CONTEMPORARY MATHEMATICS

106

Logic and Computation

Proceedings of a Workshop held at
Carnegie Mellon University, June 30–July 2, 1987

Wilfried Sieg, Editor

AMERICAN MATHEMATICAL SOCIETY • PROVIDENCE, RHODE ISLAND

The Workshop on Logic and Computation was held at Carnegie Mellon University on June 30–July 2, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03, 68.

Library of Congress Cataloging-in-Publication Data

Workshop on Logic and Computation (1987: Carnegie Mellon University)
Proceedings of the Workshop on Logic and Computation: proceedings of a conference held June 30–July 2, 1987, at Carnegie Mellon University/Wilfried Sieg, editor.
p. cm.—(Contemporary mathematics, ISSN 0271-4132; v. 106)
ISBN 0-8218-5110-1 (alk. paper)
1. Computable functions—Data processing—Congresses. I. Sieg, Wilfried, 1945-. II. Title. III. Series: Contemporary mathematics (American Mathematical Society); v. 106.
QA9.59.W67 1987 90-40
511.3—dc20 CIP

Printed in the United States of America.
This volume was printed directly from author-prepared copy.
The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability. ♾
Portions of this publication were typeset using AMS-TEX, the American Mathematical Society's TEX macro system.

10 9 8 7 6 5 4 3 2 1 95 94 93 92 91 90

Contents

Contemporary Mathematics
Volume 106, 1990

A NOTE ON POLYNOMIAL TIME COMPUTABLE ARITHMETIC

Wilfried Buchholz and Wilfried Sieg

ABSTRACT. In Ferreira's contribution to these Proceedings the class $\mathscr{P}$ of polynomial time computable functions is characterized as the class of provably recursive functions of some weak formal theories. The first such characterization of $\mathscr{P}$ was given, of course, by Buss. A form of Herbrand's theorem for partially normalized derivations is used in this note to obtain Ferreira's results. Such "Herbrand-analyses" have been applied in a variety of contexts (see [F/S],[L], [S1]): they are most appropriate if one wants to extract computational information from derivations; they are conceptually clear and technically strong.

A. INTRODUCTION. The class $\mathscr{P}$ of polynomial time computable functions is characterized in [F] as the class of provably recursive functions of three restricted theories for binary trees or 0-1-words. The basic theory , PTCA, allows induction for polynomial time decidable predicates; PTCA$^+$ is obtained from it by expanding the induction schema to NP-predicates. The third theory, (Σ_1^b-PIND), is like PTCA$^+$, but its language contains only symbols for some basic functions, not for all elements of $\mathscr{P}$. That the latter theory has exactly the elements of $\mathscr{P}$ as its provably recursive functions is the analogue of the main theorem in [B] for n=1. Ferreira obtains this result by a mixture of model- and proof- theoretic techniques. We give a canonical, purely proof-theoretic Herbrand-analysis that yields Ferreira's result for PTCA$^+$ and brings out most sharply the central problem; namely, the analysis of weak induction schemata by recursive functions of low complexity.

The main ideas for this paper emerged in the summer of 1988, when we gave a joint seminar at the Ludwigs-Maximilians-Universität in München. Buchholz presented [F] in the seminar; Sieg was working on his [S2] in which Herbrand-analyses for systems of (bounded) arithmetic are given. So it was natural to explore whether they can be given for Ferreira's theories of binary trees. Our note is thus complementing [F].

B. BOUNDED LOGICAL COMPLEXITY. We use the same formal framework as [F]; in particular, L is the first order language with constant symbols $\emptyset, 0, 1$, function symbols $\frown$ and $\times$, and two binary relation symbols $\subseteq$ and $=$. The language $L(\mathscr{P})$, i.e. L_P in [F], is obtained from L by adding function symbols for each element of $\mathscr{P}$. The

1980 Mathematics Subject Classification (1985 Revision). 03F30

latter class can be defined inductively as the smallest class X of functions, such that X contains certain initial functions (Z; P_i^n, $1 \le i \le n$, $n \in \mathbb{N}$; C_0, C_1, and Q), and is closed under composition and bounded iteration. Let st abbreviate $s^\frown t$ for L-terms s and t: $x|_z = y$ stands for $(1 \times z \subseteq 1 \times x \;\&\; y \subseteq x \;\&\; 1 \times z = 1 \times y) \vee (1 \times x \subseteq 1 \times z \;\&\; y = x)$. Using these abbreviations we formulate the schema of bounded iteration :

f is defined by iteration from g, h_0, h_1 with bound $t[\mathbf{x},y]$ if

$$f(\mathbf{x},\emptyset) = g(\mathbf{x})$$

$$f(\mathbf{x},yi) = h_i(\mathbf{x},y,f(\mathbf{x},y))|_{t[\mathbf{x},y]} \quad (i = 0,1)$$

where t is an L-term and $\mathbf{x}$ indicates a possibly empty sequence of variables. As we are going to work in a Tait-style sequent calculus, it is convenient to build up formulas from literals (atomic or negations of atomic formulas) by using $\&$, $\vee$, $\forall$, $\exists$. Negations of complex formulas, conditionals and biconditionals are defined as usual.

1. DEFINITIONS

1.1. QF($\mathcal{P}$) denotes the set of quantifier-free formulas of L($\mathcal{P}$).

1.2. $(\forall x \subseteq y)\varphi$ [$(\exists x \subseteq y)\varphi$] abbreviates $(\forall x)(x \subseteq y \to \varphi)$ [$(\exists x)(x \subseteq y \;\&\; \varphi)$, resp.].

1.3. $(\exists x \le t)\varphi$ abbreviates $(\exists x)(x \le t \;\&\; \varphi)$, where $s \le t$ is $1 \times s \subseteq 1 \times t$.

1.4. A formula φ is in $\Delta_0^b(\mathcal{P})$ [$\Sigma_1^b(\mathcal{P})$, resp.] if it has been obtained from literals in L($\mathcal{P}$) by $\&$, $\vee$, $\forall\subseteq$, $\exists\subseteq$, [and $\exists\le$, resp.].

1.5. An L($\mathcal{P}$)-formula φ is in s-$\Sigma_1^b(\mathcal{P})$ if it is of the form $(\exists y \le t)\psi$ with $\psi \in$ QF($\mathcal{P}$).

The formulas in $\Delta_0^b(\mathcal{P})$ are exactly the polynomial time computable matrices of [F]. — The theories for binary trees to be investigated contain the basic axioms for the non-logical symbols of L (see [F]), the defining equations for the elements of $\mathcal{P}$ in case the theory is formulated in L($\mathcal{P}$), and the induction principle on notations for classes of formulas $\mathcal{F}$: $\varphi\emptyset \;\&\; (\forall x)(\varphi x \to \varphi x0 \;\&\; \varphi x1) \to (\forall x)\varphi x$ ($\varphi \in \mathcal{F}$). The latter schema is denoted by $\mathcal{F}$-NIA; the resulting theory - always with classical logic — is called ($\mathcal{F}$-NIA).

We formulate a few properties of $\mathcal{P}$ that are provable in (QF($\mathcal{P}$)-NIA).

2. LEMMA.

(i) For every term s of L($\mathcal{P}$) there is a term t of L, such that (QF($\mathcal{P}$)-NIA) proves $s \le t$.

(ii) For any $\varphi_1(\mathbf{x}),\dots,\varphi_n(\mathbf{x}) \in$ QF($\mathcal{P}$) and $f_1,\dots,f_{n+1} \in \mathcal{P}$ there is an $f \in \mathcal{P}$ such that (QF($\mathcal{P}$)-NIA) proves

$$\begin{aligned}(\varphi_1(\mathbf{x}) \;\&\; f(\mathbf{x}) = f_1(\mathbf{x})) &\vee (\neg\varphi_1(\mathbf{x}) \;\&\; \varphi_2(\mathbf{x}) \;\&\; f(\mathbf{x}) = f_2(\mathbf{x}))\\ &\vee (\neg\varphi_1(\mathbf{x}) \;\&\; \neg\varphi_2(\mathbf{x}) \;\&\; \varphi_3(\mathbf{x}) \;\&\; f(\mathbf{x}) = f_3(\mathbf{x}))\\ &\;\vdots\\ &\vee (\neg\varphi_1(\mathbf{x}) \;\&\dots\&\; \neg\varphi_n(\mathbf{x}) \;\&\; f(\mathbf{x}) = f_{n+1}(\mathbf{x})).\end{aligned}$$

(iii) For any $\varphi(\mathbf{x},y) \in$ QF($\mathcal{P}$) there is an $h \in \mathcal{P}$, such that (QF($\mathcal{P}$)-NIA) proves $((\exists y \subseteq x)\,\varphi(\mathbf{x},y) \leftrightarrow \varphi(\mathbf{x},h(\mathbf{x},x)))$.

The last part of the lemma allows us to prove that in (QF($\mathcal{P}$)-NIA) every $\Delta_0^b(\mathcal{P})$-formula is equivalent to a quantifier-free formula; proposition 6 of [F] establishes in turn that in (s-$\Sigma_1^b(\mathcal{P})$-NIA) every $\Sigma_1^b(\mathcal{P})$-formula is equivalent to one in s-$\Sigma_1^b(\mathcal{P})$.

Thus we have:

3. PROPOSITION.

(i) $(\Delta_0^b(\mathcal{P})$-NIA) is equivalent to (QF($\mathcal{P}$)-NIA).

(ii) (s-$\Sigma_1^b(\mathcal{P})$-NIA) is equivalent to ($\Sigma_1^b(\mathcal{P})$-NIA).

Notice that ($\Delta_0^b(\mathcal{P})$-NIA) is Ferreira's PTCA, and (s-$\Sigma_1^b(\mathcal{P})$-NIA) is his PTCA$^+$. Now we turn our attention to bounding the complexity of formulas in derivations. The latter are now presented in a Tait-style calculus as in [Sch]; the induction principle is given equivalently by a rule $\mathcal{F}$-NIR* of the form

$$\frac{\Delta, \neg\varphi x, \varphi x0 \qquad \Delta, \neg\varphi x, \varphi x1}{\Delta, \neg\varphi\emptyset, \varphi s} \quad (\varphi \in \mathcal{F})$$

where s is a term, and x must not occur in the lower sequent. This new formulation of ($\mathcal{F}$-NIA) has two virtues – it is equivalent to the earlier one and allows us to prove partial normalization theorems.

5. DEFINITION .

A derivation in ($\mathcal{F}$-NIA) is called I-normal if and only if all its cuts are either I-cuts or have atomic cut-formulas; where a cut with cut-formula φ is called an I-cut if one of its premises is the conclusion of the induction rule with principal formula φ or $\neg\varphi$.

The standard proof of the normalization theorem for predicate logic can readily be adapted to show that any derivation in ($\mathcal{F}$-NIA) can be I-normalized.

6. THEOREM. (I-normalization) If D is a derivation of Γ in ($\mathcal{F}$-NIA), then there is an I-normal derivation D° of the same endsequent in ($\mathcal{F}$-NIA).

The length $|D^\circ|$ of D° can be bounded by $2_m^{|D|}$, $m = \rho(D) \dot- 1$; the cut-rank function ρ takes into account only the complexity of cuts that are not I-cuts. I-normal derivations do not have the subformula property, but the complexity of formulas occurring in them can nevertheless be bounded significantly.

7. COROLLARY. Let $\mathcal{F}$ and $\mathcal{G}$ be classes of formulas that are closed under substitution. If D is an I-normal derivation of Γ in ($\mathcal{F}$-NIA) with $\Gamma \subseteq \mathcal{G}$, then any formula in D is either atomic or a subformula of an element of $\mathcal{F} \cup \{\neg\varphi : \varphi \in \mathcal{F}\} \cup \mathcal{G}$.

C. EXTRACTING TERMS.

The I-normalization theorem will be used to establish a (generalized) Herbrand-theorem.

8. THEOREM. ($\exists$-inversion) Let Γ contain only existential formulas, and let ψ be quantifier-free; if $\Gamma, (\exists y)\psi y$ is provable in (QF($\mathcal{P}$)-NIA) then there is a term t^* such that $\Gamma, \psi t^*$ is also provable in (QF($\mathcal{P}$)-NIA). (ψ may contain additional variables.)

PROOF. The proof proceeds by induction on I-normal (QF($\mathcal{P}$)-NIA)-derivations D. We focus on the central step, when NIR* is the last rule applied in D. (The other non-trivial cases, e.g. $\exists$-introduction, require definition by cases.)

Then D is of the form

$$D\left\{\begin{array}{c} D_0\left\{\begin{array}{c}\vdots\\ \Delta,\neg\varphi x,\varphi x0,(\exists y)\psi y\end{array}\right. \qquad \left.\begin{array}{c}\vdots\\ \Delta,\neg\varphi x,\varphi x1,(\exists y)\psi y\end{array}\right\}D_1 \\ \hline \underbrace{\Delta,\neg\varphi\emptyset,\varphi s}_{=\Gamma},(\exists y)\psi y \end{array}\right.$$

The induction hypothesis applied to the D_i yields terms $t_i[x]$ and derivations D_i^* of

(1) $\Delta,\neg\varphi x,\varphi xi,\psi t_i[x]$ $(i=0,1)$.

Obviously (QF($\mathscr{P}$)-NIA) proves

(2) $\neg\varphi\emptyset,\varphi s,\exists x\subseteq s[\varphi x\,\&\,\neg(\varphi x0\,\&\,\varphi x1)]$.

By Lemma 2(iii) there is an $h\in\mathscr{P}$, such that (QF($\mathscr{P}$)-NIA) proves

(3) $\neg\exists x\subseteq s[\varphi x\,\&\,\neg(\varphi x0\,\&\,\varphi x1)],\ \varphi h(s)\,\&\,\neg(\varphi h(s)0\,\&\,\varphi h(s)1)$.

From (2) and (3) we obtain:

(4) $\neg\varphi\emptyset,\varphi s,\varphi h(s)$,

(5) $\neg\varphi\emptyset,\varphi s,\neg\varphi h(s)0,\neg\varphi h(s)1$.

From (1) (with h(s) substituted for x) and (5) we obtain
$\neg\varphi\emptyset,\ \varphi s,\Delta,\neg\varphi h(s),\ \psi t_0[h(s)],\psi t_1[h(s)]$ and then (by (4))
$\Delta,\ \neg\varphi\emptyset,\varphi s,\ \psi t_0[h(s)],\psi t_1[h(s)]$.
This together with Lemma 2(ii) gives us an $f\in\mathscr{P}$ such that (QF($\mathscr{P}$)-NIA) proves
$\Delta,\neg\varphi\emptyset,\varphi s,\psi f(s)$. Q.E.D.

The $\exists$-inversion is crucial for establishing the main conservation result.

9. THEOREM. (s-$\Sigma_1^b(\mathscr{P})$-NIA) is conservative over (QF($\mathscr{P}$)-NIA) with respect to Π_2^0-sentences φ of the form $(\forall x)(\exists y)\varphi^*(x,y)$ with $\varphi^*\in$ QF($\mathscr{P}$).

PROOF. As (QF($\mathscr{P}$)-NIA) is contained in (s-$\Sigma_1^b(\mathscr{P})$-NIA) we have to show only that every Π_2^0-sentence provable in the latter theory is provable in the former. This is achieved by transforming any I-normal derivation D in (s-$\Sigma_1^b(\mathscr{P})$-NIA) of a sequent Δ, where Δ contains only existential formulas, into a derivation D' of Δ in (QF($\mathscr{P}$)-NIA). We proceed by induction on the number $\#$ of applications of NIR* in D, not counting for sure NIR*-instances with formulas in QF($\mathscr{P}$). - The case $\#=0$ is trivial. So let $\#$ be m+1 and consider an uppermost instance of NIR* with ψ of the form $(\exists y)(y\le t[x]\,\&\,\psi^*yx)$, where ψ^* is in QF($\mathscr{P}$); both ψ^* and t may contain additional variables. The subderivation E of D determined by that inference is of the form

$$\left.\begin{array}{c} E_0\left\{\begin{array}{c}\vdots\\ \Gamma,\neg\psi x,\psi x0\end{array}\right. \qquad \left.\begin{array}{c}\vdots\\ \Gamma,\neg\psi x,\psi x1\end{array}\right\}E_1 \\ \hline \Gamma,\neg\psi\emptyset,\psi s\end{array}\right\}E\ .$$

Taking into account the form of ψ and the fact that D is an I-normal derivation in (s-$\Sigma_1^b(\mathscr{P})$-NIA), we can obtain (recalling corollary 7) by repeated $\forall$-inversion from the E_i derivations of $\Gamma^*,\ \neg(y\le t[x]\,\&\,\psi^*yx),\psi xi$, where Γ^* contains only existential formulas. $\exists$-inversion yields terms $t_i[y,x]$ and derivations in (QF($\mathscr{P}$)-NIA) of

$(\square_i)$ $\Gamma^*,\neg(y\le t[x]\,\&\,\psi^*yx),t_i[y,x]\le t[xi]\,\&\,\psi^*t_i[y,x]xi$.

Now we define a function f by iteration with bound $t[x0]t[x1]$ (using Lemma 2(i) and (ii) to bring the definition into the required form): $f(y,\emptyset)=y$, $f(y,xi)=t_i[f(y,x),x]$. From the derivations leading to the $\square_i$ and this definition we get derivations of

$$\Gamma^*, \neg(f(y,x) \leq t[x] \,\&\, \psi^* f(y,x)x),\ f(y,xi) \leq t[xi] \,\&\, \psi^* f(y,xi)xi$$

and by QF($\mathcal{P}$)-NIR* of

$$\Gamma^*, \neg(y \leq t[\emptyset] \,\&\, \psi^* y\emptyset),\ f(y,s) \leq t[s] \,\&\, \psi^* f(y,s)s \ .$$

With a little bit of logic we finally obtain a derivation E' in (QF($\mathcal{P}$)-NIA) of $\Gamma, \neg\psi\emptyset, \psi s$. Replace E in D by E'. The resulting derivation has only m applications of s-Σ_1^b($\mathcal{P}$)-NIR* and the induction hypothesis yields the above claim. Q.E.D.

D. CHARACTERIZING $\mathcal{P}$.

Since for every L($\mathcal{P}$)-term t[x] the function $\lambda x.t[x]$ is in $\mathcal{P}$, theorem 8 implies that the provably recursive functions of (QF($\mathcal{P}$)-NIA) are exactly the polynomial time computable ones. Using also theorem 9 and proposition 4 we obtain the sought after characterization result.

10. THEOREM.

$\mathcal{P}$ is exactly the class of provably recursive functions of (Σ_1^b($\mathcal{P}$)-NIA).

REMARKS.

(i) [F] establishes that (Σ_1^b($\mathcal{P}$)-NIA) is a conservative extension of (Σ_1^b-NIA); thus the theorem holds also for the latter theory.

(ii) The Herbrand-analysis given in C is insensitive to extensions of the various theories by Π_1^0-sentences. Thus, the main results hold also for Π_1^0-extensions of the theories involved.

REFERENCES

[B] ***Samuel Buss***, Bounded Arithmetic, Bibliopolis, Napoli, 1986.

[F/S] ***Solomon Feferman and Wilfried Sieg***, "Proof theoretic equivalences between classical and constructive theories for analysis", Springer Lecture Notes in Mathematics, vol. 897, (1981), pp. 78-142.

[F] ***Fernando Ferreira***, "Polynomial time computable arithmetic", this volume.

[L] ***Horst Luckhardt***, "Herbrand-Analysen zweier Beweise des Satzes von Roth: polynomiale Anzahlschranken", to appear in the Journal of Symbolic Logic.

[Sch] ***Helmut Schwichtenberg***, "Proof theory: some applications of cut-elimination", Handbook of Math.Logic, J. Barwise (ed.), NHPC, Amsterdam 1977, pp. 867-895.

[S1] ***Wilfried Sieg***, "Fragments of arithmetic", Annals of Pure and Applied Logic, 28 (1985), pp. 33-71.

[S2] ***Wilfried Sieg***, "Derivations as computations", manuscript.

Wilfried Buchholz
Mathematisches Institut
Ludwig-Maximilians-Universität
8000 MÜNCHEN 2, West-Germany

Wilfried Sieg
Department of Philosophy
Carnegie Mellon University
PITTSBURGH, PA 15213, USA