in Logic from Computer Science, Proc Workshop held Nov 13-17, 1989, ed. Y N Moschovakis, Mathematical Sciences Research Institute Publications 21, (1992), Springer-Verlag, pp. 287-293

NO COUNTER-EXAMPLE INTERPRETATION AND INTERACTIVE COMPUTATION

JAN KRAJÍČEK

ABSTRACT. No counter-example interpretation for bounded arithmetic is employed to derive recent witnessing theorem for S_2^{i+1}, functions $\square_{i+1}^p$-computable with counterexamples are shown to include all $\square_{i+2}^p$-functions, and two separation results for fragments of $S_2(\alpha)$ are proved.

Buss [1,2] has shown that functions $\exists\Sigma_{i+1}^b$-definable in S_2^{i+1} or T_2^i are precisely $\square_{i+1}^p$-functions. This was in [3] generalized in the following way.

Assume $T_2^i \vdash \exists x \forall y \exists z A(a,x,y,z)$, where A is a Σ_{i+1}^b-formula. Then function F assigning to a some b such that $\forall y \exists z A(a,b,y,z)$ is computable by a $\square_{i+1}^p$-algorithm which may ask constantly many times for counter-examples to $\forall y \exists z A(a,b,y,z)$ (i.e. for c such that $\neg \exists z A(a,b,c,z)$). In these questions b varies but a is fixed.

Pudlák [6] has recently proved similar theorem for S_2^{i+1}: the assumption $S_2^{i+1} \vdash \exists x \forall y \le a A(a,x,y)$ (A again Σ_{i+1}^b) implies that function F assigning to a some b such that $\forall y \le a A(a,b,y)$ is computable by a $\square_{i+1}^p$-algorithm which may ask for any (polynomial) number of counter-examples to $\forall y \le a A(a,b,y)$. Here is a simple proof of this statement.

Extending the language of S_2^1 by some $\square_{i+1}^p$-functions and adding some universal axioms about them we may form theory $S_2^1(PV_{i+1})$, a conservative extension of S_2^{i+1}. We may also assume that A is existential.

As a formula implies its Herbrand's form, the assumption

$$S_2^{i+1} \vdash \exists x \forall y \le A(a,x,y)$$

implies

$$S_2^1(PV_{i+1}, f) \vdash \exists x, f(a,x) \le a \supset A(a,x,f(a,x)),$$

where f is a new function symbol.

By (relativization of) Buss's witnessing theorem there is functional $F(a, f)$ which satisfies:

$$f(a, F(a, f)) \leq a \supset A(a, F(a, f), f(a, F(a, f))),$$

and which is computable by a deterministic algorithm which may ask for values of some $\Box^p_{i+1}$-functions (from the language of $S^1_2(PV_{i+1})$) and for values of $f(a, x)$. Moreover, if f is of polynomial growth then the algorithm computing F runs in time polynomial in $|a|$. We may therefore call F a $\Box^p_{i+1}$-functional.

The algorithm computing F is the algorithm required in Pudlák's statement. This is because if f is a function computing some counter-examples:

$$f(a, b) := \begin{cases} \text{some } c \leq a, \text{ s.t. } \neg A(a, b, c) \\ a + 1, \text{ if } \forall y \leq a A(a, b, y) \end{cases}$$

then formula:

$$f(a, b) \leq a \supset A(a, b, f(a, b))$$

implies:

$$\forall y \leq a A(a, b, y).$$

(The additional property that a is fixed in the queries follows as we can treat a as a constant.)

The same argument works also if y in $\forall y$ is not bounded. But the run time of an algorithm computing F is then bounded only by a polynomial in $|a| + \sum_i |f(a, u_i)|$, where $f(a, u_i)$'s are all function values $f(a, x)$ asked for in the computation.

The statement clearly generalizes to arbitrary quantifier complexity: the assumption

$$S^{i+1}_2 \vdash \exists x_1 \forall y_1 \ldots \exists x_k \forall y_k A(a, \vec{x}, \vec{y})$$

(bounds to y_j's implicitly in A) implies existence of $\Box^p_{i+1}$-functionals $F_1(a, \vec{f}), \ldots, F_k(a, \vec{f})$ such that for any a and $\vec{f}$ it holds:

$$A(a, \ldots x_\ell / F_\ell(a, \vec{f}), \ldots, y_j / f_j(a, F_1(a, \vec{f}), \ldots, F_j(a, \vec{f})),$$

The computation of F_ℓ's with particular f_j's computing counterexamples can be described again as an interactive computation.

The characterization of the witnessing functions in the T^i_2 case was in [3] used for a conditional separation of T^i_2 and S^{i+1}_2. The motivation for studying the S^{i+1}_2 case is the problem of separation of S^{i+1}_2 and T^{i+1}_2. Here however, a sceptical tone comes from the observation that any $\Box^p_{i+2}$-function can be computed in the interactive manner associated with S^{i+1}_2, while Skolem functions for T^{i+1}_2 are also $\Box^p_{i+2}$. This is seen as follows.

For M a deterministic oracle machine and $B(u) = \exists v C(u, v)$ a $\sum^p_{i+1}$-oracle take formula $D(a) = \exists x \forall \langle i, y \rangle A(a, x, \langle i, y \rangle)$ (bounds to v and $\langle i, y \rangle$ are implicitly in C and A resp.) where formula A is the conjunction of:

(i) $|x| \leq |a|^k$ ($|a|^k$ a time bound),
(ii) "x is a computation of M with some oracle",
(iii) "if the i-th step of computation x is a negative answer to an oracle query $[B(u_i)?]$ then either $\neg C(u_i, y)$ or ($\exists j < i$, "j-th step of x is also a negative answer to oracle query $[B(u_j)?]$ but $B(u_j)$ holds"),
(iv) "all positive answers to oracle queries are correct".

Formula A is clearly $\sum^b_{i+1}$.

Now consider the following algorithm. Take b_0 the computation of M on input a where we answer all oracle queries negatively, and ask for a counterexample to $\forall \langle i, y \rangle A(a, b_0, \langle i, y \rangle)$. If counterexample $\langle i_0, y_0 \rangle$ is provided then the negative answer to oracle query $[B(u_{i_0})?]$ in step i_0 was the first incorrect one (and y_0 witnesses the positive answer). Construct computation b_1 identical with b_0 till step $i_0 - 1$, answering oracle query $[B(u_{i_0})?]$ positively and all later queries negatively. Then ask again for a counterexample to $\forall \langle i, y \rangle A(a, b_1, \langle i, y \rangle)$. If $\langle i_1, y_1 \rangle$ is provided, step i_1 is the first incorrect one (a negative answer to an oracle query $[B(u_{i_1})?]$) and so take b_2 identical with b_1 till step $i_1 - 1$, answering $[B(u_{i_1})?]$ positively (with y_1 a witness to it), and all later queries, negatively.

In this way construct computations $b_0, b_1, b_2, \ldots$, with b_m correct at least till step m. Thus for $m := |a|^k$, b_m is the correct computation of M^B on input a. Output of M^B is read from b_m.

If unable to separate S^{i+1}_2 from T^{i+1}_2, a natural problem to look at is a separation of relativized versions of S^{i+1}_2 and T^{i+1}_2. Buss (unpublished) showed that $T^1_2(f)$ is not $\sum^b_1(f)$-conservative over $S^1_2(f)$ and Pudlák [6] employed his witnessing theorem to show that $S^{i+1}_2(\alpha) \neq T^{i+1}_2(\alpha)$, for $i = 0, 1$. Here I give an alternative proof of Buss's result and a strengthening of Pudlák's result for $i = 1$.

Theorem.

(a) *The following sequent is provable in $T^1_2(\alpha, f)$ but not in $S^1_2(\alpha, f)$:*

$$\alpha(0,0), \forall x, y \le a((\alpha(x,y) \wedge x \le y) \supset (\alpha(f(x,y), y+1) \wedge f(x,y) \le y+1)) \to \exists u \le a\ \alpha(u,a).$$

(b) *The following sequent is provable in $T^2_2(\alpha)$ but not in $S^2_2(\alpha)$:*

$$\forall u, v < a^2 \forall w < a(\alpha(u,w) \wedge \alpha(v,w) \supset u = v),$$
$$\forall u < a^2 \forall v, w < a(\alpha(u,v) \wedge \alpha(u,w) \supset v = w) \to \exists x < a^2 \forall y < a \neg\alpha(x,y).$$

Remark. The sequent from (b) is $\sum^b_2(\alpha)$ while $S^2_2(\alpha)$-axioms are $\sum^b_3(\alpha)$; in this respect (b) improves upon Pudlák's result.

Proof. In both cases we use a relativization of Buss's witnessing theorem.

(a) The sequent is clearly provable in $T^1_2(\alpha, f)$ by induction for formula $\exists u \le a\ \alpha(u,a)$. To show that the sequent is not provable in $S^1_2(\alpha, f)$ it is enough to show that for each polynomial time oracle machine $M^{\alpha,f}$ there exist $\alpha \subseteq \omega^2, a \in \omega$ and $f : \omega^2 \to \omega$ of polynomial growth such that $M^{\alpha,f}(a)$ does not witness the sequent.

Fix machine $M^{\alpha,f}$ and take $a \in \omega$ sufficiently large. We start the computation of $M^{\alpha,f}$ on a; when answering oracle queries we shall assign truth values (resp. values) to some $\alpha(x,y)$ (resp. some $f(x,y)$), for $x \le y \le a$.

(0) Assign to $\alpha(0,0)$ TRUE.

(i) Query $[\alpha(x,y)?]$: If for all $t \le y$, $t \ne x$ to $\alpha(t,y)$ is already assigned truth value FALSE, assign to $\alpha(x,y)$ TRUE and answer YES. Otherwise assign FALSE and answer NO.

(ii) Query $[f(x,y) =?]$: Consider three cases.

(1) To $\alpha(x,y)$ is assigned value TRUE. Choose some $t \le y+1$ such that to $\alpha(t, y+1)$ is assigned TRUE if it exists, or otherwise choose any $t \le y+1$ such that $\alpha(t, y+1)$ has not value assigned yet. Put $f(x,y) := t$ and assign to $\alpha(t, y+1)$ value TRUE.

(2) To $\alpha(x,y)$ is assigned value FALSE. Choose some $t \le y+1$ such that to $\alpha(t, y+1)$ is assigned FALSE if it exists, or otherwise choose any $t \le y+1$ such that $\alpha(t, y+1)$ has not value assigned yet. Put $f(x,y) := t$ and assign to $\alpha(t, y+1)$ value FALSE.

(3) $\alpha(x,y)$ has no value assigned yet. Assign to it some value according to (i) and then define $f(x,y)$ following (1) or (2) above.

The following claim is straightforward.

Claim. *To $\alpha(x,y)$ cannot be assigned value TRUE during answers to first y oracle queries.*

Hence obviously $M^{\alpha,f}(a)$ cannot find witness for the succedent. If the output is pair (x,y) such that $x \le y \le a$, $\alpha(x,y)$ is assigned TRUE then either $f(x,y)$ is correctly defined $\le y+1$ and to $\alpha(f(x,y), y+1)$ is assigned TRUE too, or $f(x,y)$ is undefined. Then define it following (iii). Take α to be those pairs (x,y) such that to $\alpha(x,y)$ is assigned TRUE and f to be any extension of the partial function constructed during the computation. Clearly $M^{\alpha,f}(a)$ does not witness the sequent.

This proves clause (a).

(b) Assume $\alpha \subseteq a^2 \times a$ does not satisfy the sequent. Then α is a graph of a $1-1$ map from a^2 into a. In Paris-Wilkie-Woods [5, Thm. 1] it is proved in $I\Delta_0 + \Omega_1$ that there cannot be a Δ_0-definable, $1-1$ map from a^2 into a. Their proof readily formalizes in $S^3_2(\alpha)$ and hence in $T^2_2(\alpha)$ too. (I do not know if this remains true if we drop the second formula from the antecedent.)

To show that $S^2_2(\alpha)$ does not prove the sequent it is enough to show that for any polynomial time oracle machine M^B, and any $\sum^p_1(\alpha)$-predicate B there are $\alpha \subseteq \omega^2$ and $a \in \omega$ such that $M^B(a)$ does not witness the sequent.

Choose $a \in \omega$ sufficiently large. Assume that the $\sum^p_1(\alpha)$-oracle B has the form:

$$B(b) = \exists w \le t(b)\ N^\alpha(w,b),$$

where $N^\alpha(w,b)$ formalizes

"w is an accepting computation of oracle machine N^α on input b".

We start the computation of M^B on a. During the computation we shall answer oracle queries and also construct partial approximations to $\alpha : \alpha^\pm_0 \subseteq \alpha^\pm_1 \subseteq \cdots \subseteq a^2 \times a$.

Put $\alpha^-_0 = \alpha^+_0 = \emptyset$. Let $[B(b_i)?]$ be the i-th oracle query. Consider two cases.

(i) There exist $\beta \subseteq a^2 \times a$ and $w \le t(b_i)$ such that:

(1) $\beta \supseteq \alpha^+_{i-1}$ and $\beta \cap \alpha^-_{i-1} = \emptyset$,

(2) $N^\beta(w, b_i)$ holds,

(3) β is a graph of a partial $1-1$ function from a^2 to a.

Answer YES. Computation w contains at most $|a|^k$ oracle queries about β (some fixed $k \in \omega$). Add pairs (c,d) to α^+_{i-1} resp. to α^-_{i-1} to form $\alpha^{\pm}_i$, according to whether the answer to oracle query $[\beta(c,d)?]$ in w was affirmative or negative.

In particular, $\mathrm{card}((\alpha^+_i \cup \alpha^-_i)\setminus(\alpha^+_{i-1} \cup \alpha^-_{i-1})) \leq |a|^k$.

(ii) There are no such β and w. Answer NO and put $\alpha^{\pm}_i := \alpha^{\pm}_{i-1}$.

Put $\alpha := \bigcup_{i \leq |a|^\ell} \alpha^+_i$ where $|a|^\ell$ is the time bound of M^B. α satisfies the antecedent and so if $M^B(a)$ should witness the sequent it must output $x < a^2$ such that $\forall y < a \neg\alpha(x,y)$. But then we can always find $y < a$, $(x,y) \notin \bigcup_{i \leq |a|^\ell} \alpha^-_i$ and add pair (x,y) into α.

This proves clause (b). □

The sequent from clause (a) is a herbrandization of induction axiom for formula $\exists u \leq a\ \alpha(u,a)$. It would seem natural to conjecture that a herbrandization of induction axiom for $\sum^b_i(\alpha)$-formula

$$\exists x_1 \leq a \forall y_1 \leq a \,.\quad \alpha(\vec{x},\vec{y},a)$$

(i alternating quantifiers), namely:

$$\alpha(\vec{0},\vec{0},0), \forall b, x_1, .\ ., x_m, t_1, \ldots, t_n \leq a[\hat{\alpha}(\vec{x}, y_j/f_j, b) \supset \hat{\alpha}(z_k/g_k, \vec{t}, b+1)] \rightarrow \exists u_1, \ldots, u_m \leq a\ \hat{\alpha}(\vec{u}, v_\ell/h_\ell, a),$$

where:

(0) $m = \frac{\ulcorner i \urcorner}{2}$, $n = \frac{i}{\llcorner 2 \lrcorner}$ and $\hat{\alpha}$ is the formula

$$(x_1 \leq b \wedge (y_1 \leq b \supset (.\quad (\alpha(\vec{x},\vec{y},b)\,.\quad),$$

(i) function f_j depends on $b, x_1, \ldots, x_j, t_1, \ldots, t_{j-1}$,
(ii) function g_k depends on $b, x_1, \ldots, x_k, t_1, \ldots, t_{k-1}$,
(iii) function h_ℓ depends on $a, u_1, \ldots, u_\ell$,

is not provable in $S^i_2(\alpha, \vec{f}, \vec{g}, \vec{h})$. However, this is not true. All these herbrandizations are provable already in $T^1_2(\alpha, \vec{f}, \vec{g}, \vec{h})$.

Remark. The problem whether S^{i+1}_2 equals T^{i+1}_2 was from a different perspective studied in [4]. Following that paper, Theorem above can be interpreted as results about structure of proofs in predicate calculus.

REFERENCES

1. S. Buss, *Bounded Arithmetic*, Bibliopolis, Naples, 1986.
2. S. Buss, *Axiomatization and conservation results for fragments of bounded arithmetic*, Proc. Workshop in Logic and Computation, Contemporary Mathematics AMS (to appear).
3. J. Krajíček, P. Pudlák and G. Takeuti, *Bounded arithmetic and the polynomial hierarchy*, Annals of Pure and Applied Logic (to appear).
4. J. Krajíček and G. Takeuti, *On induction-free provability*, Discrete Applied Mathematics (to appear).
5. J. Paris, A. Wilkie and A. Woods, *Provability of the pigeon-hole principle and the existence of infinitely many primes*, Journal of Symbolic Logic **53** no. 4 (1988), 1235–1244.
6. P. Pudlák, *Some relations between subsystems of arithmetic and complexity of computations*, this volume.

MATHEMATICAL INSTITUTE, CZECHOSLOVAK ACADEMY OF SCIENCES, ŽITNÁ 25, 115 67, PRAGUE-1