$*-formed if and only if it has no* $\frac{\mathcal{I}}{\mathcal{J}}$*-violating pairs. Also note, there is a* $\frac{\mathcal{C}\setminus\mathcal{I}}{\mathcal{I}}$*-violating pair if and only if there is a direct* $\frac{\mathcal{C}\setminus\mathcal{I}}{\mathcal{I}}$*-violating pair.*

Definition 4.29. *We set*

$$\mathcal{E}_T := \{[\text{eq}{\rightarrow}_{\text{left}}]_T, [\text{eq}{\rightarrow}_{\text{right}}]_T, [\text{eq}{\leftarrow}_{\text{left}}]_T, [\text{eq}{\leftarrow}_{\text{right}}]_T, [\text{cut}]_T\}$$

and

$$\mathcal{W}_T := \{[\text{w}_{\text{left}}]_T, [\text{w}_{\text{right}}]_T\}.$$

Now we can define what we mean by $[B_1^{\text{var}}]_T$-normal proofs:

Definition 4.30. *A $\mathcal{P}_T^{=}$-proof π is called* $[B_1^{\mathrm{var}}]_T$-normal *if all of the following hold:*

(i) π *is* EV*-regular.*

(ii) π *is* $[B_1^{\mathrm{var}}]_T$*-regular.*

(iii) π *is* $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$*-formed.*

(iv) π *is* $\mathcal{W}_T\downarrow$*-formed.*

The goal for this section is to show that we can always obtain $[B_1^{\mathrm{var}}]_T$-normal $\mathcal{P}_T^{=}$-proofs:

Proposition 4.31. *If* $\mathcal{P}_T^{=} \vdash [\Gamma]_T \longrightarrow [\Delta]_T$*, then there exists a* $[B_1^{\mathrm{var}}]_T$*-normal* $\mathcal{P}_T^{=}$*-proof of* $[\Gamma]_T \longrightarrow [\Delta]_T$*.*

4.3.1 $\mathcal{W}_T\downarrow$-formed proofs

In this subsection we show that weakenings can be moved down in $\mathcal{P}_T^{=}$-proofs which also allows us to consider proofs without weakening.

Lemma 4.32. *Let* $\pi \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$*. Then there exists a proof* $\pi' \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$ *such that:*

(i) π' *is* $\mathcal{W}_T\downarrow$ *formed.*

(ii) If π *is* EV*-regular, then so is* π'*.*

(iii) If π *is* $[B_1^{\mathrm{var}}]_T$*-regular, then so is* π'*.*

(iv) If π *is* $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$*-formed, then so is* π'*.*

Proof. This proof is similar to the procedure for removing weakenings in [2]. In this proof we write *violating pair* to mean $\frac{\mathcal{P}_T^{=}\setminus\mathcal{W}_T}{\mathcal{W}_T}$*-violating pair.*

Let $\pi' \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$. By Remark 4.28 it suffices to show that there is a proof $\pi \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$ such that π has no violating pairs. To do this, we proceed by induction on the number of violating pairs of π'. If π' has no violating pairs, we are done. Otherwise let (ρ', ρ) be a direct violating pair and let I', I be the inferences that ρ', ρ end in respectively. We distinguish two cases:

(i) If the principal occurrence of I' is in the context of I, we can exchange I and I' and still have a $\mathcal{P}_T^{=}$-proof. For example if ρ' ends in $[\mathrm{w}_{\mathrm{left}}]_T$ and $\rho =$

$$\dfrac{\dfrac{\begin{matrix}(\rho'')\\ \Pi_1 \longrightarrow \Lambda_1, \psi\end{matrix}}{\varphi, \Pi_1 \longrightarrow \Lambda_1, \psi}\,[\mathrm{w}_{\mathrm{left}}]_T \qquad \begin{matrix}(\rho''')\\ \psi, \Pi_2 \longrightarrow \Lambda_2\end{matrix}}{\varphi, \Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\,[\mathrm{cut}]_T$$

then we have a proof of $[\Gamma]_T \longrightarrow [\Delta]_T$ with at least one fewer violating pair by replacing ρ in π with

$$\dfrac{\dfrac{\begin{matrix}(\rho'')\\ \Pi_1 \longrightarrow \Lambda_1, \psi\end{matrix} \quad \begin{matrix}(\rho''')\\ \psi, \Pi_2 \longrightarrow \Lambda_2\end{matrix}}{\Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\,[\text{cut}]_T}{\varphi, \Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\,[\text{w}_{\text{left}}]_T.$$

Thus, we can apply the induction hypothesis. A similar procedure works for other rules in $\mathcal{P}_T^{=}$.

(ii) Otherwise the principal occurrence of I' is an auxiliary occurrence of I.

(a) If $\rho =$

$$\dfrac{\dfrac{\begin{matrix}(\rho'')\\ \varphi, \Pi \longrightarrow \Lambda\end{matrix}}{\varphi, \varphi, \Pi \longrightarrow \Lambda}\,[\text{w}_{\text{left}}]_T}{\varphi, \Pi \longrightarrow \Lambda}\,[\text{c}_{\text{left}}]_T,$$

then by replacing ρ in π by ρ'' we get a proof of $\Gamma \longrightarrow \Delta$ with at least one fewer violating pair. A similar argument works, if ρ ends in $[\text{c}_{\text{right}}]_T$.

(b) If $\rho =$

$$\dfrac{\dfrac{\begin{matrix}(\rho'')\\ \Pi_1 \longrightarrow \Lambda_1\end{matrix}}{\Pi_1 \longrightarrow \Lambda_1, t = u}\,[\text{w}_{\text{right}}]_T \quad \begin{matrix}(\rho''')\\ \psi(t), \Pi_2 \longrightarrow \Lambda_2\end{matrix}}{\psi(u), \Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\,[\text{eq}{\rightarrow}_{\text{left}}]_T,$$

then by replacing ρ in π by

$$\dfrac{\begin{matrix}(\rho'')\\ \Pi_1 \longrightarrow \Lambda_1\end{matrix}}{\psi(u), \Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\,[\text{w}^*]$$

we get a proof of $[\Gamma]_T \longrightarrow [\Delta]_T$ with at least one fewer violating pair than π and we can apply the induction hypothesis. A similar argument works for other equality rules, $[\text{cut}]_T$ and $[B_1^{\text{var}}]_T$ and also if ρ' is the right direct subproof of ρ.

Note that in all cases, EV-regularity, $[B_1^{\text{var}}]_T$-regularity and $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-form are preserved. □

Lemma 4.33. *Let $\pi \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$. Then there are $\Gamma' \subseteq \Gamma$, $\Delta' \subseteq \Delta$ and a proof $\pi' \vdash_{\mathcal{P}_T^{=} \setminus \mathcal{W}_T} [\Gamma']_T \longrightarrow [\Delta']_T$. If π is* EV*-regular, then so is π'.*

Proof. Let $\pi \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$. By Lemma 4.32 we can assume that π is $\mathcal{W}_T\downarrow$-formed. Note that this preserves EV-regularity. We show the statement by induction on the number of inferences from $\mathcal{W}_T$ that π uses. If π does not use any rules from $\mathcal{W}_T$ we can set $\Gamma' = \Gamma, \Delta' = \Delta$ and $\pi' = \pi$. Otherwise π ends in a rule from $\mathcal{W}_T$ since π is $\mathcal{W}_T\downarrow$-formed. If $\pi =$

$$\dfrac{\dfrac{\begin{matrix}(\pi_1)\\ \Gamma_1 \longrightarrow \Delta_1\end{matrix}}{\varphi, \Gamma_1 \longrightarrow \Delta_1}\,[\text{w}_{\text{left}}]_T,$$

then by induction hypothesis we have a $\pi_1' \vdash_{\mathcal{P}_T^{=} \setminus \mathcal{W}_T} [\Gamma_1']_T \longrightarrow [\Delta_1']_T$ for some $\Gamma_1' \subseteq \Gamma_1 \cup \{\varphi\}$ and $\Delta_1' \subseteq \Delta_1$. With $\pi' = \pi_1'$, $\Gamma' = \Gamma_1'$ and $\Delta' = \Delta_1'$ the statement follows. A similar procedure of "walking up the proof tree" works for $[\mathrm{w}_{\mathrm{right}}]_T$. □

4.3.2 $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed proofs

Now we show that $\mathcal{P}_T^{=}$-proofs can be transformed into proofs where $[B_1^{\mathrm{var}}]_T$-inferences are the last binary inferences. To do this we use a well-founded order on multisets:

Definition 4.34. *Let X be a set and let $>$ a binary relation on X. We define the* multiset order $>^{\mathrm{mul}}$ *on $\mathcal{M}(X)$ by $\Gamma >^{\mathrm{mul}} \Delta$ if and only if there are $\Pi, \Lambda \in \mathcal{M}(X)$ with $\emptyset \neq \Pi \subseteq \Gamma$, $\Delta = (\Gamma - \Pi) \cup \Lambda$ and for all $y \in \Lambda$ there exists a $x \in \Pi$ such that $x > y$. We write $\Gamma <^{\mathrm{mul}} \Delta$ if $\Delta >^{\mathrm{mul}} \Gamma$.*

Lemma 4.35. *$(X, >)$ is well-founded if and only if $(\mathcal{M}(X), >^{\mathrm{mul}})$ is.*

Proof. See for example [1] Theorem 2.5.5. □

Definition 4.36. *Let π be a $\mathcal{P}_T^{=}$-proof. Further let $\pi_1, \ldots, \pi_n$ be the direct subproofs of π. We now inductively define the* $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-violation measure of π *(denoted as $V(\pi)$) by the multiset*

$$V(\pi) = \bigcup_{i=1}^{n} V(\pi_i) \cup \begin{cases} \left\{ \#_{[B_1^{\mathrm{var}}]_T}(\pi) \right\} & \text{if } \pi \text{ ends in a rule from } \mathcal{E}_T \\ \emptyset & \text{otherwise.} \end{cases}$$

Remark 4.37. *The sum of the elements in $V(\pi)$ is the number of $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-violating pairs.*

Lemma 4.38. *Let π be a $\mathcal{P}_T^{=} \setminus \mathcal{W}_T$-proof. There holds:*

(i) π is $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed if and only if all elements in $V(\pi)$ are 0.

(ii) $\max V(\pi) \leq \#_{[B_1^{\mathrm{var}}]_T}(\pi)$.

(iii) Let ρ be a subproof of π with conclusion $[\Gamma]_T \longrightarrow [\Delta]_T$ and let $\rho' \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$ with $V(\rho') <^{\mathrm{mul}} V(\rho)$. Further let π' be the proof where ρ is replaced by ρ' in π. Then $V(\pi') <^{\mathrm{mul}} V(\pi)$.

Proof. (i) Straightforward.

(ii) Follows by a straightforward induction on π.

(iii) We proceed by induction on the number of subproofs between π and ρ. If there is only one such subproof, then $\pi = \rho$ and the statement follows by assumption. Otherwise let σ be the subproof of π such that ρ is a direct subproof of σ. Further, let σ' be the proof where ρ is replaced by ρ' in σ'. Then by the definition of V we have $V(\sigma') <^{\mathrm{mul}} V(\sigma)$ and we can apply the induction hypothesis to π and σ.

□

The following definition is useful in the upcoming proof.

Definition 4.39. *Let Γ be a multiset and $n \in \mathbb{N}$. We inductively define the multiset $n \cdot \Gamma$ by $0 \cdot \Gamma := \emptyset$ and $(n+1) \cdot \Gamma := (n \cdot \Gamma) \cup \Gamma$.*

As a reminder, note that

$$\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T = \{[A_1^{\mathrm{ax}}]_T, [B_1^{\mathrm{var}}]_T, [\mathrm{cut}]_T, [\mathrm{axiom}]_T, [\mathrm{c}_{\mathrm{left}}]_T, [\mathrm{c}_{\mathrm{right}}]_T, \\ [\mathrm{refl}]_T, [\mathrm{eq}{\to}_{\mathrm{left}}]_T, [\mathrm{eq}{\to}_{\mathrm{right}}]_T, [\mathrm{eq}{\leftarrow}_{\mathrm{left}}]_T, [\mathrm{eq}{\leftarrow}_{\mathrm{right}}]_T\}.$$

Lemma 4.40. *Let $\pi \vdash_{\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T} \vdash [\Gamma]_T \longrightarrow [\Delta]_T$. Then there exists a $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed proof proof $\pi' \vdash_{\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T} [\Gamma]_T \longrightarrow [\Delta]_T$. If π is* EV*-regular, then so is π'.*

Proof. Let $\pi \vdash_{\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T} [\Gamma]_T \longrightarrow [\Delta]_T$. We proceed by induction on $V(\pi)$ with respect to $>^{\mathrm{mul}}$ (note that $>^{\mathrm{mul}}$ is well-founded by Lemma 4.35). If all elements in $V(\pi)$ are 0 we are done by Lemma 4.38 (i). Otherwise there is an uppermost subproof ρ of π such that ρ ends in a rule from $\mathcal{E}_T$ and $\#_{[B_1^{\mathrm{var}}]_T}(\rho) > 0$ is maximal in $V(\pi)$. Since $\#_{[B_1^{\mathrm{var}}]_T}(\rho) > 0$ there is a lowermost subproof ρ' of ρ that ends in $[B_1^{\mathrm{var}}]_T$. Since we chose ρ and ρ' to be uppermost and lowermost respectively we have that the inferences of subproofs strictly between ρ and ρ' are only contractions.

Now we only consider the case where ρ ends in $[\mathrm{eq}{\to}_{\mathrm{left}}]_T$. The cases where ρ ends in a different equality rule or $[\mathrm{cut}]_T$ can be argued similarly. Further we only consider the case where ρ' is a subproof of the right direct subproof of ρ. Again, the other case can be handled analogously. Now $\rho =$

$$\dfrac{\Gamma_1 \longrightarrow \Delta_1, t = u \;(\rho_1) \qquad \dfrac{\dfrac{x = \mathsf{0}, \Gamma_2, \Phi_2(t) \longrightarrow \Delta_2 \;(\rho_2) \quad x = \mathsf{s}(y), \Gamma_3, \Phi_3(t) \longrightarrow \Delta_3 \;(\rho_3)}{\Phi_2(t), \Phi_3(t), \Gamma_2, \Gamma_3 \longrightarrow \Delta_2, \Delta_3}\,[\mathrm{c}]^*_T}{\varphi(t), \Pi \longrightarrow \Lambda}\,[B_1^{\mathrm{var}}]_T}{\varphi(u), \Gamma_1, \Pi \longrightarrow \Delta_1, \Lambda}\,[\mathrm{eq}{\to}_{\mathrm{left}}]_T$$

where $\Phi_2(t)$ and $\Phi_3(t)$ are the multisets with $\mathrm{supp}(\Phi_2(t)), \mathrm{supp}(\Phi_3(t)) \subseteq \{\varphi(t)\}$ which are contracted to the $\varphi(t)$-occurrence in the right premise of the last inference of ρ.

Now for $n \leq |\Phi_2|$ we inductively define a proof

$$\rho_2^n \vdash_{\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T} x = \mathsf{0}, n \cdot \{\varphi(u)\}, (|\Phi_2| - n) \cdot \{\varphi(t)\}, \underbrace{n \cdot \Gamma_1, \Gamma_2}_{=:\Gamma^n} \longrightarrow \underbrace{n \cdot \Delta_1, \Delta_2}_{=:\Delta^n}$$

by $\rho_2^0 = \rho_2$ and $\rho_2^{n+1} =$

$$\dfrac{\Gamma_1 \longrightarrow \Delta_1, t = u \;(\rho_1) \qquad x = \mathsf{0}, n \cdot \{\varphi(u)\}, (|\Phi_2| - n) \cdot \{\varphi(t)\}, \Gamma^n \longrightarrow \Delta^n \;(\rho_2^n)}{x = \mathsf{0}, (n+1) \cdot \{\varphi(u)\}, (|\Phi_2| - n - 1) \cdot \{\varphi(t)\}, \underbrace{\Gamma_1, \Gamma^n}_{=\Gamma^{n+1}} \longrightarrow \underbrace{\Delta_1, \Delta^n}_{=\Delta^{n+1}}}\,[\mathrm{eq}{\to}_{\mathrm{left}}]_T.$$

Note that this corresponds to a repeated application of $[\mathrm{eq}{\to}_{\mathrm{left}}]_T$ with ρ_1 as the left premise and ρ_2 as the base case for the right premise. Now we set

$$\rho_2' := \rho_2^{|\Phi_2|} \vdash_{\mathcal{P}^{=}_{T} \setminus \mathcal{W}_T} x = \mathsf{0}, \Phi_2(u), |\Phi_2| \cdot \Gamma_1, \Gamma_2 \longrightarrow |\Phi_2| \cdot \Delta_1, \Delta_2.$$

It is straightforward to see that ρ_2' uses $|\Phi_2|$ many new $[\mathrm{eq}{\to_{\mathrm{left}}}]_T$-inferences.
Similarly we obtain a proof

$$\rho_3' \vdash_{\mathcal{P}_T^{=} \setminus \mathcal{W}_T} x = \mathsf{s}(y), \Phi_3(u), |\Phi_3| \cdot \Gamma_1, \Gamma_3 \longrightarrow |\Phi_3| \cdot \Delta_1, \Delta_3$$

Note that similar constructions are possible for other equality rules and $[\mathrm{cut}]_T$.
Now set $\rho' =$

$$\dfrac{\dfrac{\rho_2' \qquad \rho_3'}{\Phi_2(u), \Phi_3(u), (|\Phi_2| + |\Phi_3|) \cdot \Gamma_1, \Gamma_2, \Gamma_3 \longrightarrow (|\Phi_2| + |\Phi_3|) \cdot \Delta_1, \Delta_2, \Delta_3}\,[B_1^{\mathrm{var}}]_T}{\varphi(u), \Gamma_1, \Pi \longrightarrow \Delta_1, \Lambda}\,[\mathrm{c}]_T^*.$$

We have

$$V(\rho) = V(\rho_1) \cup V(\rho_2) \cup V(\rho_3) \cup \underbrace{\left\{1 + \#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_2) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_3)\right\}}_{:=\Pi'}$$

and

$$\begin{aligned} V(\rho') \quad = (|\Phi_2| + |\Phi_3|) \cdot V(\rho_1) \cup V(\rho_2) \cup V(\rho_3) \quad & \cup |\Phi_2| \cdot \left\{\#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_2)\right\} \\ & \cup |\Phi_3| \cdot \left\{\#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_3)\right\}. \end{aligned}$$

Now we have $V(\rho') = (V(\rho) - \Pi') \cup \Lambda'$ for $\Lambda' :=$

$$\begin{aligned} (|\Phi_2| + |\Phi_3| - 1) \cdot V(\rho_1) \cup |\Phi_2| \cdot & \left\{\#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_2)\right\} \\ \cup |\Phi_3| \cdot & \left\{\#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_3)\right\}. \end{aligned}$$

By Lemma 4.38 (ii) we get

$$\max V(\rho_1) \leq \#_{[B_1^{\mathrm{var}}]_T}(\rho_1) < 1 + \#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_2) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_3).$$

and therefore we have

$$\max \Lambda < 1 + \#_{[B_1^{\mathrm{var}}]_T}(\rho_1) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_2) + \#_{[B_1^{\mathrm{var}}]_T}(\rho_3) \in \Pi.$$

Thus $V(\rho') <^{\mathrm{mul}} V(\rho)$. Let π' be the proof where ρ is replaced by ρ' in π, then by Lemma 4.38 (iii) we get $V(\pi') <^{\mathrm{mul}} V(\pi)$. Now, by induction hypothesis there is a $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed $\mathcal{P}_T^{=} \setminus \mathcal{W}_T$-proof of $[\Gamma]_T \longrightarrow [\Delta]_T$. Note that EV-regularity is preserved in every step. □

4.3.3 Regular proofs

In this subsection we show that we can construct EV-regular and $[B_1^{\mathrm{var}}]_T$-regular proofs. First observe that we can rename free variables in $\mathcal{P}_T^{=}$-proofs:

Lemma 4.41. *Let $\pi(x) \vdash_{\mathcal{P}_T^{=}} [\Gamma(x)]_T \longrightarrow [\Delta(x)]_T$ and let $y \in V$ with $y \notin \mathrm{EV}(\pi(x))$. Then there exists a proof $\pi(y) \vdash_{\mathcal{P}_T^{=}} [\Gamma(y)]_T \longrightarrow [\Delta(y)]_T$ such that:*

(i) *If $\pi(x)$ is $\mathcal{W}_T\downarrow$-formed, so is $\pi(y)$.*

(ii) *If $\pi(x)$ is $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed, so is $\pi(y)$.*

(iii) *If $\pi(x)$ is $[B_1^{\mathrm{var}}]_T$-regular and either $y = x$ or y is not a split variable of a $[B_1^{\mathrm{var}}]_T$-inference in $\pi(x)$, then $\pi(y)$ is $[B_1^{\mathrm{var}}]_T$-regular.*

(iv) $\mathrm{EV}(\pi(y)) = \mathrm{EV}(\pi(x))$.

(v) $\#_{[B_1^{\mathrm{var}}]_T}(\pi(y)) = \#_{[B_1^{\mathrm{var}}]_T}(\pi(x))$.

Proof. We proceed by induction on π.

If $\pi(x) =$

$$\frac{}{\mathsf{s}(u(x)) = \mathsf{0} \longrightarrow}\,[A_1^{\mathrm{ax}}]_T,$$

then $\pi(y) =$

$$\frac{}{\mathsf{s}(u(y)) = \mathsf{0} \longrightarrow}\,[A_1^{\mathrm{ax}}]_T.$$

Similarly, if $\pi(x)$ ends in $[\mathrm{refl}]_T$ or $[\mathrm{axiom}]_T$.

If π ends in a contraction or a weakening we can apply the induction hypothesis to the direct subproof π' of π. We can then reapply the contraction or weakening to π' to get the desired proof.

If $\pi(x) =$

$$\frac{\begin{array}{cc}(\pi_1(x)) & (\pi_2(x)) \\ \Gamma_1(x) \longrightarrow \Delta_1(x), u(x) = v(x) & \varphi(u(x), x), \Gamma_2(x) \longrightarrow \Delta_2(x)\end{array}}{\varphi(v(x), x), \Gamma_1(x), \Gamma_2(x) \longrightarrow \Delta_1(x), \Delta_2(x)}\,[\mathrm{eq}{\rightarrow}_{\mathrm{left}}]_T,$$

then by induction hypothesis we have $\pi_1(y) \vdash_{\mathcal{P}_T^{=}} [\Gamma_1(y)]_T \longrightarrow [\Delta_1(y)]_T, [u(y) = v(y)]_T$ and $\pi_2(y) \vdash_{\mathcal{P}_T^{=}} [\varphi(u(y), y)]_T, [\Gamma_2(y)]_T \longrightarrow [\Delta_2(y)]_T$. Thus, applying $[\mathrm{eq}{\rightarrow}_{\mathrm{left}}]_T$ to $\pi_1(y)$ and $\pi_2(y)$ gives the desired result. A similar arguments works for the other equality rules and $[\mathrm{cut}]_T$.

Now consider $\pi(x) =$

$$\frac{\begin{array}{cc}(\pi_1(x)) & (\pi_2(x)) \\ z = \mathsf{0}, \Gamma_1(x) \longrightarrow \Delta_1(x) & z = \mathsf{s}(w), \Gamma_2(x) \longrightarrow \Delta_2(x)\end{array}}{\Gamma_1(x), \Gamma_2(x) \longrightarrow \Delta_1(x), \Delta_2(x)}\,[B_1^{\mathrm{var}}]_T.$$

If $z \neq x$, then by induction hypothesis we have proofs

$$\pi_1(y) \vdash_{\mathcal{P}_T^{=}} [z = \mathsf{0}]_T, [\Gamma_1(y)]_T \longrightarrow [\Delta_1(y)]_T,$$
$$\pi_2(y) \vdash_{\mathcal{P}_T^{=}} [z = \mathsf{s}(w)]_T, [\Gamma_2(y)]_T \longrightarrow [\Delta_2(y)]_T.$$

Applying $[B_1^{\mathrm{var}}]_T$ to $\pi_1(y)$ and $\pi_2(y)$ gives the desired result.

Otherwise, if $z = x$, then by induction hypothesis we have proofs

$$\pi_1(y) \vdash_{\mathcal{P}_T^{=}} [y = \mathsf{0}]_T, [\Gamma_1(y)]_T \longrightarrow [\Delta_1(y)]_T,$$
$$\pi_2(y) \vdash_{\mathcal{P}_T^{=}} [y = \mathsf{s}(w)]_T, [\Gamma_2(y)]_T \longrightarrow [\Delta_2(y)]_T$$

and we have $\pi(y) =$

$$\dfrac{\begin{matrix}(\pi_1(y)) & (\pi_2(y))\\ y = 0, \Gamma_1(y) \longrightarrow \Delta_1(y) & y = \mathsf{s}(w), \Gamma_2(y) \longrightarrow \Delta_2(y)\end{matrix}}{\Gamma_1(y), \Gamma_2(y) \longrightarrow \Delta_1(y), \Delta_2(y)}\,[B_1^{\text{var}}]_T.$$

Note that $y \neq w$ since $y \notin \text{EV}(\pi(x))$ by assumption.

Since we do not change the proof structure we have that $\pi(y)$ preserves $\mathcal{W}_T$ $\downarrow$-form and $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-form. $[B_1^{\text{var}}]_T$-regularity is preserved by the variable change, if y is not already a split variable of a $[B_1^{\text{var}}]_T$-inference in π or if $y = x$ (i.e. the proof is not changed). Also no eigenvariables are changed, therefore $\text{EV}(\pi(x)) = \text{EV}(\pi(y))$. Furthermore note that in all cases the number of $[B_1^{\text{var}}]_T$-inferences was preserved. □

Lemma 4.42. *Let $\pi \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$ and let X be a finite set of variables. Then there exist an* EV*-regular proof $\pi' \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$ such that $\text{EV}(\pi') \cap X = \emptyset$.*

Proof. We proceed by induction on π.

If π ends in an initial rule, then π has no eigenvariables and the statement follows trivially.

If π ends in a contraction or weakening we can apply the induction hypothesis to the direct subproof π' of π. We can then reapply the contraction or weakening to π' to get the desired proof.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \Delta_1, t = u & \varphi(t), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\varphi(u), \Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\,[\text{eq}{\rightarrow_{\text{left}}}]_T,$$

then by applying the induction hypothesis to π_1 and π_2 get EV-regular $\mathcal{P}_T^=$-proofs π_1' of $[\Gamma_1]_T \longrightarrow [\Delta_1]_T, [t = u]_T$ such that $X \cap \text{EV}(\pi_1) = \emptyset$ and π_2' of $[\varphi(t)]_T, [\Gamma_2]_T \longrightarrow [\Delta_2]_T$ such that $(X \cup \text{EV}(\pi_1')) \cap \text{EV}(\pi_2') = \emptyset$. Thus, applying $[\text{eq}{\rightarrow_{\text{left}}}]_T$ to π_1' and π_2' gives the desired proof. A similar argument works for the other equality rules and $[\text{cut}]_T$.

Now consider $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2(y))\\ x = 0, \Gamma_1 \longrightarrow \Delta_1 & x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\,[B_1^{\text{var}}]_T.$$

By induction hypothesis we get an EV-regular proof $\pi_1' \vdash_{\mathcal{P}_T^=} [x = 0]_T, [\Gamma_1]_T \longrightarrow [\Delta_1]_T$ such that $\text{EV}(\pi_1') \cap (X \cup \{y\}) = \emptyset$. Also by induction hypothesis we then get an EV-regular proof $\pi_2'(y) \vdash_{\mathcal{P}_T^=} [x = \mathsf{s}(y)]_T, [\Gamma_2]_T \longrightarrow [\Delta_2]_T$ such that $\text{EV}(\pi_2') \cap (X \cup \{y\} \cup \text{EV}(\pi_1')) = \emptyset$. If $y \notin X$, then applying $[B_1^{\text{var}}]_T$ to π_1' and π_2' gives the desired result. Otherwise pick a variable y' such that $y' \notin X \cup \text{EV}(\pi_1') \cup \text{EV}(\pi_2')$ and y' is not a split variable of a $[B_1^{\text{var}}]_T$-inference in $\pi_2'(y)$. By Lemma 4.41 we have that $\pi_2'(y') \vdash_{\mathcal{P}_T^=} [x = \mathsf{s}(y')]_T, [\Gamma_2]_T \longrightarrow [\Delta_2]_T$ and $\pi_2'(y')$ preserves EV-regularity. Now $\pi' =$

$$\dfrac{\begin{matrix}(\pi_1') & (\pi_2'(y'))\\ x = 0, \Gamma_1 \longrightarrow \Delta_1 & x = \mathsf{s}(y'), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\,[B_1^{\text{var}}]_T$$

is a proof with the desired properties. □

Lemma 4.43. *Let $\pi \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$ be* EV*-regular, $\mathcal{W}_T$ $\downarrow$-formed and $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formed. Then there is a $[B_1^{\text{var}}]_T$-normal proof $\pi' \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$.*

Proof. We show that we construct a $[B_1^{\text{var}}]_T$-regular proof from π while preserving EV-regularity, $\mathcal{W}_T$ $\downarrow$-formedness and $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formedness. For this we proceed by induction on $\#(\pi)$.

If π ends in an initial rule or a rule from $\mathcal{E}_T$ then π does not use $[B_1^{\text{var}}]_T$ by $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formedness and thus is trivially $[B_1^{\text{var}}]_T$-regular. If π ends in a weakening rule we can apply the induction hypothesis to the direct subproof of π and reapply the weakening rule to get the desired proof. This works similarly if π ends in a contraction rule.

Now consider $\pi =$

$$\dfrac{\begin{matrix}(\pi_1)\\ x = 0, \Gamma_1 \longrightarrow \Delta_1\end{matrix} \quad \begin{matrix}(\pi_2)\\ x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\ [B_1^{\text{var}}]_T.$$

By induction hypothesis there are $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formed, $[B_1^{\text{var}}]_T$-regular proofs

$$\pi_1' \vdash_{\mathcal{P}_T^= \setminus \mathcal{W}_T} [x = 0]_T, [\Gamma_1]_T \longrightarrow [\Delta_1]_T,$$
$$\pi_2' \vdash_{\mathcal{P}_T^= \setminus \mathcal{W}_T} [x = \mathsf{s}(y)]_T, [\Gamma_2]_T \longrightarrow [\Delta_2]_T.$$

Note that π_1' and π_2' do not use weakening, since π is $\mathcal{W}_T$ $\downarrow$-formed. We set $\pi'' =$

$$\dfrac{\begin{matrix}(\pi_1')\\ x = 0, \Gamma_1 \longrightarrow \Delta_1\end{matrix} \quad \begin{matrix}(\pi_2')\\ x = \mathsf{s}(y), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\ [B_1^{\text{var}}]_T.$$

If x is not a split variable of any $[B_1^{\text{var}}]_T$-inference that π_1' or π_2' use, then we set $\pi' = \pi''$. Now π' is still $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formed and $[B_1^{\text{var}}]_T$-regular, since the split variable x is distinct from those in π_1' and π_2'.

If x is a split variable of some $[B_1^{\text{var}}]_T$-inference that π_1' or π_2' use, then there is a subproof of π_1' or π_2' that ends in a $[B_1^{\text{var}}]_T$-inference with split variable x. Since π_1' and π_2' are $[B_1^{\text{var}}]_T$-regular, both contain at most one such subproof. Let ρ be such a subproof, i.e. $\rho =$

$$\dfrac{\begin{matrix}(\rho_1)\\ x = 0, \Pi_1 \longrightarrow \Lambda_1\end{matrix} \quad \begin{matrix}(\rho_2(z))\\ x = \mathsf{s}(z), \Pi_2 \longrightarrow \Lambda_2\end{matrix}}{\Pi_1, \Pi_2 \longrightarrow \Lambda_1, \Lambda_2}\ [B_1^{\text{var}}]_T.$$

We now show that there is a proof $\rho' \vdash_{\mathcal{P}_T^=} [\Pi_1]_T, [\Pi_2]_T \longrightarrow [\Lambda_1]_T, [\Lambda_2]_T$ such that no $[B_1^{\text{var}}]_T$-inference in ρ' has x as split variable. For this we distinguish two cases:

(i) ρ is a subproof of π_1': As a lemma we show that the conclusion of all subproofs ρ'' between π_1' and ρ contains an occurrence of $x = 0$ which is in the context of the last inference of ρ''. Then, in particular this applies to ρ. We do this by induction on the number of subproofs between π_1' and ρ: If there is one such subproof, then $\rho = \pi_1'$ and π_1' has this property. Otherwise, since π_1' is $\mathcal{W}_T$ $\downarrow$-formed and $\frac{\mathcal{E}_T}{[B_1^{\text{var}}]_T}$-formed,

all subproofs between π_1' and ρ end in $[\mathrm{c}_{\mathrm{left}}]_T$, $[\mathrm{c}_{\mathrm{right}}]_T$ or $[B_1^{\mathrm{var}}]_T$. All these rules preserve the property from the conclusion to the premises. In particular $[B_1^{\mathrm{var}}]_T$-inferences have a split variable distinct from x because of $[B_1^{\mathrm{var}}]_T$-regularity. Thus we can apply the induction hypothesis and conclude the proof of this lemma.

Now we have $x = \mathsf{0} \in \Pi_1 \cup \Pi_2$. Again, we distinguish two cases:

(a) If $x = \mathsf{0} \in \Pi_1$, we set $\rho' =$

$$\dfrac{\dfrac{(\rho_1)}{x = \mathsf{0}, \Pi_1 \longrightarrow \Lambda_1}\,[\mathrm{c}_{\mathrm{left}}]_T}{\Pi_1 \longrightarrow \Lambda_1}\,[\mathrm{w}^*]_T.$$

(b) If $x = \mathsf{0} \in \Pi_2$, we set $\rho' =$

$$\dfrac{(\rho_1)}{x = \mathsf{0}, \Pi_1 \longrightarrow \Lambda_1}\,[\mathrm{w}^*]_T.$$

(ii) ρ is a subproof of π_2': By Lemma 4.41 we can replace the variable z in ρ_2 by y (note that π is EV-regular, thus $y \notin \mathrm{EV}(\rho_2(z))$) to get a $\mathcal{W}_T\downarrow$-formed and $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed proof $\rho_2(y) \vdash_{\mathcal{P}_T} [x = \mathsf{s}(y)]_T, [\Pi_2]_T \longrightarrow [\Lambda_2]_T$. Without loss of generality $\rho_2(y)$ is $[B_1^{\mathrm{var}}]_T$-regular. Otherwise we apply the induction hypothesis to it. Similar to the previous case we can show $x = \mathsf{s}(y) \in \Pi_1 \cup \Pi_2$. Again, we have two cases:

(a) If $x = \mathsf{s}(y) \in \Pi_1$, we set $\rho' =$

$$\dfrac{(\rho_2(y))}{x = \mathsf{s}(y), \Pi_2 \longrightarrow \Lambda_2}\,[\mathrm{w}^*]_T.$$

(b) If $x = \mathsf{s}(y) \in \Pi_2$, we set $\rho' =$

$$\dfrac{\dfrac{(\rho_2(y))}{x = \mathsf{s}(y), \Pi_2 \longrightarrow \Lambda_2}\,[\mathrm{c}_{\mathrm{left}}]_T}{\Pi_2 \longrightarrow \Lambda_2}\,[\mathrm{w}^*]_T.$$

Now we replace ρ by ρ' in π'' to get a proof $\pi''' \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$. Since ρ' does not have any $[B_1^{\mathrm{var}}]_T$-inferences which have x as split variable, we have that π''' is $[B_1^{\mathrm{var}}]_T$-regular. Also note that π''' is $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed since π_1', π_2' and ρ' are. Finally we get π' by applying Lemma 4.32 to π'''. Note that EV-regularity is preserved in every step. □

Proof of Proposition 4.31. Let $\pi \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$. We apply Lemma 4.42 for $X = \emptyset$ to π to get an EV-regular proof $\pi_0 \vdash_{\mathcal{P}_T^=} [\Gamma]_T \longrightarrow [\Delta]_T$. Then by Lemma 4.33 we get $\Gamma' \subseteq \Gamma$ and $\Delta' \subseteq \Delta$ and an EV-regular proof $\pi_1 \vdash_{\mathcal{P}_T^= \setminus \mathcal{W}_T} [\Gamma']_T \longrightarrow [\Delta']_T$. With Lemma 4.40 we get an EV-regular, $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed proof $\pi_2 \vdash_{\mathcal{P}_T^= \setminus \mathcal{W}_T} [\Gamma']_T \longrightarrow [\Delta']_T$. By Lemma 4.43 we get a $[B_1^{\mathrm{var}}]_T$-normal proof $\pi_3 \vdash_{\mathcal{P}_T^=} [\Gamma']_T \longrightarrow [\Delta']_T$. Now we apply appropriate weakenings to π_3 get the desired $[B_1^{\mathrm{var}}]_T$-normal proof. □

4.4 From $[B_1^{\mathrm{var}}]_T$-normal proofs to $\mathcal{P}_T$

In this section we finally transform $[B_1^{\mathrm{var}}]_T$-normal proofs into $\mathcal{P}_T$-proofs. First we reduce this problem to the transformation of $\mathcal{P}_T^{=}$-proofs without weakening and $[B_1^{\mathrm{var}}]_T$:

Definition 4.44. *We set*

$$\begin{aligned}\mathcal{A}_1^{=} &:= \mathcal{P}_T^{=} \setminus \{[\mathrm{w}_{\mathrm{left}}]_T, [\mathrm{w}_{\mathrm{right}}]_T, [B_1^{\mathrm{var}}]_T\}\\ &= \{[A_1^{\mathrm{ax}}]_T, [\mathrm{c}_{\mathrm{left}}]_T, [\mathrm{c}_{\mathrm{right}}]_T, [\mathrm{cut}]_T, [\mathrm{eq}{\to}_{\mathrm{left}}]_T, [\mathrm{eq}{\to}_{\mathrm{right}}]_T, [\mathrm{eq}{\leftarrow}_{\mathrm{left}}]_T, [\mathrm{eq}{\leftarrow}_{\mathrm{right}}]_T\}\end{aligned}$$

We will use the following proposition now and prove it at the end of this section

Proposition 4.45. *Let $\varphi \in A(S)$ and let Γ be a multiset with $\mathrm{supp}(\Gamma) \subseteq \{\varphi\}$ such that $\mathcal{A}_1^{=} \vdash [\Gamma]_T \longrightarrow$. Then there exists a $t \in T(S)$ with $\varphi \Leftrightarrow_T \mathsf{s}(t) = \mathsf{0}$.*

The following is a completeness result for $\mathcal{P}_T$ with respect to $\mathcal{P}_T^{=}$:

Proposition 4.46. *Let $\varphi \in A(S)$ and let Γ be a multiset with $\mathrm{supp}(\Gamma) \subseteq \{\varphi\}$ such that $\mathcal{P}_T^{=} \vdash [\Gamma]_T \longrightarrow$. Then $\mathcal{P}_T \vdash [\neg\varphi]_T$.*

Proof. Let $\rho \vdash_{\mathcal{P}_T^{=}} [\Gamma]_T \longrightarrow$. By Proposition 4.31 we can assume that ρ is $[B_1^{\mathrm{var}}]_T$-normal. Now let π be the lowermost subproof of ρ which is not a weakening or contraction. Then, since ρ is $\mathcal{W}_T\downarrow$-formed, we have $\pi \vdash_{\mathcal{P}_T^{=}\setminus\mathcal{W}_T} [\Gamma']_T \longrightarrow$ for some multiset Γ' such that $\mathrm{supp}(\Gamma') \subseteq \{\varphi\}$. We proceed by induction on $\#_{[B_1^{\mathrm{var}}]_T}(\pi)$.

If π does not use $[B_1^{\mathrm{var}}]_T$, then $\pi \vdash_{\mathcal{A}_1^{=}} [\Gamma']_T \longrightarrow$. Thus, by Proposition 4.45 we have a $t \in T(S)$ such that $\varphi \Leftrightarrow_T \mathsf{s}(t) = \mathsf{0}$ and therefore $\mathcal{P}_T \vdash [\neg\varphi]_T$ by A_1^{ax}.

Otherwise, since π is $\frac{\mathcal{E}_T}{[B_1^{\mathrm{var}}]_T}$-formed we have that π ends in $[B_1^{\mathrm{var}}]_T$, i.e. $\pi =$

$$\dfrac{\begin{array}{cc}(\pi_{\mathsf{0}}(x)) & (\pi_{\mathsf{s}}(x,y))\\ x = \mathsf{0}, \Gamma_1(x) \longrightarrow & x = \mathsf{s}(y), \Gamma_2(x) \longrightarrow\end{array}}{\Gamma_1(x), \Gamma_2(x) \longrightarrow}\ [B_1^{\mathrm{var}}]_T.$$

By Lemma 4.42 we can assume that x is not an eigenvariable of π_0 or π_s. Since π is $[B_1^{\mathrm{var}}]_T$-regular we have that x is not a split variable in any $[B_1^{\mathrm{var}}]_T$-inference that π_0 or π_s use. Furthermore $y \notin \mathrm{EV}(\pi_{\mathsf{s}}(x,y))$ since π is EV-regular. Thus, by Lemma 4.25 we have proofs

$$\pi_{\mathsf{0}}(\mathsf{0}) \vdash_{\mathcal{P}_T^{=}\setminus\mathcal{W}_T} [\mathsf{0} = \mathsf{0}]_T, [\Gamma_1(\mathsf{0})]_T \longrightarrow$$

and

$$\pi_{\mathsf{s}}(\mathsf{s}(y), y) \vdash_{\mathcal{P}_T^{=}\setminus\mathcal{W}_T} [\mathsf{s}(y) = \mathsf{s}(y)]_T, [\Gamma_2(\mathsf{s}(y))]_T \longrightarrow$$

such that $\#_{[B_1^{\mathrm{var}}]_T}(\pi_{\mathsf{0}}(\mathsf{0})) = \#_{[B_1^{\mathrm{var}}]_T}(\pi_{\mathsf{0}}(x))$ and $\#_{[B_1^{\mathrm{var}}]_T}(\pi_{\mathsf{s}}(\mathsf{s}(y), y)) = \#_{[B_1^{\mathrm{var}}]_T}(\pi_{\mathsf{s}}(x,y))$. Now we have proofs $\chi_0 =$

$$\dfrac{\dfrac{}{\longrightarrow \mathsf{0} = \mathsf{0}}\ [\mathrm{refl}]_T \quad \begin{array}{c}(\pi_{\mathsf{0}}(\mathsf{0}))\\ \mathsf{0} = \mathsf{0}, \Gamma_1(\mathsf{0}) \longrightarrow\end{array}}{\Gamma_1(\mathsf{0}) \longrightarrow}\ [\mathrm{cut}]_T$$

and $\chi_{\mathsf{s}}(y) =$

$$\dfrac{\dfrac{}{\longrightarrow \mathsf{s}(y) = \mathsf{s}(y)}\,[\mathrm{refl}]_T \quad \begin{matrix}(\pi_{\mathsf{s}}(\mathsf{s}(y), y)) \\ \mathsf{s}(y) = \mathsf{s}(y), \Gamma_2(\mathsf{s}(y)) \longrightarrow\end{matrix}}{\Gamma_2(\mathsf{s}(y)) \longrightarrow}\,[\mathrm{cut}]_T.$$

By Lemma 4.41 there is a $[B_1^{\mathrm{var}}]_T$-normal proof $\chi_{\mathsf{s}}(x) \vdash_{\mathcal{P}_T^{=} \setminus \mathcal{W}_T} \Gamma_2(\mathsf{s}(x)) \longrightarrow$ such that $\chi_{\mathsf{s}}(x)$ has the same number of $[B_1^{\mathrm{var}}]_T$-inferences as $\chi_{\mathsf{s}}(y)$. Since $\#_{[B_1^{\mathrm{var}}]_T}(\chi_{\mathsf{0}}) < \#_{[B_1^{\mathrm{var}}]_T}(\pi)$ and $\#_{[B_1^{\mathrm{var}}]_T}(\chi_{\mathsf{s}}(x)) < \#_{[B_1^{\mathrm{var}}]_T}(\pi)$, we can apply the induction hypothesis to get proofs $\pi_1 \vdash_{\mathcal{P}_T} \vdash [\neg\varphi(\mathsf{0})]$ and $\pi_2 \vdash_{\mathcal{P}_T} [\neg\varphi(\mathsf{s}(x))]$. Now $\mathcal{P}_T \vdash [\neg\varphi(x)]$ by

$$\dfrac{\begin{matrix}(\pi_1) \\ [\neg\varphi(\mathsf{0})]_T\end{matrix} \quad \begin{matrix}(\pi_2) \\ [\neg\varphi(\mathsf{s}(x))]_T\end{matrix}}{[\neg\varphi(x)]_T}\,B_1^{\mathrm{var}}.$$

□

To finish the completeness proof it remains to show Proposition 4.45. For the following proofs we use some simple results about the relation $\Leftrightarrow_\Gamma$ introduced in Chapter 3.

Lemma 4.47. *Let L be a language, Γ a multiset in $A(L)$, $\varphi \in A(L)$ and $t \in T(L)$. Then $\varphi \Leftrightarrow_\Gamma t = t$ if and only if $\mathrm{LK}^{=} \vdash \Gamma \longrightarrow \varphi$.*

Proof. $\Longrightarrow$: We have $\mathrm{LK}^{=} \vdash \Gamma, t = t \longrightarrow \varphi$. Thus, by using refl and cut we get $\mathrm{LK}^{=} \vdash \Gamma \longrightarrow \varphi$.

$\Longleftarrow$: $\mathrm{LK}^{=} \vdash \Gamma, \varphi \longrightarrow t = t$ follows from refl and weakenings. $\mathrm{LK}^{=} \vdash \Gamma, t = t \longrightarrow \varphi$ follows by using the assumption and one $\mathrm{w}_{\mathrm{left}}$. □

Lemma 4.48. *Let L be a language, $\Gamma \subseteq \Pi$ multisets of L-formulas and $\varphi, \psi \in A(L)$. If $\varphi \Leftrightarrow_\Gamma \psi$, then $\varphi \Leftrightarrow_\Pi \psi$.*

Proof. Follows immediately by using weakenings. □

Lemma 4.49. *Let L be a language, Γ a multiset in $F(L)$, $\varphi(x) \in A(L)$, $t, u \in T(L)$ and $\pi \vdash_{\mathrm{LK}^{=}} \Gamma \longrightarrow t = u$. Then $\varphi(t) \Leftrightarrow_\Gamma \varphi(u)$.*

Proof. $\mathrm{LK}^{=} \vdash \Gamma, \varphi(t) \longrightarrow \varphi(u)$ follows by

$$\dfrac{\begin{matrix}(\pi) \\ \Gamma \longrightarrow t = u\end{matrix} \quad \dfrac{}{\varphi(t) \longrightarrow \varphi(t)}\,\begin{matrix}\mathrm{axiom} \\ \mathrm{eq}{\rightarrow}_{\mathrm{right}}\end{matrix}}{\Gamma, \varphi(t) \longrightarrow \varphi(u)}$$

and $\mathrm{LK}^{=} \vdash \Gamma, \varphi(u) \longrightarrow \varphi(t)$ follows similarly by using $\varphi(u)$ in axiom and $\mathrm{eq}{\leftarrow}_{\mathrm{right}}$. □

Lemma 4.50. *Let $\varphi \in F(S)$, let Γ be a multiset in $F(S)$ and let $\psi \in \Gamma \cup \{\mathsf{0} = \mathsf{0}\}$ such that $\varphi \Leftrightarrow_{\Gamma - \{\psi\}} \psi$. Then $\mathrm{LK}^{=} \vdash \Gamma \longrightarrow \varphi$.*

Proof. We distinguish two cases:

(i) $\psi \in \Gamma$: Then $\mathrm{LK}^{=} \vdash \Gamma - \{\psi\}, \psi \longrightarrow \varphi$, i.e. $\mathrm{LK}^{=} \vdash \Gamma \longrightarrow \varphi$.

(ii) $\psi \equiv \mathsf{0} = \mathsf{0}$: Then $\mathrm{LK}^{=} \vdash \Gamma - \{\mathsf{0} = \mathsf{0}\}, \mathsf{0} = \mathsf{0} \longrightarrow \varphi$. Since $\mathrm{LK}^{=} \vdash \longrightarrow \mathsf{0} = \mathsf{0}$ by using a cut and, if $\mathsf{0} = \mathsf{0} \in \Gamma$, using a weakening we get $\mathrm{LK}^{=} \vdash \Gamma \longrightarrow \varphi$.

□

Lemma 4.51. *Let Γ, Δ be multisets in $A(S)$ and $\pi \vdash_{\mathcal{A}_1^{=}} [\Gamma]_T \longrightarrow [\Delta]_T$. Then $[\Delta]_T$ has at most one element and π does not use $[\mathrm{c}_{\mathrm{right}}]_T$.*

Proof. We show the statement by induction on π. Clearly the statement holds for the initial sequents. If π ends in $[\mathrm{c}_{\mathrm{left}}]_T$ then the statement follows by applying the induction hypothesis to the direct subproof. Note that π cannot end in $[\mathrm{c}_{\mathrm{right}}]_T$: If it did, then by induction hypothesis the succeedent of the direct subproof of π can have at most one element which means that $[\mathrm{c}_{\mathrm{right}}]_T$ cannot be applied.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \Delta_1, \psi & \chi, \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\ [\mathrm{cut}]_T,$$

with $\psi \Leftrightarrow_T \chi$, then by induction hypothesis we have $\Delta_1 = \emptyset$ and Δ_2 has at most one element and π does not use $[\mathrm{c}_{\mathrm{right}}]_T$. Thus Δ has at most one element.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \Delta_1, t = u & \psi(t), \Gamma_2 \longrightarrow \Delta_2\end{matrix}}{\psi(u), \Gamma_1, \Gamma_2 \longrightarrow \Delta_1, \Delta_2}\ [\mathrm{eq}{\rightarrow}_{\mathrm{left}}]_T,$$

then by induction hypothesis we have that Δ_1 is empty, Δ_2 has at most one element and π does not use $[\mathrm{c}_{\mathrm{right}}]_T$. Thus Δ has at most one element.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \Delta_1, t = u & \Gamma_2 \longrightarrow \psi(t), \Delta_2\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \psi(u), \Delta_1, \Delta_2}\ [\mathrm{eq}{\rightarrow}_{\mathrm{right}}]_T,$$

then by induction hypothesis we have that Δ_1 and Δ_2 are empty and π does not use $[\mathrm{c}_{\mathrm{right}}]_T$. Thus, Δ has at most one element. A similar argument works for the cases where π ends in other equality rules. □

Lemma 4.52. *Let Γ be a multiset in $A(S)$ and $\varphi \in A(S)$. If $\mathcal{A}_1^{=} \vdash [\Gamma]_T \longrightarrow [\varphi]_T$, then there exists a $\psi \in \Gamma \cup \{\mathsf{0} = \mathsf{0}\}$ such that $\varphi \Leftrightarrow_{T \cup \Gamma - \{\psi\}} \psi$.*

Proof. Let $\pi \vdash_{\mathcal{A}_1^{=}} [\Gamma]_T \longrightarrow [\varphi]_T$. We show the statement by induction on π.

If π ends in $[\mathrm{refl}]_T$, then $\varphi \Leftrightarrow_T t = t$ for some $t \in T(S)$. By Lemma 4.47 we then have $\varphi \Leftrightarrow_T \mathsf{0} = \mathsf{0}$.

If π ends in $[\mathrm{axiom}]_T$, then we have $\Gamma = \{\chi\}$ and $\chi \Leftrightarrow_T \varphi$, therefore the statement follows.

π cannot end in $[A_1^{\mathrm{ax}}]_T$, since the succeedent of the conclusion of π is not empty.

By Lemma 4.51 we have that π does not use $[\mathrm{c}_{\mathrm{right}}]_T$. If π ends in $[\mathrm{c}_{\mathrm{left}}]_T$, then the statement follows by applying the induction hypothesis to the direct subproof of π.

Now consider the case where π ends in cut. By Lemma 4.51 we have that the left premise of the last cut-inference has at most one element in the suceedent. This must be the cut formula. Therefore φ can only occur in the right premise. Thus, $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \chi_1 & \chi_2, \Gamma_2 \longrightarrow \varphi\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \varphi}\ [\text{cut}]_T$$

with $\chi_1 \Leftrightarrow_T \chi_2$. We apply the induction hypothesis to π_1 and π_2 to get a $\psi_1 \in \Gamma_1 \cup \{0 = 0\}$ with $\chi_1 \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$ and a $\psi_2 \in \Gamma_2 \cup \{\chi_2, 0 = 0\}$ with $\varphi \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi_2\} - \{\psi_2\}} \psi_2$. By Lemma 4.50 we get $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow \chi_1$. From $\chi_1 \Leftrightarrow_T \chi_2$ we now get $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow \chi_2$ by using a cut and contractions. We further distinguish two cases:

(i) $\psi_2 \neq \chi_2$: Then we have $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow \chi_2$ and $\varphi \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi_2\} - \{\psi_2\}} \psi_2$. Thus we get $\mathrm{LK}^{=} \vdash T, \Gamma - \{\psi_2\}, \psi_2 \longrightarrow \varphi$ and $\mathrm{LK}^{=} \vdash T, \Gamma - \{\psi_2\}, \varphi \longrightarrow \psi_2$ by introducing appropriate cuts and contractions. Therefore we have $\varphi \Leftrightarrow_{T \cup \Gamma - \{\psi_2\}} \psi_2$.

(ii) $\psi_2 = \chi_2$: Then $\varphi \Leftrightarrow_{T \cup \Gamma_2} \chi_2 \Leftrightarrow_T \chi_1 \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$. By using Lemma 4.48 we get $\varphi \Leftrightarrow_{T \cup \Gamma - \{\psi_1\}} \psi_1$.

Now consider the case where π ends in an equality rule. Note that φ cannot be in the succedent of the left premise since the auxiliary equality is already in the succeedent and by Lemma 4.51 there can be at most one formula in the succeedent. We first consider the case where π ends in $[\text{eq}{\rightarrow_{\text{left}}}]_T$. Thus, $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow t = u & \chi(t), \Gamma_2 \longrightarrow \varphi\end{matrix}}{\chi(u), \Gamma_1, \Gamma_2 \longrightarrow \varphi}\ [\text{eq}{\rightarrow_{\text{left}}}]_T.$$

We apply the induction hypothesis to π_1 and π_2 to get a $\psi_1 \in \Gamma_1 \cup \{0 = 0\}$ such that $t = u \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$ and a $\psi_2 \in \Gamma_2 \cup \{\chi(t), 0 = 0\}$ such that $\varphi \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi(t)\} - \{\psi_2\}} \psi_2$. By Lemma 4.50 we get $\mathrm{LK}^{=} \vdash \Gamma_1 \longrightarrow t = u$. We now distinguish two cases:

(i) $\psi_2 \neq \chi(t)$: Using Lemma 4.49 we get $\mathrm{LK}^{=} \vdash \Gamma_1, \chi(u) \longrightarrow \chi(t)$. Also, since $\varphi \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi(t)\} - \{\psi_2\}} \psi_2$ we get $\mathrm{LK}^{=} \vdash T, \Gamma - \{\psi_2\}, \chi(u), \psi_2 \longrightarrow \varphi$ as well as $\mathrm{LK}^{=} \vdash T, \Gamma - \{\psi_2\}, \chi(u), \varphi \longrightarrow \psi_2$ by introducing appropriate cuts and contractions. Therefore we have $\varphi \Leftrightarrow_{T \cup \Gamma - \{\psi_2\}} \psi_2$.

(ii) $\psi_2(t) = \chi(t)$: Then we have $\psi_2(t) \Leftrightarrow_{T \cup \Gamma_1} \psi_2(u)$ by Lemma 4.49 and thus we get $\varphi \Leftrightarrow_{T \cup \Gamma - \{\psi_2(u)\}} \psi_2(u) \in \Gamma_2(u)$ by Lemma 3.5.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow t = u & \Gamma_2 \longrightarrow \varphi(t)\end{matrix}}{\Gamma_1, \Gamma_2 \longrightarrow \varphi(u)}\ [\text{eq}{\rightarrow_{\text{right}}}]_T,$$

i.e. φ is the principal equality, then again by induction hypothesis we get a $\psi \in \Gamma_2 \cup \{0 = 0\}$ such that $\varphi(t) \Leftrightarrow_{T \cup \Gamma_2 - \{\psi\}} \psi$. We also have $\varphi(u) \Leftrightarrow_{T \cup \Gamma_1} \varphi(t)$ by Lemma 4.49 and thus $\varphi(u) \Leftrightarrow_{T \cup \Gamma - \{\psi\}} \psi$ by Lemma 4.48. The cases where π ends in $[\text{eq}{\leftarrow_{\text{left}}}]_T$ or $[\text{eq}{\leftarrow_{\text{right}}}]$ can be proven analogously. □

Lemma 4.53. *Let Γ be a multiset in $A(S)$. If $\mathcal{A}_1^{=} \vdash [\Gamma]_T \longrightarrow$, then there exist $\psi \in \Gamma$ and $t \in T(S)$ such that $\psi \Leftrightarrow_{T \cup \Gamma - \{\psi\}} \mathsf{s}(t) = 0$.*

Proof. Let $\pi \vdash_{\mathcal{A}_1^{=}} [\Gamma]_T \longrightarrow$. We show the statement by induction on π. Note that π cannot end in $[\mathrm{refl}]_T$ or $[\mathrm{axiom}]_T$ since the conclusion of π has an empty succeedent.

If π ends in $[A_1^{\mathrm{ax}}]_T$, then $[\Gamma]_T = \{[\mathsf{s}(t) = 0]_T\}$ for some $t \in T(S)$. Thus the statement follows for $\psi \equiv \mathsf{s}(t) = 0$.

By Lemma 4.51 π cannot end in $[\mathrm{c}_{\mathrm{right}}]$. If π ends in $[\mathrm{c}_{\mathrm{left}}]_T$, then the statement can be proven by applying the induction hypothesis to the direct subproof of π.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow \chi_1 & \chi_2, \Gamma_2 \longrightarrow\end{matrix}}{\Gamma \longrightarrow}\,[\mathrm{cut}]_T$$

with $\chi_1 \Leftrightarrow_T \chi_2$, then by applying the induction hypothesis to π_2 we get a $\psi_2 \in \Gamma_2 \cup \{\chi_2\}$ and a $t \in T(S)$ such that $\psi_2 \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi_2\} - \{\psi_2\}} \mathsf{s}(t) = 0$. By applying Lemma 4.52 to the conclusion of π_1 we then get a $\psi_1 \in \Gamma_1$ such that $\chi_1 \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$. We now distinguish two cases:

(i) $\psi_2 \in \Gamma_2$: We have $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow \chi_1$ by $\chi_1 \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$. By $\chi_1 \Leftrightarrow_T \chi_2$ we get $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow \chi_2$. From $\psi_2 \Leftrightarrow_{T \cup \Gamma_2 \cup \{\chi_2\} - \{\psi_2\}} \mathsf{s}(t) = 0$ we now get $\psi_2 \Leftrightarrow_{T \cup \Gamma - \{\psi_2\}} \mathsf{s}(t) = 0$ by introducing appropriate cuts and contractions.

(ii) $\psi_2 = \chi_2$: We have $\psi_2 \Leftrightarrow_{T \cup \Gamma_2} \mathsf{s}(t) = 0$. Thus we get

$$\psi_1 \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \chi_1 \Leftrightarrow_T \chi_2 = \psi_2 \Leftrightarrow_{T \cup \Gamma_2} \mathsf{s}(t) = 0$$

and in total $\psi_1 \Leftrightarrow_{T \cup \Gamma - \{\psi_1\}} \mathsf{s}(t) = 0$.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ \Gamma_1 \longrightarrow u = v & \Gamma_2, \varphi(u) \longrightarrow\end{matrix}}{\Gamma_1, \Gamma_2, \varphi(v) \longrightarrow}\,[\mathrm{eq}{\rightarrow}_{\mathrm{left}}]_T,$$

then by applying the induction hypothesis to π_2 we get a $\psi_2 \in \Gamma_2 \cup \{\varphi(u)\}$ and a $t \in T(S)$ such that $\psi_2 \Leftrightarrow_{T \cup \Gamma_2 \cup \{\varphi(u)\} - \{\psi_2\}} \mathsf{s}(t) = 0$. By applying Lemma 4.52 to the conclusion of π_1 we then get a $\psi_1 \in \Gamma_1$ such that $u = v \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$. We now distinguish two cases:

(i) $\psi_2 \in \Gamma_2$: We have $\mathrm{LK}^{=} \vdash T, \Gamma_1 \longrightarrow u = v$ by $u = v \Leftrightarrow_{T \cup \Gamma_1 - \{\psi_1\}} \psi_1$. By Lemma 4.49 we get $\varphi(v) \Leftrightarrow_{T \cup \Gamma_1} \varphi(u)$ and in particular $\mathrm{LK}^{=} \vdash T, \Gamma_1, \varphi(v) \longrightarrow \varphi(u)$. From $\psi_2 \Leftrightarrow_{T \cup \Gamma_2 \cup \{\varphi(u)\} - \{\psi_2\}} \mathsf{s}(t) = 0$ we now get $\psi_2 \Leftrightarrow_{T \cup \Gamma - \{\psi_2\}} \mathsf{s}(t) = 0$ by introducing appropriate cuts and contractions.

(ii) $\psi_2 = \varphi(u)$: Now $\psi_2 \Leftrightarrow_{T \cup \Gamma_2} \mathsf{s}(t) = 0$.

By Lemma 4.49 we have $\varphi(u) \Leftrightarrow_{T \cup \Gamma_1} \varphi(t)$. Thus $\varphi(u) \Leftrightarrow_{T \cup \Gamma - \{\varphi(u)\}} \mathsf{s}(t) = 0$.

□

Lemma 4.54. *Let $t \in T(S)$. Then $T \not\vdash 0 = 0 \longrightarrow \mathsf{s}(t) = 0$*

Proof. $\mathbb{N} \models T$ and $\mathbb{N} \models \mathsf{0} = \mathsf{0}$, but $\mathbb{N} \not\models \mathsf{s}(t) = \mathsf{0}$ for any $t \in T(S)$. □

Proposition 4.55 (consistency of $\mathcal{A}_1^=$)**.** $\mathcal{P}_T^= \not\vdash \longrightarrow$.

Proof. Assume $\pi \vdash_{\mathcal{A}_1^=} \longrightarrow$. Then π can only end in $[\mathrm{cut}]_T$ since all other rules in $\mathcal{A}_1^=$ have at least one element in the conclusion. Therefore $\pi =$

$$\dfrac{\dfrac{(\pi_1)}{\longrightarrow \varphi} \quad \dfrac{(\pi_2)}{\psi \longrightarrow}}{\longrightarrow}\,[\mathrm{cut}]_T$$

with $\varphi \Leftrightarrow_T \psi$. By Lemma 4.52 we have $\varphi \Leftrightarrow_T \mathsf{0} = \mathsf{0}$ and by Lemma 4.53 we have $\psi \Leftrightarrow_T \mathsf{s}(t) = \mathsf{0}$ for some $t \in T(S)$. Thus $\mathsf{0} = \mathsf{0} \Leftrightarrow_T \mathsf{s}(t) = \mathsf{0}$ which is a contradiction to Lemma 4.54 □

Proof of Proposition 4.45. By Proposition 4.55 we have that Γ is not empty. Now let π be an $\mathcal{A}_1^=$-proof of $[\Gamma]_T \longrightarrow$. Since $\mathrm{supp}(\Gamma) = \{\varphi\}$ we get $\mathcal{A}_1^= \vdash [\varphi]_T \longrightarrow$ by applying contractions. Now the statement follows from Lemma 4.53. □

With this we can conclude the completeness proof for $\mathcal{P}_T$:

Proof of Theorem 3.10. Let $AB \vdash \neg\varphi$. By Lemma 4.4 we have $AB \vdash \varphi \longrightarrow$. From Proposition 4.6 we get $\mathrm{LK}\mathcal{P}_T^= \vdash T, \varphi \longrightarrow$. Using Proposition 4.21 gives us $\mathcal{P}_T^= \vdash [\varphi]_T \longrightarrow$. Finally, by Proposition 4.46 we have $\mathcal{P}_T \vdash [\neg\varphi]_T$. □

5 Decidability

The goal for this chapter is to show the decidability of ${\mathcal{P}_T}^{\vdash}$. To do this, we first observe a correspondence between polynomials with coefficients in $\mathbb{N}$ and $T(S)$. We then introduce an order on polynomials as well as a normal form for polynomial equations. Finally we show a necessary condition for $\mathcal{P}_T$-provability and use this to formulate a decision procedure for ${\mathcal{P}_T}^{\vdash}$.

5.1 A polynomial normal form

The goal for this section is to show a correspondence between $T(S)$ and the polynomials with coefficients in $\mathbb{N}$ with variables as indeterminates.

Definition 5.1. *By $\mathbb{N}[V]$ we denote the set of polynomials with coefficients in $\mathbb{N}$ and indeterminates in V (i.e. the variables). A* polynomial *p is an element of $\mathbb{N}[V]$. A* monomial *m is a polynomial such that exactly one coefficient is 1 and the others are 0. The set of monomials is denoted by $M[V]$. Note that every monomial m can be identified by the finite multiset of variables $\mathrm{vars}(m) : V \to \mathbb{N} : x \mapsto$ exponent of x in m. The monomial m with $\mathrm{vars}(m) = \emptyset$ corresponds to the constant monomial and is also denoted by 1. Every polynomial p can be identified by the finite multiset of monomials $\mathrm{mons}(p) : M[V] \to \mathbb{N} : m \mapsto [m]p$ where $[m]p$ denotes the coefficient of m in p. We say m* is a monomial of *p if $[m]p > 0$. We define $<_V$ to be the strict total order on V, defined by $\mathsf{x}_n <_V \mathsf{x}_m$ if and only if $n < m$. We define $<_{M[V]}$ to be the strict total order on $M[V]$ defined by $m_1 <_{M[V]} m_2$ if and only if $\mathrm{vars}(m_1) <_V^{\mathrm{mul}} \mathrm{vars}(m_2)$, where $<_V^{\mathrm{mul}}$ denotes the multiset order with respect to $<_V$. We define the* set variables of *p by $\mathrm{v}(p) := \bigcup_{m \in \mathrm{mons}(p)} \mathrm{supp}(\mathrm{vars}(m))$. By abuse of notation we sometimes write $\mathrm{v}(p)$ for the tuple of pairwise distinct variables $(x_1, \ldots, x_n)$ such that $\mathrm{v}(p) = \{x_1, \ldots, x_n\}$ and $x_1 <_V \ldots <_V x_n$.*

It seems unusual to identify polynomials with a multiset of monomials where the multiplicity of each monomial is given by the coefficient of the monomial in the respective polynomial, but it works nicely together with a multiset order we use later on.

Lemma 5.2. *$<_{M[V]}$ is a strict total order.*

Proof. See [1] Lemma 2.5.4. □

There is a correspondence between $T(S)$ and $\mathbb{N}[V]$:

Definition 5.3. $\mathrm{poly} : T(S) \to \mathbb{N}[V]$ *is the computable function recursively defined by the following procedure:*

Let $t \in T(S)$.

If $t \equiv x$ for a variable x, then $\mathrm{poly}(t) = x$.

If $t \equiv \mathsf{0}$, then $\mathrm{poly}(t) = 0$.

If $t \equiv \mathsf{s}(u)$ for some $u \in T(S)$, then $\mathrm{poly}(t) = \mathrm{poly}(u) + 1$.

If $t \equiv u + v$ for some $u, v \in T(S)$, then $\mathrm{poly}(t) = \mathrm{poly}(u) + \mathrm{poly}(v)$.

If $t \equiv u \cdot v$ for some $u, v \in T(S)$, then $\mathrm{poly}(t) = \mathrm{poly}(u) \cdot \mathrm{poly}(v)$.

Definition 5.4. *For $n \in \mathbb{N}$ and $t_1, \ldots, t_n \in T(S)$ we inductively define the terms $\sum_{i=1}^{n} t_i$ and $\prod_{i=1}^{n} t$ by*

$$\sum_{i=1}^{0} t_i :\equiv \mathsf{0}, \quad \sum_{i=1}^{n+1} t_i :\equiv t_1 + \sum_{i=1}^{n} t_{i+1},$$

$$\prod_{i=1}^{0} t_i :\equiv \underline{1}, \quad \prod_{i=1}^{n+1} t_i :\equiv t_1 \cdot \prod_{i=1}^{n} t_{i+1}.$$

Definition 5.5. *Let $m \in M[V]$. Then the term $\underline{m} \in T(S)$ is defined by $\prod_{i=1}^{n} x_i$ where $\{x_1, \ldots, x_n\} = \mathrm{vars}(m)$ and $x_1 \leq_V \cdots \leq_V x_n$. Let $p \in \mathbb{N}[V]$, then the term $\underline{p}$ is defined by $\sum_{i=1}^{n} \underline{m_i}$ where $\{m_1, \ldots, m_n\} = \mathrm{mons}(p)$ and $m_1 \leq_{M[V]} \cdots \leq_{M[V]} m_n$.*

Lemma 5.6. *Let $t \in T(S)$. Then $T \vdash \mathsf{s}(t) = \mathsf{s}(\mathsf{0}) + t$.*

Proof. Work in T:

$$\mathsf{s}(\mathsf{0}) + t \overset{B_2}{=} t + \mathsf{s}(\mathsf{0}) \overset{A_5}{=} \mathsf{s}(t + \mathsf{0}) \overset{A_4}{=} \mathsf{s}(t).$$

□

Lemma 5.7. *Let $t, u \in T(S)$. Then $T \vdash \underline{\mathrm{poly}(t)} + \underline{\mathrm{poly}(u)} = \underline{\mathrm{poly}(t) + \mathrm{poly}(u)}$ and $T \vdash \underline{\mathrm{poly}(t)} \cdot \underline{\mathrm{poly}(u)} = \underline{\mathrm{poly}(t) \cdot \mathrm{poly}(u)}$.*

Proof sketch. Since T contains commutativity and associativity laws for $+$ and $\cdot$ and a distributivity law (B_2, B_3, B_5, B_6 and B_7), it can be shown that sums and products can be rearranged in T. □

The following lemma shows that $t \mapsto \underline{\mathrm{poly}(t)}$ acts as a normal form for S-terms:

Lemma 5.8. *Let $t \in T(S)$. Then $T \vdash \underline{\mathrm{poly}(t)} = t$.*

Proof. We proceed by induction on t.

If $t \equiv \mathsf{0}$, then $\mathrm{poly}(t) = 0$ and $\underline{0} = \mathsf{0}$, thus the statement holds.

If we have $t \equiv \mathsf{s}(u)$ for some $u \in T(S)$, then we have $\mathrm{poly}(t) = \mathrm{poly}(u) + 1$ as well as $\underline{\mathrm{poly}(u) + 1} = \mathsf{s}(\mathsf{0}) + \underline{\mathrm{poly}(u)}$. We then have $T \vdash \underline{\mathrm{poly}(t)} = \mathsf{s}(\underline{\mathrm{poly}(u)})$ by Lemma 5.6. Using the induction hypothesis we get $T \vdash \underline{\mathrm{poly}(t)} = t$.

If $t \equiv u + v$ for some $u, v \in T(S)$, then by induction hypothesis we get $T \vdash \underline{\mathrm{poly}(u)} = u$ and $T \vdash \underline{\mathrm{poly}(v)} = v$. Thus $T \vdash \underline{\mathrm{poly}(u)} + \underline{\mathrm{poly}(v)} = t$. By Lemma 5.7 we have $T \vdash \underline{\mathrm{poly}(u)} + \underline{\mathrm{poly}(v)} = \underline{\mathrm{poly}(t)}$ and thus $T \vdash \underline{\mathrm{poly}(t)} = t$.

If $t \equiv u \cdot v$ for some $u, v \in T(S)$, then by induction hypothesis we have $T \vdash \underline{\mathrm{poly}(u)} = u$ and $T \vdash \underline{\mathrm{poly}(v)} = v$. Thus $T \vdash \underline{\mathrm{poly}(u)} \cdot \underline{\mathrm{poly}(v)} = t$. Using Lemma 5.7 we get $T \vdash \underline{\mathrm{poly}(u)} \cdot \underline{\mathrm{poly}(v)} = \underline{\mathrm{poly}(t)}$ and thus $T \vdash \underline{\mathrm{poly}(t)} = t$. □

Definition 5.9. *Let $p \in \mathbb{N}\{x_1, \ldots, x_n\}$, let $x_1, \ldots, x_n$ be pairwise distinct variables and let $\underline{p} = \underline{p}(x_1, \ldots, x_n)$. Then p induces a function $p : T(S)^n \to \mathbb{N}[V] : (t_1, \ldots, t_n) \mapsto \mathrm{poly}(\underline{p}(t_1, \ldots, t_n))$.*

Lemma 5.10. *Let $p \in \mathbb{N}[V]$, let $x_1, \ldots, x_n$ be pairwise distinct variables, let $t_1, \ldots, t_n \in T(S)$ and let $\underline{p} = \underline{p}(x_1, \ldots, x_n)$. Then $T \vdash \underline{p(t_1, \ldots, t_n)} = \underline{p}(t_1, \ldots, t_n)$.*

Proof. Note that $p(t_1, \ldots, t_n) = \mathrm{poly}(\underline{p}(t_1, \ldots, t_n))$. Thus the statement follows by Lemma 5.8. □

5.2 A polynomial order

The following definition will allow us to formulate a necessary condition for provability in $\mathcal{P}_T$.

Definition 5.11. *Let $m_1, m_2 \in M[V]$ and $p, q \in \mathbb{N}[V]$. We write $m_1 <_{\mathrm{mon}} m_2$ if m_1 strictly divides m_2, i.e. if $\mathrm{vars}(m_1) \subsetneq \mathrm{vars}(m_2)$. Note that $<_{\mathrm{mon}}$ is a strict partial order. We say m_1* is a maximal monomial of *p if m_1 is maximal in $\mathrm{mons}(p)$ with respect to $<_{\mathrm{mon}}$. The multiset of maximal monomials in p is denoted by $\mathrm{maxmons}(p)$. We write $p <_{\mathrm{mon}} q$ if $\mathrm{mons}(p) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{mons}(q)$. We say p* and *q* are strictly monomially comparable (in symbols: $p \lesseqgtr_{\mathrm{mon}} q$) if either $p <_{\mathrm{mon}} q$ or $q <_{\mathrm{mon}} p$.*

We now study this monomial order in more detail.

Lemma 5.12. *$<_{\mathrm{mon}}$ is a well-founded strict partial order on $\mathbb{N}[V]$.*

Proof. It is well-known that $<_{\mathrm{mon}}$ is a well-founded strict partial order on $M[V]$. The corresponding multiset order $<^{\mathrm{mul}}_{\mathrm{mon}}$ is a well-founded strict partial order (see [1] Lemmas 2.5.4 and 2.5.5). Thus $<_{\mathrm{mon}}$ is a well-founded strict partial order on $\mathbb{N}[V]$. □

Lemma 5.13. *Let $p, q \in \mathbb{N}[V]$ with $p <_{\mathrm{mon}} q$. If $\mathrm{mons}(p) \cap \mathrm{mons}(q) = \emptyset$, then for all $x \in \mathrm{mons}(p)$ there is a $y \in \mathrm{maxmons}(q)$ such that $x <_{\mathrm{mon}} y$.*

Proof. Since $p <_{\mathrm{mon}} q$ there are $\emptyset \neq \Pi \subseteq \mathrm{mons}(q)$ and Λ with $\mathrm{mons}(p) = (\mathrm{mons}(q) - \Pi) \cup \Lambda$ such that for all $x \in \Lambda$ there exists a $y \in \Pi$ such that $x <_{\mathrm{mon}} y$. Since $\mathrm{mons}(p) \cap \mathrm{mons}(q) = \emptyset$ we have $\Pi = \mathrm{mons}(q)$ and therefore $\Lambda = \mathrm{mons}(p)$. Now for all $x \in \mathrm{mons}(p)$ there is a $y \in \mathrm{mons}(q)$ such that $x <_{\mathrm{mon}} y$. If y is not maximal in $\mathrm{mons}(q)$, then there exists a $y' \in \mathrm{maxmons}(q)$ with $y <_{\mathrm{mon}} y'$ and by extension $x <_{\mathrm{mon}} y'$. Thus the statement follows. □

Lemma 5.14. *Let $p, q \in \mathbb{N}[V]$ with $\mathrm{maxmons}(p) \cap \mathrm{maxmons}(q) = \emptyset$. Then $p <_{\mathrm{mon}} q$ if and only if $\mathrm{maxmons}(p) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{maxmons}(q)$.*

Proof. $\Longrightarrow$: By assumption there are multisets $\emptyset \neq \Pi \subseteq \mathrm{mons}(q)$ and $\Lambda \subseteq \mathrm{mons}(p)$ with $\mathrm{mons}(p) = (\mathrm{mons}(q) - \Pi) \cup \Lambda$ such that for all $x \in \Lambda$ there exists a $y \in \Pi$ such that $x <_{\mathrm{mon}} y$. Now let $x \in \mathrm{maxmons}(p)$. Then either $x \in \Lambda$ or $x \in \mathrm{mons}(q)$. We show in both cases that there is a $y' \in \mathrm{maxmons}(q)$ such that $x <_{\mathrm{mon}} y'$. If $x \in \Lambda$, there is a $y \in \Pi \subseteq \mathrm{mons}(q)$ such that $x <_{\mathrm{mon}} y$ and therefore there is a $y' \in \mathrm{maxmons}(q)$ such that

$x <_{\text{mon}} y'$. If $x \in \text{mons}(q)$, then $x \notin \text{maxmons}(q)$ since $\text{maxmons}(p) \cap \text{maxmons}(q) = \emptyset$. Thus, there is a $y' \in \text{maxmons}(q)$ such that $x <_{\text{mon}} y'$. Therefore we have

$$\text{maxmons}(p) = (\text{maxmons}(q) - \text{maxmons}(q)) \cup \text{maxmons}(p)$$

and for all $x \in \text{maxmons}(p)$ there is a $y' \in \text{maxmons}(q)$ with $x <_{\text{mon}} y$, which means $\text{maxmons}(p) <_{\text{mon}}^{\text{mul}} \text{maxmons}(q)$.

$\Longleftarrow$: By assumption there are multisets $\emptyset \neq \Pi \subseteq \text{maxmons}(q)$ and Λ such that $\text{maxmons}(p) = (\text{maxmons}(q) - \Pi) \cup \Lambda$ and for all $x \in \Lambda$ there exists a $y \in \Pi$ such that $x <_{\text{mon}} y$. Since $\text{maxmons}(p)$ and $\text{maxmons}(q)$ are disjoint we have $\Pi = \text{maxmons}(q)$ and $\Lambda = \text{maxmons}(p)$. Thus, for all $x \in \text{maxmons}(p)$, there is a $y \in \text{maxmons}(q)$ such that $x <_{\text{mon}} y$. Now let $x \in \text{mons}(p)$. Then there exists a $x' \in \text{maxmons}(p)$ and a $y' \in \text{maxmons}(q)$ such that $x \leq_{\text{mon}} x' <_{\text{mon}} y'$. Therefore with $\Pi = \text{mons}(q)$, $\Lambda = \text{mons}(p)$ we get $\text{mons}(p) = (\text{mons}(q) - \Pi) \cup \Lambda$ which means $\text{mons}(p) <_{\text{mon}}^{\text{mul}} \text{mons}(q)$. □

Lemma 5.15. *Let m be a monomial, let $x_1, \ldots, x_k$ be pairwise distinct variables and set $\mathsf{s}(\bar{x}) := (\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$. Further let m_0 be a monomial of $m(\mathsf{s}(\bar{x}))$ with $m_0 \neq m$. Then we have $m_0 <_{\text{mon}} m$ and as a consequence*

$$\text{maxmons}(m(\mathsf{s}(\bar{x}))) = \{m\}\,.$$

Proof. Let $X := \{x_1, \ldots, x_k\}$. Note that we have

$$m(\mathsf{s}(\bar{x})) = \prod_{\substack{x \in \text{vars}(m) \\ x \in X}} (x+1) \cdot \prod_{\substack{x \in \text{vars}(m) \\ x \notin X}} x.$$

Distributing out this product shows that every monomial of $m(\mathsf{s}(\bar{x}))$ has the form $\prod_{x \in X_m} x$ for some $X_m \subseteq \text{vars}(m)$, i.e. every monomial of $m(\mathsf{s}(\bar{x}))$ divides m. By assumption we have $m_0 \neq m$ and thus $m_0 <_{\text{mon}} m$. Since $m \in \text{mons}(m(\mathsf{s}(\bar{x})))$ it follows that $\text{maxmons}(m(\mathsf{s}(\bar{x}))) = \{m\}$. □

Lemma 5.16. *Let $m \in M[V]$, $(x_1, \ldots, x_k) := \text{v}(m)$ and $\mathsf{s}(\bar{x}) := (\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$. Then $\text{mons}(m(\mathsf{s}(\bar{x}))) = \{\prod_{v \in \Delta} v \mid \Delta \subseteq \text{vars}(m)\}$, i.e. $m' \in \text{mons}(m(s(\bar{x})))$ if and only m' divides m.*

Proof. Similarly to the previous proof we get

$$m(\mathsf{s}(\bar{x})) = \prod_{v \in \text{vars}(m)} (v+1).$$

Distributing out this product shows that every monomial of $m(\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$ has the form $\prod_{v \in \Delta} v$ for some multiset $\Delta \subseteq \text{vars}(m)$. Furthermore given $\Delta \subseteq \text{vars}(m)$ induces a monomial m via $\text{vars}(m) = \Delta$. This shows the second part of the statement since m' divides m if and only if $\text{vars}(m') \subseteq \text{vars}(m)$. □

Lemma 5.17. *Let $p \in \mathbb{N}[V]$ and let $x_1, \ldots, x_k$ be pairwise distinct variables. Then*

$$\text{maxmons}(p(\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))) = \text{maxmons}(p)$$

Proof. Note that m is a maximal monomial of $p(\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$ if and only m is a maximal monomial in the multiset $\bigcup_{m \in \mathrm{mons}(p)} \mathrm{maxmons}(m(\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k)))$ which equals $\mathrm{mons}(p)$ by Lemma 5.15. This means m is a maximal monomial of $p(\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$ if and only if m is a maximal monomial of p. Therefore the statement follows. □

5.3 A normal form for polynomial equations

The following function allows us to compute a normal form of negated equations between S-terms.

Definition 5.18. $\mathrm{reduce} : \mathbb{N}[V] \times \mathbb{N}[V] \to \mathbb{N}[V] \times \mathbb{N}[V]$ *is the computable function defined by* $(p, q) \mapsto (p', q')$ *where* p' *is the polynomial with* $\mathrm{mons}(p') = \mathrm{mons}(p) - \mathrm{mons}(q)$ *and* q' *is the polynomial with* $\mathrm{mons}(q') = \mathrm{mons}(q) - \mathrm{mons}(p)$.

Lemma 5.19. *Let* $p, q \in \mathbb{N}[V]$ *and* $(p', q') := \mathrm{reduce}(p, q)$. *Then*

(i) $\mathrm{mons}(p') \cap \mathrm{mons}(q') = \emptyset$

(ii) $\mathrm{mons}(p) = \mathrm{mons}(p') \cup (\mathrm{mons}(p) \cap \mathrm{mons}(q))$,

(iii) $\mathrm{mons}(q) = \mathrm{mons}(q') \cup (\mathrm{mons}(p) \cap \mathrm{mons}(q))$,

(iv) $\underline{p} = \underline{q} \Leftrightarrow_T \underline{p'} = \underline{q'}$.

Proof. *(i)* to *(iii)* follow directly from the definition of reduce. Now we show *(iv)*: By B_4 and congruence of $+$ we get $T \vdash \forall x \forall y \forall z\, x + y = x + z \leftrightarrow y = z$. In addition to commutativity and associativity of $+$ this implies that monomials that occur in both p and q can be cancelled while preserving $\Leftrightarrow_T$. □

For the following a characterization of multiset orders is useful:

Lemma 5.20. *Let* $(X, >)$ *be a strict partial order and* $M, N \in \mathcal{M}(X)$. *Then*

$$M >^{\mathrm{mul}} N \iff M \neq N \text{ and for all } n \in N - M \text{ there is an } m \in M - N \text{ with } m > n$$

Proof. See [1] Lemma 2.5.6. □

Lemma 5.21. *Let* $p, q \in \mathbb{N}[V]$ *and* $(p', q') := \mathrm{reduce}(p, q)$. *Then* $p <_{\mathrm{mon}} q$ *if and only if* $p' <_{\mathrm{mon}} q'$.

Proof. By Lemma 5.20 we have $p <_{\mathrm{mon}} q$ if and only if $\mathrm{mons}(p) \neq \mathrm{mons}(q)$ and for all $m_1 \in \mathrm{mons}(p) - \mathrm{mons}(q)$ there is a $m_2 \in \mathrm{mons}(q) - \mathrm{mons}(p)$ with $m_1 <_{\mathrm{mon}} m_2$. By the definition of reduce and Lemma 5.19 this exactly the case if $p' <_{\mathrm{mon}} q'$. □

Lemma 5.22. *Let* $p, q \in \mathbb{N}[V]$ *with* $p <_{\mathrm{mon}} q$, $\mathrm{mons}(p) \cap \mathrm{mons}(q) = \emptyset$. *Furthermore let* $\bar{x} := (x_1, \ldots, x_k)$ *be pairwise distinct variables such that* $\{x_1, \ldots, x_k\} = \mathrm{v}(p) \cup \mathrm{v}(q)$. *We set* $\mathsf{s}(\bar{x}) := (\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$ *and* $(p', q') := \mathrm{reduce}(p(\mathsf{s}(\bar{x})), q(\mathsf{s}(\bar{x})))$. *There holds:*

(i) $p' <_{\mathrm{mon}} q'$,

(ii) If $p \neq 0$, then $p' <_{\text{mon}} p$.

Proof. (i) $p' <_{\text{mon}} q'$: By Lemma 5.17 we have $\text{maxmons}(p(\mathsf{s}(\bar{x}))) = \text{maxmons}(p(\bar{x}))$ and $\text{maxmons}(q(\mathsf{s}(\bar{x}))) = \text{maxmons}(q(\bar{x}))$. By Lemma 5.14 we get $p(\mathsf{s}(\bar{x})) <_{\text{mon}} q(\mathsf{s}(\bar{x}))$. Therefore we have $p' <_{\text{mon}} q'$ by Lemma 5.21.

(ii) We show this result in two steps:

(a) $\text{supp}(\text{maxmons}(p(\mathsf{s}(\bar{x})))) \subseteq \text{supp}(\text{mons}(q(\mathsf{s}(\bar{x}))))$: Since $p \neq 0$ we get $p(\mathsf{s}(\bar{x})) \neq 0$ and thus $\text{mons}(p(\mathsf{s}(\bar{x}))) \neq \emptyset$. Now let m be a maximal monomial of $p(\mathsf{s}(\bar{x}))$. Then by Lemma 5.17 m is a maximal monomial of p. Since $\text{mons}(p) \cap \text{mons}(q) = \emptyset$ and $p <_{\text{mon}} q$ there is a maximal monomial m_q of q, with $m <_{\text{mon}} m_q$ by Lemma 5.13. Therefore $m = \prod_{v \in \Gamma} v$ for some multiset $\Gamma \subsetneq \text{vars}(m_q)$. By Lemma 5.16 we have $\text{mons}(m_q(\mathsf{s}(\bar{x}))) = \{\prod_{v \in \Delta} v \mid \Delta \subseteq \text{vars}(m_q)\}$ and therefore $m \in \text{mons}(m_q(\mathsf{s}(\bar{x}))) \subseteq \text{mons}(q(\mathsf{s}(\bar{x})))$, i.e. $m \in \text{mons}(q(\mathsf{s}(\bar{x})))$.

(b) $p' <_{\text{mon}} p$: Since $p \neq 0$ we have $\text{mons}(p(\mathsf{s}(\bar{x}))) \neq \emptyset$. By (a) we thus have $\Pi := \text{mons}(p) \cap \text{mons}(q(\mathsf{s}(\bar{x}))) \neq \emptyset$. Let

$$\text{mons}(p(\mathsf{s}(\bar{x})))_{<p} := \bigcup_{m \in \text{mons}(p)} (\text{mons}(m(\mathsf{s}(\bar{x}))) - \{m\}).$$

Since for all monomials m we have $m \in \text{mons}(m(\mathsf{s}(\bar{x})))$ by Lemma 5.15 we get $\text{mons}(p(\mathsf{s}(\bar{x}))) = \text{mons}(p) \cup \text{mons}(p(\mathsf{s}(\bar{x})))_{<p}$. Furthermore by the definition of reduce we have $\text{mons}(p') = \text{mons}(p(\mathsf{s}(\bar{x}))) - \text{mons}(q(\mathsf{s}(\bar{x})))$. Therefore we have $\text{mons}(p') = (\text{mons}(p) \cup \text{mons}(p(\mathsf{s}(\bar{x})))_{<p}) - \text{mons}(q(\mathsf{s}(\bar{x})))$. We now set $\Lambda := \text{mons}(p(\mathsf{s}(\bar{x})))_{<p} - (\text{mons}(q(\mathsf{s}(\bar{x}))) - \Pi)$ to get $\text{mons}(p') = (\text{mons}(p) - \Pi) \cup \Lambda$. Now for $x \in \Lambda$ we have $x \in \text{mons}(p(\mathsf{s}(\bar{x})))_{<p}$ and thus there is an $m \in \text{mons}(p)$ such that $x \in \text{mons}(m(\mathsf{s}(\bar{x}))) - \{m\}$ and thus $x <_{\text{mon}} m$ by Lemma 5.16. Now there exists a $y \in \text{maxmons}(p)$ such that $x <_{\text{mon}} y$ since either m is already maximal in $\text{mons}(p)$ or there is a maximal monomial $y \in \text{mons}(p)$ such that $m <_{\text{mon}} y$. By (a) we have $y \in \text{mons}(q(\mathsf{s}(\bar{x})))$ and therefore $y \in \Pi$. In total we have $p' <_{\text{mon}} p$.

□

5.4 A necessary condition for $\mathcal{P}_T$-provability

We now study the T-equivalence of equations more closely. A useful result is the following:

Proposition 5.23. *Let $(R, +_R, 0_R, \cdot_R, 1_R)$ be a commutative ring with 1. We also set $\mathcal{R} := (R, 0^{\mathcal{R}}, \mathsf{s}^{\mathcal{R}}, +^{\mathcal{R}}, \cdot^{\mathcal{R}})$ with*

$$\begin{aligned} 0^{\mathcal{R}} &:= 0_R, \\ \mathsf{s}^{\mathcal{R}}(x) &:= x +_R 1_R, \\ +^{\mathcal{R}} &:= +_R, \\ \cdot^{\mathcal{R}} &:= \cdot_R. \end{aligned}$$

Then $\mathcal{R} \models T$.

Proof. Straightforward. □

Remark 5.24. *We denote by* $\mathbb{Z}[V]$ *the set of polynomials with coefficients in* $\mathbb{Z}$ *and indeterminates in* V*. Note that* $\mathbb{Z}[V]$ *is a commutative ring with* 1*. For* $p \in \mathbb{Z}[V]$ *we define the* ideal generated by p *as* $(p) := \{q \cdot p \mid q \in \mathbb{Z}[V]\}$*. A result from abstract algebra shows that the quotient* $\mathbb{Z}[V]/(p)$ *is again a commutative ring with* 1*.*

Definition 5.25. *For* $t, u \in T(S)$ *we define* $[\![t = u]\!] := \mathrm{poly}(t) - \mathrm{poly}(u) \in \mathbb{Z}[V]$*.*

Lemma 5.26. *Let* $p \in \mathbb{Z}[V]$*,* $t, u \in T(S)$ *and* $\mathcal{M} := \mathbb{Z}[V]/(p)$*. Then* $\mathcal{M} \models t = u$ *if and only if* $[\![t = u]\!] \in (p)$*.*

Proof. Note that $\mathcal{M} \models t = u \iff t^{\mathcal{M}} = u^{\mathcal{M}}$. Since $\mathcal{M}$ satisfies ring axioms we get $t^{\mathcal{M}} = u^{\mathcal{M}} \iff t^{\mathcal{M}} - u^{\mathcal{M}} = 0 + (p)$. It is straightforward to show that for all terms $v \in T(S)$ we have $v^{\mathcal{M}} = \mathrm{poly}(v) + (p)$. Thus $t^{\mathcal{M}} - u^{\mathcal{M}} = 0 + (p) \iff (\mathrm{poly}(t) - \mathrm{poly}(u)) + (p) = 0 + (p)$. This means $t^{\mathcal{M}} - u^{\mathcal{M}} = 0 + (p) \iff [\![t = u]\!] + (p) = 0 + (p)$. This is exactly the case if $[\![t = u]\!] \in (p)$. □

Lemma 5.27. *Let* $t_1, t_2, u_1, u_2 \in T(S)$*. If* $T \vdash t_1 = t_2 \longrightarrow u_1 = u_2$*, then* $[\![t_1 = t_2]\!]$ *divides* $[\![u_1 = u_2]\!]$*.*

Proof. Set $\mathcal{M} := \mathbb{Z}[V]/([\![t_1 = t_2]\!])$. By Proposition 5.23 and Remark 5.24 we have $\mathcal{M} \models T$ and thus $\mathcal{M} \models t_1 = t_2 \supset u_1 = u_2$. By Lemma 5.26 we have $\mathcal{M} \models t_1 = t_2$. Thus $\mathcal{M} \models u_1 = u_2$. By Lemma 5.26 we get $[\![u_1 = u_2]\!] \in ([\![t_1 = t_2]\!])$, i.e. $[\![t_1 = t_2]\!]$ divides $[\![u_1 = u_2]\!]$. □

Proposition 5.28. *Let* $t_1, t_2, u_1, u_2 \in T(S)$ *such that* $t_1 = t_2 \Leftrightarrow_T u_1 = u_2$*. Then we have* $[\![t_1 = t_2]\!] = \pm[\![u_1 = u_2]\!]$*.*

Proof. By Lemma 5.27 we get that $[\![t_1 = t_2]\!]$ divides $[\![u_1 = u_2]\!]$ and $[\![u_1 = u_2]\!]$ divides $[\![t_1 = t_2]\!]$. As a consequence we have $[\![t_1 = t_2]\!] = \pm[\![u_1 = u_2]\!]$. □

Lemma 5.29. *Let* $p, q \in \mathbb{N}[V]$*. If* $\mathcal{P}_T \vdash [\underline{p} \neq \underline{q}]_T$*, then* $p \leqslant_{\mathrm{mon}} q$*.*

Proof. By Lemmas 5.19 and 5.21 we can assume $\mathrm{mons}(p) \cap \mathrm{mons}(q) = \emptyset$, otherwise apply reduce to (p, q). Now let $\pi \vdash_{\mathcal{P}_T} [\underline{p} \neq \underline{q}]_T$. We proceed by induction on π.

If π ends in A_1^{ax}, then $\underline{p} = \underline{q} \Leftrightarrow_T \mathsf{s}(v) = \mathsf{0}$ for some $v \in T(S)$. Then by Proposition 5.28 we have that $[\![\underline{p} = \underline{q}]\!] = \pm[\![\mathsf{s}(v) = \mathsf{0}]\!]$. Note that $[\![\mathsf{s}(v) = \mathsf{0}]\!] \in \mathbb{N}[V]$. Therefore $[\![\underline{p} = \underline{q}]\!]$ either has only non-negative coefficients or only non-positive coefficients. Note that not both p and q can be 0, since then $\mathcal{P}_T \vdash [\mathsf{0} \neq \mathsf{0}]_T$ which contradicts the soundness of $\mathcal{P}_T$ (Theorem 3.9). Since $\mathrm{mons}(p) \cap \mathrm{mons}(q) = \emptyset$ we get $p = 0$ or $q = 0$. In both cases we have $p \leqslant_{\mathrm{mon}} q$.

If π ends in B_1^{var}, i.e. $\pi =$

$$\frac{[\underline{p}(\mathsf{0}) \neq \underline{q}(\mathsf{0})]_T \quad [\underline{p}(\mathsf{s}(x)) \neq \underline{q}(\mathsf{s}(x))]_T}{[\underline{p}(x) \neq \underline{q}(x)]_T} \, B_1^{\mathrm{var}},$$

then $\underline{p}(\mathsf{0}) \neq \underline{q}(\mathsf{0}) \Leftrightarrow_T \underline{p(\mathsf{0})} \neq \underline{q(\mathsf{0})}$ and $\underline{p}(\mathsf{s}(x)) \neq \underline{q}(\mathsf{s}(x)) \Leftrightarrow_T \underline{p(\mathsf{s}(x))} \neq \underline{q(\mathsf{s}(x))}$ by Lemma 5.10. By induction hypothesis we have $p(\mathsf{s}(x)) \leqslant_{\mathrm{mon}} q(\mathsf{s}(x))$. By Lemma 5.17

there holds $\mathrm{maxmons}(p(\mathsf{s}(x))) = \mathrm{maxmons}(p)$ as well as $\mathrm{maxmons}(q(\mathsf{s}(x))) = \mathrm{maxmons}(q)$. Therefore $\mathrm{maxmons}(p(\mathsf{s}(x))) \cap \mathrm{maxmons}(q(\mathsf{s}(x))) = \emptyset$ and by Lemma 5.14 we either have $\mathrm{maxmons}(p(\mathsf{s}(x))) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{maxmons}(q(\mathsf{s}(x)))$ or $\mathrm{maxmons}(q(\mathsf{s}(x))) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{maxmons}(p(\mathsf{s}(x)))$. Therefore $\mathrm{maxmons}(p) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{maxmons}(q)$ or $\mathrm{maxmons}(q) <^{\mathrm{mul}}_{\mathrm{mon}} \mathrm{maxmons}(p)$ and thus $p \leqslant_{\mathrm{mon}} q$ by Lemma 5.14. □

Note that the corresponding property does not hold in $\mathbb{N}$: We have that $\mathbb{N} \models 2x \neq 2y+1$ since the left side is even and the right side is odd, but $2x \not\leqslant_{\mathrm{mon}} 2y+1$, since $x \not\leqslant_{\mathrm{mon}} y$.

5.5 A decision procedure for $\mathcal{P}_T^{\vdash}$

We now consider the terms that arise from using B_1^{var} in $\mathcal{P}_T$-proofs in more detail:

Definition 5.30. *Let $k \in \mathbb{N}$ and let $x_1, \ldots, x_k$ be pairwise distinct variables. We define the set*

$$Y(x_1, \ldots, x_k) := \{(t_1, \ldots, t_k) \mid \text{for all } i \in \{1, \ldots, k\} \;\; t_i \in \{\mathsf{0}, \mathsf{s}(x_i)\}\}\,.$$

We now show some reductions for $\mathcal{P}_T$-provability:

Lemma 5.31. *Let $\varphi(x) \in N(S)$. Then $\mathcal{P}_T \vdash [\varphi(x)]_T$ if and only if $\mathcal{P}_T \vdash [\varphi(\mathsf{0})]_T$ and $\mathcal{P}_T \vdash [\varphi(\mathsf{s}(x))]_T$.*

Proof. $\Longleftarrow$: Apply B_1^{var} to the given proofs.

$\Longrightarrow$: Let $\pi \vdash_{\mathcal{P}_T} [\varphi(x)]_T$.

If π ends in A_1^{ax}, then $\varphi(x) \Leftrightarrow_T \mathsf{s}(t(x)) \neq \mathsf{0}$ for some $t(x) \in T\,(S)$. Then by Lemma 3.5 we have $\varphi(\mathsf{0}) \Leftrightarrow_T \mathsf{s}(t(\mathsf{0})) \neq \mathsf{0}$ and $\varphi(\mathsf{s}(x)) \Leftrightarrow_T \mathsf{s}(t(\mathsf{s}(x))) \neq \mathsf{0}$. Thus $[\varphi(\mathsf{0})]_T$ and $[\varphi(\mathsf{s}(x))]_T$ are provable by A_1^{ax}.

If $\pi =$

$$\dfrac{\begin{matrix}(\pi_1) & (\pi_2)\\ [\varphi(\mathsf{0})]_T & [\varphi(\mathsf{s}(x))]_T\end{matrix}}{[\varphi(x)]_T}\; B_1^{\mathrm{var}},$$

then π_1 and π_2 are the desired proofs. □

Lemma 5.32. *Let $k \in \mathbb{N}$ and $\varphi(x_1, \ldots, x_k) \in N(S)$. Then $\mathcal{P}_T \vdash [\varphi(x_1, \ldots, x_k)]_T$ if and only if $\mathcal{P}_T \vdash [\varphi(\bar{u})]_T$ for all $\bar{u} \in Y(x_1, \ldots, x_k)$.*

Proof. We proceed by induction on k. If $k = 0$, then $Y(x_1, \ldots, x_k) = \{()\}$ and the statement follows trivially.

Now let $\varphi = \varphi(x_1, \ldots, x_k, x_{k+1})$. Note that $Y(x_{k+1}) = \{\mathsf{0}, \mathsf{s}(x_{k+1})\}$. Therefore a restatement of Lemma 5.31 is $\mathcal{P}_T \vdash [\varphi(x_1, \ldots, x_{k+1})]_T$ if and only if $\mathcal{P}_T \vdash [\varphi(x_1, \ldots, x_k, u_{k+1})]_T$ for all $u_{k+1} \in Y(x_{k+1})$. Thus, by induction hypothesis we have $\mathcal{P}_T \vdash [\varphi(x_1, \ldots, x_k, u_{k+1})]_T$ if and only if $\mathcal{P}_T \vdash [\varphi(u_1, \ldots, u_k, u_{k+1})]_T$ for all $(u_1, \ldots, u_k) \in Y(x_1, \ldots, x_k)$ and also $u_{k+1} \in Y(x_{k+1})$. Since we have

$$Y(x_1, \ldots, x_{k+1}) = \{(u_1, \ldots, u_k, u_{k+1}) \mid (u_1, \ldots, u_k) \in Y(x_1, \ldots, x_k), u_{k+1} \in Y(x_{k+1})\}$$

this concludes the proof. □

Definition 5.33. $\text{decide}_{\mathbb{N}[V]} : \mathbb{N}[V] \times \mathbb{N}[V] \to \{0,1\}$ *is recursively defined as*

Let $p', q' \in \mathbb{N}[V]$.

Compute $(p, q) := \text{reduce}(p', q')$.

If $p \not\leqslant_{\text{mon}} q$, *return* 0.

If $q = 0$ *return* 1 *if* $[1]p \geq 1$, *otherwise return* 0.

If $p = 0$ *return* 1 *if* $[1]q \geq 1$, *otherwise return* 0.

In all other cases let $\bar{x} := \text{v}(p) \cup \text{v}(q)$.

Compute $(p_{\bar{u}}, q_{\bar{u}}) := \text{reduce}(p(\bar{u}), q(\bar{u}))$ *for* $\bar{u} \in Y(\bar{x})$

Return $\min\left\{\text{decide}_{\mathbb{N}[V]}(p_{\bar{u}}, q_{\bar{u}}) \mid \bar{u} \in Y(\bar{x})\right\}$.

We introduce a well-founded strict partial order to show termination of $\text{decide}_{\mathbb{N}[V]}$:

Definition 5.34. *Let* $p_1, p_2, q_1, q_2 \in \mathbb{N}[V]$. *If* $p_1 \leqslant_{\text{mon}} p_2$ *we set*

$$\min(p_1, p_2) := \begin{cases} p_1 & \text{if } p_1 <_{\text{mon}} p_2, \\ p_2 & \text{if } p_2 <_{\text{mon}} p_1. \end{cases}$$

We define

$$(p_1, p_2) <_{\text{mon}} (q_1, q_2) : \Longleftrightarrow p_1 \leqslant_{\text{mon}} p_2 \text{ and } q_1 \leqslant_{\text{mon}} q_2 \text{ and } \min(p_1, p_2) <_{\text{mon}} \min(q_1, q_2)$$

and

$$\begin{aligned} (p_1, p_2) <_t (q_1, q_2) : \Longleftrightarrow\ & |\text{v}(p_1) \cup \text{v}(p_2)| < |\text{v}(q_1) \cup \text{v}(q_2)| \text{ or} \\ & |\text{v}(p_1) \cup \text{v}(p_2)| = |\text{v}(q_1) \cup \text{v}(q_2)| \text{ and} \\ & (p_1, p_2) <_{\text{mon}} (q_1, q_2). \end{aligned}$$

Lemma 5.35. $<_{\text{mon}}$ *on* $\mathbb{N}[V] \times \mathbb{N}[V]$ *and* $<_t$ *are well-founded strict partial orders.*

Proof. Showing that $<_{\text{mon}}$ is a strict partial order is straightforward. The well-foundedness of $<_{\text{mon}}$ follows from the well-foundedness of $<_{\text{mon}}$ on $\mathbb{N}[V]$ (Lemma 5.12). Note that $<_t$ is a lexicographic product of two well-founded strict partial orders. Therefore $<_t$ is also a well-founded strict partial order (see for example [1] Lemmas 2.4.1 and 2.4.2). □

Lemma 5.36. *Let* $p, q \in \mathbb{N}[V]$ *and let* $\bar{x} := (x_1, \ldots, x_k)$ *be pairwise distinct variables such that* $\{x_1, \ldots, x_k\} = \text{v}(p) \cup \text{v}(q)$. *Furthermore we set* $\mathsf{s}(\bar{x}) := (\mathsf{s}(x_1), \ldots, \mathsf{s}(x_k))$ *and* $(p', q') := \text{reduce}(p(\mathsf{s}(\bar{x})), q(\mathsf{s}(\bar{x})))$. *If* $p \neq 0$, $q \neq 0$ *and* $p \leqslant_{\text{mon}} q$, *then* $(p', q') <_{\text{mon}} (p, q)$.

Proof. If $p <_{\text{mon}} q$, then by Lemma 5.22 we have $p' <_{\text{mon}} q'$ and $p' <_{\text{mon}} p$, thus $(p', q') <_{\text{mon}} (p, q)$. A similar argument works, if $q <_{\text{mon}} p$. □

Lemma 5.37. $\text{decide}_{\mathbb{N}[V]}$ *terminates.*

Proof. We proceed by induction on $<_t$: First observe that $\text{decide}_{\mathbb{N}[V]}$ terminates for p', q' where $\mathrm{v}(p') \cup \mathrm{v}(q') = \emptyset$: In this case we have $p, q \in \mathbb{N}$. If $p \not\leqslant_{\text{mon}} q$, then $\text{decide}_{\mathbb{N}[V]}$ terminates (in this case $p \not\leqslant_{\text{mon}} q$ simply means $p = q$). If $p \leqslant_{\text{mon}} q$, then $p \neq q$. If $p >_{\text{mon}} q$, then $[1]p = p > 0$ and $q = 0$ by the definition of reduce. If $q >_{\text{mon}} p$, then $[1]q = q > 0$ and $p = 0$ by the definition of reduce. In both cases $\text{decide}_{\mathbb{N}[V]}$ terminates.

Now let there be at least one variable in $\mathrm{v}(p') \cup \mathrm{v}(q')$, let $p, q \neq 0$ and $p \leqslant_{\text{mon}} q$ (otherwise $\text{decide}_{\mathbb{N}[V]}$ terminates trivially). Also set $\mathsf{s}(\bar{x}) := (\mathsf{s}(x_1), \ldots, \mathsf{s}(x_{|x|}))$. Then we have $(p_{\bar{u}}, q_{\bar{u}}) <_t (p', q')$ for $\bar{u} \in Y(\bar{x}) \setminus \{\mathsf{s}(\bar{x})\}$ since $|\mathrm{v}(p_{\bar{u}}) \cup \mathrm{v}(q_{\bar{u}})| < |\mathrm{v}(p') \cup \mathrm{v}(q')|$. Further we have $(p_{\mathsf{s}(\bar{x})}, q_{\mathsf{s}(\bar{x})}) <_{\text{mon}} (p, q)$ by Lemma 5.36. Also $(p, q) <_{\text{mon}} (p', q')$ by Lemma 5.21. Therefore we have $(p_{\mathsf{s}(\bar{x})}, q_{\mathsf{s}(\bar{x})}) <_t (p', q')$ and the statement follows by the induction hypothesis. □

Lemma 5.38. *Let $p', q' \in \mathbb{N}[V]$. Then $\text{decide}_{\mathbb{N}[V]}(p', q') = 1$ if and only if $\mathcal{P}_T \vdash [\underline{p'} \neq \underline{q'}]_T$.*

Proof. We proceed by induction on (p', q') with respect to $<_t$. Let $(p, q) := \text{reduce}(p', q')$.

If $p \not\leqslant_{\text{mon}} q$, then $\text{decide}_{\mathbb{N}[V]}(p, q) = 0$ and $\mathcal{P}_T \not\vdash [\underline{p} \neq \underline{q}]_T$ by the contraposition of Lemma 5.29. Now consider the case where $p \leqslant_{\text{mon}} q$. If $p = 0$ and $[1]q \geq 1$, then $\text{decide}_{\mathbb{N}[V]}(p, q) = 1$. Also we have $T \vdash \underline{p} = \mathsf{s}(\underline{q - 1})$ and therefore $\underline{p} \neq \underline{q} \Leftrightarrow_T \mathsf{s}(\underline{q - 1}) \neq \mathsf{0}$, thus $\mathcal{P}_T \vdash [\underline{p} \neq \underline{q}]_T$ by A_1^{ax}. A similar argument applies if $q = 0$ and $[1]p \geq 1$.

If $p = 0$ and $[1]q = 0$, then $\text{decide}_{\mathbb{N}[V]}(p, q) = 0$. Now $q(\mathsf{0}, \ldots, \mathsf{0}) = 0 = p(\mathsf{0}, \ldots, \mathsf{0})$ and $\mathcal{P}_T \not\vdash [\mathsf{0} \neq \mathsf{0}]_T$ by soundness of $\mathcal{P}_T$ (Theorem 3.9). Thus, by Lemma 5.32 $\mathcal{P}_T \not\vdash [\underline{p} \neq \underline{q}]_T$. A similar argument applies if $q = 0$ and $[1]p = 0$.

Now consider the case where $p \neq 0$, $q \neq 0$ and $p \leqslant_{\text{mon}} q$. Let $(p_{\bar{u}}, q_{\bar{u}})$ as in Definition 5.33. Now

$$\text{decide}_{\mathbb{N}[V]}(p, q) = \min\left\{\text{decide}_{\mathbb{N}[V]}(p_{\bar{u}}, q_{\bar{u}}) \mid \bar{u} \in Y(\bar{x})\right\}.$$

By Lemma 5.32 we have $\mathcal{P}_T \vdash [\underline{p} \neq \underline{q}]_T$ if and only if $\mathcal{P}_T \vdash [\underline{p(\bar{u})} \neq \underline{q(\bar{u})}]_T$ for all $\bar{u} \in Y(\bar{x})$. By Lemma 5.19, this is equivalent to $\mathcal{P}_T \vdash [\underline{p_{\bar{u}}} \neq \underline{q_{\bar{u}}}]_T$. Note that $(p_{\bar{u}}, q_{\bar{u}}) <_t (p', q')$. Thus, by induction hypothesis this is equivalent to $\text{decide}_{\mathbb{N}[V]}(p_{\bar{u}}, q_{\bar{u}}) = 1$ for all $\bar{u} \in Y(\bar{x})$, i.e. if and only if $\text{decide}_{\mathbb{N}[V]}(p, q) = 1$. □

Now we can show that $\mathcal{P}_T{}^{\vdash}$ is decidable:

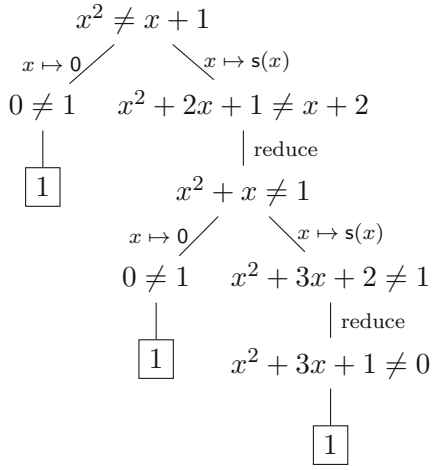
Proof of Theorem 3.11. The decision procedure is as follows:

> Let $\varphi \in N(S)$. Extract the $t, u \in T(S)$ such that $\varphi \equiv t \neq u$. Return $\text{decide}_{\mathbb{N}[V]}(\text{poly}(t), \text{poly}(u))$.

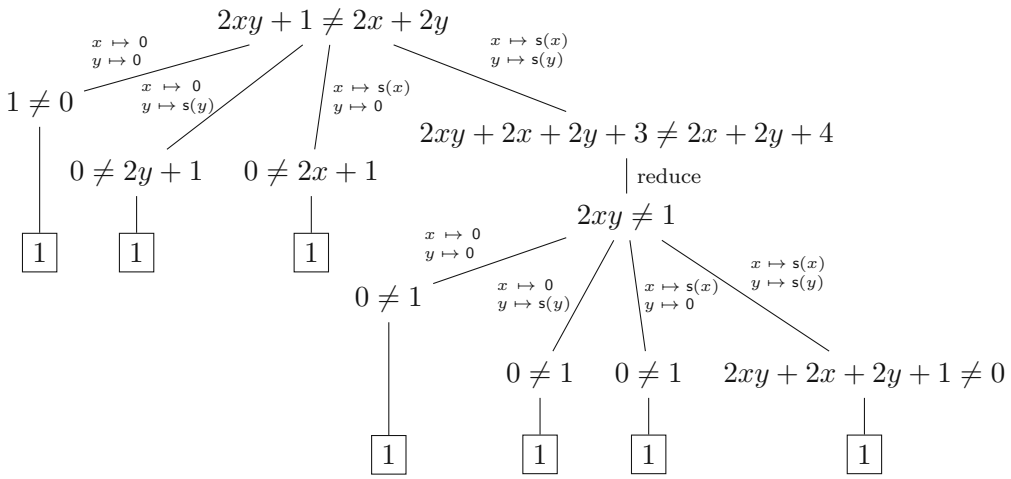
By Lemma 5.37 this procedure terminates and by Lemma 5.38 the procedure decides whether $\mathcal{P}_T \vdash [\underline{\text{poly}(t)} \neq \underline{\text{poly}(u)}]_T$. By Lemma 5.8 we get $\underline{\text{poly}(t)} \neq \underline{\text{poly}(u)} \Leftrightarrow_T \varphi$ and thus this procedure decides whether $\mathcal{P}_T \vdash [\varphi]$. □

Example 5.39. *Let $\varphi(x) :\equiv x \cdot x \neq x + \mathsf{s}(\mathsf{0})$ as in example 3.8. The decision procedure on this example proceeds as follows: Note that $\varphi(x) \in N(S)$, thus we extract the polynomials $p := x^2$ and $q := x + 1$ and compute $\text{decide}_{\mathbb{N}[V]}(p, q)$. We have $x^2 >_{\text{mon}} x + 1$, since x and 1 are strict divisors of x^2. Neither p nor q are 0, therefore we compute $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p(\mathsf{0}), q(\mathsf{0})))$ and $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p(\mathsf{s}(x)), q(\mathsf{s}(x))))$. We have $p(\mathsf{0}) = 0$, $q(\mathsf{0}) = 1$, and $\text{reduce}(p(\mathsf{0}), q(\mathsf{0})) = (0, 1)$ and therefore $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p(\mathsf{0}), q(\mathsf{0}))) =$*

1. *Furthermore we have* $p(\mathsf{s}(x)) = x^2 + 2x + 1$ *and* $q(\mathsf{s}(x)) = x + 2$. *Thus we get* $\text{reduce}(p(\mathsf{s}(x)), q(\mathsf{s}(x))) = (x^2 + x, 1) := (p', q')$. *Since neither* p' *nor* q' *are* 0 *we compute* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p'(\mathsf{0}), q'(\mathsf{0})))$ *and* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p'(\mathsf{s}(x)), q'(\mathsf{s}(x)))) = 1$. *We have* $p'(\mathsf{0}) = 0$ *and* $q'(\mathsf{0}) = 1$, *therefore* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p'(\mathsf{0}), q'(\mathsf{0}))) = 1$. *We get* $p'(\mathsf{s}(x)) = x^2 + 3x + 2$ *and* $q'(\mathsf{s}(x)) = 1$. *Thus* $\text{reduce}(p'(\mathsf{s}(x)), q'(\mathsf{s}(x))) = (x^2 + 3x + 1, 0)$. *Now* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p'(\mathsf{s}(x)), q'(\mathsf{s}(x)))) = 1$ *and* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p(\mathsf{s}(x)), q(\mathsf{s}(x))))$ *and in total* $\text{decide}_{\mathbb{N}[V]}(\text{reduce}(p, q)) = 1$. *This confirms that* $\mathcal{P}_T \vdash [\varphi(x)]_T$ *as already shown in example 3.8. Note that the computation of* $\text{decide}_{\mathbb{N}[V]}(p, q)$ *mirrors the tree structure of the proof from example 3.8. The computation can be visualized in tree form:*



Example 5.40. *Let* $\varphi(x, y) :\equiv \underline{2} \cdot x \cdot y + \underline{1} \neq \underline{2} \cdot (x + y)$. *We show* $\mathcal{P}_T \vdash [\varphi(x, y)]_T$ *by drawing the computation tree as in the previous example. We omit most of the* reduce *steps for brevity. We have* $\text{poly}(\underline{2} \cdot x \cdot y + \underline{1}) = 2xy + 1$ *and* $\text{poly}(\underline{2} \cdot (x + y)) = 2x + 2y$. *Now the computation tree looks like*



6 Conclusion

We presented a novel approach based on proof-theory to solve Diophantine satisfiability problems and applied it to a theory AB adjacent to a theory of open induction over a base arithmetical theory A whose language includes successors, predecessors, addition and multiplication (but no inequality). To do this we introduced a simple specialized proof calculus $\mathcal{P}_T$ and showed its soundness and completeness with respect to AB. Finally, showing the the decidability of $\mathcal{P}_T$ allowed us to decide Diophantine satisfiability for AB.

Using this approach leads to some avenues for future work: Note that the axioms C_m have a very similar structure to the axiom B_4, in that the implication is an equivalence. Thus, by incorporating the axioms C_m into the theory T, we suspect that the method we presented in this thesis can be adapted to show

Conjecture 6.1. D_{ABC_m} *is decidable.*

The axioms C'_m have a more complicated structure. However, it may be possible to incorporate them into the proof calculus $\mathcal{P}_T$ by introducing a new inference rule, as we did with A_1 and B_1. This will however require a more careful analysis of the interaction between that inference rule with B_1^{var}:

Conjecture 6.2. $\mathrm{D}_{\mathrm{IOpen}_\mathsf{p}}$ *is decidable.*

Note that in this thesis $\mathrm{IOpen}_\mathsf{p}$ refers to open induction over a language without $\leq$. Therefore, even if the above conjecture is true, the long-standing question of the decidability of $\mathrm{D}_{\mathrm{IOpen}}$ still remains an open problem.

Bibliography

[1] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[2] M. Baaz and S. Hetzl. On the non-confluence of cut-elimination. *The Journal of Symbolic Logic*, 76(1):313–340, 2011.

[3] E. Jeřábek. Division by zero. *Archive for Mathematical Logic*, 55(7-8):997–1013, 2016.

[4] J. Shepherdson. A non-standard model for a free variable fragment of number theory. *Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques*, 12, 1964.

[5] J. Shepherdson. The rule of induction in the three variable arithmetic based on + and −. *Annales scientifiques de l'Université de Clermont. Mathématiques*, 35(4):25–31, 1967.

[6] G. Takeuti. *Proof Theory.* Studies in logic and the foundations of mathematics. North-Holland, 1975.