A note on bounded arithmetic

by

P. Pudlák (Praha)

Abstract. We prove that bounded arithmetic S_2 does not prove the bounded consistency of its Σ_1^b-fragment S_2^1.

We consider bounded arithmetic S_2 and its fragments S_2^i introduced by Buss [1]. The language of these systems consists of the constant $\underline{0}$, function symbols S, $+$, $\cdot$, $\llcorner 1/2\, x \lrcorner$, $|x|$, $x \# y$ and predicates $=$, $\leqslant$. The interpretation of $|x|$ and $x \# y$ is

$$|x| = \ulcorner \log_2(x+1) \urcorner \quad \text{and} \quad x \# y = 2^{|x|\cdot|y|}.$$

S_2 is axiomatized by a finite set S_2^{-1} of open formulas plus schema of induction PIND:

$$A(0) \wedge \forall x \big(A(\llcorner 1/2\, x \lrcorner) \rightarrow A(x)\big) \rightarrow \forall x\, A(x)$$

for all bounded formulas A, which is equivalent to the usual schema of induction for all bounded formulas. Classes Σ_i^b of bounded formulas are defined so that in the standard formula φ, $\varphi \in \Sigma_i^b$, defines a set in Σ_i^p where Σ_i^p, $i = 0,1,\ldots$, is the polynomial time hierarchy. The fragments S_2^i, $i \geqslant 1$, are defined by restricting the schema PIND to Σ_i^b formulas.

One of the most interesting problems in bounded arithmetic is whether the hierarchy of theories S_2^i, $i \geqslant 1$, is strictly increasing. A positive answer to this question would give us some evidence that the polynomial time hierarchy is strictly increasing (which is an important open problem in complexity theory). The usual way of proving that a theory containing a fragment of arithmetic is stronger than another theory fails here, since even $S_2 \nvdash \mathrm{Con}_{S_2^{-1}}$, cf. [5]. Buss considered weaker consistency statements $BD\,\mathrm{Con}$ which refer to *proofs that use only bounded formulas.* However, these sentences are still too strong. Buss [1] proved that $S_2^{i+1} \vdash BD\,\mathrm{Con}_{S_2^i}$ holds for at most one i. Here we show:

THEOREM. $S_2 \nvdash BD\,\mathrm{Con}_{S_2^1}$.

For $n > 0$ let $\underline{n}$ denote the term inductively defined by $\underline{2n+1} = \underline{2n} + S(\underline{0})$, $\underline{2n+2} = SS(\underline{0}) \cdot \underline{n+1}$. Let $\gamma(\varphi)$ denote the minimal Gödel number of a bounded proof of φ in S_2^1 if there is such a proof and ∞ otherwise. $BD\,\mathrm{Con}_{S_2^1}(x)$ is a formalization of "$\gamma(\ulcorner 0 = 1 \urcorner) > x$"; thus

$$BD\,\mathrm{Con}_{S_2^1} \Leftrightarrow \forall x\, BD\,\mathrm{Con}_{S_2^1}(x).$$

For a formula $\varphi(a)$ we put

$$\mathrm{Ind}_{\varphi(\alpha)}(x) := \forall y \leqslant x\bigl(\varphi(\underline{0}) \wedge \forall z < y(\varphi(z) \rightarrow \varphi(z+1)) \rightarrow \varphi(y)\bigr).$$

The proof of the Theorem is based on the following lemmas.

LEMMA 1. *For every term $s(x)$ there exists a term $r(x)$ such that for all but finitely many n*

$$\gamma\bigl(BD\,\mathrm{Con}_{S_2^1}(r(\underline{n}))\bigr) > s(n).$$

LEMMA 2. *For every bounded $\varphi(a)$ and a term $t(x)$ there exists a polynomial $p(x)$ such that for every n*

$$\gamma\bigl(\mathrm{Ind}_{\varphi(a)}(t(\underline{n}))\bigr) \leqslant p(n \# n).$$

LEMMA 3. *If $\varphi(a)$ is a bounded formula and $S_2 \vdash \forall x\ \varphi(x)$ then there exists a polynomial $p(x)$ such that for every n*

$$\gamma(\varphi(\underline{n})) \leqslant p(n \# n).$$

First we derive our Theorem from Lemmas 1 and 3. Take a term $r(x)$, given by Lemma 1 for $s(x) := x \# x \# x$. By way of contradiction assume that $S_2 \vdash \forall x\, BD\,\mathrm{Con}_{S_2^1}(x)$. Then we have also $S_2 \vdash \forall x\, BD\,\mathrm{Con}_{S_2^1}(r(x))$. Now apply Lemma 3 to $\varphi(a) := BD\,\mathrm{Con}_{S_2^1}(r(a))$. Thus we obtain, for some polynomial p and every n,

$$n \# n \# n \leqslant \gamma(\varphi(\underline{n})) \leqslant p(n \# n).$$

But the function on the left-hand side grows faster than the function on the right-hand side, which is a contradiction.

It remains to prove the lemmas.

Proof of Lemma 1. Let $s(x)$ be a given term. Take a term $t(x)$ such that for every polynomial p, $p(s(n), n) < t(n)$ holds for all but finitely many n's (e.g. $t(x) := s(x) \# s(x)$). Let $D(x)$ be a formula such that

$$(1) \qquad S_2^1 \vdash D(x) \Leftrightarrow \bigl(\gamma(\ulcorner D(\mathrm{Num}(x))\urcorner) > t(x)\bigr),$$

where $\mathrm{Num}(x)$ is a formalization of the function $n \mapsto \underline{n}$. One can choose D to be bounded and also the proof of the equivalence in S_2^1 can be bounded.

CLAIM 1. $\gamma(D(\underline{n})) > t(n)$.

The proof of this claim is standard, cf. [2] (however, observe that in [2] we considered the length of proofs instead of the Gödel numbers).

CLAIM 2. *There exists a term $r(x)$ such that $\gamma\bigl(BD\,\mathrm{Con}_{S_2^1}(r(\underline{n})) \rightarrow D(\underline{n})\bigr) \leqslant p_0(n)$, for some polynomial $p_0(x)$.*

The proof of this claim is based on the formalization of Claim 1 in S_2^1. By Theorem 7.4 [1] and since $\neg D(x)$ is Σ_1^b, there exists a term $s(x)$ such that

$$S_2^1 \overset{BD}{\vdash} \neg D(x) \rightarrow \gamma(\ulcorner \neg D(\mathrm{Num}(x))\urcorner) \leqslant s(x).$$

By the definition (1) of $D(x)$ we have

$$S_2^1 \overset{BD}{\vdash} \neg D(x) \rightarrow \gamma(\ulcorner D(\mathrm{Num}(x))\urcorner) \leqslant t(x).$$

Hence for some term $r(x)$

$$S_2^1 \overset{BD}{\vdash} \neg D(x) \rightarrow \gamma(\ulcorner 0 = 1\urcorner) \leqslant r(x),$$

which is

$$S_2^1 \overset{BD}{\vdash} BD\,\mathrm{Con}_{S_2^1}(r(x)) \rightarrow D(x).$$

Now substituting $\underline{n}$ for x we obtain a proof whose Gödel number is linear in n.

We can now finish the proof of Lemma 1. Roughly speaking, the size of a proof of $BD\,\mathrm{Con}_{S_2^1}(r(\underline{n}))$ is the size of a proof of $D(\underline{n})$ minus the size of the proof of $BD\,\mathrm{Con}_{S_2^1}(r(\underline{n})) \rightarrow D(\underline{n})$. As we use Gödel numbers instead of the length of proofs, we must be a little more careful. We shall use the fact that (for a suitable coding which we assume here) the Gödel number of the concatenation depends polynomially on the Gödel numbers of its parts. Thus we have for some polynomial $p(x, y)$,

$$\gamma(D(\underline{n})) \leqslant p\bigl(BD\,\mathrm{Con}_{S_2^1}(r(\underline{n})), \gamma(BD\,\mathrm{Con}_{S_2^1}(r(\underline{n})) \rightarrow D(\underline{n}))\bigr).$$

Hence by the claims

$$t(n) < q\bigl(\gamma(BD\,\mathrm{Con}_{S_2^1}(r(\underline{n})))\bigr)$$

for some polynomial $q(x)$. Since $t(n) < q(s(n))$ holds only for finitely many n's, we have proved the lemma. ■

Proof of Lemma 2. The idea is to consider two cases according to the truth of $\mathrm{Ind}_{\varphi(a)}(t(\underline{n}))$. Imagine that we are in S_2^1. If $\mathrm{Ind}_{\varphi(a)}(t(\underline{n}))$ is true, then we have finished, if not, take the cut of those x's for which $\mathrm{Ind}_{\varphi(a)}(x)$ holds. Then this cut is contained in the interval $[0, t(\underline{n})]$. Using shortenings of cuts we can find a subcut which is closed under the functions of S_2. But then there is a short proof that $t(\underline{n})$ is in the cut, since $t(\underline{n})$ is a term obtained from $\underline{0}$ by applying $O(\log n)$ times functions of S_2. Hence $\mathrm{Ind}_{\varphi(a)}(t(n))$ follows. The construction of such shortenings is well known, however the defining formulas are not bounded. The point here is that we may add $t(\underline{n})$ as a bound to all quantifiers in these definitions of cuts, since the cuts are below $t(\underline{n})$.

Now we shall describe the proof in more detail. Let $\varphi(a)$ be a given bounded formula. Put

$$J_1(x, y) := \forall z \leqslant y\ (\mathrm{Ind}_{\varphi(a)}(z) \rightarrow \mathrm{Ind}_{\varphi(a)}(z+x)),$$

$$J_2(x, y) := \forall z \leqslant y\ (J_1(z, y) \rightarrow J_1(z \cdot x, y)),$$

$$J(x, y) := \forall z \leqslant y\ (J_2(z, y) \rightarrow J_2(z \# x, y)).$$

Let us note that if we left out the bounds at the quantifiers, we would have just the well-known definitions of shortenings closed under $+$, $\cdot$, and $\#$ respectively. One has to check that with the bounds added, the closure properties are preserved.

CLAIM 1. *The following sentences have bounded proofs in* S_2^1:

(1) $J(x, y) \to \mathrm{Ind}_{\varphi(a)}(x)$;

(2) $J(\underline{0}, y)$;

(3) $J(x, y) \& z \leqslant x \to J(z, y)$;

(4) $\mathrm{Ind}_{\varphi(a)}(y) \vee \big(J(x, y) \& J(x', y) \to J(x \# x', y)\big)$.

We shall prove (1)–(4) only for J_1 and with $\#$ replaced by $+$. Then we can prove the same for J_2 with multiplication instead of $\#$ and eventually (1)–(4) as they stand. To prove (1) for J_1 take $z = 0$ in the definition of J_1; (2) is also trivial; (3) is true because $\mathrm{Ind}_{\varphi(a)}(x)$ is closed downwards. To prove the modified (4) in S_2^1, assume $\mathrm{Ind}_{\varphi(a)}(y)$, $J_1(x, y)$ and $J_1(x', y)$. We want to prove $J_1(x+x', y)$. Thus assume also $\mathrm{Ind}_{\varphi(a)}(z)$ for $z \leqslant y$. Since $J_1(x, y)$ we have $\mathrm{Ind}_{\varphi(a)}(z+x)$. Since $\neg \mathrm{Ind}_{\varphi(a)}(y)$ and $\mathrm{Ind}_{\varphi(a)}$ is downward closed, we have $z+x < y$, hence we can use $J_1(x', y)$ to deduce $\mathrm{Ind}_{\varphi(a)}(z+x+x')$, which we needed.

CLAIM 2. *For every term* $t(x)$,

$$S_2^1 \overset{BD}{\vdash} \mathrm{Ind}_{\varphi(a)}(y) \vee \big(J(x, y) \to J(t(x), y)\big).$$

This follows from Claim 1, since it is provable in S_2^1 that $\#$ grows faster than any other function of the language of S_2.

Now we shall finish the proof of Lemma 2. By definition, numeral $\underline{n}$ is constructed in $O(\log n)$ steps from $\underline{0}$ using functions of S_2, i.e.

$$\underline{n} = t_k\big(t_{k-l}(\ldots t_l(\underline{0}))\big),$$

where $k = O(\log n)$ and $t_i(x)$ is either $SS(\underline{0}) \cdot x$ or $SS(\underline{0}) \cdot x + S(\underline{0})$. Hence

$$\neg \mathrm{Ind}_{\varphi(a)}(y) \to J(\underline{n}, y)$$

follows from Claim 1 (2) and from $O(\log n)$ applications of Claim 2. One more application of Claim 2 gives us

$$\neg \mathrm{Ind}_{\varphi(a)}(y) \to J(t(\underline{n}), y).$$

Each proof step has the Gödel number bounded by a polynomial in n. Thus the Gödel number of the proof is bounded by $p(n \# n)$, for some polynomial p. Substituting $t(\underline{n})$ for y we obtain

$$\neg \mathrm{Ind}_{\varphi(a)}(t(\underline{n})) \to J(t(\underline{n}), t(\underline{n})).$$

By (1) of Claim 1 this gives $\mathrm{Ind}_{\varphi(a)}(t(\underline{n}))$, and again the Gödel number of the proof increases only polynomially. ■

Proof of Lemma 3. Suppose $S_2 \vdash \forall x\, \varphi(x)$. Since $T_2 \equiv S_2$, the formula is provable using ordinary induction. Hence

$$S_2^1 \vdash \bigwedge_i \forall x, \bar{y}\ \mathrm{Ind}_{\varphi_i}(x) \to \forall x\ \ \varphi(x),$$

where in the conjunction we have finitely many formulas corresponding to some bounded formulas φ_i, and $\bar{y}$ is a vector of variables containing all parameters of φ_i's. By Parikh's theorem there exists a term $t(x)$ such that

$$S_2^1 \vdash \bigwedge_i \forall \bar{y} \leqslant t(x)\ \mathrm{Ind}_{\varphi_i}(t(x)) \to \varphi(x).$$

Since the axioms of S_2^1 as well as the formula are bounded, we may assume that this proof is bounded too (by cut elimination). Now we can combine this proof with the proofs of $\mathrm{Ind}_{\varphi_i}(t(n))$ constructed in Lemma 2. Since these proofs have Gödel number polynomial in $n \# n$, the proof of $\varphi(\underline{n})$ has also Gödel number bounded by a polynomial in $n \# n$. ■

It is very likely that the above proof can be extended to much weaker theories instead of S_2^1, e.g. to $S_2 \nvdash BD\,\mathrm{Con}_{S_2^{-1}}$. The corresponding Lemma 2, however, would be much more technical. For instance in S_2^{-1} we cannot prove that $\#$ majorizes other functions. Analysing our proof Takeuti [4] obtained an improvement. However, it remains open whether $S_2 \vdash BQ\,\mathrm{Con}_{S_2^i}$, for $i = 1, 2, \ldots$

This result has been presented to the Congress LMPS '87 [3].

References

[1] S. Buss, *Bounded Arithmetic*, Bibliopolis, Napoli, 1986.

[2] P. Pudlák, *On the length of proofs of finitistic consistency statements in first order theories*, in: *Logic Colloquium '84*, North-Holland, 1986, pp. 165–196.

[3] — *A note on bounded arithmetic*, Abstracts, 8th Intern. Congress of Logic, Methodology and Phil. of Sci., Moscow 1987, pp. 159–160.

[4] G. Takeuti, *Some relations among systems for bounded arithmetic*, preprint.

[5] A. Wilkie and J. Paris, *On the scheme of induction for bounded arithmetic formulas*, Ann. Pure Appl. Logic 35 (1987), 261–302.

MATHEMATICAL INSTITUTE
CZECHOSLOVAK ACADEMY OF SCIENCES
11567 Praha 1
Žitná 25
Czechoslovakia

Received 13 February 1989;
in revised form 31 July 1989