# Unprovability of Consistency Statements in Fragments of Bounded Arithmetic

by

**Samuel R. Buss and Aleksandar Ignjatović**

November 1993

Report CMU-PHIL-43

Carnegie Mellon

Philosophy
Methodology
Logic

Pittsburgh, Pennsylvania 15213-3890

# Unprovability of Consistency Statements in Fragments of Bounded Arithmetic

Samuel R. Buss[1] Aleksandar Ignjatović[2]

January 21, 1994

**Abstract**

This paper deals with the weak fragments of arithmetic $PV$ and $S_2^i$ and their induction-free fragments $PV^-$ and $S_2^{-1}$. We improve the bootstrapping of $S_2^1$, which allows us to show that the theory $S_2^1$ can be axiomatized by the set of axioms $BASIC$ together with any of the following induction schemas: $\Sigma_1^b$-*PIND*, $\Sigma_1^b$-*LIND*, $\Pi_1^b$-*PIND* or $\Pi_1^b$-*LIND*. We improve prior results of Pudlák, Buss and Takeuti establishing the unprovability of bounded consistency of $S_2^{-1}$ in $S_2$ by showing that, if $S_2^i$ proves $\forall x\varphi(x)$ with $\varphi$ a $\Sigma_0^b(\Sigma_i^b)$-formula, then $S_2^1$ proves that each instance of $\varphi(x)$ has a $S_2^{-1}$-proof in which only $\Sigma_0^b(\Sigma_i^b)$-formulas occur. Finally, we show that the consistency of the induction free fragment $PV^-$ of $PV$ is not provable in $PV$.

## 1 Technical Preliminaries

We assume familiarity with the theories of bounded arithmetic and the general notation introduced in [2]. We will denote the language of $S_2^i$ and $T_2^i$ by $L_b$. Thus, $L_b = \{0, S, +, \cdot, |a|, \lfloor \frac{1}{2}a \rfloor, \#, \leq\}$. The theories of bounded arithmetic were defined in [2] to include a finite set $BASIC$ of open axioms in addition to induction

[1] Partially supported by the NSF grant DMS-9205181.

[2] Partially supported by the Faculty Development Fund of CMU. Most of this joint work has been done while A. Ignjatović was visiting the Mathematics Department of the UCSD during the Summer of 1992.

axioms. In this paper, we shall extend the original version of $BASIC$ axioms to include two more simple axioms: $|a| \leq a$ and $|a \cdot b| \leq |a| + |b|$. The addition of these two axioms makes our arguments in section 3 considerably easier and more elegant at the cost of slightly weakening the result of section 3 that $S_2^i$ can not prove $B_i^b$-$Con(S_2^{-1})$. Although we can prove this without the use of these extra $BASIC$ axioms, we feel that this would not be worth carrying out the more complicated proof; and, as explained in [2], there is no real advantage in working in the exact original version of $BASIC$ (see also [4]). What is important is that the consistency with respect to a restricted provability notion of a very weak base theory (i.e., $S_2^{-1}$) consisting of only common properties of basic operations is not provable in the significantly stronger theory $S_2$. The equational theory axiomatized by only the BASIC axioms we call $S_2^-$ and its first order counterpart, $S_2^{-1}$. Note our $S_2^{-1}$ is not quite the usual version since it has the additional two BASIC axioms. However, the theories $S_2^i$ and $T_2^i$ for $i \geq 0$ are defined as usual since they can already prove the two new axioms.

We define the language $L_e$ to be $L_b$ plus the following set of extra symbols: $\{2^a_{|b|}, \dot{-}, sq(a), \langle a, b\rangle, (a)_1, (a)_2\}$. Here $2^a_{|b|}$ stands for the function $2^{\min\{a,|b|\}}$; $a \dot{-} b$ is the usual limited subtraction; $sq(a)$ is just the *unary* squaring function (i.e. $sq(a) = a \cdot a$) and will be used to form short terms denoting high-degree polynomials; $\langle a, b\rangle$ is the pairing function; $(a)_1$ and $(a)_2$ are the two corresponding projection functions. As shown in [2], all of the above functions can be $\Sigma_1^b$-defined in $S_2^1$ and the same theory can prove that these functions satisfy the basic properties 1-4 below, which we will take as axioms of our equational theories in the language $L_e$. We define $E^-$ to be the equational theory in the language $L_e$ axiomatized by the set of axioms $BASIC^e$ consisting of the axioms of $BASIC$ together with the following additional groups of axioms.

1. $|a| \leq a, \ \ |a \cdot b| \leq |a| + |b|$;
2. $2^a_{|0|} = 1, \ \ 2^0_{|c|} = 1, \ \ a + b \leq |c| \supset 2^{a+b}_{|c|} = 2^a_{|c|} \cdot 2^b_{|c|}$;
   $c \neq 0 \supset (2^1_{|c|} = 2 \ \wedge \ 2^a_{|c|} < 2 \cdot c)$;
3. $a \leq b \leftrightarrow a \dot{-} b = 0, \qquad a \dot{-} b = 0 \leftrightarrow (b \dot{-} a) + a = b$;
4. $sq(a) = a \cdot a$;
5. $(\langle a, b\rangle)_1 = a, \ \ (\langle a, b\rangle)_2 = b, \ \ \langle (a)_1, (a)_2\rangle = a, \ \ |\langle a, b\rangle| \leq 2 \cdot (1 + |a| + |b|)$,
   $\langle a, b\rangle = \lfloor \frac{1}{2}((a^2 + b^2 + 2ab + a + 1) \dot{-} b)\rfloor$.

Recall that a function $f(b,\vec{a})$ is obtained by *limited recursion on notation* from the functions $g(\vec{a})$ and $h(b,c,\vec{a})$ with the bounding function $k(b,\vec{a})$, provided $f(0,\vec{a}) = g(\vec{a})$ and, for all $b > 0$ and all $\vec{a}$, the following holds:[3]

$$f(b,\vec{a}) = \min\{h(b, f(\lfloor \tfrac{1}{2} b \rfloor, \vec{a}), \vec{a}), k(b,\vec{a})\}.$$

It is a classic result of Cobham's that every polynomial time computable function can be defined from functions in $L_e$ by use of composition and limited recursion on notation. We define $L_p$ to be the language containing $L_e$ plus symbols for all polynomial time computable functions. $PV''$ is an equational $L_v$-theory which is axiomatized by *BASIC** plus axioms defining the polynomial time functions in terms of their definition by limited recursion on notation. $PV$ is the equational theory obtained from the theory $PV''$ by adding the induction rule for all open formulas of $L_p$. $S_2^{-}$, $E^{-}$, $PV_1^{-}$ and $PV_1$ are the first order theories which are conservative over $S_2^{-}$, $E''$, $PV''$ and $PV$. Note that the induction rule of $PV$ is restricted to open formulas. The original definitions of $PV''$ and $PV$ are due to Cook [5].

However, to make our arguments simpler, we will not work directly with purely equational theories, as, for example, $PV$ is formulated in Cook's [5]. Proofs in our theories contain quantifier-free formulas only, but we allow in formulas also inequalities and propositional connectives. Thus, our proof-system will also include propositional rules of inference. We choose such a proof system because in order to eliminate applications of the induction rule from certain proofs we must apply the speed up induction method, and the formulas needed in this method would be extremely awkward if we worked in a purely equational theory. On the other hand, this does not weaken our results, since inequalities and propositional connectives (and the corresponding rules) can be easily removed by replacing formulas which contain inequalities and propositional connectives with suitable arithmetical combinations. For example, inequality $t_1 \leq t_2$ can be replaced by $t_1 \dot{-} t_2 = 0$, while $t_1 = 0 \vee t_2 = 0$ can be replaced by $t_1 \cdot t_2 = 0$. This transformation is easily seen to produce only polynomial increase of the length of proofs. Thus, we will work with quantifier-free theories rather than purely equational ones, and since for our purposes our formalism differs inessentially from the usual one, we use the same notation for purely equational theories like $PV$ or $PV^{-}$ and the

[3]Strictly speaking, $\min\{a,b\}$ is not in the language $L_e$; however, it can be replaced by

corresponding quantifier free theories.

We use the usual hierarchies, $\Sigma_i^b$ and $\Pi_i^b$, of formulas to measure the (bounded) quantifier complexity of formulas in our first order theories; in addition, $B_i^b$ denotes the class of formulas obtained as the least closure of $\Sigma_i^b$ formulas under Boolean connectives and sharply bounded quantifiers; the class $B_i^b$ is sometimes denoted $\Sigma_0^b(\Sigma_i^b)$ and in [3] is denoted $\Sigma_{i+1}^b \cap \Pi_{i+1}^b$.

We will use numeral terms, $\underline{n}$, whose length is linear in the logarithm of the number $n$, defined by:

$$\underline{0} \stackrel{df}{=} 0, \qquad \underline{1} \stackrel{df}{=} S(0), \qquad \underline{2} \stackrel{df}{=} S(S(0))$$
$$\underline{2n} \stackrel{df}{=} \underline{2} \cdot \underline{n}, \qquad \underline{2n+1} \stackrel{df}{=} \underline{2n} + \underline{1}$$

For notational simplicity, we will not underline numerals corresponding to the numbers $0, 1, 2$.

We use Gentzen-style sequent calculus proof systems for formal proofs in the theories $PV$, $PV^-$, $S_2^i$, etc. For first-order theories with bounded quantifiers, we use the system $LKB$ which is the usual Gentzen sequent calculus augmented with inference rules for the bounded quantifiers (described in [2]). For such theories, we will mostly consider *bounded proofs*, i.e., proofs in which all formulas have only bounded quantifiers. Proofs for equational theories are formulated in the sequent calculus without any quantifier rules, but with the substitution rule:

$$\frac{\Gamma(a) \longrightarrow \Delta(a)}{\Gamma(t) \longrightarrow \Delta(t)}$$

where $a$ is an *eigenvariable* which must not appear in the lower sequent and $t$ is an arbitrary term.

We define the size of a proof $P$ to be the total number $|P|$ of symbols in them. Sequent calculus proofs are presumed to be tree-like (our proofs will work without this assumption, however). The initial sequents in proofs can be logical axioms of the form $A \longrightarrow A$ for $A$ an arbitrary atomic formula, or equality axioms, or sequents of atomic formulas expressing $BASIC$ axioms.

Without loss of generality, we always assume that a proof $P = P(\vec{a}, \vec{b})$ of a sequent $\Gamma \longrightarrow \Delta$ is in *free variable normal form*. This means that none of the free variables $\vec{a}$ appearing in the sequent $\Gamma \longrightarrow \Delta$ are used as eigenvariables, and all other free variables $\vec{b}$ in the proof are used exactly once as an eigenvariable of an induction rule, a bounded quantifier rule or a substitution rule in the proof *P*. This assumption is permissible, since otherwise we can rename some variables and replace some variables by the term 0, and obtain a proof of the same endsequent satisfying the above property. Of course, this procedure is formalizable in any weak fragment of bounded arithmetic with minimum of induction (e.g. *S%*). We can also assume that the sequence of variables $\vec{b}$ = 60,..., 6jt-i is ordered in such a way that, on any thread of the proof (i.e. any maximal branch through the proof tree), if 6r and *bj* are eigenvariables of two rules and $i < j$, then $6_t$ is eliminated by a rule which is below (i.e. closer to the conclusion of the proof than) the rule by which *bj* is eliminated. The variables $\vec{a}$ which occur in the endsequent of a **proof are called *parameter variables.***

The outline of the remainder of the paper is as follows. In section 2, we give an improved treatment of the bootstrapping of *Si* which shows that *Si* may be equivalently axiomatized with any of *Y>\-LIND, U^-LIND* or *U^-PIND* in place of *Y,\-PIND.* This improved bootstrapping simplifies the proofs in section 3.

Pudlák [8] proved that 6'2 can not prove the consistency of *Si* using a modification of the cut-shortening technique of Solovay's. The first author [1] noted that Pudlák's methods could be modified to prove that #2 can not prove the consistency of S^"1. Takeuti [10] showed that these techniques established that $S^{x}_{2}$ could not prove the consistency of Sj"1-proofs in which only $Ej_{+5}$-formulas appear. In section 3 we give a new proof that $'2 can not prove the consistency of *S2*^1 (with our extended BASIC axioms), which improves on the prior results by establishing that *S* can not prove the consistency of 5J^1 proofs in which only l?f-formulas appear (we call this principle *the B\ -consistency of S^*^1*)*- Our proof method uses a technique of induction speed-up elaborated in [6] (see also [7]), which is closely related to a construction due originally to Solovay [9]. The essential novel feature of our induction speed-up is that it requires only the introduction of sharply bounded quantifiers. Also, the starting formula need not define a cut in the standard sense, since the set it defines need not be an initial segment of the universe (see [6] for more details).

In section 4, it is shown that *PV* can not prove the consistency of *PV~*. Since *PV* is an equational theories, the speed-up of induction can not be accomplished with the aid of quantifiers; instead, we develop a different form of the speed-up of induction based on Skolem functions.

## 2 Better Bootstrapping of *S%*

In this section, we give alternative axiomatizations of the theory *Si* based on induction schemes different from the *E^-PIND* axioms used originally by the first author [2]. We prove that the *Y\-PIND* axioms may be replaced by either the *Y>\-LIND* axioms, the *U\-LIND* axioms or the *U^-PIND* axioms without changing the strength of *S]*. Of particular interest is that either *Y^-LIND* or *H\-LIND* may be used, since these axioms are, at first glance, somewhat weaker than *Y^-PIND*. Also, the fact that *S* can be axiomatized by *Y>\-LIND* simplifies our proof of the main result of Section 3.

The results of this section do not depend on our inclusion of two additional BASIC axioms and thus apply to the theories in the form defined in [2].

To prove the equivalence of the alternative axiomatizations of 5^, it is necessary to improve on the bootstrapping given in Chapter 2 of [2]; we shall presume that the reader has [2] available and we will frequently refer to proofs therein. Our goal in this section is to improve Theorem 2.13 of the bootstrapping of [2] by showing that the following are equivalent axiomatizations of *S* even for $i = 1$; recall that in [2], the equivalence of $Y>^h_r$*PIND*, *\l\-PIND*, $Y>^h_r$*LIND* and *Hj-LIND* wets proved only in the presence of *S]* as base theory.

**Theorem 1** *The following are equivalent axiomatizations of* SJ *(for* $i \geq 1$*):*

(1) *BASIC*+$X^b_r$*PIND*

(2) *BASIC*+$Y_l$*\-LIND*

(3) *BASIC*+$H^b_r$*PIND*

(4) *BASIC*+$U^b_i$*-LIND*

By Theorem 2.13 of [2], we only need to prove Theorem 1 for the case $i = 1$. We shall prove a series of lemmas that establish this theorem.

Lemma 2 *The following three functions can be* Sj *-defined in the theory BASIC+* $T^b_i$*Q-LIND, and basic properties of these functions are provable in this theory:*

(1) c = min(a, 6).

(2) *c=LenP{a,b)* <=> ((a = 0 V *b* = 0) A *c* = 0) V *S(c)* = min(a, |6|).

**(3)** ***c=LenMinus(a,b)*** **<=>** ***(b <\a\ A 6 + c = \a\) V (\a\ < b A c = 0).***

***In fact, these functions are Efc-definable in BASIC + Z,$^{b}$$_{0}$-LIND.***

**Proof:** The fact that the minimization function $c$ = min(a, $b$) can be EQ-defined in *BASIC* + *T,Q-LIND* is proved by the argument of [2, p. 38] showing it is £j -definable in *S]* -

In the formula *LenP(a,b)* the second argument 6 occurs as a 'dummy' argument which serves only to bound the value of the function. The uniqueness condition for *LenP* follows from the *BASIC* axioms only, with no use of induction. For the existence condition, let *M(a,* 6, *c)* be the defining equation above for *LenP* and let *N(a, b)* be the formula

(Vu ≤ |6|)(3c ≤ |6|)(u ≤ *a D* M(u, 6, c)).

Then *BASIC* proves *N(Q,b)* and *(Va)(N(a,b) D N(a* + 1,6)). Thus, since *N(a,b)* is sharply bounded, *BASIC* + *E$^{b}$$_{Q}$-LIND* proves (V6)iV(|&|,6). From this last formula, the existence condition for *LenP* follows without further use of induction.

The uniqueness condition for the *LenMinus* function follows from *BASIC* without any induction. The proof of the existence condition for *LenMinus* is exactly like the proof on page 42 of [2] except that *P(y)* is replaced by *LenP(y, a).* Note that the induction used becomes *Y>$^{h}$$_{Q}$-LIND* since *LenP(y, a) has* a SQ defining equation and its value is ≤ *\a\.* •

**Lemma 3** ***BASIC + Tl^-PIND* h *TV\-LIND.***

**Proof:** Follow exactly the proof of the Theorem 2.6 of [2] except let *A* G IlJ. •

**Lemma 4** ***BASIC + U^LIND* h *Y\-LIND.***

**Proof:** This lemma is proved by essentially the same method as Theorem 2.11 of [2] (which emulates earlier proofs of analogous results in Peano arithmetic). For completeness sake, we nonetheless sketch the proof.

Let *A(b) e* Sj. To prove the *E^-LIND* axiom for *A,* we suppose that *A(0)* and *(Wx)(A(x)* D *A(x* + 1)) hold and reason informally in *BASIC* + *H^-LIND.* The idea is to let *B(b,c)* be the formula -»A(|c| ^- 6) and to use LIND induction on $B(b,c)$ with respect to $b$. The $\dot{-}$ symbol denotes restricted subtraction and is actually expressed using *LenMinus* as $\Sigma_0^b$-defined in Lemma 2. Hence $B$ can be expressed as a $\Pi_1^b$-formula. Now $BASIC + \Pi_1^b$-*LIND* can prove:

$$A(0) \leftrightarrow \neg B(|c|, c)$$

$$A(|c|) \leftrightarrow \neg B(0, c)$$

$$(\forall x < |c|)(A(x) \supset A(x+1)) \supset (\forall x < |c|)(B(x,c) \supset B(x+1,c))$$

From the third formula and our hypothesis about $A$, $\Pi_1^b$-*LIND* applied to $B$ yields $B(0,c) \supset B(|c|,c)$. From this and the other two formulas, we get $A(0) \supset A(|c|)$. From the assumption that $A(0)$ holds and since $c$ is an arbitrary free variable, it follows that $(\forall x)A(|x|)$ holds. □

**Lemma 5** *The theory $BASIC + \Sigma_1^b$-LIND can $\Sigma_1^b$-define the following functions and $\Delta_1^b$-define the following predicates:*

(1) $\mathit{SubPower2}(a) \iff S(|a|) = |S(a)|$.
*That is, $\mathit{SubPower2}(a)$ holds iff $a+1$ is a power of two.*

(2) $c = \mathit{SubExp}(a,b) \iff \mathit{SubPower2}(c) \land |c| = \min(|b|, a)$.
*That is, $\mathit{SubExp}(a,b) = 2^{\min(|b|,a)} - 1$.*

(3) $c = \mathit{Exp}(a,b) \iff c = 2^{\min(|b|,a)}$.

(4) $c = \mathit{Decomp}(a,b,c,d) \iff |c| \le b \land a = d \cdot 2^{\min(|a|,b)} + c$.
$c = \mathit{LSP}(a,b) \iff (\exists d \le a)\mathit{Decomp}(a,b,c,d)$.
$d = \mathit{MSP}(a,b) \iff (\exists c \le a)\mathit{Decomp}(a,b,c,d)$.

*Furthermore, elementary properties of these functions and predicates are provable in this theory.*

**Proof:** (1) Obviously *SubPower2* is $\Delta_1^b$-defined. Also *BASIC* can prove the following properties (for example):

(i) $\mathit{SubPower2}(a) \supset \mathit{SubPower2}(S(a+a))$,

(ii) $\mathit{SubPower2}(a) \land |b| \le |a| \supset b \le a$,

(iii) $\mathit{SubPower2}(a) \wedge \mathit{SubPower2}(b) \wedge |a| = |b| \supset a = b$,

(iv) $\mathit{SubPower2}(a) \supset \mathit{SubPower2}(\lfloor \frac{1}{2}a \rfloor)$.

(2) The existence and uniqueness properties of the $\Sigma_1^b$-definition of *SubExp* are proved analogously to the proof of paragraph (d), page 39 of [2]. Note that only $\Sigma_1^b$-*LIND* is used for the existence proof.

(3) *Exp* is easily definable from *SubExp*. (4) The existence and uniqueness properties of the definitions of *LSP* and *MSP* are proved by the same argument as used in [2] — note that this used only $\Sigma_1^b$-*LIND*. □

**Lemma 6** *BASIC* + $\Sigma_1^b$-*LIND* $\vdash$ $\Sigma_1^b$-*PIND*.

**Proof:** This proof is exactly the same as the proof of Theorems 2.11 and 2.12 of [2], noting that Lemmas 2 and 5 imply that the function

$$a, u \mapsto MSP(a, |a| \dot{-} u)$$

is $\Sigma_1^b$-definable in *BASIC* + $\Sigma_1^b$-*LIND*. □

Recall that [2, Theorem 2.6] showed that *BASIC* + $\Sigma_1^b$-*PIND* $\vdash$ $\Pi_1^b$-*PIND*. Thus, the above sequence of lemmas clearly implies Theorem 1; namely that the following four theories are equivalent:

(1) *BASIC* + $\Sigma_i^b$-*PIND*

(2) *BASIC* + $\Sigma_i^b$-*LIND*

(3) *BASIC* + $\Pi_i^b$-*PIND*

(4) *BASIC* + $\Pi_i^b$-*LIND*

Theorem 1 allows us to prove that Theorem 4.9 of [2] applies to $S_2^1$ and $T_2^1$ (see also the comment on page 81 of [2]):

**Theorem 7** *Let $i \geq 1$ and $S_2^i$ and $T_2^i$ be axiomatized using $\Sigma_i^b$-LIND and $\Sigma_i^b$-IND, respectively. If $\Gamma \longrightarrow \Delta$ is a bounded sequent provable in $S_2^i$ or $T_2^i$, then there is a proof of $\Gamma \longrightarrow \Delta$ in that theory which has no free cuts, is in free variable normal form and is restricted by parameter variables.*

# 3 Unprovability of consistency for the first order theories

In this section, we prove that $S^\wedge$ does not prove the consistency of the fragment $5J^1$ for proofs which contain only $B\backslash$-formulas, with $5J^1$-proofs encoded in the standard efficient coding of the syntax of the language L& (see [2]). Thus, expressions like terms, formulas, sequents or proofs are coded by sequences containing the Gödel numbers of the symbols in these expressions. For any such expression A, we denote by /(A) the length of its code, i.e. $/(A) = |{}^{r}A^{n}|$. Thus, /(A) is proportional to the sums of the lengths of the codes of the symbols occurring in A.

By Theorem 1, we may assume that $S^{x}_2$ is axiomatized by *Y^-LIND.* We first must define the notion of a *supplemented proof,* which is similar to the notion of a "proof restricted by parameter variables" used in [2], and the notion of a normal proof used by Takeuti in [10]. A term of the language *Lb* is a *polynomial* if it does not contain the smash function #; if it also does not contain any free variables we call it a *closed polynomial.* The next lemma shows that the lengths of terms can be polynomially bounded; this will help us to apply the speed-up induction technique below.

**Lemma 8** *Let $t(\vec{x})$ be an arbitrary term of Lb with k variables. Then, there exists a polynomial $p^*_t$ such that*

$$S_2^- \vdash |t(\vec{a})| \leq p^*_t(|\vec{a}|). \tag{1}$$

$$S_2^- \vdash \left(\bigwedge_{i<k}(a_i \leq b_i)\right) \supset \text{tf}(|S|) \_< \vec{K}(H)- \tag{2}$$

Recall that $S^-_2$ is the equational theory axiomatized by BASIC, including the two extra axioms.

**Proof:** We define a suitable polynomial by induction on the complexity of the term $t(\vec{a})$.

1. $lit(a)$ is a, then $p^*_t(|a|)$^$|a|$;

2. iff is 0, then $p_t^* \stackrel{df}{=} 0$;

3. if $t(\vec{a})$ is $S(h(\vec{a}))$, then tf $(|\vec{a}|) \stackrel{*}{=}$ ^$(|S|) + 1$;

4. if $t(\vec{a})$ is $\lfloor \frac{1}{2} t_1(\vec{a}) \rfloor$ or $|t_1(\vec{a})|$, then $p^*_t(|\vec{a}|) \stackrel{df}{=} p^*_{t_1}(|\vec{a}|)$;

5. if $t(\vec{a})$ is $t_1(\vec{a}) + t_2(\vec{a})$, then $p^*_t(|\vec{a}|) \stackrel{df}{=} p^*_{t_1}(|\vec{a}|) + p^*_{t_2}(|\vec{a}|)$;

6. if $t$ is $t_1 \cdot t_2$, then $p^*_t(|\vec{a}|) \stackrel{df}{=} p^*_{t_1}(|\vec{a}|) + p^*_{t_2}(|\vec{a}|)$; and

7. if $t$ is $t_1 \# t_2$, then $p^*_t(|\vec{a}|) \stackrel{df}{=} (p^*_{t_1}(|\vec{a}|) \cdot p^*_{t_2}(|\vec{a}|)) + 1$.

By using induction on the complexity of the term $t$, it is easy to see that $S_2^-$ can prove both (1) and (2). The induction step in the cases for $\cdot$ and $|\,|$ uses the extra BASIC axioms $|a \cdot b| \leq |a| + |b|$ and $|a| \leq a$.

**Definition:** Let $P(\vec{a})$ be a proof in a fragment of bounded arithmetic $S_2$ in which all formulas are bounded, with parameter variables $\vec{a}$ and eigenvariables $b_0, \ldots, b_n$. For each eigenvariable $b_j$ of either an instance of an induction rule or a quantifier rule, let the corresponding principal term be $t_j(\vec{a}, b_1, \ldots, b_{j-1})$, for $j \leq n$. Let $\mathcal{Q} = \{Q_j | j \leq n\}$ be a set of equational proofs in the theory $S_2^-$ which use only structural rules and the cut rule. Thus, we can assume that in such proofs all variables are parameter variables. Then the set $\mathcal{Q}$ is a set of *supplementary proofs* for the proof $P(\vec{a})$ provided:

> For every principal term $t_j(\vec{a}, b_0, \ldots, b_{j-1})$, there is a polynomial $p_j(|\vec{a}|)$, and a proof $Q_j \in \mathcal{Q}$ which is a proof of the sequent
>
> $$|b_0| \leq p_0(|\vec{a}|), |b_1| \leq p_1(|\vec{a}|), \ldots, |b_{j-1}| \leq p_{j-1}(|\vec{a}|) \longrightarrow |t_j(\vec{a}, b_0, \ldots, b_{j-1})| \leq p_j(|\vec{a}|).$$

**Lemma 9** *For every bounded proof $P(\vec{a}, b_0, \ldots, b_k)$ in $S_2^i$ there exists a set $\mathcal{Q}$ of supplementary proofs in $S_2^-$.*

**Proof:** By induction on the complexity of the term $t$; we just take the natural candidate $p_j(|\vec{a}|) \equiv p^*_{t_j}(|\vec{a}|, p_0(|\vec{a}|), \ldots, p_{j-1}(|\vec{a}|))$ and use the monotonicity of polynomials, which is provable in $BASIC$. □

**Definition:** A *supplemented* $B_i^b$-proof of $S_2^i$ is a pair $\pi \equiv \langle P, \mathcal{Q} \rangle$ such that $P$ is a proof in $S_2^i$ which contains only $B_i^b$-formulas and $\mathcal{Q}$ is a set of supplementary proofs for $P$.

Unfortunately, the construction from Lemma 9 is not formalizable (with the coding of the syntax we use) in any theory whose provably total functions have polynomial growth rate. The reason is that, due to the possible multiple occurrences of a variable $a$, the substitution of the variable $a$ in the term $t_1(a)$ by a term $t_2$ can result in a term whose length is approximately equal to the product of the lengths of terms $t_1$ and $t_2$. Thus, we cannot freely iterate substitution of terms, since the lengths of the resulting terms do not grow polynomially in the number of iterations of substitution. Consequently, $S_2^i$ cannot prove that for every bounded proof there exists a set $\mathcal{Q}$ of supplementary proofs. This is why Takeuti [10], in order to show that $T_2^i$ does not prove the consistency of $S_2^{-1}$ for proofs in which all formulas are either $\Sigma_{i+5}^b$ or $\Pi_{i+5}^b$, first proves that $T_2^i$ does not prove the consistency of itself for proofs in which all formulas are either $\Sigma_{i+5}^b$ or $\Pi_{i+5}^b$ and for which *there exists* a supplementary proof. Using a method from [1] and a (formalized) conservativeness result, we will avoid proving the second incompleteness theorem for the notion of consistency of supplemented proofs.

We prove (and show that it can be formalized in $S_2^1$) the above mentioned conservativeness result as Theorem 12 below. For this purpose we first develop the speed-up induction method for the first order theories which extend (or prove) axioms of $BASIC$. We associate with each bounded formula $A^0$ several corresponding formulas in a manner similar to Solovay's cut shortening technique.

**Definition:** Let $L$ be a first order language extending $L_b$, $A^0(d,\vec{e})$ an arbitrary formula and $t(\vec{e})$ an arbitrary term of the language $L$ (from now on we will suppress in our notation all free variables, e.g., $\vec{e}$, which are not essential for keeping track of our constructions). Then we define

$$A^1(a) \equiv (\forall y \leq |t|)(\forall x \leq |t|)(y \leq x \wedge (x \leq y + a) \wedge A^0(y) \supset A^0(x))$$

$$A^2(c) \equiv (\forall z \leq |t|)(\forall w \leq |t|)(w \leq z \cdot c \wedge A^1(z) \supset A^1(w))$$

Note that $A^1$ and $A^2$ have the same quantifier complexity as $A^0$ in the hierarchy of formulas $B_i^b$.

**Definition:** A $B_i^b$ proof is a sequent calculus proof in which every formula is in $B_i^b$.

**Lemma 10** *Let* $A^0$ *be an arbitrary formula of the language L. Then the following formulas are provable in* S^"$^1$ *with B\ proofs which involve no free variables (and thus no eigenvariables) other than those appearing in the formulas being proved:*

$$\mathbf{(6 \leq a)\ A\ A\backslash a)\ D\ A^1(6)\ A\ A^1\{2 - a)} \tag{3}$$

$$\mathbf{(6 \leq c)\ A\ A^2(c)\ D\ A^2(b)\ A\ A\backslash c^2)} \tag{4}$$

$$A^2(0) A A^2(l) A A^2(2) \tag{5}$$

$$A^2(_{Cl})\ A\ A\backslash c_2)\ D\ A^2(_{Cl} \bullet c_2)\ A\ A^2(_{Cl} + c_2) \tag{6}$$

$$\mathbf{(Vx \leq \backslash t\backslash)(A°\{x)\ D\ A°(x + 1)) \sim A\backslash l)} \tag{7}$$

$$\mathbf{A\backslash c)\ A\ (c \geq \backslash t\backslash)\ A\ (Vx \leq |i|)(A°(x)\ D\ A°(x + 1))\ D\ (A°(0)\ D\ A°(|i|))} \tag{8}$$

**Proof:** The first conjunct of the conclusion of (3) follows from the elementary properties of + and • with respect to $\leq$, contained among the axioms of the theory *BASIC*. To show the second part, we consider arbitrary x, y, *a* such that $V \leq$ £ 5? *V* + 2a. If x $\leq$ y + a we apply $A^x(a)$ once; if x > j/ + a we apply $A^x(a)$ twice, once on *y* and j/ + *a* and once on y + *a* and x. The proof of (4) is similar; if *z* • c < *w* $\leq$ *z* • $c^2$, we consider the intermediate point z • c. In the formula (5) the first two conjuncts are trivial and the third one is equivalent to (3). To prove statement (6), we notice that if *C*\ $\leq c_2$ then *c*\ • $c_2 \leq$ c^ A *c*\ + $c_2 \leq 2 \bullet c_2$ and so this statement follows from (4) and (5). Formula (7) is an immediate consequence of the definition of $A^1(l)$. Notice that formula $A^1(a)$ contains the conjunct $y \leq x$ in the premise of the implication because the formula *A°(d)* need not define an initial segment; on the other hand, such a conjunct is not needed in $A^2(c)$, because $A^1(a)$ always does define an initial segment: if *A°(a)* satisfies (Vx < |i|)(A°(x) D A°(x + 1)) then $A^x(a)$ defines a cut containing 1 and closed for addition, while if this property fails then $A^1(a)$ defines just the singleton {0}. Finally, to prove (8), we note that by (4), $A^2(c)$ A (c $\geq$ |t|) implies $A^2(|i|)$. Thus, instantiating the universal quantifiers in $A^2$ with *z* = 1 and *w* = |i|, we get $A^x(l)$ *D* $A^l(\backslash t\backslash)$. Since $A^x(l)$ is equivalent to (Vx $\leq$ *\t\)(A°(x) D* A°(x + 1)), this implies $A^1(|i|)$. Instantiating universal quantifiers in $A^1(|<|)$ with *y* = 0 and *x* — *\t* we get A°(0) D A°(|t|) which clearly implies our claim. •

The above proofs are uniform in $A^0$ in the following sense. Each of them can be obtained from a single proof containing a new predicate symbol *U* in all places where formula $A^0$ appears by replacing *U* by the formula $A^0$. Consequently, the sizes of the proofs of all formulas from Lemma (10) are linear in the length of the formula $A^0$. This fact has the following important consequence.

Corollary 11 *The following statement is provable in S% - There is a quadratic polynomial $Pi_nd\{x,y,z)$ such that, if t is an arbitrary term of Lb, r is a closed polynomial and A(x) is an arbitrary B\ -formula of Lb, then there is a B\ proof* £(£,T, *A) in* $S2^1$ *of the formula*

$$(1*1 \leq r) \text{ D } ((V* \leq |*|)(A°(x) \ D \ A°(x + 1)) \text{ D } (A°(0) \text{ D } A°(|*|))) \qquad (9)$$

*such that* /(*(*, r, *A))* $\leq$ jw(/(t), /(r), *1{A)).*

**Proof:** Since r is built using only 0,1,+ and •, by induction on subterms of r one can prove that using less than /(r) instances of (5) and (6), together with their corresponding proofs, one can obtain a proof of $A^2(r)$ of length bounded by a quadratic polynomial p*(|$^r$r$^n$|, |$^r$A$^n$|). We combine this proof with a proof of the instance of (8) for $c = r$; such an instance has a proof linear in /(A), *l(t)* and /(r). Thus, the length of the whole proof *8(t,* r, A) of (9) can be bounded by a quadratic polynomial, and since this argument is by induction on a parameter bounded by the length of the term r, clearly it can be proved in *S]* using *Y,\-LIND.* •

As an aside, we note that the previous lemma cannot be used for equational theories since the formulas $A^1$ and $A^2$ involve quantifiers; nonetheless, in section 4, we shall prove an analogue of Lemma 10 using a different construction.

Let *T* be a theory of the language Z^; then *B\-PrfT(p,y>)* denotes a formalization (in the usual way for the theories of bounded arithmetic - see [2]) of the notion "P is a proof of *(p* in *T* and *P* contains only *B* formulas", with the corresponding predicates *B\-ThrriT(<p)—= (3x)B$^f$--PrfT(x,cp)* and $B^h{}_rCon(T) \equiv$ *^-Thrn$_T$($^r$0 = V).*

Theorem 12 *Let ip(a) be a B\ formula such that* $S^x{}_2$ h Vxy?(x). *Then there are numbers m, n such that for the term r(x)* = $(x\#(x\#x))^m + n$

$$S] \text{ h } Vx3w\_ < T(x)B^h{}_rPrf_s\text{-}i\{w,{}^rip(xy).$$

Note that Theorem 12 depends on the presence of the two extra *BASIC* axioms.

**Proof:** We first apply the (partial) cut elimination procedure to an *S*\-proof of y(a), and obtain a free cut free proof *P(a)* of y>(a). This proof is clearly a *B* proof. By Lemma 9 there are supplementary proofs *Q* for *P{a).* Let the eigenvariables of *P(a)* be 6Q, ..., $6_n$. We now argue informally, but it will be clear that the argument can be carried out in *S].* We first fix a value for *x* and replace the free variable $a$ in the proof $P(a)$ and in the proofs in $Q$ by the numeral $\underline{x}$. The length of the proof $P(\underline{x})$ is then linear in \x\. Since $P(\underline{x})$ is a proof of a sentence, $P(\underline{x})$ has no parameter variables. Thus, for every principal term ifc(6o, • • -, &fc-i) , $k \leq$ n, the corresponding polynomial p* is now a closed term built using only +, •, the numerals 0,1, and \x\. Consequently, for each $k \leq$ n, the proof $Qk$ is a proof of the sequent

**M ≤Po,|&i| ≤Pi,...,|6jb-i| ≤ Pib-i—>|ifc(6o,...,6fc-i)| ≤*Pk***

**Claim:** There exists a polynomial $p(x,y)$ such that for every sub-proof $D(b_0,\ldots$ ,6fc-i) of the proof P with the endsequent II—>A there exists a $B$\-proof £>* in $S^{\wedge 1}$ such that ID*! $\leq$ *p(\D(b)l \Q\)* and £>* has the endsequent:

M ≤Po, **|6i|** ≤ Pi, •.., |&*-i| ≤ **p*-i, n—>A**

**Proof:** We proceed by induction on the height of subderivations $D$ of P. Consider the last inference of Z). If Z? is just an initial sequent F—>A, let $D^*$ be a proof of

N ≤Po, |6i| ≤ Pi, •. •, |&*-i| ≤ *Pk-i,* T - ^ A .

JD* consists of an axiom and weakenings and is easily seen to have length |JD*| ≤ \P\ + \Q\ - So our estimate follows for any p(x, $y) \geq x + y$.

If $D$ is not just an axiom, let the immediate subderivation(s) of $D$ be $D$\ (or, $Di$ and $Z?_2$)• The cases in which the last inference is a propositional or a cut rule, the claim is an easy consequence of the induction hypothesis. If the last inference is by an existential quantifier rule of the form

$$\frac{\Gamma \longrightarrow \Delta, A(s)}{s \leq t, T \longrightarrow A, (\exists x \leq t)A(x)}$$

the claim again follows easily from the induction hypothesis. The case where the last inference of $D$ is an V ≤: *left* inference is similar.

Now assume that the last inference of $D$ is is an application of the V ≤: *right* rule of the form

$$\frac{h \leq t_k(\vec{b}), r \longrightarrow A, A(b_k)}{\Gamma \longrightarrow \Delta, (\forall x \leq t_k(\vec{b}))A(x)}$$

where $b$ is the sequence $60, \ldots, b_k$-\. By the induction hypothesis there is a $B$\ -proof $D$\ in $S2^1$ of the sequent

s*-i, N ≤ $p_k$, $h \leq t_k(b)$, r -^A, $A\{h)$

with $|D_1^*| \le p(|D_1|, |\mathcal{Q}|)$, where $\Sigma_{k-1}$ denotes the cedent

$$|b_0| \le p_0, |b_1| \le p_1, \ldots, |b_{k-1}| \le p_{k-1}.$$

Using an initial sequent expressing the transitivity of $\le$, we get a proof of

$$|b_k| \le |t_k(\vec{b})|, |t_k(\vec{b})| \le p_k \longrightarrow |b_k| \le p_k;$$

we now apply the cut rule on this and on the endsequent $\Sigma_{k-1} \longrightarrow |t_k(\vec{b})| \le p_k$ of the proof $Q_k \in \mathcal{Q}$ to get a proof of the sequent

$$\Sigma_{k-1}, |b_k| \le |t_k(\vec{b})| \longrightarrow |b_k| \le p_k.$$

Using once again a cut , with the initial sequent $b_k \le t_k(\vec{b}) \longrightarrow |b_k| \le |t_k(\vec{b})|$, we get a proof of

$$\Sigma_{k-1}, b_k \le t_k(\vec{b}) \longrightarrow |b_k| \le p_k.$$

With another cut against the endsequent of $D_1^*$, we obtain a proof of

$$\Sigma_{k-1}, \Gamma, b_k \le t_k(\vec{b}) \longrightarrow \Delta, A(b_k).$$

Finally, we use an application of the $\forall \le$: *right* rule and get the desired proof $D^*$ of

$$\Sigma_{k-1}, \Gamma \longrightarrow \Delta, (\forall x \le t_k(\vec{b}))A(x).$$

Notice that the number of lines in the proof $D^*$ which are not in the subderivations $D_1^*$ or $Q_k$ does not depend on either $D_1^*$, $Q_k$ or the endsequent of the proof $D_1$. The lengths of the sequents in the proof $D^*$ which do not appear in the subderivations $D_1^*$ or $Q_k$ are linear in the sum of the length of the endsequent of the proof $D$ and the length of the proof $Q_k$. Thus, if $p(x, y)$ is at least a quadratic polynomial with sufficiently large coefficients, the hypothesis that $|D_1^*| \le p(|D_1|, |\mathcal{Q}|)$ clearly implies that $|D^*| \le p(|D|, |\mathcal{Q}|)$. This finishes the case of the $\forall \le$: *right* rule. The case where the last inference in $D$ is an $\exists \le$: *left* inference is handled similarly.

The last remaining case is when the last derivation in $P$ is an application of the $\Sigma_i^b$-*LIND* rule,

$$\frac{A(b_k), \Gamma \longrightarrow \Delta, A(b_k + 1)}{A(0), \Gamma \longrightarrow \Delta, A(|t(\vec{b})|)}$$

We use our speed-up induction technique. Let $D_1$ be the immediate subderivation of $D$ with endsequent $A(b_k), \Gamma \longrightarrow \Delta, A(b_k+1)$. Let $\vec{b}$ and $\Sigma_{k-1}$ be the same as above. By the induction hypothesis, there is a proof $D_1^*$ of

$$\Sigma_{k-1}, |b_k| \leq p_k, A(b_k), \Gamma \longrightarrow \Delta, A(b_k+1)$$

such that $|D_1^*| \leq p(|D_1|, |\mathcal{Q}|)$.

Combining $D_1^*$ with the initial sequents $b_k \leq |t_k(\vec{b})|, |t_k(\vec{b})| \leq p_k \longrightarrow b_k \leq p_k$ and $b_k \leq p_k \longrightarrow |b_k| \leq p_k$ from the BASIC axioms, we get a proof of

$$\Sigma_{k-1}, |t_k(\vec{b})| \leq p_k, b_k \leq |t_k(\vec{b})|, A(b_k), \Gamma \longrightarrow \Delta, A(b_k+1).$$

Using a propositional inference and an $\forall \leq$ *:right* inference we get a proof $D_1^+$ of

$$\Sigma_{k-1}, |t_k(\vec{b})| \leq p_k, \Gamma \longrightarrow \Delta, (\forall x \leq |t_k(\vec{b})|)(A(x) \supset A(x+1)).$$

By Corollary 11, there is a $B_2^i$-proof $\delta$ in the theory $S_2^{-1}$ of

$$|t_k(\vec{b})| \leq p_k, (\forall x \leq |t_k(\vec{b})|)(A(x) \supset A(x+1)) \longrightarrow (A(0) \supset A(|t_k(\vec{b})|))$$

of length bounded by a quadratic polynomial in the length of terms $t_k$ and $p_k$ and the length of the formula $A(x)$. Using $D^+$ and $\delta$, and a few structural and propositional inferences, we get a proof of

$$\Sigma_{k-1}, |t_k(\vec{b})| \leq p_k, A(0), \Gamma \longrightarrow \Delta, A(|t_k(\vec{b})|).$$

We combine this proof with the proof $Q_k$ of $\Sigma_{k-1} \longrightarrow |t_k(\vec{b})| \leq p_k$, to get a proof $D^*$ of

$$\Sigma_{k-1}, A(0), \Gamma \longrightarrow \Delta, A(|t_k(\vec{b})|).$$

It is easy to see analogously to the above estimates that $|D^*| \leq p(|D|, |\mathcal{Q}|)$ if $p$ is a polynomial of degree 3 with sufficiently large coefficients.

That completes the proof of the Claim. Since the above argument is clearly formalizable in $S_2^1$ and since the size $|\mathcal{Q}|$ of the supplementary proofs is constant, we get that

$$S_2^1 \vdash \forall x \exists p \leq \tau(x) B_i^b\text{-}Prf_{S_2^{-1}}(p, \ulcorner \varphi(\underline{x}) \urcorner)$$

for some term $\tau(x) = 2^{c|x|^3} + c$ for $c$ a sufficiently large constant. This completes the proof of Theorem 12. □

Combining the above theorem with a diagonalization trick we mentioned before, we easily get the following, main result of this section.

**Theorem 13** *Let i* > 0. *Then* $S^{*}_{2}$ *\f B\-C<m{S?).*

**Proof:** Assume the theorem fails: let *1* — (x#x)#(x#x) and use Gödel's diagonalization lemma to obtain an *Lf,*-formula *xf>(a)* such that

S$^{*}_{2}$ h Va#(*) <> -«(3ti> ≤ *T)B$-Prfs-i* (to, ^(x)"$^{1}$)] (10)

Since ->V($^{X}$) *1S* a ^<$ formula, we have (see [2]) for a suitable term *t(a)*

*S]* h Vx[-^(x) D 3t; ≤ f(x)^-Pr/$_{s}$-$_{1}$(t;,$^{r}$-t/'(xr)].

Thus, for some term *r(x),* we have

5] h Vx[^(x) D 3u ≤ T(x)fi?-Pr/^-i(u,$^{r}$O = T)].

Consequently, *S^* h B$^{b}_{t}$—Con(5j$^{1}$) D *Vxrj)(x),* and so, since by our assumption that 5^ H ^-Con(5$_{2}$~$^{a}$) we get that 5j h *Vxxj>(x).* But then, by Theorem 12 we have for the term r(i) = (x#(x#x))$^{m}$ + n:

SJ h Vx3p ≤ *r(x)*$B^{b}_{i}$-$Prf_{S_2^{i-1}}(p, \ulcorner\psi(x)\urcorner)$

which contradicts (10), since for a sufficiently large number £,

*S* h Vx(fc ≤ x D (x#(x#x))$^{m}$ + n ≤ (x#x)#(x#x)). •

Since T^ C 5^$^{+1}$, Theorem 13 also implies that TJ does not prove $B^{b}_{i+1}$-$Con(S_2^{-1})$.

# 4 Equational Theories

The main result of this section is that *PV \f Con(PV~).* As already mentioned, we must develop a new speed-up induction technique for the equational theories, since it is necessary to avoid the use of quantifiers in the formulas constructed in speeding up induction. It turns out that the existence of supplementary proofs for arbitrary proofs will no longer be a problem (because of the presence of a function symbol for the squaring function), so we can now prove a formalized (partial) conservativeness result with a polynomial bound on the length of proofs.

Accordingly, our strategy will be somewhat different than in the case of the first order theories.

First we must specify the coding of the syntax of the language $L_p$. We take functions of $L_e$ as primitive, in the sense that they are not defined in terms of any other functions, and we assign to them Gödel numbers. For the function symbols of $L_p$ not in $L_e$ we distinguish the following cases.

1. If a function $f(\vec{a})$ is obtained by composition from the functions $h(\vec{b}), g_1(\vec{a}), \ldots g_k(\vec{a})$ then $f$ has Gödel number $\ulcorner f \urcorner = \langle \ulcorner h \urcorner, \ulcorner g_1 \urcorner, \ldots, \ulcorner g_k \urcorner \rangle$.

2. If a function $f(d, \vec{a})$ is obtained by limited recursion on notation from the functions $g(\vec{a})$ and $h(b, c, \vec{a})$ with the bounding function $k(b, \vec{a})$, then we set $\ulcorner f \urcorner = \langle \ulcorner g \urcorner, \ulcorner h \urcorner, \ulcorner k \urcorner \rangle$.

We assign Gödel numbers to arbitrary terms in the usual way, as it is done for the syntax of $S_2^1$; namely, a term is coded by the sequence containing the Gödel numbers of the symbols in the terms. Thus, if $f$ is defined by composition from $h, g_1, \ldots, g_k$ then $l(f) \geq l(h) + l(g_1) + \cdots + l(g_k)$; if $f$ is defined by limited recursion on notation from the functions $g$ and $h$ with the bounding function $k$, then $l(f) \leq l(g) + l(h) + l(k)$. We define a sequence of terms $sq^k(x)$ for $k \geq 0$ by $sq^0(x) = x$ and $sq^{k+1} = sq(sq^k(x))$, Note that the term $sq^k(sq^m(x))$ is identical to the term $sq^{k+m}(x)$. It is easy to see that $E^-$ can prove

$$x \leq sq^m(y) \wedge y \leq sq^k(z) \supset x \leq sq^{m+k}(z)$$

and that the length of this proof is quadratic in $k+m$. Formalizing in $PV$ yields:

**Lemma 14** *For every $n$, the sequence of terms $\{sq^i(a) \mid i \leq |n|\}$ can be defined by limited recursion on notation, and one can prove in in $PV$ by induction on $n$ that for every $n$ and every $k, m \leq |n|$, the above $E^-$-proofs of length quadratic in $n$ exist.*

**Lemma 15** *Let $t(a_0, \ldots, a_k)$ be an arbitrary $L_p$-term. Then $PV^-$ can prove*

$$\bigwedge_{i \leq k} (|a_i| \leq c) \wedge (1 < c) \supset |t(\vec{a})| \leq sq^{l(t)}(c).$$

*with a proof whose length is quadratic in $l(t)$.*

**Proof:** We first prove that Lemma 15 holds for every function $f \in L_p$. We proceed by induction on the complexity of the definition of $f$. If $f$ is defined by limited recursion on notation from the functions $g(\vec{a})$ and $h(b, c, \vec{a})$ with the bounding function $k(b, \vec{a})$, then, assuming $\bigwedge_{i<k}(|a_i| \leq c) \wedge (1 < c)$, by the inductive hypothesis, the properties of the function $sq(c)$ and the above-mentioned properties of our coding, $PV$ proves:

$$|f(\vec{a})| \leq |k(\vec{a})| \leq sq^{l(k)}(c) \leq sq^{l(f)}(c),$$

with a proof of length bounded by a quadratic function of $l(f)$. Similarly, if $f$ is defined by composition from $h, g_1, \ldots, g_k$ then $l(f) \geq l(h) + l(g_1) + \cdots + l(g_k)$. If $m = \max\{l(g_i) \mid 1 \leq i \leq k\}$, then again, assuming $\bigwedge_{i<k}(|a_i| \leq c) \wedge (1 < c)$, by the induction hypothesis and the properties of our coding, $|f(\vec{a})| \leq sq^{l(h)+m}(c)$, which clearly implies our claim.

Finally, if $t$ is an arbitrary term then $l(t) \geq l(f) + l(t_1) + \cdots + l(t_k)$ implies our claim exactly as in the previous case. □

**Lemma 16** *For all natural numbers $n$ there is a $E^-$ proof $p_n$ of length quadratic in $n$ of the inequality*

$$||sq^n(x)|| \leq \underline{n} + ||x||.$$

**Proof:** : Since $||sq^n(x)|| = ||(sq^{n-1}(x))^2|| \leq |2 \cdot |sq^{n-1}(x)|| \leq 1 + ||sq^{n-1}(x)||$, it takes $n$ iterations of the above inference in which every equality is of length linear in $n$. Thus $||sq^n(x)|| \leq \underline{n} + ||x||$ has a proof quadratic in $n$. □

Thus, we get the following useful consequence of the previous lemma.

**Corollary 17** *Let $t(a_0, \ldots, a_{k-1})$ be an $L_p$-term. The following inequality is provable in $PV^-$*

$$\bigwedge_{i<k}(|a_i| \leq c) \wedge (1 < c) \supset |||t(\vec{a})||| \leq \underline{l(t)} + ||c|| \tag{11}$$

*with a uniform proof of length quadratic in $l(t)$.*

The above facts allow us to prove in $PV$ the existence of supplementary proofs. We now develop the speed-up technique for equational theories.

For notational convenience, we let $2^x_{|y|}$ denote the function $Exp(x, y) = 2^{\min\{x, |y|\}}$. Let $A_0$ be an open formula; consider the following formula

$$A_0^*(z) \equiv (\forall y \leq t)(\forall y' \leq t)((y' \leq y) \wedge (y \leq y' + 2^z_{|t|}) \wedge A_0(y') \supset A_0(y)).$$

Let A^(z, *y*, *y')* denote the formula

$$(y \le t) \text{ A } (y^f\_ <y)/\backslash(y<y' + 2f_{t|}) \text{ A } A_0(y') \ D \ A_0(y)).$$

Lemma 18 *The following sentences are provable in PV{~:*

1. $(\forall x)(A_0(x) \supset A_0(x+1)) \supset A_0^*(0)$;
2. $(\forall z)(A_0^*(z) \supset A_0^*(z+1))$;
3. $A_0^*(|t|) \supset (A_0(0) \supset A_0(t))$.

The above lemma has a proof similar to the proof of Lemma 10.

Lemma 19 *Let $A_0(x)$ be an open formula, then there are polynomial-time computable functions $F^0_y(y,y\backslash z)$ and $F^0_{y'}\{y,y',z)$ such that, for $A^f_0$ as above, PV~ proves the following formulas*[4]

$$A[>(z,F^\circ_y(j/,y\backslash z),F^\circ_{y'}(y,y',z)) \ D \ A^\prime_0(z + l,F^\circ_y(y,y\backslash z + 1),F^\circ_{y'}(y,y',z + 1))$$

*and*

$$4(1*1, *J(y. \wedge 1*1). \wedge (y\wedge, 1*1) \wedge <(\backslash A,y,y')-$$

**Proof:** By Lemma 18.2 we have

$$PVf \ \backslash\text{- } \forall\bar{y}\forall F4(z,\bar{y},7) \ D \ \forall y\forall y'\wedge(\wedge + 1,y,y'). \tag{12}$$

Putting this in prenex normal form and applying Herbrand's theorem, there must exist terms $T_y(z,t/,y')$ and $T_yt(z,y,y')$ such that *PV~* proves

$$A'_0(z,T_y\{z,y,y'),T_{y'}\{z,y,y')) \ D \ A'_0(z+ l,y,y'). \tag{13}$$

It is, in fact, easy to explicitly construct the terms r and $r^7$, and they are uniformly defined in terms of $A_o$. In particular, the size of the terms r and r' and the size of the *PV~*-proof of (13) are linearly bounded by the size of the formula $A_o$; this fact can either be proved by direct construction, but also follows immediately from the fact *PV~*-proof of (12) used $A'_o$ only schematically. Let now $t^*$ be a

[4] The construction we present here significantly simplifies an older version of this proof; the idea for this simplification was suggested to us by Teddy Seidenfeld.

term such that |£*| $\geq$ (|i|, |i|). It is easy to see that using limited recursion on notation we can define a new function *F®{y, y', u)* such that

$$F^0_*(y, y', 0) = \langle y, y' \rangle,$$

and, for all $1 \leq u \leq |i|$,

$$\begin{aligned} F^\circ_*\{y,y\backslash_U) \quad &= \quad (r_v(M\wedge u, (F^0_*(y,y',u \dot- 1))_1, (F^0_*(y,y',u \dot- 1))_2), \\ & \qquad ry(\backslash t\backslash - u,(F?(y,y',u - 1))_{1f}\ (*?(?,\bullet,u \dot- 1))_2)); \end{aligned}$$

and, for all $u > |i|$,

$$F^0_*(y, y', u) = F^0_*(y, y', |t|).$$

Notice that we automatically have |i^(y, *y', u)* $\leq$ *t**\\, so *F?* is defined by limited recursion on notation. Let

$$\begin{aligned} F^\circ_y\{y,y',z) \quad &= \quad (F.^\circ(y,y',|i|- z))_1 \\ FZ(y,y',z) \quad &= \quad (F^0_*(y,y',|t| \dot- z))_2 \end{aligned}$$

Then *PV"* can prove that, for $z < |£|$,

$$\begin{aligned} F^0_y(y, y', z) &= (F^0_*(y, y', |t| \dot- z))_1 \\ &= \quad r_y(\backslash t\backslash - (|*| - z)),\ (F,^\circ(y, y', ((\backslash t\backslash - z) - 1))x, (F^0(y, y', ((|t| \dot- z) \dot- 1))_2) \\ &= \quad r,(|*| - (|*| - z)),\ (F.^\circ(y,y', (|t| - (z + 1)))),, (F^0(y, y', (|t| \dot- (z+1))))_2) \\ &= \quad T,(z_1 f;(y,y',z + 1), i5(y_>y',z + 1)) \end{aligned} \tag{14}$$

and similarly, *PV~* proves that, for $z < |t|$,

$$F2.(y,y',z) = T_y,(z,F2(y,_y',z + l),F^\circ_{y'}(y,y',z + l)). \tag{15}$$

Thus, substituting *x* by *F2(y,y',z* + 1) and y by $F^\circ_y$,(y,y',^ + 1) in (13), *PV~* can prove, for $z < \backslash t\backslash$,

$$A'_0(z, \tau_y(z, F^0_y(y, y', z+1), F^0_{y'}(y, y', z+1)), \tau_{y'}(z, F^0_y(y, y', z+1), F^0_{y'}(y, y', z+1)))$$

implies

$$A'_0(z+1, F^0_y(y, y', z+1), F^0_{y'}(y, y', z+1)),$$

which, together with (14) and (15), implies the first part of Lemma 19. The second part of Lemma 19 follows from the fact that $F^{\circ}_{y}$(y, y', \t\) = y and $F^{\circ}_{y'}$(y, y', \t\) = y'. Notice that functions $F^{\circ}_{*}$, $F^{®}_{y}$ and $F^{\circ}_{y}$, depend on the formula $A^0$, since they are defined using $r_y$ and $r_{y}$, which are obtained either from Herbrand's theorem or by direct definition using formula $A^0$.

If we set Ai(z,y,y') = A'0(z, $F^{\circ}_{y}$(y,y',2), F$(y,y',z)) then it is easy to check that the above implies:

$$PV\sim \text{ h } A\text{^}z\text{^}y')\ D\ A,\{z + l,y,y'); \tag{16}$$

$$A_0(x)\ D\ A_0(x + 1),\ PV\sim \text{ h } A_1(0,y_iy'); \tag{17}$$

$$PV"\ I\text{- } Axdtl.O,*)\ D\ (A_o(0)\ D\ A>(0)\text{-} \tag{18}$$

Note that in (17), we write Ao(x) D Ao(x +1) to the right of the turnstile, instead of (Vx)(Ao(x) D AQ(X + 1)) since we are using equational theories.

Iterating the above procedure twice more, we can form formulas A^w, z,z') and Ai(w, z, z') defined as follows: (recall that we are suppressing in our notation all the variables irrelevant for the construction)

$$A[\ \_\ =\_\ ((z<\underline{\backslash}t\backslash)A(z'<z)\underline{A}(z<z' + 2l\backslash_j)AA_1(z')DA_1(z))$$

$$A_2\ \_ = A'_x\{w,Fl\{z,z',w),F^l_{z},\{z,z',w))$$

Similarly, we define formula A^s, tu, w')

$$(w \_< \backslash\backslash t\backslash\backslash)\ A\ (\underline{N}/\ <W)A(W\underline{\leq}W' + 2f|_W||)\ A\ A_2(z')\ D\ A_2(z),$$

and finally formula $A_3$(u, w;, $w^1$) is

$$A'_2\{v,Fl\{w,w',v),Fl,\{w,w',v)),$$

where F}(z,z',w), F},(z,z',w)) and Fl(w,w',v), $F^{*}_{w}$(w,w',v)) are defined in the analogous way for A[ and $A'_2$ respectively as ⁰Fy(y,y',z), Fy,(y,y',z)) were defined for $A'_o$. It is easy to see that for all $i \leq 3$, and u,- = \t\, \\t\\ or |||t||| respectively, PV~ proves

$$(ui \leq u)\ A\ Ai(u, x, x')\ D\ Ai(ui, x, x') \tag{19}$$

$$(u \leq u')\ A\ (u' \leq u,\text{-})\ A\ A,\text{-}(u', i, x')\ D\ A;(u, x, x').$$

So, with proofs similar to those before, we have

$$PV^- \vdash A_2(w, z, z') \supset A_2(w+1, z, z') \tag{20}$$

$$A_1(x, y, y') \supset A_1(x+1, y, y'),\ PV^- \vdash A_2(0, z, z') \tag{21}$$

$$PV^- \vdash A_2(||t||, 0, |t|) \supset (A_1(0, y, y') \supset A_1(|t|, y, y')) \tag{22}$$

$$PV^- \vdash A_3(s, w, w') \supset A_3(s+1, w, w') \tag{23}$$

$$A_2(x, z, z') \supset A_2(x+1, z, z'),\ PV^- \vdash A_3(0, w, w') \tag{24}$$

$$PV^- \vdash A_3(|||t|||, 0, ||t||) \supset (A_2(0, w, w') \supset A_2(||t||, w, w')). \tag{25}$$

From (17) and (22) we get

$$A_0(x) \supset A_0(x+1), PV^- \vdash A_2(||t||, 0, |t|) \supset A_1(|t|, y, y') \tag{26}$$

Similarly (16) and (21) implies

$$PV^- \vdash A_2(0, z, z'), \tag{27}$$

which together with (25) implies that

$$PV^- \vdash A_3(|||t|||, 0, ||t||) \supset A_2(||t||, w, w'). \tag{28}$$

Instantiating (28) with $w = 0$ and $w' = |t|$ and using (26) we get that

$$A_0(x) \supset A_0(x+1), PV^- \vdash A_3(|||t|||, 0, ||t||) \supset A_1(|t|, y, y'). \tag{29}$$

Instantiating (29) with $y = 0$ and $y' = t$ and using (19) and (18), we get a proof of the following lemma.

**Lemma 20**

$$A_0(x) \supset A_0(x+1), PV^- \vdash (|||t||| \leq u) \wedge A_3(u, 0, ||t||) \supset (A_0(0) \supset A_0(t)).$$

Also, (20) and (24) imply

$$PV^- \vdash A_3(0, w, w'); \tag{30}$$

so, by instantiating (30) and (23) with $w = 0$ and $w' = ||t||$, we get a proof of the following lemma.

**Lemma 21**

$$PV^- \vdash A_3(0, 0, ||t||) \wedge (A_3(s, 0, ||t||) \supset A_3(s+1, 0, ||t||)) \tag{31}$$

The last two lemmas summarize all the properties of the formulas *AQ* and *A3* needed for our results for equational theories. Formulas *A* and *A2* are only auxiliary formulas needed to define and prove the properties of the formula A3 and its relationship to the starting formula *AQ* .

Definition: A sequent F—>*A* with all free variables among $a_0, \ldots,$ a^-i has *numerically restricted variables* if for every free variable $a_{J5}$ *j<_k* — 1 occurring in a formula in F there exists in F a formula of the form *\aj* < $sq^{nj}(2)$ for some natural number *rij.*

Clearly, any sequent of closed formulas is a sequent with numerically restricted variables; furthermore, any sequent can be made numerically restricted by introducing new formulas with weakening inferences. We are now ready to prove the main result of this section, i.e. that *PV \f Con(PV~).* Our proof is based on the following lemma.

Lemma 22 *There is a polynomial time transformation f such that, PV can prove that for every proof* $P(a_0, \ldots,$ a^_i) *in PV of a sequent* F—>A *with numerically restricted variables, f(p) is a PV~ proof of the same sequent.*

**Proof:** We shall prove, for an appropriate polynomial p, that if *P* is a *PV'* -proof of a sequent with numerically restricted variables, then there is a *PV~* -proof *P** of the same endsequent with $|P^*| \leq p(|P|)$. Our argument will be formalizable in *PV* and this automatically shows P* is polynomial time constructible from *P*. We proceed by induction on the height of the proof *P*, considering various cases depending on the final inference of *P*. The only non-trivial cases are when the last inference is either a substitution rule or an induction rule; thus, let Pi be the immediate subderivation of P and *S* the last sequent of P. Clearly $l(P_1) + l(S) \leq l(P)$.

If the last inference is a substitution rule, then we may assume without loss of generality that it is of the form

$$\frac{\Gamma \longrightarrow A(b)}{\Gamma \longrightarrow A(t(\vec{a}))}$$

where F contains formulas of the form *\aj* $\leq sq^{n_j}(2)$, for all $j < k$ and must not contain 6. As before, we can prove (with a short proof) in *PV~* that

$$\bigwedge_{j<k} (\text{hi} \leq c) \wedge (2 \leq c) \supset |t(\vec{a})| \leq s_q W(c). \qquad (32)$$

Let $m = \max\{n_0, \ldots, n_{k-1}\}$, and $s = l(t) + m$. Then $s \leq l(S)$. Substituting $c$ by $sq^m(2)$ in 32, we can obtain a short proof of $\bigwedge_{j<k}(|a_j| \leq sq^m(2)) \longrightarrow |t(\vec{a}) \leq sq^s(2)$, and then, since $n_i \leq m$ for $i < k$, also a proof of

$$|a_0| \leq sq^{n_0}(2), \ldots, |a_{k-1}| \leq sq^{n_{k-1}}(2) \longrightarrow |t(\vec{a})| \leq sq^s(2). \tag{33}$$

By applying a weakening inference to the proof $P_1$, we obtain a proof $P_1^*$ of the numerically restricted sequent

$$\Gamma, |b| \leq sq^s(2) \longrightarrow A(b).$$

So, by the induction hypothesis, there is a proof in $PV^-$ of length $p(|P_1^*|)$ of the same sequent. Using the substitution rule, we get a $PV^-$ proof of

$$\Gamma, |t(\vec{a})| \leq sq^s(2) \longrightarrow A(t(\vec{a})).$$

Finally, applying the cut rule to this and to (33), we get a $PV^-$ proof with the same endsequent as the original proof $P$.

Assume now that the last inference in $P$ was an application of the induction rule which, without loss of generality, is of the form

$$\frac{\Gamma, A(b) \longrightarrow A(b+1)}{\Gamma, A(0) \longrightarrow A(t(\vec{a}))}$$

and let $P_1$, $S$, $m$ and $s$ be as in the previous case. By using weakening inferences, we get a proof of

$$\Gamma, |b| \leq sq^s(2), b \leq t(\vec{a}), A(b) \longrightarrow A(b+1).$$

By the induction hypothesis there is a $PV^-$ proof $P_1^*$ of the same endsequent. As in the case of the first order theories, we can combine this proof with the proof of (33), to get a $PV^-$ proof of

$$\Gamma, b \leq t(\vec{a}), A(b) \longrightarrow A(b+1);$$

adding a few propositional inferences and applying basic properties of $\leq$, we can transform this proof into a $PV^-$ proof of

$$\Gamma, (b \leq t(\vec{a})) \supset A(b) \longrightarrow (b+1 \leq t(\vec{a})) \supset A(b+1)$$

Let $A_0(b)$ be the formula $(b \leq t(\vec{a})) \supset A(b)$. Then, by Lemma 20, there exists a $PV^-$ proof of

$$\Gamma, |||t||| \leq \underline{s}, A_3(\underline{m}, 0, |t||), A_0(0) \longrightarrow A_0(t(\vec{a})).$$

It is easy to see that there is a short proof that $A_0(t(\vec{a}))$ is equivalent in $PV^-$ to $A(t(\vec{a}))$, while $\neg A_0(0)$ is equivalent to $\neg A(0)$. Thus we get a short proof of

$$\Gamma, |||t||| \leq \underline{s+2}, A_3(\underline{s+2}, 0, ||t||), A(0) \longrightarrow A(t(\vec{a})). \tag{34}$$

Since $m$ equals the maximum of $n_0, \ldots, n_{k-1}$, Corollary 17 implies that

$$PV^- \vdash |a_0| \leq sq^{n_0}(2), \ldots, |a_{k-1}| \leq sq^{n_{k-1}}(2) \longrightarrow |||t(\vec{a})||| \leq \underline{l(t)} + ||sq^m(2)||.$$

Since $PV^-$ proves $||sq^m(2)|| = \underline{m} + ||2|| = \underline{m} + 2$ with a proof of length quadratic in $m$ (and consequently quadratic in $s$), it follows that there is a short $PV^-$ proof of

$$|a_0| \leq sq^{n_0}(2), \ldots, |a_{k-1}| \leq sq^{n_{k-1}}(2) \longrightarrow |||t(\vec{a})||| \leq \underline{s+2}.$$

Combining these two proofs we get a proof of

$$\Gamma, A_3(\underline{s+2}, 0, ||t||), A(0) \longrightarrow A(t(\vec{a})). \tag{35}$$

Using Lemma 21 we have $PV^- \vdash A_3(0, 0, ||t||)$ and

$$PV^- \vdash A_3(b, 0, ||t||) \supset A_3(b+1, 0, ||t||).$$

Instantiating the above formula with $b = \underline{0}, \ldots, \underline{s+2}$, and applying applying cuts $(s+2)$- many times, we get

$$PV^- \vdash A_3(\underline{M}, 0, ||t||). \tag{36}$$

Combining (35) and (36), we get

$$\Gamma, A(0) \longrightarrow A(t(\vec{a})). \tag{37}$$

From our estimates it is clear that the entire proof is of length polynomial in the length of the original proof $P$ and has the same endsequent.

This finishes the proof of Lemma 22. □

**Theorem 23** *PV \f Con{PV)*

**Proof:** Clearly, any proof of 0 = 1 would be a proof of a numerically restricted sequent. Thus, by Lemma 22

*PV* h *Prfpvip/0 = V) D Prfp*$_V$*-(f(pV0* = H-

In other words, *PV* h *Con(PV) D Con(PV).* Thus, since *PV \f Con(PV)* (see [5]), we get *PV \f Con(PV~).* •

**Concluding remark.** Our results are an effort towards answering the question of whether 52 proves the consistency of the *equational* theory S£". This question is clearly relevant for the search of sentences which would show that the hierarchy of theories *S%* ˙*$^s$ proper without any complexity assumptions.

# References


[1] S. R. Buss. Letter to P. Pudlák, July 1986.

[2]———, *Bounded Arithmetic,* Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[3]———, *Axiomatizations and conservation results for fragments of bounded arithmetic,* in Logic and Computation, proceedings of a Workshop held Carnegie-Mellon University, 1987, vol. 106 of Contemporary Mathematics, American Mathematical Society, 1990, pp. 57-84.

[4]———, *A note on bootstrapping intuitionistic bounded arithmetic,* in Proof Theory: A selection of papers from the Leeds Proof Theory Programme 1990, Cambridge University Press, 1992, pp. 149-169.

[5] S. A. COOK, *Feasibly constructive proofs and the propositional calculus,* in Proceedings of the 7-th Annual ACM Symposium on Theory of Computing, 1975, pp. 83-97.

[6] A. IGNJATOVIĆ, *Delineating classes of computational complexity via second order theories with weak set existence principles (I).* Technical report CMU-PHIL-22, November 1991.

[7] ——, *Induction in theories of bounded arithmetic*. In preparation.

[8] P. PUDLÁK, *A note on bounded arithmetic*, Fundamenta Mathematicae, 136 (1990), pp. 85–89.

[9] R. M. SOLOVAY. Letter to P. Hájek, August 1976.

[10] G. TAKEUTI, *Some relations among systems for bounded arithmetic*, in Mathematical Logic, P. Petkov, ed., Plenum Press, 1990, pp. 139–154.

Department of Mathematics
University of California at San Diego
La Jolla, CA 92130-0112
USA

Department of Philosophy
Carnegie Mellon University
Pittsburgh, PA 15213-3890
USA