# Introduction to Context Proofs

Michał Stanisław Wójcik

January 12, 2026

### Abstract

The paper describes a system for structuring proofs in first-order logic, inspired by the intuitive methods commonly employed by mathematicians. Traditional formalizations of proof, as found in most introductory logic textbooks, rely on linear sequences of formulas constructed via axioms and inference rules. While rigorous, such representations are ill-suited to capturing the contextual and hierarchical nature of proofs as they are typically written and understood. In this paper, we introduce a context-based proof system that formally models the dynamic management of assumptions and auxiliary constructions—analogous to the way contexts are established and dissolved in both informal mathematical writing and declarative programming languages. We develop a precise framework for referencing and manipulating these contexts and demonstrate that our approach retains the formal strength of classical derivation systems. This framework not only provides a closer alignment with mathematical practice but also lays the groundwork for efficient implementation of automated proof verification tools tailored to first-order logic.

## 1   Introduction

The purpose of this paper is to present a formal description of context-proofs, intended as a kernel for an automatic proof-checking system. Since there are several related approaches (see Section 6), it is useful to provide a complete formal specification of the proof mechanism, serving as precise documentation of the kernel.

When proving a theorem, mathematicians frequently use phrases such as "take any $n \in \mathbb{N}$", "there exists an $m$ such that...", "we will now prove that...", or "we have just proved...". Intuitively, with a phrase like "we will now prove that...", a specific context is established in which we define or construct objects, manipulate these objects, and, upon reaching a conclusion, often dismiss these auxiliary constructions with a phrase such as "we have just proved...". At this point, only the elements essential for the subsequent steps of the argument are retained. In this sense, writing a mathematical proof closely resembles writing a declarative program: we open and close contexts, introducing and discarding

1

objects as they become relevant or obsolete.

In contrast, the standard approach to formalizing proofs in most first-order logic textbooks is to represent proofs as sequences of formulas. Typically, we begin by selecting a set of logical axioms and domain-specific axioms, and by specifying derivation rules (such as modus ponens and generalization). We then construct a sequence, where each member is either an axiom or a formula obtained by applying these rules to earlier formulas in the sequence. If the sequence concludes with the desired statement, the proof is considered complete.

At first glance, these two paradigms—the informal, intuitive style and the formal, sequential style—seem quite different. The sequential approach, while formally rigorous, is often less amenable to writing intuitive proofs or building practical automatic proof checkers. The informal approach, on the other hand, is more natural for mathematicians but lacks formal precision.

In this paper, we seek to develop a formal system of context-based proving in first-order logic, constructed from the ground up. The goal is to create a system that not only mirrors the intuitive approach used by mathematicians but can also be readily translated into the core of an automatic, machine-verifiable proof checker for first-order logic.

Let's first observe an example of what I mean by context proof.

```
# we state an assumption and a thesis of the theorem we are going to
    prove
(0)  ¬(∃x.φ(x)) → ∀x.¬φ(x)

# we open a context of a proof
(0, 0)  ¬(∃x.φ(x)) # we recall assumption
# we state an auxiliary fact we are going to prove under assumption (0,
    0).
(0, 1)  φ(x) → ¬φ(x)

# we open a sub-context of a proof
(0, 1, 0)  φ(x) # we recall assumption
(0, 1, 1)  φ(x) → ∃x.φ(x) # we write down a logical tautology
(0, 1, 2)  ∃x.φ(x) # we apply modus ponens to (0,1,1) and (0,1,0).
(0, 1, 3)  ¬(∃x.φ(x)) ∧ (∃x.φ(x)) # we gather (0, 0) and (0, 1, 2)
(0, 1, 4)  ¬(∃x.φ(x)) ∧ (∃x.φ(x)) → ¬φ(x) # we write down a logical
    tautology
(0, 1, 5)  ¬φ(x) # we apply modus ponens to (0, 1, 4) and (0, 1, 3)

# we close the sub-context and we proceed with main context of the proof
(0, 2)  (φ(x) → ¬φ(x)) → ¬φ(x) # we write down a logical tautology
(0, 3)  ¬φ(x) # we apply modus ponens to (0, 2) amd (0, 1)
(0, 4)  ∀x.¬φ(x) # we apply generalisation rule to (0, 3)

# and this concludes proof as we arrived to the thesis
```

Only one variable was used but one can note that the formulas above are correctly stated since this is clear which variable is bound and which is free.

If we analyse the above example we will notice that at the left side of each line there is a reference and at the right side there is a formula.

In Section 2 we will define references as a finite sequences of nonnegative integers. By Definition 2.2, we will introduce a reference order $<$ in which for the line with reference $r$, we can refer only to lines with references $\rho$ for which $\rho < r$. We intuitively understand that we can refere to line $(0,0)$ from line $(0,1,3)$, but we can not refere to line $(0,1,2)$ from line $(0,4)$ which would have caused imediate contradiction. Indeed, in the reference order $(0,0) < (0,1,3)$ but $(0,1,2) \not< (0,4)$. To give a formal definition of *a context* we will also need a common "being a prefix" relation e.g. $(0,1) \prec (0,1,0)$. In Section 2, we will also prove basic properties of these two orders and relations between them.

The observation that at the left side of each line there is a reference and at the right side a formula, leads to the idea that *a context proof* is some function from a set of references to the set of formulas. This idea will be developed in Section 3. We will call such a function *a refernce system* and we will define in Definition 3.16 formal conditions for *a refernce system* to be a proof.

In Section 4, we will prove completness of context proofs, i.e that if $\models \phi$, there exists a context proof of $\phi$. In Section 5, we will prove soundness of context proofs, i.e. that if there exists a context proof of $\phi$ with respect to $T$, then $T \models \phi$.

## 2  Context

**Definition 2.1** (**finite sequences**). *For an arbitrary set $A$ by $A^*$ we mean a set of all finite sequences of $A$.*

We will often use notation in which we will denote sequences as $[a_1, \ldots, a_n]$. So if $a_i \in A$ then for $s = [a_1, \ldots, a_n]$, we have $s \in A^*$.
For a sequence $s = [a_1, \ldots, a_n]$, $*s$ means just $a_1, \ldots, a_n$, which allows us to write in a compact form many sequence operations. E.g. concatenation of sequences $s_1, s_2$ is $[*s_1, *s_2]$. If $a \in A$, then $[*s, a]$ is just a sequence with appended $a$, etc.
To access $n-th$ element of a sequence we will use 0-based indexing $a_i = s[i-1]$. Also $s[-1] = a_n$. We will denote a length of a sequence as $|s|$. We will denote empty sequence as $[]$.
In this paper finite sequence of nonnegative integers will be sometimes called *a reference*.

**Definition 2.2** (**reference order**). *Let $r_1, r_2 \in \mathbb{N}^*$.*

$$r_1 < r_2 \tag{1}$$

3

*iff there exist $k \in N$ and $r, s \in \mathbb{N}^*$ such that $s \neq [\,]$, $r_1 = [*r, k]$ and $r_2 = [*r, *s]$ and $s[0] > k$.*

$$r_1 \leq r_2 \tag{2}$$

*iff $r_1 < r_2$ or $r_1 = r_2$.*

**Corollary 2.3.** *Let $r_1, r_2 \in \mathbb{N}^*$. If $r_1 < r_2$, then $|r_1| \leq |r_2|$.*

**Corollary 2.4.** *For any non empty $r \in N^*$, we have $[0] \leq r$.*

**Corollary 2.5.** *For any non empty $r \in N^*$, we have $[\,] \not< r$.*

**Definition 2.6.** *Let $r_1, r_2 \in \mathbb{N}^*$ and $r_1 < r_2$.*

$$\mathrm{i}_{r_1, r_2} \overset{\mathrm{def}}{=} \max\{i < |r_1| : r_1[i] = r_2[i]\}, \tag{3}$$

$$\hat{\mathrm{i}}_{r_1, r_2} \overset{\mathrm{def}}{=} \mathrm{i}_{r_1, r_2} + 1. \tag{4}$$

**Definition 2.7 (prefix order).** *Let $r_1, r_2 \in \mathbb{N}^*$.*

$$r_1 \prec r_2 \tag{5}$$

*iff there exists $s \in \mathbb{N}^*$ such that $s \neq [\,]$ and $r_2 = [*r_1, *s]$.*

$$r_1 \preceq r_2 \tag{6}$$

*iff $r_1 \prec r_2$ or $r_1 = r_2$.*

**Corollary 2.8.** *$\preceq$ on $N^*$ is a locally finite poset.*

**Corollary 2.9.** *Let $r_1, r_2 \in \mathbb{N}^*$. If $r_1 \prec r_2$, then $|r_1| < |r_2|$.*

**Corollary 2.10.** *For any $r_1, r_1 \in \mathbb{N}^*$, if $r_1 < r_2$ then $r_1 \not\prec r_2$ and $r_2 \not\prec r_1$.*

*Proof.* If $r_1 < r_2$ then by definition $r_1 \not\prec r_2$. Since $|r_1| \leq |r_2|$, it is clear that $|r_2| \not< |r_1|$ and thus $r_2 \not\prec r_1$. $\qquad\square$

**Corollary 2.11.** *For any $r \in \mathbb{N}^*$, we have $[\,] \preceq r$.*

**Proposition 2.12.** *Let $r, r_1, r_2 \in \mathbb{N}^*$. If $r_1 \prec r$ and $r_2 \prec r$, then $r_1 \preceq r_2$ or $r_2 \preceq r_1$.*

*Proof.* Without loss of generality, we can assume that $|r_1| \leq |r_2|$. Let $s\mathbb{N}^*$ be a non empty sequence such that $r = [*r_2, *s]$. Now, since $r_1 \prec r$ and $|r_1| \leq |r_2|$, we must have $r_1 \preceq r_2$. $\qquad\square$

**Lemma 2.13.** *Let $r_1, r_2, r_3 \in \mathbb{N}^*$. If $r_1 < r_2$ and $r_2 \prec r_3$, then $r_1 < r_3$*

*Proof.* We have

$$r_1 = [*r, k], r_2 = [*r, *s], r_3 = [*r, *s, *z]$$

where $s[0] > k$, thus $r_1 < r_3$. $\qquad\square$

**Lemma 2.14.** *Let $r_1, r_2, r_3 \in \mathbb{N}^*$. If $r_1 \prec r_2$ and $r_2 < r_3$, then $r_1 \prec r_3$*

*Proof.* We have
$$r_2 = [*r_1, *z, *k], r_3 = [*r_1, *z, *s],$$
where $z \neq []$, then $r_1 \prec r_3$. $\qquad\square$

**Lemma 2.15.** *For any $r_1, r_2, r_3 \in \mathbb{N}^*$ we have*

$$r_1 \not< r_1, \tag{7}$$

$$r_1 < r_2 \text{ and } r_2 < r_3 \implies r_1 < r_3. \tag{8}$$

*Proof.* $r_1 \not< r_1$ follows directly from definition.
Now, take any $r_1, r_2, r_3 \in \mathbb{N}^*$ such that $r_1 < r_2$ and $r_2 < r_3$. Assume that $\mathsf{i}_{r_1, r_2} \leq \mathsf{i}_{r_2, r_3}$. Then
$$r_1[k] = r_2[k] = r_3[k]$$
for all $k \leq \mathsf{i}_{r_1, r_2}$. Note that

$$r_1[\hat{\mathsf{i}}_{r_1, r_2}] < r_2[\hat{\mathsf{i}}_{r_1, r_2}] \leq r_3[\hat{\mathsf{i}}_{r_1, r_2}],$$

thus $r_1 < r_3$.
Now, assume that $\mathsf{i}_{r_1, r_2} > \mathsf{i}_{r_2, r_3}$, then
$$r_1[k] = r_2[k] = r_3[k]$$
for all $k \leq \mathsf{i}_{r_2, r_3}$. Note that

$$r_1[\hat{\mathsf{i}}_{r_2, r_3}] = r_2[\hat{\mathsf{i}}_{r_2, r_3}] < r_3[\hat{\mathsf{i}}_{r_2, r_3}],$$

thus $r_1 < r_3$. $\qquad\square$

**Corollary 2.16.** $\leq$ *on $N^*$ is a locally finite poset.*

**Definition 2.17** (**context**)**.** *A $D$ is a context iff $D \subset \mathbb{N}^*$ and there exists $r \in \mathbb{N}^*$ such that for all $x \in D$, we have*

  *1. $r \prec x$,*

  *2. $\{y \in \mathbb{N}^* : r \prec y < x\} \subset D$,*

  *3. $\{y \in \mathbb{N}^* : r \prec y \prec x\} \subset D$.*

*Such $r$ will be called a root of a context $D$.*

Note that $\emptyset$ is a context and for any $r \in \mathbb{N}^*$ r is a root of $\emptyset$.

**Proposition 2.18.** *If $D$ is a nonempty context with a root $r$, then $[*r, 0] \in D$.*

*Proof.* Take any $x \in D$. Since $r \prec x$, there exists $k \in \mathbb{N}$ and $s \in \mathbb{N}^*$ such that $x = [*r, k, *s]$. If $k > 0$, we have $r \prec [*r, 0] < x$, thus by definition $[*r, 0] \in D$. If $k = 0$, then we have $r \prec [*r, 0] \prec x$, and again by definition $[*r, 0] \in D$. $\qquad\square$

**Proposition 2.19.** *If $r_1$ and $r_2$ are roots of a context $D \neq \emptyset$, then $r_1 = r_2$.*

*Proof.* Since $[*r_1, 0], [*r_2, 0] \in D$ we have both $r_1 \prec [*r_2, 0]$ and $r_2 \prec [*r_1, 0]$. And thus $r_1 \preceq r_2$ and $r_2 \preceq r_1$. Thus $r_1 = r_2$. $\qquad\square$

We can then introduce a function root. For any non empty $D$, $\mathrm{root}(D)$ is a root of a context $D$.
Also for any nonempty $D$, $\overline{D} \overset{\text{def}}{=} D \cup \mathrm{root}(D)$.

**Definition 2.20.** *Let $D$ be a context and $x_0 \in D$.*

$$Ctx(D, x_0) \overset{\text{def}}{=} \{x \in D : x_0 \prec x\}. \tag{9}$$

**Theorem 2.21.** *If $D$ is a context and $x_0 \in D$, then $Ctx(D, x_0)$ is a context with a root $x_0$.*

*Proof.* Let $r$ be a root of $D$. Take any $x \in \mathrm{Ctx}(D, x_0)$. By definition $x \in D$ and $x_0 \prec x$.
Take any $y \in \mathbb{N}^*$ such that $x_0 \prec y < x$. We have $r \prec x_0$, thus $r \prec y < x$ and since $D$ is a context with root $r$, we have $y \in D$. But $x_0 \prec y$, thus $y \in \mathrm{Ctx}(D, x_0)$.
Thus $\{y \in \mathbb{N}^* : x_0 \prec y < x\} \subset \mathrm{Ctx}(D, x_0)$.
Take any $y \in \mathbb{N}^*$ such that $x_0 \prec y \prec x$, thus $r \prec y \prec x$, so $y \in D$. But $x_0 \prec y$, thus $y \in \mathrm{Ctx}(D, x_0)$.
Thus $\{y \in \mathbb{N}^* : x_0 \prec y \prec x\} \subset \mathrm{Ctx}(D, x_0)$. $\qquad\square$

**Theorem 2.22.** *Let $D$ be a context and $x_0 \in D$.*
*For any $x \in Ctx(D, x_0)$ and $z \in D$, if $x < z$, then $z \in Ctx(D, x_0)$.*

*Proof.* Since $x_0 \prec x$ and $x < z$, by Lemma 2.13, $x_0 \prec z$ and thus $z \in \mathrm{Ctx}(D, x_0)$. $\qquad\square$

**Theorem 2.23.** *Let $D$ be a context. If $r_1 \not\prec r_2$, $r_2 \not\prec r_1$ and $r_1 \neq r_2$ we have*

$$Ctx(D, r_1) \cap Ctx(D, r_2) = \emptyset.$$

*Proof.* Assume to the contrary that there exists $r \in \mathrm{Ctx}(D, r_1) \cap \mathrm{Ctx}(D, r_2)$. Thus by Proposition 2.12, we have $r_1 \preceq r_2$ or $r_2 \preceq r_1$, which contradics assumptions of this theorem. $\qquad\square$

And then by Corollary 2.10, we have the following:

**Corollary 2.24.** *Let $D$ be a context. If $r_1 < r_2$, then*

$$Ctx(D, r_1) \cap Ctx(D, r_2) = \emptyset.$$

**Lemma 2.25.** *Let $r, s \in \mathbb{N}^*$. If $[*r, 0] \not\prec [*s, 0]$ and $[*r, 0] < [*s, 1]$, then $r = s$.*

*Proof.* Let $r_1 = [*r, 0]$ and $r_2 = [*s, 1]$. Since $[*r, 0] < [*s, 1]$, $\mathfrak{i}_{r_1, r_2} \leq |r| - 1$. Since $[*r, 0] \not\prec [*s, 0]$, we must have $\mathfrak{i}_{r_1, r_2} = |r| - 1$. Thus $r = s$. $\qquad\square$

**Lemma 2.26.** *Let $r, x \in \mathbb{N}^*$ and $r_0 = [*r, 0]$, then for any $x < r_0$, we have $x < r$.*

*Proof.* Assume that $x < r_0$. Note that $\mathfrak{i}_{x,r_0} < |r| - 1$. Thus

$$x[\mathfrak{i}_{x,r_0}] = r_0[\mathfrak{i}_{x,r_0}] = r[\mathfrak{i}_{x,r_0}]$$

and

$$x[\hat{\mathfrak{i}}_{x,r_0}] < r_0[\hat{\mathfrak{i}}_{x,r_0}] = r[\hat{\mathfrak{i}}_{x,r_0}].$$

$\square$

**Theorem 2.27.** *Let $D$ be a context, $s \in \mathbb{N}^*$ and $k_0 \in \mathbb{N}$. If $[*s, k_0] \in D$, then for all $k \in \langle 0, k_0 \rangle$, we have $[*s, k] \in D$.*

*Proof.* Take an $r \in \mathbb{N}^*$ which is a root of $D$. Take $[*s, k_0] \in D$. Since $r \prec [*s, k_0]$, we have $r \preceq s$. Since $[*r, 0] \in D$ and we have $[*r, 0] < [*s, k] < [*s, k_0]$ for $k \in (0, k_0)$, hence $[*s, k] \in D$. If $[*r, 0] < [*s, 0]$ then $[*r, 0] < [*s, 0] < [*s, k_0]$ and $[*s, 0] \in D$. If $[*r, 0] \not< [*s, 0]$ but $[*r, 0] < [*s, 1]$, there must be $r = s$ and thus anyway $[*s, 0] \in D$. $\square$

**Definition 2.28.** *Let $D$ be a nonempty context.*

$$\mathit{final}(D) \stackrel{\text{def}}{=} [*\mathit{root}(D), k_0] \in D, \tag{10}$$

*such that for all $k \in \mathbb{N}$ and $k > k_0$, $[*\mathit{root}(D), k] \notin D$.*

**Definition 2.29.** *$d : \mathbb{N}^* \to \mathbb{N} \cup \{-1\}$ such that $d(\rho) \stackrel{\text{def}}{=} |\rho| - 1$.*

**Lemma 2.30.** *Let $D$ be a nonempty context with root $r \in \mathbb{N}^*$. Let $r_k = [*r, k]$ for $k = 0, \ldots, k_f$ where $r_{k_f} = \mathit{final}(D)$. Let $A_{-1} = \{x < r : x \in \mathbb{N}^*\}$ and*

$$A_k = \{x < r_k : x \in \mathbb{N}^*\}$$

*for $k = 0, \ldots, k_f$, then*

$$A_{-1} = A_0$$

*and*

$$A_{k-1} \subset A_k$$

*for $k = 0, \ldots, k_f$.*

*Proof.* By Lemma 2.13, we have $A_{-1} \subset A_0$. By Lemma 2.26, we have $A_0 \subset A_{-1}$. Thus $A_{-1} = A_0$.

$$A_{k-1} \subset A_k$$

for $k = 1, \ldots, k_f$ follows from transitivity of $<$.

$\square$

**Lemma 2.31.** *Let $D$ be a nonempty context with root $r \in \mathbb{N}^*$. Let $r_k = [*r, k]$ for $k = 0, \ldots, k_f$ where $r_{k_f} = \text{final}(D)$. For any $z \in Ctx(D, r_k)$,*

$$\{x \in D \setminus Ctx(D, r_k) : x < z\} = \{r_0, \ldots, r_{k-1}\}.$$

*Proof.* Take any $z \in \text{Ctx}D, r_k$. Then $z = [*r, k, *s]$ with $s \neq []$. Take $x \in D \setminus \text{Ctx}(D, r_k)$ such that $x < z$. If $\mathfrak{i}_{x,z} \geq |r|$, then $x \in D$, so $\mathfrak{i}_{x,z} < |r|$. But if $\mathfrak{i}_{x,z} < |r| - 1$, then $x \notin D$, thus $\mathfrak{i}_{x,z} = |r| - 1$. Hence $x = [*r, k']$ where $0 \leq k' < k$. $\qquad\square$

# 3 Reference System and Proof

## 3.1 First Order Logic Preleminaries

We consider a language of first order logic. Let $\mathscr{V}$ be an infinite countable set of variable symbols.

**Definition 3.1.** *Let $\mathscr{C}$ be a set of constant symbols, let $\mathscr{P}$ be a set of predicate symbols and $\mathscr{F}$ be a set of function symbols. then $\mathscr{L} \stackrel{\text{def}}{=} (\mathscr{C}, \mathscr{P}, \mathscr{F})$ is a signature of a language.*

**Definition 3.2** (**Skolem symbols**). *Let $\mathcal{S}_C \stackrel{\text{def}}{=} \{\mathfrak{s}_r^0 : r \in \mathbb{N}^*\}$. Let $\mathcal{S}_F \stackrel{\text{def}}{=} \{\mathfrak{s}_r^k : r \in \mathbb{N}^*, k \in \mathbb{N} \setminus \{0\}\}$ If $\mathscr{L} = (\mathscr{C}, \mathscr{P}, \mathscr{F})$ is a signature of a language, then*

$$\mathscr{L}^+ = (\mathscr{C} \cup \mathcal{S}_C, \mathscr{P}, \mathscr{F} \cup \mathcal{S}_F).$$

$\mathfrak{s}_r^k$ is intended to use as function symbol of arity $k$ for $k > 0$ and constant symbol for $k = 0$. When not ambiguous we will use $\mathfrak{s}_r^k$ for $k > 0$ to denote the whole term with $k$ free variables.

Let $\mathcal{F}(\mathscr{L})$ be a set of all first order logic formulas with all non logical symbols from signature $\mathscr{L}$ and variables from the set $\mathscr{V}$.

**Definition 3.3.** *Let $\mathscr{L} = (\mathscr{C}, \mathscr{P}, \mathscr{F})$ be a signature of a language and let $r \in \mathbb{N}^*$.*

$$\mathscr{L}_r \stackrel{\text{def}}{=} \left(\mathscr{C} \cup \{\mathfrak{s}_\rho^0 : \rho < r\}, \mathscr{P}, \mathscr{F} \cup \left\{\mathfrak{s}_\rho^m : \rho < r, m \in \mathbb{N} \setminus \{0\}\right\}\right). \tag{11}$$

$$\overline{\mathscr{L}}_r \stackrel{\text{def}}{=} \left(\mathscr{C} \cup \{\mathfrak{s}_\rho^0 : \rho \leq r\}, \mathscr{P}, \mathscr{F} \cup \left\{\mathfrak{s}_\rho^m : \rho \leq r, m \in \mathbb{N} \setminus \{0\}\right\}\right). \tag{12}$$

**Definition 3.4.** *Let $\mathscr{L}(\mathscr{C}, \mathscr{P}, \mathscr{F})$ be a signature of a language, let $\alpha \in \mathcal{F}(\mathscr{L})$ and let $\tau$ be an arbitrary term.*

$$\textit{free}(\alpha) \stackrel{\text{def}}{=} \{v \in \mathscr{V} : \text{there is at least one occurence of } v \in \alpha \tag{13}$$
$$\textit{not bound by any quantifier}\}, \tag{14}$$

$$\textit{free}(\tau) \stackrel{\text{def}}{=} \{v \in \mathscr{V} : v \text{ occurs in } \tau\}, \tag{15}$$

$$\textit{bound}(\alpha) \stackrel{\text{def}}{=} \{v \in \mathscr{V} : \text{ there exists a quantifier which bounds variable } v\}. \tag{16}$$

**Definition 3.5** (**substitution**). *Let $\mathscr{L}$ be a signature of a language. If $\alpha \in \mathcal{F}(\mathscr{L})$ and $\tau$ is an arbitrary term and $x \in \mathscr{V}$, then by $\alpha(x/\tau)$ we denote a formula in which each instance of a free variable $x$ is replaced by a term $\tau$.*

**Definition 3.6** (**simultaneous substitution**). *Let $\mathscr{L}$ be a signature of a language. If $\alpha \in \mathcal{F}(\mathscr{L})$, $\tau_1, \ldots, \tau_k$ are arbitrary terms and $x_1, \ldots, x_k \in \mathscr{V}$ are pairwise distinct, then by $\alpha(x_1/\tau_1, \ldots, x_k/\tau_k)$ we denote a formula in which each instance of a free variable $x_i$ is replaced by a term $\tau_i$ for $i = 1, \ldots, k$.*

**Definition 3.7** (**admissible substitution**). *Let $\mathscr{L}$ be a signature of a language. Let $\alpha \in \mathcal{F}(\mathscr{L})$ and $\tau$ be an arbitrary term. $\alpha(x/\tau)$ is admissible iff no free occurrence of $x$ in $\alpha$ is in the range of a quantifier that binds any variable which appears in $\tau$.*

**Definition 3.8** (**admissible simultaneous substitution**). *Let $\mathscr{L}$ be a signature of a language. Let $\alpha \in \mathcal{F}(\mathscr{L})$, $\tau_1, \ldots, \tau_k$ be arbitrary terms and $x_1, \ldots, x_k \in \mathscr{V}$ pairwise distinct. $\alpha(x_1/\tau_1, \ldots, x_k/\tau_k)$ is admissible iff no free occurrence of $x_i$ in $\alpha$ is in the range of a quantifier that binds any variable which appears in $\tau_i$ for $i = 1, \ldots, k$.*

We will also employ the well-established notion of an $\mathscr{L}$-structure from the literature, (e.g. [**?** ]) which is defined as a domain equipped with a set of relations, a set of functions, and a set of objects corresponding to the predicate symbols, function symbols, and constants of $\mathscr{L}$, respectively.

**Definition 3.9.** *Let $\mathscr{L}$ be a signature of a language. Let $\mathbf{M}$ be a $\mathscr{L}$-structure with domain $A$ and let $j : \mathscr{V} \to A$ be an assignment of variables. Then we define*

$$j\frac{a}{x}(v) \overset{\text{def}}{=} \begin{cases} a \text{ if } v = x, \\ j(v) \text{ otherwise.} \end{cases} \tag{17}$$

**Theorem 3.10.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha \in \mathcal{F}(\mathscr{L})$ and let $\tau$ be an arbitrary term. If $\alpha(x/\tau)$ is admissible, then for any $\mathscr{L}$-structure $\mathbf{M}$ with domain $A$ and for any assignment of variables $j : \mathscr{V} \to A$ we have*

$$(\mathbf{M}, j\frac{\tau^{(\mathbf{M}, j)}}{x}) \models \alpha \ \text{ iff } (\mathbf{M}, j) \models \alpha(x/\tau). \tag{18}$$

*Proof.* Denote $\tau$ by $\tau(x_1, \ldots, x_n)$ whete $x_i$ are all free variables used in term $\tau$. Take any place in a formula $\alpha(x/\tau)$ where $\tau(x_1, \ldots, x_n)$ sits after replacement for $x$. Since $\alpha(x/\tau)$ is addmissable, all $x_i$ in this place are free. Then under interpretation $j$ term $\tau$ becomes $\tau^{\mathbf{M}}(j(x_1), \ldots, j(x_n))$. Since there is no free variable $x$ in $\alpha(x/\tau)$, $\alpha$ under interpretation $j\frac{\tau^{(\mathbf{M},j)}}{x}$ is exactly the same thing as $\alpha(x/\tau)$ under interpretation $j$. $\square$

We can easily demonstrate that the assumption of *admissability* in the above theorem is neccesary. Consider a trivial example for a model of Peano Aryth-metic. Let $\alpha$ be a formula $\ulcorner \exists y.x = y \urcorner$ and let $\tau$ be $\ulcorner S(y) \urcorner$. Obviously $\alpha(x/\tau)$ is

not admissable and becomes $\ulcorner \exists y.S(y) = y \urcorner$ which is simply false in any model of Peano Arythmetic.

**Definition 3.11.** *Let $\mathscr{L} = (\mathscr{C}, \mathscr{P}, \mathscr{F})$ be a signature of a language, $P \in \mathscr{P}$ and $\alpha, \phi \in \mathcal{F}(\mathscr{L})$. By $\alpha(P(x_1, \ldots, x_k)/\phi)$ with $x_1, \ldots, x_k \in \mathscr{V}$ pairwise distinct, we will denote a formula $\alpha$ with each occurence of $P(\tau_1, \ldots, \tau_k)$, where $\tau_1, \ldots, \tau_k$ are terms from a given occurence, replaced by $\phi(x_1/\tau_1, \ldots, x_k/\tau_k)$.*

*We say that $\alpha(P(x_1, \ldots, x_k)/\phi)$ is admissible if for each occurnce of $P(\tau_1, \ldots, \tau_k)$ in $\alpha$:*

1. *$\phi(x_1/\tau_1, \ldots, x_k/\tau_k)$ is admissible,*

2. *an occurence $P(\tau_1, \ldots, \tau_k)$ is not in range of any quantifier which binds a variable from $free(\phi) \setminus \{x_1, \ldots, x_k\}$.*

**Lemma 3.12.** *Let $\mathscr{L} = (\mathscr{C}, \mathscr{P}, \mathscr{F})$ be a signature of a language and let $P \in \mathscr{P}$. Let $\phi \in \mathcal{F}(\mathscr{L})$ and $x_1, \ldots, x_k \in \mathscr{V}$ be pairwise distinct. Let $j_0 : free(\phi) \setminus \{x_1, \ldots, x_k\} \to A$, where $A$ is a domain of an $\mathscr{L}$-structure $M$ for which*

$$M, j \models P(x_1, \ldots, x_k) \text{ iff } M, j \models \phi \tag{19}$$

*for any $j$ that is an extention of $j_0$. If $\psi \in \mathcal{F}(\mathscr{L})$ and $\psi(P(x_1, \ldots, x_k)/\phi)$ is admissible, then*

$$M, j \models \psi \text{ iff } M, j \models \psi(P(x_1, \ldots, x_k)/\phi) \tag{20}$$

*for any $j$ that is an extention of $j_0$.*

*Proof.* We will prove it via induction over structure of $\psi$. Assume that $\psi(P(x_1, \ldots, x_k)/\phi)$ is admissible. In first step we will show the "if" part holds for an atomic formula $\psi$. If $\psi$ is $B(\tau_1, \ldots, \tau_m)$ where $B$ is not $P$ or $m \neq k$, then $\psi$ is the same as $\psi(P(x_1, \ldots, x_k)/\phi)$ and "if" part holds trivially.

Let's assume that that $\psi$ is $P(\tau_1, \ldots, \tau_k)$. Take an arbitrary $j$ that is an extension of $j_0$.

$$M, j \models P(\tau_1, \ldots, \tau_k) \text{ iff } M, j \frac{\tau_1^{M,j}}{x_1} \ldots \frac{\tau_k^{M,j}}{x_k} \models P(x_1, \ldots, x_k). \tag{21}$$

Note that $j \frac{\tau_1^{M,j}}{x_1} \ldots \frac{\tau_k^{M,j}}{x_k}$ is still an extension of $j_0$, therefore

$$M, j \models P(\tau_1, \ldots, \tau_k) \text{ iff } M, j \frac{\tau_1^{M,j}}{x_1} \ldots \frac{\tau_k^{M,j}}{x_k} \models \phi. \tag{22}$$

Since $\phi(x_1/\tau_1, \ldots, x_k/\tau_k)$ is admissible, we have

$$M, j \models P(\tau_1, \ldots, \tau_k) \text{ iff } M, j \models \phi(x_1/\tau_1, \ldots, x_k/\tau_k). \tag{23}$$

And therefore by Definition 3.11, we have

$$M, j \models \psi \text{ iff } M, j \models \psi(P(x_1, \ldots, x_k)/\phi). \tag{24}$$

It is an easy exercise to show that if "if" part holds for formulas $\alpha$ and $\beta$, then it holds for a formula $\alpha \rightarrow \beta$. Having this done for $\rightarrow$ we can go easily through all other logical connectives.

This leaves us with quantifiers to deal with.

Assume that "if" part holds for formulas $\alpha$, we will show that "if" part holds for $\psi$ being $\forall u.\alpha$. Note that since $\psi(P(x_1, \ldots, x_k)/\phi)$ is admissible, $\alpha(P(x_1, \ldots, x_k)/\phi)$ is admissible.

Take an arbitrary $j$ that is extension of $j_0$. We have

$$M, j \models \forall u.\alpha \text{ iff } M, j\frac{a}{u} \models \alpha \text{ for any } a \in A. \tag{25}$$

Take any $a \in A$. If $u \in \{x_1, \ldots, x_k\}$ then $j\frac{a}{u}$ is still an extension of $j_0$. If $u \notin \{x_1, \ldots, x_k\}$, then since $\psi(P(x_1, \ldots, x_k)/\phi)$ is admissible, we must have $u \notin \text{free}(\phi)$, thus $j\frac{a}{u}$ is still an extension of $j_0$. Since $j\frac{a}{u}$ is an extension of $j_0$, by induction assumption we have

$$M, j\frac{a}{u} \models \alpha \text{ iff } M, j\frac{a}{u} \models \alpha(P(x_1, \ldots, x_k)/\phi). \tag{26}$$

Since $a \in A$ was arbitrary, therefore

$$M, j \models \forall u.\alpha \text{ iff } M, j \models \forall u.\alpha(P(x_1, \ldots, x_k)/\phi). \tag{27}$$

Analogously one can show that 'if" part holds for $\psi$ being $\exists u.\alpha$. It is enough to repeat the above argument for a chosen $a \in A$.

$\square$

**Theorem 3.13.** *Let $\mathscr{L} = (\mathscr{C}, \mathscr{P}, \mathscr{F})$ be a signature of a language and $P \in \mathscr{P}$. Let $\phi, \psi \in \mathcal{F}(\mathscr{L})$ and let $x_1, \ldots, x_k \in \mathscr{V}$ be pairwise distinct. If $\models \psi$ and $\psi(P(x_1, \ldots, x_k)/\phi)$ is admissible, then $\models \psi(P(x_1, \ldots, x_k)/\phi)$.*

*Proof.* Let $P' \notin \mathscr{P}$, let $\mathscr{L}' = (\mathscr{C}, \mathscr{P} \cup \{P'\}, \mathscr{F})$. Let $\psi'$ be $\psi$ with simple replacement of predicative symbol $P$ into $P'$. One can easily show that $\models \psi'$.

Take an arbitrary $\mathscr{L}$-structure $M$ and take an arbitrary $j_0 : \text{free}(\phi)\backslash\{x_1, \ldots, x_k\} \rightarrow A$. Let $M'_{j_0}$ be a $\mathscr{L}'$-structure which is an extention of $M$ and $P'$ is modeled such that

$$M'_{j_0}, j \models P'(x_1, \ldots, x_k) \text{ iff } M'_{j_0}, j \models \phi \tag{28}$$

for any assignment $j$ that is an extention of $j_0$. Then by Lemma 3.12, we have

$$M'_{j_0}, j \models \psi' \text{ iff } M'_{j_0}, j \models \psi(P'(x_1, \ldots, x_k)/\phi) \tag{29}$$

for any assignment $j$ that is an extention of $j_0$. And since $\models \psi'$, we have

$$M'_{j_0}, j \models \psi(P'(x_1, \ldots, x_k)/\phi) \tag{30}$$

for any assignment $j$ that is an extention of $j_0$.
But since $\psi(P'(x_1, \ldots, x_k)/\psi) \in \mathcal{F}(\mathscr{L})$ and $M'_{j_0}$ is an extension of $M$, we have

$$M, j \models \psi(P'(x_1, \ldots, x_k)/\phi) \tag{31}$$

for any assignment $j$ that is an extention of $j_0$. Since $j_0$ was arbitrarly chosen we have proven the thesis.

$\square$

## 3.2  Context Proof Definition

**Definition 3.14.** *A tuple $(D, \mathscr{L}, \gamma)$ is called a reference system iff*

1. *$\mathscr{L}$ is a signature of a language*

2. *$D \subset \mathbb{N}^*$ and $D$ is an notempty context,*

3. *$\gamma : \overline{D} \to \mathcal{F}(\mathscr{L}^+)$.*

**Definition 3.15.** *Let $\Gamma = (D, \mathscr{L}, \gamma)$ be a reference system. For $\rho \in D$ we define*

$$\mathit{fixed}_\Gamma(\rho) \overset{\text{def}}{=} \bigcup_\eta \{\mathit{free}(\alpha_\eta) : \eta \in D \text{ and } \eta \prec \rho \text{ and } \gamma_\eta = \ulcorner \alpha_\eta \to \beta_\eta \urcorner\}. \tag{32}$$

In other words $\mathit{fixed}_D(\rho)$ is a set of all free variables which occurs in antecedent if $\gamma_\eta$ is in implication form for all $\eta \in D$ which are prefix of $\rho$.

**Definition 3.16** (**proof**). *Let $\mathscr{L}$ be a signature of a language. A reference system $\Gamma = (D, \mathscr{L}^+, \gamma)$ is a proof of $\psi \in \mathcal{F}(\mathscr{L}^+)$ with respect to $\mathcal{A} \subset \mathcal{F}(\mathscr{L}^+)$ iff for $r = root(D)$, $\gamma_r = \psi$ and for any $\rho \in \overline{D}$ the following conditions holds:*

1. *if $Ctx(D, \rho) = \emptyset$, then $\gamma_\rho \in \mathcal{F}(\overline{\mathscr{L}}_\rho)$ and at least one of the following holds:*

    (a) *(AXM) $\gamma_\rho \in \mathcal{A}$,*

    (b) *(ASM) there exists $\eta \prec \rho$ and $\beta \in \mathcal{F}(\mathscr{L}^+)$ such that $\gamma_\eta = \ulcorner \gamma_\rho \to \beta \urcorner$,*

    (c) *(MOD) there exist $\eta_1, \eta_2 < \rho$, such that*

    $$\gamma_{\eta_1} = \ulcorner \gamma_{\eta_2} \to \gamma_\rho \urcorner, \tag{33}$$

    (d) *(GEN) there exists $\eta < \rho$ and $x \in \mathscr{V} \setminus \mathit{fixed}_\Gamma(\rho)$ such that*

    $$\gamma_\rho = \ulcorner \forall x. \gamma_\eta \urcorner, \tag{34}$$

12

(e) *(SKO) there exists $\eta < \rho$, $x \in \mathscr{V}$, $\beta \in \mathcal{F}(\mathscr{L}^+)$ and $m \in \mathbb{N}$ such that $\gamma_\rho = \beta(x/\mathfrak{s}_\rho^m)$, $\mathit{free}(\mathfrak{s}_\rho^m) = \mathit{free}(\gamma_\eta)\backslash\mathit{fixed}_\Gamma(\rho)$ with $\beta(x/\mathfrak{s}_\rho^m)$ admissible and*

$$\gamma_\eta = \ulcorner \exists x.\beta \urcorner, \tag{35}$$

2. *if $\mathit{Ctx}(D, \rho) \neq \emptyset$, then $\gamma_\rho \in \mathcal{F}(\mathscr{L}_\rho)$ and there exists $\alpha \in \mathcal{F}(\mathscr{L}^+)$ such that*

$$\gamma_\rho = \ulcorner \alpha \rightarrow \gamma_\eta \urcorner, \tag{36}$$

*where $\eta = \mathit{final}(\mathit{Ctx}(D, \rho))$.*

The usage of $\mathit{fixed}_\Gamma(\rho)$ for GEN rule is a motivation for the word *fixed* in Definition 3.15.

## 4 Completness

Let us introduce a certain set of logical axioms. An implication transitivity axiom and 2 other quantifier related axioms are omitted for a purpose.

**Definition 4.1** (**logical axioms**). *Let $\mathfrak{t}$ be a chosen predicate symbol of $0$-arity. For any formulas $\alpha, \beta, \gamma \in \mathcal{F}(\mathscr{L}^+)$ the following are logical axioms:*

1. *(THR) $\mathfrak{t}$*

2. *(LEM) $\alpha \vee \neg\alpha$*

3. *(IMP) $\alpha \rightarrow (\beta \rightarrow \alpha)$*

4. *(ANL) $\alpha \wedge \beta \rightarrow \alpha$*

5. *(ANR) $\alpha \wedge \beta \rightarrow \beta$*

6. *(AND) $\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta))$*

7. *(ORL) $\alpha \rightarrow \alpha \vee \beta$*

8. *(ORR) $\beta \rightarrow \alpha \vee \beta$*

9. *(DIS) $(\alpha \rightarrow \gamma) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \vee \beta \rightarrow \gamma))$*

10. *(CON) $\neg\alpha \rightarrow (\alpha \rightarrow \beta)$*

11. *(IFI) $(\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \alpha) \rightarrow (\alpha \leftrightarrow \beta))$*

12. *(IFO) $(\alpha \leftrightarrow \beta) \rightarrow (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$*

13. *(ALL) $(\forall x.\alpha) \rightarrow \alpha(x/\tau)$ where $\tau$ is an arbitrary term and $\alpha(x/\tau)$ is admissible.*

14. *(EXT) $\alpha(x/\tau) \rightarrow \exists x.\alpha$ where $\tau$ is an arbitrary term and $\alpha(x/\tau)$ is admissible.*

*Let $\mathfrak{A}$ denotes a set of all formulas which can be obtained by the above schemas.*

**Definition 4.2 (consequence).** *Let $\phi \in \mathcal{F}(\mathscr{L})$ and $\mathcal{A} \subset \mathcal{F}(\mathscr{L})$.*
*$\phi \in Cn_R(\mathcal{A})$ iff there exists a proof $(D, \mathscr{L}, \gamma)$ of $\phi$ or $\ulcorner t \to \phi \urcorner$ with respect to $\mathcal{A}$ with $root(D) = [\,]$.*

**Lemma 4.3 (TRN).** *Let $r \in \mathbb{N}^*$ and $\alpha, \beta, \gamma \in \mathcal{F}(\mathscr{L}_r)$*
*There exists a reference system $(D, \mathscr{L}_r, \gamma)$ with $root(D) = r$ which is a proof of*

$$\ulcorner (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)) \urcorner \tag{37}$$

*with respect to $\mathfrak{A}$.*

*Proof.* ────────────────────────────────────
`[*r]` $\mapsto (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$
`[*r, 0]` $\mapsto (\alpha \to \beta) \to (\alpha \to \gamma)$
`[*r, 0, 0]` $\mapsto \alpha \to \gamma$
`[*r, 0, 0, 0]` $\mapsto \alpha$ **# ASM** $\gamma_{*r,0,0}$
`[*r, 0, 0, 1]` $\mapsto \alpha \to \beta$ **# ASM** $\gamma_{*r,0}$
`[*r, 0, 0, 2]` $\mapsto \beta$ **# MOD** $\gamma_{*r,0,0,1}, \gamma_{*r,0,0}$
`[*r, 0, 0, 3]` $\mapsto \alpha \to (\beta \to \gamma)$ **# ASM** $\gamma_{*r}$
`[*r, 0, 0, 4]` $\mapsto \beta \to \gamma$ **# MOD** $\gamma_{*r,0,0,3}, \gamma_{*r,0,0,0}$
`[*r, 0, 0, 5]` $\mapsto \gamma$ **# MOD** $\gamma_{*r,0,0,4}, \gamma_{*r,0,0,2}$
────────────────────────────────────

$\square$

**Lemma 4.4 (ALH).** *Let $r \in \mathbb{N}^*$ and $\phi, \psi \in \mathcal{F}(\mathscr{L}_r)$. If $\phi$ is a formula for which $x \notin free(\phi)$, then there exists a reference system $(D, \mathscr{L}_r, \gamma)$ with $root(D) = r$ which is a proof of*

$$\ulcorner \big( \forall x.(\phi \to \psi) \big) \to \big( \phi \to \forall x.\psi \big) \urcorner \tag{38}$$

*with respect to $\mathfrak{A}$.*

*Proof.* ────────────────────────────────────
`[*r]` $\mapsto \big( \forall x.(\phi \to \psi) \big) \to \big( \phi \to \forall x.\psi \big)$
`[*r, 0]` $\mapsto \phi \to \forall x.\psi$
`[*r, 0, 0]` $\mapsto \forall x.(\phi \to \psi)$ **# ASM** $\gamma_{*r}$
`[*r, 0, 1]` $\mapsto \big( \forall x.(\phi \to \psi) \big) \to (\phi \to \psi)$ **# Axiom ALL**
`[*r, 0, 2]` $\mapsto \phi \to \psi$ **# MOD** $\gamma_{*r,0,1}, \gamma_{*r,0,0}$
`[*r, 0, 3]` $\mapsto \phi$ **# ASM** $\gamma_{*r,0}$
`[*r, 0, 4]` $\mapsto \psi$ **# MOD** $\gamma_{*r,0,2}, \gamma_{*r,0,3}$
`[*r, 0, 5]` $\mapsto \forall x.\psi$ **# GEN** $\gamma_{*r,0,4}$
────────────────────────────────────

Note that the assumption that $x \notin \text{free}(\phi)$ is needed to be able to apply a rule GEN $\gamma_{*r,0,5}$. $\square$

**Lemma 4.5 (EXH).** *Let $r \in \mathbb{N}^*$ and $\phi, \psi \in \mathcal{F}(\mathscr{L}_r)$. If $\phi$ is a formula for which $x \notin free(\phi)$, then there exists a reference system $\Gamma = (D, \mathscr{L}^+, \gamma)$ with $root(D) = r$ which is a proof of*

$$\ulcorner \big( \forall x.(\psi \to \phi) \big) \to \big( (\exists x.\psi) \to \phi \big) \urcorner \tag{39}$$

*with respect to $\mathfrak{A}$.*

*Proof.*

```
[*r]       ↦ (∀x.(ψ → φ)) → ((∃x.ψ) → φ)
[*r, 0]    ↦ (∃x.ψ) → φ
[*r, 0, 0] ↦ ∀x.(ψ → φ) # ASM γ_*r
[*r, 0, 1] ↦ ∃x.ψ # ASM γ_*r,0
[*r, 0, 2] ↦ ψ(x/𝔰⁰_[*r,0,2]) # SKO γ_*r,0,1
[*r, 0, 3] ↦ (∀x.(ψ → φ)) → (ψ(x/𝔰⁰_[*r,0,2]) → φ), # ALL
[*r, 0, 4] ↦ ψ(x/𝔰⁰_[*r,0,2]) → φ # MOD γ_*r,0,3, γ_*r,0,0
[*r, 0, 5] ↦ φ # MOD γ_*r,0,4, γ_*r,0,2
```

Note that the assumption that $x \notin \mathrm{free}(\phi)$ is needed for $\ulcorner \psi \to \phi \urcorner (x/\mathfrak{s}^m_{[*r,0,2]})$ to become $\psi(x/\mathfrak{s}^m_{[*r,0,2]}) \to \phi$. Note that all free variables of $\exists x.\psi$ are in assumption from $[*r,0]$, then $\mathrm{free}(\psi) \setminus \mathrm{fixed}_\Gamma([*r,0,2]) = \emptyset$ and thus we can take const $\mathfrak{s}^0_{[*r,0,2]}$, so $\psi(x/\mathfrak{s}^m_{[*r,0,2]})$ is admissable. $\qquad\square$

**Definition 4.6.** *Let $\mathfrak{B}$ be a set of all formulas from $\mathcal{F}(\mathscr{L}^+)$ which can be obtained by schemas from Lemma 4.3(TRN), Lemma 4.4(ALH) and Lemma 4.5(EXH). Let $\mathfrak{A}^s = \mathfrak{A} \cup \mathfrak{B}$.*

We will use $\vdash$ to indicate established provability known from standard textbooks for First Order Logic. Described e.g. in [**?** ]. Let's recall:

**Definition 4.7.** *Let $T \subset \mathcal{F}(\mathscr{L})$ and $\phi \in \mathcal{F}(\mathscr{L})$. $T \vdash \phi$ iff there exists a sequence $[\phi_i]_{i=0}^n \subset \mathcal{F}(\mathscr{L})$ such that $\phi = \phi_n$ and for any $i = 0, \ldots, n$ at least one of the following holds:*

1. *(AXM) $\phi_i \in (\mathfrak{A}^s \cup T) \cap \mathcal{F}(\mathscr{L})$,*

2. *(MOD) there exist $j_1, j_2 < i$, such that*

$$\phi_{j_1} = \ulcorner \phi_{j_2} \to \phi_i \urcorner, \tag{40}$$

3. *(GEN) there exists $j < i$ and $x \in \mathscr{V}$ such that*

$$\phi_i = \ulcorner \forall x.\phi_j \urcorner. \tag{41}$$

One can show the following lemma.

**Lemma 4.8.** *Let $\mathcal{A} \subset \mathcal{F}(\mathscr{L}^+)$, $(D, \mathscr{L}^+, \gamma)$ be a reference system with $r = \mathrm{root}(D)$, $\gamma_r = \ulcorner \mathfrak{t} \to \phi \urcorner$ with $\phi \in \mathcal{F}(\mathscr{L}^+)$ and let $\mathrm{final}(D) = [*r, k_f]$. If for each $k \in \langle 0, k_f \rangle$, the following statements holds for $\rho = [*r, k]$:*

1. *if $Ctx(D, \rho) = \emptyset$, then $\gamma_\rho \in \mathcal{F}(\overline{\mathscr{L}}_\rho)$ at least one of the following holds:*

   (a) *(AXM) $\gamma_\rho \in \mathcal{A}$,*

   (b) *(MOD) there exist $\eta_1, \eta_2 < \rho$, such that*

   $$\gamma_{\eta_1} = \ulcorner \gamma_{\eta_2} \to \gamma_\rho \urcorner, \tag{42}$$

*(c) (GEN) there exists $\eta < \rho$ and $x \in V$ such that*

$$\gamma_\rho = \ulcorner \forall x.\gamma_\eta \urcorner, \tag{43}$$

*2. if $Ctx(D,\rho) \neq \emptyset$, then $\big(Ctx(D,\rho), \mathscr{L}^+, \gamma\big)$ is a proof of $\gamma_\rho$ with respect to $\mathcal{A}$.*

*Then $(D,\gamma)$ is a proof of $\gamma_r$ with respect to $\mathcal{A}$.*

**Theorem 4.9.** *Let $T \subset \mathcal{F}(\mathscr{L})$ and $\phi \in \mathcal{F}(\mathscr{L})$.*
*If $T \vdash \phi$, then $\phi \in Cn_R(\mathfrak{A} \cup T)$.*

*Proof.* Assume that $T \vdash \phi$. Then by Definition 4.6 we have a sequence $[\phi_i]_{i=0}^n \subset \mathcal{F}(\mathscr{L})$ such that $\phi = \phi_n$ and for any $i = 0, \ldots, n$ at least one of the following holds:

1. (AXM) $\phi_i \in (\mathfrak{A} \cup \mathfrak{B} \cup T) \cap \mathcal{F}(\mathscr{L})$,

2. (MOD) there exist $j_1, j_2 < i$, such that

$$\phi_{j_1} = \ulcorner \phi_{j_2} \to \phi_i \urcorner, \tag{44}$$

3. (GEN) there exists $j < i$ and $x \in \mathscr{V}$ such that

$$\phi_i = \ulcorner \forall x.\phi_j \urcorner. \tag{45}$$

We will construct now a reference system $(D, \mathscr{L}^+, \gamma)$. Let $\gamma_{[]} = \ulcorner \mathfrak{t} \to \phi \urcorner$. Let's define $\gamma_{[i]} = \phi_i$ for $i = 0, \ldots, n$. Note that our main problem are $\phi_i \in \mathfrak{B}$ (the rest is either from $\mathfrak{A}$, or $T$ or are derived from the rest by MOD or GEN). But we can add to each of them their own context proof. Let

$$D_i = \begin{cases} \emptyset \text{ for } \phi_i \in \mathcal{F}(\mathscr{L}) \setminus \mathfrak{B}, \\ P_i \text{ for } \phi_i \in \mathcal{F}(\mathscr{L}) \cap \mathfrak{B}, \end{cases} \tag{46}$$

where in case of $\phi_i \in \mathcal{F}(\mathscr{L}) \cap \mathfrak{B}$, $(P_i, \mathscr{L}^+, \gamma)$ is a proof of $\phi_i$ with respect to $\mathfrak{A}$ where $P_i$ is a context with root $[i]$ as given by Lemma 4.3(TRN), Lemma 4.4(ALH) or Lemma 4.5(EXH). Since all $P_i$ are disjoint, the definition of function $\gamma$ on them is correct.
Now we are ready to define $D$. Let

$$D = \{[i] : i = 0, \ldots, n\} \cup \bigcup_{i=0}^n D_i. \tag{47}$$

By Lemma 4.8, one can show that a refernce system $(D, \mathscr{L}^+, \gamma)$ is a proof of $\ulcorner \mathfrak{t} \to \phi \urcorner$ with respect to $\mathfrak{A}$. $\qquad\square$

**Corollary 4.10 (completness).** *Let $\phi \in \mathcal{F}(\mathscr{L})$. If $\models \phi$, then $\phi \in Cn_R(\mathfrak{A})$.*

*Proof.* Follows from Theorem 4.9 and Gödel's Completeness Theorem (for proof e.g. [**?** ]).

$\qquad\square$

16

# 5 Soudness

**Definition 5.1.** *Let $\mathscr{L}$ be a signature of a language. Let $\Gamma = (D, \mathscr{L}^+, \gamma)$ be a reference system and $T \subset \mathcal{F}(\mathscr{L}^+)$ and $\rho \in D$.*

$$ref_\Gamma(\rho, T) = \{\gamma_\eta : \eta \in D \text{ and } \eta < \rho\} \cup T. \tag{48}$$

**Definition 5.2** (**constrained-proof**). *Let $\mathscr{L}$ be a signature of a language. A reference system $\Gamma = (D, \mathscr{L}^+, \gamma)$ is a constrained-proof of $\psi \in \mathcal{F}(\mathscr{L}^+)$ with respect to $\mathcal{A} \subset \mathcal{F}(\mathscr{L}^+)$ with fixed variables $V \subset \mathscr{V}$ iff for $r = root(D)$, $\gamma_r = \psi$ and for any $\rho \in \overline{D}$ the following conditions holds:*

1. *if $Ctx(D, \rho) = \emptyset$, then $\gamma_\rho \in \mathcal{F}(\overline{\mathscr{L}}_\rho)$ and at least one of the following holds:*

   (a) *(AXM) $\gamma_\rho \in \mathcal{A}$,*

   (b) *(ASM) there exists $\eta \prec \rho$ and $\beta \in \mathcal{F}(\mathscr{L}^+)$ such that $\gamma_\eta = \ulcorner \gamma_\rho \to \beta \urcorner$,*

   (c) *(MOD) there exist $\phi_1, \phi_2 \in ref_\Gamma(\rho, \mathcal{A})$, such that*

   $$\phi_1 = \ulcorner \phi_2 \to \gamma_\rho \urcorner, \tag{49}$$

   (d) *(GEN) there exists $\phi \in ref_\Gamma(\rho, \mathcal{A})$ and $x \in \mathscr{V} \setminus (V \cup fixed_\Gamma(\rho))$ such that*

   $$\gamma_\rho = \ulcorner \forall x. \phi \urcorner, \tag{50}$$

   (e) *(SKO) there exists $\phi \in ref_\Gamma(\rho, \mathcal{A})$, $x \in \mathscr{V}$, $\beta \in \mathcal{F}(\mathscr{L}^+)$ and $m \in \mathbb{N}$ such that $\gamma_\rho = \beta(x/\mathfrak{s}_\rho^m)$, $free(\mathfrak{s}_\rho^m) = free(\phi) \setminus (V \cup fixed_\Gamma(\rho))$ with $\beta(x/\mathfrak{s}_\rho^m)$ admissible and*

   $$\phi = \ulcorner \exists x. \beta \urcorner. \tag{51}$$

2. *if $Ctx(D, \rho) \neq \emptyset$, then $\gamma_\rho \in \mathcal{F}(\mathscr{L}_\rho)$ and there exist $\eta < \rho$ and $\alpha \in \mathcal{F}(\mathscr{L}^+)$ such that*

   $$\gamma_\rho = \ulcorner \alpha \to \gamma_\eta \urcorner, \tag{52}$$

   *where $\eta = final(Ctx(D, \rho))$.*

The intuition behind a *constrained-proof* is that it is a proof in which certain variables are required to behave as constants and it does not require to place axioms in the reference system but rules can be aplied directly to them.
Note that each proof is a *constrained-proof* with $V = \emptyset$.

**Theorem 5.3.** *Let $r \in \mathbb{N}^*$ and let $\mathbf{M}$ be a $\mathscr{L}_r$-structure. Let $T \subset \mathcal{F}(\mathscr{L}_r)$ and $\phi \in \mathcal{F}(\mathscr{L}_r)$. Let $D$ be a context with $r = root(D)$ If $(D, \mathscr{L}^+, \gamma)$ is a constrained-proof of $\phi \in \mathcal{F}(\mathscr{L}_r)$ with respect to $\mathfrak{A} \cup T$ with fixed variables $V \subset \mathscr{V}$, then for any variables assignment $j$ such that $(\mathbf{M}, j) \models T$, we have $(\mathbf{M}, j) \models \phi$.*

*Proof.* We will prove this by induction over $|D|$. Let $|D| = n$. By induction we can assume that

$$\text{Theorem 5.3 holds for any } |D| < n. \tag{53}$$

Let $A$ be a domain of $\mathbf{M}$. Let final$(D) = [*r, k_f]$.

Let $r_k = [*r, k]$ for $k = 0, \ldots, k_f$. Let $\gamma_r = \ulcorner \alpha \to \omega \urcorner$. Note that by Definition 3.16, we have $\phi = \gamma_r$. To simplify notation let $\mathscr{L}_k := \mathscr{L}_{r_k}$ for $k = 0, \ldots, k_f$. Let $\mathcal{F}_k = \mathcal{F}(\mathscr{L}_k)$ for $k = 0, \ldots, k_f$ and let $\mathcal{F}_{-1} = \mathcal{F}(\mathscr{L}_r)$. Let $\overline{\mathcal{F}}_k = \mathcal{F}(\overline{\mathscr{L}_k})$ for $k = 0, \ldots, k_f$ and let $\overline{\mathcal{F}}_{-1} = \mathcal{F}(\overline{\mathscr{L}_r})$. By Lemma 2.30 we have $\mathcal{F}_{k-1} \subset \mathcal{F}_k$ for $k = 0, \ldots, k_f$.

Let

$$T_k = \begin{cases} T & \text{for } k = 0, \\ T \cup \{\gamma_{r_0}, \cdots, \gamma_{r_{k-1}}\} & \text{for } k \in (0, k_f). \end{cases} \tag{54}$$

By Definition 5.2, we have $\gamma_{r_k} \in \overline{\mathcal{F}}_k$. Thus $T_k \subset \mathcal{F}_k$ for $k = 0, \ldots, k_f$.

Take an arbitrary $j_0 : \text{free}(\alpha) \cup V \to A$. Take an arbitrary assignment $j : \mathscr{V} \to A$ such as $j$ is an extension of $j_0$ and $(\mathbf{M}, j) \models T$.

If $(\mathbf{M}, j) \not\models \alpha$, then $(\mathbf{M}, j) \models \neg\alpha$ and thus $(\mathbf{M}, j) \models \ulcorner \alpha \to \omega \urcorner = \phi$.

Hence, we can assume

$$(\mathbf{M}, j) \models \alpha. \tag{55}$$

We will construct recursively a sequence $\mathbf{M}_k$. Let $\mathbf{M}_{-1} = \mathbf{M}$. We will take a special care to construct $\mathbf{M}_k$ in a way which does not depend on assignment $j$ (but it will depend on choice of $j_0$). We will need to rely on this fact in 1d.

We will prove by induction that $(\mathbf{M}_k, j) \models \gamma_k$. Let us write down our induction assumptions.

$$(\mathbf{M}_i, j) \models \gamma_i \text{ for } 0 < i < k, \tag{56}$$

$$\mathbf{M}_i \text{ is } \overline{\mathscr{L}_i}\text{-structure for } 0 < i < k, \tag{57}$$

$$\mathbf{M}_i \text{ is an extension of } \mathbf{M}_{i-1} \text{ for } 0 < i < k \tag{58}$$

Take $k$ from $0, \ldots, k_f$. Note that $(\mathbf{M}_{k-1}, j) \models T_k$. We will consider two cases:

1. $\text{Ctx}(D, r_k) = \emptyset$. By Definition 3.16, $\gamma_{r_k} \in \mathcal{F}_k$ and one of the following cases holds. We will stop a construction step of $\mathbf{M}_k$ after first satisfied case in the following order.

   (a) (AXM) $\gamma_{r_k} \in T \cup \mathfrak{A}$. If $\gamma_{r_k} \in T$, then $(\mathbf{M}_{k-1}, j) \models \gamma_{r_k}$. If $\gamma_{r_k} \in \mathfrak{A}$, then $(\mathbf{M}_{k-1}, j) \models \gamma_{r_k}$ since $\gamma_{r_k}$ is a logical axiom. Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$. Then $(\mathbf{M}_k, j) \models \gamma_{r_k}$.

   (b) (ASM) $\gamma_{r_k} = \alpha$. Then trivially $(\mathbf{M}_k, j) \models \gamma_{r_k}$. Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$. Then $\mathbf{M}_k \models \gamma_{r_k}$.

   (c) (MOD) there exist $\phi_1, \phi_2 \in \text{ref}_D(r_k, T \cup \mathfrak{A})$, such that $\phi_1 = \ulcorner \phi_2 \to \gamma_{r_k} \urcorner$. Note that $\phi_1, \phi_2 \in T_k \cup \mathfrak{A}$. So $(\mathbf{M}_{k-1}, j) \models \ulcorner \phi_2 \to \gamma_{r_k} \urcorner, \phi_2$ and therefore $(\mathbf{M}_{k-1}, j) \models \gamma_{r_k}$. Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$. Then $(\mathbf{M}_k, j) \models \gamma_{r_k}$.

18

(d) (GEN) there exists $\phi \in \mathrm{ref}_D(r_k, T \cup \mathfrak{A})$ and $x \in \mathscr{V} \setminus (V \cup \mathrm{free}(\alpha))$ such that $\gamma_{r_k} = \ulcorner \forall x.\phi \urcorner$. Since $\phi \in T_k \cup \mathfrak{A}$, we have $(\mathbf{M}_{k-1}, j) \models \phi$. Take any $a \in A$. Let

$$j\frac{a}{x}(v) \overset{\text{def}}{=} \begin{cases} a \text{ if } v = x, \\ j(v) \text{ otherwise.} \end{cases} \tag{59}$$

Since $x \notin \mathrm{free}(\alpha)$ and $(\mathbf{M}, j) \models \alpha$, we have $(\mathbf{M}, j\frac{a}{x}) \models \alpha$. Since $x \notin \mathrm{free}(\alpha) \cup V$, $j\frac{a}{x}$ is an extension of $j_0$ similarily as $j$ is, and since $j$ was arbitrarily chosen, we can repeat the reasoning from (55) for an interpretation $j\frac{a}{x}$ up to this point and got $(\mathbf{M}_{k-1}, j\frac{a}{x}) \models \phi$. This is possible because construction of $\mathbf{M}_{k-1}$ nowhere depends on $j$. But since $a \in A$ was arbitrary chosen, we have $(\mathbf{M}_{k-1}, j) \models \forall x.\phi$, and thus $(\mathbf{M}_{k-1}, j) \models \gamma_{r_k}$. Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$. Then $(\mathbf{M}_k, j) \models \gamma_{r_k}$.

(e) (SKO) there exists $\phi \in \mathrm{ref}_D(r_k, T \cup \mathfrak{A})$, $x \in \mathscr{V}$, $\beta \in \mathcal{F}_k$ and $m \in \mathbb{N}$ such that $\gamma_{r_0} = \beta(x/\mathfrak{s}_{r_k}^m)$, $\phi = \ulcorner \exists x.\beta \urcorner$ and $\mathrm{free}(\mathfrak{s}_{r_k}^m) = \mathrm{free}(\phi) \setminus (V \cup \mathrm{free}(\alpha))$ with $\beta(x/\mathfrak{s}_\rho^m)$ admissible. This can only hold for $k > 0$. Since $\phi \in T_k \cup \mathfrak{A}$, we have $(\mathbf{M}_{k-1}, j) \models \exists x.\beta$.

Assume that $\mathrm{free}(\phi) \setminus (V \cup \mathrm{free}(\alpha)) = \{x_1, \ldots, x_n\}$ and that $\beta = \beta(x, x_1, \ldots, x_n, y_1, \ldots, y_m)$ where $y_1, \ldots, y_m \in V \cup \mathrm{free}(\alpha)$ (this sequence can be empty). We will now establish a model for $\mathfrak{s}_{r_k}^m$.

Take any $a_1, a_2, \ldots, a_n \in A$.

If there exists $a \in A$ such that

$$\beta^{\mathbf{M}_{k-1}}(a, a_1, \ldots, a_n, j_0(y_1), \ldots, j_0(y_m)),$$

we choose such an $a$ and set $(\mathfrak{s}_{r_k}^m)^{\mathbf{M}_k}(a_1, \ldots, a_n) = a$.

Otherwise we set $(\mathfrak{s}_{r_k}^m)^{\mathbf{M}_k}(a_1, \ldots, a_n)$ to arbitrary but fixed element of $A$.

Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$ and contains a function $(\mathfrak{s}_{r_k}^m)^{\mathbf{M}_k}$ as defined above. Note that construction of $\mathbf{M}_k$ does not depend on choice of an arbitrary assignment $j$. Since $(\mathbf{M}_{k-1}, j) \models \exists x.\beta$, we have

$$\beta^{\mathbf{M}_{k-1}}\left((\mathfrak{s}_{r_k}^m)^{\mathbf{M}_k}(j(x_1), \ldots, j(x_n)), j(x_1), \ldots, j(x_n), j_0(y_1), \ldots, j_0(y_m)\right).$$

Since $j$ is an extension of $j_0$, we have:

$$\beta^{\mathbf{M}_{k-1}}\left((\mathfrak{s}_{r_k}^m)^{\mathbf{M}_k}(j(x_1), \ldots, j(x_n)), j(x_1), \ldots, j(x_n), j(y_1), \ldots, j(y_m)\right).$$

Therefore $(\mathbf{M}_k, j \dfrac{(\mathfrak{s}_{r_k}^m)^{(\mathbf{M}_k, j)}}{x}) \models \beta$ and since $\beta(x/\mathfrak{s}_\rho^m)$ is admissible, by Theorem 3.10, we have $(\mathbf{M}_k, j) \models \beta(x/\mathfrak{s}_{r_k}^m)$, which is the same as $(\mathbf{M}_k, j) \models \gamma_{r_k}$.

Note that the all above cases work for $k = 0$ without assumptions (56), (57) and (58).

2. $\mathrm{Ctx}(D, r_k) \neq \emptyset$. By Definition 5.2, $\gamma_{r_k} \in \mathcal{F}_k$. Since $T_k \subset \mathcal{F}_k$ and by Lemma 2.31 and by Definition 5.2 we have $\alpha \in \mathcal{F}_{-1} \subset \mathcal{F}_k$, and therefore $\{\alpha\} \cup T_k \subset \mathcal{F}_k$ one can show that $(\mathrm{Ctx}(D, r_k), \mathscr{L}^+, \gamma)$ is a constrained-proof of $\gamma_{r_k}$ with respect to $\mathfrak{A} \cup T_k \cup \{\alpha\}$ with fixed variables $V \cup free(\alpha)$. Since $\mathbf{M}_{k-1}$ is a $\mathscr{L}_k$-structure, $(\mathbf{M}_{k-1}, j) \models T_k \cup \{\alpha\}$ and $|\mathrm{Ctx}(D, r_k)| < n$, by induction assumption (53), we have $(\mathbf{M}_{k-1}, j) \models \gamma_{r_k}$. Let $\mathbf{M}_k$ be an arbitrary chosen but fixed $\overline{\mathscr{L}_k}$-structure which is an extension of $\mathbf{M}_{k-1}$. Then $(\mathbf{M}_k, j) \models \gamma_{r_k}$. Note that the above argument works for $k = 0$ without assumptions (56), (57) and (58).

We showed that $(\mathbf{M}_k, j) \models \gamma_{r_k}$ for $k = 0, \ldots, k_f$. In particular, $(\mathbf{M}_{k_f}, j) \models \gamma_{r_{k_f}}$. But $\gamma_{r_{k_f}} = \omega$ where $\phi = \ulcorner \alpha \to \omega \urcorner \in \mathcal{F}(\mathscr{L}_r)$. Since $\mathbf{M}_{k_f}$ is an extension of $\mathbf{M}$ but $\mathbf{M}$ is a $\mathscr{L}_r$-structure, we have $(\mathbf{M}, j) \models \omega$ and then $(\mathbf{M}, j) \models \phi$. Since $j_0 : free(\alpha) \cup V \to A$ was arbitrarly chosen and $j$ was its arbitrary extension, we proved the thesis. $\qquad \square$

Since there is an additional constrain on (GEN) rule in Definition 3.16 compared to Definition 4.7, that you can not apply generalisation to a variable used as free in any assumption to which you are able to refer and this constrain played a crucial role in a proof of Theorem 5.3, one may wonder if this constrain is really necessary. We will show now a trivial example, how *naive* (GEN) could lead to a false proof.

---

```
[]  ↦ φ(x) → ∀x.φ(x)
[0] ↦ φ(x) # ASM γ[]
[1] ↦ ∀x.φ(x) # 'naive GEN γ₀
```

---

If the above proof was correct, we would have had $\models \phi(x) \to \forall x.\phi(x)$, which is obviously falsifiable.

One may also wonder, if in a rule (SKO) it is really necessary to take a whole function symbol $\mathfrak{s}_\rho^m$ with all free variables instead of just a simple constant $\mathfrak{s}_\rho^0$. After all this is a feature which allowed a construction of model $\mathbf{M}_k$ to be independent on interpretation $j$ in a proof of Theorem 5.3. We will show again a simple example, how such a *naive* rule (SKO) would lead to a false proof.

---

```
[]  ↦ (∀x.∃y.φ(x, y)) → (∃y.∀x.φ(x, y))
[0] ↦ ∀x.∃y.φ(x, y) # ASM γ[]
[1] ↦ (∀x.∃y.φ(x, y)) → (∃y.φ(x, y)) # Axiom ALL
[2] ↦ ∃y.φ(x, y) # MOD γ₁, γ₀
```

---

```
[3]  ↦ φ(x, 𝖘⁰₍₃₎) # naive SKO γ₂
[4]  ↦ ∀x.φ(x, 𝖘⁰₍₃₎) # GEN γ₃
[5]  ↦ (∀x.φ(x, 𝖘⁰₍₃₎)) → (∃y.∀x.φ(x, y)) # Axiom EXT
[6]  ↦ ∃y.∀x.φ(x, y) # MOD γ₅, γ₄
```

if the above proof was correct, we would have had
$\models \big(\forall x.\exists y.\phi(x,y)\big) \to \big(\exists y.\forall x.\phi(x,y)\big)$, which is obviously falsifiable.

# 6    Related Work

The objective of this paper is to describe the logical framework of the kernel for an automatic proof checker and to demonstrate its completeness and soundness. Although analyzing and establishing relationships between this specific solution and related work is an important aspect of scientific research, such an analysis is beyond the scope of the present study. Therefore, we include only a preliminary list of potentially related solutions, leaving a detailed comparative analysis for future work.

The idea of managing local assumptions within proofs has a long history in proof theory, dating back to the Jaśkowski-Fitch [? ], [? ] style of natural deduction, where subproofs or "boxes" represent temporary contexts that are opened and discharged (see also the survey in the Stanford Encyclopedia of Philosophy [? ]).

Several systems have sought to formalize or mechanize this structure. Nested sequent calculi [? ], [? ] generalize Gentzen's sequent systems by organizing sequents in a tree, thereby making the hierarchical proof structure explicit.

Standefer [? ] investigates translations between tree-structured and linear natural-deduction proofs, clarifying how subproof hierarchies can be represented sequentially.

Labelled deductive systems [? ] extend natural deduction by attaching labels to formulas, capturing contextual or modal information within the syntax; this approach resembles the role of reference indices in our system.

Structured proof languages such as Isar [? ] pursue the same goal from a computational perspective, aiming for human-readable, block-structured proofs with machine-checkable semantics.

# A    Formulas isomorphism

We may consider in kernel implementation a variant of proof definitition in Definition 3.16 with case 1 enriched with a rule:

(ISO) there exists $\eta < \rho$ and $\gamma_\eta$ is isomporphic to $\gamma_\rho$.

We will propose the following rigorous treatment of formula isomorphism.

**Definition A.1.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha, \beta \in \mathcal{F}(\mathscr{L})$ and let $f : bound(\alpha) \to \mathscr{V}$.*

$$[f](\alpha) \stackrel{\text{def}}{=} (\alpha \text{ with each bound variable } u \text{ replaced by } f(u)). \qquad (60)$$

**Definition A.2.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha, \beta \in \mathcal{F}(\mathscr{L})$. We will say that $\alpha, \beta$ are isomorphic iff there exists function*

$$f : bound(\alpha) \xrightarrow[onto]{1\text{-}1} bound(\beta)$$

*and $[f](\alpha) = \beta$ and $[f^{-1}](\beta) = \alpha$.*

**Lemma A.3.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha, \beta \in \mathcal{F}(\mathscr{L})$. If*

$$f : bound(\alpha) \xrightarrow[onto]{1\text{-}1} bound(\beta)$$

*such that $[f](a) = \beta$ and for any $u \in bound(\alpha)$ such that $f(u) \neq u$, we have $f(u) \notin free(\alpha)$, then $\alpha$ is isomorphic with $\beta$.*

*Proof.* To show that $[f^{-1}](\beta) = \alpha$ it is enough to show that for any $u \in bound(\beta)$ at place $p$ in $\beta$, there is $f^{-1}(u)$ at place $p$ in $\alpha$.

Take any $u \in bound(\beta)$ at place $p$ in $\beta$. Then the place $p$ is in a range of $Qu$. in $\beta$. Thus place $p$ is in a range of $Qf^{-1}(u)$. in $\alpha$.

If variable in place $p$ in $\alpha$ is free, then it must be $u$. If $u = f^{-1}(u)$, it will be in a range of $Qu$. and thus it can't be free. Then we must assume $f^{-1}(u) \neq u$. But $f^{-1}(u) \in bound(\alpha)$ and thus $u = f(f^{-1}(u)) \notin free(\alpha)$. Hence, variable in place $p$ in $\alpha$ must be bounded. But then it must be $f^{-1}(u)$. $\qquad \square$

**Theorem A.4.** *Let $\mathscr{L}$ be a signature of a language and let $\alpha, \beta \in \mathcal{F}(\mathscr{L})$. If $\alpha, \beta$ are isomorphic then for any $\mathscr{L}$-structure $\mathbf{M}$ with domain $A$ and any assignment of variables $j : \mathscr{V} \to A$ we have*

$$(\mathbf{M}, j) \models \alpha \text{ iff } (\mathbf{M}, j) \models \beta.$$

*Proof.* It is enough to show that, a variable $x$ is free in place $p$ in $\alpha$ iff a variable $x$ is free in place $p$ in $\beta$. In fact, since there is a symetry between $\alpha$ and $\beta$, it is enough to show that, if a variable $x$ is free in place $p$ in $\alpha$ then a variable $x$ is free in place $p$ in $\beta$.
Let $f$ be as in Definition A.2.
Assume that a variable $x$ is free in a place $p$ in $\alpha$.

1. If there is a bounded variable $u$ in place $p$ in $\beta$, then place $p$ is in a range of some quantifier $Qu.$ in $\beta$ and $f^{-1}(u) = x$. Then place $p$ is in a range of quantifier $Qx.$ in $\alpha$. Then $x$ can't be free in $\alpha$. Contradiction.

2. If there is a free variable $u$ in place $p$ in $\beta$, then $u = x$.

$\square$

**Definition A.5.** *We can construct a special shift operator.* $shift_\alpha : bound(\alpha) \xrightarrow[onto]{1\text{-}1} \mathscr{V}$, *such that*

$$shift_\alpha\big(bound(\alpha)\big) \cap free(\alpha) = \emptyset.$$

Indeed, if $\mathscr{V}$ is coutable and infinite, we can establish a linear order on $\mathscr{V}$. With such an order, the construction of $shift_\alpha$ is just a technical exercise whose details are irrelevant from the perspective of this paper.

**Definition A.6.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha \in \mathcal{F}(\mathscr{L})$, Let $x \in free(\alpha)$. we will define a special operator $\langle \cdot \rangle_x : \mathcal{F}(\mathscr{L})$. Let*

$U_x = \{u \in bound(\alpha) \cap free(\alpha) : \text{there exists quantifier with } x \text{ in its range which binds } u\}$

*Let*

$$f_{\alpha,x}(u) = \begin{cases} shift_\alpha(u) \text{ for } u \in U_x, \\ u \text{ otherwise} . \end{cases} \tag{61}$$

*Let*

$$\langle \alpha \rangle_x \stackrel{\text{def}}{=} [f_{\alpha,x}](\alpha). \tag{62}$$

**Theorem A.7.** *Let $\mathscr{L}$ be a signature of a language. Let $\alpha \in \mathcal{F}(\mathscr{L})$ and let $x \in free(\alpha)$. Then we have*

$$\alpha \text{ is isomorphic to } \langle \alpha \rangle_x, \tag{63}$$

*and for any term $\tau$ with $free(\tau) \subset free(\alpha)$, $\langle \alpha \rangle_x (x/\tau)$ is admissable.*

*Proof.* By Theorem A.3 and Definition 3.8. $\square$