Annals of Pure and Applied Logic 52 (1991) 143–153
North-Holland

Bounded arithmetic and the polynomial hierarchy

Jan Krajíček
University of Illinois, Urbana, IL 61801, USA, and Mathematical Institute, Prague, Czechoslovakia

Pavel Pudlák
Mathematical Institute, Prague, Czechoslovakia

Gaisi Takeuti
University of Illinois, Urbana, IL 61801, USA

Communicated by D. van Dalen
Received 21 May 1989
Revised 25 January 1990

Abstract

Krajíček, J., P. Pudlák and G. Takeuti, Bounded arithmetic and the polynomial hierarchy, Annals of Pure and Applied Logic 52 (1991) 143–153.

(1) $T_2^i = S_2^{i+1}$ implies $\Sigma_{i+1}^p \subseteq \Delta_{i+1}^p/\text{poly}$.
(2) $S_2(\alpha)$ and $I\Delta_0(f)$ are not finitely axiomatizable.
The main tool is a Herbrand-type witnessing theorem for $\exists\forall\exists\Pi_i^b$-formulas provable in T_2^i where the witnessing functions are $\square_{i+1}^p$.

There are two main systems of bounded arithmetic, $I\Delta_0$ and S_2 studied in [9, 10] and [2] respectively. The major open questions in this area are whether $I\Delta_0$ or S_2 are finitely axiomatizable and whether various fragments of these theories are somehow conservative one over another.

The known results relevant to these questions are the following:

(a) If $I\Delta_0$ (resp. S_2) proves that the polynomial hierarchy PH collapses, then $I\Delta_0$ (resp. S_2) is finitely axiomatizable, cf. [9].

(b) S_2^{i+1} is $\forall\Sigma_{i+1}^b$-conservative over T_2^i $(i \geq 1)$, cf. [3].

(c) $\forall\Sigma_j^b$-consequences of T_2^i are finitely axiomatizable $(i \geq 1, j \geq 2)$, cf. [8].

(d) $S_2^0 \neq T_2^0$, cf. [12].

(e) If S_2 is Π_1^0-conservative over $I\Delta_0$ (even over $I\Delta_0$ augmented by a form of the pigeonhole principle), then $I\Delta_0$ is not finitely axiomatizable, cf. [8].

There is an evident similarity between fragments of S_2 and levels of PH, and between the separation problems for them. This is supported by the theorem of [2] that Σ_i^b-definable functions in S_2^i are precisely $\square_i^p$-functions. However, no relation of the problem whether S_2 is finitely axiomatizable (i.e., whether the hierarchy of fragments S_2^i collapses) to the problem whether PH collapses was known.

Here we prove such a relation; we show that $T_2^i = S_2^{i+1}$ implies $\Sigma_{i+1}^p \subseteq \Delta_{i+1}^p/\text{poly}$. The later inclusion implies that $\Sigma_{i+2}^p = \Pi_{i+2}^p$, cf. [6], and thus the collapse of S_2 implies the collapse of PH.

For this result we use a Herbrand-type witnessing theorem for $\exists\forall\exists\Pi_i^b$-formulas provable in T_2^i where the witnessing functions are in $\square_{i+1}^p$. This theorem extends the main theorem of [2].

The whole proof easily relativizes and as there is an oracle A such that PH^A does not collapse (cf. [5] or [14]), it follows that $S_2(\alpha)$ is not finitely axiomatizable. However, it is considerably simpler to construct an oracle sufficient for separation of $T_2^1(\alpha)$ and $S_2^2(\alpha)$, and we present this construction too.

The paper is organized as follows. The witnessing theorem is proved in Section 1. We actually prove a stronger statement than is needed later and we give two independent proofs of it, a proof-theoretic and a model-theoretic.

In Section 2 we study a computational principle suggested by the witnessing theorem and we show that it implies $\Sigma_{i+1}^p \subseteq \Delta_{i+1}^p/\text{poly}$. In this section we also construct an oracle for which an instance of the principle is false.

In the last section we show that $T_2^i = S_2^{i+1}$ implies that the computational principle is true which entails the results.

We use the notation of [2] and we assume familiarity with that paper. In particular, recall that $\square_{i+1}^p$-functions are functions computable by a polynomial time Turing machine using a Σ_i^p-oracle.

1. Herbrand-type witnessing theorem

Buss [3] has shown that S_2^{i+1} is $\forall\Sigma_{i+1}^b$-conservative over T_2^i by showing that $\square_{i+1}^p$-functions are in a natural way Σ_{i+1}^b-definable in T_2^i. As axioms of T_2^i are $\forall\Sigma_{i+1}^b$ it follows that Skolem functions for T_2^i are $\square_{i+1}^p$ and that T_2^i is equivalent to a universal theory with function symbols (infinitely many) for $\square_{i+1}^p$-functions. It is not difficult to give an explicit axiomatization of such a theory—call it PV_{i+1}—in the style of Cook's theory PV [4]. PV_{i+1} has (inductively defined) characteristic functions of Σ_i^p-predicates, is closed under the definition by cases and under the limited recursion on notation, and contains BASIC and all equality axioms. Moreover, PV_{i+1} contains a form of induction; for $\varphi(x)$ an open formula define function $h(b, u)$ by:

(a) $h(b, 0) = (0, b)$,

(b) if $h(b, \lfloor \frac{1}{2}u \rfloor) = (x, y)$ and $u > 0$, then put:

$$\begin{aligned} h(b,u) &:= \left(\left\lceil\frac{x+y}{2}\right\rceil, y\right) && \text{if } \left\lceil\frac{x+y}{2}\right\rceil < y \text{ and } \varphi\left(\left\lceil\frac{x+y}{2}\right\rceil\right), \\ &:= \left(x, \left\lceil\frac{x+y}{2}\right\rceil\right) && \text{if } x < \left\lceil\frac{x+y}{2}\right\rceil \text{ and } \neg\varphi\left(\left\lceil\frac{x+y}{2}\right\rceil\right), \\ &:= (x, y) && \text{otherwise.} \end{aligned}$$

Then PV_{i+1} contains an axiom:

$$(\varphi(0) \wedge \neg\varphi(b) \wedge h(b, b) = (x, y)) \rightarrow (x + 1 = y \wedge \varphi(x) \wedge \neg\varphi(y)).$$

It is not difficult to show that PV_{i+1} is conservative over T_2^i (see also the second proof of Theorem A).

Theorem A. *Let* $i \geq 1$ *and let* $\varphi(a, x, y)$ *be a* $\exists\Pi_i^p$*-formula. Suppose:*

$$T_2^i \vdash \exists x\, \forall y\, \varphi(a, x, y).$$

Then there are $\square_{i+1}^p$*-functions* $f_1(a), f_2(a, b_1), \ldots, f_k(a, b_1, \ldots, b_{k-1})$ *with the free variables displayed such that*

$$T_2^i \vdash \varphi(a, f_1(a), b_1) \vee \varphi(a, f_2(a, b_1), b_2) \vee \cdots \varphi(a, f_k(a, b_1, \ldots, b_{k-1}), b_k).$$

For $i = 0$ *the same is true with* PV_1 $(=\forall\Sigma_1^b(S_2^1))$ *replacing* T_2^0.

Recall that in T_2^i we can talk about $\square_{i+1}^p$-functions. We give two independent proofs of this theorem.

Proof I. Let $\varphi(a, x, y)$ be of the form

$$\exists z\, \psi(a, x, y, z),$$

where ψ is Π_i^b. ψ is in PV_{i+1} equivalent to $g(a, x, y, z) = 1$, where g is the characteristic function of ψ.

From the assumption of the theorem we have:

$$PV_{i+1} \vdash \exists x\, \forall y\, \exists z\, g(a, x, y, z) = 1.$$

PV_{i+1} is a universal theory and thus we can apply Gentzen's midsequent theorem, cf. [13], (or equivalently Herbrand's theorem) to find PV_{i+1}-terms t_u and $s_{u,v}$ such that (after possible renaming of free variables) the disjunction:

$$(g(a, t_1(a), b_1, s_{1,1}) = 1 \vee \cdots \vee g(a, t_1(a), b_1, s_{1,n}) = 1)$$
$$\vee \cdots \vee$$
$$(g(a, t_k(a, b_1, \ldots, b_{k-1}), b_k, s_{k,1}) = 1 \vee \cdots g(a, t_k(a, b_1, \ldots, b_{k-1}), b_k, s_{k,n}) = 1)$$

is provable in PV_{i+1} (terms $s_{u,v}$ generally depend on all $\boldsymbol{a}$, $\boldsymbol{b}$, and t_u depends only on $a, b_1, \ldots, b_{u-1}$).

Now existentially quantify terms $s_{u,v}$ and contract occurrences of $\exists z\;\; g(a, t_j, b_j, z) = 1$, for $1 \leq j \leq k$. The required functions f_j are those defined by terms t_j. □

For the second proof we shall need the following lemma.

Lemma 1.1. *Let* $\mathfrak{M}$ *be a model of* T_2^i *(or of* $\forall\Sigma_1^b(S_2^1)$ *in the case* $i = 0$*) and let* $\mathfrak{M}^* \subseteq \mathfrak{M}$ *be a subset closed under all (standard)* $\square_{i+1}^p$*-functions definable in* $\mathfrak{M}$ *with* *parameters from* $\mathfrak{M}^*$. *Then*

(1) $\mathfrak{M}^*$ *is a substructure of* $\mathfrak{M}$ *and* $\mathfrak{M}^* \prec_{\Sigma_i^b} \mathfrak{M}$,

(2) $\mathfrak{M}^* \models T_2^i$ (*or* $\forall\Sigma_1^b(S_2^1)$).

Proof. (1) is obvious as Skolem functions for Σ_i^b-formulas are Σ_{i+1}^b-definable in T_2^i and thus are in $\square_{i+1}^p$.

For (2) take $\varphi(x) \in \Sigma_i^b$ with parameters from $\mathfrak{M}^*$ and $b \in \mathfrak{M}^*$. We want to show that:

$$\mathfrak{M}^* \models \neg\varphi(0) \vee \varphi(b) \vee \exists x < b\ (\varphi(x) \wedge \neg\varphi(x+1)).$$

Since $\mathfrak{M}^* \prec_{\Sigma_i^b} \mathfrak{M}$ it suffices to find a $\square_{i+1}^p$-function f such that if $\varphi(0) \wedge \neg\varphi(b)$, $f(b)$ is such an $x < b$ where the induction for φ fails. Put $f(b) :=$ 'first component of $h(b, b)$', where h is the function defined before Theorem A. □

Proof II. Assume on the contrary that for no $f_1, \ldots, f_k \in \square_{i+1}^p$, T_2^i proves the disjunction required by the theorem.

Take some enumeration $f_0, f_1, f_2, \ldots$ of all $\square_{i+1}^p$-functions having the properties:

(i) The jth function f_j depends on $\leqslant j$ arguments.

(ii) Each $\square_{i+1}^p$-function occurs in the list infinitely many times.

By a compactness argument the theory

$$T_2^i + \neg\varphi(c, f_1(c), d_1) + \cdots + \neg\varphi(c, f_j(c, d_1, \ldots, d_{j-1}), d_j) + \cdots$$

is consistent, where $c, d_1, d_2, \ldots$ are new constants.

Let $\mathfrak{M}$ be a model of this theory and let $\mathfrak{M}^* \subseteq \mathfrak{M}$ be

$$\mathfrak{M}^* = \{f_1(c), f_2(c, d_1), f_3(c, d_1, d_2), \ldots\}.$$

As the projections are $\square_{i+1}^p$ and as each function occurs infinitely many times we have:

(a) $c, d_1, d_2, \ldots \in \mathfrak{M}^*$,

(b) $\mathfrak{M}^*$ is closed under ($\mathfrak{M}$-definable, standard) $\square_{i+1}^p$-functions.

Hence by Lemma 1.1, $\mathfrak{M}^* \models T_2^i$ and $\mathfrak{M}^* \prec_{\Sigma_i^b} \mathfrak{M}$. But then it holds:

$$\mathfrak{M}^* \models \forall x\ \exists y\ \neg\varphi(c, x, y),$$

for $x = f_j(c, d_1, \ldots, d_{j-1})$ take $y := d_j$. This contradicts the hypothesis of the theorem. □

As already mentioned we shall need Theorem A only for the case $\exists x\ \forall y\ \varphi \in \Sigma_{i+2}^b$.

2. A computational complexity principle

Consider the following type of computational problem. For some fixed binary predicate $P(x, y)$, given a, find b such that:

(i) $(|b| \leq |a| \wedge P(a, b)) \vee b = 0$,

(ii) whenever $|b| < |c| \leq |a|$ then $\neg P(a, c)$.

A prominent example is when $P(x, y)$ is the relation "y is a clique in graph x"; here the problem is to find a clique of maximum size.

We will consider the following computational complexity principle associated with the above problem. This principle is inspired by Theorem A. Π_0^p denotes the class of polynomial time predicates.

Principle $\Omega(i)$. For any relation $P(x, y) \in \Pi_i^p$ there are $\square_{i+1}^p$-functions

$$f_1(a), f_2(a, b_1), \ldots, f_k(a, b_1, \ldots, b_{k-1})$$

which solve the problem above in the interactive manner of Theorem A. That is, if we write $P^*(x, y, z)$ for the conjunction:

$$|y| \leq |x| \wedge (y = 0 \vee P(x, y)) \wedge (|y| < |z| \leq |x| \rightarrow \neg P(x, z))$$

then the following is true:

either $\forall z\, P^*(a, f_1(a), z)$ is true, *or* if b_1 is s.t. $\neg P^*(a, f_1(a), b_1)$
then $\forall z\, P^*(a, f_2(a, b_1), z)$ is true, *or* if b_2 is s.t. $\neg P^*(a, f_2(a, b_1), b_2)$
then $\forall z\, P^*(a, f_3(a, b_1, b_2), z)$ is true, *or* $\cdots$
$\cdot$
then $\forall z\, P^*(a, f_k(a, b_1, \quad, b_{k-1}), z)$ is true. □

Lemma 2.1. *Principle $\Omega(i)$ is implied by $\Sigma_{i+1}^p = \Delta_{i+1}^p$*

Proof. Use binary search. Principle $\Omega(i)$ holds with $k = 1$. □

More interesting is the next statement.

Lemma 2.2. *Principle $\Omega(i)$ implies $\Sigma_{i+1}^p \subseteq \Delta_{i+1}^p/\text{poly}$ and thus also $\Sigma_{i+2}^p = \Pi_{i+2}^p$.*

Proof. Let $A(v)$ be a Σ_{i+1}^p-predicate, i.e., $A(v)$ can be defined by a formula of the form:

$$\exists w \leq v\, B(v, w),$$

where B is Π_i^p.

We want to prove that for some function $g \in \square_{i+1}^p$ the following is true:

(*) $\qquad \forall n\, \exists u\, |u| \leq p(n) \wedge \forall v\, [|v| = n \rightarrow ((\exists w \leq v\, B(v, w)) \rightarrow B(v, g(u, v)))]$.

Here $p(n)$ is some polynomial and u is a polynomial advice.

We shall say that w is a witness for v if $w \leq v \wedge B(u, w)$ holds.

Define the relation:

$$R(a, b) := \text{"if } a = \langle v_1, \ldots, v_r\rangle \text{ and } b = \langle w_1, \ldots, w_s\rangle, \text{ then } s \leq r \text{ and for all } l \leq s,\ w_l \text{ is a witness for } v_l\text{"}.$$

The relation $R(a, b)$ is Π_i^b as well (and Δ_1^b if $i = 0$).

By principle $\Omega(i)$ there are $\square_{i+1}^p$-functions $f_1(a), \ldots, f_k(a, b_1, \ldots, b_{k-1})$ interactively computing b s.t. $R(a, b)$ for which a is maximal. (Observe that there is no apparent way to combine functions f_j into one $\square_{i+1}^p$-function with the argument a only, as it is difficult to search for 'counterexamples' $b_1, b_2, \ldots$.)

Let $n < \omega$ be given. We now describe how to find a polynomial advice u; the computation of the witness $g(u, v)$ will then be clear.

Put $V_1 = \{v \mid |v| = n \wedge \exists w \leq v\, B(v, w)\}$. Assign to any $v \in V_1$ a witness $w(v)$.

To each k-tuple $a = \langle v_1, \ldots, v_k\rangle$ of different elements of V_1 (here k is the number of functions guaranteed by $\Omega(i)$) we shall assign a pair (l, w), $1 \leq l \leq k$, by the following procedure:

Step 1. Compute $f_1(a)$.

Step 2. **If** $f_1(a) = \langle w_1', \ldots, w_j'\rangle$ where $j \geq 1$ and $R(a, f_1(a))$ is true
then put $l := 1$ and $w := w_1'$ and **Stop**.
Else compute $f_2(a, \langle w(v_1)\rangle)$ and **go to** Step 3.

Step m $(1 < m < k + 1)$
If $f_{m-1}(a, \langle w(v_1)\rangle, \ldots, \langle w(v_1), \ldots, w(v_{m-2})\rangle) = \langle w_1', \ldots, w_j'\rangle$ where $j \geq m - 1$ and $R(a, \langle w_1', \ldots, w_j'\rangle)$ is true
then put $l := m - 1$ and $w := w_{m-1}'$ and **Stop**.
Else compute $f_m(a, \langle w(v_1)\rangle, \ldots, \langle w(v_1), \ldots, w(v_{m-1})\rangle)$ and **go to** Step $m + 1$.

Step $k + 1$. If we have reached this step, then it necessarily holds that

$$f_k(a, \langle w(v_1)\rangle, \ldots \langle w(v_1), \ldots, w(v_{k-1})\rangle) = \langle w_1', \ldots w_k'\rangle \quad \text{and}$$
$$R(a, \langle w_1', \ldots, w_k'\rangle) \quad \text{is true.}$$

Put $l := k$ and $w := w_k'$ and **Stop**.

The point of this computation is that having witnesses $w(v_j)$ for all $j < l$ enables us to compute some witness (namely w) for v_l.

For Q a $(k - 1)$-element subset of V_1 and $v \in V_1 \backslash Q$ we shall say that the pair (Q, v) is *good* if for some arrangement $\{v_1, \ldots, v_{l-1}, v_{l+1}, \ldots, v_k\}$ of Q and $v = v_l$, (l, v) is assigned to $\langle v_1, \ldots, v_k\rangle$ in the procedure above.

Define a sequence of subsets of V_1: $V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$ having $N_j = |V_j|$ elements. V_{j+1} is chosen as follows: find a $(k - 1)$-element subset $Q_j \subseteq V_j$ such that

$$|\{v \in V_j \mid \text{pair } (Q_j, v) \text{ is good}\}| \geq \frac{N_j - k + 1}{k}$$

and take

$$V_{j+1} := V_j \setminus \{v \in V_j \mid \text{pair } (Q_j, v) \text{ is good}\}.$$

We have to show that such a $Q_j \subseteq V_j$ always exists. The procedure above constructs a good pair from each k-element subset of V_j and this mapping is one-to-one, since the k-element subset is determined by the good pair. Thus there are at least $\binom{N_j}{k}$ good pairs. On the other hand there are $\binom{N_j}{k-1}$ $(k-1)$-element subsets Q of V_j, so at least one such Q must form good pairs with at least

$$\binom{N_j}{k} \Big/ \binom{N_j}{k-1} = \frac{N_j - k +}{k} \quad \text{elements.}$$

An easy computation shows that

$$N_{j+1} < \left(\frac{k-1}{k}\right)^j N_1 + k$$

Hence we get $N_t \leq k$ after t steps, for

$$t = \mathrm{O}\left(\frac{1}{\log_2(k/(k-1))} \cdot \log_2(N_1)\right) = \mathrm{O}(\log_2(2^n)) = \mathrm{O}(n).$$

We take the polynomial size advice u to be all elements v of

$$Q_1 \cup Q_2 \cup \cdots \cup Q_{t-1} \cup V_t$$

along with their witnesses $w(v)$.

Then we have: if $v \in V_1$, then either $v \in V_t$ (and hence we have a witness for it in u) or, by the construction of $Q_1, \ldots, Q_{t-1}$, for some j, $1 \leq j \leq t-1$, (Q_j, v) is a good pair. Then the procedure above constructs a witness for v from witnesses for the elements of Q_j. This concludes the proof of the first part of the lemma.

$\Sigma^{\mathrm{p}}_{i+2} = \Pi^{\mathrm{p}}_{i+2}$ now follows easily by the following argument. Take $A(a) \in \Pi^{\mathrm{p}}_{i+2}$ of the form

$$\forall x \leq a \, \exists y \leq a \, C(a, x, y),$$

C a Π^{p}_i-formula. Define

$$B(\langle a, x \rangle, y) := (x \leq a \rightarrow (y \leq a \wedge C(a, x, y))).$$

Let $g \in \square^{\mathrm{p}}_{i+1}$ and a polynomial $p(n)$ satisfy (*) as guaranteed by the first part of the lemma. Then we can write predicate $A(a)$ in the following $\Sigma^{\mathrm{b}}_{i+2}$-form (as g is $\Sigma^{\mathrm{b}}_{i+1}$-definable):

$$A(a) \equiv \exists u \, [|u| \leq p(|a|) \wedge \forall x \, C(a, x, g(u, \langle a, x \rangle))]$$

(polynomial bounds for x are omitted). □

By Lemmas 2.1 and 2.2 it is apparently difficult to decide whether principle $\Omega(i)$ is true or not. As the proofs of these lemmas easily relativize we can reduce the relativized principle $\Omega(i)$ to the question whether the relativized Polynomial Hierarchy collapses. In [1] it is proved that $P^B = NP^B$ for some oracle B, hence the relativized Polynomial Hierarchy collapses to P^B. In [5, 14] it is proved that there is an oracle A such that the relativized Polynomial Hierarchy is proper. Hence both $\neg\Omega(i)^A$ and $\Omega(i)^B$ are possible:

Lemma 2.2. *There are oracles A and B such that for each* $i \geq 0$:

(a) $\Omega(i)^A$ *is false,*

(b) $\Omega(i)^B$ *is true.*

The construction of an oracle such that the relativized Polynomial Hierarchy does not collapse requires a deep result about boolean circuits. This is the case already with $\Sigma_2^p \neq \Pi_2^p$, which is needed for $\Omega(1)$. In what follows we shall present a direct construction of an oracle A such that $\Omega(1)^A$ fails. The existence of such an oracle for $\Omega(0)$ is an immediate corollary. We construct A such that there are no $(\square_2^p)^A$-functions witnessing a particular $P(a, b) \in (\Pi_1^p)^A$ in the sense of Ω.

We shall use the binary relation symbol $\alpha(x, y)$ as the name for the yet unconstructed oracle A. We take $P^\alpha(a, y)$ to be $\forall u \leq a\, \alpha(y, u)$. Let φ be the relativized P^*, i.e.

$$\varphi(a, y, z) := [(\forall u \leq a\, \alpha(y, u)) \wedge (z \leq a \wedge |y| < |z| \rightarrow \exists u \leq a\, \neg\alpha(z, u))].$$

An $f \in (\square_2^p)^A$ uses two oracles: A and a $(\Sigma_1^p)^A$-oracle (we will call it Σ-oracle). The Σ-oracle is determined by a binary predicate B^A computable in polynomial time using oracle A. The machine computing f may construct a word w and ask the Σ-oracle whether

$$\exists x\, |x| \leq p(|w|) \wedge B^A(w, x),$$

where p is a polynomial. To simplify the notation we shall assume that the polynomial bound to $|x|$ is implicit in $P^A(w, x)$.

Take an enumeration of all finite sequences $f_1^\alpha, \ldots, f_k^\alpha$ of $(\square_2^p)^\alpha$-functions. Although we have not constructed A (i.e. α) we may yet assume that we have polynomial bounds to the number of computationsl steps and queries. (A Σ-oracle can ask exponentially many queries, but this will be resolved below.)

A will be constructed in ω stages as

$$A = A_0 \cup A_1 \cup A_2 \cup \qquad A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdot$$

At the ith stage we shall add to A only pairs (y, u) such that $|y| > n_{i-1}$. Moreover, we shall add only polynomially many pairs with $|y| > n_i$. At this stage we diagonalize the ith sequence $f_1^\alpha, \ldots, f_k^\alpha$: this means that we will find some $a, b_1, \ldots, b_k$ of length $\leq n_i$ such that

$$(*) \qquad \neg\varphi(a, f_1^{A_i}(a), b_1)^{A_i} \wedge \qquad \wedge \neg\varphi(a, f_k^{A_i}(a, b_1, \quad , b_{k-1}), b_k)^{A_i}$$

and this property will be preserved at later stages. Hence it will hold for A as well.

For definiteness take $a := 0^{n_i}$. We take the enumeration and the sequence $n_1 < n_2 < \cdots$ so that the number of words of length between n_{i-1} and n_i is sufficiently larger than any polynomial bounds occurring up to this stage.

During the construction of A we not only add pairs into the oracle, but we also proclaim some pairs to be 'non-elements' of A, i.e., they can be never added to it. Thus formally A_i is a partial function from $\mathbb{N} \times \mathbb{N}$ to $\{0, 1\}$.

We now describe the ith stage. Start the computation of f_1^α on $a = 0^{n_i}$ with oracle A_{i-1}. We do not change A_{i-1} until we reach a state where the Σ-oracle is asked "$\exists x\, B^\alpha(w, x)$?". Then we try all 'consistent' extensions A' of A_{i-1} (i.e., extensions which do not contain non-elements). If there is an extension A' for which the answer is "Yes", then we take one x such that $B^{A'}(w, x)$ and add elements and non-elements, which are queried during the computation of $B^{A'}(w, x)$.

If the answer is "No" for all consistent extensions, we do not add any elements or non-elements.

In this way we have in both cases added only polynomially many requirements so that any further consistent extension of the oracle will not alter the answer of the Σ-oracle.

We repeat this procedure for all queries of the Σ-oracle.

Let A' be the extension of A_{i-1} obtained after the procedure. Consider $y := f_1^{A'}(a)$.

(1) If $y > a$, take $b_1 := 0$ and $A_i^1 := A'$.

(2) If $\forall z\, \varphi(a, f_1^{A'}(a), z)^{A'}$ is true, then $|y| \leq n_{i-1}$, because we have added only polynomially many pairs with elements longer than n_{i-1}. Thus we can take an arbitrary b_1 such that $|b_1| = n_{i-1} + 1$ and put

$$A_i^1 = A' \cup \{(b_1, u) \mid |u| \leq |a|\}.$$

(3) If $n_{i-1} < |y| \leq n_i$, then we can proceed similarly except that we take b_1 different from y and we add (y, u) as non-element for some suitable u. Thus we have $\neg(\forall u \leq a\, \alpha(y, u))$, hence

$$\neg\varphi(a, f_1^{A_i^1}(a), b_1)^{A_i^1}$$

and this will be preserved for all consistent extensions of A_i^1.

For $f_2^\alpha, \ldots, f_k^\alpha$ the construction is similar with only a minor difference. Consider $y = f_2^{A''}(a, b_1)$, where A'' is the extension of A_i^1 obtained as above. Then it may be that $y = b_1$ and (if (2) or (3) above holds):

$$\forall u\, (b_1, u) \in A''.$$

Hence in order to get

$$\neg\varphi(a, f_2^{A_i^2}(a, b_1), b_2)^{A_i^2}$$

we must take b_2 such that $|b_2| > |b_1|$. We can always take $|b_{l+1}| = |b_l| + 1$ since we assume that the number of elements of length $|b_l|$ is large.

$A_i := A_i^k$ gives us (*) above; note only that we have added only polynomially many pairs with elements of length $>n_i$ and hence the procedure can be repeated. □

3. The relation of S_2 to principle Ω

Using Theorem A and the results from Section 2 we now deduce a relation between S_2 and principle Ω.

Theorem B. *For $i \geq 1$, $T_2^i = S_2^{i+1}$ implies that principle $\Omega(i)$ is true. This in turn implies $\Sigma_{i+1}^p \subseteq \Delta_{i+1}^p/\text{poly}$ and $\Sigma_{i+2}^p = \Pi_{i+2}^p$.*

For $i = 0$ the same is true with PV_1 $(=\forall\Sigma_1^p(S_2^1))$ replacing T_2^0.

Proof. Take a Π_i^b-formula $B(a, b)$. By Σ_{i+1}^b-LIND it can be proved that there is a largest $t \leq |a|$ such that:

$$\exists z \leq a\, B(a, z) \to \exists x \leq a\, (|x| = t \wedge B(a, x)).$$

Thus S_2^{i+1} proves the following formula $\varphi(a)$:

$$\varphi(a) := \exists z \leq a\, B(a, z) \to \exists x \leq a\, \forall y \leq a\, B(a, x) \wedge (|x| < |y| \to \neg B(a, y)).$$

Assume $T_2^i = S_2^{i+1}$. Then $T_2^i \vdash \varphi(a)$ and since $\varphi(a)$ is a Σ_{i+2}^b-formula we can apply Theorem A to get $\Box_{i+1}^p$-functions $f_1(a), \ldots, f_k(a, b_1, \ldots, b_{k-1})$ which interactively compute x from a, as is required by principle $\Omega(i)$.

The rest of the theorem follows from Lemma 2.2. □

Recall that $S_2(\alpha)$ is S_2 augmented by a new unary predicate symbol $\alpha(x)$ which can occur in induction axioms but there are no new axioms about α in BASIC, cf. [2]. A similar theory $\text{I}\Delta_0(f)$, $\text{I}\Delta_0$ with a new unspecified function symbol $f(x)$, was considered in [11].

Theorem C. *For all $i \geq 1$, $T_2^i(\alpha) \neq S_2^{i+1}(\alpha)$. Also $\forall\Sigma_1^b(S_2^1(\alpha)) \neq S_2^1(\alpha)$. Thus neither $S_2(\alpha)$ nor $\text{I}\Delta_0(f)$ are finitely axiomatizable.*

Proof. The proofs of Theorems A, B relativize and by Lemma 2.2 there is an oracle making $\Omega(i)$ false, for all i. This gives the statements about $S_2(\alpha)$. But if $S_2(\alpha)$ is not finitely axiomatizable, then neither is $\text{I}\Delta_0(f)$. □

By $T_2 \vdash \Sigma_i^p = \Pi_i^p$ we mean that for each Σ_i^b-formula $A(a)$ there is a Π_i^b-formula $B(a)$ such that $T_2 \vdash A(a) \equiv B(a)$. As there are complete Σ_i^p-problems, $\Sigma_i^p = \Pi_i^p$ follows from one of its instances and then actually $\Sigma_i^p = \text{PH}$. Thus $T_2 \vdash \Sigma_i^p = \Pi_i^p$ implies that $T_2^j \vdash \Sigma_i^p = \text{PH}$, for some $j \geq i$, and hence $T_2 = T_2^j$ is then finitely axiomatizable.

It would be interesting to know whether the opposite implication is also true. One way to prove this would be to formalize the proof of Theorem B in T_2. The obstacle to such a formalization is the definition of the polynomial advice, i.e., the counting argument in the proof of Lemma 2.1.

Hence it remains an open question whether the assumption $T_2 = T_2^i$ implies $T_2 \vdash \Sigma_{i+2}^p = \Pi_{i+2}^p$.

References

[1] T. Baker, J. Gill and R. Solovay, Relativizations of the $P = ?$ NP question, SIAM J. Comput. 4 (1975) 431–442.

[2] S. Buss, Bounded Arithmetic (Bibliopolis, Napoli, 1986).

[3] S. Buss, Axiomatizations and conservation results for fragments of bounded arithmetic, Proc. of Workshop in Logic and Computation (1987), Contemporary Math., to appear.

[4] S.A. Cook, Feasibly constructive proofs and the propositional calculus, Proc. 7th Ann. ACM Symp. Theory of Comput. (1975) 83–97.

[5] J. Håstad, Computational Limitations of Small-Depth Circuits (MIT Press, Cambridge, MA, 1987).

[6] R.M. Karp and R.J. Lipton, Some connections between nonuniform and uniform complexity classes, Proc. 12th ACM Symp. Theory of Comput. (1980) 302–309.

[7] J. Krajíček, Π_1-conservativeness in systems of bounded arithmetic (1988), submitted.

[8] J. Krajíček and P. Pudlák, Quantified propositional calculi and fragments of bounded arithmetic, Z. Math. Logik 36 (1989) 29–46.

[9] J. Paris and A. Wilkie, Δ_0-sets and induction, in: W. Guzicki, ed., Open Days on Model Theory and Set Theory (Warsaw, 1984) 237–248.

[10] J. Paris and A. Wilkie, On the scheme of induction for bounded arithmetic formulas, Ann. Pure Appl. Logic 35(3) (1987) 205–303.

[11] J. Paris, A. Wilkie and A. Woods, A note on the provability of the Δ_0-PHP and the existence of infinitely many primes, J. Symbolic Logic 53(4) (1988) 1235–1244.

[12] G. Takeuti, Sharply bounded arithmetic and the function $a \dot{-} 1$, Proc. of Workshop in Logic and Computation (1987), Contemporary Math., to appear.

[13] G. Takeuti, Proof Theory (North-Holland, Amsterdam, 1975; 2nd ed. 1987).

[14] A. Yao, Separating the polynomial-time hierarcy by oracles, Proc. 26th Annual IEEE Symp. on Found. of Comput. Sci. (1985) 1–10.