Generalizing Theorems in Real Closed Fields*

Matthias Baaz[a,1], Richard Zach[b,2]

[a] *Institut für Algebra und Diskrete Mathematik E118.2, Technische Universität Wien, A-1040 Vienna, Austria*
[b] *Group in Logic and the Methodology of Science, University of California at Berkeley, 731 Evans Hall, Berkeley, CA 94720, USA*

Abstract. Jan Krajíček posed the following problem: Is there is a generalization result in the theory of real closed fields of the form: If $A(1+\cdots+1)$ (n occurrences of 1) is provable in length k for all $n \in \omega$, then $(\forall x)A(x)$ is provable? It is argued that the answer to this question depends on the particular formulation of the "theory of real closed fields." Four distinct formulations are investigated with respect to their generalization behavior. It is shown that there is a positive answer to Krajíček's question for (1) the axiom system *RCF* of Artin–Schreier with Gentzen's **LK** as underlying logical calculus, (2) *RCF* with the variant $\mathbf{LK}_{\mathrm{B}}$ of **LK** allowing introduction of several quantifiers of the same type in one step, (3) $\mathbf{LK}_{\mathrm{B}}$ and the first-order schemata corresponding to Dedekind cuts and the supremum principle. A negative answer is given for (4) any system containing the schema of extensionality.

1 Introduction

In [5], Jan Krajíček posed the following problem, inspired by a similar problem for Peano Arithmetic known as *Kreisel's Conjecture:*

23. (Krajíček) For the theory RCF of real closed fields, is there a generalization result of the form: If there exists an integer k for which $\phi(1+\ldots+1)$ (with n occurrences of 1) is provable in k lines, for all $n \in N$, then $\forall x \phi(x)$ is provable?

This and similar problems deal with the concept of *short proofs*, i.e., proofs of theorems in a fixed number of steps, in various circumstances, namely relative to different axiom systems and relative to different formulations of the underlying deductive system for first-order classical logic. Results in the literature indicate that questions about generalizations like the above problem provide a way to distinguish between different proof systems for one and the same theory, i.e., to distinguish between formulations which are indistinguishable by model theoretic properties.

* to appear in *Annals of Pure and Applied Logic*
[1] Corresponding author. Email: baaz@logic.tuwien.ac.at
[2] Email: zach@math.berkeley.edu

For our present purposes, we first consider the usual system of axioms for real closed fields arising from the algebraic analysis of Artin and Schreier [1]. These are quantified equality axioms (not the equality schema), the (purely universal) axioms for ordered fields, plus

$$(\forall x)(\exists y)\big(x = y^2 \vee (-x) = y^2\big) \tag{sqrt}$$

asserting the existence of square roots, and the infinite list of formulas

$$(\forall x_0)\ldots(\forall x_{2n})(\exists y)(x_0 + x_1 y + \cdots + x_{2n} y^{2n} + y^{2n+1} = 0) \tag{zro$_{2n+1}$}$$

asserting the existence of zeroes of every polynomial of odd degree. This system is denoted by RCF, and its open extension by RCF_{op}. The language of RCF contains $=$ and $<$ as predicate symbols, the constants 0, 1, and the function symbols $-$, $^{-1}$ (unary) and $+$, $\cdot$ (binary); the language of RCF_{op} consequently contains in addition the function symbols $\sqrt{|x|}$ (unary), and $h_{2n+1}(x_0, \ldots, x_{2n})$ ($2n+1$-ary). RCF_{op} consists of all instances of the axioms of RCF, in particular of all instances of (sqrt′) and (zro$'_{2n+1}$) below:

$$x = (\sqrt{|x|})^2 \vee (-x) = (\sqrt{|x|})^2 \tag{sqrt′}$$

$$\begin{aligned} &x_0 + x_1 h_{2n+1}(x_0, \ldots, x_{2n}) + \cdots \\ &\quad \cdots + x_{2n} h_{2n+1}(x_0, \ldots, x_{2n})^{2n} + h_{2n+1}(x_0, \ldots, x_{2n})^{2n+1} = 0 \end{aligned} \tag{zro$'_{2n+1}$}$$

We also add all instances of the following equality axioms:

$$\begin{aligned} &x = y \supset \sqrt{|x|} = \sqrt{|y|} \\ &x = y \supset h_{2n+1}(x_0, \ldots, x, \ldots, x_{2n}) = h_{2n+1}(x_0, \ldots, y, \ldots, x_{2n}) \end{aligned}$$

Generalization results are usually investigated for number theories. The principal interest of Krajíček's question lies in the fact that RCF has properties which number theories do not have, viz., it is complete, and it admits elimination of quantifiers. So what can be said about RCF w.r.t. generalization of theorems using only these properties?

One consequence of quantifier elimination for RCF is the following observation: If $A(x_0)$ is true for a *sufficiently large* x_0, then $(\forall x \geq x_0)A(x)$ is true. By quantifier elimination, $A(x)$ is equivalent to a quantifier free $A_0(x)$ which is a disjunction of conjunctions of polynomial equalities and inequalities. For x_0 sufficiently large and the leading coefficient of p_i positive, formulas of the form $p_i(x_0) = 0$ and $p_i(x_0) < 0$ will certainly be false. So at least one disjunct must be of the form $\bigwedge p_j(x) > 0$, where the leading coefficient of every p_j is positive. But if $p_j(x_0) > 0$ holds, then it holds for all $x \geq x_0$. In fact, the first such x_0 can be computed from $A(x)$.

A second observation is the following: Take the open extension RCF_{op}: If $A(t)$ is provable for every variable-free term t (in the extended language), then $(\forall x)A(x)$ is provable. This holds, by completeness, because $(\forall x)A(x)$ is true in the standard model of algebraic numbers.

These two observations put Krajíček's question in perspective: By the second observation, the question would be trivial if instead of the sums of 1's one would ask for *all* terms. So the decisive aspect is which subsets of the set of terms are considered for the generalization problem. A more glaring distinction between terms and their values will be given in the next section, where we show that all infinite sequences of sums of 1's (and even of 0's) generalize, but there are sequences of terms with the values of all (natural) numbers which do not.

We give four answers to Krajíček's question, three positive and one negative: The generalization result holds for

(1) the standard formulation of *RCF* with Gentzen's **LK** as underlying logical system,
(2) *RCF* with the calculus $\mathbf{LK}_{\mathrm{B}}$ (which allows introduction of blocks of quantifiers of the same type in one step, instead of single quantifiers) as underlying logical system,
(3) Dedekind cuts and supremum principles for existentially defined sets and $\mathbf{LK}_{\mathrm{B}}$;

while it fails for

(4) any axiomatization of the real closed fields including the extensionality schema

$$(\forall x)\big(s(x) = s'(x)\big) \supset r\big(s(t_1), \ldots, s(t_n)\big) = r\big(s'(t_1), \ldots, s'(t_n)\big) \qquad \text{(ext)}$$

for r, s, s', and t_i arbitrary terms and $n \in \omega$.

The method used to obtain the results is to reduce the structure of the proofs to their Herbrand disjunctions. In fact, we want to generalize theorems and not proofs per se. One can, however, view the generalization of theorems as a borderline case of generalization of proofs, namely where every sound transformation of a proof is permitted. In a sense then, generalization of theorems has a similar relation to generalization of proofs as model theory has to to proof theory.

2 Calculi, terms, unification

In the course of this paper we shall work with two logical calculi: The first one is Gentzen's [7] sequent calculus for classical logic **LK**. The definition of this system we use is standard. The choice of **LK** over other, in particular, Hilbert-type calculi has no bearing on our results, since **LK** and these systems simulate each other (polynomially in the length of the proof; cf. [6], [7]).

For the definition of **LK** and basic terminology, see [12]. One convention should be explicitly pointed out: Free and bound variables are treated as syntactically distinct. They are denoted by a, b, etc., and x, y, etc., respectively. A *semi-term* may contain bound variables, a *term* contains only free variables. Similarly, a *semi-formula* may contain bound variables only if they are in the scope of a binding quantifier. For instance, $(\forall x)A(x)$ contains the semi-formula $A(x)$

which is not a formula. As might be expected, by $A(a)$ we denote the formula obtained from $A(x)$ by replacing x by a wherever x does not occur in the scope of a binding quantifier. The convention about free and bound variables is often very convenient (e.g., we do not have to worry about terms being substitutable for variables in a formula). When speaking in general terms about substitutions, etc., we will use letters from the end of the alphabet to denote either kind of variable. It will be clear from the context whether x stands for a bound variable or any variable at all. If a definition or a statement applies equally to terms and semi-terms, we drop the prefix "semi."

***LK**-Block* ($\mathbf{LK}_\mathrm{B}$) is the logical calculus obtained from **LK** by replacing the quantifier introduction rules rules by

$$\frac{A(t_1,\ldots,t_n),\Gamma \to \Delta}{(\forall x_1)\ldots(\forall x_r)A(x_1,\ldots,x_n),\Gamma \to \Delta}\ \forall_B\text{: left}$$

and

$$\frac{\Gamma \to \Delta, A(a_1,\ldots,a_n)}{\Gamma \to \Delta,(\forall x_1)\ldots(\forall x_r)A(x_1,\ldots,x_n)}\ \forall_B\text{: right}$$

and similarly for $\exists$. The variables $a_1, \ldots, a_n$ in ($\forall_B$:right) and ($\exists_B$:left) must be distinct and satisfy the eigenvariable condition. The case $n = 0$ is allowed; an actual block quantifier inference with $n = 0$ is called *improper*.

The calculus $\mathbf{LK}_\mathrm{B}$ was introduced in [4], where its k-provability problem was investigated. **LK** and $\mathbf{LK}_\mathrm{B}$ are obviously equivalent in terms of provability; any block quantifier inference can be replaced by a sequence of usual quantifier inferences.

Proofs in **LK** and $\mathbf{LK}_\mathrm{B}$ are upward rooted trees of sequents. We define the *length* $\mathrm{len}(\pi)$ of a proof π (also: its number of steps) as the number of applications of inference rules (of the respective calculus) with the exception of the exchange rule.

Given a set of formulas (a theory) T, we say that T *derives* a formula A, in symbols: $T \vdash A$, if there is a proof (in **LK** or $\mathbf{LK}_\mathrm{B}$) of the sequent $T_0 \to A$ where T_0 is a finite sequence of formulas in T. If we want to emphasize the calculus or that the proof has length $\leq k$ we write it thus: $T \overset{k}{\underset{\mathbf{LK}}{\vdash}} A$. We continue with some definitions about terms and their measures:

Definition 2.1. By $\{s\}^n(t)$ we denote $\underbrace{s+(s+\cdots+(s+(s}_{n \text{ occurrences of } s}+t)\ldots)$; $\{s\}^n$ stands for $\{s\}^{n-1}(s)$. In general, $+$ and $\cdot$ are taken to associate to the right.

Definition 2.2. With any term t we can associate a rooted, labeled tree $T(t)$ as follows:

(1) If $t = c$ or $t = x$ for a constant or variable, then $T(t)$ is the vertex t by itself.
(2) If $t = f(t_1,\ldots,t_n)$, and $T(t_i)$ has the root v_i, then $T(t)$ consists of the vertex f plus the union of $T(t_i)$, $i = 1, \ldots, n$, has root f, and edges from f to v_i.

Every formula A can be considered as a term in the language which has as unary function symbols $\neg$, $(\forall x_i)$, and $(\exists x_i)$ $(i \in \omega)$, as binary function symbols $\wedge$, $\vee$, $\supset$, and as constants the atomic formulas. This language, together with additional propositional variables, is called the *propositional term language*.

Definition 2.3. We say a term s *occurs at depth* d in a term t if there is an occurrence of s in t, and the length of the path from the outermost function symbol of s to the root of t in $T(t)$ is n. For instance, $(1 + x)$ occurs at depth 1 in $1 + (1 + x)$.

The *depth* $\mathrm{dp}(t)$ of a term is the length of the longest path in $T(t)$. The *logical depth* $\mathrm{ld}(A)$ of a formula A is the length of the longest path in $T(A')$ where A' is the term corresponding to A in the propositional term language. The logical depth of a sequent is the maximum logical depth of a formula in it.

Definition 2.4. A *unification problem* U is a set of pairs of terms. The *depth* of U is the maximum depth of a term occurring in it: $\mathrm{dp}(U) = \max\{\mathrm{dp}(s), \mathrm{dp}(t) \mid \langle s, t\rangle \in U\}$. A *solution* for U is a substitution σ s.t. for all $\langle s, t\rangle \in U$ it holds that $s\sigma = t\sigma$; σ is called a *unifier*.

Similarly, a substitution μ is called a *matcher* for $\langle s, t\rangle$, if $s\mu = t$.

If a unifier σ for U has the property that, for every unifier σ' of U, there is a substitution θ s.t. $\sigma' = \theta \circ \sigma$ then σ is called a *most general unifier* for U.

For first-order languages the problem of finding a most general unifier for U is decidable; for the following we will use the algorithm of [9].

Lemma 2.5. *Let U be a unification problem, w the number of variables in U, v_0 the number of variables in U which only occur at depth 0, and $v = w - v_0$. Then $\max \mathrm{dp}(U\sigma) \leq 2^v \max \mathrm{dp}(U)$, where σ is any most general unifier for U.*

Proof. By induction on v: For $v = 0$ the claim follows immediately. So assume $v > 0$. In the first unification step a term s replaces a variable x throughout U, yielding a new unification problem U' with variable counts v' and v'_0.

Case (1): x is a variable occurring only at depth 0. Applying the substitution $s \mapsto x$ does not increase the term depth, since x occurs at depth 0 everywhere. The variable x disappears, and the depths of all other variables remain the same.

Case (2): x does not only occur at depth 0. If s happens to be a variable, the term depth of U' equals the term depth of U. If s occurs only at depth 0, then after replacing x by s, s does also occur at depth > 0 in U', i.e., $v' = v$ and $\mathrm{dp}(U') = \mathrm{dp}(U)$. So assume s is not a variable occurring only at depth 0. We have $v' = v - 1$ and $\mathrm{dp}(U') \leq 2 \cdot \mathrm{dp}(U)$. Let σ' be a most general unifier for U'. By induction hypothesis, $\mathrm{dp}(U'\sigma') \leq 2^{v-1} \mathrm{dp}(U')$. The most general unifier σ of U produced by the algorithm is $\sigma = \sigma' \circ \{s \mapsto x\}$, and $U'\sigma' = U\sigma$. Hence, $\mathrm{dp}(U\sigma) \leq 2^{v-1} 2 \cdot \mathrm{dp}(U) = 2^v \mathrm{dp}(U)$. $\square$

Definition 2.6. A *congruence unification problem* over a propositional term language is a pair $\langle U, C\rangle$ where:

(1) U is a unification problem

(2) C is a set of sets of pairs $\langle p, A\rangle$, where p is a propositional variable, and A is a semi-formula. For every variable p there is exactly one A and X s.t. $\langle p, A\rangle \in X \in C$. Hence, C defines a partition of the variables in classes; the class $[p]_C$ of a variable p is the one set $X \in C$ s.t. $\langle p, A\rangle \in X$.

A substitution σ together with a congruence partition C' is a *congruence unifier* of the problem $\langle U, C\rangle$ if σ is a unifier of U and the following congruence requirement is met:

Assume $\{\langle p, A\rangle, \langle p', A'\rangle\} \subseteq X \in C$ and $\sigma(p) = t(q_1, \ldots, q_n)$. Then $\sigma(p') = t(q'_1, \ldots, q'_n)$ where $\{\langle q_i, B_i\rangle, \langle q'_i, B'_i\rangle\} \subseteq [q_i]_{C'}$, t matches with A and A', i.e., $t\mu = A$ and $t\mu' = A'$, and we have $\mu(q_i) = B_i$ and $\mu'(q'_i) = B'_i$.

To simplify matters, we only consider the case where U does not contain variable-free terms. The congruence unification problems constructed below all have this property.

The congruence unification problem defined above can be solved by an extension of the unification algorithm of Martelli and Montanari, yielding a *most general* congruence unifier. It is only necessary to deal with variable elimination:

Suppose $(p, t) \in U$: If t contains a variable q with $\langle q, B\rangle \in [p]_C$, then stop with failure. This check subsumes the usual "occurs check," i.e., failure if p occurs properly in t. Assume $[p]_C = \{\langle p, A\rangle, \langle p_1, A_1\rangle, \ldots, \langle p_k, A_k\rangle\}$. Let $r_1, \ldots, r_\ell$ be all variables in t in order of occurrence. In order for the congruence requirement to be met, t must match with each of A, A_1, $\ldots$, A_k. So if not, terminate with failure; otherwise, let μ_i be a matcher for t and A_i: $t\mu_i = A_i$.

We introduce $k\ell$ new variables $r_{1i}, \ldots, r_{\ell i}$ $(1 \leq i \leq k)$ and form k variable-disjoint copies $t_1, \ldots, t_k$ of t by: $t_i = t[r_{1i}/r_1, \ldots, r_{\ell i}/r_\ell]$. Now replace (everywhere in U) p by t and p_i by t_i, obtaining U'. We partition the set of variables of the resulting unification problem into C' by (1) marking the class $[p]_C$ as removed and (2) setting $[r_j]_{C'} = [r_j]_C \cup \{\langle r_{ji}, \mu_i(r_j)\rangle \mid 1 \leq i \leq k\}$.

By inspection, the above algorithm has the same termination properties as usual unification, and has the same bound for the depth of terms.

3 *k*-Provability for *RCF* w.r.t. LK reduces to *k*-provability of finite subtheories

The likely interpretation of Krajíček's problem suggests a formulation of the theory of real closed fields in a usual logical inference system, such as Gentzen's sequent calculus **LK**.

An early result of Parikh shows that the logical complexity of formulas in a proof (in **LK**) can be bounded by a function depending on k and the end-sequent. The argument, in modern presentation, uses unification on the skeleton of the proof of, say, $T \to A$. We can extend this result in our setting to show that the logical complexity of formulas in a proof of a formula A in *RCF* can be bounded by a function depending on k and A alone. In particular, any proof of A in k steps need only use a fixed number (depending on k and the logical structure of

A) of axioms (zro_{2n+1}). In effect then, we are working in a finite axiom system. For finite axiom systems, however, the generalization result always holds. In fact, a stronger statement is true: there is always a *finite term basis.*

Definition 3.1. A finite set of n-tuples of terms $B = \{\langle t_1^i, \ldots, t_n^i\rangle\}_{i=1}^m$ is called a *term basis* for $A(x_1, \ldots, x_n)$ and $k \in \omega$ in a theory T if

(1) $T \vdash A(t_1^i, \ldots, t_n^i)$ for $1 \leq i \leq m$,
(2) if $T \stackrel{k}{\vdash} A(s_1, \ldots, s_n)$ (s_j variable free) then there is a substitution σ s.t. for some i ($1 \leq i \leq m$) it holds that $s_j = t_j^i\sigma$ for all j, $1 \leq j \leq n$.

The existence of finite term bases implies a positive solution to Krajíček's problem for *RCF*, as we will see below. First we show how the degree of the axioms (zro_{2n+1}) used in a proof of length k can be bounded (by a function depending on k and the logical complexity of the formula proved). The proof uses congruence unification.

Theorem 3.2. *Assume T is a finite set of formulas containing a true closed formula (e.g., $0 = 0$) and $T' = \{(\mathsf{Q}x_1)\ldots(\mathsf{Q}x_n)A_n \mid n \in I\}$, where $I \subseteq \omega$ is infinite, and the A_n are atomic. Let $T' \upharpoonright m$ denote $\{(\mathsf{Q}x_1)\ldots(\mathsf{Q}x_n)A_n \mid n \in I, n \leq m\}$.*

There is a recursive function ϕ_T s.t. if $T \cup T' \stackrel{k}{\vdash_{LK}} A$ then $T \cup T_0' \stackrel{k}{\vdash_{LK}} A$ where $T_0' = T' \upharpoonright \phi_T(k, \mathrm{ld}(A))$.

Proof. We use an argument similar to Parikh's [10], see also [8]. Let π be an **LK**-proof of length k of the sequent $T, T_1' \rightarrow A$, where $T_1' \subset T'$. We construct a congruence unification problem from π and $T, T_1' \rightarrow A$ as follows:

For every *occurrence* B_i of a semi-formula B in π we have a propositional variable p_{B_i}; a pair in $X \in C$ will always be of the form $\langle p_{B_i}, B\rangle$. For convenience, we define the function $\mathrm{frm}(p_{B_i}) = B$. The congruence partition will be so that $\{\langle p, B\rangle, \langle p', B'\rangle\} \subseteq X \in C$ means that B and B' are equal up to substitution of terms for bound variables.

$\langle U, C\rangle$ is defined as follows: Start by setting $U = \emptyset$ and $C = \big\{\{\langle p_{B_i}, B\rangle\} \mid B_i$ is an occurrence of B *in* $\pi\big\}$.

Recursively traverse the proof tree π from the root upwards. At every inference, add appropriate term pairs to U and extend the partition C:

(1) The inference is a weakening: Proceed.
(2) The inference is an exchange:

$$\frac{\Pi \rightarrow \Lambda, B_{j'}, A_{i'}, \Lambda'}{\Pi \rightarrow \Lambda, A_i, B_j, \Lambda'}$$

Add to U the pairs $(p_{A_i}, p_{A_{i'}})$, $(p_{B_j}, p_{B_{j'}})$ (similarly for left exchange).
(3) The inference is a contraction:

$$\frac{\Pi \rightarrow \Lambda, B_j, B_{j'}}{\Pi \rightarrow \Lambda, B_i}$$

Add to U the pairs (p_{B_i}, p_{B_j}), $(p_{B_i}, p_{B_{j'}})$ (similarly for left contraction).

(4) The inference is a cut:

$$\frac{\Pi \to \Lambda, B_i \quad B_j, \Pi' \to \Lambda'}{\Pi, \Pi' \to \Lambda, \Lambda'}$$

Add to U the pair (p_{B_i}, p_{B_j}).

(5) The inference is ($\wedge$:right):

$$\frac{\Pi \to \Lambda, A_{i'} \quad \Pi \to \Lambda, B_{j'}}{\Pi \to \Lambda, (A_i \wedge B_j)_\ell}$$

Add to U the pairs $(p_{(A_i \wedge B_j)_\ell}, p_{A_i} \wedge p_{B_j})$, $(p_{A_i}, p_{A_{i'}})$, $(p_{B_j}, p_{B_{j'}})$.
The other propositional rules are handled similarly.

(6) The inference is ($\exists$:right):

$$\frac{\Pi \to \Lambda, B(t)_{j'}}{\Pi \to \Lambda, \big((\exists x) B(x)_j\big)_i}$$

Add to U the pair $(p_{((\exists x)B(x)_j)_i}, (\exists x) p_{B(x)_j})$. Change C by adding the class $[p_{B(t)_{j'}}]_C \cup [p_{B(x)_j}]_C$ and by subsequently deleting $[p_{B(t)_{j'}}]_C$ and $[p_{B(x)_j}]_C$.
The other quantifier rules are handled similarly.

(7) If an axiom $B_i \to B_j$ is reached, then add to U the pair (p_{B_i}, p_{B_j}).

(8) At every inference, do the following: If D_i and D_j are corresponding occurrences of sub-semi-formulas of side formulas in the conclusion and a premise, respectively, then add to U the pair (p_{D_i}, p_{D_j}).

Clearly, π itself defines a congruence unifier θ for $\langle U, C\rangle$, via $\theta(p_{B_i}) = B$ (where B_i is an occurrence of the semi-formula B in π). So $\langle U, C\rangle$ has a solution.

Let $\langle \sigma, C'\rangle$ be a most general congruence unifier of $\langle U, C\rangle$. Write down the structure π' obtained from π by replacing every formula occurrence in π by its corresponding propositional variable, and apply σ to it. Let $t, t_1, \ldots, t_n$ be those terms in the end sequent of π' corresponding to A and $A_1, \ldots, A_n$, respectively, where $T = \{A_1, \ldots, A_n\}$.

(1) Match t with A and t_i with A_i: $t\mu = A$ and $t\mu_i = A_i$. Replace the variables in t, t_i according to μ, μ_i. (2) Perpetuate the replacement of variables by semi-formulas throughout π': If p is replaced by the semi-formula $\mathrm{frm}(p)$, and $\langle p', \mathrm{frm}(p')\rangle \in [p]_{C'}$, then replace p' by $\mathrm{frm}(p')$. (3) Replace all remaining variables by $(0 = 0)$. (4) remove all quantifier introductions which introduce dummy quantifiers to formulas $(0 = 0)$ introduced in (3).

Clearly, the resulting structure is indeed a proof. Furthermore, the number of variables in U which do not only occur at depth 0 is $\leq 2k$ (In the construction of U, at most 2 variables occurring at depth 1 were introduced per inference). By Lemma 2.5, the maximal logical depth of a formula in π' is bounded above by $\ell = 2^{2k} \max(\mathrm{ld}(T), \mathrm{ld}(A)) = \phi_T(k, \mathrm{ld}(A))$, so in particular it is independent of T_1'.

Now consider the part T_2' of the end sequent of π' corresponding to T_1': A formula B in T_2' can be of one of two forms: (1) $B \in T_1'$, i.e., $B \equiv (\mathsf{Q}x_1) \ldots (\mathsf{Q}x_n) A_n$

for some n. This can be the case only if $\mathrm{ld}(B) \leq \ell$, hence $n \leq \ell$ and therefore $B \in T_0'$. (2) $B \equiv (0 = 0)$ (dummy quantifiers were already removed). Since $(0 = 0) \in T$, the end sequent (up to exchanges and contractions) is contained in $T \cup T_0'$; the length of π' is $\leq k$. $\square$

The reader can now see the motivation for the definition of a congruence unification problem. The basic idea of the preceding proof is to rewrite the given proof in its most general form, so to speak, by replacing the formulas occurring in it by propositional variables. The unification problem defined ensures that only connectives and quantifiers which *must* occur in the more general proof (because they are introduced at an inference rule) *do* occur. It rules out the possibility that a given end sequent could only be proved by introducing arbitrarily complex formulas in the axioms or using weakenings, which disappear in cuts elsewhere in the proof. Were we only dealing with propositional proofs, Parikh's result could be obtained using conventional unification. The slightly problematic case is that of the quantifier rules, where the auxiliary formula in the premise is *not* a literal sub-formula of the principal formula in the conclusion, but only modulo the term structure. Hence, we cannot use the same propositional variable for, say, $B(t)$ and $B(x)$. Congruence unification is designed to take care of that.

In what follows, we abbreviate the tuple $x_1, \ldots, x_n$ by $\boldsymbol{x}$.

Theorem 3.3. *If T is a finite theory containing only prenex formulas, then T has finite term bases for all prenex $A(\boldsymbol{x})$ and k.*

Proof. Let $\boldsymbol{s}$ be some n-tuple of terms. If $A(\boldsymbol{s})$ is not provable in length k for any $\boldsymbol{s}$ then we can take $B = \emptyset$. So assume that $T \vdash^k A(\boldsymbol{s})$, i.e., $\mathbf{LK} \vdash^k T \to A(\boldsymbol{s})$. By Theorem 3.2 there is a proof π of $T \to A(\boldsymbol{s})$ containing only formulas of logical depth $\leq \ell' = \phi_T(k, \mathrm{ld}(A))$. In particular the maximal degree (number of logical symbols) of a cut formula in π is $\leq 2^{\ell'}$. By cut elimination we obtain a cut-free proof π' of the same end-sequent from atomic axioms of length $2^k_{2^{\ell'}} = \ell$. We skolemize this proof to obtain a proof π_s (of the same or lesser length) of $T_s \to A_s(\boldsymbol{s})$, where T_s and A_s are the skolemized variants of T and A, respectively. See [2] for how to skolemize a proof in situ: π_s contains the skolemized versions of the formulas occurring in π'. In particular, it contains no strong quantifiers, and π_s differs structurally from π' only insofar as the (redundant) strong quantifier inferences have been removed. Using the Midsequent Theorem we obtain an Herbrand sequent; the length of this Herbrand sequent is also $\leq \ell$; w.l.o.g. we can assume that its length on either side equals ℓ. Assume that $T_s = \{(\forall y_{i1}) \ldots (\forall y_{iq_i} B(y_{i1}, \ldots, y_{iq_i})\}_i$ and $A_s(\boldsymbol{s}) = (\exists z_1) \ldots (\exists z_p) A'(z_1, \ldots, z_p, \boldsymbol{x})[\boldsymbol{s}/\boldsymbol{x}]$. Then the Herbrand sequent H has the following form:

$$\langle B(t^1_{i1}, \ldots, t^1_{iq_i})\rangle_i, \ldots, \langle B(t^\ell_{i1}, \ldots, t^\ell_{iq_i})\rangle_i \to A'(s^1_1, \ldots, s^1_p, \boldsymbol{s}), \ldots, A'(s^\ell_1, \ldots, s^\ell_p, \boldsymbol{s})$$

Modulo the usual interpretation of a sequent, H is a propositional tautology. Every atomic formula defines a propositional variable. Now consider the following (semi-)sequent H'

$$\langle B(y^1_{i1}, \ldots, y^1_{iq_i})\rangle_i, \ldots, \langle B(y^\ell_{i1}, \ldots, y^\ell_{iq_i})\rangle_i \to A(z^1_1, \ldots, z^1_p, \boldsymbol{x}), \ldots, A(z^\ell_1, \ldots, z^\ell_p, \boldsymbol{x})$$

Define a unification problem as follows: Assume $P(r_1, \ldots, r_m)$ is an atomic formula in H, and let $P_i(u_{i1}, \ldots, u_{im})$ be all corresponding atomic formulas in H'. Then set $u_{ij} = r_j$. In other words, equate two atomic formulas in H' if the corresponding formulas in H are identical. Clearly, this unification problem is solvable, since H defines a solution. Hence there is a most general unifier σ. Furthermore, $H'\sigma\theta$ is a tautology for any substitution θ. Now let $\boldsymbol{s}^* = \sigma(\boldsymbol{x})$. $H'\sigma$ is a propositional tautology, so $T \to A(\boldsymbol{s}^*)$ is provable. Furthermore, the depth of $\boldsymbol{s}^*$ depends only on k and $A(\boldsymbol{x})$. Also, $\boldsymbol{s} = \boldsymbol{s}^*\theta$ for some unification θ.

Starting from $\boldsymbol{s}$ s.t. $A(\boldsymbol{s})$ is provable in k steps, we have found $\boldsymbol{s}^*$ s.t. $A(\boldsymbol{s}^*)$ is provable and $\boldsymbol{s}$ is a substitution instance of $\boldsymbol{s}^*$. But $\boldsymbol{s}^*$ did not directly depend on $\boldsymbol{s}$, rather on the Herbrand sequent obtained from the skolemized proof. In other words, every $\boldsymbol{s}$ where $A(\boldsymbol{s})$ is provable in k steps is a substitution instance of some $\boldsymbol{s}^*$ obtained from some Herbrand sequent of the skolemized end-sequent of length $\leq \ell$. But there are only finitely many Herbrand sequents, so there are only finitely many $\boldsymbol{s}^*$. The set of all of them gives a finite term basis. □

A way to find the term basis is writing down a semi-sequent of the form given by H', and partitioning the atomic formulas with the same leading predicate symbol. If the unification problem arising from such a partition has a solution σ, $H'\sigma$ is a propositional tautology, and $\sigma(\boldsymbol{x})$ contains no Skolem functions, then $\sigma(\boldsymbol{x})$ is an element of the term basis.

A different method of obtaining the above result would be to use unification over a cut-free proof skeleton; cf. [8]. Its advantage is that the structure of the original proofs is not changed as drastically as in our approach (by cut-elimination and skolemization); its disadvantage is, however, that it is prima facie much harder to calculate all realizable cut-free proof skeleta than it is to calculate all Herbrand disjunctions.

Corollary 3.4. *Assume that* $RCF \mid\!\!\frac{k}{\overline{LK}}\, A(\{1\}^n)$ *for some* k *and each* n. *Then* $RCF \mid\!\!\frac{}{\overline{LK}}\, (\forall x)A(x)$.

Proof. $A(t)$ is logically equivalent to some prenex formula $A'(t)$, and the equivalence is provable independently of t, say, in k' steps. So if $RCF \mid\!\!\frac{k}{\overline{\mathrm{LK}}}\, A(t)$, then $RCF \mid\!\!\frac{k+k'}{\overline{\mathrm{LK}}}\, A'(t)$ By Theorem 3.2, $RCF_0 \mid\!\!\frac{k+k'}{\overline{\mathrm{LK}}}\, A'(\{1\}^n)$ for all n and a finite subtheory $RCF_0 \subseteq RCF$. By Theorem 3.3, there is a finite term basis for $A'(x)$ and $k + k'$. Since every term of the form $1 + \cdots + 1$ must be a substitution instance of a term in the basis, one of the basis terms must be of the form $1 + \cdots + 1 + a = \{1\}^m(a)$, for a free variable a. We have $RCF_0 \mid\!\!\frac{}{\overline{\mathrm{LK}}}\, A'\big(\{1\}^m(a)\big)$, hence also $RCF \mid\!\!\frac{}{\overline{\mathrm{LK}}}\, A'\big(\{1\}^m(\{(-1)\}^m(a)\big)$. Since RCF also proves $A'\big(\{1\}^m(\{(-1)\}^m + a)\big) \leftrightarrow A'(a) \leftrightarrow A(a)$ we have $RCF \mid\!\!\frac{}{\overline{\mathrm{LK}}}\, (\forall x)A(x)$. □

We see that the generalization depends on the structure of the terms alone and not on their values, for the generalization result also holds for (1) the sequence $\{0\}^n$ and (2) any infinite subsequence of $\{1\}^n$ or $\{0\}^n$. Still, it is an interesting question how far the relations between large terms and terms with large values go.

Definition 3.5. An infinite sequence of terms s_i in 0, 1, $-$, $+$, $\cdot$ is a *notation for numbers*, if every $n \in \omega$ is the value of some s_i.

For the general case of notations, Krajíček's question has a negative answer: There are number notations where $A(s_i)$ is provable in k steps for all $i \in \omega$, but $(\forall x)A(x)$ is false: Take for $A(x) \equiv x \geq 0$ and for $s_i = (\{1\}^{a_i})^2 + (\{1\}^{b_i})^2 + (\{1\}^{c_i})^2 + (\{1\}^{d_i})^2$, where $\langle a_i, b_i, c_i, d_i \rangle$ enumerates all of ω^4. By Lagrange's Theorem, every natural number is the sum of four squares, so s_i ranges over all of ω. Furthermore, *RCF* proves that a sum of squares is not negative, i.e., $RCF \vdash (\forall x_1) \ldots (\forall x_4)(x_1^2 + x_2^2 + x_3^2 + x_4^2 \geq 0)$. Hence, $RCF \stackrel{k}{\vdash} s_i \geq 0$ for some fixed k.

We recapitulate a remark made in the introduction: If $A(s)$ is true for terms s of sufficiently large value, then it is true for all terms with larger value. This is in contrast to the following result, which holds in any number theory N strong enough to formalize Matiyasevič's theorem, e.g., $\mathbf{I\Sigma_1}$.

Proposition 3.6. *For every recursive formula $A(a)$ which is true for all natural numbers, there is a notation for numbers s_i in 0, 1, $+$, $\dot{-}$, $\cdot$ s.t. $N \stackrel{k}{\vdash} A(s_i)$ for all i and some $k \in \omega$. Consequently there is an $A(a)$ s.t. $N \stackrel{k}{\vdash} A(s_n)$ for all n but $N \nvdash (\exists y)(\forall x)\big(x \geq y \supset A(x)\big)$.*

Proof. By Matiyasevič's Theorem we have $N \vdash (\exists \boldsymbol{z})d(a, \boldsymbol{z}) = d'(a, \boldsymbol{z}) \leftrightarrow A(a)$ (d and d' are polynomials containing only 0, $'$, $+$, $\cdot$). Define

$$v(a, \boldsymbol{c}) = a \cdot \big(1 \dot{-} \big[\big(d(a, \boldsymbol{c}) \dot{-} d'(a, \boldsymbol{c})\big) + \big((d'(a, \boldsymbol{c}) \dot{-} d(a, \boldsymbol{c})\big)\big]\big).$$

First, observe that $N \vdash A(v(a, \boldsymbol{c}))$: $N \vdash v(a, \boldsymbol{c}) = 0 \supset A(v(a, \boldsymbol{c}))$, since $N \vdash A(0)$. $N \vdash v(a, \boldsymbol{c}) \neq 0 \supset A(v(a, \boldsymbol{c}))$, because $N \vdash v(a, \boldsymbol{c}) \neq 0 \supset d(a, \boldsymbol{c}) = d'(a, \boldsymbol{c})$ and $N \vdash d(a, \boldsymbol{c}) = d'(a, \boldsymbol{c}) \supset \big(A(a) \wedge v(a, \boldsymbol{c}) = a\big)$.

By assumption there is, for true recursive $A(a)$ and for each n, a solution $\boldsymbol{g}_n$ to the Diophantine representation for $A(a)$. Define $s_n \equiv v(\{1\}^n, \boldsymbol{g}_n)$. By definition, s_n has value n. Take for $A(a)$ the formula $\neg Prf(a, \lceil 0 = 1 \rceil)$, where Prf is a proof predicate for N. By the Incompleteness Theorem, $(\exists y)(\forall x)\big(x \geq y \supset A(x)\big)$ cannot be provable. $\square$

4 Introduction of blocks of quantifiers: Using zeroes of arbitrary polynomials

We have seen in the last section that generalization results hold for the theory of real closed fields, simply because in k steps an **LK**-proof can make use only of zeroes of polynomials with degree bounded in k. This, however, is counterintuitive. The length measure of a proof should take into account which, and how many axioms are used, in particular how many zeroes-of-polynomial axioms, but not the degree of the polynomials themselves. Any mathematician would feel equally entitled to the use of all axioms (zro_{2n+1}). One way to overcome this problem would

be to replace (zro_{2n+1}) by the formulas $(\exists y)y^{2n+1} + t_{2n}y^{2n} + \ldots + t_1 y + t_0 = 0$, where the t_i are arbitrary terms. This option has serious drawbacks, however. These instances of the zeroes axioms cannot be used in the familiar way to formulate lemmata etc. in a fixed number of steps. In particular, not even (zro_{2n+1}) is provable in a fixed length independent of n.

To do better justice to the above requirement, we can work, instead of in **LK** or a similar system, in a calculus where sequences of quantifiers of the same kind behave, w.r.t. proof length, like one quantifier. Such a system is $\mathbf{LK}_{\mathrm{B}}$.

Parikh's argument goes through for $\mathbf{LK}_{\mathrm{B}}$ relative to a modified measure of logical depth:

Definition 4.1. The *flat depth* $\mathrm{ld}^\flat(A)$ of a formula A is the logical depth of A where sequences of quantifiers of the same kind count only like one quantifier. More precisely:

(1) $\mathrm{ld}^\flat(A) = 0$ if A is atomic
(2) $\mathrm{ld}^\flat(A) = 1 + \mathrm{ld}^\flat(A_1)$ if $A \equiv \neg A_1$
(3) $\mathrm{ld}^\flat(A) = 1 + \max(\mathrm{ld}^\flat(A_1), \mathrm{ld}^\flat(A_2))$ if $A \equiv A_1 * A_2$ for $* \in \{\wedge, \vee, \supset\}$
(4) $\mathrm{ld}^\flat(A) = 1 + \mathrm{ld}^\flat(A_1)$ if $A \equiv (\mathsf{Q}x_1)\ldots(\mathsf{Q}x_n)A_1$ and A_1 does not start with $(\mathsf{Q}y)$ $(\mathsf{Q} \in \{\forall, \exists\})$.

Definition 4.2. A formula occurrence A *gives rise* to a formula occurrence A' in a proof π if there is a sequence of formula occurrences $A = B_1, \ldots, B_n = A'$, where B_{i+1} occurs in a sequent immediately above B_i and is either the principal formula of an introduction with auxiliary formula B_i or is obtained from B_i by repetition or exchange.

Definition 4.3. An $\mathbf{LK}_{\mathrm{B}}$-proof π is *simple* provided it satisfies the following properties:

(1) If a formula occurrence A in π contains a string of quantifiers of the same type, then no proper substring thereof is the string of quantifiers introduced at some quantifier inference acting on a formula occurrence that gives rise to A.
(2) No quantifier inference is improper.
(3) All eigenvariables are distinct (regularity).

Proposition 4.4. *Let π be an $\boldsymbol{LK}_{\mathrm{B}}$-proof of the sequent $\Gamma \to \Delta$. Then there is a proof π' of $\Gamma \to \Delta$ which is simple and* $\mathrm{len}(\pi') \leq 2\,\mathrm{len}(\pi)$.

Proof. We construct π' as follows: First we rename eigenvariables to ensure regularity. Take some occurrence of a formula $A = (\forall x_1)\ldots(\forall x_n)A'$ on the right side of a sequent in π, where the $\forall$-string is maximal, i.e., (a) A' does not start with $\forall$ and (b) no proper $\forall$-introduction rule is applied to A below the occurrence considered.

Consider the tree T of formula occurrences in π with vertices the formula occurrences which give rise to A, and which are subformulas of A but not of

(instances of) A', and with an edge between B and B' if B gives rise to B'. This tree branches only at contractions, its leaves are either axioms, weakening formulas, or subformulas of A', and if it contains the edge $\langle B, B' \rangle$, then $B = B'$ or B' is obtained from B by a ($\forall$:right) introduction. We now alter π' as follows: Let $a_i, \ldots, a_n$ be new free variables. If $(\forall x_i) \ldots (\forall x_n) A''$ is a leaf in an axiom, replace that axiom by

$$\frac{A''' \to A'''}{(\forall x_i) \ldots (\forall x_n) A'' \to A'''} \; \forall\text{:left}$$

where $A''' = A''[a_i/x_i, \ldots, a_n/x_n]$. In the graph T there are several vertices which are premises to bottommost ($\forall$:right) inferences, i.e., there are no other ($\forall$:right) inferences between them and the root A (there are essentially only contractions). Replace all occurrences of formulas in the subtrees ending in such vertices by $A'[b_1/x_1, \ldots, b_n/x_n]$, and replace free variables as needed to obtain a correct proof. Change the bottommost ($\forall$:right) inferences so as to introduce the entire string $(\forall x_1) \ldots (\forall x_n)$; the other inferences are now improper. The eigenvariable condition for the bottommost $\forall$-introductions are satisfied, since they were satisfied even already further above in the original proof.

Now consider the case of $A = (\exists x_1) \ldots (\exists x_n) A'$ occurring on the right side of some sequent, where the $\exists$-string is again maximal, and define the graph T as above. Let $a_i, \ldots, a_n$ be new free variables. If $(\exists x_i) \ldots (\exists x_n) A''$ is a leaf in an axiom, replace that axiom by

$$\dfrac{\dfrac{A''' \to A'''}{A''' \to (\exists x_1) \ldots (\exists x_n) A'} \; \exists\text{:right}}{(\exists x_i) \ldots (\exists x_n) A'' \to (\exists x_1) \ldots (\exists x_n) A'} \; \exists\text{:left}$$

where $A''' = A''[a_i/x_i, \ldots, a_n/x_n]$. Then consider a topmost ($\exists$:right) inference in T: Replace all occurrences of formulas in T below this inference by A. This changes all ($\exists$:right) introductions below this topmost one to improper inferences. Since this is done on every branch, contractions are still correct. Eigenvariable conditions cannot be violated by this modification, since potential eigenvariables are only replaced by bound variables *earlier* in the proof.

Similar considerations apply to ($\exists$:left) and ($\forall$:left). Note that the modification of axioms does not interfere with the modifications for another occurrence of the same formula. After these modifications have been performed, property (1) holds. Now delete all improper quantifier inferences and rename eigenvariables to obtain (2) and (3) $\Box$

Theorem 4.5. *Let π be a simple $\boldsymbol{LK}_{\mathrm{B}}$-proof of length k of the sequent $\Gamma \to \Delta$. Then there is a proof π' of $\Gamma \to \Delta$ with the same skeleton as π, and the flat depth of formulas occurring in π' is bounded above by $2^k \, \mathrm{ld}^\flat(\Gamma \to \Delta)$.*

Proof. We proceed as in the proof of Theorem 3.2 with the following modifications to accommodate the block quantifier inferences. We augment the propositional term language by second-order monadic *quantifier variables* of two types,

denoted $q_\forall$ and $q_\exists$. The unification problem is obtained from a simple proof, and so we can restrict the solutions so that (a) no two quantifier variables of the same kind immediately follow another, i.e., every quantifier variable corresponds to a maximal string of quantifiers of the same type, and (b) every quantifier variable has as a solution a *non-empty* string of quantifiers. The quantifier variables are unified as follows:

(1) $p = q_{\mathsf{Q}}(t)$: as in variable elimination
(2) $q_{\mathsf{Q}}(t) = (\mathsf{Q}x_1)\ldots(\mathsf{Q}x_n)s$, where s does not start with $(\mathsf{Q}y)$: replace $q_{\mathsf{Q}}(\cdot)$ throughout by $(\mathsf{Q}x_1)\ldots(\mathsf{Q}x_n)(\cdot)$.
(3) $q_{\mathsf{Q}}(t) = q'_{\mathsf{Q}}(t')$: replace $q_{\mathsf{Q}}(\cdot)$ throughout by $q'_{\mathsf{Q}}(\cdot)$, and add the equation $t = t'$.
(4) all other cases: not unifiable

Cases (1) and (2) are justified by (a) and (b) above (note that $q_{\mathsf{Q}}(t) = q'_{\mathsf{Q}}(q''_{\mathsf{Q}}(s)$ cannot occur); and (b) justifies that—as (4) dictates—$q_\forall(t) = q_\exists(t')$, $q_{\mathsf{Q}}(t) = \neg s$ and $q_{\mathsf{Q}}(t) = s * s'$ $(* \in \{\wedge, \vee, \supset\})$ do not unify. We construct a (monadic second-order) congruence unification problem U from π in the propositional term language extended by $q_\forall$ and $q_\exists$ just like in the proof of Theorem 3.2. We only give the case of the block quantifier introductions:

(4′) The inference is $\exists_B$:right:

$$\frac{\Pi \rightarrow \Lambda, A(t_1, \ldots, t_n)_{j'}}{\Pi \rightarrow \Lambda, \left((\exists x_1)\ldots(\exists x_n)A(x_1, \ldots, x_n)_j\right)_i}$$

Introduce a new second-order variable $q_\forall$, and add to U the pair $\left(p_{((\exists \boldsymbol{x})A(\boldsymbol{x})_j)_i}, q_\exists(p_{A(\boldsymbol{x})_j})\right)$. Add $[p_{A(\boldsymbol{t})_{j'}}]_C \cup [p_{A(\boldsymbol{x})_j}]_C$ to C and subsequently delete $[p_{A(\boldsymbol{t})_{j'}}]_C$ and $[p_{A(\boldsymbol{x})_j}]_C$.

Clearly, the proof π again defines a solution to the congruence unification problem U. The unification algorithm terminates and gives a substitution σ of which π is an instance; this is easily seen by inspection of the algorithm. As before, define π', mapping leftover propositional variables to a formula, say, $(0 = 0)$. In addition, σ maps quantifier variables to the corresponding actual string of quantifiers in π. For the *flat* depth of σ, the same bound holds as for usual unification. □

Lemma 4.6. *Cut elimination holds for simple* $\boldsymbol{LK}_{\mathrm{B}}$*-proofs, and the bound (w.r.t.* $\mathrm{ld}^\flat$*) for the cut-free proof is the same as for cut elimination in* $\boldsymbol{LK}$*.*

Proof. By inspection of the proof for **LK**. The critical step is the reduction of a cut formula which is introduced by two quantifier inferences. Since the proof is simple, the same quantifiers are introduced on the left and right side above the cut, and can be reduced as usual. □

Corollary 4.7. *There are finite term bases for any finite prenex theory w.r.t.* $\boldsymbol{LK}_{\mathrm{B}}$*.*

Theorem 4.8. *There are finite term bases for RCF w.r.t* $\boldsymbol{LK}_{\mathrm{B}}$*.*

Proof. We proceed as in the proof of Theorem 3.3. Again, we consider a proof π of $T \to A(\boldsymbol{s})$ of length k, where $T \subset RCF$ is finite. By Theorem 4.5, we know that there is a bound on the flat depth of all formulas in π. By Lemma 4.6, there is a cut-free proof π' of length k', and k' is bounded by a function in k and $A(x)$. By the Midsequent Theorem adapted to $\mathbf{LK}_{\mathrm{B}}$ we obtain a Herbrand sequent from the skolemized proof, and we construct the unification problem as before. The only obstacle is now to obtain a bound on the depth of the terms substituted into the position $\boldsymbol{x}$ to be generalized, since the depth of terms in T can be arbitrarily large. However, all large terms in H' are of the very specific form of the polynomial zeroes:

$$y_0 + y_1 h(y_0, \ldots, y_{2n}) + \ldots + y_{2n} h(y_0, \ldots, y_{2n})^{2n} + h(y_0, \ldots, y_{2n})^{2n+1} = 0$$

Now consider the following depth measure for terms t in the language of RCF_{op}. Color a branch in the term tree $T(t)$ if it passes through a function symbol h_{2n+1} for the zero of a polynomial. The *flat depth* of an occurrence of a term s in t is the depth of s in t if t is not colored at all, 0 if s itself is colored, and otherwise the length of the uncolored part of the path from s to the root, minus 1. The flat depth $\mathrm{dp}^\flat(t)$ of t is the maximum flat depth of a constant or variable in t. For instance, in $(1 + s_1) + h(1, s_2)$, s_1 occurs at depth 1, and s_2 occurs at depth 0.

By inspection of the proof of Lemma 2.5 we see that the same bound holds for the language of RCF_{op} w.r.t. $\mathrm{dp}^\flat$ as for the ordinary term depth. As is easily seen, (1) the large terms above have flat depth 0, in particular, all variables in them occur at flat depth 0, and (2) $\mathrm{dp}(t) = \mathrm{dp}^\flat(t)$ if t does not contain a symbol h_{2n+1}. Hence, $\mathrm{dp}^\flat\, \sigma(\boldsymbol{x})$ is bounded above by a function depending only on k and $A(\boldsymbol{x})$. We have $\mathrm{dp}^\flat\, \sigma(\boldsymbol{x}) = \mathrm{dp}\, \sigma(\boldsymbol{x})$, since $\boldsymbol{s}$ is a tuple of terms in the original language, and therefore does not contain h_j. By the same argument as before we have a finite term basis for RCF. □

Observe that here, however, the computation of the term basis is not effective, since there are infinitely many possible Herbrand sequents (with the same flat term depth but increasing real term depth). Furthermore, there are no term bases if the language is extended to include all the function symbols of RCF_{op}. The following result holds nevertheless:

Corollary 4.9. *RCF_{op} has finite term bases w.r.t. $\boldsymbol{LK}_{\mathrm{B}}$ for terms from the language restricted to the language of RCF plus $\sqrt{|\cdot|}$ and* finitely *many h_{2n+1}.*

Proof. For proofs containing the equality axioms for h_{2n+1}, the argument of the proof goes through, since variables occur only at flat depth 0 there. Axioms (sqrt′) and (zro'_{2n+1}) for the finitely many h_{2n+1} are treated like the other axioms in the finite part T. □

Consequently, Krajíček's question has a positive answer for *RCF and RCF_{op}* w.r.t. $\mathbf{LK}_{\mathrm{B}}$ (cf. Corollary 3.4).

5 Generalization for axiom schemata

Alternative approaches to axiomatize the reals are Dedekind cuts and supremum principles. (A Dedekind cut is a partition of $\mathbb{R}$ into two disjoint sets A and B s.t. $A \leq B$. The corresponding axiom says that for every such cut, there is an x s.t. $A \leq x \leq B$.) These principles are, of course, second order formulations. The corresponding first order schemata are complete for the theory of real closed fields. These are as follows:

$$\begin{aligned}(\exists x)A(x) \wedge (\exists x)B(x) \wedge (\forall x)\big[A(x) \vee B(x)\big] \wedge \\ \wedge\ (\forall x)(\forall y)\big[A(x) \wedge B(y) \supset x \leq y\big] \supset \\ \supset (\exists x)(\forall z)\big[(A(z) \supset z \leq x) \wedge (B(z) \supset x \leq z)\big]\end{aligned} \tag{ded}$$

$$(\exists x)C(x) \wedge (\exists x)B_C(x) \supset (\exists x)\big[B_C(x) \wedge (\forall y)\big(B_C(y) \supset x \leq y\big)\big] \tag{sup}$$

$$(\exists x)C(x) \supset (\exists x)(\forall y)\big[B_C(y) \supset \big(B_C(x) \wedge x \leq y\big)\big] \tag{sup$'$}$$

where $B_C(x) \equiv (\forall z)\big(C(z) \supset z \leq x\big)$ (x is an upper bound for C).

We will see that all these schemata are equivalent in a strong sense, even if restricted to existential A and C: Whenever we can prove something with one of them in k steps, we can prove it with one of the other two in $\phi(k)$ step in $\mathbf{LK}_{\mathrm{B}}$ (not in $\mathbf{LK}$, however).

Proposition 5.1. *The axioms for ordered fields with (sqrt) plus (sup) with quantifier free C gives an axiomatization of the theory of real closed fields, denoted RCF_{sup}.*

Proof. It suffices to show that (sup) implies the existence of zeroes for every polynomial of odd degree. Take for $C(x) \equiv p(x) < 0$, where $p(x)$ is a polynomial of odd degree. The hypotheses of (sup) are satisfied, so (sup) provides a least upper bound x_0 of C. It can be shown using the binomial theorem that if $p(x_0) < 0$ there is an $\epsilon > 0$ s.t. $p(x_0 + \epsilon) < 0$ (so x_0 is not an upper bound) and that if $p(x_0) > 0$ there is a $\delta > 0$ s.t. $p(x_0 - \epsilon) > 0$ for $0 < \epsilon < \delta$ (so x_0 is not the least upper bound). Hence, $p(x_0) = 0$. $\square$

Proposition 5.2. *(1) The schema (ded) with existential A derives (sup) with existential C in a fixed number of steps in $\boldsymbol{LK}_{\mathrm{B}}$.*
(2) The schema (sup) with existential C derives (ded) with existential A in a fixed number of steps in $\boldsymbol{LK}_{\mathrm{B}}$.
(3) The schemata (sup) and (sup$'$) derive each other in a fixed number of steps in $\boldsymbol{LK}_{\mathrm{B}}$.

Proof. (1) Let $C(x) \equiv (\exists \boldsymbol{z})C'(x, \boldsymbol{z})$ and suppose $(\exists x)C(x)$ and $(\exists x)(B_C(x))$ hold. Define $A(x) \equiv (\exists z)(\exists \boldsymbol{z})\big(C'(z, \boldsymbol{z}) \wedge x \leq z\big)$ and $B(x) \equiv (\forall z)(\forall \boldsymbol{z})\big(C'(z, \boldsymbol{z}) \supset z \leq x\big)$. $B(x)$ defines the set of all upper bounds of C, and A its complement. By the assumptions, $(\exists x)A(x)$ and $(\exists x)B(x)$ hold; by the dichotomy of $\leq$ we

have $(\forall x)(A(x) \vee B(x))$; by transitivity we get $(\forall x)(\forall y)\big(A(x) \wedge B(y) \supset x \leq y\big)$. We can apply (ded) and obtain an x_0 with $A \leq x_0 \leq B$. Since $A \leq x_0$, x_0 is an upper bound of A; since $x_0 \leq B$, x_0 is the least such bound.

(2) Let $C \equiv A$ and suppose the hypotheses of (ded) are satisfied. Then also the hypotheses of (sup) are satisfied for A, so there is a least upper bound x_0. Clearly, $A \leq x_0$ and also $x_0 \leq B$, since every z s.t. $B(z)$ is an upper bound of A.

(3) (sup) simulates (sup$'$): If $(\exists x)B_C(x)$ is false, then both schemata are obviously true. Otherwise we obtain $(\exists x)\big[B_C(x) \wedge (\forall y)\big(B_C(y) \supset x \leq y\big)\big]$ from (sup). We obtain (sup$'$) by shifting the quantifier $(\forall y)$ outside, and applying the tautology $A \wedge (B \supset C) \supset B \supset (A \wedge C)$.

(sup$'$) simulates (sup): Assume the hypotheses of (sup). By (sup$'$) we obtain $(\exists x)D$, where $D \equiv (\forall y)\big[B_C(y) \supset \big(B_C(x) \wedge x \leq y\big)\big]$. This implies $(\exists x)(D \wedge D)$. D implies $D' \equiv (\exists y)B_C(y) \supset \big(B_C(x) \wedge (\exists y)(x \leq y)\big)$, where the antecedent is among the hypotheses, and the second part of the consequent is simply true, leaving only $B_C(x)$. On the other hand, D also implies $D'' \equiv (\forall y)\big(B_C(y) \supset x \leq y\big)$.

Note that the arguments above can all be formalized schematically, and since we work in $\mathbf{LK}_{\mathrm{B}}$, the length of the quantifier prefixes $(\exists \boldsymbol{z})$ of C has no influence on the proof length. Hence, the proof length is independent of C. $\square$

From the preceding proposition it follows that, for purposes of generalization, we need only consider one of the above schemata. We will restrict attention therefore to (sup$'$), which has a striking similarity to the least number principle in number theory.

Theorem 5.3. *There are finite term bases for RCF_{sup} w.r.t. $\boldsymbol{LK}_{\mathrm{B}}$.*

Proof. This follows from the proofs of Theorems 4.1 and 4.2 of [3]. There it is shown that the schema $L\exists_1$

$$(\exists x)(\forall y)\big(A(y) \supset (A(x) \wedge x \leq y)\big)$$

with A purely existential (the *least number principle*) admits finite term bases. The proof also goes through for universal A, since it is based only on the assumption that the quantifier prefix of A consist of one type of quantifier. Now compare $L\exists_1$ to (sup$'$) for existential $C(z) \equiv (\exists \boldsymbol{z})C'(z, \boldsymbol{z})$; we expand the definition of $B_C(x)$ and shift quantifiers:

$$\begin{aligned}(\exists x)C(x) \supset (\exists x)(\forall y)\ \big[\ & (\forall z)(\forall \boldsymbol{z})\big(C'(z, \boldsymbol{z}) \supset z \leq y\big) \supset \\ & \supset (\forall z)(\forall \boldsymbol{z})\big(C'(z, \boldsymbol{z}) \supset z \leq x\big) \wedge x \leq y\big]\end{aligned}$$

We see that in this formulation, $B_C(x)$ is a purely universal formula. This form of (sup$'$) is of the same form as $L\exists_1$ (but has an additional premise which does not interfere with the proof, and it contains universal instead of existential formulas). $\square$

In summary, the same generalization results hold for RCF_{sup} as for RCF, in particular, Krajíček's question has a positive answer. It does not follow, however, that the axioms of RCF are derivable in a fixed number of steps from (sup).

6 Generalization fails for extensionality

Finally, we give conditions under which Krajíček's question must be answered negatively for any formulation of the theory of real closed fields: We take a theory T with constants 0, 1, functions $+$ and $\cdot$, and equality axioms, plus the following schema of extensionality:

$$(\forall x)\big(s(x) = s'(x)\big) \supset r(s(t_1), \ldots, s(t_n)) = r(s'(t_1), \ldots, s'(t_n)) \qquad \text{(ext)}$$

This schema is obviously true, so adding it does not change the set of provable formulas. It does, under certain assumptions, permit one to add and multiply in a fixed number of steps, something which cannot be done in, e.g., RCF alone.

We assume the following to hold in T:

(1) $T \vdash a + b = b \supset a = 0$ $(*)$
(2) T proves the recursion formulas for addition:
  (a) $T \vdash a + 0 = a$ $(+_1)$
  (b) $T \vdash a + (1 + b) = 1 + (a + b)$ $(+_2)$
(3) T proves the recursion formulas for multiplication:
  (a) $T \vdash a \cdot 1 = a$ $(\times_1)$
  (b) $T \vdash a \cdot (1 + b) = a + (a \cdot b)$ $(\times_2)$
(4) There is a term $\psi(a, b)$ which satisfies
  $T \vdash \psi(a, b) = 0 \leftrightarrow a = b$ (ψ)

Proposition 6.1. *In $T + (ext)$, short addition is possible:*
$T + (ext) \stackrel{k}{\vdash} \{1\}^n + \{1\}^m = \{1\}^{m+n}$.

Proof. We use a variant of *Yukami's Trick* [13]. Consider

$$A = \overbrace{\psi(\{1\}^n + (1 + \{1\}^{m-1}), \{1\}^{m+n})}^{D} + \underbrace{\psi(\{1\}^1(\{1\}^n + \{1\}^{m-1}), \{1\}^{m+n}) + \cdots + \psi(\{1\}^{m-1}(\{1\}^n + 1), \{1\}^{m+n})}$$

$$B = \overbrace{\psi(\{1\}^1(\{1\}^n + \{1\}^{m-1}), \{1\}^{m+n}) + \cdots + \psi(\{1\}^{m-1}(\{1\}^n + 1), \{1\}^{m+n})}^{B'} + \underbrace{\psi(\{1\}^{m-1}(\{1\}^n + 1), \{1\}^{m+n})}_{C}$$

By $(+_2)$ we have $T \vdash \{1\}^n + (1 + b) = \{1\}^1(\{1\}^n + b)$. The i-th summand $\psi(\{1\}^i(\{1\}^n + \{1\}^{m-i})$ of B equals the $(i+1)$-st summand of A. Using (ext), we have $T \vdash A = B$ independently of n and m. On the other hand, we can transform C (using (ext) for $a + 1 = 1 + a$, which is provable from $(+_1)$ and $(+_2)$ using (ext)) into $\psi(\{1\}^{m+n}, \{1\}^{m+n})$, and subsequently into 0 using (ψ) and (ext). Using (ext) again for $(+_1)$ transforms $B' + 0$ to B'. Using $(*)$, we get the desired result, namely $D = 0$. $\square$

Proposition 6.2. *In $T + (ext)$, short multiplication is possible:* $T + (ext) \stackrel{k}{\vdash} \{1\}^n \cdot \{1\}^m = \{1\}^{mn}$.

Proof. We argue as before:

$$A = \overbrace{\psi(\{1\}^n \cdot \{1\}^m, \{1\}^{mn})}^{D} + \underbrace{\psi(\{1\}^n + (\{1\}^n \cdot \{1\}^{m-1}), \{1\}^{mn}) + \cdots + \psi(\{1\}^{n(m-1)} + (\{1\}^n \cdot 1), \{1\}^{mn})}$$

$$B = \overbrace{\underbrace{\psi(\{1\}^n + (\{1\}^n \cdot \{1\}^{m-1}), \{1\}^{mn}) + \cdots + \psi(\{1\}^{n(m-1)} + (\{1\}^n \cdot 1), \{1\}^{mn})}_{C} + \underbrace{\psi(\{1\}^{n(m-1)} + (\{1\}^n \cdot 1), \{1\}^{mn})}}^{B'}$$

By $(\times_2)$, we have $T \vdash \{1\}^n \cdot (1 + b) = \{1\}^n + (\{1\}^n \cdot b)$ (in a constant number of steps independent of n). Using (ext), we get $A = B$, again independently of m and n. On the other hand, we can transform C (using (ext) for $(\times_1)$) into $\psi(\{1\}^{n(m-1)} + \{1\}^n, \{1\}^{mn})$. By Proposition 6.1 we can then prove, independently of m and n, that $C = \psi(\{1\}^{mn}, \{1\}^{mn})$. Hence we can transform C (by using (ψ) and (ext)) to 0, and finally (again using $(+_1)$ and (ext)) $B' + 0$ to B'. Using $(*)$ and (ext), we get $D = 0$, which was to be proved. □

Note that the ability to multiply arbitrary numbers in fixed length falsifies Kreisel's Conjecture for number theories; cf. [3], p. 43.

Theorem 6.3. *There is a formula $A(x)$ s.t. $RCF + (ext) \stackrel{k}{\vdash\!\!\!\vdash}_{LK} A(\{1\}^n)$ for all $n \in \omega$, but $(\forall x)A(x)$ is false.*

Proof. Observe that the required properties hold for RCF, a suitable ψ is given by $\psi(a, b) = a - b$. Since $RCF + (ext)$ adds and multiplies in a constant number of steps, we can prove in a constant number of steps for each n that $\{1\}^n = (\{1\}^a)^2 + (\{1\}^b)^2 + (\{1\}^c)^2 + (\{1\}^d)^2$, for some a, b, c, and d, since every natural number is the sum of four squares (Lagrange's theorem). For the latter terms, however, $t \geq 0$ is certainly provable in a fixed number of steps (independent of a, b, c, d), and so we have $\stackrel{k}{\vdash} \{1\}^n \geq 0$ for all $n \in \omega$. If $RCF + (ext)$ would admit generalization, $(\forall x)(x \geq 0)$ were provable, which is absurd. □

Corollary 6.4. *There is no k s.t. RCF (RCF_{op}, RCF_{sup}) $\stackrel{k}{\vdash} E$ for all instances E of (ext) (cf. Proposition 5.2).*

Proposition 6.5. *$RCF + (ext)$ proves $\{1\}^n \neq \{1\}^m$ for $n \neq m$ in a constant number of steps.*

Proof. W.l.o.g. assume $m > n$. Then $m - n - 1 \geq 0$, and there are a, b, c, d s.t. $a^2 + b^2 + c^2 + d^2 = m - n - 1$. Since (ext) allows short addition and multiplication, we can prove (in length independent of m and n) that $(\{1\}^a)^2 + (\{1\}^b)^2 + (\{1\}^c)^2 + (\{1\}^c)^2 = \{1\}^{m-n-1}$. RCF proves that a sum of squares is ≥ 0, so we have: $\{1\}^{m-n} > 0$. Using short addition on $\{1\}^{m-n} + \{1\}^n > \{1\}^n$ we get $\{1\}^m > \{1\}^n$. □

7 Conclusion

All our results relate to theories of specific syntactic forms, which the formulations of the real closed fields we have considered also have. The importance of these results for the theories of real closed fields themselves is that they give information about the relationship between proofs and computations. We give a simple example: If Krajíček's question can be answered positively for T, then it is not possible to quickly distinguish between unequal numbers (i.e., T does not prove $\{1\}^n \neq \{1\}^m$ for $n \neq m$, uniformly within a fixed number of steps). The schema (ext) is strong enough for this sort of decision (cf. Proposition 6.5), just like number theories including successor induction

$$A(0) \wedge (\forall x)\big(A(x) \supset A(x+1)\big) \supset (\forall x)A(x).$$

(§1 of [11] states that short addition is possible using successor induction. Assume $m > n$: $0 < x + 1$ is provable, and therefore $0 < \{1\}^{m-n}$ is provable. From this we obtain the desired result by short addition.)

References

[1] E. Artin and O. Schreier, Algebraische Konstruktion reeller Körper, Abh. Math. Sem. Univ. Hamburg 5 (1927) 100–115.

[2] M. Baaz and A. Leitsch, On skolemization and proof complexity, Fund. Inform. 20(4) (1994) 353–379.

[3] M. Baaz and P. Pudlák, Kreisel's conjecture for $L\exists_1$, in: P. Clote and J. Krajíček, eds., Arithmetic, Proof Theory and Computational Complexity (Oxford University Press, Oxford, 1993) 29–59.

[4] M. Baaz and R. Zach, Algorithmic structuring of cut-free proofs, in: E. Börger et. al., eds., Computer Science Logic. Selected Papers from CSL'92, LNCS 702 (Springer, Berlin, 1993) 29–42.

[5] P. Clote and J. Krajíček, Open problems, in: P. Clote and J. Krajíček, eds., Arithmetic, Proof Theory, and Computational Complexity (Oxford University Press, Oxford, 1993) 1–19.

[6] E. Eder, Relative Complexities of First Order Calculi, (Vieweg, Braunschweig, 1992).

[7] G. Gentzen, Untersuchungen über das logische Schließen I–II, Math. Z. 39 (1934) 176–210, 405–431.

[8] J. Krajíček and P. Pudlák, The number of proof lines and the size of proofs in first order logic, Arch. Math. Logic 27 (1988) 69–84.

[9] A. Martelli and U. Montanari, An efficient unification algorithm, ACM Trans. Prog. Lang. Sys. 4(2) (1982) 258–282.

[10] R. J. Parikh, Some results on the length of proofs, Trans. Am. Math. Soc. 177 (1973) 29–36.

[11] D. Richardson, Sets of theorems with short proofs, J. Symbolic Logic 39(2) (1974) 235–242.

[12] G. Takeuti, Proof Theory, 2nd ed. (North-Holland, Amsterdam, 1987).

[13] T. Yukami, Some results on speed-up, Ann. Japan Assoc. Philos. Sci. 6 (1984) 195–205.