Archive for Mathematical Logic manuscript No.
(will be inserted by the editor)

Matthias Baaz · Georg Moser

Herbrand's Theorem and Term Induction

Abstract. We study the formal first order system TIND in the standard language of Gentzen's LK. TIND extends LK by the purely logical rule of *term-induction*, that is a restricted induction principle, deriving numerals instead of arbitrary terms. This rule may be conceived as the logical image of *full induction.*

1. Introduction

Our object of study is the first order formal system TIND defined over the standard language of Gentzen's LK [16,28]. TIND extends LK by the following logical inference rule (A is quantifier-free, c eigenvariable).

$$\frac{A(c), \mathit{\Gamma} \to \mathit{\Delta}, A(S(c))}{A(0), \mathit{\Gamma} \to \mathit{\Delta}, A(S^n(0))} \ (tind)$$

The rule is called *Term Induction.* It formalises a *restricted* induction principle. Given the base and the step case for some quantifier-free property A, we are allowed to infer that A holds for all terms of the form $0, S(0), S(S(0)), \ldots$; i.e. all *numerals.*[1]

This restricted induction principle is in stark contrast to the number-theoretic (or mathematical) induction principle. The term-induction principle is part of pure logic. Consider mathematical induction (originally called *Kästner's principle*), axiomatised as a rule.

$$\frac{A(c), \mathit{\Gamma} \to \mathit{\Delta}, A(S(c))}{A(0), \mathit{\Gamma} \to \mathit{\Delta}, A(t)} \ (ind)$$

Matthias Baaz: Institut für Diskrete Mathematik und Geometrie, E104, Wiedner Hauptstrasse 8–10, Vienna University of Technology, Austria, email: baaz@logic.at

Georg Moser: Computational Logic, Technikerstrasse 21a, University of Innsbruck, Austria, email: georg.moser@uibk.ac.at

Key words or phrases: Term induction, Successor Induction, Herbrand's theorem, Generalisation of Proofs

Mathematics Subject Classification (2000): 03F07,03F20,03B10,03B35

[1] We write $\mathbf{n}$ instead of $S^n(0)$; this notation is used with respect to tuples of terms, too.

Suppose the base and step case for the property A are provable. Then we infer that A holds for an *arbitrary* term t, not only for a *numeral.*

We conceive mathematical induction as a rule that combines two principles that we aim to separate. Firstly a specific generation of terms is stipulated. Secondly a sort of *closed world* assumption is imposed asserting that all terms in the basic language can be generated in this way. Our study of term-induction accounts for an analysis of the first aspect. We think that term-induction precisely captures the *logical image* of 'full' induction.

Observe that the viewpoint of induction as a logical inference rule is implicit in the literature. Recall Gentzen's second consistency proof [17, 28] of number theory. In the cut-elimination argument one has to deal with induction inference-rules. These are analysed by firstly *evaluating* the arbitrary terms possible occurring in the induction formulas, thus reducing those terms to *numerals* and secondly by eliminating the obtained (term-)induction rule. (Compare [28], pp. 97–114.) Further, note that (variants of) term induction were already employed in mathematical proofs long before the concept of *mathematical induction* was introduced, cf. [18].

Consider Herbrand's Theorem; let $A := \exists\overline{x}P(x_1, \dots, x_n)$ be an existential formula with $P(x_1, \dots, x_n)$ quantifier free, provable in length[2] k within a usual Hilbert or Gentzen type system of pure logic. Herbrand's Theorem expresses the existence of a valid disjunction

$$C_1 \vee \cdots \vee C_m \ , \tag{1}$$

such that the C_i are instances of $P(x_1, \dots, x_n)$; this disjunction is called *Herbrand disjunction.*

It is a well-known fact that m, the number of disjuncts, is bounded by a primitive recursive function which depends only on k and the logical complexity of A. This is an immediate consequence of Gentzen's Hauptsatz.[3] Using unification-theoretic methods one can even bound the term-complexity of the Herbrand disjunction. As the obtained bound does not depend on the term-structure of the proof Π or the end-formula A, this bound is called *uniform.* In particular a uniform bound is independent on *term-parameters* occurring in A.

In TIND, there is no uniform bound on the number of disjuncts in Herbrand disjunctions. We show this in Section 2.3; the reason for it is quite obvious. Through the rule (tind) we allow the introduction of arbitrary large numerals in a single proof step. Hence the (subtle) interdependence between term-complexity and proof-complexity needed to gain the uniform bound is lost. However, bounds on the length and the term-complexity of Herbrand disjunctions can partly be secured. Suppose A denotes the existential statement $\exists\overline{x}P(x_1, \dots, x_n)$. A Herbrand disjunction H of A is called

[2] In the following we conceive proofs as rooted trees whose vertices are sequents. The *length* of a proof Π is the number of vertices in this tree.

[3] In fact it is possible to bound m by a function that depends only on k. This follows from the first ϵ-elimination theorem, cf. [20] pages 27–33, compare [2].

in matrix-form with respect to the matrix $C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p)$, if it is represented in the following way for some N.

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p) \ , \tag{2}$$

where each $C_i(\mathbf{i}_1, \ldots, \mathbf{i}_p)$ is an instance of $P(x_1, \ldots, x_n)$ such that all numerals in this instance are fully indicated. Note that the number of quantifiers n and the number of 'big' disjunctions p may be different. A *generalised Herbrand's Theorem* for TIND is established. We prove that if an (existential) formula A is provable in TIND, then there exists a Herbrand disjunction H in matrix-form as above, such that the following holds.

- The length of the *matrix*

  $$C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p) \ ,$$

  is *uniformly* bounded by a primitive recursive function depending on the length of the proof of A and the logical complexity of A.
- The number of '*big´* disjunctions

  $$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} \ ,$$

  is *uniformly* bounded by a primitive recursive function depending on the maximal *iteration* of (tind)-rules in the proof of A and the logical complexity of A.
- Let the *reduct* of H be obtained by ignoring all occurring numerals. We show that the term-complexity of the reduct of H is uniformly bounded primitive recursively in the length of the proof and the size of the reduct of A.

Assume that the proof Π of A is almost cut-free, i.e. it contains only propositional cuts.

- Then (i) the length of the matrix is bounded by $k+1$, if k denotes the length of the proof of Π. Further, (ii) the number of 'big' disjunctions is bounded by the number of iterations of (tind)-rules in Π. This bound is optimal. Finally (iii) the term-complexity of H is bounded elementarily in the length of the proof and the size of the reduct of A.

Due to those results we conceive Herbrand disjunctions in matrix-form as natural characterisation of theorems of TIND. On one hand the usual results (see e.g. [21, 2]) on uniform bounds known for Herbrand disjunctions hold with respect to the *inner* disjunction. While on the other, the *outer* part of the Herbrand disjunction given through the 'big' disjunctions is linked to the structure of (tind)-rules in the initial proof. I.e. the effect of introducing the restricted form of induction can be captured in a specific form of Herbrand disjunctions.

We consequently study a *reversion* of Herbrand's Theorem: Given a valid disjunction of the above form, does there exists a proof in TIND of the existential statement A? This becomes a non-trivial task only, if we consider sequences of Herbrand disjunctions (of $A(\mathbf{n})$) and seek *uniform* proofs (of $A(\mathbf{n})$).[4] The existence of *some* proof in TIND follows already by the completeness of first-order logic.

As basis for our investigation on a reversion of Herbrand's theorem, we study the decidability of the validity problem for disjunctions in matrix-forms: Given a disjunction D of the special form (2) above, then the *validity problem* for D is the query whether there exists an N such that D becomes valid.

- We show that the presence of two 'big' disjunction in D is already sufficient to reduce the general halting problem to the uniform validity problem. Using a Parikh-style argument we conclude that a reversion of Herbrand's theorem is not possible in this case.
- On the other hand if we restrict our attention to disjunctions D with only one 'big' disjunction, then the validity problem remains decidable.

The latter result can be sharpened. We consider disjunctions $D(\mathbf{n})$ with a single parameter $\mathbf{n}$ of the form:

$$\bigvee_{i=0}^{N(n)} C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n}) \ , \tag{3}$$

where the length m of the inner disjunction is independent on n; such disjunctions are called *uniform*. The *uniform validity problem* for $D(\mathbf{n})$ is the query whether there exists for all $\mathbf{n}$ a number $N(n)$ such that $D(\mathbf{n})$ is valid.

- We introduce the following restrictions on the form of D. Let the matrix M of D be denoted as

  $$C_1(\mathbf{a},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{a},\mathbf{n}) \ ,$$

  for some free variable $\mathbf{a}$. Assume that for any occurrence of an atomic formula A in M the variable $\mathbf{a}$ and the parameter $\mathbf{n}$ do not both occur in A; such disjunctions are called *simple*. The uniform validity problem for simple disjunctions is decidable.

For the class of simple uniform Herbrand disjunctions of form (3), we obtain a reversion of Herbrand's theorem in the above sense. Let $A(\mathbf{n})$ denote the formula

$$\exists x (C_1(x,\mathbf{n}) \vee \cdots \vee C_m(x,\mathbf{n})) \ .$$

[4] We call a formula $A(\mathbf{n})$ *uniformly derivable* if there exists an infinite sequence of proofs $\Pi(\mathbf{n})$ of $A(\mathbf{n})$, such that $|\Pi(\mathbf{n})|$, the length of proof $\Pi(\mathbf{n})$, is independent on the parameter $\mathbf{n}$.

- If for any n, $H(\mathbf{n})$ denotes a simple uniform Herbrand disjunction of $A(\mathbf{n})$, then $A(\mathbf{n})$ is uniformly derivable in TIND by $\Pi(\mathbf{n})$. The $\Pi(\mathbf{n})$ do not need iterated occurrences of (tind) rules: All occurring term-induction inference occur in parallel. Further, the proofs $\Pi(\mathbf{n})$ are almost cut-free.

In this sense we capture the uniformity of the Herbrand disjunctions $H(\mathbf{n})$ of $A(\mathbf{n})$ by showing the existence of uniform proofs $\Pi(\mathbf{n})$ of $A(\mathbf{n})$. This renders further basis for our claim that (tind) expresses precisely the logical content of induction.

In Section 2 we give basic definitions and notions and define the investigated system TIND formally. We initially only consider almost cut-free proofs; the general case is handled in Appendix A.

In Section 3.1 we show the uniform bound on the length of the inner disjunction of Herbrand disjunction in matrix-form of form (2). Section 3.2 provides the results on the bounded term-complexity of Herbrand disjunctions. These investigations dwell on the use of unification techniques whose basics are introduced in Section 3.2; additional material on unification is giving in Appendix C.

Section 4 deals with the reversion of Herbrand's theorem studied. In Section 4.1 the validity problem is investigated. The proof of the reversion of Herbrand's theorem studied, is given in the Sections 4.2, 4.3 and Section 4.4. Some technical considerations have been collected in Appendix D. In Appendix B we give applications of our results to questions related to the structure and complexity of proofs.

2. Term Induction

2.1. Notions and Definitions

A first-order language is determined by specifying its *constants*, *variables*, *logical symbols*, and other auxiliary symbols like brackets or comma. In particular *constants* are either individual constants, function symbols of specific arities, or predicate symbols of specific arities. We use the metasymbols $f, g, h, \ldots$ to denote function symbols, while the metasymbols $P, Q, R, \ldots$ vary through predicate symbols. *Variables* are either *free* variables or *bound* variables. Free variables are denoted by lower-case letters from the beginning of the alphabet, while bound variables are denoted by lower-case letter from the end of the alphabet. The set of free variables is denoted as $\mathbf{FV}$ while the set of bound variables is denoted as $\mathbf{BV}$. We set $\mathbf{V} := \mathbf{FV} \cup \mathbf{BV}$. As logical symbols $\land, \lor, \neg, \supset, \forall, \exists$ are used. As usual the binary logical operators $\land, \lor, \supset$ are written in infix notation.

We fix a first-order language $\mathcal{L}$ which will henceforth be referred to as the *basic language*. We assume that the constants of $\mathcal{L}$ include at least a nullary constant 0 and an unary function symbol S. Apart from this assumption we do not pose any restrictions which of the above mentioned symbols $\mathcal{L}$

actually contains. In every argument below we assume that $\mathcal{L}$ is fixed, and hence omit the phase "of $\mathcal{L}$".

Terms are constructed as usually from constants, free variables, and function symbols; while *semi-terms* are like terms but may as well contain bound variables. We will use the metasymbols $r, s, t, u, v, w, \dots$ to denote terms and semi-terms. *Formulas* are defined as usual with the proviso that only bound variables are allowed to be quantified and only free variables may occur free. *Semi-formulas* are similar to formulas with the exception that both free and bound variables may occur free in a semi-formula. Henceforth $A, B, C, \dots$ will be meta-variables ranging over formulas. To denote quantifier free formulas we usually use the metasymbols $P, Q, R, \dots$

An occurrence of a formula A in a formula B is called *positive* if it occurs in the scope of an even number of negations, otherwise the occurrence is called *negative*. An occurrence of $\exists$ in a formula is called *weak* (*strong*) if it is the leading symbol of a positive (negative) subformula. Dually for $\forall$.

A sequence of symbols from $\mathcal{L}$ is called *expression*. Expressions which are formed according to the recursive definitions of terms or formulas are called *well-formed*. We use the metasymbol e to denote well-formed expressions. If not noted otherwise we assume that an expression is well-formed, and hence omit the phrase "well-formed". We sometimes abbreviate sequences of expressions like $t_1, \dots, t_n$ by $\bar{t}$. Instead of $A(t_1, \dots, t_n)$ we may write $A(\bar{t})$. The set of variables occurring in an expression e is denoted as $\mathbf{V}(e)$.

Definition 1. *A tree is a structure $(T, \leq_T)$ such that*

1. *T is a finite set.*
2. *$\leq_T$ is partial order on T.*
3. *There is a unique maximal element $\widetilde{T}$ of T; i.e. for all $u \in T$ $u \leq_T \widetilde{T}$ holds. $\widetilde{T}$ is called the root of the tree $(T, \leq_T)$.*
4. *For any $u \in T$, the set $\{v \in T \mid u \leq_T v\}$ is linearly ordered.*

Since there is no chance of confusion we use the symbol T to denote the whole structure $(T, \leq_T)$. The elements of T are called nodes. Due to Definition 1.4 any node v uniquely defines a linearly ordered set $N = \{w \in T \mid v \leq_T w\}$. Assume $u \in N$, then u specifies a subset P of N. A *path* from u to v is defined as the sequence of (linearly ordered) elements of P. We often confuse the set notation $\{v_1, \dots, v_n\}$ of a path and its notation as a sequence $(v_1, \dots, v_n)$. The *length* of P—denoted as $|P|$—is given by the number of nodes in it.

Definition 2. *If $(T_1, \leq_{T_1}), \dots, (T_n, \leq_{T_n})$ are mutually disjoint trees, then the structure*

$$(T_1, \dots, T_n) = (\bigcup T_i, \bigcup \leq_{T_i}) \ ,$$

is called forest. Note that if $u \in (T_1, \dots, T_n)$, then there exists a unique $i \in \{1, \dots, n\}$ such that $u \in T_i$.

A labelled tree T (or forest T) is a tree (forest) together with a label function $L\colon T \to X$, where X is some set of labels. Usually X will be a set of expressions. Any expression e can be conceived as a labelled tree $T(e)$ such that the root of $T(e)$ corresponds to expression e itself and sons of the node u corresponds to immediate subexpressions of $L(u)$. Thus any subexpression e_0 of e uniquely defines an inner node u in the labelled tree $T(e)$ such that $L(u) = e_0$. The *position* p of e_0 in e is defined as the path P from the root of $T(e)$ to u. Given a position p in e, we denote the subexpression at p as $e/_p$; hence $e_0 = e/_p$.

Definition 3. *Let e_0 be a subexpression of an expression e, such that p is the position of e_0 in e. Then the depth (of occurrence) of e_0 in e is $|p| - 1$, the length of the position p minus* 1*. The depth of e_0 in e is denoted as* $\mathrm{dp}(e_0, e)$*.*

Definition 4. *The depth of an expression e is defined as*

$$\max\{|p| \mid p \textit{ is a position in } e\} \ .$$

The depth of e is denoted as $\mathrm{dp}(e)$*. Let E be a set of expressions. Then* $\mathrm{dp}(E) := \max\{\mathrm{dp}(e) | e \in E\}$*.*

Definition 5. *The size of an expression is the number of symbols in e, denoted as* $\textsc{size}(e)$*.*

Definition 6. *The complexity or logical depth of a formula (or a semiformula) A is defined as*

$$\max\{|p| \mid p \textit{ is a position of an atomic formula in } e\} \ .$$

The complexity of A is denoted as $\mathrm{ld}(A)$*.*

Let the set of terms in $\mathcal{L}$ be denoted as $\mathcal{T}$.

Definition 7. *A substitution $\sigma\colon \mathbf{V} \to \mathcal{T}$ is a mapping from the set of free variables to the set of terms. To denote a substitution σ we write*

$$\sigma = \{a_1 \mapsto t_1, \ldots, a_n \mapsto t_n\} \ .$$

Then $\sigma(a_i) = t_i$ for $i = 1, \ldots, n$ and for all $a \in \mathbf{V}$ distinct from $a_1, \ldots, a_n$, we stipulate $\sigma(a) = a$. The substitution that maps any variable to itself is called empty. It is denoted as ϵ.

The application of a substitution σ to an expression e is usually written as $e\sigma$ instead of $\sigma(e)$. We call the set $\{a \mid \sigma(a) \neq a\}$ the *domain*—$\mathrm{dom}(\sigma)$—of σ and the set $\{\sigma(a) \mid a \in \mathrm{dom}(\sigma)\}$ the *range*, denoted as $\mathrm{rg}(\sigma)$. The concatenation of two substitution σ and λ (such that σ is applied before λ) is written as $\sigma \circ \lambda$. An expression e_0 is an *instance* of e if $e\sigma = e_0$ for some substitution σ; alternatively we write $e \leq e_0$.

Definition 8. *1. Let A be a formula and $t_1, \dots, t_n$ terms. If there exists a formula B and n distinct variables $a_1, \dots, a_n$ such that A is equal to*

$$B\{a_1 \mapsto t_1, \dots, a_n \mapsto t_n\} ,$$

then for each i ($1 \leq i \leq n$), the occurrences of t_i in A are said to be indicated in A. This fact is also expressed (less accurately) in writing B as $B(a_1, \dots, a_n)$ and A as $B(t_1, \dots, t_n)$.

2. We say that a term t is fully indicated in A if every occurrence of t in A can be obtained by such an replacement (from some formula B, $n = 1$ and $t = t_1$).

We assume familiarity with the theory of standard unification, compare e.g. [1]. However, we will review some crucial notions. A *unification problem* U is either $\top$ or $\bot$ or a conjunction of equations $(s_1 = t_1 \wedge \dots \wedge s_k = t_k)$.[5] A unification problem U is called *solved* if all s_i are pairwise distinct variables and $s_i \notin \mathbf{V}(t_j)$; for all i, j. If $U = (a_1 = t_1 \wedge \dots \wedge a_k = t_k)$ is in solved form, then $\sigma_1 \circ \dots \circ \sigma_k$ is the unifier *induced* by U; where $\sigma_i := \{a_i \mapsto t_i\}$ and $\circ$ denotes the concatenation of substitutions.

Let σ, ρ be substitutions. If there exists a substitution ρ with $\tau \circ \rho = \sigma$ we say that τ is *more general* than σ. On the other hand σ is called an *instance* of τ. A substitution $\rho = \{a_1 \mapsto b_1, \dots, a_n \mapsto b_n\}$, where the variables in $\overline{a}$ are distinct, similarly for $\overline{b}$, is called *renaming.* Note that it must not be the case that variable positions in e that are named differently, are named equal in $e\rho$.

2.2. *The system* TIND

The calculus underlying our investigation is Gentzen's LK, compare [16,28]; for our version of LK, see below. In order to formulate the sequent calculus, we must first introduce an auxiliary symbol $\rightarrow$. For arbitrary formulas $A_1, \dots, A_n$ and $B_1, \dots, B_m$ the expression

$$A_1, \dots, A_n \rightarrow B_1, \dots, B_m ,$$

is called a *sequent.* Intuitively this means (for $n, m \geq 1$) the formula $A_1 \wedge \dots \wedge A_n \supset B_1 \vee \dots \vee B_m$. For $n \geq 1$, $A_1, \dots, A_n \rightarrow$ means that $A_1 \wedge \dots \wedge A_n$ yields a contradiction. For $m \geq 1, \rightarrow B_1, \dots, B_m$ means that $B_1 \vee \dots \vee B_m$ is valid. The empty sequent $\rightarrow$ is interpreted as contradiction. For a given sequent $S = (\Gamma \rightarrow \Delta)$, the standard interpretation is denoted as $\widehat{S}$ or more expressively as $(\bigwedge \Gamma \supset \bigvee \Delta)$. A sequent S is valid, iff $\widehat{S}$ is valid.

The formulas occurring in a sequent are called *sequent formulas*, where the formulas left to $\rightarrow$ are the *antecedent* and the formulas right to $\rightarrow$ are the *succedent.* In the following we abstract from the ordering in the sequent formulas $A_1, \dots, A_n$ and $B_1, \dots, B_m$. I.e. we consider these lists as

[5] We often confuse the logical notation of a unification problem $(s_1 = t_1 \wedge \dots \wedge s_k = t_k)$ and its multiset notation $\{s_1 = t_1, \dots, s_k = t_k\}$.

(finite) multisets rather than as sequences. Greek capital letter $\varGamma, \varDelta, \varLambda, \ldots$ will be metasymbols that range over finite multisets of sequent formulas. The *length* of a sequent $S = (A_1, \ldots, A_n \rightarrow B_1, \ldots, B_m)$ (written $|S|$) equals $n + m$. The *size* of S is the number of symbols in S. The *depth* of S (written $\mathrm{dp}(S)$) equals $\max\{\mathrm{dp}(C) \mid C$ is a sequent formula in $S\}$. The *(logical) complexity* of S (written as $\mathrm{ld}(S)$) is defined as $\max\{\mathrm{ld}(C) \mid C$ is a sequent formula in $S\}$.

The axioms of LK are sequents of the form $A \rightarrow A$. Note that A may be an arbitrary complex formula. The structural and logical rules of LK are given in Table 1, Table 2, respectively. The auxiliary and principal formulas of the inferences mentioned are defined as usual, compare [28]. Note that in $\forall$: right and in $\exists$: left the *eigenvariable* condition has to hold for a. In $\forall$: right and in $\exists$: left all occurrences of the free variable a are indicated, while in $\forall$: left and in $\exists$: right not necessarily every t is indicated. We write LK $\vdash S$ to denote that S is the endsequent of a proof in LK.

Table 1. Structural Rules

Weakening:	$\dfrac{\varGamma \rightarrow \varDelta}{A, \varGamma \rightarrow \varDelta}$	$\dfrac{\varGamma \rightarrow \varDelta}{\varGamma \rightarrow \varDelta, A}$
Contraction:	$\dfrac{A, A, \varGamma \rightarrow \varDelta}{A, \varGamma \rightarrow \varDelta}$	$\dfrac{\varGamma \rightarrow \varDelta, A, A}{\varGamma \rightarrow \varDelta, A}$
Cut:	$\dfrac{\varGamma_1 \rightarrow \varDelta_1, A \quad A, \varGamma_2 \rightarrow \varDelta_2}{\varGamma_1, \varGamma_2 \rightarrow \varDelta_1, \varDelta_2}$	

Table 2. Logical Rules

$\neg$: left:	$\dfrac{\varGamma \rightarrow \varDelta, A}{\neg A, \varGamma \rightarrow \varDelta}$	$\neg$: right:	$\dfrac{A, \varGamma \rightarrow \varDelta}{\varGamma \rightarrow \varDelta, \neg A}$
$\wedge$: left:	$\dfrac{A, B, \varGamma \rightarrow \varDelta}{A \wedge B, \varGamma \rightarrow \varDelta}$	$\wedge$: right:	$\dfrac{\varGamma \rightarrow \varDelta, A \quad \varLambda \rightarrow \varTheta, B}{\varGamma, \varLambda \rightarrow \varDelta, \varTheta, A \wedge B}$
$\vee$: left:	$\dfrac{A, \varGamma \rightarrow \varDelta \quad B, \varLambda \rightarrow \varTheta}{A \vee B, \varGamma, \varLambda \rightarrow \varDelta, \varTheta}$	$\vee$: right:	$\dfrac{\varGamma \rightarrow \varDelta, A, B}{\varGamma \rightarrow \varDelta, A \vee B}$
$\supset$: left:	$\dfrac{\varGamma \rightarrow \varDelta, A \quad B, \varLambda \rightarrow \varTheta}{A \supset B, \varGamma, \varLambda \rightarrow \varDelta, \varTheta}$	$\supset$: right:	$\dfrac{A, \varGamma \rightarrow \varDelta, B}{\varGamma \rightarrow \varDelta, A \supset B}$
$\forall$: left:	$\dfrac{A(t), \varGamma \rightarrow \varDelta}{\forall x A(x), \varGamma \rightarrow \varDelta}$	$\forall$: right:	$\dfrac{\varGamma \rightarrow \varDelta, A(a)}{\varGamma \rightarrow \varDelta, \forall x A(x)}$
$\exists$: left	$\dfrac{A(a), \varGamma \rightarrow \varDelta}{\exists x A(x), \varGamma \rightarrow \varDelta}$	$\exists$: right:	$\dfrac{\varGamma \rightarrow \varDelta, A(t)}{\varGamma \rightarrow \varDelta, \exists x A(x)}$

Definition 9. *Terms of the form* $0, S(0), S(S(0)), \dots$ *are called numerals. The* n*-times iterated application of the function symbol* S *to* 0 *is denoted as* $S^n(0)$*. We usually write* $\mathbf{n}$ *for the numeral* $S^n(0)$*,* $n \geq 0$*. In addition we write* $\overline{\mathbf{n}} = (\mathbf{n}_1, \dots, \mathbf{n}_r)$ *to denote the tuple* $(S^{n_1}(0), \dots, S^{n_r}(0))$*.*

Remark 1. Usually the unary function symbol S is interpreted as the successor function. We want to emphasise that our results do not depend on this interpretation. Our apology for still using the symbol S is that some of the question considered in this work where originally posed in terms of Peano arithmetic.

Definition 10. *Term Induction (tind) is the following inference rule.*

$$\frac{P(c), \Gamma \rightarrow \Delta, P(S(c))}{P(\mathbf{0}), \Gamma \rightarrow \Delta, P(\mathbf{n})}$$

where P *is quantifier-free. The* eigenvariable *a must not occur in the lower sequent of the inference.* $P(\mathbf{0})$ *and* $P(\mathbf{n})$ *are called the principal formulas and* $P(c), P(S(c))$ *are called the auxiliary formulas of (tind).*

Extending LK by term induction, we obtain the formal system TIND that will be studied in this paper. We write TIND $\vdash^k S$ to denote that S is the endsequent of a proof in TIND (with length k). If no confusion is possible, we drop the reference to TIND.

Note that TIND and LK derive the same sequents. It is sufficient to observe that any (tind)-inference

$$\frac{P(c), \Gamma \rightarrow \Delta, P(S(c))}{P(\mathbf{0}), \Gamma \rightarrow \Delta, P(\mathbf{n})}$$

can be replaced by $n-1$ iterated applications of the cut-rule on the sequents

$$P(\mathbf{0}), \Gamma \rightarrow \Delta, P(\mathbf{1}) \quad \cdots \quad P(\mathbf{n-1}), \Gamma \rightarrow \Delta, P(\mathbf{n}) \ ,$$

which are obtained as instances of the upper sequent $P(c), \Gamma \rightarrow \Delta, P(S(c))$.

We conceive proofs Π in TIND as labelled trees $T(\Pi)$ such that the root of $T(\Pi)$ corresponds to the endsequent of Π and sons of the node u corresponds to upper sequents of $L(u)$. Let S_1 and S_2 be sequents in Π. We say S_1 is *above* S_2 or S_2 is *below* S_1 if there exists a path in $T(\Pi)$ containing sequents S_1 and S_2, such that $S_1 \leq_{T(\Pi)} S_2$. A proof in TIND is called *regular* if firstly all eigenvariables are distinct from one another, and secondly if a free variable a occurs as an eigenvariable in a sequent S of the proof, then a occurs only in sequents above S. In the following all considered proofs are supposed to be regular.

Definition 11. *The length of a proof* Π *is the number of sequents that occur in the proof. The length of* Π *is denoted as* $|\Pi|$*.*

A sequent $S(\mathbf{n})$ is *uniformly derivable*, if there exists an infinite sequence of proofs $\Pi(\mathbf{n})$ of $S(\mathbf{n})$, such that $|\Pi(\mathbf{n})|$ is independent on the parameter $\mathbf{n}$. We say that $S(n)$ is *uniformly derivable in k steps* if $|\Pi(n)| \leq k$ for some constant k independent on n. Let $\widehat{S}(\mathbf{n})$ denote the standard interpretation of $S(\mathbf{n})$, then $\widehat{S}(\mathbf{n})$ is called uniformly derivable (in k steps) if $S(\mathbf{n})$ is uniformly derivable (in k steps).

2.3. What makes TIND *different from* LK*?*

Before we can assess the proof-theoretic difference between TIND and LK we need some further definitions, compare [28].

Definition 12. *A sequent $S = (\Gamma \rightarrow \Delta)$ satisfies the property* (P)*, if*

1. *All sequent formulas in Γ are either of form $\forall y_1, \dots, \forall y_n P(y_1, \dots, y_n)$ ($P(y_1, \dots, y_n)$ quantifier-free) or are quantifier-free.*
2. *All sequent formulas in Δ are either of form $\exists x_1, \dots, \exists x_n P(x_1, \dots, x_n)$ ($P(x_1, \dots, x_n)$ quantifier-free) or are quantifier-free.*

Convention. If not mentioned otherwise, we will assume that considered endsequent satisfies the property (P).

We cannot drop this restrictions without crucially affecting some of our theorems below, cf. Section 3.1. However this restriction is not too severe as shown by the following proposition. We write $A \leftrightarrow B$ to abbreviate the conjunction $A \supset B \wedge B \supset A$.

Proposition 1. *Let S be an arbitrary endsequent. Then there exists a sequent S' satisfying property* (P) *provable in* TIND *such that $S' \leftrightarrow S$ holds (provable in* TIND*). Furthermore, $\Pi \vdash S$ implies the existence of a proof Π' such that $\Pi' \vdash S'$ and $|\Pi'| \leq O(|\Pi|)$ holds.*

To prove the proposition one firstly uses *structural Skolemisation* (see [4]) to eliminate strong quantifiers from S. The idea is simple: Any quantifier-introduction rule, introducing a strong quantifier, is removed. Simultaneously the respective *eigenvariables* are replaced by suitable chosen Skolem functions. See [4] for a formal definition. This transforms Π to a proof with an endsequent S_1 free of strong quantifier occurrences. Furthermore, the proof-transformation does not increase the proof-length. Secondly one transforms the sequent S_1 into a sequent satisfying property (P). To this end, it suffices to move all occurring (weak) quantifiers to the front of the sequent formulas. This is established by adding suitable cuts representing quantifier-shiftings, cf. [6]. The length-bound follows from the proof in [6].

Definition 13. *Let S be a sequent satisfying property* (P)*.*

$$A_1, \dots, A_n \rightarrow B_1, \dots, B_m \ ,$$

so that the A_i ($i = 1, \dots, n$) can be written as $\forall \overline{y} P_i(\overline{y})$ and the B_i ($i = 1, \dots, m$) can be written as $\exists \overline{x} Q_i(\overline{x})$. We assume the variables $\overline{y}$ are not *shared among the A_i and the $\overline{x}$ are not shared among the B_i. If there exists a valid sequent T*

$$C_1, \ldots, C_k \rightarrow D_1, \ldots D_l \ ,$$

so that each C_i is an instance of some $P_j(\overline{y})$ ($1 \leq j \leq n$) and each D_i is an instance of some $Q_j(\overline{x})$ ($1 \leq j \leq m$), then T is called Herbrand sequent (of S).

Any Herbrand sequent T (of S) uniquely defines a *Herbrand disjunction* (of S) via the standard interpretation of sequents. It is a well-known fact that any LK-provable sequent satisfying property (P) admits a Herbrand sequent, cf. [19]. Furthermore, the length of a Herbrand sequent of S can be bounded in the length of the LK-proof of S and the complexity of S. One uses the fact that LK admits cut-elimination and that the length of the cut-free proof is bounded in the length and the maximal complexity of the cut formulas in the initial proof. Furthermore, one employs Parikh's Theorem cf. [24,15] to bound the complexity of the cut formulas in the proof-length and the complexity of S. We will state and prove a suitable version of Parikh's Theorem in Appendix A.

Hence if S is provable by a proof in LK, then the bound on the length of a Herbrand sequent of S is independent on the term-complexity in S. We call such a bound *uniform*. The situation can be shortly described by saying that LK admits uniform bounds on the length of Herbrand disjunctions. This is no longer true if we consider the system TIND.

Theorem 1. *In general no function can exist that bounds the length of the Herbrand sequents of some sequent S in the length of the proof of S and its logical complexity.*

Proof. For any $\mathbf{n}$, any Herbrand sequent of

$$\forall x(P(x) \supset P(S(x))), P(\mathbf{0}) \rightarrow P(\mathbf{n}) \ ,$$

has to contain in the antecedent all $n-1$ implications $P(\mathbf{i}) \supset P(S(\mathbf{i}))$. This is easily seen by applying the pigeon-hole principle. On the other hand consider the trivial proof Π (P is atomic) given in Table 3. □

Table 3. No uniform bound.

$$\dfrac{\dfrac{\dfrac{P(c) \rightarrow P(c) \quad P(S(c)) \rightarrow P(S(c))}{P(c) \supset P(S(c)), P(c) \rightarrow P(S(c))}}{\forall x(P(x) \supset P(S(x))), P(c) \rightarrow P(S(c))}}{\forall x(P(x) \supset P(S(x))), P(\mathbf{0}) \rightarrow P(\mathbf{n})}\ (tind)$$

Corollary 1. *Let A be a formula of the form $\exists\overline{x}P(x_1,\dots,x_n)$, $P(x_1,\dots,x_n)$ is quantifier free. Let $C_1 \vee \dots \vee C_m$ be a valid disjunction such that each C_i $(i = 1,\dots,n)$ is a instance of $P(x_1,\dots,x_n)$. Then no function can exist that bounds m in the length of the proof of A and its logical complexity.*

3. A generalised Herbrand's Theorem for TIND

From the observations above we know that TIND does not admit uniform bounds on the length of Herbrand disjunctions. The example given suggests that this is connected to the fact that a (tind)-inference allows to introduce arbitrary large numerals in one step. Thus in this section, we define and study a special form of Herbrand disjunctions that allows us to reveal the impact of term-induction.

We introduce a separate set of *variables* $\mathbf{NV}$ to $\mathcal{L}$. We use $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}$ as meta-variables that range over the elements of $\mathbf{NV}$. If not noted otherwise expressions are free of variables from $\mathbf{NV}$. Let e denote an expression, then $\mathbf{NV}(e)$ denotes the set of variables belonging to $\mathbf{NV}$ that occur in e.

Definition 14. *Let $S = (\Gamma \to \Delta)$ be a sequent; assume the formulas in Γ can be written as $\forall\overline{y}\ P_i(\overline{y})$, where $P_i(\overline{y})$ is quantifier-free, and the formulas in Δ can be written as $\exists\overline{x}\ Q_i(\overline{x})$, $Q_i(\overline{x})$ quantifier-free. We assume the variables $\overline{y}$ ($\overline{x}$) are not shared among the A_i (B_i).*

Let M denote a sequent

$$C_1,\dots,C_k \to D_1,\dots,D_l$$

such that each C_i is an instance of some $P_j(\overline{y})$ and each D_i is an instance of some $Q_j(\overline{x})$. Both the C_i's and the D_i's may contain variables from $\mathbf{NV}$.

Assume further there exists a number N s.t. the sequent $T = (\Gamma^\star \to \Delta^\star)$ is valid, where

$$\Gamma^\star := \{C_i\sigma \mid 1 \le i \le k \text{ and } \sigma\colon \mathbf{NV}(C_i) \to \{\mathbf{0},\dots,\mathbf{N}\}\}\ ,$$

and

$$\Delta^\star := \{D_i\sigma \mid 1 \le i \le l \text{ and } \sigma\colon \mathbf{NV}(D_i) \to \{\mathbf{0},\dots,\mathbf{N}\}\}\ .$$

Then T is called a Herbrand sequent in matrix-form (with respect to M). The sequent M is called (Herbrand) matrix *of T.*

Definition 15. *Let S be a sequent; assume there exists a Herbrand sequent T in matrix-form of S. Assume further T is chosen such that the length of the induced Herbrand matrix is minimal (among all possible choices of T). Let M denote the Herbrand matrix of T. Then the matrix complexity (written as $\mathrm{HC}(S)$) of S is defined as the length of M.*

Example 1. Let $S(\mathbf{n})$ denote the sequent

$$P(\mathbf{0},\mathbf{0}), \forall xy(P(x,y) \supset P(S(x),y), \forall xy(P(x,y) \supset P(x,f(y))) \to \\ \to P(\mathbf{n}, f^m(0))\ .$$

The sequent

$$P(\mathbf{0},\mathbf{0}), P(\mathbf{0},\mathbf{0}) \supset P(S(\mathbf{0}),\mathbf{0}), \dots, P(\mathbf{n}-\mathbf{1},\mathbf{0}) \supset P(\mathbf{n},\mathbf{0}),$$
$$P(\mathbf{n},\mathbf{0}) \supset P(\mathbf{n}, f(\mathbf{0})), \dots, P(\mathbf{n}, f^{m-1}(\mathbf{0})) \supset P(\mathbf{n}, f^m(\mathbf{0})) \to P(\mathbf{n}, f^m(\mathbf{0}))\ ,$$

denotes a Herbrand sequent T of S with (Herbrand) matrix M ($\mathbf{c} \in \mathbf{NV}$):

$$P(\mathbf{0},\mathbf{0}), P(\mathbf{c},\mathbf{0}) \supset P(S(\mathbf{c}),\mathbf{0}), P(\mathbf{n},\mathbf{0}) \supset P(\mathbf{n}, f(\mathbf{0})), \dots$$
$$P(\mathbf{n}, f^{m-1}(\mathbf{0})) \supset P(\mathbf{n}, f^m(\mathbf{0})) \to P(\mathbf{n}, f^m(\mathbf{0}))\ .$$

□

We study the possible shapes of Herbrand sequents in matrix-form and obtain uniform bounds on the matrix complexities. This allows us to characterise the Herbrand disjunctions of Σ_1-formulas provable in TIND. Note that the matrix complexity can only be studied if we assume the existence of a *proof* of a particular Σ_1-formula. To simplify the presentation we firstly consider proofs that admit only quantifier-free cut formulas. We dwell on the general case in Appendix A.

Definition 16. *A proof in* TIND *that admits only quantifier-free cut formulas is called almost cut-free.*

Convention. For the remainder of this section we assume that the considered proofs are almost cut-free and the respective endsequent satisfy property (P).

3.1. Extraction of Herbrand disjunctions from proofs

Let $(A)^m$ denote the multiset $\{A, \dots, A\}$, if the cardinality of this set equals m. The number m is called the *multiplicity* of A. We introduce a notation that counts the maximal number of iterations of (tind)-rules in TIND-proofs.

Definition 17. $\mathrm{it}(\Pi)$ *is defined inductively:*

- *If Π is an axiom, then* $\mathrm{it}(\Pi) = 0$.
- *Otherwise consider the last inference rule* Q *of Π: If* Q *is a (tind)-inference, then* $\mathrm{it}(\Pi) = \mathrm{it}(\Pi_0) + 1$, *where Π_0 denotes the subproof deducing the upper sequent of* Q. *Now suppose* Q *is not a (tind)-inference, but an inference with with upper sequents S_i, deduced by proofs Π_i. Then* $\mathrm{it}(\Pi) = \max\{\mathrm{it}(\Pi_i)\}$.

Lemma 1. *Let Π be proof of $S = (\Gamma \to \Delta)$ such that $|\Pi| = k$. Assume $\Gamma = A_1, \dots, A_n$ and $\Delta = B_1, \dots, B_m$. Then there exists a proof Π' of*

$$(A_1)^{a_1}, \dots, (A_n)^{a_n} \to (B_1)^{b_1}, \dots, (B_m)^{b_m}\ ,$$

such that Π' only admits contractions on quantifier-free formulas; $|\Pi'| \leq k^2$, $\Sigma_{i=1}^n a_i + \Sigma_{i=1}^m b_i \leq k+1$, and $\mathrm{it}(\Pi) = \mathrm{it}(\Pi')$. Moreover, if A_i (B_i) is quantifier-free, then $a_i = 1$ ($b_i = 1$).

Lemma 2. *Let Π be a proof of $S = (\Gamma \to \Delta)$ admitting contractions only on quantifier-free formulas. Assume $\Gamma = A_1, \ldots, A_n$ and $\Delta = B_1, \ldots, B_m$, so that the A_i ($i = 1, \ldots, n$) can be written as $\forall \overline{y} P_i(\overline{y})$ and the B_i ($i = 1, \ldots, m$) can be written as $\exists \overline{x} Q_i(\overline{x})$. Then there exists a proof Π' (admitting contractions only on quantifier-free formulas) of*

$$C_1, \ldots, C_n \to D_1, \ldots, D_m \ ,$$

such that each C_i is an instances of $P_i(\overline{y})$ and each D_i is an instances of $Q_i(\overline{x})$. Moreover in Π' only quantifier-free formulas occur as weakening formulas, $|\Pi| = |\Pi'|$, and $\mathrm{it}(\Pi) = \mathrm{it}(\Pi')$.

Theorem 2. *Let Π be a proof of $S = (\Gamma \to \Delta)$, such that $|\Pi| = k$ and $\mathrm{it}(\Pi) = l$. There exists a Herbrand sequent T of S in matrix-form with matrix M:*

$$C_1, \ldots, C_n \to D_1, \ldots, D_m \ ,$$

where each C_i can be written as $P_i(\mathbf{a}_1, \ldots, \mathbf{a}_{p_i})$ (P_i quantifier-free) and each D_i can be written as $Q_i(\mathbf{b}_1, \ldots, \mathbf{b}_{q_i})$ (Q_i quantifier-free). The variables in $\overline{\mathbf{a}}$ need not be distinct from those in $\overline{\mathbf{b}}$. The Herbrand sequent T fulfils

1. *For each quantifier-free formula P in Γ there exists an C_i, $P = C_i$ and similarly for each quantifier-free $P \in \Delta$ exists D_i, $P = D_i$.*
2. *$|M| \leq k + 1$ and $\max(\{p_i \mid i = 1, \ldots, n\} \cup \{q_i \mid i = 1, \ldots, m\}) \leq l$.*

Proof. W.l.o.g. we can assume that in Π all structural rules act on quantifier-free formulas only. This is a consequence of Lemma 1 and Lemma 2. As Π is an almost cut-free proof, Π is either cut-free or all cut formulas in Π are quantifier-free. Furthermore, S satisfies property (P), cf. Definition 12. This implies that the initial sequents in Π must not contain quantifiers, because no existential quantifier may occur in the antecedent, while no universal quantifier may occur in the succedent. Another consequence of property (P) is that propositional inferences, i.e. inferences introducing propositional logical symbols, are applied only to quantifier-free formulas. We proceed by induction on k. We abbreviate induction hypothesis by i.h.

Let $k = 1$, then Π is an axiom $A \to A$. We already know that A has to be quantifier-free. We set M equal to $A \to A$. By assumption A does not contain elements of $\mathbf{NV}$, therefore the sequent $\Gamma^\star \to \Delta^\star$ is equal to $A \to A$ which is trivially valid. Furthermore, $|M| \leq 2$, and the number of different variables in $\mathbf{NV}(A)$ is $\leq 0 = \mathrm{it}(\Pi)$.

This establishes the base case. Now assume $k > 1$. We proceed by case distinction on the last inference Q of Π. Let Π_i, $i = 0$ or $i = 1, 2$ denote the subproof(s) deducing the upper sequent(s) of Q. We only consider the case where $\mathsf{Q} = (\mathit{tind})$.

- Assume Q is a (tind)-inference. By i.h. we conclude the existence of matrix M_0 of the form

$$P(c), \overline{C} \to \overline{D}, P(S(c)) \ ,$$

where P is quantifier-free. Note that the eigenvariable c may occur in $\overline{C}$ and in $\overline{D}$. There exists a number N and variables $\mathbf{a}_1, \dots, \mathbf{a}_p$; $p \leq \mathrm{it}(\Pi_0)$, such that $T(c) = (P(c), \Gamma^\star(c) \rightarrow \Delta^\star(c), P(S(c))$ is valid, where $\Gamma^\star$ is the multiset of formulas $\{C_i(c, \mathbf{a}_1, \dots, \mathbf{a}_p)\sigma \mid \sigma\colon \mathbf{NV}(C_i) \rightarrow \{\mathbf{0}, \dots, \mathbf{N}\}\}$ and $\Delta^\star$ is the multiset of formulas $\{D_i(c, \mathbf{a}_1, \dots, \mathbf{a}_p)\sigma \mid \sigma\colon \mathbf{NV}(D_i) \rightarrow \{\mathbf{0}, \dots, \mathbf{N}\}\}$. As $T(c)$ is valid, each instance $T(\mathbf{0}), \dots, T(\mathbf{n})$ is valid, too. Therefore the sequent T

$$P(\mathbf{0}), \Gamma^\star(\mathbf{0}), \dots, \Gamma^\star(\mathbf{n}) \rightarrow \Delta^\star(\mathbf{0}), \dots, \Delta^\star(\mathbf{n}), P(\mathbf{n}) ,$$

is valid. Let $\mathbf{a}$ denotes a fresh variable from $\mathbf{NV}$; we define the matrix of T as the sequent

$$E_1, \dots, E_n \rightarrow F_1, \dots, F_m ,$$

where $E_i = C_i(\mathbf{a}, \mathbf{a}_1, \dots, \mathbf{a}_p)$ for $i = 1, \dots, n$ and $F_i = D_i(\mathbf{a}, \mathbf{a}_1, \dots, \mathbf{a}_p)$ for $i = 1, \dots, m$.

It remains to verify (1)—(2). The first condition follows trivially by i.h. The first part of condition (2) follows by i.h. as $|M| = |M_0|$. The second part follows as the number of different variables in $\mathbf{NV}(\overline{E})$ or $\mathbf{NV}(\overline{F})$ is $\leq p + 1 \leq \mathrm{it}(\Pi_0) + 1 = \mathrm{it}(\Pi)$.

□

Proposition 2. *Assume the notation of the theorem. Then the bound l on* $\max(\{p_i \mid i = 1, \dots, n\} \cup \{q_i \mid i = 1, \dots, m\})$ *is optimal.*

Proof. Let n be arbitrary and let $S(\mathbf{n}) =$

$$\forall \overline{x}\, (P_1(x_i) \supset P_1(S(x_i)) \vee \cdots$$
$$\cdots \vee P_1(x_1) \supset P_1(S(x_1)))\, , P_1(\mathbf{0}), \dots, P_m(\mathbf{0}) \rightarrow P_1(\mathbf{n}), \dots, P_m(\mathbf{n})$$

where $\overline{x} = x_1, \dots, x_m$ and P denotes a unary predicate symbol. In Table 4 we give the end-piece of a cut-free derivation of $S(\mathbf{n})$ that uses exactly m iterated (tind)-inferences. The form of the omitted subproof Π_0 is obvious. We claim that any Herbrand sequent of $S(\mathbf{n})$ in matrix-form, that fulfils the requirements of the theorem has an Herbrand matrix $C_1, \dots, C_k \rightarrow D_1, \dots, D_l$ s.t. for at least one i, C_i (or D_i) has the form $C_i(\mathbf{a}_1, \dots, \mathbf{a}_m)$ (or $D_i(\mathbf{a}_1, \dots, \mathbf{a}_m)$), where the $\mathbf{a}_i$ are distinct variables from $\mathbf{NV}$.

Clearly the proposition follows from this claim. We show the claim. Let $n_{i1}, \dots, n_{im}$ denote arbitrary natural numbers $< n$. Firstly observe that any Herbrand sequent T of $S(\mathbf{n})$ has to include all formulas

$$(P_1(\mathbf{n}_{i1}) \supset P_1(S(\mathbf{n}_{i1}))) \vee \cdots \vee (P_m(\mathbf{n}_{im}) \supset P_m(S(\mathbf{n}_{im}))) \, , \qquad (4)$$

as sequent formulas in the antecedent. Assume to the contrary there exists numbers $n_1, \dots, n_m < n$ s.t. $\bigvee_{i=1}^{m} P_i(\mathbf{n}_i) \supset P_i(S(\mathbf{n}_i))$ is not present in T. We define an evaluation function $v_{(\mathcal{I})}$ on a suitable first-order structure I.

$$v_{(\mathcal{I})}(P_i(\mathbf{r})) := \begin{cases} \textbf{true} & r \leq n_i \\ \textbf{false} & r > n_i \end{cases}$$

Then $v_{(\mathcal{I})}$ falsifies the sequent. Now the claim states that for at least one i, the number of *different* variables in $\mathbf{NV}(C_i)$ (or $\mathbf{NV}(D_i)$) has to be at least m. Assume to the contrary that for all i the number of different such variables is strictly less than m. Then a counting argument reveals that it is not possible to represent all necessary formulas of form (4) through suitable instantiations of matrix $C_1, \dots, C_k \rightarrow D_1, \dots, D_l$. This completes the proof of the claim. □

Table 4. Uniform cut-free derivation of $S(\mathbf{n})$

$$\begin{array}{c}
\mathit{\Pi}_0 \\
\bigvee_{i=1}^{m} \left(P_i(a_i) \supset P_i(S(a_i))\right), P_1(a_1), \dots, P_m(a_m) \rightarrow P_1(S(a_1)), \dots, P_m(S(a_m)) \\
\hline\hline
\forall \overline{x} \left(\bigvee_{i}^{m} P_i(x_i) \supset P_i(S(x_i))\right), P_1(a_1), \dots, P_m(a_m) \rightarrow P_1(S(a_1)), \dots, P_m(S(a_n)) \\
\hline
\forall \overline{x} \left(\bigvee_{i=1}^{m} P_i(x_i) \supset P_i(S(x_i))\right), P_1(\mathbf{0}), \dots, P_m(a_m) \rightarrow P_1(\mathbf{n}), \dots, P_m(S(a_n)) \\
\hline\hline
\forall \overline{x} \left(\bigvee_{i=1}^{m} P_i(x_i) \supset P_i(S(x_i))\right), P_1(\mathbf{0}), \dots, P_m(\mathbf{0}) \rightarrow P_1(\mathbf{n}), \dots, P_m(\mathbf{n})
\end{array}$$

The a_i, $i = 1, \dots, m$, are distinct eigenvariables and $\mathit{\Pi}_0$ deduces the topmost sequent.

Corollary 2. *Let $\mathit{\Pi}$ be an almost cut-free proof of $S = (\rightarrow \exists \overline{x} P(x_1, \dots, x_n))$, P quantifier-free, such that $|\mathit{\Pi}| = k$ and $\mathrm{it}(\mathit{\Pi}) = l$. Then there exists a number N and a Herbrand disjunction of the form*

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \dots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \dots, \mathbf{i}_p) , \tag{5}$$

where each $C_i(\mathbf{i}_1, \dots, \mathbf{i}_p)$ is an instance of $P(x_1, \dots, x_n)$ such that all numerals in this instance are fully indicated. Furthermore

1. *The length of the 'inner' disjunction $C_1 \vee \cdots \vee C_m$ is $\leq k + 1$.*
2. *The length of the 'outer' disjunction $\bigvee_{i_1} \cdots \bigvee_{i_p}$ is $\leq l$.*
3. *The maximal iteration of (tind)-inferences in $\mathit{\Pi}$ is an optimal bound on the length of the 'outer' disjunction.*

Proof. If we employ the lemma on the $\mathit{\Pi}$ and S we conclude the existence of a Herbrand sequent $T = (\rightarrow \mathit{\Gamma}^{\star})$ in matrix-form and a Herbrand matrix M: $\rightarrow C_1, \dots, C_m$, such that $\mathit{\Gamma}^{\star}$ is the multiset $\{C_i\sigma;\ \sigma\colon \mathbf{NV} \rightarrow \{\mathbf{0}, \dots, \mathbf{N}\}\}$.

By Theorem 2.2 together with the standard interpretation of sequents, we conclude $m \leq k + 1$. This shows the first assertion. Now if we fully indicate the variables in $\mathbf{NV}(C_i)$, C_i can be written as $C_i(\mathbf{a}_1, \dots, \mathbf{a}_{p_i})$. Let $p = \max\{\overline{p}\}$, then the C_i can be written more uniformly as $C_i(\mathbf{a}_1, \dots, \mathbf{a}_p)$. Due to Theorem 2.2 if follows that $p \leq l$. Furthermore, this bound is optimal, by Proposition 2. Recalling the standard interpretation of sequents this implies the validity of the sequent

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p)$$

□

Definition 18. *Herbrand disjunctions which are written in the form (5) are called of* matrix-form *(with respect to the matrix* $C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p)$*)*

Example 1 (continued). Let S,T, and M be defined as above. Then the Herbrand disjunction D of S can be written as

$$\bigvee_{i=0}^{n} \left(C(\mathbf{i}, \mathbf{0}) \vee \cdots \vee C(\mathbf{i}, f^{m-1}(\mathbf{0}))\right) ,$$

where $C(\mathbf{i}, t)$ equals

$$\neg P(\mathbf{0}, \mathbf{0}) \vee (P(\mathbf{i}, t) \wedge \neg P(S(\mathbf{i}), t)) \vee (P(\mathbf{n}, t) \wedge \neg P(\mathbf{n}, f(t))) \vee P(\mathbf{n}, f^m(\mathbf{0})) .$$

□

Remark 2. Theorem 2 shows that we can only 'contract' iterated occurrences of (tind)-inference in proofs into a single inference by an increase in prooflength that depends on the occurring numerals in the endsequent.

Let Π, S be defined as in Theorem 2. The following proposition shows that the assumptions that Π is almost cut-free and the fact that S satisfies property (P) cannot be lifted without loosing the optimal bound on the 'outer' disjunction in the Herbrand disjunction H of S.

Proposition 3. *1. Let Π be an almost cut-free proof of T (not necessarily fulfilling property* (P)*). Then no function f, depending only on* $\mathrm{it}(\Pi)$*, can exist that bounds the length of the outer disjunction of any Herbrand disjunction H, where H has the form (5).*

2. Let Π be proof of T (not necessarily almost cut-free). Then no function f, depending only on $\mathrm{it}(\Pi)$*, can exist that bounds the length of the outer disjunction of any Herbrand disjunction H, where H has the form (5).*

Proof. First we show Proposition 3.1. Consider the sequents $T(\mathbf{n}) =$

$$(\forall x_1 P_1(x_1) \supset P_1(S(x_1))) \vee \cdots$$
$$\cdots \vee (\forall x_m P_m(x_m) \supset P_m(S(x_m))), P_1(\mathbf{0}), \ldots, P_m(\mathbf{0}) \rightarrow P_1(\mathbf{n}), \ldots, P_m(\mathbf{n})$$

These sequents are uniform derivable from m instances of the proof-fragment $\Pi_i(\mathbf{n})$; $i = 1, \ldots, m$, given in Table 5 together with $m-1$ $\vee$: left-inferences. Obviously $\mathrm{it}(\Pi_i) = 1$ holds, hence by definition $\mathrm{it}(\Pi) = \max\{\mathrm{it}(\Pi_i)\} = 1$.

However, any Herbrand sequent of $T(\mathbf{n})$ has to have the form described in the proof of Proposition 2 and the proposition follows.

To prove Proposition 3.2, we observe that the quantifiers in $T(\mathbf{n})$ can be shifted outward by a single cut-inference with the sequent

$$\forall\overline{x}(P_1(x_1)\supset P_1(S(x_1)))\vee\cdots\vee(P_m(x_m)\supset P_m(S(x_m)))\rightarrow$$
$$\rightarrow(\forall x_1P_1(x_1)\supset P_1(S(x_1)))\vee\cdots\vee(\forall x_mP_m(x_m)\supset P_m(S(x_m)))$$

It is easy to see that the length of the derivation of this sequent depends only on the number of quantifiers m but not on n. Hence $T(\mathbf{n})$ can uniformly transformed into the sequent $S(\mathbf{n})$ for any n. □

Table 5. Proof fragment $\Pi_i(\mathbf{n})$

$$\dfrac{\dfrac{\dfrac{P_i(a_i)\rightarrow P_i(a_i)\quad P_i(S(a_i))\rightarrow P_i(S(a_i))}{P_i(a_i)\supset P_i(S(a_i)),P_i(a_i)\rightarrow P_i(S(a_i))}}{\forall x_iP_i(x_i)\supset P_i(S(x_i)),P_i(a_i)\rightarrow P_i(S(a_i))}}{\forall x_iP_i(x_i)\supset P_i(S(x_i)),P_i(\mathbf{0})\rightarrow P(\mathbf{n})}$$

The a_i denotes a free eigenvariable.

The next proposition shows that for the results above the restriction of (tind) to quantifier-free formulas is necessary. We assume an extension TIND$^+$ of the system TIND such that in TIND$^+$ term-induction for Σ_1-formulas is admitted.

Proposition 4. *Let Π be a proof of S in* TIND$^+$. *Then no function f, independent on the term-structure of S, can exist that bounds the length of the shortest Herbrand matrix.*

Proof. For any unary function symbol f, we define the n^{th} iteration f^n by $f^0(t)=t$; $f^{n+1}(t)=f(f^n(t))$. In TIND$^+$ the sequent $S(\mathbf{n})$

$$P(\mathbf{0},\mathbf{0}),\forall y_1\forall y_2(P(y_1,y_2)\supset P(S(y_1),f(y_2))\rightarrow\exists x\ P(\mathbf{n},x)\ ,$$

is uniformly derivable, see Table 6 for the interesting proof-fragment. Every Herbrand sequent $H(\mathbf{n})$ for fixed n, has to include all implications $P(\mathbf{i},f^i(\mathbf{0}))\supset P(S(\mathbf{i}),f^{i+1}(\mathbf{0}))$ for arbitrary i; $0\leq i\leq n-1$. (This follows by the same argument as in the proof of Proposition 2.) Hence the length of any Herbrand matrix of $H(\mathbf{n})$ will always depend on n. □

Proposition 5. *Assume $\mathcal{L}$ is restricted to a* monadic *language, where at most unary function symbols and predicate symbols are admitted. Let Π be a proof of $S=(\rightarrow\exists x_1,\ldots,\exists x_nP(x_1,\ldots,x_n))$, P quantifier-free, such that $|\Pi|=k$ and $\text{it}(\Pi)=l$. Then there exists a number N and a Herbrand disjunction of the form (5) such that*

Table 6. Proof fragment in $\textsc{Tind}^+$

$$\begin{array}{c}
\forall y_1 \forall y_2 P(y_1, y_2) \supset P(S(y_1), f(y_2)), P(c_1, c_2) \rightarrow P(S(c_1), f(c_2)) \\
\hline
\forall y_1 \forall y_2 P(y_1, y_2) \supset P(S(y_1), f(y_2)), P(c_1, c_2) \rightarrow \exists x P(S(c_1), x) \\
\hline
\forall y_1 \forall y_2 P(y_1, y_2) \supset P(S(y_1), f(y_2)), \exists x P(c_1, x) \rightarrow \exists x P(S(c_1), x) \\
\hline
\forall y_1 \forall y_2 P(y_1, y_2) \supset P(S(y_1), f(y_2)), \exists x P(\mathbf{0}, x) \rightarrow \exists x P(\mathbf{n}, x)
\end{array}\ (tind)^+$$

1. The length of the 'inner' disjunction $C_1 \vee \cdots \vee C_m$ *is* $\leq k + 1$.
2. The length of the 'outer' disjunction $\bigvee_{i_1} \cdots \bigvee_{i_p}$ *is* $\leq \min\{l, n\}$.

3.2. Term-complexities of Herbrand disjunctions

In the previous section we have analysed the logical structure of a Herbrand disjunction H of a sequent S that satisfies property (P). In this section we study the term-structure of Herbrand disjunctions.

This study is motivated by Krajicek and Pudlak's analysis of the term-structure of sequent calculi proofs in [21]. These results imply that we can assume w.l.o.g that the maximal depth of any term t occurring in a Herbrand disjunction of a sequent S (provable in LK by Π) is bounded uniformly, i.e. there exists an elementary function f, such that $\mathrm{dp}(t) \leq f(|\Pi|, \textsc{size}(S))$. We exemplify the general argument on the basis of the system LK: We show directly (i.e. without reference to the results of [21]) how-to uniformly bound the term-complexity of a given Herbrand disjunction.

Let $S(\overline{r})$ be a sequent with parameters $\overline{r} = r_1, \ldots, r_l$

$$A_1, \ldots, A_n \rightarrow B_1, \ldots, B_m \ .$$

We assume the A_i $(i = 1, \ldots, n)$ can be written as $\forall \overline{y} P_i(\overline{y}, \overline{r})$ and the B_i $(i = 1, \ldots, m)$ as $\exists \overline{x} Q_i(\overline{x}, \overline{r})$. As above, we assume the indicated bound variables are not shared. On the other hand the series of parameter terms $\overline{r}$ may be shared among the A_i and B_j. Assume

$$C_1, \ldots, C_k \rightarrow D_1, \ldots, D_l \ ,$$

is an arbitrary Herbrand sequent T of S, where each C_i is an instance of some $P_i(\overline{y}, \overline{r})$ of the form $P_i(t_1, \ldots, t_{p_i}, \overline{r})$. Similarly the D_i have the form $Q_i(t_1, \ldots, t_{q_i}, \overline{r})$.

Definition 19. *Let T be defined as above. We define a sequent H*

$$E_1, \ldots, E_k \rightarrow F_1, \ldots, F_l \ ,$$

such that the E_i are of the form $P_i(a_{i1}, \ldots, a_{ip_i}, \overline{r})$, similarly the D_i have the form $Q_i(b_{i1}, \ldots, b_{iq_i}, \overline{r})$, such that for each i fresh variables $\overline{a}$ and $\overline{b}$ are used. The sequent H is called an abstraction of T. The formulas $P_i(a_1, \ldots, a_{p_i}, \overline{r})$ are called abstraction formulas.

Example 1 (continued). The abstraction H of T can be written as

$$P(\mathbf{0},\mathbf{0}), P(a_0,b_0) \supset P(S(a_0),b_0), \dots, P(a_{n-1},b_{n-1}) \supset P(S(a_{n-1}),b_{n-1}),\\ P(c_0,d_0) \supset P(c_0,f(d_0)), \dots, P(c_{m-1},d_{m-1}) \supset P(c_{m-1},f(d_{m-1})) \rightarrow\\ \rightarrow P(\mathbf{n},f^m(\mathbf{0}))\ .$$

□

Remark 3. For the time being we do not abstract the parameters $\overline{r}$ in S. This however, will become necessary later on.

Note that the length of an abstraction equals the length of T, and for a given T an abstraction of T is unique up-to renaming of (free) variables. Therefore, we speak of *the* abstraction of T. The abstraction H and the Herbrand sequent T induce an *unification problem* U: Let

$$R(u_1,\dots,u_n) \qquad\qquad R(v_1,\dots,v_n)$$

be atomic formulas in H, such that there exist occurrences R^1, R^2 of the same subformula R in T, and a substitution δ with $R^1 = R(\overline{u})\delta$, $R^2 = R(\overline{v})\delta$. For each such pair $(R(\overline{u}), R(\overline{v}))$, we add the equations

$$u_1 = v_1 \quad \cdots \quad u_n = v_n\ ,$$

to U. As T itself defines a solution to the unification problem U, this unification problem is solvable. Employing well-known results from unification theory[6] there exists a most general unifier σ such that σ solves U. Furthermore, we can find a substitution η, such that $H\sigma\eta = T$.

Example 1 (continued). The unification problem U induces by H is defined by

$$a_0 = \mathbf{0}, b_0 = \mathbf{0}, a_1 = S(a_0), b_0 = b_1, \dots, c_0 = S(a_{n-1}), d_0 = b_{n-1},\\ c_0 = c_1, d_1 = f(d_0), \dots, f^m(0) = f(d_{m-1}), c_{m-1} = \mathbf{n}\ .$$

□

It follows by definition of U that $H\sigma$ is valid iff T is valid. We say that $H\sigma$ is a *generalisation* of T. Note that for $H\sigma$ holds: For any term t, the maximal term depth of t is grossly bounded by $\leq 2^m \mathrm{dp}(H)$, where m denotes the number of variables in U. This observation is the key step in giving an upper bound for the term-complexity of Herbrand disjunctions. As $\mathrm{dp}(H) \leq \mathrm{dp}(S)$ the claim follows as soon as we can bound the number m in the size of S and the length of Π. This is an easy consequence of Herbrand's Theorem, as long as we can assume that Π is an LK-proof.

[6] See e.g. [1] for a survey paper on the theory of unification; we review some basic concepts in Section 2.1

We would like to emphasise that the employed proof method is well-established: Let $S = (\rightarrow \exists \overline{x} P(x_1, \ldots, x_n))$, P quantifier-free. We consider a disjunction of instances of $P(x_1, \ldots, x_n)$.

$$P(a_{1_1}, \ldots, a_{1_n}) \vee \cdots \vee P(a_{m_1}, \ldots, a_{m_n}) \ ,$$

of fixed length m, where the sequences of variables $\overline{a}_1, \ldots, \overline{a}_m$ are all different. It is well-known that it is decidable whether there exists sequences of terms $\overline{t}_1, \ldots, \overline{t}_m$ such that $P(t_{1_1}, \ldots, t_{1_n}) \vee \cdots \vee P(t_{m_1}, \ldots, t_{m_n})$ is valid; to establish this, one proceeds as above, cf. [14,19].

If we alter the assumption such that the given proof Π of S is a proof in TIND, rather than a proof in LK, we cannot directly apply this proof method, if we want to bound the term-complexity of the reduct of a Herbrand disjunction in matrix-form. Due to Lemma 1, the length of the abstraction H of the Herbrand sequent T, and hence the number of variables in H, cannot be uniformly bounded. However, due to Theorem 2, we can assume that the Herbrand sequent T is in matrix-form, where the length of the *Herbrand matrix* of T can uniformly bounded.

This observation will allows us to define a suitable unification problem $U^\star$ adapted to the new situation. To this end we use (a variant of) *congruence unification* which has already been introduced in [10]. Below we present a modular variant of congruence unification, that can be applied in a variety of situation.

3.3. Bounding the Depth in Herbrand Disjunctions of matrix-form

Definition 20. *Let e be an expression, i.e. a term, a formula, or a sequent. Assume e includes m occurrences of numerals; we write e as $e(\mathbf{n}_1, \ldots, \mathbf{n}_m)$. Then the reduct of e is defined as $e(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, where $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are new variables from* **NV**. *Upto renaming of variables the reduct is unique; we write e° to denote the reduct of e.*

Definition 21. *Two expressions s, t are* variants *if $s^\circ = t^\circ \rho$, for some renaming substitution ρ:* $\mathbf{NV} \rightarrow \mathbf{NV}$.

Example 2. Let g and h denote unary (respectively binary) function symbols; k, l, m, n denote natural numbers. Assume $s = h(S^n(\mathbf{0}), g^m(\mathbf{0}), S^l(\mathbf{c}))$, $\mathbf{c} \in \mathbf{NV}$. The term $t = h(S^l(\mathbf{0}), g^m(\mathbf{0}), S^n(\mathbf{c}))$ is a variant of s (regardless whether l equals n or not, while $r = h(S^n(\mathbf{0}), g^k(\mathbf{0}), S^l(\mathbf{c}))$, if $k \neq m$ is not. □

Clearly the 'variant' relation is an equivalence relation. Let E be a set of expressions, then we define the *reduct of E* (denoted E°) as the set $\{e^\circ \mid e \in E\}$. We set $\mathrm{dr}(e) := \mathrm{dp}(e^\circ)$ to denote the depth of the reduct of an expression e. Suppose E is a set, then $\mathrm{dr}(E) := \mathrm{dp}(E^\circ)$.

Definition 22. *A congruence unification problem is a pair (U, X) such that U denotes a standard unification problem (over the set of terms) and X is a partition of a subset of* **V**. *A congruence unification problem (U, X) is solved by an unifier σ, if*

1. *σ is a standard unifier of U and*
2. *σ in addition fulfils: Let $C = \langle a_1, \dots, a_n \rangle$ denotes a variables-class in X. Then $a_1\sigma, \dots, a_n\sigma$ are all variants.*

The property 2 is called congruence (unification) property*.*

Congruence unification has similar properties as standard unification. This is established by Theorem 3 and Theorem 4, below. The proofs of these theorems together with a definition of a congruence unification procedure can be found in Appendix C. We conceive the unification problem U as a set and define $\mathrm{dp}((U, X)) := \mathrm{dp}(U)$.

Theorem 3. *Let (U, X) be a congruence unification problem. Then there exists a set of most general congruence unifiers of (U, X) iff (U, X) is solvable. Let the set of most general solutions of (U, X) be denoted as $\mathrm{Sol}((U, X))$. Then its reduct $(\mathrm{Sol}((U, X)))^\circ$ is finite.*

Theorem 4. *Let $\sigma \in \mathrm{Sol}((U, X))$. There exists an elementary function f, s.t. $\mathrm{dr}((U, X)\sigma) \leq f(d, n)$, where $d = \mathrm{dr}((U, X)))$ and $n = card(\{a \mid \mathrm{dp}(a, U) > 0\})$, the cardinality of the set $\{a \mid \mathrm{dp}(a, U) > 0\}$.*

Recall that the set of variables occurring in an expression e is denoted as $\mathbf{V}(e)$. In this section we define the unification problem promised in Section 3.2. Let S be a sequent (satisfying property (P)) provable in TIND, and assume T is a Herbrand sequent of S. Following Definition 19, we define an abstraction H of T. As emphasised in Section 3.2, H induces a (standard) unification problem U

$$u_1 = v_1, \dots, u_n = v_n \ . \tag{6}$$

It follows from the existence of T that the problem (6) is solvable. Hence for each pair $(u_i = v_i)$ exists a common instance w_i.

Definition 23. *Let λ be solution for (6). We define a relation $\sim$ on the equations in (6) such that $(u_i = v_i) \sim (u_j = v_j)$ iff*

1. *$(u_i = v_i)\lambda$ is a variant of $(u_j = v_j)\lambda$, and*
2. *there exists a renaming ρ, such that $(u_i = v_i)\rho = (u_j = v_j)$.*

With respect to a fixed solution λ of (6) the relation $\sim$ is an equivalence relation. For each class $C \in U/_\sim$ we choose an equation $(u = v)$ as representative and write $[u = v]$ to denote C. The set of all these representatives is denoted as $U^\star$. Let $C := [u = v]$; we define a partition X_C of the variables occurring in C and to this avail we define an equivalence relation $\approx$. Assume $(u = v), (r = s) \in C$, such that $\mathbf{V}(u = v) = \{a_1, \dots, a_m\}$ and $\mathbf{V}(r = s) = \{b_1, \dots, b_m\}$. By definition of $\sim$ there exists a renaming ρ: $\mathbf{V}(u = v) \to \mathbf{V}(r = s)$, we define an equivalence relation $\approx$: W.l.o.g we assume that $a_i = b_i\rho$ for each i and set $a_1 \approx b_1, \dots, a_m \approx b_m$. The definition of X_C is complete if all equations $(r = s) \in C$ have been considered. X is defined as the union of the partitions X_C, that is by extending the equivalence relation $\approx$ in the natural way..

This completes the definition of the congruence unification problem $(U^\star, X)$.

Example 1 (continued). We define the unification problem $(U^\star, X)$ that is based on the unification problem U. Then $U^\star$ is defined as follows

$$a_0 = \mathbf{0}, b_0 = \mathbf{0}, a_1 = S(a_0), b_0 = b_1, d_1 = f(d_0), \dots,$$
$$\dots, f^m(\mathbf{0}) = f(d_{m-1}), c_{m-1} = \mathbf{n}\ .$$

such that X includes:

$$\langle a_0, a_1, \dots, a_{n-1}, b_0, \dots, b_{n-1}, c_0, \dots, c_{m-1}, d_0\rangle$$
$$\langle d_1\rangle, \dots, \langle d_{m-1}\rangle\ .$$

Set

$$\begin{aligned}\sigma_1 :=\{&a_0 \mapsto \mathbf{0}, \dots, a_{n-1} \mapsto \mathbf{n-1},\\ &b_0 \mapsto \mathbf{0}, \dots, b_{n-1} \mapsto \mathbf{0},\\ &c_0 \mapsto \mathbf{n}, \dots, c_{m-1} \mapsto \mathbf{n},\\ &d_0 \mapsto \mathbf{0}, \dots, d_{m-1} \mapsto f^{m-1}(\mathbf{0})\}\\ \sigma_2 :=\{&a_0 \mapsto \mathbf{0}, a_1 \mapsto \mathbf{1}, \dots, a_{n-1} \mapsto \mathbf{1},\\ &b_0 \mapsto \mathbf{0}, b_1 \mapsto \mathbf{0}, b_2 \mapsto \mathbf{2}, \dots, b_{n-1} \mapsto S^{n-1}(0),\\ &c_0 \mapsto \mathbf{n}, \dots, c_{m-1} \mapsto \mathbf{n},\\ &d_0 \mapsto \mathbf{0}, \dots, d_{m-1} \mapsto f^{m-1}(\mathbf{0})\}\ .\end{aligned}$$

Both σ_1 and σ_2 are solutions to $(U^\star, X)$. □

The following lemmas show that $(U^\star, X)$ is well-defined. The assertions follow easily from the definitions.

Lemma 3. *Let U denote the standard unification problem (6). Suppose $(U^\star, X)$ is defined as above and is solvable with σ, then for each equation $(u_i = v_i) \in [u = v] \subseteq U$, $(u = v)\sigma$ is a variant of $(u_i = v_i)\sigma$.*

Lemma 4. *Let U and $(U^\star, X)$ be defined as above. Assume U and $(U^\star, X)$ are solvable; suppose the most general congruence unifier solving $(U^\star, X)$ is denoted as σ. Then there exists an instance λ of σ such that λ solves the standard unification problem U and λ is a solution to $(U^\star, X)$. Moreover, if S includes all instances of $\sigma \in \mathrm{Sol}((U^\star, X))$ fulfilling these requirements, then $\max\{\mathrm{dr}(e\lambda) | \lambda \in S\} = \mathrm{dr}(e\sigma)$, for an arbitrary expression e.*

Definition 24. *Suppose T, T' denote Herbrand sequents in matrix-form of a provable sequent S with respect to the matrix*

$$C_1, \dots, C_n \rightarrow D_1, \dots, D_m \qquad C'_1, \dots, C'_n \rightarrow D'_1, \dots, D'_m \quad \textit{respectively}\ ,$$

fulfilling the requirements of Theorem 2.

The Herbrand sequent T' is said to be more general than T, if there exists a substitution $\sigma\colon \mathbf{FV} \cup \mathbf{NV} \to \mathcal{T}$ with $C'_i\sigma = C_i$ for all $i = 1, \dots, n$ and $D'_i\sigma = D_i$ for all $i = 1, \dots, m$.

The following proposition is a direct consequence of the completeness of congruence unification procedure, cf. Theorem 3 and Lemma 4.

Proposition 6. *Let $S(\overline{r}) = (\varGamma(\overline{r}) \rightarrow \varDelta(\overline{r}))$ be provable in* TIND *and suppose T denotes a Herbrand sequent of S in matrix-form, fulfilling the requirements of Theorem 2. Then there exists a Herbrand sequent T' of S in matrix-form, fulfilling the requirements of Theorem 2, such that T' is more general than T.*

Theorem 5. *Let $\varPi$ be a proof of $S(\overline{r}) = (\varGamma(\overline{r}) \rightarrow \varDelta(\overline{r}))$, such that $|\varPi| = k$ and $\mathrm{it}(\varPi) = l$ and the series $\overline{r}$ denotes parameters in S. Let T denote a Herbrand sequent in matrix-form of S such that the Herbrand matrix M of T has the form*

$$C_1, \ldots, C_n \rightarrow D_1, \ldots, D_m \ ,$$

where each $C_i(\overline{r})$ can be written as $P_i(\mathbf{a}_1, \ldots, \mathbf{a}_{p_i}, \overline{r})$ (P_i quantifier-free) and each $D_i(\overline{r})$ can be written as $Q_i(\mathbf{a}_1, \ldots, \mathbf{a}_{q_i}, \overline{r})$ (Q_i quantifier-free); $\overline{\mathbf{a}} \in \mathbf{NV}$. Then T fulfils

1. *For each quantifier-free formula P in $\varGamma$ there exists an C_i, $P = C_i$ and similarly for each quantifier-free $P \in \varDelta$ exists D_i, $P = D_i$.*
2. *$|M| \leq k + 1$ and $\max(\{p_i \mid i = 1, \ldots, n\} \cup \{q_i \mid i = 1, \ldots, m\}) \leq l$.*
3. *There exists an elementary function f, such that $\mathrm{dr}(M) \leq f(c, s, d)$, where $c = |M|$, $s = \textsc{size}(S(\overline{c}))$ ($c_i \in \mathbf{FV}$) and $d = \mathrm{dp}(S(\overline{c}))$.*

Proof. We employ Theorem 2 to conclude the existence of a Herbrand sequent in matrix-form T fulfilling properties (1)—(2). Now we construct an abstraction H of the Herbrand sequent T together with the induced unification problem U. Then we construct the congruence unification problem, entailed by U as above. This unification problem is denoted as $(U^\star, X)$.

Suppose M denotes the Herbrand matrix T. Then it is not difficult to argue, that $\mathrm{card}(X)$ and thus $\mathrm{card}(\{a \mid \mathrm{dp}(a, U^\star) > 0\})$ depends only on $|M|$ and the number of argument positions in $S(\overline{c})$ ($\leq \textsc{size}(S(\overline{c}))$). Hence, $\mathrm{card}(X)$ can be elementary bounded in $|M|$ and $\textsc{size}(S(\overline{c}))$.

Employing Theorem 3 there exists a most general solution σ to $(U^\star, X)$. Furthermore, due to Theorem 4 there exists exists an elementary function g, such that $\mathrm{dr}((U^\star, X)\sigma) \leq g(e, n)$, where $e = \mathrm{dr}((U^\star, X))$ and $n = \mathrm{card}(\{a \mid \mathrm{dp}(a, U) > 0\})$. Due to the just given argument this implies the existence of an elementary function h, such that

$$\mathrm{dr}((U^\star, X)\sigma) \leq h(\mathrm{dr}((U^\star, X)), c, s) \ .$$

To observe the stated term bound it suffices to realise that $\mathrm{dr}((U^\star, X))) \leq \textsc{size}(S(\overline{c}))$.

By Lemma 4 there exists an instantiation σ' of σ that solves U. We may assume that σ' is a ground substitution, otherwise we replace all variables in $\mathrm{rg}(\sigma')$ by $\mathbf{0}$. Finally, using σ' we define a Herbrand sequent of matrix-form T' fulfilling properties (1)—(3). □

The following corollary is (by now) an easy consequence of the theorem.

Corollary 3. *Let Π be an (almost cut-free) proof of $S \Longrightarrow \exists \overline{x} P(x_1, \dots, x_n)$, P quantifier-free, such that $|\Pi| = k$ and $\mathrm{it}(Pi) = l$. Then there exists a number N and a Herbrand disjunction of the form*

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \dots, \mathbf{i}_p) \lor \cdots \lor C_m(\mathbf{i}_1, \dots, \mathbf{i}_p) ,$$

where each $C_i(\mathbf{i}_1, \dots, \mathbf{i}_p)$ is an instance of $P(x_1, \dots, x_n)$, furthermore the following holds.

1. *The length of the 'inner' disjunction $C_1 \lor \cdots \lor C_m$ is $\leq k + 1$.*
2. *The length of the 'outer' disjunction $\bigvee_{i_1} \cdots \bigvee_{i_p}$ is $\leq l$.*
3. *The depth of the reduct of the 'inner' disjunction $C_1 \lor \cdots \lor C_m$ is $\leq f(k, s, d)$, for some elementary function f, where $s = \textsc{size}(S(\overline{c}))$ ($c_i \in FV$) and $d = \mathrm{dp}(S(\overline{c}))$.*

4. Herbrand's Theorem reversed

Let $\exists \overline{x} P(x_1, \dots, x_n)$, P quantifier-free, be a Σ_1-formula, provable (by an almost cut-free proof) in TIND. Due to Theorem 2 we conclude the existence of a disjunction

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \dots, \mathbf{i}_p) \lor \cdots \lor C_m(\mathbf{i}_1, \dots, \mathbf{i}_p) , \tag{7}$$

where each $C_j(\mathbf{i}_1, \dots, \mathbf{i}_p)$ is an instances of $P(x_1, \dots, x_n)$. In this section we study a reversion of Herbrand's Theorem: Given a valid disjunction of the above form, there exists a proof in TIND of the existential statement $\exists x_1, \dots, \exists x_n P(x_1, \dots, x_n)$.

We call disjunctions $D(\mathbf{n})$ with a single parameter $\mathbf{n}$ of form (7) *uniform* if the length m of the matrix $C_1(\mathbf{i}_1, \dots, \mathbf{i}_p) \lor \cdots \lor C_m(\mathbf{i}_1, \dots, \mathbf{i}_p)$ is independent on n. If for any n there exists an N such that an uniform disjunction $D(\mathbf{n})$ is valid, we say that $D(\mathbf{n})$ is *uniformly valid*. Given uniform Herbrand disjunctions, we construct *uniform* proofs, i.e. proofs whose length are independent on the parameter occurring. The construction presented only works, if we admit some mild restrictions on the form of $H(\overline{\mathbf{n}})$, see below. We start with some general reflections.

4.1. Reflections on Herbrand disjunctions

As basis for the reversion of Herbrand's theorem investigated, we study the validity problem for disjunctions of the special form (7). Let D be a valid disjunction of the above form. The next proposition shows that the presence of two 'outer' disjunctions in D is already sufficient to reduce the problem to the general halting problem.

Proposition 7. *For any r.e. set X we can define a disjunction*

$$\bigvee_{i=0}^{N(n)} \bigvee_{j=0}^{N(n)} C(\mathbf{i}, \mathbf{j}, \mathbf{n}) \ ,$$

which is valid for some $N(n)$, (depending on n) iff $n \in X$.

Proof. We assume acquaintance with the theory of 2-register machines, compare [11]. Our proof is closely related to the proof of Theorem 2.1.15, p. 28 [11]. Let M be some arbitrary 2-register machine with instructions $I_i; i = 0, \dots, k$; where k is the total number of instructions. We denote the configurations of the machine M by triples $\langle i, m, n \rangle$. Our first step is to give a particular encoding of a machine M through a disjunction of form (5).

For each state i we assert binary predicate symbols K_i. The set of instructions I_i is represented by a conjunctions of implications, denoted by $\mathrm{STEP}_M(a, b)$. It suffices to describe the implications for each I_i. Assume I_i is an adding instruction $\langle i, r, j \rangle$: *at state i add 1 to register r and goto state j*. If $r = 1$ this is represented by the implication $K_i(c, b) \supset K_j(S(c), b)$. If $r = 2$ then the representation is similar. Now assume I_i is a subtracting instruction $\langle i, r, j, k \rangle$: *at state i subtract 1 from register r if this r is non-empty and goto state k; otherwise goto j*. We denote this case-distinction (for case $r = 1$) by $K_i(S(c), b) \supset K_k(c, b)$ and $K_i(\mathbf{0}, b) \supset K_j(\mathbf{0}, b)$, the other case being similar.

In the second step, we specialise M to a register machine that enumerates the (r.e.) set X: If $n \in X$, M started on input $(n, 0)$ terminates with output $(1, 0)$. The termination of M is equivalent to the fact that

$$K_0(\mathbf{n}, \mathbf{0}) \wedge \bigwedge_{i}^{N} \bigwedge_{j}^{N} \mathrm{STEP}_M(\mathbf{i}, \mathbf{j}, \mathbf{n}) \supset K_1(\mathbf{1}, \mathbf{0}) \ ,$$

is valid for some N. The above implication can be transformed into the form of the disjunction stated in the proposition. □

Hence, we restrict our attention to disjunctions of form (7) with only one 'outer' disjunction. Furthermore, we introduce mild restrictions on the interplay between parameters and other numerals occurring in the disjunction. To denote that N depends on the parameters $\overline{n}$, we write $N(\overline{n})$ instead of N (as we have already done, above). Recall that a valid disjunction H that can be written in the form

$$\bigvee_{i=0}^{N(\overline{n})} C_1(\mathbf{i}, \overline{\mathbf{n}}) \vee \cdots \vee C_m(\mathbf{i}, \overline{\mathbf{n}}) \ , \tag{8}$$

for some $N(\overline{n})$ is called a Herbrand disjunction in matrix-form cf. Definition 18. Its Herbrand matrix can be written as

$$C_1(\mathbf{a}, \overline{\mathbf{n}}) \vee \cdots \vee C_m(\mathbf{a}, \overline{\mathbf{n}}) \ , \tag{9}$$

for some variable $\mathbf{a} \in \mathbf{NV}$. Let D be a disjunction of the form (8). In an abuse of notation we refer to the disjunction (9) as *matrix* of D, even if D is not valid (for some $N(\overline{n})$).

Convention. In the following we will only be concerned with disjunctions of form (8) with a single parameter. The argument below is sufficiently general to be easily extended to the case for an arbitrary number of parameters.

Definition 25. *Let D be a disjunction of the form (8), let M denote its matrix. Furthermore, D contains at most one parameter $\mathbf{n}$. Assume that for any occurrence of an atomic formula A in M the variable $\mathbf{a}$ and the parameter $\mathbf{n}$ do not both occur in A. Then D is called* simple.

Example 1 (continued). Let $D(\mathbf{n})$ denote the simple uniform disjunction defined on page 18. We indicate the occurring parameter $\mathbf{n}$. Then $D(\mathbf{n})$ becomes

$$\bigvee_{i=0}^{n} \left(C(\mathbf{i},\mathbf{0},\mathbf{n}) \vee \cdots \vee C(\mathbf{i}, f^{m-1}(\mathbf{0}),\mathbf{n})\right) \ ,$$

where $C(\mathbf{i},t,\mathbf{n})$ equals

$$\neg P(\mathbf{0},\mathbf{0}) \vee (P(\mathbf{i},t) \wedge \neg P(S(\mathbf{i}),t)) \vee (P(\mathbf{n},t) \wedge \neg P(\mathbf{n},f(t))) \vee P(\mathbf{n},f^{m}(\mathbf{0})) \ .$$

Clearly the disjunction $D(\mathbf{n})$ is valid for all n. □

We define the language $\mathcal{L}(\mathrm{mon})$ as a restriction of $\mathcal{L}$ such that only nullary and unary predicate symbols occur in $\mathcal{L}(\mathrm{mon})$.

Lemma 5. *Let $D(\mathbf{n})$ be a simple uniform disjunction of the form*

$$\bigvee_{i=0}^{N(n)} C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n}) \ .$$

Then there exists a uniform disjunction $E(\mathbf{n}) \in \mathcal{L}(\mathrm{mon})$ in matrix form

$$\bigvee_{i=0}^{N(n)} E_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee E_k(\mathbf{i},\mathbf{n}) \ ,$$

such that $D(\mathbf{n})$ is uniformly valid iff $E(\mathbf{n})$ is uniformly valid.

Proof. Let $M(\mathbf{a},\mathbf{n})$ denote the matrix

$$C_1(\mathbf{a},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{a},\mathbf{n}) \ ,$$

of $D(\mathbf{n})$, where $\mathbf{a} \in \mathbf{NV}$. Let P be an atomic subformula of M. By definition either the variable $\mathbf{a}$ or the parameter $\mathbf{n}$ can occur in P.

We define a transformation of $D(\mathbf{n})$ into a formula in $\mathcal{L}(\mathrm{mon})$. We write c to denote either $\mathbf{a}$ or $\mathbf{n}$. Let $P(c)$ be an atomic subformula of M. Let Q be a new, at most unary predicate constant. We replace P by $Q(c)$. This construction is repeated for all atomic formulas in $M(\mathbf{a},\mathbf{n})$ and the resulting matrix is denoted as $M'(\mathbf{a},\mathbf{n})$. Hence, any atomic formula in M' is either a nullary predicate symbol Q or of the form $Q'(c)$, and M' has the form

$$C_1'(\mathbf{a},\mathbf{n}) \vee \cdots \vee C_m'(\mathbf{a},\mathbf{n}) \ .$$

The transformation of the matrix is sufficient to yield a transformation of $D(\mathbf{n})$ into a disjunction

$$\bigvee_{i=0}^{N(n)} C_1'(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m'(\mathbf{i},\mathbf{n}) \ . \tag{10}$$

To establish the properties of the lemma, we extend (10) by equivalences between atomic subformulas of M'. Replace the parameter $\mathbf{n}$ uniformly by $\mathbf{b}$ in $M(\mathbf{a},\mathbf{n})$, where $\mathbf{b} \in \mathbf{NV}$. The result is denoted as $M(\mathbf{a},\mathbf{b})$. Consider any pair (P,Q) of atomic formulas

$$P = R(t_1,\ldots,t_n) \qquad Q = R(s_1,\ldots,s_n) \ ,$$

in $M(\mathbf{a},\mathbf{b})$, such that P,Q are unifiable with a m.g.u. σ, where in the range of σ only numerals or terms of the form $S^k(\mathbf{a})$, $k \geq 0$ are present. Let the transforms of P and Q (in the above sense) be denoted as P',Q', respectively. Define the equivalence

$$P'\sigma \leftrightarrow Q'\sigma \ .$$

and including it into the set of equivalences A. Note that the only variables from $\mathbf{NV}$ occurring in $P'\sigma \leftrightarrow Q'\sigma$, are $\mathbf{a},\mathbf{b}$; we write A as $A(\mathbf{a},\mathbf{b})$, respectively. This step is repeated for each pair (P,Q) in $M(\mathbf{a},\mathbf{b})$. Finally, specialise the set of equivalences $A(\mathbf{a},\mathbf{b})$ for each parameter $\mathbf{n}$, by replacing $\mathbf{b}$ uniformly by $\mathbf{n}$ if $\mathbf{b}$ has not already been instantiated by σ. The result is written as $A(\mathbf{a})$. To obtain the uniform disjunction $E(\mathbf{n})$ in matrix form

$$\bigvee_{i=0}^{N(n)} E_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee E_k(\mathbf{i},\mathbf{n}) \ ,$$

we rewrite the disjunction $\bigvee_{i=0}^{N(n)}(\bigwedge A(\mathbf{i}) \supset M'(\mathbf{i},\mathbf{n}))$ suitable. ($\bigwedge A(\mathbf{i})$ denotes the conjunction of the equivalences in $A(\mathbf{i})$.)

It remains to verify:

$$D(\mathbf{n}) \text{ is uniformly valid iff } E(\mathbf{n}) \text{ is uniformly valid .}$$

Assume, firstly, $D(\mathbf{n})$ is uniformly valid, fix $\mathbf{n}$. To make sure that $E(\mathbf{n})$ is uniformly valid it suffices to make sure that any identity of subformulas in $D(\mathbf{n})$ is reflected in $E(\mathbf{n})$. This is achieved by the set of equivalences $A(\mathbf{n})$. Now assume $E(\mathbf{n})$ is uniformly valid. It is easy to see how the reversion of the above given transformation is defined, such that any equivalence $P'\sigma \leftrightarrow Q'\sigma$ in $A(\mathbf{n})$ gives rise to identical atomic formulas $P\sigma, Q\sigma$ in the matrix $M(\mathbf{a},\mathbf{n})$ of $D(\mathbf{n})$. Thus the lemma follows. □

Example 1 (continued). Let $D(\mathbf{n})$ be defined as above. We apply Lemma 5 to transform $D(\mathbf{n})$ to a simple disjunction over nullary and unary predicate symbols. It is not difficult to argue that the resulting formula can be represented as follows.

$$\bigvee_{i=0}^{n} (C_0(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_{m-1}(\mathbf{i},\mathbf{n})) \ ,$$

where $C_j(\mathbf{i},\mathbf{n})$ equals

$$\neg Q_0(\mathbf{0}) \vee (Q_{f^j(\mathbf{0})}(\mathbf{i}) \wedge \neg Q_{f^j(\mathbf{0})}(S(\mathbf{i})))\vee$$
$$\vee(Q_{f^j(\mathbf{0})}(\mathbf{n}) \wedge \neg Q_{f^{j+1}(\mathbf{0})}(\mathbf{n})) \vee Q_{f^m(\mathbf{0})}(\mathbf{n}) \ ,$$

and the Q_t for $t \in \{\mathbf{0}, f(\mathbf{0}), \ldots, f^m(\mathbf{0})\}$ denote newly introduced unary predicate constants; the new disjunction is again denoted as $D(\mathbf{n})$. □

Let D be a simple disjunction, as defined above. Due to the lemma we can restrict our attention to simple disjunctions with nullary or unary predicate symbols, only. Sometimes we write $\overline{C}(\mathbf{i},\mathbf{n})$ for the 'inner' disjunction of D

$$C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n}) \ .$$

The next proposition states that the validity problem for simple disjunct remains decidable.

Proposition 8. *Assume a simple disjunction $D(\mathbf{n})$ of form as above. It is decidable whether for all n there exists an N such that $D(\mathbf{n})$ is valid.*

Proof. Let $\mathcal{I}$ denote a first-order structure such that quantifiers in $\mathcal{I}$ are to be interpreted over the set of numerals. Then we can reduce the meta-statement:

"*For all n there exists an N such that $\bigvee_i^N \overline{C}(\mathbf{i},\mathbf{n})$ is valid.*"

to

"*For all $\mathcal{I}$ defined as above $\mathcal{I} \models \forall y \exists x \overline{C}(x,y)$ holds.*"

and vice versa. Replace the introduced monadic predicate constants by monadic predicate variables $\mathbf{Z}_1, \mathbf{Z}_2, \ldots$ Now the meta-statement can be formalised as $\forall \mathbf{Z}_i \forall y \exists x \mathbf{E}(x,y)$. This is a sentence of the monadic second-order theory of $(\omega, succ)$. This theory is, employing Büchi's Theorem, decidable. For a proof of Büchi's Theorem see [11] pp. 316–323. Hence the validity problem is decidable. □

Remark 4. As a corollary to the Proposition we see that the query, whether a disjunction $\bigvee_i^N C_1(\mathbf{i}) \vee \cdots \vee C_m(\mathbf{i})$ is valid for some N, is decidable, too.

Remark 5. The presented decidability result for simple disjunctions does not answer the question whether Proposition 8 holds if we drop the (mild) restriction stated in Definition 25. However, we were not able to answer this problem satisfactorily.

Due to Proposition 8 we can effectively decide whether a simple disjunction is valid, i.e. represents a Herbrand disjunction (of matrix-form). We proceed with our proof of the reversion of Herbrand's theorem. We sketch the proof plan. We introduce the language $\mathcal{L}(\forall\!\!\!\!\forall)$. In $\mathcal{L}(\forall\!\!\!\!\forall)$ we replace the 'usual' first-order quantifiers $\forall, \exists$ by *quantifier on numerals* $\forall\!\!\!\!\forall$ and $\exists\!\!\!\exists$, respectively. (For a formal definition see below.) Let $\mathcal{C}$ denote a suitable defined class of Herbrand disjunction (in matrix-form). It is possible to define a (partial) interpretation of $\mathcal{L}$ in $\mathcal{L}(\forall\!\!\!\!\forall)$, i.e. it is possible to define a class of $\mathcal{L}(\forall\!\!\!\!\forall)$-formulas $\mathcal{C}^{\oplus}$, such that any valid formula $H \in \mathcal{C}$, corresponds to a valid formula $H^{\oplus} \in \mathcal{C}^{\oplus}$. We define an auxiliary system TL, which will be complete for $\mathcal{C}^{\oplus}$. Furthermore, we define a (partial) interpretation of $\mathcal{L}(\forall\!\!\!\!\forall)$ in $\mathcal{L}$. We employ this interpretation to show how a proof in TL can be embedded into TIND.

The employed transformations will be such that the final proof is almost cut-free (see Definition 16). Moreover, uniform Herbrand disjunctions give rise to uniform proofs. This will establish the stated reversion of Herbrand's Theorem.

We cannot prove the stated reversion of Herbrand's theorem, if we consider uniformly valid disjunctions $D(\mathbf{n})$ with more than one 'big' disjunct. Assume we have that for any n, there exists $N(n)$, such that the Herbrand disjunction

$$\bigvee_{i=0}^{N(n)} \bigvee_{j=0}^{N(n)} C(\mathbf{i}, \mathbf{j}, \mathbf{n}) \ ,$$

is valid, where $C(\mathbf{i}, \mathbf{j}, \mathbf{n})$ denotes a disjunction with parameter n. Now assume to the contrary that this suffices to establish uniform TIND proofs of $\exists i \exists j C(i, j, \mathbf{n})$ for all n.

Let W_e be a r.e. set with index e; we can apply Proposition 7. Let $e \in X$ be fixed, then there exists a formula C_e, such that there exists N with $\bigvee_{i=0}^{N} \bigvee_{j=0}^{N} C_e(\mathbf{i}, \mathbf{j}, \mathbf{n})$ valid iff $W_e(n)$ holds. Note that C_e is uniform in n and that C_e only contains the function symbols $0, S$. Let T denote the extension of Peano Arithmetic, formalised as in [24], such that identity axioms and induction schema apply also to the predicates in C_e. From [24] and [9] we conclude for any formula A (over the language of T) the following fact.

$$\exists k \forall n \mathrm{T} \vdash^{k} A(\mathbf{n}) \leftrightarrow \mathrm{T} \vdash \forall x A(x) \ . \tag{11}$$

By assumption and use of (11), $W_e = \mathbb{N}$ implies

$$\mathrm{T} \vdash \forall x \exists i \exists j C_e(i, j, x) \ .$$

On the other hand $W_e \neq \mathbb{N}$ implies the existence of some n such that for all K, $\bigvee_{i=0}^{K} \bigvee_{j=0}^{K} C_e(\mathbf{i}, \mathbf{j}, \mathbf{n})$ is not valid, hence

$$\mathrm{T} \not\vdash \forall x \exists i \exists j C_e(i, j, x) \ ,$$

as $\mathrm{T} \not\vdash \exists i \exists j C_e(i, j, \mathbf{n})$. As a consequence, we obtain $\{e \mid W_e = \mathbb{N}\}$ is r.e., a contradiction.

4.2. The formal system TL

In this section we define the auxiliary formal system TL. The definition of TL, employs ideas from [22]. The system is based on the language $\mathcal{L}(\forall)$. The novel feature of $\mathcal{L}(\forall)$ is the presence of a *numeral quantifiers* $\forall$ and $\exists$. Due to Lemma 5, we can assume that all predicate constants in $\mathcal{L}(\forall)$ are either nullary or monadic. Furthermore, the only function symbols occurring in $\mathcal{L}(\forall)$ are 0 and S. We include truth constants $\top, \bot$ in $\mathcal{L}(\forall)$ and we restrict the logical symbols of $\mathcal{L}(\forall)$ to $\neg$, $\wedge$, and $\forall$. The symbols $\vee$, $\supset$ and $\exists$ are defined in the obvious way. Formulas in $\mathcal{L}(\forall)$ are defined as above.

Let $\mathcal{I}$ denote a first-order structure. Let A be an arbitrary formula in $\mathcal{L}(\forall)$. Let $v_{\mathcal{I}} \colon \mathcal{L}(\forall) \to \{\mathbf{true}, \mathbf{false}\}$ denote the evaluation function of $\mathcal{I}$. With respect to the function and predicate constants, as well as the propositional junctors, $v_{\mathcal{I}}$ is defined as usual; however the interpretation of the quantifiers is altered. We only consider the case of a numeral universal quantifier $\forall$:

$$v_{\mathcal{I}}(\forall \mathbf{x} A(\mathbf{x})) = \mathbf{true} \iff v_{\mathcal{I}}(A(\mathbf{n})) = \mathbf{true} \quad \text{for all } n \ .$$

Definition 26. *We inductively define an operation* $()^{(+1)} \colon \mathcal{L}(\forall) \to \mathcal{L}(\forall)$.

1. *Consider an atomic formula* $A = B(\mathbf{n})$. *Then set* $A^{(+1)}$ *equal to* $B(S(\mathbf{n}))$.
2. *Consider* $A = \neg B$. *Then* $A^{(+1)} := \neg B^{(+1)}$.
3. *Consider* $A = (B \wedge C)$. *Then* $A^{(+1)} := B^{(+1)} \wedge C^{(+1)}$.
4. *Consider* $A = \forall \mathbf{x} B(S^k(\mathbf{x}))$. *Then* $A^{(+1)} := \forall \mathbf{x} B^{(+1)}(S^{k+1}(\mathbf{x}))$.

The definition of the operator $^{(+1)}$ *is canonical extended to multisets of formulas, and sequents, respectively.*

Example 3. Consider the formula $A(\mathbf{n}) = \exists \mathbf{x}(Q_1(\mathbf{n}) \wedge Q_2(\mathbf{x}))$. Then $A(\mathbf{n})^{(+1)}$ becomes $\exists \mathbf{x}\,(Q_1(S(\mathbf{n})) \wedge \neg Q_2(S(\mathbf{x})))$. □

We axiomatise TL as a sequent calculus. The axioms, propositional and structural rules of TL are the axioms, propositional and structural rules, respectively of TIND, cf. Section 2.2. The remaining rules of TL are presented in Table 7.

Note that the rules $\forall$: left and $\forall$: right are not analytic, i.e. the subformula property is violated. It is not difficult to see that the given rules fit into the intended semantics, hence are correct.

4.3. Embedding $\mathcal{L}(\text{mon})$ *in* $\mathcal{L}(\forall)$

Note that due to Lemma 5 we can restrict our attention to simple disjunctions $H(\mathbf{n})$ with nullary or unary predicate symbols only.

Remark 6. Note that the construction presented below also works if H if free of parameters. However, in this case, the resulting proof will be free of (tind)-inference. Thus the presented method is superseded by the usual reversion of Herbrand's theorem for pure logic. cf. [28].

Table 7. The formal system TL

$\forall$: left:	$\dfrac{A(\mathbf{m}), \forall\mathbf{x}A(S^{m+1}(\mathbf{x})), \Gamma \to \Delta}{\forall\mathbf{x}A(S^{m}(\mathbf{x})), \Gamma \to \Delta}$
$\forall$: right:	$\dfrac{\Gamma \to \Delta, A(\mathbf{m}) \quad \Gamma \to \Delta, \forall\mathbf{x}A(S^{m+1}(\mathbf{x}))}{\Gamma \to \Delta, \forall\mathbf{x}A(S^{m}(\mathbf{x}))}$
(nex):	$\dfrac{\Gamma \to \Delta}{\Gamma^{(+1)} \to \Delta^{(+1)}}$
(ind):	$\dfrac{A(c), \Lambda \to A(S(c)) \quad A(\mathbf{n}), \Theta \to B(\mathbf{n})}{A(\mathbf{n}), \Lambda, \Theta \to \forall\mathbf{x}B(\mathbf{x})}$

where the sequent formulas in Λ, Θ can be written as $\forall\mathbf{x}C(\mathbf{x})$ and the *principal* formulas of the inference A, B are quantifier-free.

Definition 27. *Let $\mathcal{L}^{-}$ denote a restriction of $\mathcal{L}(\mathrm{mon})$ where all quantifier symbols have been removed. We define an interpretation $()^{\oplus} \colon \mathcal{L}^{-} \to \mathcal{L}(\forall)$. Let A be a formula in $\mathcal{L}^{-}$. Suppose A can be written as*

$$\bigvee_{i=1}^{N(n)} C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n})\ .$$

Then $A^{\oplus} := \exists\mathbf{x}(\overline{C}(\mathbf{x},\mathbf{n}))$, where $\overline{C}(\mathbf{x},\mathbf{n})$ abbreviates $C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n})$.

Example 4 (continued). Let $D(\mathbf{n})$ be defined as on page 30. Then $D(\mathbf{n})^{\oplus}$ becomes

$$\exists\,\mathbf{x}\,(C_0(\mathbf{x},\mathbf{n}) \vee \cdots \vee C_{m-1}(\mathbf{x},\mathbf{n}))\ ,$$

where $C_j(\mathbf{x},\mathbf{n})$ equals

$$\neg Q_0(\mathbf{0}) \vee (Q_{f^j(\mathbf{0})}(\mathbf{x}) \wedge \neg Q_{f^j(\mathbf{0})}(S(\mathbf{x}))) \vee$$
$$\vee (Q_{f^j(\mathbf{0})}(\mathbf{n}) \wedge \neg Q_{f^{j+1}(\mathbf{0})}(\mathbf{n})) \vee Q_{f^m(\mathbf{0})}(\mathbf{n})\ .$$

□

Definition 28. *Let $\mathcal{C}$ be the set of simple uniform Herbrand disjunctions $H(\mathbf{n})$ (in matrix-form) of form*

$$\bigvee_{i=0}^{N(n)} C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n})\ ,$$

with one parameter n. I.e. for each n, there exists $N(n)$, such that $H(\mathbf{n})$ is valid.

We assume that for any n, there exists an $N(n)$, such that $H(\mathbf{n})$ is valid. Let $\mathcal{I}$ be an arbitrary structure of $\mathcal{L}(\forall)$. Then by definition we have the following:

For all n there exists an N such that $\bigvee_{i=1}^{N} \overline{C}(\mathbf{i}, \mathbf{n})$ is valid $\Rightarrow$
For all n there exists an m such that $v_{\mathcal{I}}(\overline{C}(\mathbf{m}, \mathbf{n})) = \mathbf{true}$ $\iff$
For all n $v_{\mathcal{I}}(\exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{n})) = \mathbf{true}$ $\iff$
$v_{\mathcal{I}}(\forall\, \mathbf{y}\, \exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{y})) = \mathbf{true}$.

As $\mathcal{I}$ was arbitrary, we can conclude that for all structures $\mathcal{I}$ of $\mathcal{L}(\forall)$ $\mathcal{I} \models \forall\, \mathbf{y}\, \exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{y})$ holds.

Example 4 (continued). Using the fact that $D(\mathbf{n})$ is valid for all n. We can rephrase $D(\mathbf{n})$ in $\mathcal{L}(\forall)$ as

$$\forall\, \mathbf{y}\, \exists\, \mathbf{x}\, (C_0(\mathbf{x}, \mathbf{y}) \lor \cdots \lor C_{m-1}(\mathbf{x}, \mathbf{y})) \ ,$$

where $C_j(\mathbf{x}, \mathbf{n})$ equals

$$\neg Q_0(\mathbf{0}) \lor (Q_{f^j(\mathbf{0})}(\mathbf{x}) \land \neg Q_{f^j(\mathbf{0})}(S(\mathbf{x}))) \lor$$
$$\lor (Q_{f^j(\mathbf{0})}(\mathbf{y}) \land \neg Q_{f^{j+1}(\mathbf{0})}(\mathbf{y})) \lor Q_{f^m(\mathbf{0})}(\mathbf{y}) \ .$$

□

Definition 29. *Let $\mathcal{C}^{\oplus}$ be defined as the class of formulas*

$$\forall\, \mathbf{y}\, \exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{y}) \ , \tag{12}$$

representing in $\mathcal{L}(\forall)$ the simple disjunctions in $\mathcal{C}$.

To prove the reversion of Herbrand's theorem, we have to establish completeness of TL. As alluded to on page 31 it suffices to establish completeness of TL for $\mathcal{C}^{\oplus}$. To simplify the completeness proof we make use of the following (technical) lemma.

Lemma 6. *Let $\forall\, \mathbf{y}\, \exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{y}) \in \mathcal{C}^{\oplus}$. Then there are formulas $A_{(i_1,\ldots,i_l)}$*

$$P_{1i_1} \land \forall\, \mathbf{x} P_{2i_2}(\mathbf{x}) \land \cdots \land \forall\, \mathbf{x} P_{qi_q}(\mathbf{x})) \supset (\forall\, \mathbf{y}(P_{q+1i_{q+1}}(\mathbf{y}) \lor \cdots \lor P_{ni_l}(\mathbf{y})) \tag{13}$$

where the P_{i_j} are quantifier-free and contain the indicated variables only; q depends on the particular choice of indices $(i_1, \ldots, i_l)$ and there exits p such that the conjunction

$$\bigwedge_{i_1=1}^{p} \cdots \bigwedge_{i_q=1}^{p} A_{(i_1,\ldots,i_l)} \ , \tag{14}$$

is (in TL*) provable equivalent to $\forall\, \mathbf{y}\, \exists\, \mathbf{x}\overline{C}(\mathbf{x}, \mathbf{y})$.*

Proof. Recall that $\overline{C}(\mathbf{x}, \mathbf{y})$ abbreviates the disjunction

$$C_1(\mathbf{x}, \mathbf{y}) \lor \cdots \lor C_m(\mathbf{x}, \mathbf{y}) \ .$$

In the first step, we transform this disjunction into its disjunctive normal form $D_1 \lor \cdots \lor D_n$ and distribute the existential quantifier over $\lor$. Let $\exists\, \mathbf{x} D_i$ have the form

$$\exists\, \mathbf{x}(A_1 \land A_2(\mathbf{x}) \land \cdots \land A_a(\mathbf{x}) \land B_1(\mathbf{y}) \land \cdots \land B_b(\mathbf{y})) \ ,$$

where A_1 does not contain bound variables. Then the existential quantifier is moved directly in front of the conjunction $A_2(\mathbf{x})\wedge\cdots\wedge A_a(\mathbf{x})$. For the rest of the construction in each D_i the existential part $\exists\,\mathbf{x}(A_2(\mathbf{x})\wedge\cdots\wedge A_a(\mathbf{x}))$ is treated as an atomic statement.

As second step the altered disjunction is transformed into conjunctive normal form and $\forall$ is distributed over $\wedge$. We obtain a conjunction

$$\forall\mathbf{y}E_1\wedge\cdots\wedge\forall\mathbf{y}E_p\ ,$$

which is clearly equivalent to $\forall\,\mathbf{y}\,\exists\,\mathbf{x}\overline{C}(\mathbf{x},\mathbf{y})$. Now consider $\forall\mathbf{y}E_i$ for arbitrary i. It is easy to see that this formula can only have the form

$$\forall\mathbf{y}(F_1\vee F_2\vee\cdots\vee F_q\vee G_{q+1}(\mathbf{y})\vee\cdots\vee G_n(\mathbf{y}))\ ,$$

for some q_0 $(1\le q_0\le n)$. The F_i either have the form $\exists\,\mathbf{x}(A_1(\mathbf{x})\wedge\cdots\wedge A_a(\mathbf{x}))$ or are quantifier-free. Finally, the quantifier $\forall$ is moved inward in front of $G_{q_0+1}(\mathbf{y})\vee\cdots\vee G_n(\mathbf{y})$. To obtain the form described in the lemma, set q appropriately and rewrite disjunctions as implications. □

Due to Lemma 6 for each element of $\mathcal{C}^{\oplus}$ there exists an equivalent conjunction F of the form (14). To simplify notation, we fix a tuple of numbers $(i_1,\ldots,i_l)$ and q and concentrate in the sequel on a single conjunct of F

$$(P_1\wedge\forall\,\mathbf{x}P_2(\mathbf{x})\wedge\cdots\wedge\forall\,\mathbf{x}P_q(\mathbf{x}))\supset(\forall\,\mathbf{y}(P_{q+1}(\mathbf{y})\vee\cdots\vee P_l(\mathbf{y}))\ ,$$

To prove completeness for $\mathcal{C}^{\oplus}$ we need only consider sequents of the form above. At this point in our argumentation we only state the crucial theorem, the proof of it can be found in Appendix D. Set $G(\mathbf{y}):=(P_{q+1}(\mathbf{y})\vee\cdots\vee P_l(\mathbf{y}))$. Note that $G(\mathbf{y})\neq P_j$ for any $j=1,\ldots,q$. Let Π be a proof in TIND. Recall the definition of it(Π), cf. Definition 17. We extend this definition in the obvious way to TL-proofs. Furthermore, we need the following technical definition to express the assertions of the following theorem precisely.

Definition 30. *Let a sequent* $(\Gamma,\Lambda\rightarrow\Delta,\Theta)$ *be given;* Γ *and* Δ *quantifier-free. Then the sequent is said to satisfy property* (Q)*, if*

1. $\Theta=\forall\mathbf{y}G(\mathbf{y}),\forall\mathbf{y}G(S(\mathbf{y}))$.
2. *For all* $A\in\Lambda$*,* A *is either of form* $\forall\,\mathbf{x}P_i(\mathbf{x})$ *or of form* $\forall\mathbf{x}P_i(S(\mathbf{x}))$*;* $i\in\{1,\ldots,q\}$.
3. *If* $\forall\,\mathbf{x}P_i(\mathbf{x})$ *occurs in* Λ*, then* $(\forall\mathbf{x}P_i(S(\mathbf{x})))\in\Lambda$*, holds, and vice versa.*
4. *No formula of form* $\forall\mathbf{y}G(\mathbf{y})$ *occurs (as a subformula) in* Λ.

Theorem 6. *Let* S *be the sequent*

$$P_1,\forall\,\mathbf{x}P_2(\mathbf{x}),\ldots,\forall\,\mathbf{x}P_q(\mathbf{x}))\rightarrow\forall\,\mathbf{y}G(\mathbf{y})\ ,\tag{15}$$

representing a conjunct of the form above. Assume S *is valid. Then the following holds.*

1. *There exists an almost cut-free proof* Π *of* S *in* TL*, such that* it$(\Pi)\le 1$.

2. *Let* Q *denote an (if any) (ind)-rule application in* Π. *Assume* $\Gamma \to \Delta$ *occurs below* Q *in* Π. *Then* $\Gamma \to \Delta$ *satisfies property* (Q).

Remark 7. We hint at a one crucial fact of the given completeness proof. Let Π be as in the theorem and suppose Q denotes an (ind) rule application in Π. It follows from the completeness proof that the principal formulas of Q are disjunctions of (quantifier-free) instances of the formulas P_1, $\forall \mathbf{x} P_2(\mathbf{x})$,..., $\forall \mathbf{x} P_q(\mathbf{x})$). For further details kindly see Appendix D.

Let us summarise the results: Assume a formula $F \in \mathcal{C}^{\oplus}$ can be written as $\forall \mathbf{y} \exists \mathbf{x} \overline{C}(\mathbf{x}, \mathbf{y})$. By assumption this formula is valid in all structures $\mathcal{I}$ of $\mathcal{L}(\forall)$. Due to Lemma 6, $\forall \mathbf{y} \exists \mathbf{x} \overline{C}(\mathbf{x}, \mathbf{y})$ is equivalent to a formula (14) whose conjuncts are all of the form (15). Due to Theorem 6, $\forall \mathbf{y} \exists \mathbf{x} \overline{C}(\mathbf{x}, \mathbf{y})$ is provable in TL. Thus we have established completeness of TL with respect to the class $\mathcal{C}^{\oplus}$.

4.4. Embedding $\mathcal{L}(\forall)$ *in* $\mathcal{L}(\mathrm{mon})$

We proceed with the proof of the reversion of Herbrand's theorem. We define an interpretation $()^{\ominus(\cdot)}$ of $\mathcal{L}(\forall)$ in $\mathcal{L}(\mathrm{mon})$.

Definition 31. *Let* $F \in \mathcal{L}(\forall)$; *let* n *be fixed. We define an interpretation* $()^{\ominus(n)}\colon \mathcal{L}(\forall) \to \mathcal{L}(\mathrm{mon})$ *inductively on subformulas* A *of* F.

1. *Consider* A *is quantifier-free, then set* $A^{\ominus(n)} = A$.
2. *Consider* $A = (\neg B)$. *Then* $A^{\ominus(n)} := \neg B^{\ominus(n)}$.
3. *Consider* $A = (B \wedge C)$. *Then* $A^{\ominus(n)} := (B^{\ominus(n)} \wedge C^{\ominus(n)})$. *Similarly for the other binary junctors.*
4. *Consider* $A = (\forall \mathbf{z} B(S^m(\mathbf{z})))$ *for* m *arbitrary. Assume* A *occurs negatively in* F. *Then* $A^{\ominus(n)} := \forall z B^{\ominus(n)}(S^m(z))$.
5. *Consider* $A = (\forall \mathbf{z} B(S^m(\mathbf{z})))$ *for* m *arbitrary. Assume* A *occurs positively in* F. *Then* $A^{\ominus(n)} := B^{\ominus(n)}(S^m(\mathbf{n}))$.

The definition of the interpretation $^{\ominus(n)}$ is canonical extended to multisets of formulas, and sequents, respectively.

Lemma 7. 1. *Let* $\Gamma(\mathbf{n}) \to \Delta(\mathbf{n})$, Γ, Δ *quantifier-free be a provable sequent in* LK. *Assume* $\mathbf{n}$ *is fully indicated in* Γ, *and* Δ. *Then* $\Gamma(a) \to \Delta(a)$ *is provable in* TIND, *where* a *is some new free variable.*

2. *Let* $A(\mathbf{k}_1, \dots, \mathbf{k}_p), \forall x B_1(x), \dots, \forall x B_q(x) \to C(\mathbf{l}_1, \dots, \mathbf{l}_r)$ *be a provable sequent in* LK, *such that* A, *the* B_i, *and* C *are quantifier-free and all occurring numerals are fully indicated. Then*

$$A(S(\mathbf{k}_1), \dots, S(\mathbf{k}_p)), \forall x B_1(S(x)), \dots, \forall x B_q(S(x)) \to C(S(\mathbf{l}_1), \dots, S(\mathbf{l}_r)) ,$$

is provable too.

Proof. The fact (1) is trivial; fact (2) follows directly from (1) and Gentzen's mid-sequent theorem.

Lemma 8. *Let S be of the form (15). Let Ψ be an almost cut-free* TL*-proof of S, admitting at most one (ind)-inference* Q*, such that the sequents occurring in Ψ below* Q *fulfil property* (Q)*. Then there exists m such that for all $n \geq m$, there exist proofs $\Pi(\mathbf{n})$ in* Tind *of*

$$P_1, \forall x P_2(x), \ldots, \forall x P_q(x) \to G(\mathbf{n}) \ ,$$

such that the $\Pi(\mathbf{n})$ are almost cut-free proofs that admit exactly one (tind) rule, each. Furthermore, for all $n \geq m$ the proofs $\Pi(\mathbf{n})$ have equal length bounded by $O(|\Psi|)$.

Proof. It turns out that the obtained proofs $\Pi(\mathbf{n})$ share the same logical structure. Hence the $\Pi(\mathbf{n})$ (for all $n \geq m$) are called *essentially equal.*

The proof proceeds by induction on $|\Psi|$: Let S be an arbitrary sequent. We show that when Ψ proves S in TL, such that Ψ fulfils the properties expressed, then there exist essential equal Tind-proofs $\Pi(\mathbf{n})$ of $S^{\ominus(n)}$ fulfilling the properties stated. It is then easy to see that the endsequent of these proofs has the form stated in the lemma. We only treat some interesting cases.

Step: $|\Psi| > 1$. We proceed by case-distinction on the form of the last rule Q in Ψ.

- Assume Q is a $\forall$-right rule.

$$\frac{\Sigma \to \Omega, C(\mathbf{k}) \quad \Sigma \to \Omega, \forall \mathbf{y} C(S^{k+1}(\mathbf{y}))}{\Sigma \to \Omega, \forall \mathbf{y} C(S^{k}(\mathbf{y}))}$$

  By (i.h.) exists a number m_0 and essentially equal proofs of $\Sigma^{\ominus(n)} \to \Omega^{\ominus(n)}, C(S^{k+1}(\mathbf{n}))$ for $n \geq m_0$. Thus there exist (essentially equal) proofs of sequents $\Sigma^{\ominus(n)} \to \Omega^{\ominus(n)}, C(S^{k}(\mathbf{n}))$ for $n \geq m_0 + 1$. Setting $m = m_0 + 1$, the assertion follows.
- Let Q be an (ind)-rule. W.l.o.g we assume Q has the following form, where the sequent formulas in Λ can be written as $\forall \mathbf{x} C(\mathbf{x})$.

$$\frac{A(c), \Lambda \to A(S(c)) \quad A(\mathbf{0}) \to C(\mathbf{0})}{A(\mathbf{0}), \Lambda \to \forall\, \mathbf{y} C(\mathbf{y})}$$

  By (i.h.) we conclude the existence of essentially equal proofs $\Psi_1'(\mathbf{n})$ of $A(c), \Lambda^{\ominus(n)} \to A(S(c))$, $n \geq m$, for some m, and a proof Ψ_2' of $A(\mathbf{0}) \to C(\mathbf{0})$, respectively. It is not difficult to see that that these proofs do not admit any (tind)-rules. Thus the sequent $A(\mathbf{0}) \to C(\mathbf{0})$ is a theorem of LK. Exploiting Lemma 7, $A(b) \to C(b)$ (b a free variable) is provable, too. Therefore, the following is a correct proof-fragment in Tind.

$$\dfrac{\dfrac{A(c), \Lambda^{\ominus(n)} \to A(S(c))}{A(\mathbf{0}), \Lambda^{\ominus(n)} \to A(\mathbf{n})} \quad A(\mathbf{n}) \to C(\mathbf{n})}{A(\mathbf{0}), \Lambda^{\ominus(n)} \to C(\mathbf{n})}$$

  This proof fragment is applicable for each parameter $\mathbf{n}$ and the assertion follows.

– Assume Q is a (nex)-rule. We consider two cases (i) the single (ind)-rule occurs below Q; (ii) it occurs above. Firstly we consider (i): Assume Q has the form

$$\frac{\begin{array}{c}\Psi_0\\ \Gamma, \Lambda \to \Delta, \Theta\end{array}}{\Gamma^{(+1)}, \Lambda^{(+1)} \to \Delta^{(+1)}, \Theta^{(+1)}}$$

where Λ, Θ may contain formulas of the form $\forall \mathbf{z} A(\mathbf{z})$.
As (ind) occurs below Q it is safe to assume that Θ is empty. (This follows by an easy induction on $|\Psi_0|$ and the assumptions on Ψ.) By (i.h.) exists an m and for $n \geq m$ we have essentially equal TIND-proofs $\Pi(\mathbf{n})$ of $(\Gamma, \Lambda \to \Delta, \Theta)^{\ominus(n)}$. W.l.o.g. assume that $\Gamma^{\ominus(n)} = A(\mathbf{k}_1, \ldots, \mathbf{k}_p)$, $\Lambda^{\ominus(n)} = \forall x B_1(x), \ldots, \forall x B_q(x)$, and $\Delta^{\ominus(n)} = B(\mathbf{l}_1, \ldots, \mathbf{l}_r)$, such that all occurring numerals are fully indicated; we rewrite the upper sequent as

$$A(\mathbf{k}_1, \ldots, \mathbf{k}_p), \forall x B_1(x), \ldots, \forall x B_q(x) \to C(\mathbf{l}_1, \ldots, \mathbf{l}_r) \ .$$

It follows by Lemma 7 that

$$A(S(\mathbf{k_1}), \ldots, S(\mathbf{k}_p), \forall x B_1(S(x)), \ldots, \forall x B_q(S(x)) \to C(S(\mathbf{l}_1), \ldots, S(\mathbf{l}_r))$$

is derivable. The latter sequent equals $(\Gamma^{(+1)}, \Lambda^{(+1)} \to \Delta^{(+1)})^{\ominus(n)}$.
Now we consider (ii): We assume the premise of Q can be written as

$$A, \forall \mathbf{x} B(\mathbf{x}) \to \forall \mathbf{y} C(\mathbf{y}), \forall \mathbf{y} C(S(\mathbf{y})) \ . \tag{16}$$

This form is sufficiently general, such that the proof of the general case follows from our treatment below. Accordingly, the translation of the premise of Q has the form

$$A, \forall x B(x) \to C(\mathbf{n}), C(S(\mathbf{n})) \ .$$

By (i.h.) this translation of the upper sequent of Q is provable by (essentially equal) proofs $\Pi_0(\mathbf{n})$ ($n \geq m$, for some m). We assume the induction formula in $\Pi_0(\mathbf{n})$ is denoted as $D(\mathbf{n})$. Hence there exists a (tind)-inference in $\Pi_0(\mathbf{n})$ of the form

$$\frac{D(c), \Lambda, \forall x B(x) \to D(S(c))}{D(\mathbf{0}), \Lambda, \forall x B(x) \to D(\mathbf{n})} \ (\mathsf{R})$$

where the sequent formulas in Λ can be written as $\forall \mathbf{x} C(\mathbf{x})$. This together with Lemma 7 implies that $D(S(c)), \Lambda', \forall x B(S(x)) \to D(S^2(c)$, is derivable, Λ' suitably defined. Hence we may replace R by the following inference.

$$\frac{D(S(c)), \Lambda', \forall x B(S(x)) \to \Theta, D(S^2(c))}{D(S(\mathbf{0})), \Lambda', \forall x B(S(x)) \to \Theta, D(S(\mathbf{n}))}$$

It remains to show that all inferences between R and the end-sequent of $\Pi_0(\mathbf{n})$ are valid. This is shown by induction on the length of the path from R to the end-sequent. □

The next lemma follow by utilising the pattern of the proof of Lemma 8. We omit the proof.

Lemma 9. *Assume the assertions of Lemma 8 hold, such that essentially equal, almost cut-free* TIND*-proofs $\Pi(\mathbf{n})$ of*

$$P_1, \forall x P_2(x), \ldots, \forall x P_q(x) \to G(\mathbf{n}) \ ,$$

exists for $n \geq m$, m. If $m > 0$, then for $k \in \{0, \ldots, m-1\}$ there exists almost cut-free proofs $\Phi(\mathbf{k})$ with $|\Phi(\mathbf{k})| \leq O(|\Psi|)$ of

$$P_1, \forall x P_2(x), \ldots, \forall x P_q(x) \to G(\mathbf{k}) \ .$$

The above two lemmas dealt only with the case that the TL-proof Ψ admitted at most one (*ind*)-inference. The following theorem weakens this assumption such that all occurring (*ind*)-inference in Ψ have to occur in parallel.

Theorem 7. *Assume S is defined as above. Assume Ψ is an almost cut-free proof of S such that* $\mathrm{it}(\Psi) \leq 1$*. Then for all $n \geq m$, there exist (essentially equal) proofs $\Pi(\mathbf{n})$ ($|\Pi(\mathbf{n})| \leq O(|\Psi|)$) in* TIND *of*

$$P_1, \forall x P_2(x), \ldots, \forall x P_q(x) \to G(\mathbf{n}) \ .$$

Furthermore, for $k \in \{0, \ldots, m-1\}$ there exists proofs $\Sigma(\mathbf{k})$ ($|\Sigma(\mathbf{k})| \leq O(|\Psi|)$) of

$$P_1, \forall x P_2(x), \ldots, \forall x P_q(x) \to G(\mathbf{k}) \ .$$

The proofs $\Pi(\mathbf{n})$ and $\Sigma(\mathbf{k})$ are almost cut-free and $\mathrm{it}(\Pi(\mathbf{n})), \mathrm{it}(\Sigma(\mathbf{k})) \leq 1$.

Proof. The proof is by main induction on the number of (ind)-inferences in Ψ and side induction on $|\Pi|$. □

Suppose $\forall y \, \exists x \overline{C}(\mathbf{x}, \mathbf{y}) \in \mathcal{C}^{\oplus}$. Then this denotes the representative of a simple Herbrand disjunction $H(\mathbf{n})$, so that $H(\mathbf{n})$ valid for all $\mathbf{n}$. We calculate $\forall y \, \exists x \overline{C}(\mathbf{x}, \mathbf{y})^{\ominus(n)}$:

$$(\forall y \, \exists x \overline{C}(\mathbf{x}, \mathbf{y}))^{\ominus(n)} \equiv \exists x \overline{C}(x, \mathbf{n}) \equiv \exists x (C_1(x, \mathbf{n}) \vee \cdots \vee C_m(x, \mathbf{n})) \ .$$

Theorem 8. *Given a simple Herbrand disjunction over $\mathcal{L}(\mathrm{mon})$, valid for every n*

$$\bigvee_{i=1}^{N} C_1(\mathbf{i}, \mathbf{n}) \vee \cdots \vee C_m(\mathbf{i}, \mathbf{n}) \ .$$

Then there exists k and almost cut-free proofs $\Pi(\mathbf{n})$, with $|\Pi(\mathbf{n})| \leq k$ for all n of

$$\exists x C_1(x, \mathbf{n}) \vee \cdots \vee C_m(x, \mathbf{n}) \ ,$$

such that $\mathrm{it}(\Pi(\mathbf{n})) \leq 1$.

Proof. We use the notation of Lemma 6. An application of Lemma 6 yields that any formula $\forall\mathbf{y}\,\exists\mathbf{x}\overline{C}(\mathbf{x},\mathbf{y})$ in $\mathcal{L}(\forall)$ can be represented as conjunction of implications of the form $A_{(i_1,\dots,i_l)}$:

$$P_{1i_1} \wedge \forall\mathbf{x}P_{2i_2}(\mathbf{x}) \wedge \cdots \wedge \forall\mathbf{x}P_{qi_q}(\mathbf{x})) \supset \forall\mathbf{y}G(\mathbf{y}) \ . \tag{17}$$

By assumption $A_{(i_1,\dots,i_l)}$ is valid in $\mathcal{L}(\forall)$. By Definition 31 its transform for any n into $\mathcal{L}(\mathrm{mon})$ has the form

$$P_{1i_1} \wedge \forall x P_{2i_2}(x) \wedge \cdots \wedge \forall x P_{qi_q}(x) \supset G(\mathbf{n}) \ . \tag{18}$$

Due to Theorem 6 and Theorem 7 the latter is provable in TIND by uniform proofs $\Pi(\mathbf{n})$ for any number n. It remains to combining, for fixed n, the TIND-proofs of the conjuncts in the obvious way. A final application of Lemma 6 (in the reversed direction) yields the theorem. □

Remark 8. If follows from the proof of Lemma 8 that the logical form of sequent-formulas in the TL-proof Ψ is kept in the embedding. Hence, let Q denote a (tind)-rule in one of the proofs $\Pi(\mathbf{n})$. Then note that the principal formulas of Q are disjunctions of (quantifier-free) instances of the formulas P_{1i_1}, $\forall x P_{2i_2}(x)$, …, $\forall x P_{qi_q}(x)$.

Corollary 4. *Given a simple Herbrand disjunction over $\mathcal{L}$, valid for every n*

$$\bigvee_{i=1}^{N} C_1(\mathbf{i},\mathbf{n}) \vee \cdots \vee C_m(\mathbf{i},\mathbf{n}) \ ,$$

Then there exists k and almost cut-free proofs $\Pi(\mathbf{n})$, with $|\Pi(\mathbf{n})| \leq k$ for all $\mathbf{n}$ of

$$\exists x(C_1(x,\mathbf{n}) \vee \cdots \vee C_m(x,\mathbf{n})) \ ,$$

such that $\mathrm{it}(\Pi(n)) \leq 1$, *and vice versa.*

Proof. Direction ⇒: It remains to utilise Lemma 5 in both directions to see that the result of the theorem holds equally well for an unrestricted language.

Direction ⇐: This is a re-statement of Theorem 2. □

5. Conclusion

In Gentzen's second consistency proof of **PA**, in fact generalisations of term-induction rules are employed in the cut-elimination process. To make this precise we refer to the presentation of Gentzen's proof in [28], using for brevity the notation employed there. For each induction rule (ind) in the end-piece of the active proof.

$$\frac{\Gamma, A(c) \rightarrow A(S(c)), \Delta}{\Gamma, A(\mathbf{0}) \rightarrow A(v), \Delta}$$

we can assume that v is closed and can therefore be evaluated to a numeral $\mathbf{n}$. An inessential cut is introduced such that (ind) is transformed to the following rule.

$$\frac{\Gamma, A(c) \rightarrow A(S(c)), \Delta}{\Gamma, A(\mathbf{0}) \rightarrow A(\mathbf{n}), \Delta}$$

Now this inferences is replaced by n cuts to reduce the ordinal assigned.

Further research will provide insight into the structure of the Herbrand disjunctions associated with proofs of existential statements from universal statements employing full successor induction. In the light of Proposition 4 and Proposition 11 in Appendix B, together with its extensions to arbitrary terms, the structure will exhibit iterations of more complex terms than successors and will be based on suitable atomic instances of identity schemes of the form $t = S^n(0) \supset A(t) \supset A(S^n(0))$.

Note that term induction need not be restricted to the form of generation of terms as used for successor induction. It can be generalised to arbitrary *constructor-style* [13] term induction. Furthermore, it is easy to check that the main results presented in this paper remain valid when suitably reformulated to deal with this extension, cf. [23]. With respect to the later, further work will be dedicated towards applications of our results in the area of *inductive theorem proving*, see e.g. [12, 29, 13] and in the area of *automated analysis of proofs*, cf. [6, 5, 7].

Appendix

A. From almost cut-free proofs to general proofs

Let Π be an almost cut-free proof of a sequent S satisfying property (P). In Section 3 we established a characterisation on the possible shape of the Herbrand disjunctions of S. We have already seen how to deal with the restriction on the form of the endsequent S, cf. Proposition 1. In this section we will show that the characterisation of the Herbrand disjunction of S, given previously, does not depend on the fact that Π is almost cut-free.

To this avail, we prove a suitable variant of Parikh's Theorem, cf. [24, 15].

Proposition 9. *If a sequent S has a proof (in* TIND*) of length k then there exists a proof Π of S, $|\Pi| = k$, so that the maximal logical depth of the formulas in Π is bounded by some elementary function $f(c, k)$, where $c = \mathrm{ld}(S)$.*

Before we give the formal proof, we state the main ideas. Let A be formula, depending on (the atomic subformulas of) A we define a *propositional term language* including function constants $f_\neg$, $f_\forall$, $f_\exists$, $f_\wedge$, and $f_\vee$; individual constants $k_1, k_2, \ldots, k_n$, associated to atomic (semi-)formulas in A, and free (propositional) variables $p_1, p_2, \ldots$ We refer to this language as $\mathcal{P}(A)$. Let $B_1, \ldots, B_n$ denote the atomic (semi-)formulas of A. Then, to simplify reading, the constants of $\mathcal{P}(A)$ are sometimes denotes as $k_{B_1}, \ldots, k_{B_n}$. Similar we define the propositional term language $\mathcal{P}(\Pi)$. If A or Π are obvious from context we drop the reference. Furthermore, we introduce a nullary predicate $\top$.

For a given formula F (in Π) we denote its representation in $\mathcal{P}(\Pi)$ by $F^\star$. The idea of the proof is to define a unification problem U over $\mathcal{P}(\Pi)$. The equations in U will reflect the subformula relation between principal and auxiliary formula(s) in Π. This is straight-forward for the propositional inferences. However, as the subformula of $QxA(x)$, $Q \in \{\forall, \exists\}$ is unequal $A(x)$, some care is necessary in the definition of the unification problem with respect to quantifier rules. A similar problem appears with respect to (tind)-rules.

In principle it is possible to use the usual unification procedure to carry on with the proof. See [25] for an argument in this direction. However, we will employ *congruence unification* as defined in Section 3.2. The term-structure of Π is more clearly preserved when reflecting the subformula relations, when using congruence unification than it would be with standard unification. It is simple to adjust congruence unification to the present purpose. It suffices to replace the definition of the 'variant' relation by the following 'formula variants' relations, compare Definition 23.

Definition 32. *Two (semi-)formulas are term variants if their logical structure coincides, i.e. if they can be transformed into each other through replacements of terms.*

Clearly the 'term variant' relation is an equivalence relation. It is easy to see how this equivalence relation on (semi-)formulas is adapted to an equivalence relation on terms in $\mathcal{P}$. Based on Definition 32, congruence unification as defined in Section 3.2 is transformed to congruence unification on $\mathcal{P}$. It is not difficult to argue that all lemmas remain true if the notions are relativised appropriately; in particular Proposition 4 remains correct. Note that due to the different 'variant' relation the meaning of dr(.) is changed, i.e. $\mathrm{dr}((U,X))$ now denotes the maximal logical complexity of the formulas represented in U.

We allow substitution to be applied to sequent proofs: Let Π be a proof, and σ be a substitution such that $\mathrm{dom}(\sigma) \subset \mathbf{V}(\Pi)$. Then $\Pi\sigma$ denotes the proof Π' obtained from Π by uniformly replacing every formula A in Π by $A\sigma$. To make this definition independent on the choice of σ, we assume that $\Pi\sigma := \Pi$, if $\mathrm{dom}(\sigma) \cap \mathbf{V}(\Pi) = \emptyset$. It remains to prove the proposition.

Proof (of Proposition 9). For a given proof Φ, we define a rooted tree T whose vertices are terms in $\mathcal{P}(\Phi)$: Replace all atomic sequent-formulas A in Φ by their associated constants k_A in $\mathcal{P}$. Furthermore, all *occurrences* of sequent-formulas A are replaced by different propositional variables. Suppose the propositional variable p_i replaces the sequent-formula A, then the former is written as p_A.

By induction on the length of Φ we define a congruence unification problem (U,X) over $\mathcal{P}$. We proceed by case analysis on the last inference rule Q in Π concentrating on the case (tind). The other cases are treated similarly and for initial sequent $p_{A^1} \rightarrow p_{A^2}$, add $p_{A^1} = p_{A^2}$ to U. (This step is redundant, if the initial sequent is atomic.) Assume Q has the form

$$\frac{\begin{array}{c}\Pi_0\\ A(c), \Gamma \rightarrow \Delta, A(S(c))\end{array}}{A(0), \Gamma \rightarrow \Delta, A(\mathbf{n})}$$

We distinguish two sub-cases: In the case where A is atomic, set (U,X) equal to the previously constructed unification problem $\langle U_0, X_0\rangle$. Otherwise extend X_0 by the tuple $\langle p_{A(0)}, p_{A(c)}, p_{A(S(c))}, p_{A(\mathbf{n})}\rangle$ and set U equal to U_0. With respect to (the propositional variables associated to) the side formulas in Γ, Δ, add the corresponding equations to (U,X).

Finally, for all sequent formulas A in the end-sequent $\Gamma \rightarrow \Delta$ we add the equations $p_A = A^\star$ to U, where $A^\star$ denotes the representation of A in $\mathcal{P}$. As Π defines a solution to (U,X) the constructed unification problem is solvable. Now we apply Theorem 4 (relativised to $\mathcal{P}$). We assume the notation of the proposition. There exists a most general congruence unifier σ such that $\mathrm{dr}(U\sigma) \leq 2^n d$, where $d = \mathrm{dr}((U,X)))$ and $n = \mathrm{card}(\{a \mid \mathrm{dp}(a,U) > 0\})$. By construction of (U,X) we have $\mathrm{dr}((U,X)) \leq \mathrm{ld}(S)$ and it is not difficult to argue that $n \leq 2k$, $k = |\Phi|$.

To obtain Π we apply σ to T, denoting the result as $T\sigma$. Furthermore, all non-instantiated propositional variables are replaced by $\top$. Clearly this structure is not yet a proof in TIND as it is defined over $\mathcal{P}(\Phi)$. However, it is easy to see how an inverse mapping $\rho\colon \mathcal{P}(\Phi) \to \mathcal{L}$ is defined. Applying ρ to $T\sigma$ we obtain Π. □

The system TIND admits cut-elimination. However, we have to keep trace of the *positions* of the (tind)-inferences. To apply the results of Section 3 the maximal number of *iterations* of (tind)-inferences in the finally obtained almost cut-free proof has to be bounded. We define

$$2^y_0 := y \qquad 2^y_{x+1} := 2^{2^y_x} .$$

The *cut-degree* $\rho(\Pi)$ of a proof Π is defined by induction. Let $\Pi_i, i = 1, 2$ be direct subproofs of Π. Assume the last inference rule in Π is a Cut with cut-formula A. Let $\rho(\Pi) := \max(\mathrm{ld}(A), \rho(\Pi_1), \rho(\Pi_2))$. Otherwise let $\rho(\Pi) := \max(\rho(\Pi_1), \rho(\Pi_2))$.

Proposition 10. *Let Π be a proof in* TIND*; $k := |\Pi|$, $i := \mathrm{it}(\Pi)$. Then we can transform Π to a proof Φ of the same end-sequent S such that Φ admits propositional cuts only. Moreover $|\Phi| < 2^k_{2\rho(\Pi)}$ and $\mathrm{it}(\Pi') \leq 2^i_{\rho(\Pi)-1}$.*

The first step is to transform Π to a proof in which initial sequents are atomic. In [4] an explicit proof transformation to this avail is presented. Moreover an exponential bound on the length of the transformed proof is given. Using the same idea—suitable adapted for our formal system LK—we obtain the following proposition.

Lemma 10. *Let Π be an proof in* TIND *with length k, such that d denotes the maximal logical complexity of an initial sequent in Π. Then there exists a* TIND*-proof Π' such that all initial sequents in Π' are atomic and $|\Pi'| \leq 2^{3d} \cdot k$.*

Proof. The proof almost exactly follows the proof in [4]. Note that our bound is different from the one established in [4]; this mainly due to the fact that the notion of logical complexity employed here is different. □

To show the admissibility of cut-reduction it suffices to investigate a variant of the Reduction Lemma. The theorem then follows by induction on the cut-degree as usual.

Lemma 11. *Let Π_1, Π_2 be derivations of $\Gamma_1 \to \Delta_1, A$; $A, \Gamma_2 \to \Delta_2$, respectively such that $\rho(\Pi_i) \leq \mathrm{ld}(A)$. Then we can find a proof $\Pi^\star$ of $\Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2$ and $|\Pi| < (|\Pi_1| + |\Pi_2| + 1)^2$ such that $\rho(\Pi) < \mathrm{ld}(A)$. Moreover $\mathrm{it}(\Pi) \leq \mathrm{it}(\Pi_1) + \mathrm{it}(\Pi_2)$.*

Proof. The proof follows by taking the pattern from the proof of the corresponding lemma in [14]. □

As a corollary to Proposition 9 and 10 we conclude that Theorem 2 and Theorem 5 remain valid if the (implicit) reference to almost cut-free proofs is dropped. However, it is necessary to recalculate the stated bounds.

Let Π_0 be an arbitrary proof in TIND of an arbitrary sequent S. Let k denote the length of Π_0 and c the maximal complexity of sequent formulas in the endsequent S. Furthermore, assume $l := \mathrm{it}(\Pi_0)$. Due to Proposition 1 we conclude the existence of a sequent S' fulfilling property (P), equivalent to S, and derivable by a proof Π_1, such that $|\Pi_1| \leq O(k) =: k'$ holds. Note that the complexity of formulas in Π_1 cannot increase through this step.

Let $c := \mathrm{ld}(S)$. Applying Proposition 9 we can transform Π_1 to a proof Π_2 of S' such that the complexity of the sequent formulas in Π_2 is bounded by $2^{2k'}c$, while $|\Pi_1| = |\Pi_2|$. Set $d := 2^{2k'}c$. Now, applying Lemma 10 we transform Π_2 to a proof Π_3 featuring only atomic initial sequents, such that $|\Pi_3| \leq 2^{3d} \cdot k'$. Furthermore, the complexity of formulas in Π_3 cannot increase. Finally applying Proposition 10 we conclude the existence of an almost cut-free proof Π of S'. The length of Π is

$$\leq 2^{2^{3d} \cdot k'}_{2^{2k'+1}c} ,$$

where $k' = e \cdot k$ for some constant e. On the other hand the maximal number of iterated (tind)-inferences is

$$\leq 2^{l}_{2^{2k'}c-1} .$$

Thus it is easy to see that the bounds stated in Theorem 2 and Theorem 5 remain correct in general setting if 'elementary' is replaced by 'primitive recursive'.

Theorem 9. *Let Π be a proof of $S = (\rightarrow \exists \overline{x} P(x_1, \ldots, x_n)$, P quantifier-free, such that $|\Pi| = k$ and $\mathrm{it}(Pi) = l$. Then there exists a number N and a Herbrand disjunction of the form*

$$\bigvee_{i_1=0}^{N} \cdots \bigvee_{i_p=0}^{N} C_1(\mathbf{i}_1, \ldots, \mathbf{i}_p) \vee \cdots \vee C_m(\mathbf{i}_1, \ldots, \mathbf{i}_p) ,$$

where each $C_i(\mathbf{i}_1, \ldots, \mathbf{i}_p)$ is an instance of $P(x_1, \ldots, x_n)$ such that all numerals in this instance are fully indicated, furthermore

1. *The length of the 'inner' disjunction $C_1 \vee \cdots \vee C_m$ is bounded primitive recursively in k and $\mathrm{ld}(S)$.*
2. *The length of the 'outer' disjunction $\bigvee_{i_1} \cdots \bigvee_{i_p}$ is bounded primitive recursively in k and the cut-degree of Π. (The degree of Π can in turn be bounded elementarily in k and $\mathrm{ld}(S)$.)*
3. *The depth of the reduct of the 'inner' disjunction $C_1 \vee \cdots \vee C_m$ is $\leq f(k, s, d)$, for some primitive recursive function f, where $s = \mathrm{SIZE}(S(\overline{c}))$ ($c_i \in FV$) and $d = \mathrm{dp}(S(\overline{c}))$.*

We conclude the section with the observation that we cannot prevent the fact that cut-reduction increases the number of iterations of (tind)-inferences. This follows from Proposition 3.

B. Term induction and its strength to manipulate terms

The purpose of this section is to assess the possibilities in the manipulation of terms in TIND, in contrast to theories where the 'full' induction scheme is present. The results in this section are obtained as applications to our result on the term-complexities in Herbrand disjunctions of matrix-form, cf. Corollary 3.

Recall that a sequent $S(n)$ is called uniformly derivable in k-steps—denoted $\vdash^k S$—if there exists uniform proofs $\Pi(n)$ of $S(n)$, such that $|\Pi(n)| \leq k$ for all n. We employ Yukami's trick [30]. (For a detailed analysis of Yukami's trick see [3].)

Theorem 10 (cf. [30]). *Using two instances of the following scheme of identity*

$$t = 0 \supset g(t) = g(0) \ , \tag{19}$$

we can uniformly derive $0^k := \overbrace{0 + (0 + \cdots (0 + 0))}^{k \text{ times } 0} = 0$*, from (i)* $0 + 0 = 0$*, (ii)* $\forall x, y, z\ x = y \land y = z \supset x = z$*, and (iii)* $\forall x, y\ x + y = y \supset x = 0$*.*

Proof. The following equalities can be derived if we employ 2 instances of (19) together with additional instances of the transitivity axiom (ii) and axiom (i).

$$\begin{gathered} 0^n + \overbrace{(0^{n-1} + \cdots + (0^2 + 0))}^{A} = \\ 0^{n-1} + (0^{n-2} + \cdots + (0 + 0)) = \\ \underbrace{0^{n-1} + (0^{n-2} + \cdots + (0^2 + 0))}_{A} \end{gathered}$$

Hence we have derived $0^n + A = A$; we employ axiom (iii) to obtain the desired result. □

Proposition 11. *Using full induction we can derive (19) uniformly from (i)* $\forall x\ S(x) \neq 0$ *and (ii)* $\forall x\ x = x$*.*

This follows from the formal proof given in Table 8 together with a cut with the sequent $\rightarrow 0 = 0 \supset g(0) = g(0)$, which is derivable by axiom (ii). However, in TIND we obtain the following:

Proposition 12. *Assume* $\forall x\ 0{+}x = x$ *and suitable instances of the identity-axioms are present in* Γ *then*

$$\exists k \forall n \text{TIND} \vdash^k \Gamma \rightarrow A(0^n) \ \textit{iff} \ \text{TIND} \vdash \Gamma \rightarrow \forall x A(x)$$

Proof. Let $S(n)$ denote $\Gamma \rightarrow A(0^n)$. We alter the abstraction procedure described in Section 3.3. Instead of leaving the parameter t unchanged, it is replaced by a new free variables c. Apart from this change the definition of the congruence unification problem $(U^\star, X)$ follows the pattern on page 20

Table 8. The restricted identity scheme

$$\dfrac{\dfrac{\to S(c) \neq 0 \qquad \dfrac{S(c) \neq 0 \to S(c) \neq 0}{S(c) \neq 0, c = 0 \supset g(c) = g(0) \to S(c) = 0 \supset g(S(c)) = g(0)}}{a = 0 \supset g(c) = g(0) \to S(c) = 0 \supset g(S(c)) = g(0)}}{0 = 0 \supset g(0) = g(0) \to t = 0 \supset g(t) = g(0)}$$

ff. It is not difficult to argue that the results of Lemma 4, Proposition 6 and Theorem 5 are still valid.

Given short proofs of $S(n)$ for all n, we apply Theorem 9 to conclude the existence of a term $t(a) = \overbrace{(0 + (\cdots (0 + a) \dots))}^{h \text{ times } 0}$; a some free variable such that there exists a Herbrand sequent $T(t(a))$ of $S(t(a))$. Using the validity of $T(t(a))$ we find a proof of $S(t(a))$ in the LK, hence $\textsc{Tind} \vdash \Gamma \to \forall x A(t(a))$. Applying the axiom $\forall x\ 0 + x = x$ and suitable identity axioms the result follows. □

Other properties of full induction, like fast addition and fast compare, prevail for Tind, cf. [26].

Proposition 13. *Assume (i) $\forall x, y\ x = y \supset S(x) = S(y)$, (ii) $\forall x\ x + 0 = x$, (iii) $\forall x, y\ x + S(y) = S(x + y)$, and (iv) $\forall x, y, z\ x = y \wedge y = z \supset x = z$ are present in Γ. Then then there exists a k so that*

$$\textsc{Tind} \vdash^k \Gamma \to \mathbf{l} + \mathbf{m} = \mathbf{n}\ ,$$

iff $n = l + m$, for all l, n, m.

Proof. We use term induction to prove $\mathbf{l} + \mathbf{m} = \mathbf{n}$ uniformly for all $n = l + m$. We argue informally in Tind. The base case follows using $\forall x\ x + 0 = x$; as we obtain $\forall x\ x + 0 = x \to \mathbf{l} + 0 = \mathbf{l}$ in 2 steps. For the step case: $\mathbf{l} + c = S^l(c) \to \mathbf{l} + S(c) = S^l(S(c))$, we use the axioms (i), (iii), (iv) for a uniform proof. The result follows by a single application of (tind) and a final cut inference with $(ii) \to \mathbf{l} + 0 = \mathbf{l}$. □

Remark 9. We can achieve a (logically) equivalent result by assuming an extension of Tind such that the sequents $\to P(a, 0, a)$ and $P(a, b, c) \to P(a, S(b), S(c))$ are (uniformly) provable, compare [24]. Then we see more clearly that identity schema applied in the above proof and the presence of a function symbol for addition are inessential for the argument.

Proposition 14. *Assume Γ includes the axioms (i)—(iv) from above, together with $\forall x\ S(x) \neq 0$ and $\forall xy\ S(x) = S(y) \supset x = y$. Then there exists a k, such that*

$$\textsc{Tind} \vdash^k \Gamma \to \mathbf{m} \neq \mathbf{n}\ ,$$

iff $m \neq n$, for all m, n.

Proof. Using (tind) (on the second operand $\mathbf{n}$) $\forall x\, S(x) \neq 0$, and $\forall x, y\, S(x) = S(y) \supset x = y$ we can prove the sequent $\mathbf{m} + \mathbf{n} = \mathbf{n} \rightarrow \mathbf{m} = 0$ in a fixed number of steps for all m, n. (The base case is trivial, and the step case $\mathbf{m} + c = c \supset \mathbf{m} = 0 \rightarrow \mathbf{m} + S(c) = S(c) \supset \mathbf{m} = 0$ follows by elementary transformations from $S(\mathbf{m} + c) = S(c) \rightarrow \mathbf{m} + c = c$.)

The proposition then follows from contraposition, another application of $\forall x S(x) \neq 0$ together with Proposition 13. □

Consider the following property **KC**:

$$\exists k \forall n (\mathrm{T} \vdash^k A(\mathbf{n})) \leftrightarrow \mathrm{T} \vdash \forall x A(x) \ ,$$

for some formal system T. This property is sometimes called *Kreisel's conjecture.* **KC** holds for finitely axiomatised number-theories T strong enough to prove $\forall x(x = 0 \vee x = S(0) \vee \cdots \vee x = S^{m-1}(0) \vee \exists y(x = S^m(y)))$, that is

$$\mathrm{LK} \vdash^k \Gamma \rightarrow A(\mathbf{n}) \leftrightarrow \mathrm{LK} \vdash \Gamma \rightarrow \forall x A(x) \ ,$$

where Γ includes all axioms of T.

The latter result does not hold for TIND. Suppose T is a weak finitely axiomatised number-theory admitting the above requirement, but not strong enough to prove induction. We consider the proof in Table 3; let $S(\mathbf{n})$ denote the endsequent. Hence we have $\mathrm{TIND} \vdash^5 S(\mathbf{n})$ for all n and thus the left hand side holds. Clearly the sequent $\forall x(P(x) \supset P(S(x))), P(0) \rightarrow \forall x P(x)$ is not derivable in T, hence in the above formulation **KC** doesn't hold for TIND.

It is an interesting corollary of our results on Herbrand disjunctions that this property becomes true, if we replace the numerals $S^n(0)$ in the formulation of the property by 1^n, where

$$1^n := \overbrace{1 + (1 + \cdots (1 + 1))}^{n \text{ times } 1} \ .$$

The following proposition follows similarly as Proposition 12.

Proposition 15. *Assume that Γ contains axioms sufficiently strong to derive in* TIND.

$$\Gamma \rightarrow \forall x(x = 1 \vee x = 1^2 \vee x = 1^3 \cdots \vee x = 1^n \vee \exists y\ x = \overbrace{(1 + (\cdots (1 + y) \ldots)))}^{n+1 \textit{ times } 1} \ .$$

Then $\exists k \forall n\ \mathrm{TIND} \vdash^k \Gamma \rightarrow A(1^n)$ *iff* $\mathrm{TIND} \vdash \Gamma \rightarrow \forall x A(x)$

A standard disprove of Kreisel's conjecture (within an arbitrary system T) would be to show that fast multiplication, i.e. uniform derivability of multiplication in some fixed number of steps for all numerals, is possible: Assume the uniform derivability of multiplication and take polynomials p, q in $+$ and $\times$ such that $A(\mathbf{n})$ defined by $\exists \overline{x} p(\overline{x}, \mathbf{n}) = q(\overline{x}, \mathbf{n})$ is true for all $n \in \mathbb{N}$, but $\forall x A(x)$ is not provable in T, cf. [8].

This motivates the question whether it is possible to give uniform proofs for multiplication in TIND. However, we can establish the following negative result.

Theorem 11. *No formula $M(\mathbf{n},\mathbf{m},\mathbf{l})$ can exist such that there exists k and*

$$\textsc{Tind} \vdash^k M(\mathbf{n},\mathbf{m},\mathbf{l})\ ,$$

iff $l = n \cdot m$, for all n, m, l.

We will not prove this theorem, a complete presentation of the argument is given in [23]. Let a sequent S, satisfying property (P) with parameters $c_1, \dots, c_n$ be given. Then the set of term-tuples $(\mathbf{m}_1, \dots, \mathbf{m}_n)$ such that $S(\mathbf{m}_1, \dots, \mathbf{m}_n)$ is provable in Tind with some partial proof description Σ (e.g. its proof skeleton) is called *solution set* of S (relative to Σ). The key idea is to characterise the solution sets $\mathrm{X}(\Sigma, S)$ based on a suitable partial proof description Σ and an endsequent S.

C. Congruence Unification

Recall the definition of a *congruence unification problem*, (U, X), cf. Definition 22. As the partition X induces an (uniquely defined) equivalence relation $\approx$ it is convenient to denote the partition X through the relation $\approx$. Hence Definition 22.2 can be alternatively stated as the property: *If $a \approx b$, then $a\sigma$ and $b\sigma$ are variants.* In the course of (congruence) unification it may become necessary to extend the previous existing partition X; we write $X \oplus \langle a, b \rangle$ (or alternatively $X \oplus a \approx b$) to indicate the extension of X by the pair $\langle a, b \rangle$. Let $\overline{s} = s_1, \dots, s_n$ and $\overline{t} = t_1, \dots, t_n$; we write $\overline{s} = \overline{t}$ to denote $s_1 = t_1, \dots, s_n = t_n$. If $\overline{a} = a_1, \dots, a_n$ and $\overline{b} = b_1, \dots, b_n$, then we write $\overline{a} \approx \overline{b}$ to denote $a_1 \approx b_1, \dots, a_n \approx b_n$. If no confusion can arise, we sometimes drop the 'congruence' and simply speak of an unification problem.

To define the unification procedure for congruence unification, we employ the usual rule-set for standard unification, cf. [1] and extend this set of rules by a *Partition* rule. The only changes needed in the definition of the standard unification rules, are that we mark considered equations instead of deleting them and variable renamings are applied to the partition X, too. The purpose of the partition rule is to assert that the *congruence unification property*, cf. Definition 2 is fulfilled.

To simplify the definition of the unification rule *Partition* we extend the definition of 'variant', cf. Definition 21 as the earlier given definition is too restrictive to obtain a suitable unification step.

Definition 33. *Two expressions s, t are* extended variants *if $s^\circ = t^\circ\rho$, for some renaming substitution $\rho \colon \mathbf{V} \to \mathbf{V}$.*

Definition 34. *The* congruence unification procedure *is defined as the extension of the rule-set for standard unification by the rule Partition, as defined in Table 9.*

We indicate why the second case in Partition is essential: Consider the trivial example $(\{a = c\}, \langle a, b \rangle)$ such that $a, b, c \in \mathbf{V}$. This example shows

Table 9. Partition

Consider an equation $a = s$, such that $s \equiv f(s_1, \dots, s_n)$, f a function symbol and the pair $a \approx b$ is unmarked.

$$(a = s \wedge U, a \approx b \oplus X) \longrightarrow (a = s \wedge b = t \wedge U, a \approx b \oplus \overline{a} \approx \overline{b} \oplus X) \ ,$$

where $a, b \in \mathbf{V}$, $a \notin \mathbf{V}(s)$ and s and t are extended variants. Further, s can be written as $e(a_1, \dots, a_k)$ and $t = e'(b_1, \dots, b_k)$, respectively; $\overline{a} = a_1, \dots, a_k$, $\overline{b} = b_1, \dots, b_k$. The pair $a \approx b$ is marked.

Consider an unmarked pair $a \approx b$, such that no equation $a = t$ nor $b = t$ for some term t, $t \notin \mathbf{V}$ exists in U.

$$(U, a \approx b \oplus X) \longrightarrow (a = \mathbf{n} \wedge b = \mathbf{m} \wedge U, a \approx b \oplus X) \ ,$$

where $a \in \mathbf{V}$. The pair $a \approx b$ is marked.

that the procedure would not be complete. The only possible unification steps would be Application resulting in $(\emptyset, \langle b, c \rangle)$; i.e. an empty unification problem together with the partition $\langle b, c \rangle$. Then the unification is trivially solved by the empty substitution, but property 22.2 is not fulfilled.

Remark 10. Let (U, X) be a congruence unification problem. Note that due to Definition 21 a term s has infinitely many variants t. Hence (U, X) in principle has infinitely many solution. This is reflected in the non-deterministic nature of the rule Partition.

Congruence unification has similar properties as standard unification. We restate the central propositions.

Theorem 3. *Let (U, X) be a congruence unification problem. Then there exists a (not necessarily finite) set of most general congruence unifiers of (U, X) iff (U, X) is solvable. Let the set of most general solutions of (U, X) be denoted as* $\mathrm{Sol}((U, X))$. *Then its reduct* $(\mathrm{Sol}((U, X)))^\circ$ *is finite.*

Proof. The proof of correctness proceeds by induction on the number of applications of standard unification rules an the rule *Partition*, cf. Table 9. To establish completeness on proceeds as follows. Let (U, X) be a solvable congruence unification problem. Given a particular solution δ to (U, X), one shows how to obtain a more general solution through the procedure defined. These proofs are standard. □

Let e be an expression; recall the definition of $\mathrm{dr}(e)$, on page 22; (U_0, X_0) be a congruence unification problem with solution σ and $\{a_1, \dots, a_n\}$ denotes the set of variables in U_0. In the remainder of this section we prove the existence of an elementary function f, such that $\mathrm{dr}((U_0, X_0)\sigma) \leq f(d, n)$, where $d = \mathrm{dr}((U_0, X_0))$. We denote the unification problem after some applications of the standard unification rules and the rules in Table 9 as (U, X). The property will follow, if we prove that any unification step on (U, X) can only increase the term depth, if at the same time one of the variables in $\{a_1, \dots, a_n\}$ is eliminated. An obstacle in the proof is that through Partition steps new variables c with $\mathrm{dp}(c, U) > 1$ are introduced. Variables introduced in Partition steps—thus not present in (U_0, X_0)—are called *auxiliary variables.* We gather some observations on auxiliary variables; these are easily proven by induction on the number of unification steps.

Lemma 12. *Let e be an expression, we write $\mathrm{occ}(e, U)$ to denote the number of distinct occurrences of e in U. Let $c \in X$ be a auxiliary variable. Then either there either exists an equation $(c = t) \in U$ or $\mathrm{occ}(c, U) = 1$.*

The property implies that an auxiliary variable c, s.t. $\mathrm{occ}(c, U) > 1$ can always be eliminated by the Application rule. Let t be a term. If for any auxiliary variable $c \in \mathbf{V}(t)$, we have $\mathrm{occ}(c, U) = 1$, then t is called *almost free* of auxiliary variables.

Lemma 13. *For any $c \in X$, c auxiliary, there exists an equation $(d = t) \in U$ such that t is almost free of auxiliary variables and $c \approx d$ holds.*

Definition 35. *Let (U, X) be a defined as above. We assume (U, X) is solvable; let $t \in U$. A term $v \in U$ is called principal term of t, if v is almost free of auxiliary variables and if for any solution σ of (U, X), $v\sigma$ is a variant of $t\sigma$.*

Lemma 14. *Let (U, X) be a defined as above. We assume (U, X) is solvable; assume c is an auxiliary variable. Let $t(c)$ be a term in U such that $t(c) \not\equiv c$. Then either $\mathrm{occ}(c, U) = 1$, or it holds that*

1. *There exists a principal term v of $t(c)$.*
2. *Let v be a principal term of $t(c)$; let p be the position, such that $t(c)/_p = c$. If $(c = r) \in U$ holds, then $v/_p$ is a principal term of r and there exists a substitution ζ, such that $r\zeta = v/_p$.*

Now we are in the position to prove the main result of this section.

Theorem 4. *Let $\sigma \in \mathrm{Sol}((U, X))$. There exists an elementary function f, such that $\mathrm{dr}(U\sigma) \leq f(d, n)$, where $d = \mathrm{dr}(U))$ and $n = card(\{a \mid \mathrm{dp}(a, U) > 0\})$.*

Proof. Assume the current unification problem is denoted as (U, X), and the initial one by (U_0, X_0). Let $\{a_1, \dots, a_n\}$ denote the set $\{a \in \mathbf{V} \mid \mathrm{dp}(a, U_0) > 0\}$. To prove the lemma, we show that $\mathrm{dr}(U\sigma) \leq 2^n \mathrm{dr}(U)$.

The proof is by induction on the number of unification steps. Consider an arbitrary unification step Q applied to (U, X). Let (U', X') denote the congruence unification problem after Q is applied. Obviously $\mathrm{dr}(U') > \mathrm{dr}(U)$ can only be true, if Q is the rule Application

$$(a = t \wedge U, X) \longrightarrow (a = t \wedge U\{a \mapsto t\}, X) ,$$

where $a \in \mathbf{V}$. We have to verify that an Application step can only increase the term depth iff $a \equiv a_i$; $a_i \in \{a_1, \dots, a_n\}$. We consider only the critical case where a is an auxiliary variable. We assume $\mathrm{occ}(a, U) > 1$. As a corollary to Lemma 14 we see that $\mathrm{dr}(U') = \mathrm{dr}(U)$. Let $g(a) \in U$. There are two cases, either $g(a) = S^k(a)$ and t is a numeral, then

$$\mathrm{dr}(g(a)\{a \mapsto t\}) \leq \mathrm{dr}(U) ,$$

follows trivially. Otherwise, due to Lemma 14.2, there exists a term v, v free of auxiliary variables, such that if p denotes the position of a in $g(a)$, then $v/_p$ is principal term of t. Hence, $\mathrm{dp}(a, g(a)) + \mathrm{dr}(t) \leq \mathrm{dr}(v)$. This in turn implies

$$\mathrm{dr}(g(a)\{a \mapsto t\}) \leq \mathrm{dp}(a, g(a)) + \mathrm{dr}(t) \leq \mathrm{dr}(U) .$$

Thus the assertion follows. □

Remark 11. To establish the lemma, we have given an exponential upper bound. Admittingly this bound is not optimal. However, for the results presented it is not necessary to establish an optimal term bound, but to establish a *uniform* bound on the increase of term depth through (congruence) unification.

D. Completeness for the generation of induction

In the completeness proof we follow Kröger completeness proof of the temporal logic TL [22]. Kröger applies Schütte's method cf. [27,28].

The first step is to construct a reduction tree for an arbitrary sequent S in TL by reading backwards the propositional rules of TIND together with the $\forall$: left and $\forall$: right rules. It may happen that a reduced sequent formula gives rise to a new sequent formula, which is a term variant of the original one. Then no further reduction is allowed. At this stage one is not concerned with the rule (nex).

The *reduction tree* $(\textsc{Red}(S), \leq_{\textsc{Red}(S)}, L)$ of a sequent S is a labelled tree whose labels are sequents. We denote the reduction tree by RED(S). The root of RED(S) is labelled by S.

Proposition 16. *Let S be a sequent.*

1. *If S is provable, then every sequent $L(u)$, $u \in \textsc{Red}(S)$ is provable.*
2. *If S is unprovable, then there is a path P (in RED(S)), such that for all $u \in P$, $L(u)$ is unprovable.*

Proof. The proof proceeds as the proof of the related Proposition 8.13 in [28], page 54. □

A leaf $u \in \textsc{Red}(S)$ is called *open* if no formula A occurs on both sides in $L(u)$; $L(u)$ is called an *open sequent*. It follows by the above proposition that for any unprovable sequent S, its reduction tree $\textsc{Red}(S)$ contains at least one open sequent.

Example 4. Let S in $\mathcal{L}(\forall)$ be defined as

$$P(\mathbf{0}), \forall\mathbf{x}(P(\mathbf{x}) \supset P(S(\mathbf{x}))) \to \forall\mathbf{y}P(\mathbf{y}) \ ,$$

Set $\Gamma = P(\mathbf{0}), \forall\mathbf{x}(P(\mathbf{x}) \supset P(S(\mathbf{x})))$ and $\Delta = \forall\mathbf{y}P(\mathbf{y})$. The (significant part of the) reduction tree $\textsc{Red}(S)$ of sequent S is given in Table 10. Only one of the three leaves is open, the sequent V:

$$\begin{gathered} P(\mathbf{0}), P(S(\mathbf{0})), P(\mathbf{0}) \supset P(S(\mathbf{0})), \forall\mathbf{x}(P(\mathbf{x}) \supset P(S(\mathbf{x})), \\ \forall\mathbf{x}(P(S(\mathbf{x})) \supset P(S^2(\mathbf{x}))) \to \forall\mathbf{y}P(\mathbf{y}), \forall\mathbf{y}P(S(\mathbf{y}) \ . \end{gathered}$$

□

Table 10. The reduction tree for S

$$\dfrac{\Gamma \to P(\mathbf{0}) \qquad \dfrac{\dfrac{B, C, \Gamma \to \Delta, A, P(\mathbf{0}) \qquad P(S(\mathbf{0})), B, C, \Gamma \to \Delta, A}{P(\mathbf{0}) \supset P(S(\mathbf{0})), \forall\mathbf{x}P(S(\mathbf{x})) \supset P(S^2(\mathbf{x})), \Gamma \to \Delta, A}}{\Gamma \to \Delta, \forall\mathbf{y}P(S(\mathbf{y}))}}{\Gamma \to \Delta}$$

such that $A := \forall\mathbf{y}P(S(\mathbf{y}))$, $B := P(\mathbf{0}) \supset P(S(\mathbf{0}))$, $C := \forall\mathbf{x}P(S(\mathbf{x})) \supset P(S^2(\mathbf{x}))$. Finally $V = P(S(\mathbf{0})), B, C, \Gamma \to \Delta, A$.

Definition 36. *We inductively define an operation* $()^{(-1)} \colon \mathcal{L}(\forall) \to \mathcal{L}(\forall)$.

1. *Consider an atomic formula A that can be written as $B(S(\mathbf{n}))$, such that $S(\mathbf{n})$ is fully indicated in A. Then $A^{(-1)} := B(\mathbf{n})$. If A cannot be represented in the indicated form, then $A^{(-1)}$ is undefined.*
2. *Consider $A = \neg B$. Then $A^{(-1)} := \neg B^{(-1)}$.*
3. *Consider $A = (B \wedge C)$. Then $A^{(-1)} := B^{(-1)} \wedge C^{(-1)}$. Similarly for all other binary junctors.*
4. *Consider $A = \forall\mathbf{x}B(S^{k+1}(\mathbf{x}))$. Then $A^{(-1)} := \forall\mathbf{x}B^{(-1)}(S^k(\mathbf{x}))$.*

Let Γ be a multiset of sequent formulas. Let $\sigma(\Gamma)$ denote the multiset

$$\{A^{(-1)} \mid A \in \Gamma \text{ and } A^{(-1)} \text{ is defined}\} \ .$$

For a sequent $S = (\Gamma \to \Delta)$, $\sigma(S)$ is defined as $\sigma(\Gamma) \to \sigma(\Delta)$; if both $\sigma(\Gamma)$ and $\sigma(\Delta)$ are empty, then $\sigma(S)$ is the empty sequent. Let $\widehat{S}$ denote the standard interpretation of S, cf. Section 2.2; we define $\sigma(\widehat{S}) := \widehat{\sigma(S)}$. If $\sigma(S)$ is the empty sequent $\to$, then $\sigma(\widehat{S}) = \bot$.

Example 4 (continued). Let V defined as above. Then $\sigma(V)$ becomes

$$P(\mathbf{0}), \forall \mathbf{x}(P(\mathbf{x}) \supset P(S(\mathbf{x}))) \to \forall \mathbf{y} P(\mathbf{y}) \ ,$$

which happens to be the same formula as the original sequent S. □

Definition 37. *Let T be an open sequent of some (unprovable) sequent S. We define a labelled tree $(\textsc{Succ}(T), \leq_{\textsc{Succ}(T)}, L)$ inductively:*

1. *Let $\widetilde{\textsc{Succ}(T)}$ denote the root of $\textsc{Succ}(T)$. Then $L(\widetilde{\textsc{Succ}(T)}) := T$.*
2. *Assume inductively that $\textsc{Succ}(T)$ has been constructed till node u; assume $L(u) = (\Sigma \to \Lambda) = R$. Construct $\textsc{Red}(\sigma(\Sigma) \to \sigma(\Lambda))$, the reduction tree of $\sigma(R)$. Assume it has n open leaves with labels $R_1, \ldots, R_n$. Then we define an extension of $\textsc{Succ}(T)$ by adding nodes $v_1, \ldots, v_n$ as immediate successors of u. $L(v_i)$ is set equal to R_i.*

The labelled tree $\textsc{Succ}(T)$ is called successor tree of T.

Let S be an unprovable sequent with open sequents $T_1, \ldots, T_n$. Let $\textsc{Succ}(T_i)$ denote the successor trees of the T_i. We can assume that the $\textsc{Succ}(T_i)$ are mutually exclusive. We define a labelled forest $\textsc{Succ}(S) = (\textsc{Succ}(T_1), \ldots, \textsc{Succ}(T_n))$ as the structure

$$(\bigcup \textsc{Succ}(T_i), \bigcup \leq_{\textsc{Succ}(T_i)}, \bigcup L_i) \ .$$

Note that $\textsc{Succ}(S)$ is only well-defined, if there exists at least one open sequent in the reduction tree $\textsc{Red}(S)$. We call $\textsc{Succ}(S)$ the *successor forest* of S.

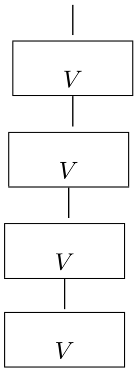
Example 4 (continued). Let S and V be defined as above. Then the successor forest of S is actually a tree, consisting of a single branch, see Table 11. Each box can be thought of as representation of $\textsc{Red}(V)$ in Table 10. □

Definition 38. *Let S be a sequent, and let $u, v \in \textsc{Succ}(S)$. If v is the immediate successor of u in $\textsc{Succ}(S)$ (in the tree-order), then $L(v)$ is called successor of $L(u)$.*

Lemma 15. *Only finitely many different sequents $T_1, \ldots, T_n$ occur as labels in $\textsc{Succ}(S)$.*

Proof. In the following we write $\textsc{Succ}$ instead of $\textsc{Succ}(S)$. Furthermore, we will denote the reduction tree of S—$\textsc{Red}(S)$—as $\textsc{Red}$. We show that the number of different labels in $\textsc{Succ}$ is finite. The construction of $\textsc{Succ}$

Table 11. The successor forest for S



is based on the sequent calculus TL. The only rules that produce new formulas that are not subformulas of S are $\forall$-left and $\forall$-right. In the reduction tree of S, occurrences of $\forall \mathbf{z} A(\mathbf{z})$ in the succedent may be extended by an occurrence of $\forall \mathbf{z} A(S(\mathbf{z}))$ (in the succedent), and occurrences of $\forall \mathbf{z} A(\mathbf{z})$ in the antecedent can be extended by $\forall \mathbf{z} A(S(\mathbf{z}))$ (in the antecedent). Note that by definition of the reduction-tree no further reduction on $\forall \mathbf{z} A(S(\mathbf{z}))$ is possible.

Let u be a node in Succ with label T. Assume $\forall \mathbf{z} A(S(\mathbf{z}))$ occurs in T. By definition the successors of T are the open nodes in Red$(\sigma(T))$. Hence the occurrence of $\forall \mathbf{z} A(S(\mathbf{z}))$ in T causes another occurrence of $\forall \mathbf{z} A(\mathbf{z})$ in Red$(\sigma(T))$. However no formula of the form $\forall \mathbf{z} A(S^m(\mathbf{z}))$, $m > 1$ can occur in Red$(\sigma(T))$.

Proceeding inductively, we see that together with subformulas of S, Succ may contain formulas of the form $\forall \mathbf{z} A(S(\mathbf{z}))$, if $\forall \mathbf{z} A(\mathbf{z})$ is a subformula of S. As only finitely many subformulas of S exists, the number of different nodes is finite, too. □

Recall that it suffices to prove completeness for sequents of the form (13), cf. page 34. We fix a tuple of numbers $(i_1, \dots, i_l)$ and q. We rename the indices and concentrate in the sequel on the following sequent S.

$$P_1, \forall \mathbf{x} P_2(\mathbf{x}), \dots, \forall \mathbf{x} P_q(\mathbf{x})) \rightarrow \forall \mathbf{y}(P_{q_0+1}(\mathbf{y}) \vee \cdots \vee P_l(\mathbf{y}) \,. \qquad (20)$$

We abbreviate the formula in the succedent as $\forall \mathbf{y} G(\mathbf{y})$. As no confusion can arise we will not necessarily distinguish between nodes in labelled trees and the respective labels. Hence, instead of "let $u \in$ Succ(S) and $L(u) = T$" we will shortly write "let $T \in$ Succ". Recall property (Q), defined above, cf. Definition 30, page 35.

Lemma 16. *Let S be of the form* (20)*. Then for any sequent $T \in$ Succ(S), T satisfies property* (Q)*.*

Proof. By induction on the construction of Succ. □

Lemma 17. *Assume $T \in \textsc{Succ}(S)$. Let $T_1, \ldots, T_n$ denote immediate successors of T. Assume T has the form*

$$\Gamma, \Lambda \rightarrow \Delta, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ ,$$

where Γ, Δ are quantifier-free. Assume the T_i can be written as

$$\Gamma_i, \Lambda_i \rightarrow \Delta_i, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ ,$$

with Γ_i,Δ_i quantifier-free. Let $P_i = (\bigwedge \Gamma_i \supset \bigvee \Delta_i)$. Then

$$P_1{}^{(+1)}, \ldots, P_n{}^{(+1)}, \Gamma, \Lambda \rightarrow \Delta \ ,$$

is (cut-free) provable in TL.

Proof. Fix $i \in \{1, \ldots, n\}$. By iterated application of $\wedge$-right ($\Gamma_i \rightarrow \bigwedge \Gamma_i$) becomes derivable. Dually ($\bigvee \Delta_i \rightarrow \Delta_i$) is derivable. Hence

$$\bigwedge \Gamma_i \supset \bigvee \Delta_i, \Gamma_i \rightarrow \Delta_i, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ ,$$

is derivable. As i was arbitrary, this holds for all $i \in \{1, \ldots, n\}$. Taking the structure of $\textsc{Red}(T)$ as pattern

$$P_1, \ldots, P_n, \Gamma', \Lambda' \rightarrow \Delta' \ ,$$

is derivable. A further application of (nex), together with suitable weakenings, then yields

$$P_1{}^{(+1)}, \ldots, P_n{}^{(+1)}, \Gamma, \Lambda \rightarrow \Delta, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ . \tag{21}$$

Note that (21) is cut-free provable. To prove the lemma we fix a proof of (21), denoted as Π. Let $(T(\Pi), \leq_T, L)$ denote the tree-representation of Π. $T(\Pi)$ is transformed to a labelled tree $(T^\star, \leq_T, L^\star)$. For every $u \in T(\Pi)$, if $L(u) = (\Sigma \rightarrow \Omega)$, then set $L^\star(u) = (\Sigma \rightarrow \Omega^\star)$, where $\Omega^\star$ is obtained from Ω by removing all occurrences of $\forall \mathbf{y} G(S^m(\mathbf{x}))$, m arbitrary.

Claim. The sequent-tree $T^\star$ is a proof in TL.

The claim is shown by induction on the length of Π. The base cases follows as property (Q), prevents the critical case of an initial axiom of form $\forall \mathbf{y} G(S^m(\mathbf{x})) \rightarrow \forall \mathbf{y} G(S^m(\mathbf{x}))$. Assume $|\Pi| > 1$: We proceed by a case-distinction on the last inference rule Q applied in Π. Recall that Π is cut-free. We will only present the case where Q is a $\forall$-right rule.

$$\frac{\Sigma \rightarrow \Omega, G(\mathbf{m}) \quad \Sigma \rightarrow \Omega, \forall \mathbf{y} G(S^{m+1}(\mathbf{y}))}{\Sigma \rightarrow \Omega, \forall \mathbf{y} G(S^m(\mathbf{x}))}$$

By (i.h.) $\Sigma \rightarrow \Omega^\star, G(\mathbf{m})$ and $\Sigma \rightarrow \Omega^\star$ are derivable. The latter is equal to $\Sigma \rightarrow (\Omega, \forall \mathbf{y} G(S^m(\mathbf{x}))^\star$. The assertion follows, if we remove Q and the sub-proof above $\Sigma \rightarrow \Omega^\star, G(\mathbf{m})$ from $T^\star$. Thus the claim is established. □

Lemma 18. *Let $T \in \textsc{Succ}(S)$. Assume $\forall \mathbf{z} A(\mathbf{z})$ occurs in the succedent of T and for all $T' \in \textsc{Succ}(T)$, $A(\mathbf{0})$ occurs only in the antecedent of T'. Then T is provable.*

Proof. Due to Lemma 16, we can assume that $\forall \mathbf{z} A(\mathbf{z}) = \forall \mathbf{y} G(\mathbf{y})$, where G as defined above. Hence, T can be written as $\Gamma, \Lambda \to \Delta, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y}))$ where Γ, Δ are quantifier-free. Let $T_1, \dots, T_n$ be the sequents in $\textsc{Succ}(T)$. (Due to Lemma 15 we know that n exists). Again by Lemma 16, the T_i can be written as

$$\Gamma_i, \Lambda_i \to \Delta_i, \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ ,$$

where Γ_i, Δ_i are quantifier-free. Set $A_i :\Leftrightarrow \neg(\bigwedge \Gamma_i \supset \bigvee \Delta_i)$.

Fix $i \in \{1, \dots, n\}$. Let $T_{i_1}, \dots, T_{i_k}$ denote the immediate successors of T_i. Note that by assumption $\Gamma_{i_j} \neq \emptyset$ for all $j \in \{1, \dots, k\}$. Lemma 17 is applicable and for all $i \in \{1, \dots, n\}$

$$\neg A_{i_1}{}^{(+1)}, \dots, \neg A_{i_k}{}^{(+1)}, \Gamma_i, \Lambda_i \to \Delta_i \ ,$$

is provable (cut-free). Thus $\neg A_{i_1}{}^{(+1)}, \dots, \neg A_{i_k}{}^{(+1)}, \Lambda_i \to \bigwedge \Gamma_i \supset \bigvee \Delta_i$ is derivable and by contraposition and the fact $\neg A_i \leftrightarrow (\bigwedge \Gamma_i \supset \bigvee \Delta_i)$ we conclude:

$$A_i, \Lambda_i \to A_{i_1}{}^{(+1)}, \dots, A_{i_k}{}^{(+1)} \ .$$

In the last step, we exploit that $\neg(A^{(+1)}) = (\neg A)^{(+1)}$, for A arbitrary. Set $\overline{\Lambda} = \Lambda_1, \dots, \Lambda_n$. In summary

$$A_1 \vee \cdots \vee A_n, \overline{\Lambda} \to A_1{}^{(+1)} \vee \cdots \vee A_n{}^{(+1)} \ ,$$

holds. By assumption $G(\mathbf{0})$ is in Γ_i for all i. Hence $\neg(\bigwedge \Gamma_i \supset (\bigvee \Delta_i)) \to G(\mathbf{0})$ holds for all i. Therefore

$$A_1 \vee \cdots \vee A_n \to G(\mathbf{0}) \ .$$

As all premises of (ind) are derivable

$$A_1 \vee \cdots \vee A_n, \overline{\Lambda} \to \forall \mathbf{y} G(\mathbf{y}) \ ,$$

is a theorem of TL. Note that for some i it holds that $A_i \leftrightarrow \neg(\bigwedge \Gamma \supset \bigvee \Delta)$. Hence $\Gamma \to \Delta, A_1 \vee \cdots \vee A_n$ is a theorem. Using a cut (on a quantifier-free formula) together with weakenings one derives

$$\Gamma, \overline{\Lambda} \to \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ .$$

It follows from Lemma 16 that the Λ_i denote multisets of sequent formulas of the form $\forall \mathbf{x} P_j(\mathbf{x})$, and $\forall \mathbf{x} P_j(S(\mathbf{x}))$, such that $j \in \{1, \dots, q_0\}$. We claim that $\Lambda_i \subset \Lambda$ for every i. Assume otherwise, then there exists an i and j so that $\forall \mathbf{x} P_j(\mathbf{x})$ occurs in Λ_i but only $\forall \mathbf{x} P_j(S(\mathbf{x})) \in \Lambda$, contradicting Lemma 16. This holds for all Λ_i. Hence $\bigcup \Lambda_i \subset \Lambda$ and we have established an almost cut-free TL-proof of

$$\Gamma, \Lambda \to \forall \mathbf{y} G(\mathbf{y}), \forall \mathbf{y} G(S(\mathbf{y})) \ .$$

□

Note that the proof of the lemma tells us more than the mere fact that T is provable: T is provable by a single application of (ind) such that the principal formulas of this rule applications are disjunctions of quantifier-free A_i, that stem from the quantifier-free part of the sequents in $\textsc{Succ}(T)$. We express this property by the following definition.

Definition 39. *Let $T \in \textsc{Succ}(S)$. Assume $\forall \mathbf{z} A(\mathbf{z})$ occurs in the succedent of T and for all $T' \in \textsc{Succ}(T)$, $A(\mathbf{0})$ occurs only in the antecedent of T'. Then T is said to be provable by a* single loop.

A *path* in $\textsc{Succ}$ is a sequence $(L(u_0), L(u_1), L(u_2), \dots)$ of sequents such that $L(u_0)$ is an open sequent in the reduction-tree of S and for every i $L(u_{i+1})$ is an immediate successor of $L(u_i)$. A path *terminates* in a node v, if $L(v) = T$ does not have a successors, or if $\forall \mathbf{z} A(\mathbf{z})$ occurs in the succedent of $L(v)$ and for all $T' \in \textsc{Succ}(T)$, $A(\mathbf{0})$ occurs only in the antecedent of T'. A path is *closed* if it terminates (in some node).

To show completeness we show that for any unprovable sequent S, there exists a (partial) structure $\mathcal{I}$ such that $\mathcal{I}$ falsifies S. Each non-terminating path $(T_0, T_1, T_2, \dots)$ defines a partial evaluation $v_{\mathcal{I}}$: It suffices to define $v_{\mathcal{I}}$ on sequent formulas in $\bigcup T_i$. We consider only atomic formulas in $\bigcup_i T_i$.

- Assume $P(\mathbf{0})$ is an atomic formula in $T_n = (\Gamma \rightarrow \Delta)$. If $P(\mathbf{0}) \in \Gamma$, then set $v_{\mathcal{I}}(P(\mathbf{n})) = \mathbf{true}$. If otherwise $P(\mathbf{0}) \in \Delta$, then set $v_{\mathcal{I}}(P(\mathbf{n})) = \mathbf{false}$.
- For all atomic formulas $A \in \bigcup T_i$, which are not yet defined, set $v_{\mathcal{I}}(A) = \mathbf{false}$.

The evaluation function $v_{\mathcal{I}}$ is well-defined: If there exists i, such that $P(\mathbf{0})$ occurs in the antecedent and in the succedent of T_i, then the path $(T_0, T_1, \dots)$ would be terminating. This evaluation on atomic formulas is lifted to the level of arbitrary formulas in the usual way. It remains to verify that $\mathcal{I}$ falsifies S. To be able to prove this, we need the following Lemma.

Lemma 19. *Let S and $\mathcal{I}$ be defined as above, and assume S is unprovable. Let $(T_0, T_1, \dots)$ denote an open path in* $\textsc{Succ}$. *Then for $T_0 = (\Gamma \rightarrow \Delta)$ holds: If $A \in \Gamma$, then $v_{\mathcal{I}}(A) = \mathbf{true}$. If $A \in \Delta$, then $v_{\mathcal{I}}(A) = \mathbf{false}$.*

Proof. We prove the lemma by induction on the logical complexity of $A \in T_0$. We consider the interesting case only.

- Assume A can be written as $\forall \mathbf{z} B(\mathbf{z})$. Let A be a sequent formula occurring in the antecedent of T_0. Hence $B(\mathbf{0})$ and $\forall \mathbf{z} B(S(\mathbf{z}))$ occur in the antecedent of T_0, too. Hence $\forall \mathbf{z} B(\mathbf{z})$ occurs in the antecedent of T_1. Iterating the argument yields that $v_{\mathcal{I}}(B(\mathbf{n})) = \mathbf{true}$, for all n. Hence $v_{\mathcal{I}}(\forall \mathbf{z} B(\mathbf{z})) = \mathbf{true}$. On the other hand assume $A \in \Delta$. We have to show that there exists an n, such that $v_{\mathcal{I}}(B(\mathbf{n})) = \mathbf{false}$. This is possible in two cases: Either $B(\mathbf{0})$ occurs in the succedent of T_n or $B(\mathbf{0})$ doesn't occur in T_n at all. Thus we have to exclude the case that for all i, $i \geq 0$, $B(\mathbf{0})$ occurs in the antecedents of T_i, only. However, if this would be the case, then the path $(T_0, T_1, T_2, \dots)$ would terminate in T_0; thus by Lemma 18 by provable. □

Proposition 17. *For any unprovable sequent S of the form (20), there exists a path $(T_0, T_1, T_2, \ldots)$ in* $\textsc{Succ}(S)$ *such that this path defines uniquely a counter-model $\mathcal{I}$ of S.*

We have established the proof of Theorem 6, restated here in a slightly stronger form.

Theorem 6. *Let S be the sequent*

$$P_{1i_1}, \forall \mathbf{x} P_{2i_2}(\mathbf{x}), \ldots, \forall \mathbf{x} P_{qi_q}(\mathbf{x}) \rightarrow \forall \mathbf{y}(P_{q+1 i_{q+1}}(\mathbf{y}) \vee \cdots \vee P_{li_l}(\mathbf{y}))$$

representing a conjunct of the form (13), page 34. Assume S is valid. Then the following holds.

1. *There exists an almost cut-free proof Π of S in* TL, *such that* $\mathrm{it}(\Pi) \leq 1$.
2. *Let* Q *denote the occurrence (if any) of an (ind)-rule in Π. Assume $\Gamma \rightarrow \Delta$ occurs below* Q *in Π. Then $\Gamma \rightarrow \Delta$ satisfies property* (Q).
3. *Suppose $\Gamma \rightarrow \Delta$ denotes the lower-sequent of* Q. *Then $\Gamma \rightarrow \Delta$ is proven by a single loop.*

Proof. Let S be defined as in the proposition. Assume S is unprovable. Due to the theorem this implies the existence of a structure $\mathcal{I}$ that falsifies S. Contradiction. Hence S is provable in TL by a almost cut-free proof Π. Hence its standard interpretation $\widehat{S}$ is provable. By definition of S, $\widehat{S}$ is of the form of the formula (15). This establishes a). Similarly b) follows from the construction of Π. Moreover, the proof of Lemma 18 verifies that any lower-sequent of a (ind)-rule application is provable by a single loop. This establishes c). □

References

1. F. Baader and W. Snyder. *Unification Theory*, volume I, pages 445–532. Elsevier Science Publisher, 2001.
2. M. Baaz. Über den allgemeinen Gehalt von Beweisen. In *Contributions to General Algebra 6*, pages 21–29. Hölder-Pichler-Tempsky, Teubner, 1988.
3. M. Baaz and C. Fermüller. A Note on the Proof-Theoretic Strength of a Single Application of the Schema of Identity. In *Proof Theory in Computer Science, International Seminar, PTCS 2001, Dagstuhl Castle, Germany, October 7-12, 2001, Proceedings*, pages 38–48. Springer Verlag, 2001.
4. M. Baaz and A. Leitsch. On Skolemization and Proof Complexity. *Fund. Informaticae*, 20(4):353–379, 1994.
5. M. Baaz and A. Leitsch. Cut Elimination by Resolution. *J. Symb. Comp.*, 1999.
6. M. Baaz and A. Leitsch. Cut Normal Forms and Proof Complexity. *Ann. Pure Appl. Logic*, 97:127–177, 1999.
7. M. Baaz, A. Leitsch, and G. Moser. System Description: `CutRes 0.1`: Cut Elimination by Resolution. In *Proc. of CADE'99*, pages 212–216, 1999.
8. M. Baaz and P. Pudlák. Kreisel's conjecture for $L\exists_1$. In P. Clote and J. Krajíćek, editors, *Arithmetic, Proof Theory and Computational Complexity*, pages 29–59. Oxford University, 1993. With a postscript by G. Kreisel.
9. M. Baaz and P. Wojtylak. Generalizing Proofs in Monadic Languages. With a postscript by G. Kreisel, submitted to Ann. Pure Appl. Logic, 2001.

10. M. Baaz and R. Zach. Generalizing Theorems in Real Closed Fields. *Ann. Pure Appl. Logic*, 75:3–23, 1995.
11. E. Boerger, E. Graedel, and Y. Gurevich. *The Classical Decision Problem.* Springer-Verlag, 1997.
12. R.S. Boyer and J.S. Moore. *A Computational Logic Handbook.* Academia Press, 1988.
13. A. Bundy. The Automation of Proof by Mathematical Induction. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 13, pages 845–911. Elsevier Science, 2001.
14. S. R. Buss. An Introduction to Proof Theory. In S. R. Buss, editor, *Handbook of Proof Theory*, pages 1–79. Elsevier Science, 1998.
15. W.M. Farmer. *Length of Proofs and Unification Theory.* PhD thesis, University of Wisconsin-Madison, Madison, Wisconsin, 1984.
16. G. Gentzen. Untersuchungen über das logische Schließen I–II. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1934.
17. G. Gentzen. Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie. *Forschungen zur Logik und zur Grundlegung der exakten Wissenschaften*, 4, 1938.
18. H. Gericke. *Mathematik in Antike und Orient.* Springer Verlag, 1984.
19. J. Herbrand. *Jacques Herbrand: Logical Writings.* D. Reidel Publishing Company, Holland, 1971.
20. D. Hilbert and P. Bernays. *Grundlagen der Mathematik 2.* Spinger Verlag, 1970.
21. J. Krajíćek and P. Pudlák. The Number of Proof Lines and the Size of Proofs in First-Order Logic. *Arch. Math. Logic*, 27:69–84, 1988.
22. F. Kröger. *Temporal Logics of Programs.* Springer Verlag, 1985.
23. G. Moser. *Term Induction.* PhD thesis, Vienna University of Technology, June 2001.
24. R.J. Parikh. Some Results on the Length of Proofs. *Trans. Amer. Math. Soc.*, pages 29–36, 1973.
25. P. Pudlak. The Lengths of Proofs. In S. Buss, editor, *Handbook of Proof Theory*, pages 547–639. Elsevier, 1998.
26. D. Richardson. Sets of theorems with short proofs. *J. Symb. Logic*, 39(2):235–242, 1974.
27. K. Schütte. *Proof Theory.* Springer, Berlin and New York, 1977.
28. G. Takeuti. *Proof Theory.* North-Holland, Amsterdam, 2nd edition, 1987.
29. C. Walther. *Mathematical Induction*, volume 12, pages 122–227. Oxford University Press, 1994.
30. T. Yukami. Some Results on Speed-up. *Ann. Japan Assoc. Philos. Sci.*, 6:195–205, 1984.