Archive for Mathematical Logic Manuscript-Nr.
(will be inserted by hand later)

Note on Generalizing Theorems in Algebraically Closed Fields

Matthias Baaz and Richard Zach

Institut für Algebra und Diskrete Mathematik 118.2,
Technische Universität Wien, A–1040 Vienna, Austria
Group in Logic and the Methodology of Science
University of California, Berkeley, CA 94720–3840

Received: / Accepted:

Summary. The generalization properties of algebraically closed fields ACF_p of characteristic $p > 0$ and ACF_0 of characteristic 0 are investigated in the sequent calculus with blocks of quantifiers. It is shown that ACF_p admits finite term bases, and ACF_0 admits term bases with primality constraints. From these results the analogs of Kreisel's Conjecture for these theories follow: If for some k, $A(1 + \cdots + 1)$ (n 1's) is provable in k steps, then $(\forall x)A(x)$ is provable.

Mathematics Subject Classification (1991): 03F07, 03F20, 12L99

1. Introduction

Questions of generalizations of theorems are, typically, questions of the form: Suppose $A(t)$, where t is a large term, is provable in a relatively small number of steps. Is it possible to find a general term t' of which t is a substitution instance s.t. $A(t')$ is also provable? The most notorious open problem of this flavor is *Kreisel's Conjecture*, posed for Peano Arithmetic: If, for some k, $A(\bar{n})$ is provable in k steps for all $n \in \mathbb{N}$, then $(\forall x)A(x)$ is provable. (In PA, the numeral $\bar{n}$ is the constant 0 followed by n primes).

The analysis of a calculus w.r.t. generalization properties which can be easily formulated (such as Kreisel's Conjecture) can help to answer deeper questions such as

1. What are the components of large terms which are actually used in short calculations?
2. Is there a correspondence of proof steps and calculation steps, or, viewed the other way round, are there large terms which have evaluations by proofs in few steps?

Correspondence to: M. Baaz. Email: baaz@logic.tuwien.ac.at

3. Are there terms which might be used as variables in initial fragments of proofs disregarding their semantical meaning?

Such questions are purely *proof theoretical* in the sense that they cannot be expressed model theoretically. For instance, consider the theory of algebraically closed fields of a given characteristic. This theory is complete, decidable, and admits elimination of quantifiers. As long as one is only interested in *provability* (as is the case in classical, "analytic" proof theory), nothing can be said about it that cannot be said better in model theoretic terms. Only by considering complexity measures on formulas, terms, and proofs can proof theory yield *genuinely proof-theoretic* results.

In this note we investigate the behavior of the usual axiomatizations of extensions of the theory of algebraically closed fields ACF w.r.t. generalizations of theorems. We show that the finite extensions of ACF, in particular, the theories of algebraically closed fields of finite characteristic, admit *finite term bases* (see Definition 6.1). The theory ACF_0 of algebraically closed fields does not admit finite term bases, but it does admit a kind of finite term basis with constraints. We use these results to prove the analogs of Kreisel's Conjecture for these systems: If, for some k, $A(1+\cdots+1)$ (n 1's) is provable in k steps, then $(\forall x)A(x)$ is provable. (The methods used are related to those used in [1], with which we assume familiarity.)

2. Preliminaries

By $\mathbf{t}$ we denote the tuple $\langle t_1, \ldots, t_n\rangle$. The set of finite subsets of X is $\wp_{fin}(X)$. As is customary in proof theory, we use different sorts for free and bound variables, this allows us to disregard questions of substitutability. Context will determine the sort to be used. Formulas and terms are defined as usual. $\mathrm{Trm}_{\mathcal{L}}$ denotes the set of terms in the language $\mathcal{L}$. If X is a (set of, etc.) term(s), then $\mathrm{Var}(X)$ denotes the set of all variables in X.

A term t occurs in a term s at depth 0 if $s = t$ (syntactically equals) and otherwise at depth $n+1$ if $s = f(u_1, \ldots, u_n)$ (f an n-ary function symbol) and t occurs in u_j at depth n for some j. The depth of a term, denoted $\mathrm{dp}(t)$, is the maximum depth of an occurrence of a variable or constant symbol in t. The logical depth, $\mathrm{ld}(A)$, of a formula is defined similarly, the function symbols being the connectives and quantifiers.

Definition 2.1. 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: $\mathrm{dp}(U) = \max\{\mathrm{dp}(s), \mathrm{dp}(t) : \langle s, t\rangle \in U\}$. 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*.

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; an efficient algorithm is given in [3].

Lemma 2.2. *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. See [1], Lemma 2.5.

3. Axiom systems for algebraically closed fields

The language $\mathcal{L}$ of algebraically closed fields contains $=$ as predicate symbol, the constants 0, 1, and the function symbols $-$, $^{-1}$ (unary) and $+$, $\cdot$ (binary).

For our present purposes, we consider the usual system ACF of axioms for algebraically closed fields. These are:

1. quantified equality axioms,
2. the (purely universal) axioms for fields, plus
3. the infinite list of formulas, one for each $n \geq 1$,

$$(\forall x_0)\ldots(\forall x_{n-1})(\exists y)(x_0 + x_1 y + \cdots + x_{n-1}y^{n-1} + y^n = 0) \qquad (\mathrm{zro}_n)$$

asserting the existence of zeroes of every polynomial.

ACF becomes complete if axioms for the characteristic are added. These are either

$$\underbrace{1 + \cdots + 1}_{p\ 1's} = 0 \qquad (\mathrm{char}_p)$$

for characteristic p, p prime, or the infinite list

$$\underbrace{1 + \cdots + 1}_{q\ 1's} \neq 0 \qquad (\mathrm{inf}_q)$$

for every prime q. ACF plus (char_p) yields the axiom system ACF_p for the theory of algebraically closed fields of characteristic p; ACF plus $\{(\mathrm{inf}_q) : q \text{ prime}\}$ is denoted ACF_0. By skolemizing the axioms (zro_n) we obtain purely universal extensions ACF^{sk}, ACF_p^{sk}, and ACF_0^{sk}, respectively. The language $\mathcal{L}^{\mathrm{sk}}$ of ACF^{sk} contains in addition the function symbols $h_n(x_0, \ldots, x_{n-1})$ (n-ary). ACF^{sk} (ACF_p^{sk}, ACF_0^{sk}) consists of the axioms of ACF (ACF_p, ACF_0), with (zro_n) replaced by (zro'_n):

$$\begin{aligned}(\forall x_0)\ldots(\forall x_{n-1})(x_0 + x_1 h_n(x_0, \ldots, x_{n-1}) + \cdots \\ \cdots + x_{n-1} h_n(x_0, \ldots, x_{n-1})^{n-1} + h_n(x_0, \ldots, x_{n-1})^n = 0)\end{aligned} \qquad (\mathrm{zro}'_n)$$

4. Sequent calculus with blocks of quantifiers

A primary requirement in considering length of proofs is that the axioms of the theory should be treated uniformly w.r.t. length of proofs, i.e., that proofs of a given length may use *any* set of axioms of the theory. This is trivial for finite theories, but not for infinite theories like ACF where the quantifier complexity of the axioms is unbounded. A consequence of this is that Gentzen's sequent calculus **LK** is *not* suited for considerations of proof length. In [1], Theorem 3.2, it was shown how proofs in **LK** of a formula A of length k can only use a finite subtheory which depends only on k and the logical complexity of A. For this

reason, we use the calculus $\mathbf{LK}_\mathrm{B}$ in which blocks of quantifiers of one type can be treated as a single quantifier w.r.t. proof length.[1]

LK-*Block* ($\mathbf{LK}_\mathrm{B}$) is the logical calculus obtained from **LK** (see [4]) by replacing the quantifier introduction rules rules by

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

and

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

and similarly for $\exists$. The variables a_1, ..., a_n in ($\forall_B$:right) and ($\exists_B$:left) must be distinct and satisfy the eigenvariable condition.

Proofs in $\mathbf{LK}_\mathrm{B}$ 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 $\mathbf{LK}_\mathrm{B}$) of the sequent $T_0\to A$ where T_0 is a finite sequence of formulas in T. If we want to emphasize that the proof has length $\leq k$ we write it thus: $T\stackrel{k}{\vdash}A$.

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 like one symbol.

Any $\mathbf{LK}_\mathrm{B}$-proof can be transformed into one that has the following properties ([1], Proposition 4.4):

1. If a formula occurrence A 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, i.e., introduces an empty string of quantifiers.
3. All eigenvariables are distinct (regularity).

Such proofs are called *simple*. Both Parikh's Theorem and cut-elimination hold for simple proofs and we get:

Theorem 4.2. *If π is an $\mathbf{LK}_\mathrm{B}$-proof of $\Gamma\to\Delta$, then there is a simple, cut-free $\mathbf{LK}_\mathrm{B}$-proof π' of $\Gamma\to\Delta$ and the length of π' depends only on the length of π and the flat depth of the formulas in $\Gamma\to\Delta$.*

Proof. [1], Theorem 4.5 and Lemma 4.6.

[1] This example illustrates the fact that the concept of proof length as measured by number of steps, or number of symbols, etc., is only appropriate relative to a given application.

5. Generalizations from Herbrand sequents

Definition 5.1. Suppose T is a purely universal theory and A is a purely existential formula. A *Herbrand sequent of length ℓ for A in T_0 (or T)* is a tautological sequent H of the form

$$\langle B_i(\mathbf{t}_i^1)\rangle_i, \ldots, \langle B_i(\mathbf{t}_i^\ell)\rangle_i \to A'(\mathbf{s}^1), \ldots, A'(\mathbf{s}^\ell)$$

where $T_0 = \{(\forall \mathbf{y}) B_i(\mathbf{y})\}_i \subseteq T$ is finite and $A \equiv (\exists \mathbf{z}) A'(\mathbf{z})$.

In a sense, Herbrand sequents correspond to *elementary computations:* Since they are tautologies, they are closed under cut. So, e.g., compuations of equalities which can be proved by chains may also be proved by a sequence of cuts on Herbrand sequents.

Theorem 5.2. *Let T and T_0 be as above, let $A(\mathbf{x}) \equiv (\exists \mathbf{z}) A'(\mathbf{z}, \mathbf{x})$, let ℓ be fixed, and let H_0 be the* Herbrand matrix

$$\langle B_i(\mathbf{y}_i^1)\rangle_i, \ldots, \langle B_i(\mathbf{y}_i^\ell)\rangle_i \to A'(\mathbf{z}^1, \mathbf{x}), \ldots, A'(\mathbf{z}^\ell, \mathbf{x})$$

There are finitely many substitutions σ_j s.t.

1. *$H_0\sigma_j$ is a Herbrand sequent of $A(\mathbf{x}\sigma_j)$, and*
2. *every Herbrand sequent H of $A(\mathbf{s})$ in T_0 corresponding to H_0 is s.t. $H = H_0\sigma_j\theta$ for some substitution θ.*

$H'\sigma_j$ is called a *term minimal Herbrand sequent for $A(\mathbf{x}\sigma_j)$ in T_0.*

Proof. There are finitely many partitions of the atomic formulas in the Herbrand matrix H_0, each one induces a unification problem by identifying the corresponding terms occurring in the atomic formulas in one class. Suppose such a problem is solvable with a most general unifier σ_j. If $H'\sigma_j$ is a propositional tautology it is a Herbrand sequent of $A(\mathbf{x}\sigma_j)$. If H is a Herbrand sequent for $A(\mathbf{s})$ using the B_i, we can define a partition of the atomic formulas in H_0 by collecting those into a class whose corresponding atomic formulas in H *are* identical. The unification problem arising from this partition is solvable since H is a solution. If σ_j is the most general solution, then $H = H_0\sigma_j\theta$ for some substitution θ.

We would like to obtain bounds for the depth of terms in term minimal Herbrand sequents. For finite theories, the bound on the depth of terms after unification gives this bound, it depends on the (in that case, bounded) depth of the terms occurring in the axioms and in $A(\mathbf{x})$. In ACF^{sk} and its finite extensions, however, the axioms (zro'_n) contain terms of unbounded depth. The idea is to introduce a new measure on term depth, the *flat depth* $\mathrm{dp}^\flat$ of terms,

1. relative to which unification enjoys the same bounds as relative to the usual term depth,
2. $\mathrm{dp}^\flat(t) = \mathrm{dp}(t)$ if t is in $\mathcal{L}$, and
3. the flat depth of terms occurring in (zro'_n) is 0.

The flat depth of a term t is defined as follows:

1. If s is a subterm of t of the form $h_n(s_0, \ldots, s_{n-1})$, color every function symbol in s.

2. If s is of the form $f(s_0, \ldots, s_n)$ (f any function symbol other than h_n), then color f if some function symbol in some s_i is colored.

The flat depth of t is the maximum depth of subterms of t not containing any colored function symbols. A term s *occurs at flat depth* d in a term t if s occurs at depth d in a maximal subterm of t not containing any colored function symbols.

Example 5.3. Consider the following term, where the colored function symbols are underlined:

$$(1 + (1 + x))\underline{+}\big((1 + 1)\underline{\cdot}\underline{h_3}(y, (1\underline{+}(1\underline{+}z)))\big)$$

The flat depth is the maximum depth of $(1 + (1 + x))$ and $(1 + 1)$, i.e., 2. In it, x occurs at depth 2, and $(1 + 1)$, y, and z at depth 0.

We see that

1. unification has the same bounds on the flat depth of the result as on the depth (by inspection of the unification algorithm),
2. if no h_n's occur in t, $\mathrm{dp}^\flat(t) = \mathrm{dp}(t)$, and
3. the flat depth of the terms occurring in (zro'_n) is 0. In particular, the variables in (zro'_n) all occur at flat depth 0, so the bounds (w.r.t. flat depth) on unification involving these terms is independent of their depth (recall that only the number of variables occurring at depth > 0 matter, cf. Lemma 2.2).

Proposition 5.4. *In the notation of the theorem, let $H' = H_0\sigma$ be a term minimal Herbrand sequent for $A(\mathbf{x}\sigma)$ in ACF or ACF_p. The flat depth of $H\sigma$ is bounded in $A(\mathbf{x})$ and ℓ. (In particular, it is independent of the (zro'_n).)*

The upshot of this proposition ist that the axioms for algebraic closure are of no help in the evaluation of terms in the original language $\mathcal{L}$, in a similar way as the axioms for $^{-1}$ and $-$ and the corresponding equality axioms are immaterial for the evaluation of terms not containing these functions.

Corollary 5.5. *Suppose there is a Herbrand sequent H for $A(\mathbf{s})$ in $T_0 \subseteq ACF^{\mathrm{sk}}$ (ACF_p^{sk}) of length ℓ. Then there are terms $\mathbf{s}^*$ and a Herbrand sequent H' of length ℓ for $A(\mathbf{s}^*)$ in T_0 s.t. $\mathbf{s} = \mathbf{s}^*\theta$ for some substitution θ. The depth of $\mathbf{s}^*$ is bounded in $A(\mathbf{x})$ and ℓ.*

In the theory ACF_0 we face the additional difficulty that not even the flat depth of the terms in (inf_q) is bounded, and, more importantly, that since those terms are in the original language, they may unify with the terms to be generalized.

Definition 5.6. By $\{s\}^n(t)$ we denote $\underbrace{s + (s + \cdots + (s + (s}_{n \text{ occurrences of } s} + t)\ldots)$; $\{s\}^n$ stands for $\{s\}^{n-1}(s)$.

Corollary 5.7. *Suppose there is a Herbrand sequent H for $A(\mathbf{s})$ in ACF_0^{sk} of length ℓ. Then there are terms $\mathbf{s}^*$, a sequent H', and a mapping $p\colon \mathrm{Var}(H) \to \wp_{fin}(\mathbb{N})$ s.t.*

1. *$H = H'\theta$ for some substitution θ satisfying the property*

(∗) *for all variables* v *occurring in* $\mathbf{s}^*$ *and for all* $k \in p(v)$, $v\theta = \{1\}^{k'}$ *and* $k + k'$ *is prime.*

2. *for all substitutions* τ *satisfying* (∗) *we have that* $H'\tau$ *is a Herbrand sequent of length* ℓ *for* $A(\mathbf{s}^*\tau)$ *in* ACF_0^{sk}.

The $p(v)$ *and the depth of* $\mathbf{s}^*$ *are bounded in* $A(\mathbf{x})$ *and* ℓ.

Proof. H is of the form

$$\langle B_i(\mathbf{t}_i^1)\rangle_i, \ldots, \langle B_i(\mathbf{t}_i^\ell)\rangle_i, \{1\}^{q_1} \neq 0, \ldots, \{1\}^{q_\ell} \neq 0 \to A(\mathbf{s}^1, \mathbf{s}), \ldots, A(\mathbf{s}^\ell, \mathbf{s})$$

where q_j is some prime. We use the corresponding Herbrand matrix H_0,

$$\langle B_i(\mathbf{y}_i^1)\rangle_i, \ldots, \langle B_i(\mathbf{y}_i^\ell)\rangle_i, u_1 \neq 0, \ldots, u_\ell \neq 0 \to A(\mathbf{z}^1, \mathbf{x}), \ldots, A(\mathbf{z}^\ell, \mathbf{x})$$

as the basis of a unification problem with most general solution σ. Again, there is a bound on the flat depth of terms occurring in $H' = H_0\sigma$. Also, $H'\tau$ is a tautology for any substitution τ. *It is not guaranteed, however, that* $u_j\sigma\tau$ *is of the form* $\{1\}^{q_j}$, and so the tautology may not represent a Herbrand sequent of $A\sigma\tau$ in ACF_0^{sk}. This is a problem in particular if we want to instantiate the positions of generalization. Previously, we took $\mathbf{s}^* = \mathbf{x}\sigma$ and got Herbrand sequents for $A(\mathbf{s}^*)$ and all $A(\mathbf{s}^*\tau)$, now this is only true for τ satisfying (∗), i.e., if τ is s.t. $(u_i\tau \neq 0)$ gives axioms of the form (inf_p) for some prime p. For θ given by H, of course, this is trivially true. We take $p(v) = \{r_i : u_i\sigma = \{1\}^{r_i}(v), 1 \leq i \leq \ell\}$.

Note that the general question of whether a tautological sequent can be extended to an Herbrand sequent in ACF_0 is non-trivial. For instance, there is a substitution τ s.t.

$$(\{1\}^{n+2}(x) \neq 0, \{1\}^n(x) \neq 0 \to \{1\}^{n+2}(x) \neq 0 \wedge \{1\}^n(x) \neq 0)\tau$$

is an Herbrand sequent iff there is a twin prime above n.

6. Finite term bases for *ACF* and ACF_p, $p > 0$

Definition 6.1. A finite set of tuples of terms, $B = \{\mathbf{t}^1, \ldots, \mathbf{t}^m\}$ is called a *term basis* for $A(\mathbf{x})$ and k in a theory T if

1. $T \vdash A(\mathbf{t}^i)$ for $1 \leq i \leq m$,
2. if $T \overset{k}{\vdash} A(\mathbf{s})$ then there is a substitution θ s.t. for some i $(1 \leq i \leq m)$ it holds that $\mathbf{s} = \mathbf{t}^i\theta$.

Theorem 6.2. *Any finite extension of ACF, in particular,* ACF_p *for* $p > 0$, *admits finite term bases for* $\mathcal{L}$.

Proof. Let T be a finite extension of ACF, T^{sk} its skolemized purely universal version. We may assume that A is in prenex form, and let A^{sk} be its existential skolemization. Assume $T \overset{k}{\vdash} A(\mathbf{s})$ with proof π. Then there is a proof π' of $A^{\mathrm{sk}}(\mathbf{s})$ from T^{sk} of the same length. By Theorem 4.2 we obtain a cut-free $\mathbf{LK}_{\mathrm{B}}$-proof π'' of $A^{\mathrm{sk}}(\mathbf{s})$ of length bounded by a function in $\mathrm{ld}^\flat(A(\mathbf{x}))$ and k. From this we can extract (using the midsequent theorem) a Herbrand sequent; its length is bounded in the length of π'.

Theorem 5.5 yields a Herbrand sequent for $A^{\mathrm{sk}}(\mathbf{s}^*)$. The depth of $\mathbf{s}^*$ (which equals the flat depth of $\mathbf{s}^*$) is bounded in the length of π and $A(\mathbf{x})$, and $\mathbf{s} = \mathbf{s}^*\theta$ for some θ. The depth of all possible such $\mathbf{s}^*$ is bounded in k and $A(\mathbf{x})$, so there are only finitely many of them.

Corollary 6.3. *Let T be any finite extension of ACF. If, for some k, $T \stackrel{k}{\vdash} A(\{1\}^{i_1}, \ldots, \{1\}^{i_n})$ for all $i_j \in \mathbb{N}$, then $T \vdash (\forall x_1) \ldots (\forall x_n) A(x_1, \ldots, x_n)$.*[2]

Proof. Let ℓ be the depth of the largest term in the term basis for A and k in T. Take $\ell_1 = \ell + 1$, $\ell_{j+1} = \ell_j + \ell + 1$, and let $s_j = \{1\}^{\ell_j}$. $T \stackrel{k}{\vdash} A(\mathbf{s})$, so there are terms $\mathbf{t}$ and a substitution θ s.t. $T \vdash A(\mathbf{t})$ and $\mathbf{s} = \mathbf{t}\theta$. By the choice of ℓ_j (i.e., since the maximum depth of $\mathbf{t}$ is $\leq \ell$), the t_j are of the form $\{1\}^{\ell'_j}(x_j)$, where $x_i \neq x_j$ for $i \neq j$. By substituting $(-\{1\}^{\ell'_j}(x_j))$ for x_j we get $T \vdash A(\mathbf{x})$ and so $T \vdash (\forall \mathbf{x}) A(\mathbf{x})$.

Note that this result makes crucial use of the bound on the proof length, in contrast to the fact that if ACF_p (ACF_0) $\vdash A(t)$ for *all* closed terms t in $\mathcal{L}^{\mathrm{sk}}$, then ACF_p (ACF_0) $\vdash (\forall x) A(x)$. This last fact holds by the completeness of ACF_p (ACF_0).

Definition 6.4. A term t is called *noncollapsible* in ACF_p, p prime, if, for every term $t'(\mathbf{x})$ resulting from t by replacing subterms by variables, there is no closed term s s.t. $ACF_p \vdash (\forall \mathbf{x})(t'(\mathbf{x}) = s)$.

Example 6.5. $\{1\}^n$ and $\{0\}^n$ ($n \in \mathbb{N}$) are all noncollapsible.

Corollary 6.6. *Suppose $ACF_p \stackrel{k}{\vdash} A(t)$ for a sufficiently large (w.r.t. k and $A(x)$) noncollapsible t. Then $ACF_p \vdash (\forall x) A(x)$.*

In fact, even more is true: We call a tuple $\langle I_1, \ldots, I_n \rangle$ of sets of terms an *n-system*, if

1. I_j contains infinitely many noncollapsible terms (which, since the language contains only finitely many function symbols, are therefore also arbitrarily deep), and
2. if $s \in I_i$ and $t \in I_j$ ($i \neq j$), then all subterms common to s and t are of depth $\leq n$.

For instance, $\mathbf{I} = \langle I_1, \ldots, I_n \rangle$ with $I_j = \{\{1\}^i(1 \cdot (1 \cdot \ldots (1 \cdot 1) \ldots)) : i \in \mathbb{N}\}$ (product of j 1's) is an n-system for every n. We now get:

Corollary 6.7. *Suppose $ACF_p \stackrel{k}{\vdash} A(t_1, \ldots, t_n)$ for t_j sufficiently large and $t_j \in I_j$, where $\mathbf{I} = \langle I_1, \ldots, I_n \rangle$ is an n-system. Then $ACF_p \vdash (\forall x_1) \ldots (\forall x_n) A(x_1, \ldots, x_n)$.*

Proof. By Theorem 6.2, there is a finite term basis, and the terms therein are of bounded complexity, say ℓ. $ACF_p \stackrel{k}{\vdash} A(t_1, \ldots, t_n)$, so if t_i is deeper than $\ell + n$, some tuple of terms $\langle s_1(x_1, \mathbf{y}), \ldots, s_n(x_n, \mathbf{y}) \rangle$ in the term basis has $\langle t_1, \ldots, t_n \rangle$ as a substitution instance, each s_i contains at least one variable x_i and is noncollapsible. Here, the x_i are chosen so that if $t_i = s_i(u_i, \mathbf{v})$,

[2] This version of Kreisel's Conjecture for the theory of real closed fields was posed (for $n = 1$) as an open problem by Krajíček [2, Problem 23]; see [1].

the depth of u_i is $> n$. By condition (2) of the definition of n-system, then, u_i and u_j must be different, and hence $x_i \neq x_j$. As is easily seen, there are terms $s_i'(x_i, \mathbf{y})$ which are polynomials in x_i s.t. $ACF_p \vdash s_i(x_i, \mathbf{y}) = s_i'(x_i, \mathbf{y})$. We can choose constant terms $\mathbf{c}$ s.t. $s_i'(x_i, \mathbf{c})$ is not a constant function. $ACF_p \vdash (\forall x_1) \ldots (\forall x_n) A(s_1'(x_1, \mathbf{c}), \ldots, s_n'(x_n, \mathbf{c}))$, and also $T \vdash (\forall y)(\exists x_i)(s_i'(x_i, \mathbf{c}) = y)$, by algebraic closure. Hence, $ACF_p \vdash (\forall \mathbf{x}) A(\mathbf{x})$.

The following corollary illustrates how calculating with large terms is related to calculating with transcendent elements, or equivalently, variables. In other words, algebraic elements may take the place of transcendent elements in proofs under certain circumstances, namely when the complexity of the terms representing them is sufficiently large relative to the length of the proof.

Corollary 6.8. *There is a function $\Psi: \wp_{fin}(\mathrm{Trm}_{\mathcal{L}}) \times \mathbb{N} \to \mathbb{N}$ s.t. for all polynomials $p_1, \ldots, p_r$ in the variables $x_1, \ldots, x_n$, the following are equivalent:*

1. *There are a $k \in \mathbb{N}$ and noncollapsible terms $t_1 \in I_1, \ldots, t_n \in I_n$ in an n-system $\mathbf{I}$ with $\mathrm{dp}(t_i) > \Psi(\{p_1, \ldots, p_r\}, k)$ s.t.*

$$ACF_p \stackrel{k}{\vdash} p_1(t_1, \ldots, t_n) \neq 0 \vee \ldots \vee p_r(t_1, \ldots, t_n) \neq 0$$

2. *There are polynomials $q_1, \ldots, q_r$ in the variables $x_1, \ldots, x_n$ s.t.*

$$ACF_p \vdash (\forall \mathbf{x})(p_1(\mathbf{x})q_1(\mathbf{x}) + \cdots + p_r(\mathbf{x})q_r(\mathbf{x}) = 1).$$

Proof. (2) implies (1) is obvious. For (1) implies (2), consider the following special case of Hilbert's Nullstellensatz [5, p. 5]: If K is a field and $L \supseteq K$ an algebraically closed extension field, and the polynomials $p_1, \ldots, p_r \in K[x_1, \ldots, x_n]$ have no common zero in L, then there are polynomials $q_1, \ldots, q_r \in K[x_1, \ldots, x_n]$ s.t. $p_1q_1 + \cdots + p_rq_r = 1$. Take $A \equiv p_1 \neq 0 \vee \ldots \vee p_r \neq 0$. We generalize as in Corollary 6.7, taking Ψ the function given by the maximum depth of terms in the term basis for A and k, plus $n+1$, and obtain $ACF_p \vdash (\forall \mathbf{x}) A(\mathbf{x})$. The Nullstellensatz is applicable, and we have the polynomials $q_1, \ldots, q_r$ s.t. $p_1q_1 + \cdots + p_rq_r = 1$. The length of the proof of this only depends on the p_i.

7. Term bases and generalization for ACF_0

Definition 7.1. A finite set of n-tuples of terms $B = \{\mathbf{t}^1, \ldots, \mathbf{t}^m\}$ together with a mapping $p : \mathrm{Var}(B) \times \{1, \ldots, m\} \to \wp_{fin}(\mathbb{N})$, is called a *term basis with primality constraints for $A(\mathbf{x})$ and k* in ACF_0 if

1. $T \vdash A(\mathbf{t}^i\tau)$ for for all τ s.t. the following condition holds:
   $(**)$ for all v occurring in t_j^i and all $k \in p(v, i)$, we have $v\tau = \{1\}^{k'}$ and $k + k'$ is prime.
2. if $T \stackrel{k}{\vdash} A(\mathbf{s})$ then there is a substitution θ s.t. for some i $(1 \leq i \leq m)$ it holds that $\mathbf{s} = \mathbf{t}^i\theta$ and $(**)$ holds for θ.

Theorem 7.2. *ACF_0 admits finite term bases with primality constraints for $\mathcal{L}$.*

Proof. Exactly like the proof of Theorem 6.2, using Corollary 5.7, using the fact that both $\mathrm{dp}(\mathbf{s}^*)$ and $p(v)$ are bounded in $A(\mathbf{x})$ and k. The $p(v, i)$ are obtained from the respective $p(v)$'s.

Corollary 7.3. *If, for some k, $ACF_0 \stackrel{k}{\vdash} A(\{1\}^{i_1}, \ldots, \{1\}^{i_n})$ for all $i_j \in \mathbb{N}$, then $ACF_0 \vdash (\forall x_1) \ldots (\forall x_n) A(x_1, \ldots, x_n)$.*

Proof. Let B be a term basis with primality constraints p for $A(\mathbf{x})$ and k as given by Theorem 7.2, let $B_0 \subseteq B$ consist of all tuples $\mathbf{t}^i$ in B of the form $\langle \{1\}^{\ell^i_j}(v^i_j) : 1 \leq j \leq n \rangle$ (only these are candidates for generalizations). We want to find $\mathbf{t}^i \in B_0$ s.t.

1. $v^i_j \neq v^i_{j'}$ whenever $j \neq j'$, and
2. the primality constraints on the variables in $\mathbf{t}^i$ are empty.

The theorem then follows, since without constraints $ACF_0 \vdash A(\mathbf{t}^i\tau)$ for *any* substitution τ, in particular $ACF_0 \vdash A(\{1\}^{\ell^i_1}(\{-1\}^{\ell^i_1}(v^i_1), \ldots, \{1\}^{\ell^i_n}(\{-1\}^{\ell^i_n}(v^i_1))$ and hence $ACF_0 \vdash (\forall \mathbf{x}) A(\mathbf{x})$.

The existence of such a tuple $\mathbf{t}^i$ follows from a suitable choice of the i_j, which have to satisfy

$1'$. $i_1 > \ell$ and $i_{j+1} > i_j + \ell$ for (1), and
$2'$. $\min\{|i_j - p| : p \text{ prime}\} > \ell$ for (2),

where ℓ is the maximum term depth of the term basis elements. We choose

$$i_1 = \prod_{r=1}^{h_1} p_r + \ell + 2,$$

where p_r denotes the r-th prime, p_{h_1} is the smallest prime $> 2\ell$, and

$$i_{j+1} = \prod_{r=1}^{h_j} p_r + \ell + 2$$

where p_{h_j} is the smallest prime $> i_j$. The result follows since $i_j - \ell, \ldots, i_j + \ell$ are all composite.

The reader will note right away that the generalization result would not hold for the case of characteristic 0, had the axiomatization of ACF_0 contained (char_q) for *all* $q \in \mathbb{N}$, since $(\forall x)(x = 0)$ is certainly not provable. Also note that the corollary implies that ACF_0 does not prove, in a fixed number of steps, that $\{1\}^n \neq 0$. This result does not depend on the *values* of the terms $\{1\}^n$, but only on their *form*. For instance, for $t_n = \{1\}^n \cdot (1 - (\{1\}^n)^{-1}) + 1$, ACF_0 *does* prove in a constant number of steps that $t_n \neq 0$ (case distinction according to whether $\{1\}^n = 0$ or not).

It is easily seen that Corollary 6.7 transfers to ACF_0 if noncollapsible terms are defined as noncollapsible terms of ACF_p not containing subterms of the form $\{1\}^j$ where $j > 1$.

8. Conclusion

One potential application of the results of this note is the analysis of the impact of incorrect identifications of terms: What happens if $T \cup \{t = c\}$ is used in a proof of A even though $T \vdash t \neq c$? For $T = ACF_p$ or ACF_0, Corollary 6.7

and the remark at the end of the preceding section tell us that the incorrect assumption can be eliminated from the proof (the calculation) of length k if t is an noncollapsible term of sufficiently large size relative to $x = c \to A$ and k. This fact might be used for the speed-up of a priori bounded calculations by the identification of large noncollapsible terms with, e.g., 0.

References

1. Baaz, M., Zach, R. (1995). Generalizing theorems in real closed fields. Ann. Pure Appl. Logic **75**, 3–23.
2. Clote, P., Krajíček, J. (1993). Open problems. In *Arithmetic, Proof Theory, and Computational Complexity*, 1–19. Oxford University Press, 1993.
3. Martelli, A., Montanari, U. (1982). An efficient unification algorithm. ACM Trans. Prog. Lang. Sys. **4**(2), 258–282.
4. Takeuti, G. (1987). Proof theory, 2nd ed. Studies in Logic 81. North-Holland, Amsterdam.
5. van der Waerden, B. L. (1950). Modern algebra, vol. II. Ungar, New York.